E. Fried

ABSZTRAKT ALGEBRA – ELEMI ÚTON

Budapest, Műszaki Könyvkiadó, 1972

Э. Фрид

ЭЛЕМЕНТАРНОЕ ВВЕДЕНИЕ В АБСТРАКТНУЮ АЛГЕБРУ

Перевод с венгерского Ю. А. Данилова

Издательство «Мир»
Москва 1979

17.2.2
Ф88

Фрид Э.

Элементарное введение в абстрактную алгебру.
Ф88 Пер. с венгер. Ю. А. Данилова. — М.: Мир, 1979.
260 с. с ил.

Книга крупного венгерского математика посвящена одному из наиболее важных и бурно развивающихся разделов современной математики — абстрактной алгебре.

Написанная простым и доходчивым языком, она позволяет овладеть основными понятиями современной алгебры и рассчитана на студентов, инженеров и всех тех, чья работа или интересы связаны с математикой.

17.2.2

Редакция научно-популярной
и научно-фантастической литературы

1702020000
Ф $\frac{20202-187}{041(01)-79}$ 187—79

© dr. Fried Ervin, 1972
© Перевод на русский язык, «Мир», 1979

Оглавление

От переводчика 7
Предисловие 8

1. АБСТРАКТНАЯ АЛГЕБРА

Глава первая. ГРУППЫ И ПОЛУГРУППЫ 12

1. Группы подстановок 12
   1.1. Перестановки и подстановки 12
   1.2. Последовательное выполнение подстановок 14
   1.3. Разложение подстановок, циклы, транспозиции 20
2. Понятие группы 27
   2.1. Числовые примеры групп 27
   2.2. Другие примеры групп 31
   2.3. Определение группы 37
3. Свойства элементов группы 38
   3.1. Различные способы определения группы 38
   3.2. Тождества в группе 43
   3.3. Коммутативные группы 49
4. Теоретико-групповые конструкции 49
   4.1. Подгруппа группы 49
   4.2. Фактор-группа группы 59
   4.3. Прямое произведение групп 69
5. Отображение групп 71
   5.1. Изоморфизм групп 71
   5.2. Гомоморфные отображения 75
   5.3. Операции, осуществляемые гомоморфизмами 81
6. Полугруппы и автоматы 83
   6.1. Полугруппа, полугруппа с единицей, группа 83
   6.2. Свободные полугруппы с единицей 86
   6.3. Алгебраическая теория автоматов 88
7. Представления групп 90

Глава вторая. КОЛЬЦА, ТЕЛА И ВЕКТОРНЫЕ ПРОСТРАНСТВА 92

1. Кольца и тела 92
   1.1. Целые числа и многочлены 92
   1.2. Разложение на простые множители 99

2. Векторные пространства и модули 107
2.1. Свойства векторов и элементов 107
2.2. Пространства, порожденные векторами, линейная зависимость, размерность 117
2.3. Изоморфизм и прямая сумма векторных пространств 125
2.4. Модули 130

3. Однородные линейные отображения 132
3.1. Гомоморфизм векторных пространств 132
3.2. Операции над однородными линейными отображениями 138
3.3. Матрицы 143

4. Группы и кольца 153
4.1. Представления групп матрицами 153
4.2. Групповые алгебры 156

Глава третья. СТРУКТУРЫ. БУЛЕВЫ АЛГЕБРЫ 161

1. Структуры и операции над множествами 161
1.1. Операции над частями одного множества 161
1.2. Структуры, специальные структуры 167
1.3. Частично упорядоченные множества и структуры 171

2. Соотношения между структурами 179
2.1. Подструктура, гомоморфизм, прямое произведение 179
2.2. Идеал, примарный идеал, логические связки 182
2.3. Представления структур 187

Глава четвертая. ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ СОВРЕМЕННОЙ АЛГЕБРЫ 191

1. Общая алгебра, алгебраические структуры 191

2. Категории, гомологическая алгебра 193

2. РЕШЕНИЯ ЗАДАЧ

К главе первой 196
К главе второй 222
К главе третьей 242

3. КРАТКИЙ СЛОВАРЬ ТЕРМИНОВ

От переводчика

Мощь и красота идей и методов современной абстрактной алгебры общепризнаны, а сфера ее применения расширяется столь стремительно, что иногда поговаривают об «алгебраической чуме», охватившей не только математику, но и другие науки. Тем не менее основы абстрактной алгебры известны далеко не так широко, как они того заслуживают. Одна из причин этой несколько парадоксальной ситуации кроется в том, что в отличие от специальной литературы, рассчитанной на профессионала, учебная и в особенности научно-популярная литература по абстрактной алгебре чрезвычайно бедны.

Предлагаемая вниманию читателя книга венгерского математика Эрвина Фрида в какой-то мере восполняет этот пробел. Тщательно продуманная последовательность изложения, простые, но достаточно строгие доказательства, умение выделить главное и выразительные иллюстрации позволят читателю сравнительно легко войти в круг основных алгебраических структур, а многочисленные примеры и задачи помогут ему активно овладеть специфическими особенностями алгебраического мышления.

Тем, кто пожелает продолжить свое знакомство с одним из важнейших разделов современной математики, для более углубленного изучения абстрактной алгебры рекомендуем обратиться к таким руководствам, как «Лекции по общей алгебре» А. Г. Куроша (М., Наука, 1973) и «Алгебра» Б. Л. ван дер Вардена (М., Наука, 1976), в которых приведена обширная библиография.

Ю. Данилов

Предисловие

Успешная научно-исследовательская работа во второй половине двадцатого века немыслима без углубленного изучения той или иной узкой дисциплины. Соблюдение этого непременного условия приводит к тому, что специалисты в различных областях науки не понимают языка своих ученых коллег, даже если те трудятся «по соседству». Такое положение дел весьма прискорбно, так как разобщенность научных дисциплин лишает исследования благотворного влияния взаимосвязей, существующих между различными областями науки. Ущерб, наносимый узкой специализацией, в какой-то мере восполняют работы популярного или полупопулярного характера, предназначенные не для более подробного изложения результатов, имеющих наибольшее значение, а для ознакомления читателя с более широким кругом сведений. Решению именно такой задачи и посвящена эта книга.

Как уже упоминалось, в наши дни невозможно получить сколько-нибудь значительные результаты, не овладев основательно определенной областью знаний. Вместе с тем именно в наши дни проникновение методов одних наук в другие началось в невиданных ранее масштабах. В первую очередь это относится к математике, методы которой находят применение в языкознании, биологии, экономике и других науках. Но для использования в этих областях требуется совершенно «новая» математика. Математика нового типа необходима для современных вычислительных машин и физики элементарных частиц. Раньше большинство физических или инженерных задач сводили к «подходящему» дифференциальному уравнению, решение которого давало ответ на поставленный вопрос. (Если найти точное решение оказывалось невозможно, то удовлетворительных результатов удавалось достичь при помощи достаточно «хорошего» приближения.) В настоящее время общепринятые взгляды на решение задач претерпели изменения.

Вместо того чтобы, как прежде, рассматривать «индивидуальные» задачи, исследователи обратились к решению «массовых» задач. Например, в языкознании наряду с изучением структуры конкретных языков возник вопрос о выяснении общей структуры языков (стимулом для постановки такого вопроса послужили проблемы машинного перевода). При проектировании заводов было бы неразумно стремиться к чрезмерному разнообразию: гораздо целесообразнее сосредоточить внимание на возможностях, таящихся в типовом проектировании. При анализе работы математических машин было бы весьма неудобно привлекать для описания каждой машины все новые и новые принципы. Гораздо проще описывать вычислительные машины на основе некоторых общих признаков.

Ни в одном из перечисленных выше случаев исследователям не приходится прибегать к математике типа «дважды два — четыре». Гораздо чаще речь идет о том, чтобы, исходя из тех или иных свойств, принятых за основные, при помощи допустимых умозаключений вывести определенные следствия. (Вспомним хотя бы о языкознании, которое учит нас, как из тех или иных частей речи по определенным правилам строить грамматически допустимые предложения.) При проведении «доказательств» мы отвлекаемся от конкретных

особенностей основных свойств подобно тому, как в языкознании нас интересует не содержание, а лишь грамматическая правильность предложения. Намеченный выше подход к изучению различных областей науки называется *аксиоматическим методом*, а свойства, принятые за основные, — *аксиомами*.

В математике аксиоматический метод известен с незапамятных времен. Впервые он был применен в геометрии (в «Началах» Евклида), но в своем первоначальном варианте аксиоматический метод существенно отличается от сформулированных выше требований. Аксиоматизация геометрии понадобилась для того, чтобы выделить некоторый единичный объект (плоскость или пространство) из множества других объектов. Аксиоматизация, о которой говорилось выше, необходима для того, чтобы мы могли одновременно рассматривать многие, быть может, самые различные по своим свойствам объекты.

Внутри самой математики аксиоматические исследования нового типа впервые появились в абстрактной алгебре. Более того, можно с полным основанием утверждать, что они ознаменовали рождение абстрактной алгебры как науки. На вопрос «Что такое абстрактная алгебра?» ответить довольно трудно: абстрактная алгебра связана с другими разделами математики весьма прочными узами. Вероятно, проще всего на этот вопрос можно было бы ответить так: абстрактная алгебра представляет собой не что иное, как естественное развитие аксиоматического метода, которое занимается изучением операций, производимых над определенными элементами. Результаты, полученные в абстрактной алгебре, находят широкое применение в математике и других науках. Тем не менее возрастающее день ото дня значение абстрактной алгебры основано не на полученных результатах, а на развитых в этой области математики *методах*.

Для понимания книги, безусловно, необходима определенная математическая подготовка. Мы имеем в виду не столько знание фактического материала, сколько определенную культуру математического мышления. В нашей книге мы пытались показать, насколько «абстрактное алгебраическое мышление» отличается от «общематематического мышления». Особенностям последнего (в более или менее популярной форме) посвящено очень много книг. Три из них мы рекомендуем вниманию читателя особенно горячо: «Диалоги о математике» недавно скончавшегося выдающегося венгерского математика Альфреда Реньи (М., Мир, 1969), занимательную книгу Розы Петер «Игра с бесконечностью» (М., Просвещение, 1968), знакомство с которой вопреки несколько «легкомысленному» названию полезно не только для тех, кто не сведущ в математике, и, наконец, книгу Дьердя Пойа «Как решать задачу» (М., Учпедгиз, 1959), позволяющую читателю овладеть основами математического мышления. Названные нами работы не только позволят читателю подготовиться к чтению нашей книги, но и послужат прекрасным введением в изучение всей математики в целом.

В этой книге мы прежде всего намеревались показать, какие методы встречаются в абстрактной алгебре, какого типа задачи они позволяют решать и каково их происхождение. Важным звеном в осуществлении намеченной нами программы являются доказательства. В большинстве случаев их легко отличить от основного текста, так как они набраны петитом.

Мы отнюдь не намеревались рассматривать приложения алгебры, поскольку для этого потребовалось бы основательное знакомство с теми областями науки и техники, в которых применяются методы абстрактной алгебры. Для выполнения столь обширной задачи ограниченный объем нашей книги явно недостаточен. Тем не менее мы убеждены в том, что все читатели, от любознательных учащихся средних школ до инженеров, экономистов и математиков-неалгебраистов, найдут в книге немало интересного для себя.

Наибольшей простотой и наглядностью отличается первая глава, в которой вводится понятие группы в интерпретации, предусматривающей возможность дальнейшего развития. Для понимания этой части не требуется особой математической подготовки. Те примеры, в которых предполагается знакомство с комплексными числами, можно опустить, хотя разбор их, несомненно, будет способствовать лучшему усвоению материала.

Центральная тема второй главы — векторное пространство, играющее весьма важную роль в более новых приложениях математики, в первую очередь тех, которые возникли в связи с появлением цифровых вычислительных машин. В этой главе все вопросы рассмотрены главным образом «теоретически».

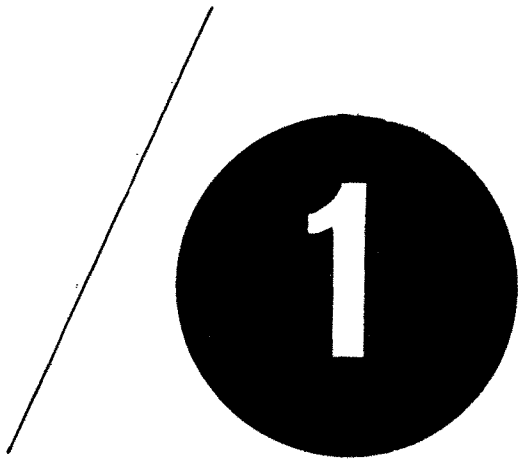
Третья глава посвящена множествам, над элементами которых производятся операции, совсем не похожие на обычные. Этим мы хотели подчеркнуть, сколь широким может быть диапазон операций в абстрактной алгебре. (В свое время считалось, что множества, наделенные «необычными» операциями, «не имеют смысла».)

Наконец, в четвертой главе приведен совсем краткий обзор «современной» алгебры. Разумеется, речь идет не о том, что те разделы алгебры, с которыми читатель познакомился в предыдущих главах, устарели. Мы хотели лишь показать, что проводимые ныне исследования можно рассматривать как новые самостоятельные разделы алгебры.

Мне доставляет особое удовольствие выразить свою признательность Дьюлане Олах за добросовестное редактирование и любовь, с которой она отнеслась к книге, а также Яношу Герцегу за забавные рисунки, как нельзя лучше передающие существо дела.

Автор

АБСТРАКТНАЯ АЛГЕБРА



Глава первая
Группы и полугруппы

1
Группы подстановок

1.1. Перестановки и подстановки

В популярных книжках и школьных учебниках математики часто встречаются разделы, посвященные комбинаторике и, в частности, перестановкам. Под перестановками некоторых элементов (чаще всего чисел) принято понимать все возможные способы, которыми эти элементы можно выстроить в ряд. Подсчет числа таких способов представляет собой задачу комбинаторики.

Ясно, что один-единственный элемент можно «выстроить в ряд» лишь одним способом. Если число элементов равно двум (например, если мы рассматриваем числа 1 и 2), то выстроить их в ряд можно двумя способами: 12 и 21. Числа 1, 2 и 3 можно выстроить в ряд следующими способами: 123, 132, 213, 231, 312 и 321. Всего их шесть. Все они различны, и других способов выстроить в ряд три элемента не существует. Действительно, на первом месте могут стоять только числа 1, 2 и 3, а два остальных числа в каждом из трех возможных случаев можно выстроить в ряд двумя способами. Аналогичный принцип позволяет подсчитать число перестановок из четырех элементов: 1, 2, 3 и 4. Любое из чисел 1, 2, 3 и 4 может стоять на первом месте, а число всех перестановок трех остальных чисел равно 6:

1234	2134	3124	4123
1243	2143	3142	4132
1324	2314	3214	4213
1342	2341	3241	4231
1423	2413	3412	4312
1432	2431	3421	4321.

Нетрудно видеть, что число перестановок из четырех элементов равно 24.

Число перестановок из четырех элементов мы получим, умножив число перестановок из трех элементов (равное 6) на 4 ($24 = 4 \cdot 6$). Шесть перестановок из трех элементов мы получим, умножив число перестановок из двух элементов (равное 2) на 3. Следовательно, число перестановок из четырех элементов можно представить в виде $24 = 4 \cdot 3 \cdot 2 \cdot 1$. Проводя аналогичные рассуждения, нетрудно показать, что число перестановок из пяти элементов равно $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ и т.д.

В общем случае число перестановок из n элементов равно произведению всех целых чисел от 1 до n. Это число принято обозначать $n!$ (читается: «эн факториал»).

Выполнение перестановок, или, иначе говоря, рассмотрение подстановок, выходит за рамки задач комбинаторики. О подстановке мы говорим в том случае, если, например, от перестановки 1432 требуется перейти к перестановке 3124.

Подстановка — это операция, изменяющая порядок элементов в перестановке.

В нашем примере

это — одна перестановка, а это — другая перестановка.

1432 → 3124

Если эту перестановку заменить этой перестановкой (замену можно обозначить горизонтальной стрелкой →), то получится подстановка.

Итак, подстановка приводит к замене каждого элемента исходной перестановки некоторым другим элементом (этот элемент может случайно совпадать с исходным). В рассмотренном выше примере подстановка приводит к замене 1 на 3, 4 на 1, 3 на 2 и 2 на 4. Если подстановку задавать простым перечислением всех производимых ею замен, то результат получится труднообозримым. Поступим иначе: запишем под каждым элементом исходной перестановки тот элемент, в который он переходит под действием подстановки. В этих обозначениях описанная выше подстановка будет иметь следующий вид:

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

Сама подстановка не зависит от того, в каком порядке выписаны пары, состоящие из элемента исходной перестановки и соответствующего ему элемента конечной перестановки. В рассмотренном выше примере элементы исходной перестановки можно расположить по номерам: 1 переходит в 3, 2 — в 4, 3 — в 2 и 4 — в 1. Следовательно, интересующую нас подстановку можно записать в виде

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

Что необходимо для того, чтобы подстановку можно было считать полностью заданной?

1. Необходимо задать всю совокупность элементов, над которыми производится подстановка, то есть конечное множество, называемое *областью определения подстановки*.

2. Необходимо задать *алгоритм подстановки*, то есть для каждого элемента, принадлежащего области определения подстановки, указать тот элемент, в который он переходит под действием подстановки, причем так, чтобы различные элементы при подстановке переходили в различные.

Две подстановки называются одинаковыми, если их области определения совпадают и каждый элемент, принадлежащий совместной области определения, они переводят в один и тот же элемент.

ПРИМЕРЫ

1. Уже рассмотренные нами подстановки $\begin{pmatrix}1&4&3&2\\3&1&2&4\end{pmatrix}$ и $\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}$ одинаковы, поскольку область определения каждой из них состоит из чисел 1, 2, 3, 4 и второе условие «равенства» подстановок также выполнено.

2. Подстановку, одинаковую с предыдущей, можно получить по следующему сложному алгоритму: «Рассмотреть натуральные числа, которые меньше 5. К тем из них, которые расположены на числовой оси левее числа 2,5, прибавить по 2, а остальные числа заменить разностями между числом 5 и числами, симметрич-

ными им относительно точки 2,5». Обе области определения, очевидно, совпадают. Второе условие одинаковости подстановок также выполнено, поскольку согласно приведенному рецепту 1 переходит в $1+2=3$, 2 — в $2+2=4$, 3 — в $5-3=2$ и 4 — в $5-4=1$.

3. Подстановки $\begin{pmatrix}1&4&3&2\\3&1&2&4\end{pmatrix}$ и $\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$ различны. Области определения их совпадают (более того, элементы нижней строки расположены в одном и том же порядке), но первая подстановка переводит, например, 4 в 1, в то время как вторая подстановка переводит 4 в 4.

4. Подстановки $\begin{pmatrix}1&4&3&2\\3&1&2&4\end{pmatrix}$ и $\begin{pmatrix}1&4&3&2&5\\3&1&2&4&5\end{pmatrix}$ также различны, хотя каждый элемент, который подвергается «перемещению», в обоих случаях переходит в один и тот же элемент: области определения этих подстановок не совпадают.

5. Алгоритм $\begin{pmatrix}1&2&3&4\\4&3&2&4\end{pmatrix}$ вообще не задает никакой подстановки, поскольку согласно ему числа 1 и 4 должны были бы переходить в одно и то же число 1.

6. О подстановке можно говорить (что часто и делают) и в случае бесконечных множеств. Но при этом уже недостаточно требовать, чтобы различные элементы переходили в различные. Рассмотрим, например, натуральные числа и вместо каждого из них запишем число, которое больше исходного на 2. У нас получится бесконечный алгоритм $\begin{pmatrix}1&2&3&4&5&\dots\\3&4&5&6&7&\dots\end{pmatrix}$. Видно, что некоторые натуральные числа отсутствуют. Поэтому в случае бесконечных множеств должно выполняться условие: в каждый из элементов должен переходить какой-то из элементов.

ЗАДАЧИ

Доказать следующие утверждения:

1. Если множества конечны, то условие, приведенное в примере 6, в действительности становится лишним, поскольку оно всегда выполняется.

2. Если множества бесконечны, то из условия, приведенного в примере 6, не следует, что различные элементы переходят в различные.

3. Если множества конечны, то из условия, приведенного в примере 6, всегда следует, что различные элементы переходят в различные.

1.2. Последовательное выполнение подстановок

Мы рассматривали подстановки как своего рода алгоритмы. Если у нас имеется не один, а несколько алгоритмов, то их можно выполнять последовательно, один за другим. Аналогично можно поступить и с подстановками.

Прежде всего выберем область определения подстановок: пусть это будет, например, множество чисел 0, 1, 2, 3 и 4. Рассмотрим две подстановки:

первую подстановку $\begin{pmatrix}0&1&2&3&4\\3&2&4&0&1\end{pmatrix}$

вторую подстановку $\begin{pmatrix}0&1&2&3&4\\2&3&4&0&1\end{pmatrix}$

Поскольку нам придется иметь дело с двумя подстановками, удобно их как-то назвать. Лучше всего говорить не о «первой» и «второй» подстановках, а обозначить каждую из подстановок так, как это принято в математике, особой буквой.

Пусть P — первая подстановка, а Q — вторая подстановка.

Посмотрим, что получится, если сначала мы выполним подстановку P, а затем подстановку Q.

Если выполнить подстановки не полностью, а частично, то получится следующее.

Подстановка P: $\begin{matrix}2&2\\4&\end{matrix}$
Подстановка Q: $\begin{matrix}4&1\\1&\end{matrix}$
После подстановки P выполнена подстановка Q.

Подстановка P: $\begin{matrix}0&1&2&3&4\\3&2&4&0&1\end{matrix}$ } Эти перестановки можно вычеркнуть.

Подстановка Q: $\begin{matrix}3&2&4&0&1\\0&4&1&2&3\end{matrix}$ }

Во что перейдет под действием подстановок любое из заданных чисел, можно определить, взглянув на числа, стоящие в нижних перестановках. Например, в подстановке P под числом 2 стоит число 4. Если после подстановки P требуется произвести подстановку Q, то необходимо выяснить, во что перейдет под действием подстановки Q число 4. Поскольку под ним стоит число 1, то после выполнения двух подстановок число 2 перейдет в 1.

Итак, элементы верхней строки подстановки Q удобно расположить в том же порядке, в каком они следуют в нижней строке подстановки P.

Выполнив сначала подстановку P, а затем подстановку Q, мы получим подстановку $PQ = \begin{pmatrix}0&1&2&3&4\\0&4&1&2&3\end{pmatrix}$.

Нетрудно видеть, что полученная подстановка имеет ту же область определения, что и подстановки P и Q. Содержащийся в подстановке PQ алгоритм всегда выполним (рис. 1).

Если после любой подстановки P выполнить подстановку Q, то получится подстановка, которая называется произведением подстановок P и Q и обозначается PQ.

Например, рассмотрим вместе с заданными выше подстановками P и Q подстановки PP и QQ.

Подстановку P можно представить в различных видах:

$$P = \begin{pmatrix}0&1&2&3&4\\3&2&4&0&1\end{pmatrix} = \begin{pmatrix}3&2&4&0&1\\0&4&1&3&2\end{pmatrix}.$$

Поскольку нижняя строка в первой записи совпадает с верхней строкой во второй записи, то верхняя строка произведения PP совпадает с верхней строкой первой записи, а нижняя строка — с нижней строкой второй записи:

$$PP = \begin{pmatrix}0&1&2&3&4\\0&4&1&3&2\end{pmatrix}.$$

Аналогичным образом можно построить и подстановку QQ:

$$Q = \begin{pmatrix}0&1&2&3&4\\2&3&4&0&1\end{pmatrix}$$
$$Q = \begin{pmatrix}2&3&4&0&1\\4&0&1&2&3\end{pmatrix}$$
} исключив эти строки, получим $\begin{pmatrix}0&1&2&3&4\\4&0&1&2&3\end{pmatrix}$.

Из того что последовательное выполнение подстановок называется умножением, может показаться, будто для этого «умножения» справедливы все правила обычного умножения. Посмотрим, так ли это.

Прежде всего выясним, как обстоит дело с коммутативностью, или переместительным законом, умножения подстановок. В обычном умножении (чисел) произведение не зависит от порядка сомножителей. Для умножения подстановок такое утверждение не верно! Чтобы убедиться в этом, достаточно привести один-единственный пример того, как изменение порядка сомножителей сказывается на произведении. Вернемся к рассмотренному выше примеру. Подстановка PQ уже известна. Найдем теперь подстановку QP:

$$Q = \begin{pmatrix}0&1&2&3&4\\2&3&4&0&1\end{pmatrix},$$

$$P = \begin{pmatrix}2&3&4&0&1\\4&0&1&3&2\end{pmatrix},$$

откуда

$$QP = \begin{pmatrix}0&1&2&3&4\\4&0&1&3&2\end{pmatrix}.$$

Эта подстановка заведомо отличается от подстановки PQ, поскольку, например, та переводит 3 в 2, в то время как в подстановке QP 3 переходит снова в 3.

Разумеется, в силу «случайного» стечения обстоятельств умножение подстановок может оказаться коммутативным. Например, подстановка PP не изменяется при перестановке сомножителей, поскольку оба сомножителя одинаковы.

Умножение чисел обладает еще одним весьма важным свойством —

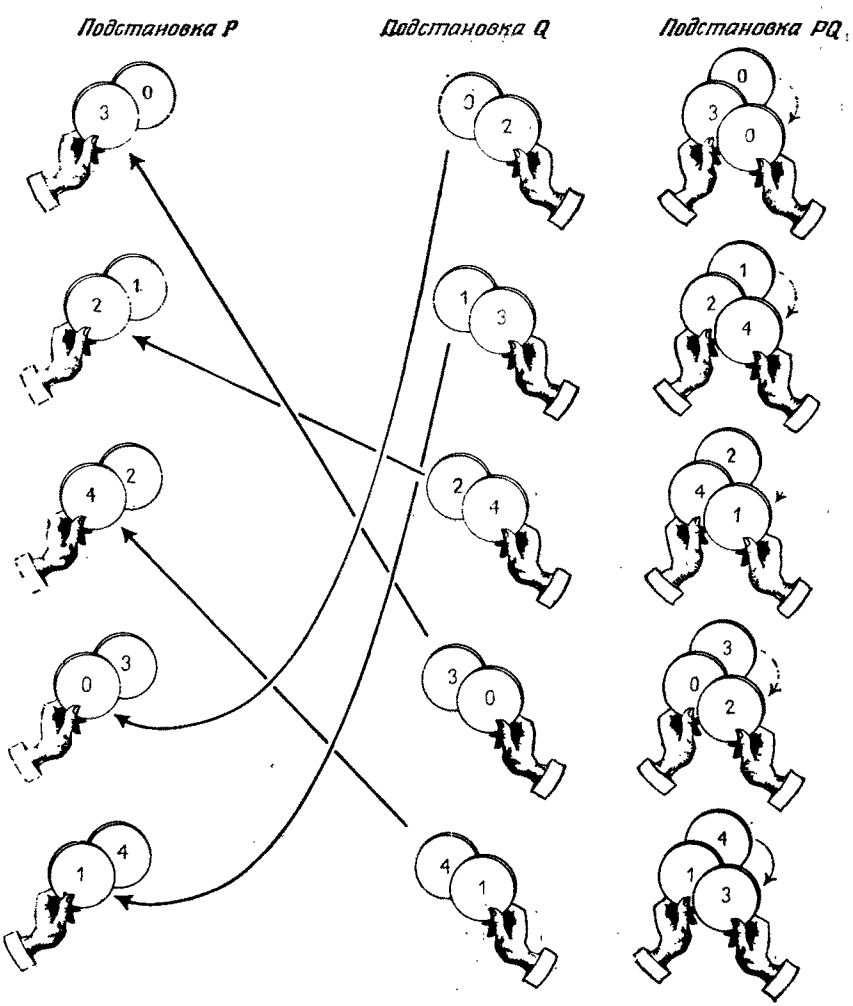


Рис. 1.

ассоциативностью, или сочетательным законом.

Ассоциативность означает, что произведение трех сомножителей не зависит от того, в каком порядке производится умножение: $a(bc) = (ab)c$.

Покажем, что это тождество выполняется при умножении подстановок. Рассмотрим три подстановки и обозначим их в том порядке, в котором они входят в произведение: A, B и C. Требуется доказать, что $A(BC) = (AB)C$.

Это равенство выполняется в том случае, если подстановки, стоящие в его правой и левой частях, имеют одну и ту же область определения и задаваемые ими «алгоритмы» совпадают. Поскольку подстановки A, B и C имеют одну и ту же область определения, области определения подстановок $A(BC)$ и $(AB)C$ совпадают. Совпадение алгоритмов обеих подстановок будет доказано, если мы убедимся в том, что обе подстановки всегда переводят любой элемент в один и тот же элемент.

Выберем произвольный элемент и обозначим его a. Предположим, что подстановка A переводит элемент a в элемент b, подстановка B переводит элемент b

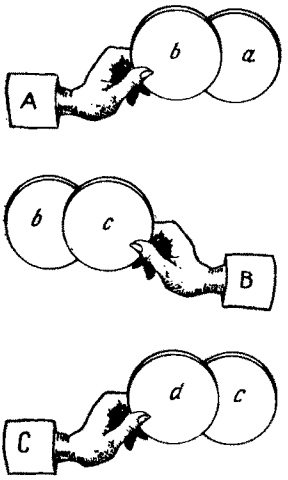


Рис. 2.

в элемент c и, наконец, подстановка C переводит элемент c в элемент d (рис. 2). Тогда подстановка AB переводит элемент a в элемент c, а подстановка BC переводит элемент b в элемент d (рис. 3).

Выполнив сначала подстановку A, а затем подстановку BC, или сначала подстановку AB, а затем подстановку C, мы придем к следующему результату:

элемент a в обоих случаях переходит в элемент d, а это и означает, что подстановки $A(BC)$ и $(AB)C$ в действительности совпадают (рис. 4).

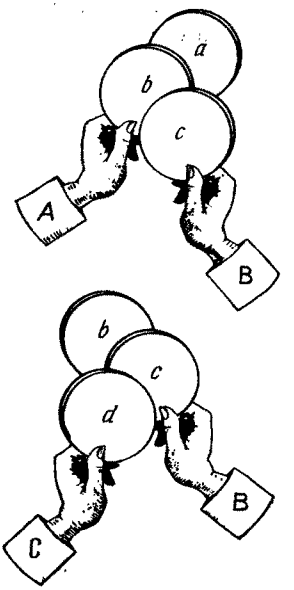


Рис. 3.

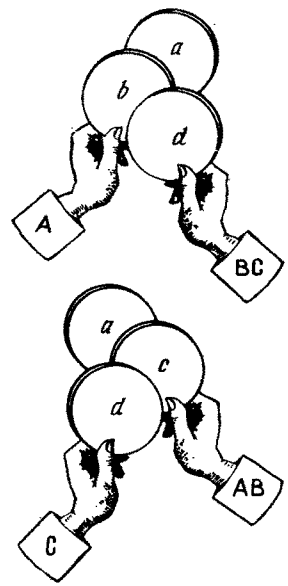


Рис. 4.

Для человека непривычного умножение подстановок таит удивительные «сюрпризы». Например, перемножим подстановки $P = \begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}$ и $Q = \begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}$. Записав подстановку Q в виде $Q = \begin{pmatrix}3&4&2&1\\1&2&3&4\end{pmatrix}$, нетрудно видеть, что $PQ = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$.

Мы получили «подстановку», которая, строго говоря, не переставляет элементы. Но если мы хотим, чтобы умножение подстановок в некоторых случаях не приводило к появлению новых подстановок, то предыдущую «подстановку» (при «выполнении» которой в действительности ничего не происходит) также надлежит считать подстановкой.

Заданная на некотором множестве подстановка называется тождественной, или единичной, если под действием ее все элементы множества переходят в себя.

Поскольку для тождественной подстановки алгоритм подстановки задан, то тем самым указана и ее область определения. Так как тождественные подстановки «ничего не делают в своей области определения», то их можно считать независимыми

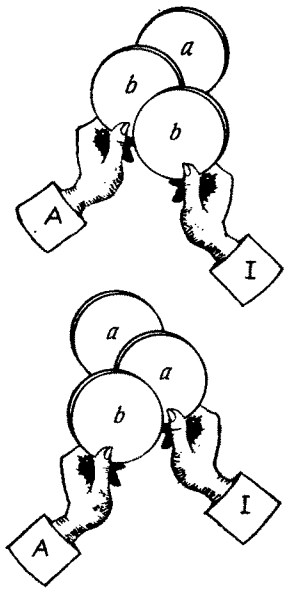


Рис. 5.

от области определения. Поэтому для единообразия тождественные подстановки принято всегда обозначать одной и той же буквой I.

Тождественная подстановка играет в множестве подстановок такую же роль, какая отведена в умножении чисел единице: если A — любая подстановка, то подстановки AI и IA совпадают с A.

Действительно, предположим, что подстановка A переводит элемент a в элемент b. Так как тождественная подстановка переводит элемент a в a, а элемент b в b, то подстановки AI и IA переводят элемент a в элемент b. Тем самым соотношения $AI = IA = A$ доказаны (рис. 5).

Нетрудно проверить, что в частном случае, когда одна из двух подстановок тождественная, умножение подстановок *коммутативно*. К аналогичному выводу мы придем, рассмотрев произведения подстановок $P = \begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}$ и $Q = \begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}$. Как было показано, подстановка PQ совпадает с тождественной. Записав подстановку P в виде $P = \begin{pmatrix}4&3&1&2\\1&2&3&4\end{pmatrix}$, мы без труда убедимся в том, что произведение QP также представляет собой не что иное, как тождественную подстановку.

Рассмотрим теперь две подстановки, связанные друг с другом достаточно тесно: то, что порождает одна подстановка, «уничтожает» другая. Если воспользоваться аналогией с умножением чисел, то выяснится, что такие подстановки образуют пары, весьма напоминающие пары «число и обратное ему число» (разумеется, речь идет только о числах, для которых обратные числа существуют, то есть о числах, отличных от нуля). Такого же рода связь можно обнаружить между функцией и обратной функцией (обратные функции также существуют далеко не для всех функций, но здесь мы имеем в виду такие функции, для которых обратные функции существуют). Последняя аналогия навела на мысль назвать каждую из подстановок, образующих пару, обратной по отношению к другой подстановке.

Если P и Q — такие подстановки, что как произведение PQ, так и произведение QP совпадает с тождественной подстановкой, то подстановка Q называется обратной подстановке P. (Разумеется, в этом случае P является подстановкой, обратной подстановке Q.)

Определение обратной подстановки начинается со слова «Если ...» Это означает, что заранее неизвестно, существует ли подстановка, обратная данной. Как будет показано, обратная подстановка в действительности существует для любой подстановки. Проблема будет состоять в том, чтобы научиться находить подстановку, обратную данной. Ответить на эти два вопроса проще всего следующим образом: сначала мы предложим способ, позволяющий по данной подстановке выписывать обратную, а затем проверим, что наш рецепт действительно порождает подстановку.

Как уже упоминалось, подстановки P и Q взаимно-обратны, если одна из них «уничтожает» действие другой. Предположим, что задана некоторая подстановка

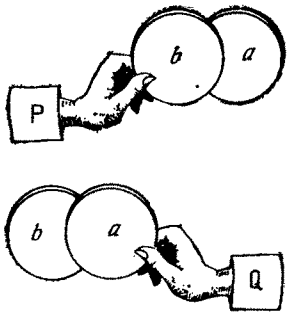


Рис. 6.

P. Попытаемся найти обратную подстановку Q исходя из замечания о связи между действием «прямой» и обратной подстановок: если подстановка P переводит элемент a в элемент b, то подстановка Q переводит элемент b в элемент a (рис. 6).

Отсюда следует, что подстановки PQ и QP тождественные (рис. 7).

Осталось еще проверить, что Q — действительно подстановка. Но по определению Q получается из подстановки P, если в P поменять местами верхнюю и нижнюю строку.

$$P \qquad\qquad Q$$

$$\begin{pmatrix}\text{верхняя строка}\\ \text{нижняя строка}\end{pmatrix} \nearrow\!\!\searrow \begin{pmatrix}\text{нижняя строка}\\ \text{верхняя строка}\end{pmatrix}$$

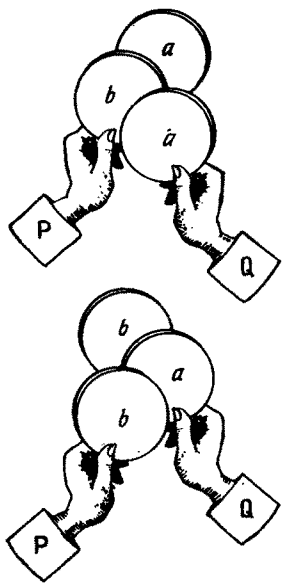


Рис. 7.

Следовательно, в верхней и нижней строках подстановки Q встречается, причем ровно один раз, каждый элемент, принадлежащий области определения, а это и означает, что Q действительно является подстановкой.

В связи с обратной подстановкой необходимо обратить внимание еще на одну проблему. Мы указали способ, позволяющий находить обратную подстановку, но осталось невыясненным, нельзя ли каким-нибудь другим способом получить «другую» обратную подстановку. Покажем, что, даже если какой-нибудь другой способ построения подстановки, обратной заданной подстановке P, и существует, он приводит не к другой, а к той же самой обратной подстановке, которую мы научились находить.

Мы приведем два доказательства этого утверждения. Для первого из них существенно лишь *само определение подстановки*, второе основано на использовании *некоторых свойств операций, производимых при подстановке*.

Первое доказательство. Предположим, что для подстановки P мы по уже известному «рецепту» нашли обратную подстановку Q и что R — некоторая подстановка, обратная подстановке P. Требуется доказать, что подстановки Q и R переводят любой элемент в один и тот же элемент. (Области определения подстановок Q и R, очевидно, совпадают.) По предположению подстановка Q переводит элемент b в элемент a. Следовательно, выполнив подстановку Q после подстановки P, мы переведем элемент b в элемент a. Если подстановка R переводит элемент b в элемент c, то по определению произведения подстановок подстановка PR переводит элемент a в элемент c. Но PR — тождественная подстановка и поэтому должна переводить элемент a в a, что возможно лишь в том случае, если $c = a$. Но это означает, что подстановка R так же, как и подстановка Q, переводит элемент b в элемент a. Поскольку элемент b выбран произвольно, то доказываемое утверждение выполняется для всех элементов. Следовательно, $R = Q$.

Второе доказательство. Предположим теперь, что, следуя приведенному выше «рецепту», мы нашли подстановку Q, обратную подстановке P, и что R — не-

которая подстановка, обратная подстановке P. Выписав цепочку равенств, начинающуюся подстановкой R и кончающуюся подстановкой Q, мы докажем, что эти подстановки совпадают.

1. По свойству тождественной подстановки $R = RI$.

2. Так как Q — подстановка, обратная подстановке P, то $I = PQ$, в силу чего $RI = R(PQ)$.

3. Умножение подстановок ассоциативно, поэтому $R(PQ) = (RP)Q$.

4. Так как R — подстановка, обратная подстановке P, то $RP = I$, в силу чего $(RP)Q = IQ$.

5. Воспользуемся еще раз тем, что I — тождественная подстановка: $IQ = Q$. Итак, получаем следующую цепочку равенств:

$$R = RI = R(PQ) = (RP)Q = IQ = Q.$$

Подстановку, обратную подстановке P, принято обозначать P^{-1}.

Согласно доказанному, обратная подстановка однозначно определяется по заданной подстановке. Поэтому для обозначения обратной подстановки можно использовать ту же букву (или любой другой «символ функциональной зависимости»), которая выбрана для обозначения «прямой» подстановки. Именно так принято обозначать обратные числа.

ЗАДАЧИ

1. Выписать подстановки, обратные всем рассмотренным выше подстановкам.

2. Найти подстановку, обратную тождественной подстановке I.

3. Для заданной подстановки P найти подстановку, обратную обратной подстановке.

4. Найти подстановку, обратную произведению подстановок (подстановки, обратные сомножителям, считаются известными).

1.3. Разложение подстановок, циклы, транспозиции

Выясним, как «ведет себя» подстановка в области определения. В качестве примера рассмотрим подстановку $P = \begin{pmatrix}0123456789\\3587209146\end{pmatrix}$. Эта подстановка заменяет нуль тройкой. Поскольку тройка «уходит» с того места, которое она занимала сначала, то полезно сразу же установить, какое число займет освободившееся место. Поскольку под тройкой стоит семерка, то она и заполнит образовавшийся «пробел». На место, которое прежде занимала семерка, встанет единица (поскольку под 7 стоит 1). Далее мы видим, что место единицы в исходной перестановке займет пятерка, а на место пятерки встанет нуль, который уже встречался нам, то есть нуль также будет «как-то пристроен». Если все перечисленные замены записать в той последовательности, в которой мы их производили, то подстановка P примет вид $P = \begin{pmatrix}0371524689\\3715082946\end{pmatrix}$. Нетрудно видеть, что подстановка P по существу оказалась разложенной на две части. Первые пять мест содержат сведения о том, как подстановка P действует на числа 0, 1, 3, 5, 7, а последние пять мест хранят информацию о действии подстановки P на числа 2, 4, 6, 8, 9.

Все это можно записать, например, так:

$$P = \left[\begin{pmatrix}03715\\37150\end{pmatrix} \text{ и } \begin{pmatrix}24689\\82946\end{pmatrix}\right].$$

Со второй частью подстановки $\begin{pmatrix}24689\\82946\end{pmatrix}$ можно поступить так же, как ранее мы поступили с подстановкой P. Заметив, что 2 переходит в 8, 8 — в 4, а 4 — в 2, получим:

$$\begin{pmatrix}24689\\82946\end{pmatrix} = \begin{pmatrix}28469\\84296\end{pmatrix}.$$

Это означает, что подстановка P допускает следующее разложение (рис. 8):

$$P = \left[\begin{pmatrix}03715\\37150\end{pmatrix}, \text{ и } \begin{pmatrix}284\\842\end{pmatrix}, \text{ и } \begin{pmatrix}69\\96\end{pmatrix}\right].$$

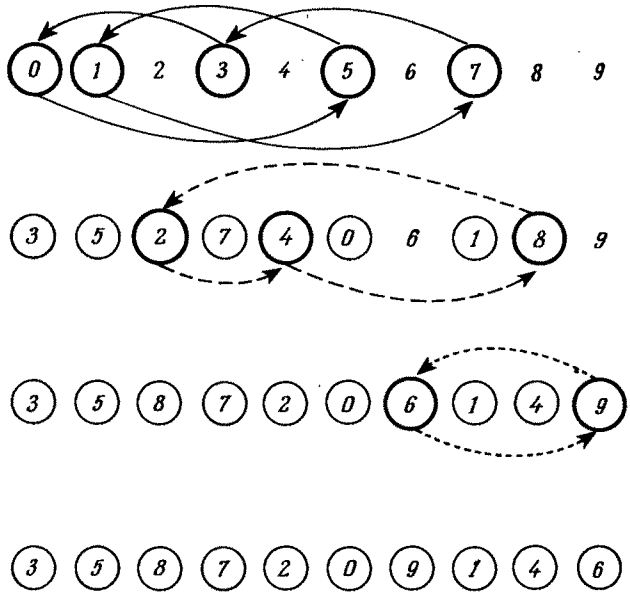


Рис. 8.

Полученное разложение показывает, что подстановка P в действительности состоит из трех независимых частей, каждая из которых перемещает элементы, принадлежащие ее области определения, на одно место в ту сторону, куда направлен «указательный палец» (см. рис. 10).

Именно потому, что все три части подстановки P независимы, совершенно безразлично, какую из подстановок $\begin{pmatrix}0&3&7&1&5\\3&7&1&5&0\end{pmatrix}$, $\begin{pmatrix}2&8&4\\8&4&2\end{pmatrix}$ или $\begin{pmatrix}6&9\\9&6\end{pmatrix}$ выполнять первой, какую — второй и какую — третьей.

Кроме того, две подстановки можно считать одинаковыми, если их области определения различны, но алгоритмы обеих подстановок совпадают.

Если подстановки $\begin{pmatrix}0&3&7&1&5\\3&7&1&5&0\end{pmatrix}$, $\begin{pmatrix}2&8&4\\8&4&2\end{pmatrix}$ и $\begin{pmatrix}6&9\\9&6\end{pmatrix}$ выполнять последовательно, одну за другой, то такие действия можно рассматривать как умножение подстановок. Однако до сих пор мы говорили об умножении подстановок лишь в тех случаях, когда области определения подстановок совпадали. Здесь же области определения подстановок различ-

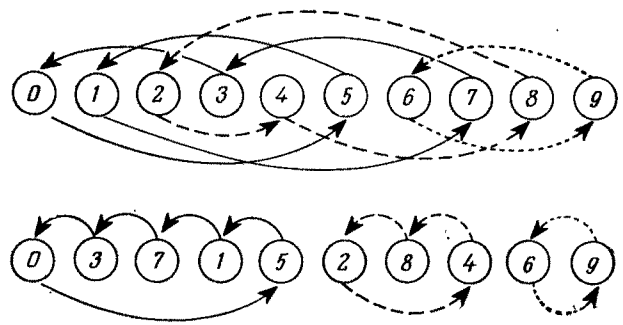


Рис. 9.

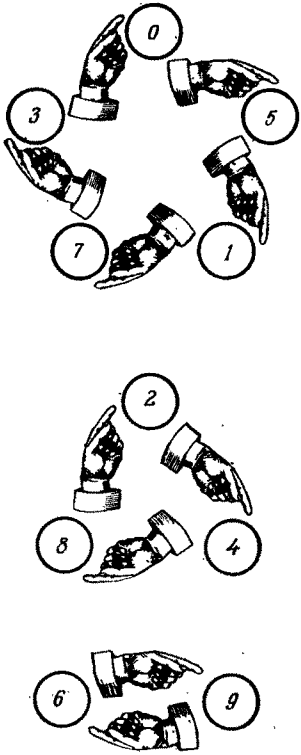


Рис. 10.

ны. Преодолеть возникшую проблему не представляет особого труда: условимся считать, что наши подстановки переводят каждый «недостающий» элемент в самого себя.

Итак, подстановка P допускает следующее разложение (рис. 9):

$$P = \begin{pmatrix} 0123456789 \\ 3587209146 \end{pmatrix} =$$

$$= \begin{pmatrix} 03715 \\ 37150 \end{pmatrix} \begin{pmatrix} 284 \\ 842 \end{pmatrix} \begin{pmatrix} 69 \\ 96 \end{pmatrix}.$$

Это разложение более точно показывает, какие действия производит подстановка P, но выглядит более сложным, чем исходная запись подстановки. Кроме того, из него не видно, допускают ли отдельные части подстановки P дальнейшее разложение.

Оба недостатка можно исправить, если заметить, что в разложении, стоящем в правой части равенства, нижние строки совершенно излишни. *Действительно, верхние строки в правой части состоят из тех же элементов, что и нижние, причем каждый элемент под действием подстановки переходит в следующий.*

Этот порядок не нарушается до тех пор, пока мы не доходим до последнего элемента каждой части. Однако нетрудно видеть, что под последним элементом в нижней строке всегда стоит первый элемент. Следовательно, под действием подстановки последний элемент каждой части переходит в первый элемент той же части. Посмотрим, как можно записать подстановку после произведенных упрощений.

В новых обозначениях подстановка P выглядит так:

$$P = (03715)(284)(69).$$

Подстановки, стоящие в правой части, называются циклическими подстановками или циклами (рис. 10).

Точное определение циклической подстановки весьма длинно, и поэтому мы его опускаем. Заметим, что циклы в новой записи подстановок не могут быть какими угодно. Нетрудно видеть, что каждая цифра входит лишь в один цикл. Такие циклы, не имеющие общих элементов, принято называть независимыми. Пользуясь этим определением, можно сказать, что мы разложили подстановку P в произведение независимых циклов.

Аналогичное разложение можно получить для любой подстановки.

Те элементы, которые циклическая подстановка C переводит в другие элементы (то есть элементы, входящие в запись цикла), называются элементами цикла C. Если два цикла не имеют ни одного общего элемента, то мы говорим, что они независимы.

«Строгое» доказательство теоремы о разложении любой подстановки в произведение независимых циклов также было бы весьма гро-

моздким и сложным, но из приведенного выше способа построения циклов видно, что такое разложение осуществимо. Более того, ясно, что *разложение подстановки в произведение независимых циклов* однозначно определено (то есть два разложения одной и той же подстановки могут отличаться самое большее порядком, в котором следуют циклы-сомножители).

Итак, любая подстановка допускает разложение в произведение независимых циклов.

В качестве примера найдем разложение подстановки

$$Q = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 2\,4\,0\,5\,9\,1\,8\,7\,6\,3 \end{pmatrix}$$

в произведение независимых циклов.

Проще всего это сделать так. Выбрав любой элемент в верхней строке, выяснить, какой элемент окажется на его месте в результате подстановки. Затем найти элемент, который займет освободившееся место, и продолжать так до тех пор, пока мы не встретим в нижней строке элемент, выбранный нами в верхней строке с самого начала. Поскольку этот элемент первым «уступил» свое место, то до этого момента он не появлялся.

Итак, подстановку Q можно представить (рис. 11) в виде

$$Q = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 2\,4\,0\,5\,9\,1\,8\,7\,6\,3 \end{pmatrix} = \\ = (02)\,(1\,4\,9\,3\,5)\,(6\,8)\,(7).$$

Цикл (7) в этой записи можно опустить, поскольку мы условились считать, что элементы, не указанные в явном виде, как бы незримо присутствуют, но под действием подстановки переходят сами в себя. Следовательно, $Q = (02)\,(14935)\,(68)$.

Из двух подстановок P и Q можно образовать подстановки PQ, QP, PP, QQ и проверить, что их разложения в произведения независимых циклов имеют следующий вид:

$$PQ = (0\,5\,2\,6\,3\,7\,4)\,(9\,8),$$
$$PP = (0\,7\,5\,3\,1)\,(2\,4\,8),$$
$$QP = (1\,5\,8\,6\,7\,2\,9\,4\,3),$$
$$QQ = (1\,9\,5\,4\,3).$$

Глядя на эти разложения, трудно догадаться, в каком порядке сомножители P и Q входят в подстановки PQ и QP. Гораздо проще подметить зависимость между разложениями подстановок P и PP или Q и QQ в произведения независимых циклов. Запишем для этого подстановки P и PP, Q и QQ одну под другой.

$$P = (0\,3\,7\,1\,5)\,(2\,8\,4)\,(6\,9),$$
$$PP = (0\,7\,5\,3\,1)\,(2\,4\,8),$$
$$Q = (0\,2)\,(1\,4\,9\,3\,5)\,(6\,8),$$
$$QQ = (1\,9\,5\,4\,3).$$

Нетрудно видеть, что каждый из циклов в нижней строке содержит только те элементы, которые входят в цикл, стоящий непосредственно над ним в верхней строке (некоторые или даже все циклы в нижней строке могут отсутствовать). Так происходит потому, что произведение независимых циклов не изменяется от перестановки сомножителей. Например, в произведении $PP = (03715)\,(284)\,(69)\,(03715)\,(284)\,(69)$ четвертый цикл можно поставить вслед за первым, пятый — вслед за вторым и шестой — вслед за третьим:

$$PP = (0\,3\,7\,1\,5)\,(0\,3\,7\,1\,5)\,(2\,8\,4)\,(2\,8\,4) \times \\ \times (6\,9)\,(6\,9) = (0\,7\,5\,3\,1)\,(2\,4\,8).$$

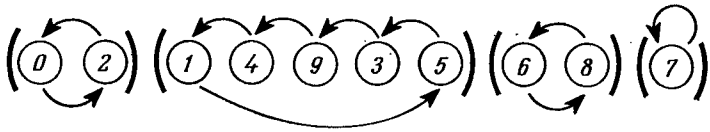


Рис. 11.

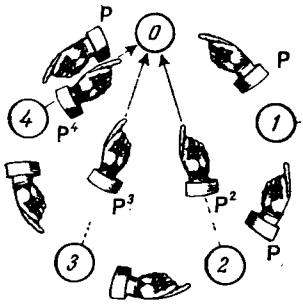


Рис. 12.

Такой способ вычисления подстановок оказывается весьма удобным, если требуется найти произведение нескольких одинаковых подстановок. В этом случае произведение называется степенью подстановки и обозначается $PP = P^2$, $PPP = P^3$ и т. д.

Из сказанного выше следует, что если подстановка разложена в произведение независимых циклов, то степень подстановки равна произведению соответствующих степеней циклов.

Итак, чтобы вычислить степень подстановки, необходимо вычислить ту же степень образующих ее циклов. Прежде чем приступать к решению этой задачи, сделаем два замечания, которые понадобятся нам в дальнейшем.

Для цикла, как и для любой подстановки, несущественно, что представляют собой те элементы, на которые он действует. Не ограничивая общности, можно считать, что речь всегда идет о числах. Именно поэтому для вычислений нам не понадобятся никакие «свойства» отдельных циклов, кроме их «длины».

Длиной цикла называется число входящих в него элементов.

Например, циклы (01), (01234), (352140) имеют длину, равную 2, 5 и 6.

Своим вторым замечанием мы хотели бы особо подчеркнуть «неразличимость» элементов цикла. Если задан какой-то цикл, то с точки зрения подстановки существенно лишь, какой элемент следует за данным элементом, поскольку именно он займет место своего «предшественника» после того, как подстановка будет выполнена. Из этого правила существует лишь одно исключение: элемент, занимающий почетное последнее место, поскольку под действием подстановки он переходит на первое место. *Именно поэтому можно считать, что, переставив в конец элемент, стоявший в записи цикла на первом месте, мы получим тот же самый цикл.*

Например, все циклы (01234), (12340), (34012) и (40123) в действительности обозначают одну и ту же подстановку. Поэтому при возведении цикла в степень достаточно следить лишь за элементом, стоящим на первом месте. Полученный результат без труда переносится на все остальные элементы.

После этих предварительных замечаний рассмотрим, например, цикл (01234).

Нетрудно видеть, что под действием подстановки P^2 нуль перейдет в двойку, а место любого другого элемента займет элемент, находившийся на втором месте позади него. Аналогично под действием подстановки P^3 каждый элемент окажется замещенным элементом, находившимся на третьем месте позади него, под действием подстановки P^4 — элементом, находившимся на четвертом месте позади него, и т. д. (рис. 12). Разумеется, всякий раз, когда мы доходим до «конца» цикла, необходимо, не прерывая счета, возвращаться к «началу». Итак,

$$(01234)^2 = (02413),\ (01234)^3 = (03142),\ (01234)^4 = (04321).$$

Если рассматриваемый нами цикл возвести в пятую степень, то в соответствии все с тем же принципом каждый элемент уступит место элементу, стоявшему на пятом месте позади него, и мы получим тождественную подстановку. Наш метод вы-

числения степеней остается в силе для цикла любой длины!

Если k — длина цикла C, то C^k — тождественная подстановка.

Ясно, что тогда $C^{2k} = C^k \cdot C^k = I = I$ окажется тождественной подстановкой и подстановки C^{3k}, C^{4k} и т. д. будут совпадать с тождественной подстановкой.

Предположим, что подстановка P допускает разложение в произведение, например, трех независимых циклов: $P = ABC$ (при большем числе циклов рассуждения останутся те же, но потребуется большее число букв.) Пусть k — длина цикла A, m — длина цикла B и n — длина цикла C. Поскольку циклы A, B и C независимы, то любая степень подстановки P совпадает с произведением циклов A, B и C, возведенных в ту же степень. В частности, $P^{kmn} = A^{kmn} B^{kmn} C^{kmn}$. Но по предположению A^{kmn}, B^{kmn}, C^{kmn} — тождественные подстановки, так как произведение kmn кратно длине каждого из трех циклов. Поэтому и подстановка P^{kmn} как произведение тождественных подстановок A^{kmn}, B^{kmn} и C^{kmn} также совпадает с тождественной подстановкой.

Наименьшее натуральное число n, при котором P^n совпадает с тождественной подстановкой, называется порядком подстановки P.

Из приведенных выше рассуждений следует, что *любая подстановка в некоторой степени равна тождественной подстановке.*

Обратимся теперь снова к рассмотрению циклов. Мы видим, что $(01234)^5$ — тождественная подстановка. Запишем ее несколько иначе: $(01234)\,(01234)^4 = I$. С другой стороны, нам известно, что две подстановки, связанные такой зависимостью, взаимно-обратны, поскольку для каждой подстановки существует обратная подстановка, и причем только одна. Следовательно, $(01234)^4$ — подстановка, обратная циклу (01234). При более внимательном рассмотрении нетрудно заметить, что цикл $(01234)^4 = (04321) = (43210)$ получается из исходного цикла, если элементы исходного цикла записать в обратном порядке. Тем же способом можно получить и подстановку, обратную любому циклу. Но можно воспользоваться и тем, что обратная подстановка действует как бы «наперекор» прямой подстановке. Из обоих соображений следует, что цикл, обратный данному, мы получим, записав элементы исходного цикла в обратном порядке.

Итак, обратный цикл можно получить, записав элементы исходного цикла в обратном порядке.

Интересным свойством обладают самые короткие циклы — циклы длины 2 (циклов длины 1 не существует, поскольку, если все элементы, за исключением одного, остаются на своих местах, то и этому элементу не остается ничего другого, как остаться на своем месте).

Циклы длины 2 называются транспозициями.

Циклы длины 2 выделяются среди всех прочих циклов тем, что каждый цикл длины 2 совпадает с обратным циклом (то есть обладает таким же свойством, как и число — 1 относительно обычного умножения). Действительно, какой-то цикл совпадает с обратным, если, записав его элементы в обратном порядке, мы снова получим исходный цикл, то есть если перед каждым элементом и после него стоит один и тот же элемент. Но так может быть лишь в том случае, если длина цикла равна 2, причем тогда это условие действительно выполняется.

Транспозиция, как следует из самого названия, означает перемещение: она переставляет два элемента, то есть заставляет каждого из них занять то место, которое занимал другой.

Учитывая, что транспозиции являются очень простыми подстановками, было бы полезно научиться все прочие подстановки представлять в виде произведения транспозиций. Покажем, что любую подстановку действительно можно разложить в

произведение транспозиций. Поскольку любую подстановку можно представить в виде произведения (независимых) циклов, то достаточно доказать, что циклы допускают разложение в произведение транспозиций.

Рассмотрим, например, разложение цикла (12345) в произведение транспозиций (рис. 13). (Аналогичный способ применим и во всех остальных случаях.)

Мы видим, что после завершения всех операций на месте каждого элемента оказался следующий за ним (а первый элемент перешел на последнее место), то есть

$$(1\,2\,3\,4\,5) = (12)\,(13)\,(14)\,(15).$$

(Этот способ разложения циклов аналогичен «методу», к которому прибегает человек, опоздавший к началу киносеанса: на свое место в середине ряда он пробирается, пересаживаясь с места на место так, что каждый раз в «транспозиции», кроме него, участвует лишь один человек.)

Предложенный выше способ разложения циклов в произведение транспозиций не единственный. Другой способ задает, например, разложение (12345) = (23451) = (23) × × (24) (25) (21). Но, как нетрудно видеть, оба разложения содержат по четыре сомножителя. Если учесть, что, например, произведение (23) (23) совпадает с тождественной подстановкой [вместо (23) можно было бы взять любую другую транспозицию], то цикл (12345) можно было бы представить в виде

$$(1\,2\,3\,4\,5) = (12)\,(13)\,(14)\,(15)\,(23)\,(23)$$

или

$$(1\,2\,3\,4\,5) = (23)\,(23)\,(12)\,(13)\,(14)\times \times (15)\,(23)\,(23).$$

Легко заметить, что во всех этих разложениях число транспозиций четно (и равно 4, 4, 6 и 8). Ясно, что способ, «удлиняющий» разложения, всегда приводит лишь к четному числу транспозиций. Но различные разложения исходного цикла можно получить и другими способами. В первом разложении цикла (12345) элементом, входившим во все транспозиции, было число 1. Но если мы разложим подстановку в произведение независимых циклов, то транспозиции, входящие в такое разложение, уже не будут иметь фиксированного общего элемента. Тем не менее существует способ, позволяющий для любой подстановки получать разложение заданного цикла в такое произведение транспозиций, в котором любые две транспозиции содержат заранее выбранный общий элемент. Пусть, например, мы рассматриваем цикл (12345) и число 0 — тот элемент, который должен входить во все транспозиции. (Аналогичным образом можно поступать и в любом другом случае.)

Основная идея избранного нами способа состоит в том, чтобы сначала ввести нуль в цикл, затем переставить соответствующие элементы и, наконец, в том же месте, где произошло «вторжение», исключить «чужеродный» элемент из цикла. Всю процедуру в целом можно записать в следующем виде:

$$(1\,2\,3\,4\,5) = (01)\,(02)\,(03)\,(04)\,(05)\,(01).$$

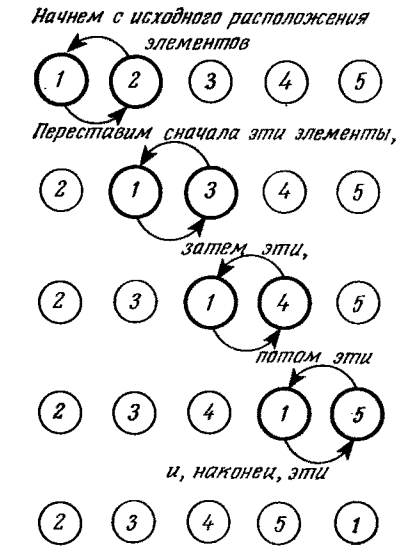


Рис. 13.

Число транспозиций, в произведение которых разложен исходный цикл, равно 6, то есть четно. Можно доказать, что число транспозиций, входящих в любое разложение данной подстановки, может быть либо всегда четным, либо всегда нечетным. Например, какими бы способами мы ни разлагали подстановку (1234), число транспозиций в произведении всегда оказывалось нечетным. Если число транспозиций в любом разложении подстановок всегда четно, то подстановка называется *четной*. В противном случае мы говорим, что *подстановка нечетная*.

ЗАДАЧИ

1. Записать различные степени цикла (012345). Всегда ли при возведении этой подстановки в степень получается один-единственный цикл?

2. Какие подстановки могут быть степенями циклических подстановок?

3. Найти произведение подстановок (01234) (0567). Сформулировать полученный результат для общего случая.

4. Что можно сказать о подстановке P^{-1} (01234) P, если P — произвольная подстановка? Какое обобщение допускает это утверждение?

2.

Понятие группы

2.1. Числовые примеры групп

На множестве подстановок мы определили операцию: последовательное выполнение подстановок. Выяснилось, что эта операция обладает достаточно многими «полезными» свойствами. Рассмотрим теперь все операции с «хорошими» свойствами.

I. Операция ассоциативна, то есть для любых трех подстановок A, B и C выполняется соотношение $(AB)C = A(BC)$.

II. Существует единичный элемент, то есть такая подстановка I, что при любой подстановке A выполняется соотношение $IA = AI = A$.

III. Существует обратный элемент, то есть для любой подстановки A можно найти такой однозначно определенный элемент A^{-1}, что $AA^{-1} = A^{-1}A = I$ (единичный элемент).

На других множествах так же, как и на множестве подстановок, можно задать операции, обладающие всеми тремя свойствами «хорошей» операции.

В таких случаях принято говорить, что выбранное множество с заданной на нем операцией образует *группу*. Сама операция называется групповым умножением. Рассмотрим теперь примеры множеств, наделенных различными операциями, и попытаемся выяснить, являются ли они группами или нет.

Изучая умножение подстановок, мы часто упоминали о том, что названия его свойств выбраны по аналогии с названиями аналогичных свойств умножения чисел. Но обладает ли само умножение чисел тремя перечисленными выше свойствами группового умножения? Ответ, разумеется, зависит от того, какие числа мы рассматриваем: как нетрудно понять, на одних множествах чисел обычное умножение наделено всеми свойствами группового умножения, на других — лишено их.

ПРИМЕРЫ

1. Целые числа. В множестве целых чисел умножение всегда выполнимо, то есть произведение любых двух целых чисел также является целым числом. Остается лишь проверить, обладает ли оно тремя свойствами группового умножения.

I. Умножение ассоциативно. Действительно, хорошо известно, что умножение чисел обладает ассоциативностью (именно поэтому в дальнейшем мы не будет проверять

умножение чисел на ассоциативность).

II. Существует такое целое число e, что при любом целом числе a выполняется соотношение $ea = ae = a$. Это целое число $e = 1$.

(В дальнейшем полезно иметь в виду следующее замечание. Если e — такое число, что при любом отличном от нуля числе a выполняется соотношение $ea = a$, то это возможно лишь в одном случае: при $e = 1$. С другой стороны, если рассматриваемое множество чисел содержит единицу, то все входящие в него числа удовлетворяют соотношениям $1a = a1 = a$. Следовательно, для множества чисел с обычным умножением в качестве предполагаемого группового умножения проверка свойства II сводится к ответу на вопрос, принадлежит ли единица к интересующему нас множеству. Единственное исключение составляет множество, содержащее только один элемент — нуль.)

III. Обратный элемент не существует. Например, для числа 2 невозможно указать такое целое число x, которое удовлетворяло бы соотношению $2x = 1$, так как в левой части стояло бы четное, а в правой — нечетное число.

Следовательно, *целые числа не образуют группу по умножению.*

Нетрудно видеть, что послужило препятствием к образованию группы: во множестве целых чисел деление выполнимо не во всех случаях. Именно поэтому в дальнейшем разумно рассматривать лишь такие множества чисел, в которых деление всегда выполнимо.

2. Рациональные числа. Поскольку произведение двух рациональных чисел — число рациональное, то обычное умножение не выводит за пределы множества рациональных чисел.

Проверим, всеми ли свойствами группового умножения оно обладает.

Ассоциативность в проверке не нуждается, единица — рациональное число. Нам остается лишь убедиться в том, что на множестве рациональных чисел умножение обладает свойством III.

Если рациональное число (дробь) умножить на обратное число, то получится единица. Возникает вопрос: для всякого ли рационального числа имеется обратное? Известно, что обратные числа существуют почти для всех рациональных чисел. Единственное исключение составляет нуль. Причина «ущербности» нуля состоит в том, что при умножении его на любое рациональное (и вообще любое число) всегда получается нуль. Это означает, что произведение двух сомножителей, один из которых равен нулю, никак не может быть равно единице. Поэтому в множестве рациональных чисел с заданным на нем умножением обратный элемент существует не для всех элементов.

Следует твердо помнить: для выполнения условий I—III необходимо (если речь идет об умножении чисел), чтобы 0 не принадлежал рассматриваемому множеству (и, в частности, оно не должно состоять из одного лишь нуля).

Итак, *рациональные числа не образуют группу по умножению.*

3. Рациональные числа, отличные от нуля. Поскольку произведение двух рациональных чисел, отличных от нуля, не равно нулю (и, как упоминалось в предыдущем примере, рационально), то умножение не выводит за пределы рассматриваемого множества чисел. А раз единица — рациональное число, отличное от нуля, то нам остается лишь проверить, выполнено ли третье условие. Но в предыдущем примере уже упоминалось о том, что для чисел, отличных от нуля, всегда существуют обратные числа: числа, которые при умножении на данные числа дают единицу. Эти обратные числа также рациональны и отличны от нуля.

Отличные от нуля рациональные числа образуют группу по умножению.

4. Положительные рациональные числа. Из предыдущего примера ясно, что проверке подлежит только третье условие. Поскольку число, обратное по-

ложительному рациональному числу, также положительно и рационально, то это условие выполнено.

Положительные рациональные числа образуют группу по умножению.

5. Числа $+1$ и -1. При умножении на $+1$ результат совпадает со вторым множителем, а $(-1)\times(-1) = +1$. Следовательно, умножение не выводит за пределы рассматриваемого множества чисел. Остается проверить, выполняется ли третье условие (выполнение остальных условий очевидно). Умножение, рассматриваемое на множестве чисел $+1$ и -1, обладает свойством III группового умножения, так как каждое из этих двух чисел совпадает с обратным.

Числа $+1$ и -1 образуют группу по умножению.

6. Отрицательные рациональные числа. Так как произведение двух отрицательных рациональных чисел является положительным рациональным числом, то в множестве отрицательных рациональных чисел обычное умножение не может служить групповым умножением (можно сказать, что умножение выводит за пределы множества отрицательных рациональных чисел).

Следовательно, отрицательные рациональные числа не образуют группу по умножению.

7. Один лишь нуль. Рассматривая пример 1, мы убедились, что проверка некоторых свойств группового умножения упрощается, если множество чисел состоит не только из нуля. Именно поэтому интересно выяснить, что происходит в том случае, когда множество чисел содержит один-единственный элемент — нуль. Так как $0 \cdot 0 = 0$, то умножение не выводит из этого множества. Замечание об ассоциативности умножения остается в силе и для множества чисел, содержащего только нуль, поскольку нуль все же остается числом, даже если ему «немного одиноко». Наконец, соотношение $0\times 0 = 0$ показывает, что на множестве чисел, содержащем только нуль, умножение обладает свойствами II и III «хорошей» операции.

Число 0 образует группу по умножению.

В примере 7 мы видели, что в роли единичного элемента выступил нуль. Поскольку это единственный случай такого рода, то элемент, соответствующий единичному, при умножении чисел принято называть *единицей*.

Но умножение — не единственная известная нам операция, производимая над числами. Вместе с умножением (и даже несколько раньше, чем с ним) мы все знакомились со сложением. Рассмотрим теперь сложение чисел некоторых типов. Но прежде чем мы приступим к рассмотрению частных случаев, выясним, нельзя ли некоторые свойства сложения установить в общем виде или свести к проверке более простых условий.

I. Об ассоциативности можно не заботиться, так как на множестве чисел сложение всегда ассоциативно.

II. Единицей относительно сложения может быть такой элемент e, который при любом элементе a, принадлежащем рассматриваемому множеству чисел, удовлетворяет соотношению $e + a = a$. Но это условие выполняется лишь для нуля: действительно, при любом a нуль удовлетворяет условию $0 + a = a + 0 = a$. Следовательно, необходимо лишь каждый раз проверять, принадлежит ли нуль рассматриваемому множеству чисел.

III. Числом, «обратным» числу a, при сложении служит число b, удовлетворяющее соотношению $a + b = 0$. Таким числом может быть лишь $b = -a$. Действительно, для него условие $(-a) + a = a + (-a) = 0$ выполнено. Поэтому достаточно каждый раз проверять, содержит ли рассматриваемое множество чисел вместе с каждым принадлежащим числом то же число, взятое со знаком минус.

Рассмотрим уже знакомые мно-

жества чисел, на которых в качестве операции задано сложение.

1а. Целые числа (операция — сложение). Так как сумма двух целым чисел также является целым числом, то сложение не выводит за пределы рассматриваемого множества. Поскольку нуль — целое число и любое целое число, взятое со знаком минус, — также целое число, то сложение, заданное на множестве целых чисел, обладает всеми свойствами группового умножения.

Целые числа образуют группу по сложению.

2а. Рациональные числа (операция — сложение). Сумма двух рациональных чисел — число рациональное, поэтому сложение не выводит за пределы множества рациональных чисел. Нуль — рациональное число. Кроме того, любое рациональное число, взятое со знаком минус, также является рациональным. Следовательно, сложение на множестве рациональных чисел обладает всеми свойствами группового умножения.

Рациональные числа образуют группу по сложению.

3а. Рациональные числа, отличные от нуля (операция — сложение). Это множество чисел по определению не содержит нуля, в силу чего сложение не обладает свойством II.

Рациональные числа, отличные от нуля, не образуют группу по сложению.

4а. Положительные рациональные числа (операция — сложение). Как показывают соображения, аналогичные приведенным в предыдущем примере,

положительные рациональные числа не образуют группу по сложению.

4б. Неотрицательные рациональные числа (операция — сложение). Если к множеству чисел из предыдущего примера присоединить нуль, то тем самым будет устранено препятствие, мешавшее сложению «обзавестись» свойством II.

Действительно, сложение не выводит за пределы множества неотрицательных рациональных чисел сложения, так как сумма таких чисел не может быть отрицательной, но в то же время она рациональна. Необходимо выяснить лишь, обладает ли сложение свойством III. Как показывает проверка, это условие оказывается невыполненным, так как любое положительное рациональное число, если его взять со знаком минус, становится отрицательным (и, следовательно, не принадлежит множеству неотрицательных рациональных чисел).

Итак, неотрицательные рациональные числа не образуют группу по сложению.

5а. Числа $+1$ и -1 (операция — сложение). 6а. Отрицательные рациональные числа (операция — сложение). В обоих случаях рассматриваемые множества чисел не содержат нуля, и это служит основным препятствием к образованию группы.

7а. Один лишь нуль (операция — сложение). Так как $0 + 0 = 0$, то сложение не выводит за пределы рассматриваемого множества. Остальные условия, очевидно, выполнены.

Число 0 образует группу по сложению.

Подробное рассмотрение всех понятий, возникающих в связи с каждым примером, увело бы нас слишком далеко от основной темы, поэтому мы будем считать их известными. Если же кто-нибудь из читателей, перейдя к очередному примеру, обнаружит, что не понимает, о чем идет речь, то соответствующий пример можно опустить. То же относится и к задачам, приведенным ниже.

ЗАДАЧИ

Определить, образуют ли следующие множества чисел группу по сложению и умножению.

1. Все вещественные числа.

2. Вещественные числа, отличные от нуля.

3. Положительные вещественные числа.

4. Неотрицательные вещественные числа.

5. Комплексные числа.

6. Комплексные числа, не равные нулю.

7. Комплексные числа с модулем, равным единице.

8. Комплексные числа с модулем больше единицы.

9. Целые положительные степени двойки (числа 2, 4, 8 и т. д.).

10. Все степени двойки (с целым положительным, целым отрицательным и нулевым показателем).

11. Числа 1, -1, $i = \sqrt{-1}$ и $-i$.

12. Числа вида $a + bi$, где a и b — целые числа, $i = \sqrt{-1}$.

13. Числа вида $a + bi$, где a и b — рациональные числа, $i = \sqrt{-1}$.

14. Те же числа, что и в предыдущем примере, кроме нуля.

2.2. Другие примеры групп

Начнем с геометрических примеров.

1. Векторы на плоскости (операция — сложение векторов). Сложив любые два вектора, мы снова получим вектор. Следовательно, в этом случае операция не выводит за пределы рассматриваемого множества.

Что касается ассоциативности, то, как известно, сложение векторов обладает этим свойством. Единичным элементом служит нулевой вектор, а элементом, обратным данному вектору, — противоположный вектор (то есть вектор, занимающий то же положение и имеющий ту же длину, что и данный вектор, но направленный в противоположную сторону).

Следовательно, в этом примере мы имеем дело с группой.

2. Движения на плоскости (операция — последовательное выполнение движений).

Преобразование плоскости называется движением, если:

1) между точками плоскости до преобразования и теми точками, в которые они переходят под действием преобразования, существует взаимно-однозначное соответствие;

2) расстояние между любыми двумя точками плоскости совпадает с расстоянием между соответствующими им точками.

Каждому движению на плоскости соответствует своя «картинка». Одни движения сводятся к сдвигам, другие — к поворотам, третьи — к повороту на 180° вокруг прямой, лежащей в плоскости (то есть к отражению относительно этой прямой). Разнообразие движений весьма затрудняет доказательства. Представьте себе, сколько случаев потребовалось бы рассмотреть, если бы мы захотели выяснить, какое движение возникает в результате последовательного выполнения двух движений перечисленных выше типов. Поэтому представляется целесообразным предварительно выяснить, что такое движение.

Движение **T** переводит каждую точку A плоскости в однозначно определенную точку A' так, что различные точки переходят в различные. Кроме того, если движение T переводит точку B в B', то расстояние между точками A и B совпадает с расстоянием между точками A' и B' (рис. 14).

(При помощи геометрических методов можно показать, что преобразования трех перечисленных выше типов обладают требуемыми свойствами.)

Точку, в которую преобразование **T** переводит точку A, обозначим $\mathbf{T}(A)$. (Интересно отметить, что выбранное нами обозначение до некоторой степени напоминает обозначения функций. «Аргументом A» служит точка плоскости, а «функцией T» — движение.)

Рассмотрим теперь два движения на плоскости: **T** и S. Выполним сначала движение **T**, затем движение S.

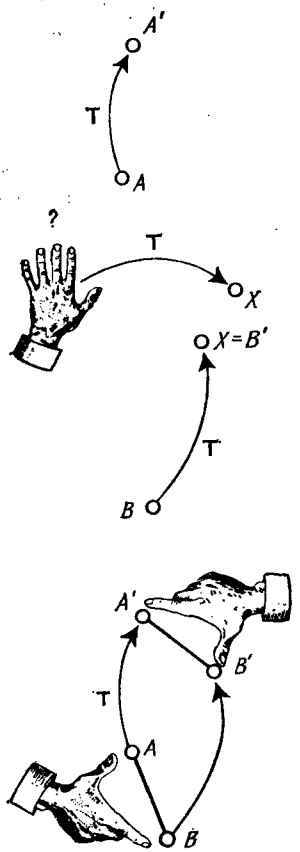


Рис. 14.

Нетрудно видеть, что преобразование **ST** [переводящее точку A плоскости в точку $S(T(A))$] также переводит каждую точку плоскости в некоторую однозначно определенную точку плоскости (рис. 15). Ясно, что различные точки под действием преобразования **ST** переходят в различные. Действительно, если A и B — различные точки плоскости, то точки $T(A)$ и $T(B)$ не могут совпадать (так как движение **T** переводит различные точки плоскости в различные, но тогда движение **S**, подействовав на точки $T(A)$ и $T(B)$, также переведет их в какие-то несовпадающие точки плоскости).

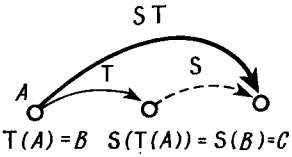


Рис. 15.

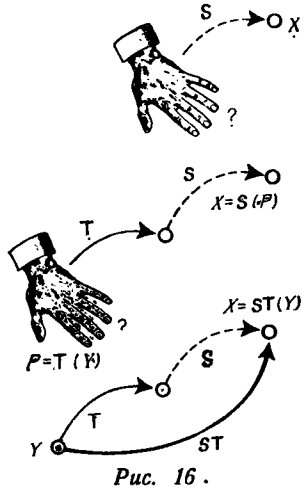


Рис. 16.

Пусть X — произвольная точка плоскости. Поскольку **S** и **T** — движения, то существует точка P, которую **S** переводит в точку X, и точка Y, которую **T** переводит в точку P. Но тогда преобразование **ST** переводит точку Y в точку X и, следовательно, обладает требуемым свойством (рис. 16).

Наконец, необходимо убедиться в том, что преобразование **ST** сохраняет расстояние между точками. Но это свойство следует из того, что ни одно из преобразований **S** и **T** не изменяет расстояний между точками (рис. 17).

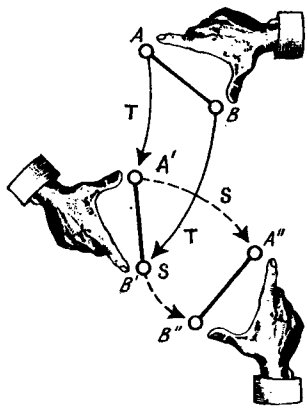


Рис. 17

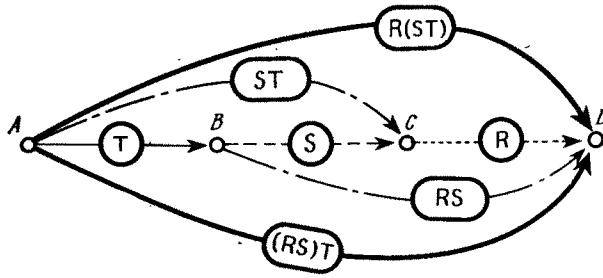


Рис. 18

Итак, мы показали, что произведение двух движений на плоскости есть также некоторое движение. Следовательно, последовательное выполнение движений не выводит за пределы рассматриваемого множества преобразований.

I. Проверим, ассоциативна ли введенная нами операция. Пусть **T**, **S** и **R** — три движения плоскости. Требуется доказать, что **R(ST)** совпадает с **(RS)T**, то есть что эти два движения переводят любую точку A плоскости в одну и ту же точку. Предположим, что **T** переводит точку A в точку B, **S** переводит точку B в точку C и **R** переводит точку C в точку D. Тогда движение **ST** переводит точку A в точку C, а движение **RS** переводит точку B в точку D. Следовательно, каждое из интересующих нас преобразований переводит точку A в точку D (рис. 18).

II. Нетрудно видеть, что единичным элементом служит тождественное преобразование **I**, переводящее все точки плоскости в самих себя. Действительно, тождественное преобразование можно считать движением, поскольку все условия для этого выполнены. Ясно также, что для любого движения **T** справедливо соотношение $\mathbf{TI} = \mathbf{IT} = \mathbf{T}$ (рис. 19).

III. Наконец, необходимо убедиться в том, что для каждого движения существует обратное. Нетрудно видеть, что обратное движение представляет собой преобразование, возвращающее все точки в исходное положение. Определим поэтому преобразование **S** так, чтобы оно переводило точку $\mathbf{T}(A)$ в точку A (A — произвольная точка плоскости). Поскольку образом точки A при движении **T** может быть любая точка плоскости [иначе говоря, любую точку плоскости можно обозначить $\mathbf{T}(A)$], то о любой точке плоскости можно утверждать, что именно в нее преобразование **S** переводит какую-то точку плоскости (рис. 20). Проблема состоит лишь в том, чтобы выяснить, однозначно ли это преобразование. Не может ли слу-

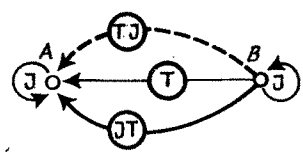


Рис. 19.

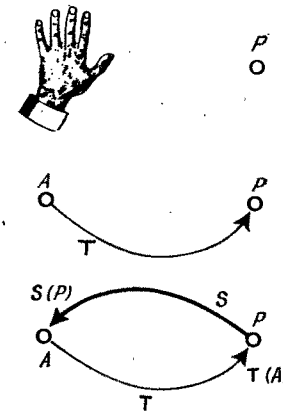


Рис. 20.

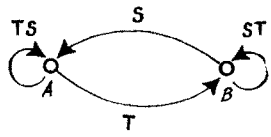


Рис. 21.

читься так, что одну и ту же точку можно обозначить $\mathbf{T}(A)$ не одним, а несколькими способами? Нет, такое никак не может произойти: по предположению движение **T** переводит различные точки плоскости в различные, поэтому любая точка плоскости является образом лишь одной-единственной точки A [то есть представима в виде $\mathbf{T}(A)$]. Нам осталось еще проверить, что в каждую точку плоскости под действием преобразования **S** переходит какая-то точка плоскости. Но это очевидно, поскольку в точку A переходит точка $\mathbf{T}(A)$. Наконец, необходимо выяснить, сохраняет ли преобразование **S** расстояния. Так как расстояние между точками $\mathbf{T}(A)$и $\mathbf{T}(B)$ совпадает с расстояниями между точками A и B, то справедливо и обратное утверждение: расстояние между точками A и B такое же, как между точками $\mathbf{T}(A)$ и $\mathbf{T}(B)$. Это и означает, что преобразование **S** сохраняет расстояния.

Итак, преобразование **S** с полным основанием можно назвать движением. Необходимо лишь проверить, что **S** — движение, обратное движению **T**. Предположим, что **T** переводит точку A в точку B. Тогда **S** переводит точку B в точку A. Поскольку движение **S** в каждую точку плоскости переводит некоторую точку плоскости, и притом только одну, то произвольно заданную точку плоскости можно считать (по выбору) либо точкой A, либо точкой B. Но $\mathbf{TS}(B) = \mathbf{T}(A) = B$, $\mathbf{ST}(A) = \mathbf{S}(B) = A$, поэтому и движение **TS** и движение **ST** переводят произвольно выбранную точку плоскости в себя и, следовательно, совпадают с тождественным преобразованием (рис. 21).

Тем самым полностью доказано, что движения на плоскости образуют группу, если в качестве «умножения» взять последовательное выполнение движений.

3. Линейные функции (операция — линейная замена переменных).

Линейной называется функция вида $y = ax + b$, где $a \neq 0$, а в остальном a и b — произвольные вещественные числа.

Подставим в функцию $y = ax + b$ вместо независимой переменной x в правой части функцию $y = cx + d$. Из тождества $a(cx + d) + b = (ac)x + (ad + b)$ следует, что «произведением» функций $y = ax + b$ и $y = cx + d$ будет функция $y = (ac)x + (ad + b)$. Поскольку на множестве функций и сложение и умножение имеют смысл и обе эти операции используются в линейной функции, то вновь введенную операцию — линейную замену независимой переменной — мы обозначим маленьким кружком:

$$(y = ax + b) \circ (y = cx + d) =$$
$$= (y = (ac)x + (ad + b)).$$

Чтобы «лишние» знаки равенства нам не мешали, опустим во всех скобках «$y =$». Тем самым мы как бы говорим, что нас интересуют выражения вида $ax + b$, где a и b — вещественные числа, причем $a \neq 0$. Выражения $ax + b$ и $cx + d$ равны, если $a = c$ и $b = d$. Но при «умножении» мы получаем

$$(ax + b) \circ (cx + d) = (ac)x + (ad + b).$$

Так как по предположению ни a, ни c не равны 0, то число ac также отлично от нуля. Поскольку ac и $ad + b$ — вещественные числа, то $(ac)x + (ad + b)$ — линейная функция. Следовательно, линейная замена независимой переменной в линейной функции не выводит за пределы множества линейных функций.

I. Прежде всего проверим, ассоциативна ли наша операция. Запишем еще одну линейную функцию $(y =)\ ex + f$. Так как $(ac)\ (ex + f) +$

$+(ad+b)=(ace)x+(acf+ad+b)$, то

$$[(ax+b)\circ(cx+d)]\circ(ex+f)=(ace)x+(acf+ad+b).$$

С другой стороны, используя соотношение $(cx+d)\circ(ex+f)=c(ex++f)+d=(ce)x+(cf+d)$, получаем $(ax+b)\circ[(cx+d)\circ(ex+f)]=a[(ce)x+(cf+d)]+b=(ace)x++(acf+ad+b)$, что и доказывает ассоциативность.

II. Проверим, существует ли единичный элемент. Им может быть лишь такая линейная функция $ux++v$, для которой при любой линейной функции $ax+b$ выполняется равенство

$$ax+b=(ax+b)\circ(ux+v)=(au)x+(av+b).$$

Но из условия равенства линейных функций следует, что $au=a$ и $b=av+b$. Из последнего равенства находим: $av=0$. В частности, если число a выбрать равным 1 (это можно сделать, так как важно лишь, чтобы оно было вещественным числом, отличным от нуля), то $u=1$ и $v=0$. Следовательно, единичным элементом может быть только линейная функция $(y=)x$. Поскольку $a(1x+0)+b=1(ax+b)+0=ax+b$ при любых вещественных a и b, то x действительно служит единичным элементом.

III. Наконец, необходимо определить обратный элемент. Если линейная функция $ux+v$ обратна линейной функции $ax+b$, то должно выполняться условие $x=(ux+v)\circ\circ(ax+b)=(ua)x+(ub+v)$, которое можно записать в виде $1=ua$ и $0=ub+v$. По предположению $a\neq 0$, поэтому число, обратное числу a, существует и $u=a^{-1}$, $v=-ub=-a^{-1}b$. Для того чтобы найденная линейная функция действительно была обратной линейной функции $ax+b$, не только произведение $(ux+v)\circ(ax+b)$, но и произведение $(ax+b)\circ(ux+v)$ должно быть равно единичному элементу. Проверяем: $(ax+b)\circ(ux++v)=(au)x+(av+b)=(aa^{-1})x++(a(-a^{-1}b)+b)=x$.

Следовательно, линейные функции образуют группу относительно линейной замены независимой переменной.

4. Определим на множестве, состоящем из вершин и центра тяжести равностороннего треугольника, следующую операцию. Произведением любой вершины и центра тяжести условимся считать ту же вершину. Произведениями любой вершины или центра тяжести на самих себя будем считать центр тяжести. Произведением двух различных вершин выберем третью вершину.

Поскольку во всех мыслимых случаях заданная операция приводит к одной из точек, принадлежащих рассматриваемому множеству, то «умножение» не выводит за пределы рассматриваемого множества точек.

Пусть A, B и C — вершины. S — центр тяжести равностороннего треугольника. По определению $SA=AS=S$, $SB=BS=B$, $SC=CS=C$ и $SS=S$. Следовательно, S — единичный элемент. Условие $AA=BB=CC=S$ означает, что элементы A, B и C совпадают со своими обратными элементами (аналогичное утверждение справедливо и относительно единичного элемента). Необходимо лишь проверить ассоциативность. Поскольку операция на множестве задана так, что мы не располагаем ни общими понятиями, ни одним алгоритмом, то все случаи необходимо рассматривать в отдельности. Это означает, что мы должны перебрать 64 произведения, содержащих по 3 сомножителя, вычислив каждое из них двумя способами. Но столь скучное занятие вряд ли придется кому-либо по вкусу. Именно поэтому необходимо по возможности сократить перебор. Если какой-нибудь из сомножителей трехчленного произведения совпадает с единичным элементом, то этот сомножитель как бы «отсутствует»: неза-

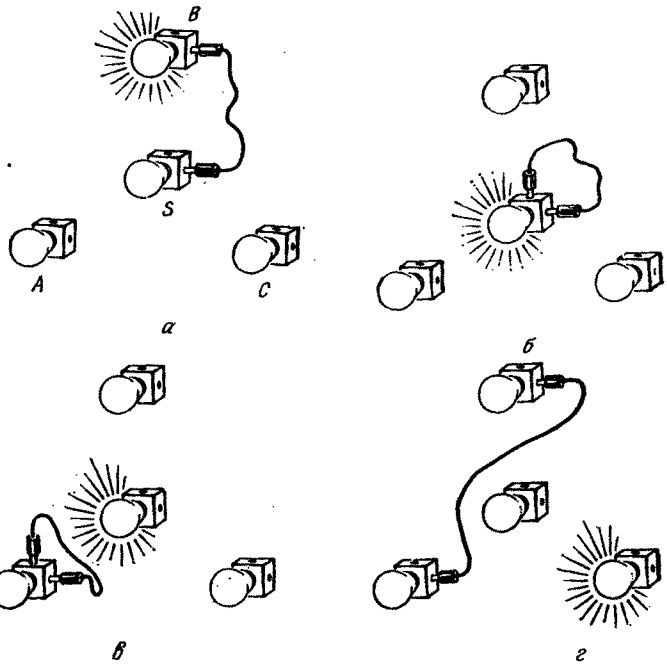


Рис. 22.

висимо от того, ассоциативно ли «умножение», произведение равно произведению двух остальных сомножителей. Следовательно, не ограничивая общности, можно предположить, что в произведение входят лишь множители A, B и C. Поскольку «умножение» определено так, что ни одна из вершин не выделена по сравнению с другой, то произведение вершин не зависит от того, какими буквами обозначены вершины равностороннего треугольника. Например, можно считать, что на первом месте в произведении стоит вершина, обозначенная буквой A. На втором месте также может стоять вершина A. Если же второе место занято другой вершиной, то, не ограничивая общности, можно предположить, что это вершина B. На третьем месте в обоих случаях может находиться вершина A, B и C. Итак, остались произведения, в которых сомножители расположены в следующем порядке: AAA, AAB, AAC и ABA, ABB, ABC. Всего набирается шесть произведений, и перебор их не представляет никакого труда. (Произведение ABB также следовало бы исключить из списка произведений, подлежащих рассмотрению, поскольку оно «зеркально симметрично» произведению AAB, но строгое обоснование «вычеркивания» слишком длинно для того, чтобы его приводить.)

Итак, $(AA)A = SA = A = AS = A(AA)$, $(AA)B = SB = B = AC = A(AB)$ (в случае AAC ассоциативность доказывается так же), $(AB)A = CA = B = AC = A(BA)$, $(AB)B = CB = A = AS = A(BB)$ и, наконец, $(AB)C = CC = S = AA = A(BC)$. Следовательно, вершины треугольника и его центр тяжести образуют группу относительно введенной операции.

ЗАДАЧИ

Доказать, что следующие множества образуют группы относительно введенных на них операций.

1. Векторы, направленные в одну и ту же сторону, относительно сложения векторов.

2. Векторы, имеющие произвольные направления в пространстве, относительно сложения векторов.

3. Сдвиги плоскости относительно умножения (последовательного выполнения) движений.

4. Повороты плоскости вокруг заданной точки относительно умножения движений.

5. Движения плоскости, переводящие некоторый заданный равносторонний треугольник (квадрат) в себя, относительно умножения движений.

6. Движения в пространстве, для которых умножение определено по аналогии с умножением движений плоскости.

7. Преобразования подобия на плоскости (при которых расстояние между любой парой точек может изменяться, но так, что отношение расстояний не зависит от выбора пары точек, а определяется только преобразованием) относительно последовательного выполнения преобразований.

8. Движения в пространстве, переводящие заданный тетраэдр в себя, относительно произведения движений.

9. Функции, принимающие в нуле значение, равное 0, в единице — значение, равное 1, а между нулем и единицей — все значения, заключенные между 0 и 1, причем так, что бóльшим значениям независимой переменной соответствуют бóльшие значения функций (такими свойствами обладают непрерывные функции, монотонно возрастающие на отрезке $[0, 1]$) относительно подстановки одной функции в другую.

2.3. Определение группы

Рассмотренные нами примеры показывают, как часто встречаются множества с заданными на них ассоциативными операциями, относительно которых существует единичный элемент и все элементы имеют обратные. В таких случаях говорят, что соответствующие множества образуют группы относительно заданных на них операций.

Попытаемся теперь дать точное определение группы. Итак, что же такое группа? Мы видели, что группы содержат элементы и эти элементы образуют те или иные множества. Можно ли отождествить группу с множеством ее элементов? Ясно, что нельзя. Ведь множество всех целых чисел может и быть группой и не быть группой в зависимости от того, какую операцию мы зададим на ней: сложение или умножение чисел. Следовательно, операция каким-то образом неразрывно связана с групповым свойством. Разумеется, столь же неразрывно связано с групповым свойством и то множество, над элементами которого производится операция.

Пара $\langle G; f \rangle$, состоящая из множества G и двухместной (или бинарной) операции f, называется группой, если операция f удовлетворяет следующим аксиомам.

I. Операция f ассоциативна, то есть для любых элементов a, b и c множества G

$$f(f(a, b), c) = f(a, f(b, c)).$$

II. Существует единичный элемент, то есть такой элемент e множества G, что для любого элемента a из G

$$f(e, a) = f(a, e) = a.$$

III. Существует обратный элемент, то есть для любого элемента a множества G можно найти такой элемент b, что

$$f(a, b) = f(b, a) = e.$$

Операция f называется групповой операцией или групповым умножением, а элементы множества G — элементами группы.

Итак, группа представляет собой пару, состоящую из множества и заданной на нем операции, которая обладает определенными свойства-

ми. Но, прежде чем переходить к описанию этих свойств, выясним, что такое операция. Групповая операция (групповое умножение) ставит в соответствие каждой паре элементов некоторый элемент — их «произведение».

Следовательно, *заданная на множестве операция есть не что иное, как функция, отображающая любую пару элементов множества в некоторый элемент того же множества.* (Осторожно! Элементы пары перенумерованы, то есть указано, какой элемент является первым и какой — вторым.)

Не столь бесспорен выбор функциональных обозначений для групповой операции (в особенности для тех, кому уже приходилось встречаться с группами), поскольку обычно групповую операцию принято обозначать каким-нибудь значком, стоящим между отображаемыми элементами. Впрочем, и мы будем использовать функциональные обозначения только в определениях. (И здесь групповую операцию можно было бы обозначить как-нибудь иначе, например $+(a, b)$, и «читать» ее как «сумма элементов a и b».) Если операция задана каким-нибудь естественным способом и обозначена, то вместо «функции» f можно использовать соответствующее обозначение. Например, если E — множество целых чисел, P — множество положительных вещественных чисел, то $\langle E; + \rangle$ означает группу, образуемую целыми числами по сложению, а $\langle P; \cdot \rangle$ — группу, образуемую положительными вещественными числами по умножению.

Вместе с тем необходимо подчеркнуть, что символ $\langle G; f \rangle$ еще не означает, будто речь непременно идет о группе. Указаны лишь множество G и заданная на нем операция f. Требуется еще проверить, выполнены ли все условия, которым должна удовлетворять групповая операция.

Мы хотели бы завершить этот раздел небольшим отступлением.

Обычно в книгах по теории групп приводится следующее определение группы: элементы некоторого множества называются группой, если на них задана операция, которая ассоциативна, существует единичный элемент и для каждого элемента — обратный элемент. Нетрудно видеть, что в таком определении существование операции устанавливается аксиоматически. Но такое понимание групповой операции не согласуется со взглядами, принятыми в современной алгебре и в последних работах по теории групп, согласно которым операции (или операции) считаются заданными вместе с множеством, а свойства операций подлежат особому изучению.

ЗАДАЧИ

Пусть E — множество целых чисел, P — множество положительных вещественных чисел и h — операция возведения в степень [то есть $h(a, b) = a^b$].

1. Группа ли $\langle E; h \rangle$?
2. Группа ли $\langle P; h \rangle$?

3.

Свойства элементов группы

3.1. Различные способы определения группы

При более внимательном рассмотрении приведенных выше доказательств того, что соответствующие множества образуют группы относительно заданных на них операций, нетрудно заметить одну особенность. Определение обратного элемента используется в этих доказательствах «односторонне»: умножая тот или иной элемент на обратный с одной стороны (либо слева, либо справа), мы получали единичный элемент, а затем доказывали, что «прямой» и обратный элементы можно поменять местами. Но если перестановка «прямого» и обратного элементов всегда допустима, то это означает, что в каждом отдельном случае можно ограничиться доказательством существования «одностороннего» обратного элемента, поскольку отсюда *в общем*

случае следует, что именно этот элемент будет и двусторонним обратным.

Возникает вопрос: нельзя ли еще более сузить круг условий, с тем чтобы подвергать проверке меньшее число свойств?

Этому вопросу в какой-то мере близка следующая проблема. Могут встретиться (и действительно встречаются) такие группы, для которых проверка соответствующих свойств сопряжена с большими трудностями. В то же время можно легко доказать, что эти группы обладают другими свойствами, из которых в общем случае следуют и свойства, подлежавшие проверке.

В дальнейшем мы всегда будем предполагать, что операция двухместна и ассоциативна. Именно поэтому для множеств с заданной на них операцией разумно ввести особое название: так как свойства группы выполнены лишь наполовину, то такие множества называются *полугруппами*.

Пара $\langle F; f \rangle$ называется полугруппой, если F — некоторое множество, а f — двухместная ассоциативная операция на множестве F.

С полугруппами нам приходилось встречаться и прежде, поэтому теперь мы лишь сошлемся на некоторые примеры. Строго говоря, особой необходимости в этом нет, так как по определению полугрупп все группы являются одновременно и полугруппами. Но для тех, кто хотел бы познакомиться с полугруппами, не принадлежащими к числу групп, упомянем о том, что если на каком-то множестве чисел определена операция сложения или умножения (не выводящая за пределы множества), то это множество образует относительно заданной на нем операции полугруппу, поскольку и сложение и умножение ассоциативны. Следовательно, задачи, приведенные в разделе 2.1 (за исключением задачи 4), могут служить примерами множеств чисел, образующих полугруппы по умножению (см. таблицу, приведенную в решении). Кроме того, задачи 3 и 4 дают примеры полугрупп по сложению, не являющихся группами по сложению.

Сравнивая определения полугруппы и группы, нетрудно видеть, что *полугруппа является группой в том и только в том случае, если*:

I) существует такой элемент e, что для любого элемента a полугруппы $ea = ae = a$;

II) для любого элемента a можно найти такой элемент b, что $ba = ab = e$.

При рассмотрении группы подстановок мы «строго» доказали, что левый обратный элемент совпадает с правым обратным элементом. Теперь мы докажем гораздо больше.

Если в полугруппе $\langle G; f \rangle$ существует левый единичный элемент и для каждого элемента существует левый обратный элемент, то:

1) все левые обратные элементы являются одновременно правыми обратными (и, следовательно, обратными) элементами;

2) левый единичный элемент является одновременно правым единичным (и, следовательно, единичным) элементом;

3) $\langle G; f \rangle$ — группа.

Перечисленные условия можно записать в следующем виде (договоримся опускать обозначение операции, как при умножении чисел, и понимать ab как результат применения f к элементам a и b множества G):

в полугруппе существует такой элемент e, что если a — любой элемент полугруппы, то $ea = a$, и для произвольно выбранного элемента a полугруппы найдется такой элемент b, что $ba = e$.

1. Прежде всего необходимо доказать, что (в принятых выше обозначениях) $ab = e$. Из соотношения $ba = e$, принятого за исходное, следует, что $bab = (ba)b = eb = b$ (здесь мы воспользовались тем, что e — левый единичный элемент). Но для элемента b существует левый обратный элемент (обозначим его c), для которого $cb = e$, поэтому, во-

первых, $c(bab) = cb = e$, во-вторых, $c(bab) = (cb)(ab) = e(ab) = ab$ (поскольку $cb = e$ и e — левый единичный элемент). Сравнивая оба равенства, получаем: $ab = e$, что и требовалось доказать.

2. Докажем теперь, что для любого элемента a полугруппы $ae = a$. Начнем с того, что уже известно: $ea = a$ и $ba = ab = e$. Из этих соотношений получаем

$$a = ea = (ab)\,a = a\,(ba) = ae,$$

что и требовалось доказать.

3. Наконец, необходимо убедиться в том, что у нас действительно получилась группа. Но это — не что иное, как своего рода общий итог доказанных ранее утверждений 1 и 2.

Нам уже неоднократно приходилось говорить о единичном элементе или об элементе, обратном данному элементу, и всякий раз речь шла об однозначно определенных элементах. Однако в общем случае мы не можем заранее утверждать, что единичный элемент или элемент, обратный данному, однозначно определены, поскольку в перечисленных выше условиях ничего не говорится ни о единственности единичного элемента, ни о единственности элемента, обратного данному. Разумеется, однозначную определенность нетрудно вывести из заданных условий. Например, из того, что в полугруппе существует левый единичный элемент и для всех элементов существует левый обратный элемент, как было показано, следует, что существует «двусторонний» единичный элемент, а левый обратный элемент совпадает с «двусторонним» обратным элементом. Следовательно, однозначная определенность единичного элемента и элемента, обратного данному, в действительности свойственна любой группе.

Итак, в любой группе единичный элемент однозначно определен, и для каждого элемента существует единственный обратный элемент.

Во всякой группе единичный элемент однозначно определен, и для каждого элемента существует единственный обратный элемент.

Нетрудно убедиться в правильности обоих утверждений. Если бы e был левым, а f — правым единичным элементом в группе, то

$ef = f$ (так как e — левый единичный элемент),

$ef = e$ (так как f — правый единичный элемент),

и, следовательно, $f = ef = e$. Аналогично, если бы b был правым, а c — левым обратным элементом для элемента a, то

$ab = e$ (так как b — правый обратный элемент для a),

$ca = e$ (так как c — левый обратный элемент для a),

откуда

$$c = ce = c\,(ab) = (ca)\,b = eb = b.$$

Однозначная определенность обратного элемента позволяет рассматривать его как функцию, заданную на элементах группы, и использовать для его обозначения два символа: функции и того элемента, от которого берется обратный элемент. Обычно элемент, обратный элементу a, принято обозначать как элемент a в «минус первой степени», то есть как a^{-1}

Элемент, обратный элементу a, обозначается a^{-1}.

Необходимость в обратном элементе возникает при выполнении деления. Всегда ли выполнимо деление, если для каждого элемента существует обратный элемент? Ответ на этот вопрос оказывается утвердительным. Всегда существуют такие элементы группы x и y, для которых $ax = b$ и $ya = b$.

Во всякой группе деление выполнимо, то есть для любых элементов группы a и b можно найти элементы группы x и y, удовлетворяющие уравнениям

$$ax = b \quad \text{и} \quad ya = b.$$

С каким элемеитом (или с какими элементами) группы мы встретимся, разрешив эти уравнения относительно x и y? Умножив первое из уравнений слева на

элемент, обратный a, получим с одной стороны

$$a^{-1}(ax) = (a^{-1}a)\,x = ex = x,$$

а с другой стороны

$$a^{-1}(ax) = a^{-1}b,$$

что возможно лишь в том случае, если $x = a^{-1}b$. В том, что найденный элемент действительно удовлетворяет уравнению, нетрудно убедиться прямой подстановкой:

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

Так как

$$ba^{-1} = (ya)\,a^{-1} = y\,(aa^{-1}) = ye = y,$$

то y может принимать лишь единственное значение и, действительно,

$$(ba^{-1})\,a = b\,(a^{-1}a) = be = b.$$

Итак, мы доказали, что в любой группе всегда выполнимо деление. Справедливо даже более сильное утверждение:

в любой группе деление выполнимо *однозначно*.

Но выполнимость деления сама по себе — условие столь сильное, что из него следует групповое свойство.

Если в некоторой полугруппе выполнимо деление, то эта полугруппа является группой.

Итак, если в некоторой полугруппе деление всегда выполнимо, то эта полугруппа является группой. Для доказательства этого утверждения необходимо убедиться в существовании левого единичного элемента и в том, что для каждого элемента существует левый обратный.

Убедиться в существовании левого единичного элемента достаточно легко: поскольку для каждого элемента a должен существовать такой элемент e, что $ea = a$, то требуется лишь доказать, что именно этот элемент e и будет левым единичным элементом. Но если мы выберем произведение вида eb, то нам не удастся продвинуться в доказательстве ни на шаг, поскольку относительно этого произведения можно что-либо утверждать, лишь когда после элемента e стоит элемент a (действительно, $ea = a$). Поэтому элемент b удобно выбрать в виде произведения, в которое первым множителем входит элемент a. Это всегда можно сделать, так как по предположению для заданного элемента a и любого элемента b найдется такой элемент x, что $ax = b$. Но тогда

$$eb = e\,(ax) = (ea)\,x = ax = b,$$

то есть e — левый единичный элемент.

Теперь уже нетрудно показать, что для каждого элемента существует левый обратный элемент. Действительно, так как деление всегда выполнимо и для любого элемента a и левого единичного элемента e можно найти такой элемент y, для которого $ya = e$, то этот элемент y и будет левым обратным для элемента a.

В приведенном выше доказательстве мы воспользовались при выборе элемента a тем, что какой-то элемент *заведомо принадлежит полугруппе*. До сих пор «содержимое» полугруппы не причиняло нам никаких хлопот, поскольку всегда предполагалось, что в полугруппе существует единичный или левый единичный элемент. Теперь же в принятых предположениях ничего не говорится о том, что в полугруппе существует какой-то элемент. Разумеется, в конкретных случаях это не приводит к каким-либо проблемам, поскольку рассматриваемые полугруппы всегда содержат какой-то элемент. Но строгие чисто логические доказательства сталкиваются с серьезными трудностями, если существование в полугруппе по крайней мере одного элемента не оговорено особо в исходных предпосылках. Поэтому мы будем предполагать, что *полугруппа содержит по крайней мере один элемент*. Тем самым нам удается избежать возможных возражений по поводу того, что соображения, облекаемые в математические формулировки, истинны не всегда или не всегда не истинны.

В любой группе действует закон сокращения элементов слева.

Действительно, деление в группе всегда выполнимо и результат его однозначно определен. Следовательно, если $au = av$, то $u = v$. Именно это свойство и называется законом сокращения слева.

В любой группе действует закон сокращения элементов справа.

Аналогично, если $ra = sa$ (r, a и s — элементы группы), то $r = s$.

Но если для какого-то множества выполняются оба закона (сокраще-

ния слева и справа), то это еще не означает, что перед нами «настоящая» группа. Например, мы убедились в том, что положительные числа образуют полугруппу по сложению. Ясно, что для этой полугруппы выполняются и правило сокращения справа, и закон сокращения слева (равенства $a + u = a + v$ и $u + a = v + a$ возможны лишь в том случае, если $u = v$). Тем не менее положительные числа не образуют группу по сложению. Можно ли наложить такие дополнительные условия, которые позволяют утверждать, что данная полугруппа является группой? Оказывается, такие условия существуют.

Если полугруппа содержит конечное число элементов и в ней выполняются законы сокращения слева и справа, то она является группой.

Покажем, что в полугруппе, обладающей указанными выше свойствами, деление всегда выполнимо. В силу симметрии достаточно доказать, что для любых элементов a и b в полугруппе найдется такой элемент x, для которого $ax = b$.

Поскольку рассматриваемая полугруппа содержит конечное число элементов, то их можно перенумеровать: $x_1, x_2, \ldots, x_n$. Образуем произведения всех элементов и выбранного элемента a: $ax_1, ax_2, \ldots, ax_n$.

Умножая элемент a на x_i, мы каждый раз получаем новые элементы полугруппы, поэтому среди произведений $ax_1, ax_2, \ldots, ax_n$ содержатся все элементы полугруппы (вообще говоря, в ином порядке, чем они были перенумерованы сначала). При этом ни один элемент полугруппы не может встретиться среди произведений $ax_1, ax_2, \ldots, ax_n$ более одного раза. Действительно, если при каких-то натуральных числах i и j выполняется равенство $ax_i = ax_j$, то по закону сокращения слева выполняется равенство $x_i = x_j$, что невозможно, если элементы x_i и x_j различны (то есть при $i \neq j$). Итак, произведения $ax_1, ax_2, \ldots, ax_n$ — различные элементы полугруппы. Их столько, сколько элементов в полугруппе, причем каждый элемент встречается среди произведений $ax_1, ax_2, \ldots, ax_n$ один и только один раз. Но это возможно лишь в том случае, если среди произведений $ax_1, ax_2, \ldots, ax_n$ встречаются все элементы полугруппы.

В частности, любой элемент b полугруппы совпадает с каким-то произведением $ax_1, ax_2, \ldots, ax_n$. Следовательно, в полугруппе существует такой элемент x_i, для которого $ax_i = b$. Но именно это и требовалось доказать.

Итак, сопоставляя и сравнивая различные определения группы, можно утверждать следующее.

Если о полугруппе известно, что

в ней существует левый единичный элемент и для каждого элемента существует обратный,

или что

в ней всегда выполнимо деление, или что

она конечна (то есть содержит конечное число элементов) и в ней действует закон сокращения справа и слева, то эта полугруппа является группой, причем

в ней существует однозначно определенный (двусторонний) единичный элемент;

всегда однозначно выполнимо (двустороннее) деление;

действует закон сокращения справа и слева.

ЗАДАЧИ

1. Доказать, что, если в полугруппе существует правый единичный элемент и для каждого элемента существует правый обратный элемент, то эта полугруппа является группой.

2. На некотором множестве (например, на множестве целых чисел) операция задана следующим образом: $ab = b$ (то есть произведение всегда совпадает со вторым множителем). Доказать, что при этом:

а) получается полугруппа;

б) в этой полугруппе существует левый единичный элемент;

в) для каждого элемента существует правый обратный элемент.

3. Получается ли в предыдущем примере группа? Какие следствия можно извлечь из ответа?

4. Доказать, что в любой группе ни один элемент не обладает «своим» особым единичным элементом, то есть, если для какого-то e и элемента a выполняется равенство $ea = a$, то e — единичный элемент группы.

5. Привести пример конечной полу-

группы с законом сокращения слева, не являющейся группой.

6. Является ли полугруппой пара $\langle P; h\rangle$ из задачи 2 в разделе 2.3?

3.2. Тождества в группе

До сих пор мы определяли группу как пару, состоящую из множества и двухместной операции, удовлетворяющей трем основным условиям. Поскольку в любой группе мы заранее требуем, чтобы эти условия были выполнены, то их можно рассматривать как *аксиомы*.

Понятие аксиомы впервые было использовано в геометрии. Первоначально аксиомы были такими «первичными» истинами, правильность которых предполагалась заранее. Именно поэтому аксиомы не требовалось доказывать, да, собственно говоря, их и невозможно было доказать. Например, такую аксиому: через две различные точки можно провести прямую, и притом только одну. Должно быть, читателю покажется странным, что мы заговорили об аксиомах после того, как во всех рассмотренных примерах со всей тщательностью *доказали*, что аксиомы группы выполнены.

Но стоит лишь внимательно присмотреться к приведенным выше примерам, как можно заметить, что каждый из них заканчивается словами: «... образует группу» (или каким-нибудь аналогичным выражением). Иначе говоря, всякий раз, когда мы говорим: «Это — группа», — *подразумевается*, что аксиомы группы выполнены.

Теоремы и доказательства, использующие только аксиомы группы, называются теоретико-групповыми теоремами и доказательствами.

Например, в предыдущем разделе из аксиом группы мы вывели правила сокращения.

Теоретико-групповые доказательства полезны тем, что результаты, к которым они приводят, остаются в силе для любых «частных» групп. Поскольку мы всегда стремимся получить результаты, обладающие наибольшей общностью, теоретико-групповые теоремы или доказательства *не могут следовать из каких-либо других предпосылок, кроме аксиом группы*. Но неожиданно выясняется, что именно такие общие теоремы и доказательства позволяют избежать многократного рассмотрения большого числа частных случаев. «Частность» означает, что помимо аксиом группы предполагаются выполненными некоторые другие условия, например новые аксиомы.

В теории групп строго соблюдаются два запрета:

1) *не говорить о том, что такое элементы группы*;

2) *не говорить о том, что такое групповая операция*.

Мы не даем точного определения того, что следует понимать под словами «не говорить». По существу они означают следующее. Если известно, например, что элементами группы являются подстановки, а групповая операция состоит в последовательном выполнении подстановок, то соответствующее утверждение уже нельзя считать теоретико-групповой теоремой.

В тех случаях, когда элементы группы и групповая операция заданы конкретно, мы говорим, что перед нами пример группы, и доказательство того или иного утверждения относительно этого примера сводится к применению общей теории групп к данному конкретному примеру. В таких случаях группу принято называть *конкретной группой*. Если же речь идет лишь о выполнении аксиом группы, то группу называют *абстрактной группой*.

Деятельность тех, кто занимается теорией групп и ее применениями, можно разделить на два типа. Во-первых, бывает необходимо доказать, что тот или иной «объект» является конкретной группой (то есть удовлетворяет не только аксиомам группы, но и некоторым другим, частным теоретико-групповым аксиомам). Во-вторых, для абстрактных групп необходимо доказывать определенные утверждения, выполняющиеся во всех конкретных случаях.

Деятельность первого типа, как уже упоминалось, не относится к теории групп, хотя, разумеется связана с ней весьма тесно (ведь именно этой разновидностью деятельности определяется полезность теории групп). Нарисуем теперь в общих чертах простейшие этапы этой деятельности.

Всякий раз, когда речь заходит о группе, предполагается, что задано некоторое множество и на нем какая-то операция. Необходимо еще выяснить, однозначно ли определено это множество (то есть известно ли, какие элементы образуют множество, в каких случаях элементы, заданные различными способами, можно считать тождественными и т. д.). Затем необходимо проверить, является ли операция, введенная на множестве, групповой операцией (то есть принадлежат ли рассматриваемому множеству элементы, сопоставляемые операцией парам элементов множества).

Далее следует проверка ассоциативности: необходимо убедиться в том, существует ли левый единичный элемент и для каждого ли элемента существует левый обратный элемент. (Последнюю проверку можно заменить выяснением того, всегда ли выполнимо деление, а в случае конечного множества — выполняются ли законы сокращения в зависимости от того, что более целесообразно.) После того как это установлено, мы знаем (из общих теорем теории групп), что левый единичный элемент однозначно определен и т. д. (Разумеется, совсем не плохо, если, например, удастся устаиовить, что существует единичный элемент, или выполняется еще какое-нибудь следствие из аксиом группы.)

Обратимся теперь к свойствам абстрактных групп.

Прежде всего докажем так называемую «обобщенную ассоциативность».

В любой группе произведение не зависит от того, как расставлены скобки.

Для трех множителей a, b и c это утверждение означает, что $a(bc) = (ab)c$. Именно поэтому и допустимо говорить об обобщенной ассоциативности. Для четырех множителей скобки можно расставить следующими способами:

$$a[b(cd)],\ a[(bc)d],\ (ab)(cd),\ [a(bc)]d,\ [(ab)c]d.$$

Утверждение относительно обобщенной ассоциативности помимо прочего состоит в том, что эти пять произведений совпадают.

Теорема об обобщенной ассоциативности позволяет в каждом произведении большого числа сомножителей избавиться от лишних скобок, поскольку независимо от расстановки скобок конечный результат оказывается одним и тем же. Следовательно, произведение трех сомножителей можно записывать в виде abc, произведение четырех сомножителей — в виде $abcd$ и т. д. До сих пор мы не упоминали об этом, так как всегда речь шла лишь о произведениях двух сомножителей.

Доказательство осложняется тем, что разобраться в огромном количестве скобок бывает довольно трудно. Поэтому разумнее всего начать с произведений, содержащих небольшое число сомножителей.

Прежде всего теорему об обобщенной ассоциативности необходимо доказать для трех сомножителей. Но в этом случае утверждение теоремы очевидно само по себе, поскольку ассоциативность произведения трех сомножителей входит в число аксиом группы.

Уже в случае четырех сомножителей доказательство ассоциативности становится громоздким. Чтобы доказать, что в каждом из пяти возможных случаев результат оказывается одним и тем же, необходимо доказать 10 равенств. Если вместо этого доказать, что каждое из пяти произведений совпадает с каким-нибудь одним из них, например с последним, то число подлежащих доказательству равенств понизится до четырех. (Здесь мы молчаливо предполагаем транзитивность: если $a = b$, $b = c$, то $a = c$.) Доказав четыре равенства, мы тем самым докажем равенства произведений четырех сомножителей при всех возможных способах расстановки скобок, поскольку, если каждое произведение совпадает с последним, то все произведения равны между собой.

Доказательство того, что четвертое, произведение совпадает с пятым, то есть что $[a(bc)]d = [(ab)c]d$, не вызывает особых трудностей, необходимо лишь воспользоваться ассоциативностью произведений трех сомножителей, заключенных в квадратные скобки (рис. 23). Аналогичным образом можно убедиться в том, что первое произведение совпадает со вторым. Остается лишь доказать, что второе и третье произведения совпадают с пятым (или с четвертым). В этом можно убедиться следующим образом. Пусть $bc = u$ и $ab = v$ (ведь каждое из произведений bc и ab

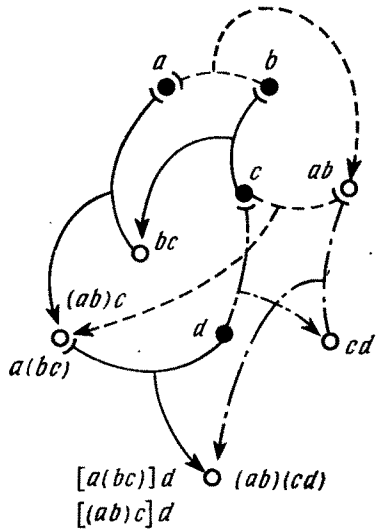


Рис. 23.

является элементом группы). Тогда второе произведение можно записать в виде $a(ud)$, третье — в виде $v(cd)$. Ассоциативность произведений трех сомножителей доказана. Следовательно,

$$a\,(ud) = (au)\,d = [a\,(bc)]\,d \text{ и } v\,(cd) = (vc)\,d = [(ab)\,c]\,d.$$

Продолжая аналогичные рассуждения, можно доказать ассоциативности произведений пяти, шести и большего числа сомножителей. По существу приведенное выше доказательство основано на полной индукции.

Нетрудно заметить, что на протяжении всего доказательства мы использовали лишь одну аксиому группы — аксиому ассоциативности. Следовательно, полученный нами результат остается в силе и для полугрупп.

Из обобщенной ассоциативности, разумеется, следует, что и в любой конкретной группе операция ассоциативна. Ассоциативно сложение и умножение чисел, последовательное выполнение подстановок и т. д. Строго говоря, гораздо важнее другое: во всех этих случаях утверждение об ассоциативности верно не само по себе, не «безусловно», а является закономерным *следствием* ассоциативности произведений трех сомножителей.

Перейдем теперь к рассмотрению одного частного случая, когда все сомножители, входящие в произведение, совпадают, то есть рассмотрим «степени» элементов группы. Поскольку групповая операция ассоциативна, то произведение, состоящее из одинаковых сомножителей, зависит лишь от того, какие сомножители в него входят и сколько их. Следовательно, такое произведение можно рассматривать как «функцию двух переменных». Если в произведение входят сомножители a и число их равно n, но такое произведение мы обозначим a^n. Так как число сомножителей не меньше 2, то и «показатель степени» n не меньше 2.

Из определения степени элемента группы видно, что ассоциативность необходима. Не будь ее, произведение одинаковых сомножителей могло бы зависеть не только от числа сомножителей и от элемента, выбранного в качестве основания степени, но и от расстановки скобок. Подчеркнем: *могло бы* зависеть, но не обязательно зависело бы. У читателя, возможно, появится подозрение, что эта осторожная формулировка — не более чем неуклюжая попытка доказать «раз и навсегда» независимость «произведения» от расстановки скобок. Чтобы рассеять эти необоснованные подозрения, приведем пример «произведения», зависящего от расстановки скобок. Разумеется, такое возможно *лишь в том случае*, если «умножение» не ассоциативно. С неассоциативной операцией нам уже приходилось встречаться: этим свойством обладало возведение в степень, то есть операция $h(a, b) = a^b$. Итак, $h(h(a, a), a) = (a^a)^a = a^{a^2}$ и $h(a, h(a, a)) = a^{a^a}$, но (если $a \neq 1$ или $a \neq 2$) оба произведения различны: например, $3^{3^3} = 3^9$ и $3^{3^3} = 3^{27}$.

Однако не следует думать, что, если операция не ассоциативна, то «возведение в степень» не имеет смысла. Нетрудно представить себе операцию, ассоциативную лишь «при возведении в степень». Это означает, что операция обладает ассоциативностью лишь в том случае, если все сомножители одинаковы, а в общем случае ассоциативно не всякое произведение. Столь «коварную» операцию можно задать даже на множестве целых чисел. Например, пусть операция состоит во взятии среднего арифметического, то есть $s(a, b) = \frac{a+b}{2}$. Так как $s(a, a) = a$, то сколько бы одинаковых элементов ни входило в «произведение», оно всегда будет совпадать с «основанием степени» — любым из элементов. Наоборот, «произ-

ведения» $s(a, s(b, c)) = \frac{1}{2}(a + \frac{b+c}{2}) = \frac{2a+b+c}{4}$ и $s(s(a, b), c) = \frac{1}{2}(\frac{a+b}{2} + c) = \frac{a+b+2c}{2}$ различны, если $a \neq c$. Следовательно, эта операция ассоциативна «при возведении в степень», но не ассоциативна вообще.

Но вернемся теперь к возведению в степень элементов группы. Все названия в этом случае остаются такими же, как при возведении в степень чисел: если $b = a^n$, то элемент b называется n-й степенью элемента a, a — основанием и n — показателем степени. Относительно последнего мы предположили, что он не меньше 2. Но поскольку при возведении в степень мы обращаемся с элементами группы, как с обыкновенными числами, то показатель степени можно определить как произвольное целое число.

Пусть $a^1 = a$, $a^0 = e$ и $a^{-n} = (a^{-1})^n$ (n — натуральное число, a^{-1} —элемент, обратный элементу a). Можно доказать, что степени элемента a удовлетворяют следующему тождеству:

$$a^n a^k = a^{n+k} \text{ и } (a^n)^k = a^{nk}$$

(n и k — произвольные целые числа).

Доказательство этих тождеств наталкивается на многие *вычислительные* трудности, поскольку n-ю степень элемента a можно определить пятью способами. Она равна

a^n — произведению n сомножителей, каждый из которых равен

a при $n > 1$;

a при $n = 1$;

e при $n = 0$;

элементу, обратному a, при $n = -1$;

произведению элементов, обратных a, при $n < -1$.

Множитель a^k также определяется пятью способами. Следовательно, для доказательства первого тождества ($a^n a^k = a^{n+k}$) необходимо рассмотреть 25 вариантов (не считая перестановки множителей a^n и a^k). К тому же возможны различные «подслучаи»: например, если n больше 1, а k меньше 1, то сумма $n + k$ все же может быть больше или равной единице. Нетрудно убедиться в том, что и при доказательстве второго тождества необходимо рассмотреть 25 возможных случаев.

Поскольку рассмотрение столь большого числа случаев было бы весьма громоздко, то мы опустим доказательство. Те, кого интересуют подробности, смогут провести его самостоятельно, используя в каждом отдельном случае соответствующие определения степени элемента.

Упомянем лишь несколько важных следствий из приведенных выше тождеств.

Из первого тождества следует, что степени одного и того же элемента можно переставлять местами

$$a^n a^k = a^k a^n.$$

Если один из показателей n и k положителен, а другой отрицателен, то это соотношение можно рассматривать как обобщение утверждения о том, что «левый обратный» для любого элемента группы совпадает с «правым обратным».

Второе тождество при $n = k = -1$ означает, что *элемент, обратный обратному, совпадает с исходным элементом*

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

(Это соотношение необходимо использовать при доказательстве второго тождества.) Действительно, по определению элемент a^{-1}, обратный элементу a, удовлетворяет соотношению $a^{-1}a = e$. Это же соотношение означает, что элемент a является правым обратным для элемента a^{-1}. Поскольку для каждого элемента группы обратный определен однозначно, то тем самым наше утверждение доказано

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

Этот частный случай также необходимо использовать для доказательства второго тождества. Так как

$-n = n(-1)$, то $a^{-n} = (a^n)^{-1}$. Сопоставляя это соотношение с первоначальным определением обратного элемента, мы приходим к следующему заключению: «n-я степень обратного элемента совпадает с элементом, обратным n-й степени». Оно следует из того, что произведение $(a^{-1})^n a^n$, как можно показать, используя ассоциативность и шаг за шагом «вычеркивая» пары $(a^{-1}a)$, равно e. Поскольку элемент, обратный данному, определен однозначно, то $(a^{-1})^n$ совпадает с элементом, обратным элементу a^n.

По существу второе тождество можно рассматривать как частный случай «возведения в степень произведения». Доказательство известного из арифметики соотношения «n-я степень произведения равна произведению n-х степеней сомножителей» не проходит даже в простейших вариантах. Разумеется, в тривиальных случаях это соотношение остается верным. Например, равенство $a^1b^1 = (ab)^1$ выполняется по определению. Соотношение $(ab)^0 = a^0b^0$ следует из того, что в правой и в левой частях равенства стоят единичные элементы. Однако в общем случае невозможно доказать, что a^2b^2 совпадает с $(ab)^2 = abab$. Действительно, умножив равенство $aabb = abab$ слева на a^{-1}, а справа на b^{-1}, получим $ab = ba$. Следовательно, соотношение $a^2b^2 = (ab)^2$ может выполняться, лишь если $ab = ba$. В этом случае говорят, что элементы a и b *коммутируют, или что их можно переставлять.*

К аналогичному результату мы пришли бы, заменив показатель степени 2 на -1. В общем случае произведение $a^{-1}b^{-1}$ не совпадает с элементом, обратным элементу ab. В этом нетрудно убедиться. Умножив произведение ab слева на произведение обратных элементов, взятых в обратном порядке, мы получим единичный элемент:

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e,$$

то есть

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

Но вернемся снова к рассмотрению степеней одного-единственного элемента. Все степени одного элемента могут быть различными — как, например, целые числа, образующие группу по сложению. Но может случиться и так, что не все степени одного элемента будут различными. Например, если группа содержит конечное число элементов, то, какой бы элемент мы ни выбрали, все его степени не могут быть различными, ибо в противном случае группа содержала бы бесконечно много элементов.

Итак, рассмотрим какой-нибудь элемент a группы, не все степени которого различны, и попытаемся навести некий порядок среди совпадающих степеней.

Прежде всего можно установить, что совпадение степеней зависит лишь от «расстояния» между показателями степени. Это означает, что, если, например, $a^n = a^k$, то, умножив на a, мы получим $a^{n+1} = a^n a = a^k a = a^{k+1}$, а умножив на a^{-1} — равенство $a^{n-1} = a^n a^{-1} = a^k \cdot a^{-1} = a^{k-1}$. Следовательно, достаточно определить те степени, которые совпадают с единичным элементом. Действительно, соотношение $a^n = a^k$ выполняется в том случае, если $a^{n-k} = e$. Это соотношение можно доказать, во-первых, повторив достаточное число раз приведенное выше рассуждение. Во-вторых, если $a^n = a^k$, то $a^{n-k} = a^n a^{-k} = a^k a^{-k} = a^{k-k} = a^0 = e$, а если $a^{n-k} = e$, то цепочка равенств $a^n = a^k a^{n-k} = a^k e = a^k$ формально доказывает наше утверждение.

Используя второе тождество для возведения в степень, получаем: если $a^n = e$, то $a^{nk} = (a^n)^k = e^k = e$ (так как $ee = e$, то любая степень единичного элемента есть единичный элемент). Следовательно, если какая-то «небольшая» степень элемента a совпадает с единичным элементом, то и многие «бóльшие» степени элемента a также совпадают с единичным элементом. Это утверждение справедливо для тем большего числа элементов, чем меньшая степень элемента a (совпадающая с единичным элементом) выбрана первоначально. Это означает, что разумно рассматривать наименьшие степени элементов, обращающиеся в единичные элементы.

Наименьшее положительное целое число d, при котором выполняется равенство $a^d = e$, называется порядком элемента a и обозначается $o(a)$.

Итак, пусть $d = o(a)$. Как нам уже известно, соотношение $a^{dk} = e$ выполняется всегда. Возникает вопрос: не может ли равенство $a^n = e$ выполняться при каком-нибудь другом n? Если n — такое число, то, поскольку $a^d = e$, тем же свойством обладают числа $n + d$ и $n - d$. Следовательно, вычитая d из n достаточное число раз (или, если n отрицательно, прибавляя d к n достаточное число раз), мы получим неотрицательное число, меньшее d и обладающее тем же свойством, что и n. Пусть $n - kd = r$ — такое целое число, для которого

$$0 \leqslant r < d$$

и $a^r = a^{n-kd} = a^n (a^d)^{-k} = ee^{-k} = e$.

Поскольку d — наименьшее положительное число, при котором $a^d = e$, то число r не может быть положительным. Но r — целое неотрицательное число и поэтому не меньше нуля. Следовательно, r может быть только равно нулю. Это означает, что $n = kd$.

Доказано, что $a^n = e$ только в том случае, если показатель степени n кратен порядку элемента a.

Отсюда прежде всего следует, что все элементы

$$e, a, \ldots, a^{d-1} \quad (d = O(a))$$

различны. Действительно, если какие-то два из этих элементов совпадают, то, во-первых, разность их показателей меньше d (поскольку каждый из показателей меньше d), во-вторых, эта разность, как было показано, делится на d и, следовательно, может быть равной только нулю, то есть оба показателя совпадают.

Нетрудно видеть, что любая степень элемента a совпадает с одним из выписанных нами элементов. Действительно, для любого целого числа n найдется такое целое число k, что $n - kd = r$ — целое число, для которого

$$0 \leqslant r < d \text{ и } a^r = a^{n-kd} = a^n (a^d)^{-k} = a^n a^{-k} = a^n.$$

Тем самым наше утверждение доказано.

Если все степени какого-нибудь элемента различны, то он называется элементом бесконечного порядка.

Нетрудно убедиться в том, что число различных степеней элемента a совпадает с порядком элемента a. Но в том случае, когда все степени элемента a различны, порядок элемента a утрачивает смысл. Поэтому определение порядка элемента целесообразно сформулировать так, чтобы порядок элемента всегда совпадал с числом его различных степеней.

ЗАДАЧИ

1. Определить порядок следующих подстановок: (12), (123), (1234). Как можно определить порядок цикла в общем случае?

2. Определить порядок следующих подстановок: (12)(34),(123)(456), (12) × ×(345), (12)(3456). Как можно определить в общем случае порядок подстановки, разложенной в произведение циклов, не имеющих общих элементов?

3. Найти элементы конечного порядка в мультипликативной (операция — обычное умножение) группе вещественных чисел, отличных от нуля.

4. Найти элементы конечного порядка в мультипликативной группе комплексных чисел, отличных от нуля.

5. Найти элементы конечного порядка в группе монотонно возрастающих функций, непрерывных на отрезке [0, 1] (точное определение группы см. в задаче 9 из раздела 2.2).

3.3. Коммутативные группы

Мы видели, что тождества для степеней удается доказать лишь в том случае, если входящие в них элементы можно переставлять. Весьма многие конкретные группы обладают

тем свойством, что любые два их элемента коммутируют. Таковы, например, группы чисел как по сложению, так и по умножению. Именно поэтому представляет интерес особо рассмотреть группы такого типа.

Группа $\langle G, f\rangle$ называется коммутативной, или абелевой, если операция f коммутативна, то есть для любых двух элементов a и b группы G выполняется равенство $f(a, b) = f(b, a)$.

Коммутативная группа обладает *обобщенной коммутативностью*, состоящей в том, что произведение любого числа сомножителей не зависит от их порядка. Истинность этого утверждения не вызывает сомнений, поскольку, переставляя соседние сомножители, мы всегда можем перейти от любого исходного расположения сомножителей к любому другому расположению. Отсюда следует, что соотношение $(ab)^n = a^n b^n$ выполняется при целых n, бóльших единицы. В свою очередь из этого соотношения мы заключаем, что аналогичное равенство выполняется при произвольном целом n и любом числе сомножителей.

Коммутативные группы играют в алгебре весьма важную роль, но мы не будем здесь рассматривать их более подробно.

ЗАДАЧИ

1. Доказать, что все числовые группы как по сложению, так и по умножению всегда коммутативны.

2. Доказать, что группа движений плоскости (с последовательным выполнением движений в качестве групповой операции) неабелева.

3. Пусть a и b — элементы коммутативной группы, причем $o(a) = n$ и $o(b) = k$. Доказать, что:

а) $o(ab)$ делит наименьшее общее кратное чисел n и k;

б) если n и k — взаимно простые числа (то есть не имеют общих делителей, отличных от 1), то $o(ab) = nk$;

в) если n и k — не взаимно простые числа, то может случиться, что $o(ab)$ будет делителем чисел n и k.

4. Доказать, что в абелевой группе произведение элемента конечного порядка и элемента бесконечного порядка всегда имеет бесконечный порядок, а произведение двух элементов бесконечного порядка может иметь конечный порядок.

4.

Теоретико-групповые конструкции

4.1. Подгруппа группы

В приведенных выше примерах групп нам неоднократно встречались такие пары групп, что каждый элемент одной из групп принадлежал другой группе. Напомним несколько таких пар.

1. Группа целых чисел по сложению и группа рациональных чисел по сложению. (Каждое целое число рационально.)

2. Группа отличных от нуля вещественных чисел по умножению и группа отличных от нуля комплексных чисел по умножению. (Каждое вещественное число можно рассматривать как комплексное число.)

3. Группа положительных вещественных чисел по умножению и группа вещественных чисел по сложению. (Каждое положительное вещественное число, разумеется, является вещественным числом.)

4. Группа сдвигов плоскости (относительно умножения преобразований) и группа движений плоскости (относительно умножения преобразований). (Каждый сдвиг принадлежит к числу движений.)

Присмотревшись к этим примерам повнимательнее, нетрудно заметить, что в третьем примере групповые операции в двух группах, образующих пару, различны, а во всех остальных примерах совпадают. Ясно, что в тех трех примерах, в которых групповые операции совпадают,

связь между группами гораздо теснее, чем в том случае, когда групповые операции различны. По существу в каждом из рассмотренных нами примеров речь шла о некоторой связи между двумя группами. Но группы — это не только наборы элементов, а пары, состоящие из множества элементов и заданной на этом множестве операции. Именно поэтому установление связи между группами должно сопровождаться установлением определенной зависимости между групповыми операциями. Если же между операциями в группах никакой зависимости не существует, то, даже располагая самыми подробными сведениями о свойствах «большей» группы, мы сможем очень мало сказать о свойствах «меньшей» группы. В тех же случаях, когда операции в двух группах «совпадают», операция, заданная на большей группе, уже полностью определяет операцию, заданную на меньшей группе — на подгруппе.

Группа $\langle H, h\rangle$ называется подгруппой группы $\langle G, g\rangle$, если H — подмножество множества G и операции g и h совпадают на множестве H.

Прежде чем переходить к рассмотрению примеров подгрупп, попытаемся выяснить, каким образом можно решить, образуют ли элементы, принадлежащие тому или иному подмножеству элементов группы, подгруппу или не образуют.

Прежде всего необходимо, чтобы интересующее нас подмножество было такой группой, в которой умножение совпадает с операцией, заданной на всей группе. На самом подмножестве никакой «своей» групповой операции не задано, и это хорошо, поскольку операцию на нем можно вводить лишь так, как она определена на исходной группе. Поэтому мы должны не задавать операцию на выбранном подмножестве, а проверить, не выводит ли за его пределы операция, определенная на исходной группе, то есть можно ли эту операцию считать групповым умножением на интересующем нас подмножестве. Если это действительно так, то заведомо выполнены следующие условия.

1. *Произведение любых двух элементов подмножества принадлежит подмножеству.* (Иногда это условие формулируют так: подмножество замкнуто относительно умножения.)

Тем самым на подмножестве оказывается заданной операция, причем именно так, что подмножество становится подгруппой. (Более того, операция, превращающая наше подмножество в подгруппу исходной группы, определена единственным образом.) Проверим, все ли аксиомы группы выполнены. Первая аксиома утверждает ассоциативность группового умножения. Но соответствующее тождество выполняется для любых трех элементов исходной группы. Следовательно, оно выполняется и в том случае, если эти три элемента выбраны из рассматриваемого подмножества. Отсюда следует вывод:

ассоциативность можно не проверять.

(Это не только «приятно», но и полезно, потому что именно проверка ассоциативности представляет наибольшую трудность.)

Далее необходимо проверить, существует ли относительно введенной на подмножестве операции левый единичный элемент. Если f — такой элемент, то $ff = f$. Но поскольку $ef = f$ (e — единичный элемент исходной группы), то $ef = ff$, откуда, применяя закон сокращения справа, получаем: $e = f$. Следовательно, если в подмножестве относительно введенной на нем операции существует единичный элемент, то этим элементом может быть только единичный элемент исходной группы. Наоборот, если единичный элемент исходной группы принадлежит выбранному подмножеству, то он, разумеется, является левым единичным элементом относительно определенной на подмножестве операции. Отсюда следует вывод:

2. *Единичный элемент должен принадлежать рассматриваемому подмножеству.*

(«Теоретически» сначала следовало бы проверить, существует ли единичный элемент в выбранном подмножестве. Но «практически» достаточно воспользоваться тем, что этим элементом может быть только единичный элемент исходной группы, и поэтому свести «поиски» к проверке принадлежности одного вполне определенного элемента группы выбранному подмножеству.)

Наконец, следует проверить, для каждого ли элемента подмножества существует принадлежащий подмножеству обратный элемент (относительно определенной на подмножестве операции). Поскольку достоверно известно, что единичный элемент исходной группы должен принадлежать подмножеству, то элемент, обратный любому элементу подмножества, совпадает с элементом, обратным этому элементу в исходной группе. А это означает следующее:

3. *Вместе с каждым элементом подмножество должно содержать обратный элемент.*

Пара $\langle H, h\rangle$ образует подгруппу группы $\langle G, g\rangle$ в том и только в том случае, если H — подмножество множества G, удовлетворяющее условиям 1, 2 и 3 (по определению операция h совпадает с операцией g на H).

Заметим, что условия 1, 2 и 3 можно представить в несколько более простом виде, но проверка условий по-прежнему осталась бы довольно сложной.

В дальнейшем при рассмотрении подгруппы мы *не будем особо задавать на ней операцию, поскольку групповое умножение в подгруппе всегда совпадает с операцией, определенной на исходной группе.*

ПРИМЕРЫ

1. Рассмотрим группу целых чисел по сложению. В ней можно выделить следующие подгруппы:

а) Множество четных чисел, так как сумма двух четных чисел четна, нуль — четное число (его можно представить в виде $2\cdot 0$) и число, обратное или противоположное четному числу, также четно.

б) Множество, содержащее только нуль, так как $0 + 0 = 0$, сам нуль принадлежит множеству и $-0 = 0$.

в) Множество всех целых чисел, так как по определению они образуют группу по сложению.

2. Рассмотрим группу рациональных чисел по сложению. В ней можно выделить следующие подгруппы:

а) Множество целых чисел, так как сумма двух целых чисел — целое число, нуль — целое число и любое число, противоположное целому (то есть равное целому числу с обратным знаком), — также целое.

б) Все подгруппы аддитивной (то есть со сложением в качестве групповой операции) группы целых чисел, так как выполнение всех трех условий «гарантировано» тем, что они выполнены в группе целых чисел.

в) Рациональные числа, представимые в виде дробей с нечетными знаменателями, так как, если знаменатели дробей a/b и c/d нечетны, то и их сумма — дробь $(ad + bc)/bd$ — имеет нечетный знаменатель, нуль можно представить, например, в виде $0/1$, то есть записать в виде дроби с нечетным знаменателем, а число, противоположное рациональному числу (то есть отличающееся от рационального числа знаком), — в виде дроби с тем же знаменателем, что и у исходного числа, в силу чего, если исходное рациональное число представимо в виде дроби с нечетным знаменателем, то и противоположное ему рациональное число также представимо в виде дроби с нечетным знаменателем.

(Мы не могли бы утверждать, что дроби с нечетными знаменателями образуют подгруппу, поскольку любую дробь можно представить в виде дроби с четным знаменателем: на-

пример дробь 2/3 можно записать в виде 4/6. Следовательно, хотя в действительности мы имеем в виду дроби с нечетными знаменателями, следует использовать лишь приведенное выше точное название подгруппы.)

3. Рассмотрим мультипликативную (то есть с умножением в качестве групповой операции) группу вещественных чисел, отличных от нуля. В ней можно выделить следующие подгруппы:

а) Мультипликативная группа положительных вещественных чисел, так как произведение двух положительных вещественных чисел положительно (и вещественно), единица — число положительное и число, обратное положительному, также положительно.

б) Мультипликативная группа рациональных чисел, отличных от нуля,

так как произведение двух отличных от нуля рациональных чисел также является рациональным числом, отличным от нуля, единица — рациональное число и число, обратное отличному от нуля рациональному числу, рационально.

в) Множество, состоящее из чисел $+1$ и -1,

так как произведение любых двух из них (не обязательно различных) равно либо $+1$, либо -1, число $+1$ принадлежит множеству, каждое из двух чисел обратно самому себе и, следовательно, вместе с каждым из чисел $+1$ и -1 множеству принадлежит и обратное число.

Рассмотренные нами примеры позволяют заметить следующее.

1. *Все группы содержат в качестве подгруппы множество, состоящее только из единичного элемента. Такая подгруппа называется единичной подгруппой.*

Это утверждение нетрудно доказать в общем виде: $ee = e$, e принадлежит рассматриваемому множеству и $e^{-1} = e$.

2. *Любая группа содержит себя в качестве подгруппы.*

Это утверждение очевидно, поскольку аксиомы группы заранее считаются выполненными.

3. *Во всякой группе все подгруппы любой подгруппы являются в то же время подгруппами исходной группы.*

Единичная подгруппа и вся группа называются тривиальными подгруппами, а все остальные подгруппы называются истинными подгруппами.

Доказать утверждение 3 можно совсем просто. Во «внутренней» группе операция, единичный элемент и обратные элементы остаются такими же, как и в объемлющей ее «большой» группе. Следовательно, проверяя выполнение условий в «малой» группе, мы тем самым как бы проверяем и выполнение условий в исходной группе.

Как показывают примеры, элементы каждой подгруппы обычно обладают каким-нибудь отличительным свойством. Иногда все элементы, входящие в подгруппу, удается «назвать поименно». К последнему способу построения подгруппы можно прибегнуть в том случае, если подгруппа содержит конечное число элементов и проще перебрать все ее элементы, чем найти их отличительный признак.

Если подгруппа задана каким-то свойством, то не составляет особого труда определить, обладает ли этим свойством единичный элемент. (Как правило, единичный элемент обладает всеми «хорошими» свойствами. Действительно, из двух других условий следует, что единичный элемент принадлежит рассматриваемому подмножеству.) Таким образом, по существу необходимо проверить лишь два условия: замкнутость относительно умножения и взятия обратного элемента. *Если группа конечна, то есть содержит конечное число элементов*, то достаточно проверить одно из этих условий.

Если некоторое подмножество элементов конечной группы содержит единичный элемент и замкнуто относительно умножения, то оно является подгруппой.

Действительно, если a — элемент конечной группы, то число различных степеней элемента a не может быть больше числа элементов в группе. Следовательно, a — элемент конечного порядка, и если $d = o(a)$, то из соотношения $aa^{d-1} = a^d = e$ мы получаем что a^{d-1} — элемент, обратный элементу a. Это означает, что в конечной группе элемент, обратный любому элементу группы, совпадает с одной из его степеней. Поэтому, если какое-то подмножество элементов конечной группы замкнуто относительно умножения, то вместе с каждым своим элемеитом оно содержит и все его степени, а следовательно, и обратный элемент.

Отображения множеств

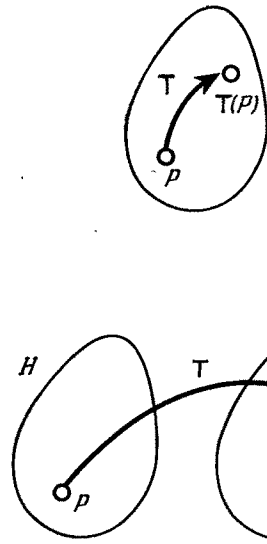
На многих примерах мы убедились, что подгруппы можно задавать, указывая какой-нибудь отличительный признак. Именно так обстояло, например, дело с движениями на плоскости, когда мы рассматривали только сдвиги или только повороты вокруг одной и той же точки. Но аналогичный принцип позволяет определить и все движения на плоскости. Действительно, преобразование плоскости называется движением, если:

1) оно устанавливает взаимно-однозначное соответствие между точками плоскости, причем

2) расстояние между любыми двумя точками до преобразования совпадает с расстоянием между теми точками, в которые они переходят под действием преобразования.

Условие 2 представляет собой не что иное, как дополнительное требование, налагаемое на взаимно-однозначные преобразования плоскости. Если о взаимно-однозначных преобразованиях плоскости известно, что они образуют группу (относительно «обычной» операции — последовательного выполнения преобразований), то условие 2 «предписывает» рассматривать лишь те из них, которые образуют определенную подгруппу.

Прежде всего необходимо проверить правильность исходного пункта наших рассуждений, то есть убедиться в том, что движения действительно составляют часть некоторой *группы*.



Это – множество H, нарисованное еще раз

Рис. 24

Но вместо того, чтобы изучать отображения плоскости на себя, гораздо удобнее рассмотреть отображения произвольного множества на себя. Итак, рассмотрим все взаимно-однозначные отображения на себя некоторого заданного множества H. Прежде всего необходимо договориться относительно того, что следует понимать под взаимно-однозначным отображением множества на себя.

Если каждому элементу множества H поставлен в соответствие некоторый элемент множества H, то мы говорим, что задано отображение множества H в себя. Если $\mathbf{T}$ — отображение множества H в себя и P — элемент множества H, то $\mathbf{T}(P)$ означает элемент, в который $\mathbf{T}$ отображает P (рис. 24).

[Рис. 24 можно рассматривать как своего рода аналогию привычного всем изображения системы координат (рис. 25). Вместо двух вещественных прямых на рис. 24 показаны множество H в «двух экземплярах». Обозначения также выбраны по ана-

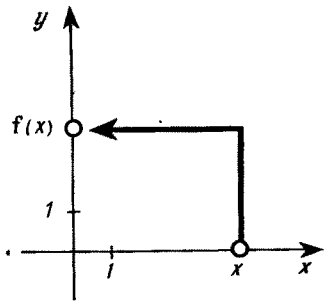


Рис. 25

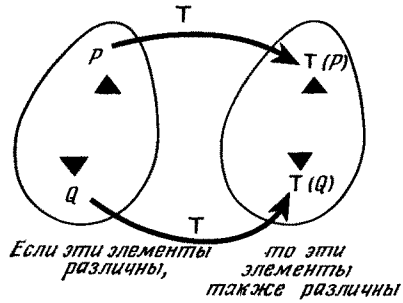


Рис. 26

логии с обозначениями функций.]

Произведение двух отображений множества H в себя определим как последовательное выполнение одного отображения за другим, то есть как «подстановку» одной «функции» в другую.

Если отображение **T** ставит в соответствие различным элементам множества H различные элементы того же множества и при этом каждый элемент множества H оказывается образом какого-нибудь элемента, то **T** называется взаимно-однозначным отображением множества H на себя.

Произведением взаимно-однозначных отображений **T** и **S** множества H на себя называется такое отображение **R**, которое любой элемент P множества H переводит в элемент $\mathbf{R}(P) = \mathbf{S}(\mathbf{T}(P))$. Это отображение **R** принято обозначать **TS**.

[Возможно, кому-нибудь покажется странным, что $\mathbf{TS}(P)$ совпадает с $\mathbf{S}(\mathbf{T}(P))$. Такое впечатление обманчиво и связано с тем, что обозначения «аргумента функции» (P) и отображения **TS** лишь стоят рядом, не «взаимодействуя» друг с другом. Во многих случаях удобно считать, что «функция» действует не «вправо», а «влево», то есть записывать ее вместо привычного обозначения $\mathbf{T}(P)$ в виде $(P)\mathbf{T}$. При такой записи $(P)\mathbf{TS} = ((P)\mathbf{T})\mathbf{S}$, что во многих случаях облегчает понимание того, как действует отображение. Иногда обозначение «функции» записывают в виде «показателя» (то есть в виде $P^{\mathbf{T}}$), что также позволяет упростить описание отображения.]

Важное значение имеет следующая теорема:

Взаимно-однозначные отображения любого множества на себя образуют группу относительно произведения отображений.

Докажем эту теорему. Ясно, что произведение двух взаимно-однозначных отображений множества H на себя также является отображением этого множества на себя. Необходимо лишь доказать, что произведение взаимно-однозначно. Пусть $\mathbf{R} = \mathbf{TS}$. Если элементы P и Q различны, то и их образы $\mathbf{T}(P)$ и $\mathbf{T}(Q)$ различны, поскольку **T** — взаимно-однозначное отображение (рис. 26). Но тогда элементы $\mathbf{S}(\mathbf{T}(P))$ и $\mathbf{S}(\mathbf{T}(Q))$ также различны, поскольку не только **T**, но и **S** — взаимно-однозначное отображение. Выберем теперь произвольный элемент R множества H. Так как отображение **S** взаимно-однозначно, то для элемента R найдется такой элемент S, что $R = \mathbf{S}(S)$ (рис. 27), а для элемента S в свою очередь найдется (поскольку отображение **T** взаимно-однозначно) такой элемент T, что $S = \mathbf{T}(T)$, то есть $R = \mathbf{S}(\mathbf{T}(T))$. Но это и означает, что произведение отображений **S** и **T** взаимно-однозначно. Следовательно, произведение отображений также порождает взаимно-однозначное отображение множества на себя.

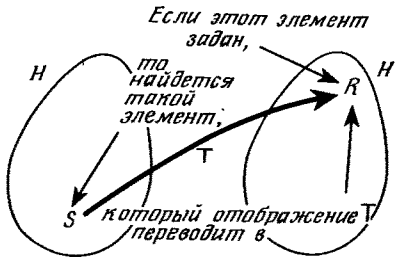
Чтобы доказать ассоциативность, рассмотрим три взаимно-однозначные отображения **T**, **S** и **U**. Отображения $\mathbf{U}(\mathbf{ST})$ и $(\mathbf{US})\mathbf{T}$ совпадают, если любой элемент P множества H они переводят в один и тот же элемент.

Но

$$[\mathbf{U}(\mathbf{ST})](P) = (\mathbf{ST})[\mathbf{U}(P)] = \mathbf{T}\{\mathbf{S}[\mathbf{U}(P)]\}$$

и, кроме того,

$$[(\mathbf{US})\mathbf{T}](P) = \mathbf{T}\{(\mathbf{US})(P)\} = \mathbf{T}\{\mathbf{S}[\mathbf{U}(P)]\}.$$



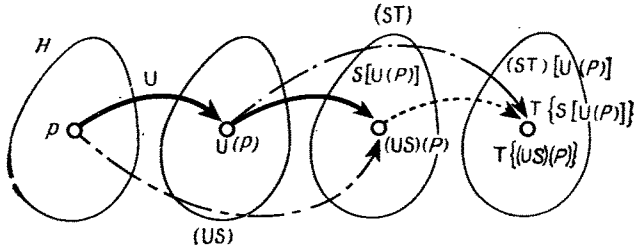


Рис. 27

Следовательно, оба произведения U(ST) и (US)T совпадают (рис. 27). Тем самым ассоциативность доказана.

Нетрудно проверить, что тождественное отображение служит единичным элементом. Действительно, если $I(P) = P$ для любого элемента P множества H, то $I(T(P)) = T(P)$. Следовательно, I — левый единичный элемент. (Ясно, что тождественное отображение взаимно-однозначно.)

Обратный элемент определим так же, как мы делали это прежде: если отображение T переводит элемент P множества H в элемент Q, то отображение T^{-1} возвращает Q на место P. Поскольку все элементы множества H можно представить в виде $T(P)$, то отображение T^{-1} задано на всем множестве H. Так как отображение T переводит различные элементы множества H в различные, то отображение T^{-1} однозначно определено на всех элементах Q множества H. По определению $T^{-1}(T(P))$ совпадает с P, поэтому T^{-1} действительно отображение, обратное отображению T. Осталось лишь доказать, что отображение T^{-1} взаимно-однозначно. Но $Q = T(P)$, $R = T(S)$. Следовательно, если $P = S$, то $Q = R$, поэтому $P = T^{-1}(Q)$ и $S = T^{-1}(R)$ не могут совпадать при различных элементах Q и R. Кроме того, из условия $T^{-1}(T(P)) = P$ мы заключаем, что отображение T^{-1} переводит в каждый элемент множества H какой-нибудь элемент того же множества. Эти два свойства и означают, что T^{-1} — взаимно-однозначное отображение множества H на себя.

Итак, взаимно-однозначные отображения множества H на себя образуют полугруппу, в которой существует левый единичный элемент и для каждого элемента — левый обратный элемент, то есть группу.

Доказанная нами теорема по существу означает следующее.

Если впредь нам понадобится доказать, что некоторые взаимно-однозначные отображения, обладающие тем или иным отличительным свойством, образуют группу, то можно не заниматься проверкой, во-первых, ассоциативности и, во-вторых, взаимной однозначности произведения отображений или обратных отображений. Необходимо проверить лишь, обладает ли произведение отображений отличительным свойством интересующего нас множества отображений.

Если взаимно-однозначные отображения множества H на себя наделены некоторым отличительным свойством, причем этим свойством обладают также:

1) произведение любых двух рассматриваемых отображений;

2) тождественное отображение;

3) отображение, обратное любому из отображений, обладающих требу-

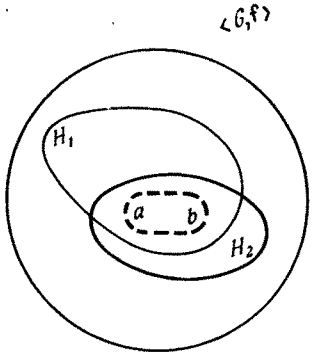


Рис. 28

емым отличительным свойством, то такие отображения образуют подгруппу группы всех взаимно-однозначных отображений множества H на себя.

Если в качестве отличительного свойства выбрана способность отображений «не изменять что-нибудь» в множестве H, то, как нетрудно доказать, условия 1—3 выполняются. Например, отображения могут сохранять расстояния между точками, отношения расстояний, расстояния и направления, упорядочение чисел на отрезке [0, 1] (это означает, что под действием отображений бо́льшие числа переходят в бо́льшие). Во всех этих случаях отличительное свойство отображений состоит в их способности оставлять «что-нибудь» неизменным. Из приведенных выше примеров видно, что все перечисленные нами отображения образуют группы.

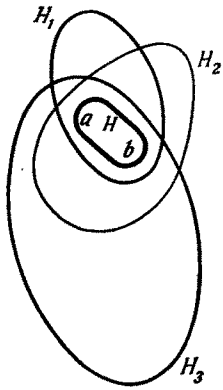


Рис. 29

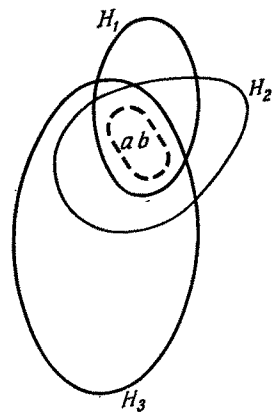


Рис. 30

Если отличительных свойств несколько, то каждое из них можно рассматривать в отдельности. Элементы группы, обладающие каждым из «подсвойств», образуют подгруппу. Образуют подгруппу и те элементы, которые обладают полным набором отличительных свойств. Эта подгруппа состоит из элементов, каждый из которых принадлежит всем подгруппам, выделенным при рассмотрении отдельных отличительных свойств. Аналогичная взаимосвязь существует и между подгруппами всех других групп:

элементы группы, принадлежащие двум или большему числу подгрупп, образуют подгруппу.

Пусть, например, H_1, H_2,... и т. д. — некоторые подгруппы группы $\langle G, f\rangle$ и H — множество элементов группы, принадлежащих каждой из подгрупп H_1, H_2,... и т. д. Предположим, что множеству H принадлежат элементы группы a и b. Тогда элементы a и b принадлежат каждой из подгрупп H_1, H_2, ... и т. д. (рис. 28 и 29). Следовательно, произведение элементов a и b также принадлежит каждой из подгрупп H_1, H_2,... и т. д. (рис. 30). Но это и означает, что произведение ab принадлежит подмножеству H, так как именно H содержит общие элемеиты всех подгрупп (рис. 31).

Аналогичным образом можно показать, что H содержит единичный элемеит (так как он принадлежит каждой из подгрупп) и что вместе с любым элементом множест-

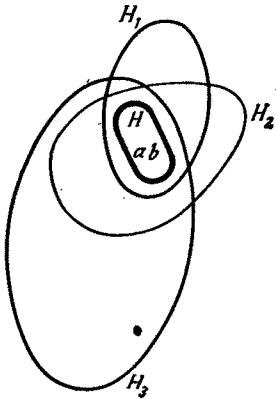


Рис. 31

во H содержит и обратный элемент (поскольку обратный элемент также принадлежит каждой из подгрупп).

Это теперь уже доказанное свойство подгрупп позволяет находить в любой группе «наименьшую» подгруппу, содержащую заранее заданные элементы группы.

Рассмотрим элементы группы a, b, c, ... Наименьшая подгруппа, которой принадлежат эти элементы, заведомо содержится во всякой другой подгруппе, включающей в себя помимо элементов a, b, c, ..., возможно, еще какие-то другие элементы группы. Следовательно, наименьшая подгруппа содержится в общей части всех таких подгрупп (состоящей из общих элементов группы $a, b, c, \ldots$). Любая меньшая подгруппа не могла бы содержать все перечисленные элементы, поскольку общая часть меньше любой другой подгруппы, содержащей элементы a, b, c, ...

Выясним теперь, что можно сказать о подгруппе, порожденной элементами a, b, c. (Во всех остальных случаях рассуждения проводятся так же.)

Общая часть подгрупп любой группы, содержащих элементы a, b, c, ..., называется подгруппой, порожденной этими элементами, и обозначается $\{a, b, c, \ldots\}$.

Подгруппа, порожденная элементами a, b, c, ... , — наименьшая из подгрупп, содержащих каждый из этих элементов.

Если подгруппа, порожденная элементами a, b, c, ..., совпадает со всей группой, то a, b, c, ... называются системой образующих элементов группы.

Поскольку подгруппа $\{a, b, c\}$ содержит элементы a, b, c, то три элемента этой подгруппы уже известны. Кроме того, мы знаем, что подгруппе $\{a, b, c\}$ принадлежит единичный элемент. По свойству подгруппы вместе с каждым из элементов a, b, c ей принадлежат и все (целые) степени элемента, а также произведения степеней. Следовательно, подгруппа $\{a, b, c\}$ состоит из элементов вида $a^{i_1} b^{i_2} c^{i_3} a^{i_4} \ldots$, где показатели $i_1, i_2, \ldots$ — целые числа. Некоторые из произведений $a^{i_1} b^{i_2} \cdot c^{i_3} a^{i_4} \ldots$ могут не содержать какого-нибудь из элементов a, b, c, но и в этом случае их можно представить в таком же виде, положив соответствующие показатели равными нулю. Произведение двух элементов, записанных в виде произведения степеней образующих элементов a, b, c, также представимо в виде произведения степеней образующих элементов; элемент, обратный элементу вида $a^{i_1} b^{i_2} c^{i_3} a^{i_4} \ldots$, имеет аналогичный вид (только сомножители следуют в обратном порядке, а каждый из показателей степени взят со знаком минус); наконец, единичный элемент также можно записать в виде произведения степеней (с показателями, равными нулю) образующих элементов.

Группа, порожденная некоторыми элементами, состоит из произведений степеней образующих элементов.

ПРИМЕРЫ

1. Найти подгруппу, порожденную числом 2, аддитивной группы целых чисел.

Эта подгруппа состоит из всех «степеней» числа 2, то есть (в силу аддитивности) из всех целых кратных числа 2, или, что то же, из четных чисел.

2. Найти подгруппу $\{4, 6\}$ аддитивной группы целых чисел.

Элементами этой подгруппы (в силу аддитивности) служат числа вида $4k + 6n$, где k и n — целые числа. Ясно, что все эти числа четные, поскольку их можно представить в виде $2(2k + 3n)$. Но все ли четные числа принадлежат интересующей нас подгруппе? Да, все, так как среди чисел вида $4k + 6n$ содержится и число $2 \cdot 2 + 6(-1) = 2$ и, следовательно, все элементы подгруппы, порожденной числом 2, то есть все четные числа. Итак, рассматриваемая подгруппа состоит из четных чисел.

3. Найти подгруппы $\{0\}$ и $\{1\}$ аддитивной группы целых чисел.

Первая подгруппа состоит из кратных нуля, а поскольку любое число, кратное нулю, равно нулю, то эта подгруппа содержит только один элемент — число 0. Вторая подгруппа состоит из всех чисел, кратных единице, и поэтому совпадает со всей аддитивной группой целых чисел. Отсюда следует, что единица — (единственный) образующий элемент аддитивной группы целых чисел.

4. Найти подгруппу $\{1/2, 1/4, 1/8, \ldots\}$ аддитивной группы рациональных чисел.

В эту подгруппу должны входить все целые кратные рационального числа $1/2$, то есть любое целое число вторых. Кроме того, подгруппе $\{1/2, 1/4, 1/8, \ldots\}$ принадлежит любое целое число четвертых, восьмых и т. д. Следовательно, эта подгруппа содержит все дроби, которые можно записать в таком виде, чтобы в знаменатель не входили никакие простые числа, кроме 2 (то есть в знаменателе стояли лишь степени числа 2). Но такие дроби образуют подгруппу, содержащую все заданные числа. Следовательно, подгруппа $\{1/2, 1/4, 1/8, \ldots\}$ состоит из дробей, знаменателями которых служат степени числа 2.

5. Найти подгруппу $\{2\}$ мультипликативной группы положительных чисел.

Эта подгруппа состоит из степеней числа 2 (на этот раз — из «настоящих» степеней, так как в мультипликативной группе положительных чисел операцией служит обычное умножение).

6. Найти подгруппу $\{1\}$ мультипликативной группы положительных чисел.

Поскольку число 1 служит единичным элементом мультипликативной группы положительных чисел, то подгруппа $\{1\}$ состоит лишь из числа 1.

7. Описать подгруппу $\{(01), (02), (03), (04), (05), (06)\}$ группы всех подстановок элементов 0, 1, 2, 3, 4, 5, 6.

При рассмотрении подстановок мы убедились, что любую подстановку можно представить в виде произведения транспозиций, перечисленных в фигурных скобках. Следовательно, подгруппа $\{(01), (02), (03), (04), (05), (06)\}$ содержит все подстановки элементов 0, 1, 2, 3, 4, 5, 6.

Один-единственный элемент, выбранный из любой группы, порождает некоторую подгруппу. Такая подгруппа, порожденная одним элементом, называется *циклической подгруппой*.

Если данная группа порождена одним элементом, то она называется циклической группой.

Если a — элемент группы, то подгруппа $\{a\}$ состоит из всех различных степеней элемента a. Следовательно, число элементов в подгруппе $\{a\}$ совпадает с порядком элемента a.

Итак, число элементов в подгруппе $\{a\}$ равно $o(a)$. В соответствии с этим порядком группы называется число элементов в ней, если группа конечна. Если же группа содержит бесконечно много элементов, то порядок ее бесконечен.

ЗАДАЧИ

1. Найти подгруппы $\{n\}$, $\{-n\}$, $\{n, k\}$, где n и k — заданные целые числа, аддитивной группы целых чисел.

2. Найти подгруппы

$\{-1\}$; $\{-1, 2\}$; $\{1, 2, 3, 4, \ldots\}$;

$\{1/2, 1/3, 1/4, \ldots\}$;

$\{-1, 2, 3, 4, \ldots\}$;

{положительные числа, меньшие единицы}

мультипликативной группы вещественных чисел, отличных от нуля.

3. Найти подгруппу $\{(01), (0123456)\}$ группы всех подстановок элементов 0, 1, 2, 3, 4, 5, 6.

4.2. Фактор-группа группы

Вернемся теперь к самому началу — к группе подстановок. Группу подстановок n элементов принято обозначать S_n. Как будет показано в дальнейшем, проводимые ниже рассуждения не зависят от n, но для большей наглядности мы выберем какое-нибудь конкретное значение n.

Стационарная подгруппа

Пусть $n = 5$. Группа подстановок S_5 содержит особые, весьма важные подгруппы. Предположим, например, что переставляемыми элементами служат цифры 0, 1, 2, 3, 4. Тогда подстановки, оставляющие на месте любую из этих цифр, очевидно, образуют подгруппу. Действительно, если каждая из двух подстановок оставляет на месте, например, цифру 0, то, выполнив эти две подстановки одну за другой (или подействовав на цифры подстановкой, обратной любой из двух подстановок), мы снова переведем цифру 0 в 0. Тождественная подстановка обладает свойством сохранять 0 (как, впрочем, и любую другую цифру) на прежнем месте. Поскольку цифра 0 остается «неподвижной», или стационарной, под действием подстановок, то рассматриваемые подстановки образуют *стационарную подгруппу* группы S_5. Говоря о стационарной подгруппе, необходимо указывать не только число элементов, на которых заданы ее подстановки, но и тот элемент, который они оставляют неподвижным. Этот элемент мы будем указывать в виде верхнего правого «индекса». Итак, группа подстановок S_5 содержит стационарные подгруппы S_5^0, S_5^1, S_5^2, S_5^3 и S_5^4.

Как уже говорилось, подгруппа S_5^0 состоит из подстановок, оставляющих на месте цифру 0. Выясним, образуют ли подгруппу подстановки, переводящие в 0 не 0, а 1.

Нетрудно убедиться в том, что такие подстановки не могут образовывать подгруппу. Объясняется это среди прочего и тем, что тождественная подстановка переводит 0 именно в 0, а не в 1. Тем не менее выделение таких подстановок в особое множество полезно, поскольку то, что каждая из входящих в множество подстановок переводит в 0 один и тот же элемент, свидетельствует о тесной связи между подстановками.

Все подстановки можно разбить на классы в зависимости от того, какой из переставляемых ими элементов они переводят в нуль.

В приведенных выше примерах мы видели, что любая подстановка переводит каждый элемент в какой-нибудь из элементов, принадлежащих ее области определения. Обозначим через S_5^{ij} множество подстановок, переводящих элемент i в элемент j. То, что подстановка P переводит элемент i в элемент j, то есть принадлежит множеству S_5^{ij}, мы условимся обозначать так: $P \in S_5^{ij}$. В частном случае при $i = j$ полученное множество подстановок совпадает со стационарной подгруппой S_5^i.

Выясним прежде всего, как подмножество S_5^{0i} связано со стационарной подгруппой вуля S_5^0.

Если подстановка P переводит 0 в 0, а подставовка Q переводит 0 в 1, то подстановка PQ (произведение подстановок понимается в обычном смысле) переводит 0 в 1. (Сведения, которыми мы располагаем о подставовках P и Q, слишком скудны и ве позволяют ничего утверждать о том, «что происходит» с подстановкой QP.) Отсюда следует, что, если выбрать любой элемент из мвожества S_5^{01}, например подстановку (01), то при любой подста-

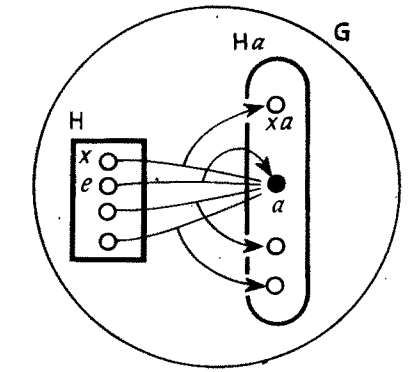


Рис. 32

иовке P из стационарной подгруппы S_5^0 подстановка $P(01)$ всегда будет принадлежать миожеству S_5^{01}. Вопрос заключается лишь в том, все ли элементы множества S_5^{01} удастся при этом получить. Действительно, если подстановка Q переводит 0 в 1, то можно ли найти в стациокарной подгруппе нуля такую подстановку P, при которой $Q = P(01)$? Поскольку подстановки образуют группу, то подстановка P существует, и притом только одна. Но это еще не все: требуется установить, прииадлежит ли подстаиовка P стационарной подгруппе нуля или не принадлежит. Так как $Q = P(01)$, то $P = Q(01)^{-1} = Q(01)$, поскольку подстаиовка (01) совпадает со своей обратной подстаиовкой. Подстановка Q переводит 0 в 1, а за ней следует подстановка (01), переводящая 1 снова в 0. Это и означает, что $P \in S_5^0$.

Итак, все элементы множества S_5^{01} можно получить, умножая по порядку все элементы множества S_5^0 на подстановку (01), поэтому вместо обозначения S_5^{01} часто бывает удобно использовать обозначение $S_5^0 \cdot (01)$. Оно лучше раскрывает «структуру» множества S_5^{01}.

Аналогичным образом, выбирая вместо 1 цифры 2, 3 и 4, мы получим, что все элементы группы подстановок встречаются среди элементов подмножеств

$$S_5^0,\ S_5^0(01),\ S_5^0(02),\ S_5^0(03),\ S_5^0(04)$$

только один раз.

Смежные классы

Эти множества называются *правыми смежными классами* группы S_5 по подгруппе S_5^0.

Аналогичным образом можно определить и *левые смежные классы* группы S_5 по подгруппе S_5^0. В их число помимо подгруппы S_5^0 входят множества вида $(0i)S_5^0$.

Элементами этих множеств являются подстановки вида $(0i)P$, где P — любая подстановка, принадлежащая стационарной подгруппе S_5^0. Поскольку подстановка $(0i)$ переводит i в 0, а подстановка P оставляет 0 на месте, то все элемекты одного левого смежного класса переводят число i в 0. Отсюда следует, что левые смежные классы не имеют общих элементов. Остается лишь выяснить, все ли элементы группы принадлежат какому-нибудь левому смежному классу. Рассмотрим, например, подстановку Q, переводящую 1 в 0. Подстановка $P = (01)\,Q$ переводит сначала 0 в 1, а затем 1 снова в 0. Действительно, $P \in S_5^0\,(01)^{-1} = (01)$, так как $Q = (01)\,P$. Следовательно, любой элемент группы принадлежит одному из левых смежиых классов.

Наши рассуждения справедливы не только для конкретной группы (мы привели их для группы S_5). Пусть G — произвольная группа, H — любая из ее подгрупп. Выберем в группе G фиксированный элемент a и составим все произведения вида xa, где x — элемент подгруппы H (рис. 32). Множество произведений принято обозначать Ha. Оно называется *правым смежным классом* группы G по подгруппе H.

Множество произведений вида ax, где x — проиэвольный элемент подгруппы H, принято обозначать aH. Оно называется левым смежным классом группы G по подгруппе H. Множество Ha называется правым смежным классом.

Покажем, что *каждый элемент группы принадлежит ровно одному правому смежному классу*. (Разумеется, аналогичное утверждение справедливо и для левых смежных классов.)

Нетрудно видеть, что каждый элемент группы принадлежит какому-нибудь смежному классу. Действительно, рассмотрим элемент a группы G. Поскольку единичиый элемент e принадлежит подгруппе H, то элемент $a = ea$ входит в правый смежный класс Ha.

Предположим, что элемент a принадлежит также правому смежному классу Hb. Требуется доказать, что тогда этот смежный класс совпадает со смежным классом Ha. По предположению элемент a можно представить в виде $a = hb$, где h — некоторый фиксированный элемент подгруппы H. Но если x — произвольный элемент подгруппы, то, с одной стороны, $xa = (xh)b$, а с другой стороны, $xb = (xh^{-1})a$.

Так как H — подгруппа, то произведения xh и xh^{-1} принадлежат H. Поэтому из первого равенства следует, что каждый элемент правого смежного класса Ha принадлежит правому смежному классу Hb, а в силу второго равенства каждый элемент правого смежного класса Hb принадлежит правому смежному классу Ha. Итак, два рассмотренных нами смежных класса совпадают.

Смежные классы позволяют доказать теорему Лагранжа, в которой говорится об одном интересном свойстве конечных групп.

Теорема Лагранжа. Порядок любого элемента конечной группы является делителем порядка группы.

Пусть группа G содержит n элементов, а подгруппа H — k элементов. Правому смежному классу Ha принадлежат элементы вида xa, где x — произвольный элемент подгруппы H. Так как элементов x может быть не больше, чем элементов в подгруппе H, то смежный класс Ha содержит не больше элементов, чем подгруппа H. Но все элементы вида xa различны (это следует из закона сокращения), поэтому смежный класс Ha содержит ровно столько элементов, сколько содержит их подгруппа H. Если число правых смежных элементов равно m, то общее число элементов группы равно mk, так как каждый из m смежных классов содержит по k элементов (рис. 33). Но соотношение $n = mk$ означает, что k—делитель числа n, то есть *порядок конечной группы всегда делится на порядок любой подгруппы.*

Теорема Лагранжа устанавливает довольно жесткие пределы для существования подгрупп данной группы. Из нее нетрудно вывести важное следствие относительно элементов группы.

Если a — элемент группы G, то порядок $o(a)$ элемента a и порядок подгруппы $\{a\}$ по определению совпадают. По теореме Лагранжа порядок подгруппы $\{a\}$ делит порядок группы G. Следовательно, и порядок $o(a)$ элемента a также делит порядок группы G.

На примере подстановок мы видели, что для стационарной подгруппы левые смежные классы, как правило, отличаются от правых смежных классов. Но если группа коммутативна, то все равно, записан ли элемент в виде xa или ax. Рассмотрим, например, аддитивную группу целых чисел и выделим в ней подгруппу всех четных чисел. Смежный класс по этой подгруппе мы получим, выбрав все числа вида $a + x$, где x — произвольное четное число. Возможны два случая: если число a четно, то смежный класс содержит четные числа; если число a нечетно, то мы получим нечетные числа. Следовательно, существуют два смежных класса аддитивной группы целых чисел по подгруппе четных чисел.

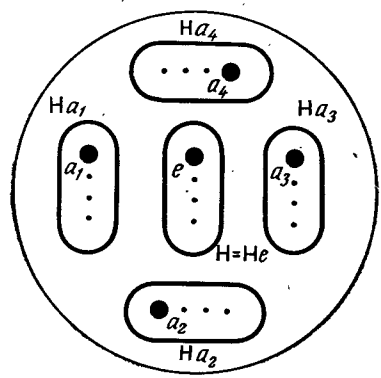


Рис. 33

Нетрудно заметить, что сумма двух четных чисел *всегда четна*, сумма одного четного и нечетного чисел *всегда нечетна*, а сумма двух нечетных чисел *всегда четна*.

Аналогичным образом можно получить разбиение аддитивной группы целых чисел по подгруппе не четных, а, например, делящихся на 3 чисел.

Смежный класс, содержащий число 0, представляет собой не что иное, как выбранную подгруппу, то есть состоит из чисел, делящихся на 3. Обозначим его [0]. Элементы смежного класса, содержащего число 1, мы получим, прибавив по 1 к числам, делящимся на 3. Все числа, образующие новый смежный класс, при делении на 3 дают остаток 1. Обозначим этот смежный класс [1]. Аналогичным образом можно убедиться в том, что смежный класс, которому принадлежит число 2, состоит из чисел,

дающих при делении на 3 остаток 2. Обозначим этот смежный класс [2].

Поскольку всякое целое число (в том числе и отрицательное) при делении на 3 дает в остатке 0, 1 или 2, то других смежных классов не существует.

Таким образом, ответ на вопрос, какому из смежных классов принадлежит сумма двух чисел, зависит не от самих чисел, а от того, какие остатки они дают при делении на 3. Например, если одно из двух чисел при делении на 3 дает остаток 1, а другое — остаток 2, то их сумма всегда будет делиться на 3.

Выясним, на чем основано это свойство. Пусть H — подгруппа группы $\langle G, f\rangle$, а aH и bH — два левых смежных класса. Мы хотим убедиться в том, что произведение элементов, взятых из смежных классов aH и bH (порядок классов одинаков для всех произведений), не зависит от выбора элементов и всегда принадлежит одному и тому же смежному классу.

Ясно, что элемент a принадлежит смежному классу aH, а элемент b — смежному классу bH. Следовательно, произведение любых двух элементов, из которых первый взят из смежного класса aH, а второй — из смежного класса bH, должно принадлежать тому же смежному классу, что и произведение ab. Элементы смежных классов aH и bH можно представить в виде ax и by, где x и y — произвольные элементы подгруппы H, а их произведение — в виде $axby$. Поскольку все произведения $axby$ должны принадлежать тому же смежному классу, что и произведение ab, то в подгруппе H существует элемент h, при котором $axby = abh$, или (после сокращения на a) $xby = bh$. Умножая обе стороны последнего равенства справа на y^{-1} и полагая $z = hy^{-1}$, получаем: $xb = bz$. Но поскольку элементы h и y^{-1} принадлежат H, то и $z = hy^{-1}$ также принадлежит H, поэтому соотношение $xb = bz$ позволяет прийти к приведенному ниже выводу.

Для любого элемента b группы G и любого элемента a подгруппы H существует элемент z подгруппы H, удовлетворяющий соотношению $xb = bz$, в силу чего каждый правый смежный класс по подгруппе H содержится в некотором левом смежном классе по той же подгруппе H.

Этот результат очень напоминает одно свойство, обнаруженное у коммутативных групп: всякий левый смежный класс коммутативной группы является одновременно и правым смежным классом, и наоборот. Более того, с помощью довольно хитроумного «трюка» можно показать, что это утверждение следует из полученного результата. Итак, требуется доказать, что для любого элемента b и любого элемента x подгруппы найдется элемент u подгруппы, для которого выполняется соотношение $bx = ub$. Вместо этого равенства рассмотрим соотношение для обратных элементов, которое запишем в виде $x^{-1}b^{-1} = b^{-1}u^{-1}$.

Поскольку вместе с элементом x подгруппа содержит обратный элемент x^{-1}, то в левой части равенства стоит некоторый элемент правого смежного класса Hb^{-1}. Следовательно, как показано выше, этот элемент принадлежит левому смежному классу b^{-1}H, то есть его можно представить в виде $b^{-1}v$, где v — некоторый элемент подгруппы H. Если теперь элемент v подгруппы записать в виде $v = u^{-1}$ (при этом, разумеется, $u = v^{-1}$), то элемент u также принадлежит подгруппе H, и мы получаем требуемое равенство.

Итак мы показали, что смежные классы могут обладать интересующим нас свойством лишь в том случае, если левые и правые смежные классы по подгруппе совпадают. Но остается не выясненным, следует ли из совпадения левых и правых смежных классов неизменная принадлежность произведения элементов двух смежных классов одному и тому же смежному классу. Нетрудно видеть, что ответ на этот вопрос утвердительный.

Действительно, если для заданного элемента b группы и произвольного элемента x подгруппы существует такой элемент z подгруппы, для которого выполняется соотношение $xb = bz$, то, выбрав еще один элемент y подгруппы, мы получим цепочку равенств $(ax)(by) = a(xb)y = a(bz)y = (ab)(zy)$. Следовательно, произведение элементов группы ax и by принадлежит тому же левому смежному классу, что и элемент ab, поскольку вместе с элементами

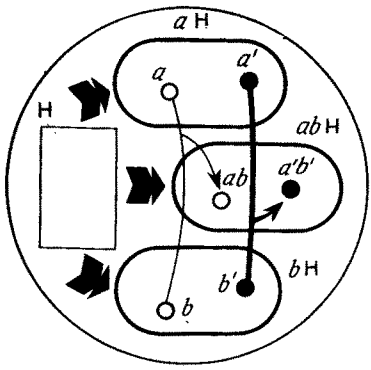


Рис. 34

z и y подгруппа содержит и их произведение. Этот важный результат заслуживает того, чтобы мы сформулировали его еще раз.

Подгруппа H группы G называется *нормальным делителем*, или *инвариантной подгруппой*, если для любых двух смежных классов aH и bH по подгруппе H произведение $a'b'$ произвольного элемента a' из класса aH и произвольного элемента b' из класса bH всегда принадлежит одному и тому же смежному классу abH (рис. 34).

Как мы видели, в коммутативных группах всякая подгруппа является нормальным делителем. Прежде чем приводить новые примеры нормальных делителей, попытаемся заменить отличительный признак, приведенный в определении инвариантной подгруппы, каким-нибудь другим, более «удобным в обращении».

Подгруппа H группы G является нормальным делителем в том и только в том случае, если каждый левый смежный класс по H совпадает с некоторым правым смежным классом по H (и наоборот).

Отличительный признак нормального делителя, состоящий в том, что всякий левый смежный класс по нормальному делителю H является одновременно и правым смежным классом, можно сформулировать следующим образом: для произвольного элемента a группы G смежные классы aH и Ha совпадают. Более того, как мы заметили, для этого достаточно, чтобы все элементы смежного класса aH (разумеется, при *любом* элементе a группы G) лежали в смежном классе Ha. Иначе говоря, в подгруппе H для произвольного элемента x существует (также принадлежащий подгруппе H) такой элемент z, что $ax = za$. Это равенство позволяет найти элемент z: $z = axa^{-1}$. Следовательно, отличительный признак нормального делителя H утверждает, что если a — произвольный элемент группы, а x — элементы подгруппы H, то z также должен принадлежать H.

Итак, *подгруппа* H *группы* G *является нормальным делителем в том и только в том случае, если при любом элементе* a *группы* G *и произвольном элементе* x *подгруппы* H *элемент* axa^{-1} *принадлежит подгруппе* H

Рассмотрим некоторые примеры подгрупп.

ПРИМЕРЫ

1. Четные подстановки (в группе всех подстановок, содержащей n элементов). Четными называются подстановки, разложимые в произведение четного числа транспозиций. (Мы воспользуемся сейчас тем, что четность подстановки не зависит от того, в произведение каких транспозиций она разложена.) Поскольку произведение двух четных подстановок заведомо представимо в виде произведения четного числа транспозиций, то оно также принадлежит подмножеству четных подстановок. Единичный элемент группы подстановок можно записать, например, в виде (01)(01). В случае конечной группы этих двух свойств уже достаточно, чтобы мы получили подгруппу. Далее, если P — произвольная подстановка, представимая в виде произведения k транспозиций, то разложение подстановки P^{-1} мы получим, записав обратные транспозиции в обратном порядке. Поскольку каждая транспозиция совпадает с обратной себе, то в разложение под-

становки P^{-1} входят те же k транспозиций, что и в разложение подстановки P, только в обратном порядке. Рассмотрим теперь четную подстановку Q. По определению она допускает разложение в произведение некоторого четного числа (например, $2m$) транспозиций. Следовательно, подстановку PQP^{-1} можно представить в виде произведения $k + 2m + k$, то есть $2(k + m)$ подстановок, а это означает, что PQP^{-1} — четная подстановка. Именно это и требовалось доказать.

2. Функции вида $y = x + c$ (в группе линейных функций). Линейными называются функции вида $y = ax + b \quad (a \neq 0)$. Они образуют группу относительно линейной замены переменной x : $y = (ax + b) \circ (cx + d) = a(cx + d) + b = (ac)x + (ad + b)$.

В силу соотношения $y = (x + c) \circ (x + d) = x + (d + c)$ «произведение» двух функций заданного вида также имеет требуемый вид. Единичный элемент группы — функция $y = x$ — представима в виде $y = x + c$ $(c = 0)$. Наконец, функцией, обратной функции $y = x + c$, является линейная функция $y = x - c$, так как $(x + c) - c = x$. Эта функция представима в требуемом виде $y = x - c = x + (-c)$. Итак, мы показали, что функции вида $y = x + c$ образуют подгруппу в группе линейных функций. Для того чтобы эта подгруппа была нормальным делителем, она вместе с любыми двумя элементами f и g должна содержать и элемент $g \circ f \circ g^{-1}$. Если g — функция $y = ax + b$, то g^{-1} — функция $y = (a^{-1})x + (a^{-1}b)$. Следовательно, для произвольной функции $y = x + c$ мы получаем:

$$(ax + b) \circ (x + c) \circ (a^{-1}x - a^{-1}b) =$$
$$= (ax + b) \circ (a^{-1}x - a^{-1}b + c) =$$
$$= a(a^{-1}x - a^{-1}b + c) + b =$$
$$= x - b + ac + b = x + ac,$$

то есть функция $g \circ f \circ g^{-1}$ также имеет требуемый вид. Тем самым доказано, что функции $y = x + c$ действительно образуют нормальный делитель в группе линейных функций (относительно линейной замены независимой переменной).

3. Движения на плоскости (в группе преобразований подобия). Как уже говорилось, преобразованиями подобия на плоскости называются такие преобразования, при которых расстояния между парами точек изменяются, но так, что отношение расстояний постоянно. Иначе говоря, для всякого преобразования подобия $\mathbf{T}$ найдется такое положительное вещественное число λ (зависящее от преобразования), что, если расстояние между произвольно выбранными точками P и Q плоскости равно d, то расстояние между точками $\mathbf{T}(P)$ и $\mathbf{T}(Q)$ равно λd. Ранее мы уже убедились в том, что все движения на плоскости, как и все преобразования подобия, образуют группу относительно произведения (последовательного выполнения) преобразований. Поскольку групповая операция в обоих случаях одинакова и все движения являются преобразованиями подобия (с $\lambda = 1$), то движения на плоскости образуют подгруппу группы преобразований подобия.

Необходимо еще доказать, что движения образуют не просто подгруппу, а *нормальный делитель* в группе преобразований подобия. Возьмем движение $\mathbf{S}$ и образуем преобразование подобия $\mathbf{TST}^{-1}$ ($\mathbf{T}$ — произвольное преобразование подобия).

Для доказательства того, что $\mathbf{TST}^{-1}$ — движение, воспользуемся следующим замечанием. Если расстояние между точками $\mathbf{T}(P)$ и $\mathbf{T}(Q)$ равно умноженному на λ расстоянию между точками P и Q, то расстояние между точками $P = \mathbf{T}^{-1}(\mathbf{T}(P))$ и $Q = \mathbf{T}^{-1}(\mathbf{T}(Q))$ равно умноженному на λ^{-1} расстоянию между точками $\mathbf{T}(P)$ и $\mathbf{T}(Q)$. Следовательно, зная коэффициент подобия для исходного преобразования, можно найти коэффициент подобия обратного преобразования (для этого достаточно заменить λ на λ^{-1}), поскольку этот коэффициент не зависит от выбора пары точек.

Пусть P — произвольная точка плоскости, $P_1 = \mathbf{T}^{-1}(P)$, $P_2 = \mathbf{S}(P_1)$ и $P_3 = \mathbf{T}(P_2)$. Аналогичным образом определим для данной точки Q точки Q_1, Q_2 и Q_3. Пусть d — расстояние между точками P

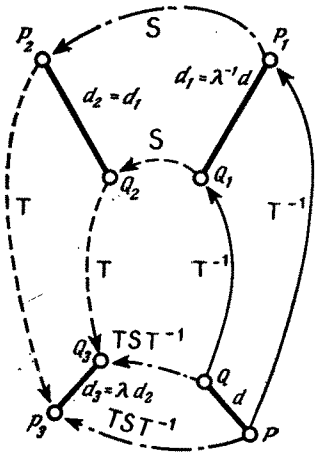


Рис. 35

и Q, d_1 — расстояние между точками P_1 и Q_1, d_2 — расстояние между точками P_2 и Q_2, d_3 — расстояние между точками P_3 и Q_3 (рис. 35).

Преобразование **T** изменяет расстояние между любыми двумя точками в λ раз, преобразование $\mathbf{T}^{-1}$ — в λ^{-1} раз, а преобразование **S** оставляет все расстояния неизменными, так как **S** — движение. Следовательно,

$$d_1 = \lambda^{-1}d, \quad d_2 = d_1 \text{ и } d_3 = \lambda d_2,$$

откуда

$$d_3 = \lambda d_2 = \lambda d_1 = \lambda(\lambda^{-1})\, d = d.$$

Поскольку полученное преобразование $\mathbf{TST}^{-1}$ также принадлежит к числу преобразований подобия, то отношение расстояний между парами точек до и после преобразования не зависит от выбора пары точек. Как показано выше, существует пара точек, для которых это отношение равно 1. Следовательно, оно всегда равно 1, а это означает, что под действием преобразования $\mathbf{TST}^{-1}$ расстояние между любой парой точек сохраняется, то есть $\mathbf{TST}^{-1}$ — движение. Итак, мы доказали, что движения образуют нормальный делитель в группе преобразований подобия.

Но оставим примеры и обратимся снова к рассмотрению смежных классов.

Нормальные делители характеризуются тем, что, выбрав по одному элементу из двух построенных по нормальному делителю смежных классов, мы всегда получим произведение, принадлежащее одному и тому же смежному классу независимо от того, какие элементы выбраны из двух заданных смежных классов (рис. 34).

Это позволяет любым двум смежным классам по нормальному делителю группы поставить в соответствие третий смежный класс — тот, которому принадлежат произведения элементов двух выбранных смежных классов. Прежде чем выводить отсюда те или иные следствия, полезно сначала рассмотреть множество произведений рассмотренного нами типа во всей общности.

Итак, пусть A и B — два подмножества произвольной группы. (Предполагается, что каждое из подмножеств содержит по крайней мере один элемент. Рассматривать подмножества, не содержащие ни одного элемента, вполне допустимо, но, поскольку мы стремимся к большей наглядности, то удобнее считать, что подмножества A и B не пусты.)

Рассмотрим произведение ab элемента a множества A и элемента b множества B. Множество всех таких произведений называется *произведением комплексов* — множеств A и B — и обозначается AB. (О «комплексах» мы заговорили потому, что подгруппы групп часто называют комплексами. Кроме того, название «произведение комплексов» удобно сохранить за произведением множеств, определение которого приведено выше, чтобы его можно было отличать от другого произведения множеств.)

Подмножества элементов группы образуют относительно умножения комплексов полугруппу. То, что умножение комплексов определено на всех подмножествах элементов группы, очевидно. Необходимо лишь показать, что эта операция ассоциативна. Выберем для этого три подмножества элементов группы и обозначим их A, B и C.

Элементами множества $(AB)C$ служат произведения, первый множитель которых принадлежит множеству AB, а второй — множеству C. Так как множество AB состоит из произведений вида ab, где a — произвольный элемент множества A,

а b — произвольный элемент множества B, то элементы множества $(AB)C$ — это произведения вида $(ab)c$, где a — произвольный элемент множества A, b — произвольный элемент множества B и c — произвольный элемент множества C. Аналогично можно убедиться в том, что множество $A(BC)$ состоит из произведений вида $a(bc)$, где элементы a, b и c выбраны так же, как это было сделано выше. Поскольку каждое произведение $(ab)c$ совпадает (в силу ассоциативности группового умножения) с составленным из тех же элементов произведением $a(bc)$, то миожества $(AB)C$ и $A(BC)$ состоят из одних и тех же элементов. Следовательно, эти два множества совпадают. (Разумеется, иногда случается, что в некоторых произведениях какой-нибудь элемент возникает «не единожды», так как произведения различных пар элементов могут совпадать.)

Умножение комплексов позволяет дать новое определение нормального делителя группы.

Подгруппа H является нормальным делителем в том и только в том случае, если произведение комплексов, в качестве которых выбраны любые два левых смежных класса по H, также является левым смежным классом по H.

Рассмотрим подгруппу H группы G и левые смежные классы aH и bH. Произведение комплексов $(a\text{H})(b\text{H})$ содержит элемент ab и поэтому является левым смежным классом, которым может быть только левый смежный класс abH. Еще до того, как мы перешли к более подробному рассмотрению умножения комплексов, было ясно, что подгруппа H является нормальным делителем в том и только в том случае, если при любых смежных классах aH и bH произведение комплексов $(a\text{H})\cdot(b\text{H})$ содержится в левом смежном классе abH.

Следовательно, достаточно доказать, что произведение комплексов $(a\text{H})(b\text{H})$ содержится в левом смежном классе abH в том и только в том случае, если оно совпадает с этим смежным классом. Ясно, что коль скоро произведение комплексов совпадает с каким-то смежным классом, то оно содержится в нем. Итак, предположим, что произведение комплексов $(a\text{H})(b\text{H})$ содержится в левом смежном классе abH. Любой элемент этого смежного класса можно представить в виде abh, где h — произвольный элемент подгруппы H. Поскольку a — элемент смежного класса aH, а $bh (h \in \text{H})$ — элемеит смежного класса bH, то abh — элемент произведения комплексов $(a\text{H})(b\text{H})$. Следовательно, это произведение комплексов действительно совпадает с левым смежным классом abH. (Впрочем, последнее утверждение справедливо для любой подгруппы: произведение комплексов всегда содержит соответствующий смежный класс, но в общем случае оно содержит не один, а несколько смежных классов.)

Полученный результат можно сформулировать в более общем и более сжатом виде:

подгруппа H *является нормальным делителем в том и только в том случае, если взятые по* H *левые смежные классы образуют полугруппу по умножению комплексов.*

Это утверждение можно разбить на две части. Одна из них гласит: на левых смежных классах определена операция умножения комплексов. По доказанному выше, именно эта часть утверждения означает, что подгруппа H является нормальным делителем. Вторая часть утверждения отмечает «полугрупповое свойство» умножения комплексов — ассоциативность. Нетрудно видеть, что этим свойством обладают любые комплексы. Следовательно, умножение комплексов всегда ассоциативно независимо от того, оговариваем ли мы это свойство заранее или обходим молчанием. Но почему бы в таком случае не опустить вторую часть утверждения и сохранить только первую? Вторую часть утверждения мы привели потому, что

если левые смежные классы по подгруппе H *образуют полугруппу по умножению комплексов, то эта полугруппа является группой.*

В правильности этого утверждения мы убедимся, если нам удастся показать, что в полугруппе существует левый единичный элемент и вместе с каждым элементом она содержит элемент, обратный ему относительно левой единицы.

Как известно, произведение левых смежных классов можно получить следующим образом: $(a\text{H})(b\text{H}) = ab\text{H}$ (разумеется, если выполнить умножеиие). При $a = e$ (e — единичный элемент группы), следуя этому правилу, находим: $(e\text{H})(b\text{H}) = b\text{H}$. Таким образом, левый смежный класс eH служит левым единичным элементом полугруппы, образуемой левыми смежми классами по умножению комплексов. Выбрав $a = b^{-1}$, приходим к соотношению $(b^{-1}\text{H})(b\text{H}) = e\text{H}$, означающему, что ле-

вый смежный класс $b^{-1}H$ является левым обратным для левого смежного класса bH (и также принадлежит рассматриваемой полугруппе).

Небезынтересно отметить, что смежный класс eH совпадает с подгруппой H. Кроме того, как нетрудно понять, левый смежный класс $b^{-1}H$ состоит из элементов, обратных элементам левого смежного класса bH.

Группа, образованная левыми смежными классами группы $\langle G; f\rangle$ по нормальному делителю N относительно умножения комплексов, называется фактор-группой исходной группы и обозначается G/N.

Нетрудно заметить, что в обозначении фактор-группы, как и в обозначении подгруппы, мы не указываем в явном виде групповую операцию. Мы поступаем так потому, что групповая операция в фактор-группе однозначно определена групповой операцией в исходной группе. В дальнейшем мы будем часто опускать символ групповой операции в обозначении группы, коль скоро по самому множеству нетрудно догадаться, какая операция на нем задана, а все другие операции лишены смысла.

Рассмотрим несколько примеров фактор-групп.

ПРИМЕРЫ

1. Пусть G — группа целых чисел, а N — подгруппа четных чисел. Найдем фактор-группу G/N. (Групповая операция в G — сложение. Фактор-группа G/N существует, так как N — нормальный делитель.)

Мы уже знаем, что в G существуют два смежных класса: один из них совпадает с подгруппой N и, следовательно, состоит из четных чисел, другой представляет собой не что иное, как множество всех нечетных чисел. Для краткости условимся первый смежный класс называть просто «четным», а второй смежный класс «нечетным». Пользуясь этой терминологией, групповую операцию фактор-группы можно описать следующим образом:

четный + *четный* = *нечетный* + *нечетный* = *четный*,

четный + *нечетный* = *нечетный* + *четный* = *нечетный*.

[Эта «таблица умножения» общеизвестна. Хотя в данном случае слова «четный» и «нечетный» имеют необычный смысл (например, «четный» означает не четное число, а множество всех четных чисел), все же наша «таблица умножения» отражает привычные всем свойства четных и нечетных чисел.]

2. Пусть G — группа целых чисел, а N — группа чисел, делящихся на 3. Найдем фактор-группу G/N (групповая операция в G — сложение. Фактор-группа существует в силу коммутативности сложения).

Смежные классы группы G, приведенной в этом примере, нам уже приходилось рассматривать, и мы обнаружили, что всего их три: множество чисел, делящихся на 3, и множества чисел, дающих при делении на 3 остатки 1 и 2. Эти смежные классы мы обозначили [0], [1] и [2]. Сумму двух классов остатков, или вычетов, определим следующим образом (это и будет групповой операцией в фактор-группе). Сложив соответствующие числа, стоящие в квадратных скобках, определим, какой остаток дает при делении на 3 их сумма, и будем считать суммой смежных классов тот, которому принадлежит полученный остаток. «Таблица умножения» для фактор-группы G/N имеет следующий вид:

$$[0] + [0] = [1] + [2] = [2] + [1] = [0];$$

$$[0] + [1] = [1] + [0] = [2] + [2] = [1];$$

$$[0] + [2] = [2] + [0] = [1] + [1] = [2].$$

Из «таблицы умножения» ясно, что фактор-группа коммутативна. Кроме того, можно утверждать, что система образующих элементов состоит из смежного класса [1], поскольку все смежные классы совпадают с его «степенями»: [1], [1] + [1] =

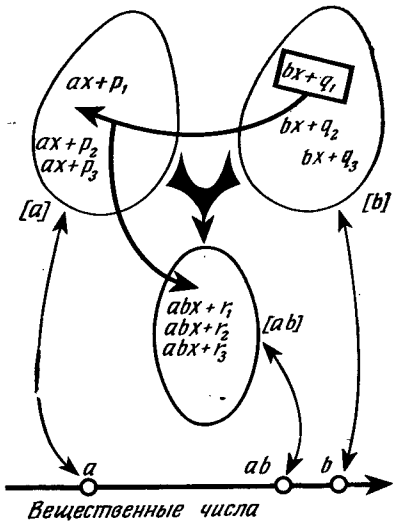


Рис. 36

$= [2]$ и $[1] + [1] + [1] = [0]$. Поскольку фактор-группа порождена одним-единственным элементом, то она циклическая.

3. Пусть G — группа всех подстановок n элементов, а N — подгруппа четных подстановок. Найдем фактор-группу G/N.

Рассматривая примеры нормальных делителей, мы убедились в том, что N действительно является нормальным делителем группы G. Было показано, что помимо смежного класса N существует еще один смежный класс — множество нечетных подстановок, который мы обозначим P. Поскольку произведение двух четных или двух нечетных подстановок — всегда четная подстановка, а произведение четной и нечетной подстановок (независимо от того, какая из них первая и какая — вторая) — всегда нечетная подстановка, то таблица умножения для смежных классов имеет следующий вид:

$$NN = PP = N \quad \text{и} \quad NP = PN = P.$$

(Из этой таблицы видно, что фактор-группа G/N коммутативная и циклическая; образующим элементом служит смежный класс P.)

Интересно заметить, что, если и в этом случае ввести сокращенные названия для смежных классов, то получится фактор-группа, состоящая, как и в первом примере, из двух элементов: «четного» и «нечетного». Более того, нетрудно проверить, что «таблицы умножения» в обоих примерах совпадают, хотя «символы» или «названия» операций различны.

4. Пусть G — группа линейных функций, а N — подгруппа линейных функций вида $x + b$. Найдем фактор-группу G/N.

Ранее мы уже имели возможность убедиться в том, что N — нормальный делитель. Следовательно, фактор-группа G/N существует, и ее элементами служат смежные классы по N. Прежде всего выясним, каким образом можно распознать, принадлежат ли данные линейные функции одному смежному классу или не принадлежат. Так как N содержит линейные функции вида $x + c$, то все функции вида $(x + c) \circ (ax + b) = (ax + b) + c = ax + (b + c)$ принадлежат тому же правому смежному классу, что и линейная функция $ax + b$. Следовательно, функции, принадлежащие одному и тому же смежному классу, имеют одинаковые коэффициенты при x. Остается ответить лишь на один вопрос: если коэффициенты при x двух линейных функций совпадают, то всегда ли такие функции принадлежат одному и тому же смежному классу? Нетрудно видеть, что всегда. Например, для линейных функций $ax + b$ и $ax + d$ получаем

$$ax + d = ax + b + (d - b) =$$

$$= (x + [d - b]) \circ (ax + b)$$

и

$$x + (d - b) \in \mathrm{N}.$$

Эта проверка показывает, что в рассматриваемом примере смежные классы можно «пометить» отличными от нуля вещественными числами: каждому вещественному числу поставить в соответствие какой-нибудь смежный класс, причем различным числам — различные смежные классы. Вещественному числу a мы со-

поставим смежный класс, которому принадлежат функции вида $ax + b$. Чтобы смежные классы можно было отличить от вещественных чисел, условимся обозначать через $[a]$ смежный класс, «помеченный» вещественным числом a. Из соотношения $(ax + b) \circ (cx + d) = a(cx + d) + b = (ac)x + (ad + b)$ следует, что умножение смежных классов производится по правилу $[a][c] = [ac]$ (рис. 36). Нетрудно видеть, что умножение смежных классов происходит «так же», как умножение отличных от нуля вещественных чисел.

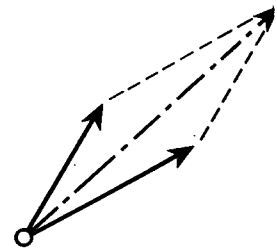


Рис. 37

ЗАДАЧИ

1. Найти фактор-группу G/N в следующих случаях:

а) G — аддитивная группа комплексных чисел, N — подгруппа вещественных чисел;

б) G — мультипликативная группа отличных от нуля комплексных чисел, N — подгруппа положительных вещественных чисел;

в) G — мультипликативная группа отличных от нуля комплексных чисел, N — подгруппа комплексных чисел с модулем, равным 1;

г) G — аддитивная группа вещественных чисел, $N = \{2\pi\}$;

д) G — группа преобразований подобия, N — подгруппа движений;

е) G — группа всех подстановок цифр 1, 2, 3, 4, N — подгруппа, порожденная подстановками (12)(34) и (13)(24).

2. Пусть G — группа линейных функций, H — подгруппа функций вида ax. Описать левые и правые смежные классы по подгруппе H. Сколько общих элементов имеет в общем случае левый смежный класс по подгруппе H с правым смежным классом по той же подгруппе? Сколько общих элементов имеет подгруппа H со смежным классом группы G по N, где N — подгруппа линейных функций вида $y = x + c$? Найти произведения комплексов HN и NH.

3. Пусть H — подгруппа, N — нормальный делитель группы G, M — множество общих элементов подгрупп H и N. Доказать, что M — нормальный делитель подгруппы H и что, если H — нормальный делитель группы G, то и M — нормальный делитель группы G.

4.3. Прямое произведение групп

Рассматривая векторы на плоскости, нетрудно убедиться в том, что они образуют группу по сложению векторов. Операция сложения векторов производится по *правилу параллелограмма*. Если считать, что все векторы отложены от некоторой фиксированной точки, то суммой двух векторов будет вектор, совпадающий с диагональю параллелограмма, сторонами которого служат векторы-слагаемые (рис. 37, 38).

Поскольку начальная точка всех векторов фиксирована, то векторы однозначно определяются заданием концов. Если ввести на плоскости систему координат и все векторы от-

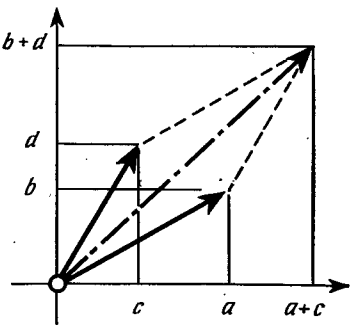


Рис. 38

кладывать от ее начала, то векторы будут однозначно определяться координатами концов, которые мы назовем координатами векторов. Зная координаты векторов-слагаемых, *можно вычислить* координаты вектора-суммы: если координаты векторов равны (a, b) и (c, d), то координаты их суммы равны $(a + c, b + d)$.

Итак, векторы задаются парами чисел, и операция сложения векторов сводится к нахождению сумм первых и вторых координат в отдельности.

Но аналогичным способом можно *из любых* двух групп строить новую группу.

Рассмотрим две группы $\langle A; f\rangle$ и $\langle B; g\rangle$. Если мы хотим построить по ним какую-то группу, то необходимо указать элементы этой группы и групповую операцию.

Пусть элементами новой группы будут пары элементов (a, b), где $a \in A$, $b \in B$, причем равенство $(a_1, b_1) = (a_2, b_2)$ выполняется лишь в том случае, если $a_1 = a_2$ и $b_1 = b_2$.

Групповую операцию h определим так, чтобы над первыми «компонентами» производилась операция f, а над вторыми — операция g:

$$h((a_1, b_1), (a_2, b_2)) = \\ = (f(a_1, a_2), g(b_1, b_2)).$$

Построенная нами группа называется прямым произведением групп A и B и обозначается $A \times B$.

Прежде всего необходимо доказать, что прямое произведение двух групп действительно является группой. Для простоты условимся опускать знаки всех операций и считать, что два элемента, стоящие рядом, означают произведение, то есть $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$. Элементы прямого произведения известны [это — пары (a, b)], и операция «умножения» на них определена (и сводится к выполнению операции f над первыми компонентами и операции g над вторыми компонентами пар). Следовательно, необходимо лишь доказать, что прямое произведение удовлетворяет трем аксиомам, входящим в определение группы.

Ассоциативность операции h будет доказана, если мы убедимся в том, что прямое произведение любых трех элементов получается одним и тем же при двух различных способах расстановки скобок. Действительно, соотношения

$$[(a_1, b_1)(a_2, b_2)](a_3, b_3) = \\ = (a_1a_2, b_1b_2)(a_3, b_3) = (a_1a_2a_3, b_1b_2b_3);$$

$$(a_1, b_1)[(a_2, b_2)(a_3, b_3)] = \\ = (a_1, b_1)(a_2a_3, b_2b_3) = (a_1a_2a_3, b_1b_2b_3)$$

доказывают ассоциативность операции, определенной на прямом произведении (при этом существенно используется ассоциативность групповой операции как в группе A, так и в группе B).

Для дальнейшего нам понадобятся единичные элементы групп A и B, а также элементы, обратные элементам этих групп. Поскольку элементы и групповые операции обеих групп легко отличимы (на «первом месте» каждой пары стоят только элементы группы A, на которые действует операция f, на «втором месте» — только элементы группы B, на которые действует операция g), то, обозначив единичные элементы обеих групп через e, а обратные элементы через «минус первые степени», мы не создадим никакой «путаницы».

Не составляет труда обнаружить в прямом произведении элемент, который может быть единичным элементом группы, а также элемент, обратный данному. Их легко угадать, и правильность догадки настолько очевидна, что по существу не требует доказательства. Мы ограничимся лишь тем, что «предъявим» читателю единичный элемент прямого произведения и элемент, обратный данному. Итак, мы утверждаем: (e, e) — левый единичный элемент прямого произведения, (a^{-1}, b^{-1}) — элемент, левый обратный элементу (a, b).

Первое утверждение [относительно (e,e)] следует из соотношения $(e, e)(a, b) = (ea, eb) = (a, b)$, второе утверждение — из соотношения $(a^{-1}, b^{-1})(a, b) = (a^{-1}a, b^{-1}b) = (e,e)$.

Используя прямое произведение групп, можно утверждать, что аддитивную группу векторов на плоскости допустимо рассматривать как прямое произведение аддитивной группы вещественных чисел на себя.

ЗАДАЧИ

1. Доказать, что, если A — циклическая группа порядка p, B — циклическая группа порядка q, где p и q — различные простые числа, то их прямое произведение $A \times B$ — циклическая группа порядка pq.

2. Доказать, что, если A и B — циклические группы порядка p, то их прямое произведение $A \times B$ — не циклическая группа.

3. Доказать, что, если A и B — конечные группы, то порядок их прямого произведения равен произведению порядков групп A и B.

4. Доказать, что элементы прямого произведения двух групп, у которых на втором месте стоит единичный элемент, образуют нормальный делитель прямого произведения.

5. Доказать, что каждый из смежных классов, полученных при разложении прямого произведения двух групп по нормальному делителю, описанному в предыдущей задаче, содержит ровно один элемент, у которого на первом месте стоит единичный элемент.

5

Отображения групп

5.1. Изоморфизм групп

Нам уже неоднократно приходилось встречать (главным образом в задачах предыдущего раздела) группы, обладавшие «сильным сходством». Например, при построении факторгруппы группы преобразований подобия по подгруппе движений мы обнаружили, что элементы факторгруппы (то есть смежные классы по подгруппе движений) однозначно определяются положительными вещественными числами. Операция, производимая над смежными классами, приводит к такому же результату, как если бы мы занимались умножением положительных вещественных чисел.

Выясним, что между фактор-группой группы преобразований подобия по подгруппе движений и мультипликативной группой положительных вещественных чисел общего и в чем различие этих двух групп.

При задании любой группы необходимо указать, из каких элементов она состоит и какая групповая операция на них задана. Элементами одной из интересующих нас групп служат множества преобразований подобия, элементами другой — вещественные числа. Следовательно, обе группы состоят из совершенно различных элементов. Различны и групповые операции. В одной из групп в роли групповой операции «выступает» умножение подмножеств, в другой — умножение вещественных чисел.

И все же, несмотря на столь заметные различия, наши две группы обладают несомненным сходством: ведь если отвлечься от того, из каких элементов состоит каждая группа и какой групповой операцией она наделена, то обе группы становятся «неотличимыми». Это означает, что, если обе группы рассматривать как абстрактные группы, то получится одна и та же группа, поскольку при «абстрактном подходе» нас интересует не природа элементов и не природа групповой операции, а лишь как действует групповая операция на элементах группы.

Группы, в которых групповые операции действуют «одинаково», называются *изоморфными*.

Наше определение не полно: необходимо пояснить, что, собственно, означают слова «действуют одинаково». Ведь их можно понять, например, так: группа целых чисел и группа вещественных чисел изоморфны потому, что обе группы наделены *одной и той же* групповой операцией. Ясно, что, говоря об «одинаковом действии» групповых операций в изоморфных группах, мы имеем в виду совсем другое.

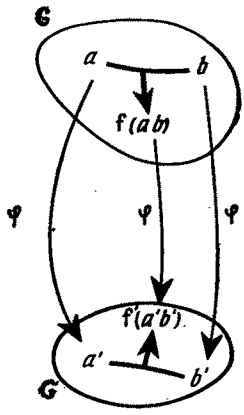


Рис. 39

В выбранном нами примере смежные классы определяются заданием одного-единственного вещественного числа, то есть функции, ставящей в соответствие каждому положительному вещественному числу λ некоторый смежный класс. Если эту функцию обозначить через φ, а смежный класс, сопоставляемый ею положительному вещественному числу λ, через $\varphi(\lambda)$, то относительно φ можно утверждать следующее:

1. Различным положительным вещественным числам соответствуют различные смежные классы. Иначе говоря, если $\varphi(\lambda) = \varphi(\mu)$, то $\lambda = \mu$.

2. Каждый смежный класс поставлен в соответствие некоторому положительному вещественному числу, то есть для каждого смежного класса $[T]$ найдется такое положительное вещественное число λ, при котором $\varphi(\lambda) = [T]$.

3. Операцию над смежными классами можно производить так, как если бы речь шла об умножении соответствующих вещественных чисел, то есть произведением смежных классов $\varphi(\lambda)$ и $\varphi(\mu)$ (взятых в надлежащем порядке) служит смежный класс, соответствующий произведению чисел $\lambda\mu$: $\varphi(\lambda)\varphi(\mu) = \varphi(\lambda\mu)$.

Первые два условия устанавливают соответствие между элементами двух групп, а третье условие означает, что групповые операции действуют одинаково. Поскольку изоморфизм групп определен при помощи функции, отображающей одну из групп на другую, то «вторую» группу удобно назвать образом (в данном случае изоморфным образом) «первой». Аналогичное определение изоморфизма можно дать и для общего случая.

Группа $\langle G'; f'\rangle$ называется изоморфным образом группы $\langle G; f\rangle$, если существует взаимно-однозначное отображение φ группы G на группу G′, сохраняющее групповую операцию, то есть:

1) если a, b — различные элементы группы G, то $\varphi(a)$, $\varphi(b)$ — различные элементы группы G′;

2) для каждого элемента a' группы G′ можно найти такой элемент a группы G, при котором $a' = \varphi(a)$;

3) если $a' = \varphi(a)$, $b' = \varphi(b)$ и $c = f(a, b)$, то $f'(a', b') = \varphi(c)$, или в более компактной записи $\varphi(f(a, b)) = f'(\varphi(a), \varphi(b))$ (рис. 39).

Это определение верно, то есть абсолютно точно, но группы $\langle G; f\rangle$ и $\langle G'; f'\rangle$ входят в него не симметрично: оно не позволяет говорить, что две группы изоморфны «друг другу», а лишь дает основание утверждать, что «одна группа изоморфна другой». Но если это так, то данное выше определение непригодно, поскольку «одинаково устроенные» группы — понятие симметричное. В действительности свойства 1 и 2 функции φ обеспечивают существование функции ψ, отображающей элемент $\varphi(a)$ группы G′ в элемент a группы G. Функция ψ отображает группу G′ на группу G и обладает свойствами 1 и 2. Нетрудно видеть, что функция ψ обладает и свойством 3.

Действительно, если элементы a', b', c' группы G′ связаны соотношением $c' = f'(a', b')$ и $a' = \varphi(a)$, $b' = \varphi(b)$, а $c' = \varphi(c)$, то

$$\psi(f'(a', b')) = \psi(c') = c$$

и

$$f(\psi(a'), \psi(b')) = f(a, b).$$

Требуется доказать, что $c = f(a, b)$. Поскольку функция φ обладает свойством 3, то

$$\varphi(f(a, b)) = f'(\varphi(a), \varphi(b)) =$$
$$= f'(a', b') = c' = \varphi(c),$$

откуда в силу свойства 1 следует, что элементы $f(a, b)$ и c группы G совпадают.

С точки зрения алгебры изоморфные группы неотличимы: отображение, порождающее изоморфизм, подобно зеркалу, переводит элементы и групповую операцию одной группы в элементы и групповую операцию другой группы. Все, что бы мы ни проделали при помощи групповой операции над элементами одной группы, повторяется «по другую сторону зеркала» — в другой группе, и это хорошо, поскольку позволяет рассматривать свойства операции «в чистом виде» независимо от конкретных особенностей элементов и групповых операций.

Если взять какую-нибудь группу и рассмотреть изоморфные ей группы, то нетрудно понять, что алгебраически они все одинаковы и отличаются только элементами и групповыми операциями. Это означает, что изоморфные группы, если их рассматривать как *абстрактные группы*, совпадают.

Множество групп, изоморфных данной, условимся понимать как абстрактную группу. Эта абстрактная группа называется представителем любой из изоморфных групп.

Определение абстрактной группы означает примерно следующее. Существует великое множество циклических групп, содержащих по два элемента. Каждая из них обладает элементами, отличными от элементов других групп, и групповой операцией, носящей иной характер, чем групповые операции других групп. Но все эти группы обладают и общими свойствами: каждая из них содержит по два элемента, которые преобразуются соответствующим образом под действием групповой операции, и один из этих двух элементов является образующим для группы. Именно это и имеют в виду, когда говорят, что абстрактная группа выражает общие свойства всех групп, изоморфных данной группе. Иногда ту же мысль облекают в несколько иную форму и утверждают, что абстрактная группа — это все множество изоморфных групп. (Мы оказались бы в аналогичной ситуации, если бы нам понадобилось определить, что такое «румяное яблоко». Мы бы сказали, что это свойство, присущее всем румяным яблокам. Но ту же мысль можно выразить и несколько иначе. Рассмотрим все румяные яблоки. Их множество и будет «тем самым» румяным яблоком, поскольку оно содержит все румяные яблоки и только их.)

Понятие абстрактной группы позволяет «перечислять» группы, узнавать, сколько существует (абстрактных) групп с заданным числом элементов. (Эту задачу можно сформулировать следующим образом: сколько существует не изоморфных групп с заданным числом элементов?) Рассмотрим несколько примеров.

ПРИМЕРЫ

1. Циклические группы заданного порядка. Если порядки циклических групп $\{a\}$ и $\{b\}$ совпадают, то отображение φ: $a^i \to b^i$, очевидно, взаимно-однозначно и сохраняет групповую операцию. Следовательно, каждая из этих групп изоморфна другой, а это означает, что существует лишь одна циклическая (абстрактная) группа данного порядка.

2. Группа заданного простого порядка. По теореме Лагранжа порядок любого элемента конечной группы является делителем порядка группы. Поскольку в рассматриваемом случае порядок группы — простое число, то порядок каждого элемента группы равен этому простому числу или 1. Группа, о которой идет речь, содержит по крайней мере один элемент, отличный от единичного (число элементов в группе не меньше двух, так как наимень-

шее простое число равно 2), поэтому существует элемент, порядок которого равен порядку группы. Но это означает, что группа циклическая. Используя результат, полученный в примере 1, приходим к выводу, что существует только одна группа данного простого порядка.

3. Группы не более чем седьмого порядка. Ясно, что существует лишь одна группа порядка 1. Кроме того, как показывает пример 2, существует по одной группе порядка 2, 3, 5 и 7.

Рассмотрим теперь группы четвертого порядка. По теореме Лагранжа порядок любого элемента такой группы является делителем числа 4. Если в группе существует элемент четвертого порядка, то этот элемент порождает группу, и, следовательно, группа циклическая. Как показано в примере 1, существует лишь одна циклическая группа четвертого порядка. Если же в группе нет элемента четвертого порядка, то квадрат любого элемента группы совпадает с единичным элементом. Нетрудно видеть, что такие группы коммутативны.

Действительно, если a и b — произвольные элементы такой группы, то, во-первых, $abab = (ab)^2 = e$, во-вторых, $e = a^2b^2 = aabb$. Используя эти соотношения, получаем: $abab = aabb$. Сокращая слева на a, а справа на b, находим: $ab = ba$, что и требовалось доказать.

Группа интересующего нас типа содержит три элемента, отличных от единичного, каждый из которых имеет порядок, равный 2. Следовательно, произведение любых двух элементов второго порядка может быть равно только третьему элементу второго порядка (для доказательства этого утверждения достаточно воспользоваться законом сокращения). Такая группа изоморфна подгруппе N, рассмотренной в задаче 1е из раздела 4.2, — так называемой четверной группе Клейна. Следовательно, существуют 2 группы четвертого порядка.

Перейдем теперь к группам шестого порядка. Прежде всего убедимся в том, что в группе шестого порядка заведомо существует элемент третьего порядка.

Действительно, если бы группа не содержала элемента третьего порядка, то в ней не могло бы быть элементов шестого порядка, поскольку квадрат элемента шестого порядка имеет порядок, равный 3. Следовательно, по теореме Лагранжа, поскольку группа не содержит элементов третьего порядка, то все элементы группы имеют порядок, равный 2. Такая группа (как показано выше) заведомо коммутативна, и два элемента, отличных от единичного, порождают подгруппу из четырех элементов. Отсюда (также по теореме Лагранжа) следует, что порядок группы делится на 4 и, следовательно, не может быть равен 6. Полученное противоречие означает, что группа шестого порядка непременно должна содержать элемент третьего порядка.

Пусть b — элемент третьего порядка. Существуют лишь 3 различные степени его: e (единичный элемент), b и b^2. Если элемент a не принадлежит циклической подгруппе, порожденной элементом b, то элементы ea, ba и b^2a образуют правый, а элементы ae, ab и ab^2 — левый смежный класс. Оба смежных класса должны совпадать, так как рассматриваемая группа содержит всего шесть элементов, а ни один из перечисленных нами элементов смежных классов не принадлежит подгруппе $\{b\}$. Это означает, что $\{b\}$ — нормальный делитель и элемент aba^{-1} принадлежит этой подгруппе. Поскольку aba^{-1} не может быть единичным элементом (в противном случае выполнялось бы равенство $b = a^{-1}aba^{-1} = a^{-1}ea = e$, что невозможно), то либо $aba^{-1} = b$, либо $aba^{-1} = b^2$. Нетрудно проверить, что в первом случае мы получаем циклическую группу шестого порядка, а во втором — группу, изоморфную группе всех подстановок трех элементов. Следовательно, всего существует две группы шестого порядка.

Аналогичным образом (но с использованием большего количества «вспомогательных средств») можно показать, что

существуют 5 групп восьмого порядка (3 из них — коммутативные), 2 группы девятого порядка (обе коммутативные), 2 группы десятого порядка (одна из которых коммутативная). Кроме того, нетрудно убедиться и в том, что, если p — нечетное простое число, то существуют 2 группы порядка $2p$ и 2 группы порядка p^2, причем одна из групп порядка $2p$ и обе группы порядка p^2 коммутативны.

$\cong$ означает изоморфиэм.

Символ $\cong$ для обозначения изоморфизма групп заимствован из геометрии, где его, как известно, используют для обозначения конгруэнтных фигур. Итак, если группы $\langle G;\ f\rangle$ и $\langle G';\ f'\rangle$ изоморфны, то это можно записать либо как $\langle G;\ f\rangle \cong \langle G';f'\rangle$, либо еще более кратко: $G \cong G'$. Если желательно указать, какая из групп служит прообразом и какая — образом при отображении φ, то используют обозначение φ: $\langle G;\ f\rangle \simeq \langle G';\ f'\rangle$ или более краткое обозначение φ: $G \simeq G'$.

ЗАДАЧИ

1. Доказать, что изоморфизм рефлексивен и транзитивен (то есть всякая группа изоморфна самой себе, и если одна группа изоморфна второй, а вторая — третьей, то первая группа изоморфна третьей).

2. Доказать, что прямое произведение коммутативно и ассоциативно, то есть, если A и B — две группы, то $A \times B \cong B \times A$ и $(A \times B) \times C \cong A \times (B \times C)$ для любых трех групп A, B и C.

3. Доказать, что, если A и B — нормальные делители группы G, порождающие вместе всю группу и не имеющие общих элементов, кроме единичного, то $G \cong A \times B$.

5.2. Гомоморфные отображения

Итак, с точки зрения алгебры изоморфные группы можно считать тождественными: не существует способа, позволяющего отличить одну изоморфную группу от другой. Вместе с тем нельзя не заметить, что в некоторых случаях такое отождествление становится «несколько преувеличенным».

Например, ясно, что отображение φ, изменяющее знак каждого целого числа на противоположный, устанавливает изоморфизм аддитивной группы целых чисел самой себе. Тем не менее элементы этой группы не совпадают со своими образами при отображении φ, поскольку, если бы они совпадали, то должно было бы, например, выполняться равенство $-1 = 1$, что, очевидно, невозможно. Вообще следует «соблюдать осторожность» во всех случаях, когда речь идет об изоморфизме различных подгрупп одной группы.

От опасений подобного рода можно избавиться, если всегда указывать отображение, осуществляющее изоморфизм. Таким образом, отображение и его свойства приобретают первостепенное значение, и их необходимо изучить более подробно.

Рассмотрим группы G и G', в каждой из которой групповую операцию условимся указывать, записывая рядом элементы-сомножители. Пусть φ: $G \to G'$ — некоторое отображение. Выясним, удовлетворяет ли оно всем условиям, «предъявляемым» к изоморфизму. Эти условия сводятся к следующим:

1) каждый элемент группы G имеет образ;

2) каждый элемент группы G' имеет прообраз;

3) групповая операция при отображении сохраняется.

Прежде всего займемся сохранением групповой операции. Это свойство отображения означает, что, если a и b — произвольные элементы группы G, то

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

Это единственное из всех условий, в котором фигурируют групповые операции. Не будь его, мы имели бы дело с отображением множеств, которое нас сейчас, естественно, не интересует.

Наоборот, мы получим весьма важный тип отображений, если потре-

буем, чтобы они удовлетворяли только условию сохранения групповых операций, и откажемся от прочих условий. Такие отображения называются *гомоморфизмами*, или *гомоморфными отображениями*.

Гомоморфизмом называется отображение одной группы в другую, сохраняющее групповую операцию.

Если гомоморфизм удовлетворяет какому-нибудь из условий (1) или (2), то мы получаем частную разновидность гомоморфизма, имеющую свое специальное название.

1. Каждый из элементов группы G имеет образ — мономорфизм.

2. Каждый из элементов группы G′ имеет прообраз — эпиморфизм.

Если выполнено каждое из условий (1) и (2), то, как известно, гомоморфное отображение называется изоморфизмом. Следовательно, изоморфизм можно определить как мономорфизм, являющийся одновременно и эпиморфизмом.

Следует заметить, что в давние времена, когда отображениям еще не уделяли достаточного внимания, гомоморфизмами называли те отображения, которые теперь принято называть эпиморфизмами. Такую терминологию можно встретить в старой литературе.

Существует четыре типа отображений, или, точнее, один тип отображений (гомоморфизм) и три его менее общие разновидности. Все они обладают общим свойством сохранять групповую операцию. Опознавать разновидности отображений нам помогают различия между ними. Следовательно, пытаясь найти различия между отображениями, мы можем не принимать во внимание их общее свойство и рассматривать их так, как если бы речь шла об отображениях множеств. (Разумеется, групповые свойства придают отображениям многие особенности, которыми не обладают произвольные отображения множеств. Но для того, кто хотел бы выяснить различия между отображениями групп, эти особенности не представляют интереса.)

Предположим, что все сведения

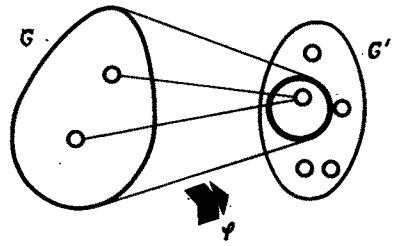


Рис. 40

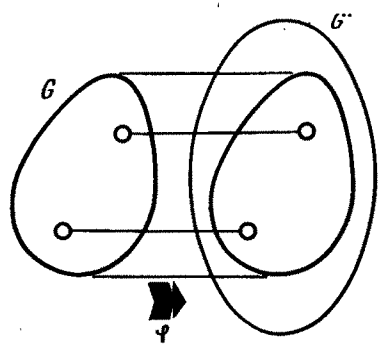


Рис. 41

об отображении φ укладываются в одну короткую фразу: $\varphi: G \to G'$ — некоторое отображение. Тогда мы можем лишь утверждать, что элементы группы G каким-то образом отображены в группу G′, и не более того. Этот случай изображен на рис. 40.

Если предполагается, что образы различных элементов различны (мономорфизм), то отображение не может переводить несколько элементов в один. Поэтому на рис. 41 отображение показано не сходящимися, а параллельными линиями.

Если требуется показать, что все элементы группы G′ служат образами каких-то элементов группы G, то на рисунке необходимо изобразить, что элементов в группе G′ «хватает» для всех элементов группы G. В этом случае опять придется воспользоваться сходящимися линиями (рис. 42).

Наконец, рисунок, изображающий изоморфизм, должен совмещать в

себе особенности обоих предыдущих рисунков (рис. 43).

«Самую узкую» разновидность гомоморфизма — изоморфизм — мы изучили достаточно подробно. Рассмотрим теперь, каким образом может осуществляться мономорфизм или эпиморфизм.

Пусть H — подгруппа группы G. Каждому элементу подгруппы H поставим в соответствие его же самого, но уже как элемент группы G. (Такое соответствие можно понимать следующим образом. Мы рассматриваем только элементы подгруппы H, «забывая» об остальных элементах группы G, но сами элементы подгруппы H считаем элементами группы G.) Мы получим отображение $H \to G$, обладающее тем свойством, что $\varphi(a) = a$ для любого элемента a подгруппы H. Это отображение — гомоморфизм, так как $\varphi(ab) = ab$, что совпадает с произведением элементов $\varphi(a) = a$ и $\varphi(b) = b$, равному ab. Кроме того, отображение φ — мономорфизм, поскольку, если $\varphi(a) = \varphi(b)$, то $a = \varphi(a) = \varphi(b) = b$, а это доказывает, что образы различных элементов при отображении φ различны.

Итак, мы показали, что любая подгруппа определяет мономорфизм в группу, а именно «естественное» отображение, при котором элементы подгруппы переходят сами в себя.

Аналогичное утверждение справедливо и относительно фактор-группы любой группы. Пусть N — нормальный делитель группы G. Как известно, элементами фактор-группы G/N являются смежные классы по N. Установим «естественное» соответствие, сопоставив каждому элементу группы G некоторый смежный класс по N. Поскольку каждый элемент группы G содержится в одном и только в одном смежном классе, то, очевидно, каждому элементу удобно сопоставить тот смежный класс, которому он принадлежит. Мы получим отображение φ: $G \to G/N$, обладающее тем свойством, что $\varphi(a) = aN$. Сохранение групповой опе-

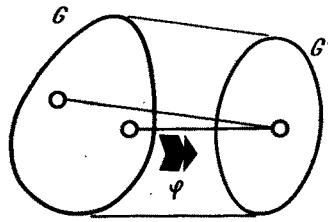


Рис. 42

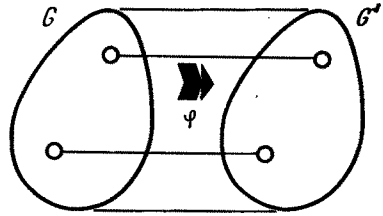


Рис. 43

рации следует из того, что N — нормальный делитель группы, именно поэтому выполняется соотношение $aNbN = abN$ (рис. 44). Таким образом, $\varphi(ab) = abN = (aN)(bN) = \varphi(a)\varphi(b)$. Отображение φ в действительности представляет собой эпиморфизм, поскольку каждый смежный класс содержит по крайней мере один элемент и поэтому в него под действием отображения переходит по крайней мере один элемент группы.

Итак, всякая фактор-группа опре-

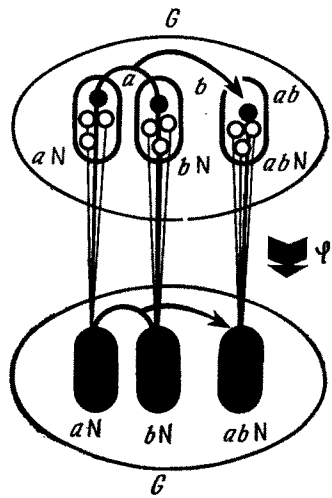


Рис. 44

деляет некоторый эпиморфизм исходной группы, а именно такое «естественное» отображение группы на фактор-группу, при котором каждый элемент группы переходит в содержащий его смежный класс.

Полученные нами результаты показывают, что мономорфизмов и эпиморфизмов существует «достаточно много». Возникает вопрос: а нельзя ли найти все мономорфизмы и эпиморфизмы? Разумеется, нет — в том смысле, что подгруппы или фактор-группы можно заменять изоморфными им группами и рассматривать соответствующие отображения как мономорфизм или эпиморфизм. Но полученные таким способом мономорфизмы и эпиморфизмы нельзя считать существенно отличающимися от рассмотренных выше, поскольку различиями между изоморфными группами мы пренебрегаем. Каждое из «отвергнутых» отображений в действительности уже известно: подставляя вместо подгрупп и фактор-групп изоморфные им группы, мы не сможем получить ни мономорфизм, ни эпиморфизм нового типа. Более того, оказывается, что все гомоморфизмы по существу «составлены» из рассмотренных нами мономорфизма и эпиморфизма.

Последнее утверждение требует доказательства. Пусть φ — произвольный гомоморфизм группы G в группу G′. Если бы G была подгруппой группы G′, как в рассмотренном выше «естественном» отображении, то гомоморфизм φ помог бы нам отобрать те элементы группы G′, в каждый из которых под действием φ переходит по крайней мере один элемент группы G. Воспользуемся тем же приемом и покажем, что те элементы группы G′, которые служат образом по крайней мере для одного элемента группы G, и в общем случае также образуют подгруппу группы G′.

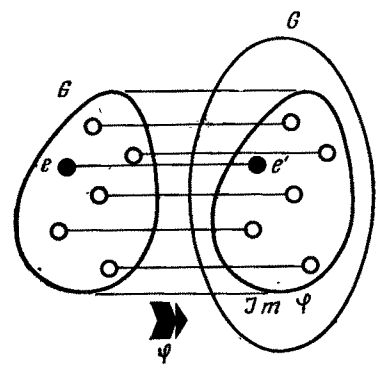


Рис. 45

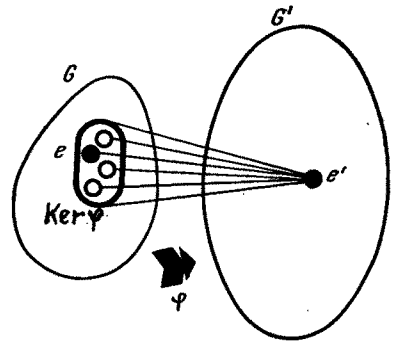


Рис. 46

Итак, рассмотрим все элементы группы G′, представимые в виде $\varphi(a)$, где a — произвольный элемент группы G (элементы $\varphi(a)$ группы G′ представляют собой не что иное, как «область значений» функции φ). Покажем, что эти элементы образуют подгруппу группы G′ (рис. 45). Эта подгруппа называется *образом гомоморфизма* φ и обозначается Im φ (от английского image — образ).

Групповое умножение не выводит за пределы Im φ, так как вследствие сохранения групповой операции $\varphi(a)\varphi(b) = \varphi(ab)$, то есть произведение образов любых двух элементов группы G имеет такой вид, какой должны иметь элементы подгруппы Im φ. Единичный элемент группы G′ также легко представить в требуемом виде. Действительно, единичный элемент группы G′ совпадает с образом единичного элемента группы G, так как в силу соотношения $\varphi(e)\varphi(a) = \varphi(ea) = \varphi(a)$ элемент $\varphi(e)$ может быть только единичным элементом группы G′. Нетрудно показать, что образ элемента, обратного любому элементу a группы G, совпадает с элементом группы G′, обратным образу элемента a: $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e)$, следовательно, $\varphi(a^{-1})$ совпадает с $(\varphi(a))^{-1}$.

Гомоморфизм сохраняет не только групповую операцию, но и единичный и обратные элементы.

Для отображения группы в фактор-группу необходим нормальный делитель. Следовательно, его надо найти прежде всего. При естественном отображении в фактор-группу элементы нормального делителя характеризуются следующим свойством: они образуют смежный класс, переходящий под действием φ в единичный элемент фактор-группы. Воспользуемся аналогичным приемом и в общем случае.

Рассмотрим элементы группы G, которые гомоморфизм φ отображает в единичный элемент e' группы G'. Покажем, что эти элементы образуют нормальный делитель группы G (рис. 46).

Эта подгруппа называется *ядром гомоморфизма* φ и обозначается $\operatorname{Ker}\varphi$ (от английского kernel — ядро).

Относительно элемента $\varphi(e)$ уже известно, что он совпадает с единичным элементом группы G', поэтому элемент e группы G принадлежит ядру гомоморфизма φ. Если a и b — элементы, входящие в $\operatorname{Ker}\varphi$, то, с одной стороны, $\varphi(ab) = \varphi(a)\varphi(b) = e'e' = e'$, а с другой стороны, $\varphi(a^{-1}) = (\varphi(a))^{-1} = (e')^{-1} = e'$, и, следовательно, $\operatorname{Ker}\varphi$ — подгруппа группы G. Наконец, если x — произвольный элемент группы G и a — произвольный элемент из $\operatorname{Ker}\varphi$, то $\varphi(xax^{-1}) = \varphi(x)\varphi(a)\varphi(x^{-1}) = \varphi(x)e'\varphi((x))^{-1}$. Это и доказывает, что $\operatorname{Ker}\varphi$ — нормальный делитель.

Связь между фактор-группой группы G по нормальному делителю $\operatorname{Ker}\varphi$ и подгруппой $\operatorname{Im}\varphi$ группы G' устанавливает *теорема о гомоморфизмах*:

если $\varphi: G \to G'$ — *произвольный гомоморфизм, то существует естественный изоморфизм* ψ: $(G/\operatorname{Ker}\varphi) \xrightarrow{\sim} \operatorname{Im}\varphi$, *при котором*

$$\psi : (a \cdot \operatorname{Ker}\varphi) \to a.$$

(Изоморфизм ψ принято называть естественным, поскольку он определяется одинаково при любом гомоморфизме φ и не использует никаких «индивидуальных» особенностей гомоморфизма.)

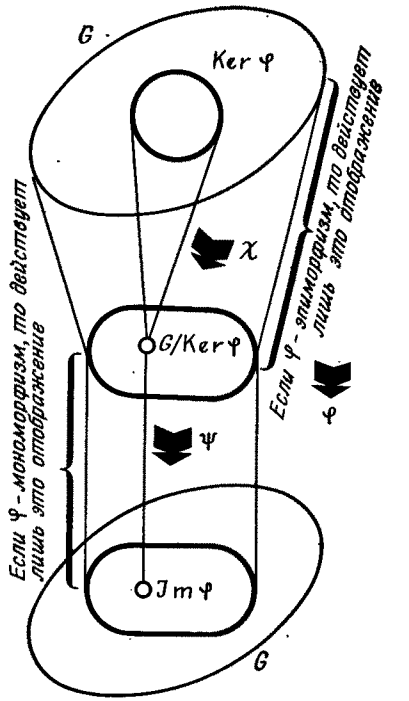


Рис. 47

Наиболее трудной частью доказательства, состоящей в отыскании используемого в теореме изоморфизма, мы уже располагаем. Следовательно, нам не остается ничего другого, как показать, что полученное нами отображение действительно является изоморфизмом.

Итак, требуется проверить, что отображение ψ — изоморфизм. Для этого нам необходимо убедиться в том, что устанавливаемое им соответствие не зависит от выбора элементов, представляющих смежные классы. Воспользуемся этим замечанием для завершения доказательства теоремы о гомоморфизмах.

Если смежные классы $a \cdot \operatorname{Ker}\varphi$ и $b \cdot \operatorname{Ker}\varphi$ совпадают, то это означает, что, например, элемент b принадлежит смежному классу $a \cdot \operatorname{Ker}\varphi$, то есть что $b = ax$ (где x — соответствующий элемент из $\operatorname{Ker}\varphi$). Иначе говоря, два смежных класса совпадают при условии, что элемент $x = a^{-1}b$ принадлежит $\operatorname{Ker}\varphi$. Выясним теперь, когда $\varphi(a)$ совпадает с $\varphi(b)$. Совпадение образов элементов a и b группы G означает, что

$(\varphi(a))^{-1}\varphi(b)$ — единичный элемент группы G'. Производя несложные преобразования, получаем $(\varphi(a))^{-1}\varphi(b)=\varphi(a^{-1})\varphi(b)=$ $=\varphi(a^{-1}b)$. По определению этот элемент совпадает с единичным элементом группы G', если $a^{-1}b$ принадлежит $\operatorname{Ker}\varphi$. Итак, мы показали, что смежные классы $a\cdot\operatorname{Ker}\varphi$ и $b\cdot\operatorname{Ker}\varphi$ совпадают в том и только в том случае, если совпадают элементы $\varphi(a)$ и $\varphi(b)$ группы G', поскольку оба «совпадения» происходят при одном условии: элемент $a^{-1}b$ должен принадлежать $\operatorname{Ker}\varphi$.

Итак, соответствие, устанавливаемое между элементами фактор-группы $G/\operatorname{Ker}\varphi$ и $\operatorname{Im}\varphi$ однозначно, то есть действительно является отображением. Но мы доказали лишь, что образы различных элементов фактор-группы различны, то есть что выполнено одно из трех условий изоморфизма (условие мономорфизма). Второе условие (условие эпиморфизма) также выполняется, поскольку все элементы множества $\operatorname{Im}\varphi$ представимы в виде $\varphi(a)$, то есть являются образами элементов фактор-группы.

Проверим, наконец, сохранение групповой операции. Смежному классу $(a\cdot\operatorname{Ker}\varphi)(b\cdot\operatorname{Ker}\varphi)=ab\cdot\operatorname{Ker}\varphi$ отображение ψ ставит в соответствие элемент $\varphi(ab)$. Но поскольку гомоморфизм φ сохраняет групповую операцию, то $\varphi(ab)$ совпадает с произведением элементов $\varphi(a)\varphi(b)$.

Если φ — эпиморфизм, то есть если G' совпадает с $\operatorname{Im}\varphi$, то группа G' изоморфна фактор-группе группы G. Если φ — мономорфизм, то $\operatorname{Ker}\varphi$ содержит лишь один элемент — единичный элемент группы G. Действительно, при гомоморфизме единичный элемент e группы G отображается в единичный элемент e' группы G', а так как φ — мономорфизм, то другие элементы группы G не могут переходить в e'. Следовательно, все смежные классы состоят из одного элемента, и отображение $a\to a\cdot\operatorname{Ker}\varphi$, очевидно, является изоморфизмом. Таким образом, в этом случае группа G изоморфна фактор-группе группы G'.

Отображение $a\to a\cdot\operatorname{Ker}\varphi$, представляющее собой не что иное, как естественный гомоморфизм на фактор-группу, вообще говоря, не является изоморфизмом. Если χ — естественный гомоморфизм, то гомоморфизм φ можно осуществить следующим образом: сначала выполнить гомоморфизм χ (сопоставляющий элементу a группы G смежный класс $a\cdot\operatorname{Ker}\varphi$), а затем — изоморфизм ψ (сопоставляющий смежному классу $a\cdot\operatorname{Ker}\varphi$ элемент $\varphi(a)$ группы G'). Отображение χ — эпиморфизм, а если бы $\operatorname{Im}\varphi$ совпадал с G', то отображение ψ можно было бы считать мономорфизмом. Итак, «разложение» произвольного гомоморфизма на эпиморфизм и мономорфизм получено. Оно изображено на рис. 47.

ЗАДАЧИ

1. Пусть a — произвольный элемент группы G. Доказать, что существует однозначно определенный гомоморфизм φ, отображающий в G аддитивную группу целых чисел и удовлетворяющий условию $a=\varphi(1)$. Что можно сказать об этом отображении, когда φ — мономорфизм и когда φ — эпиморфизм? Каким образом дополнительные сведения о φ можно было бы использовать для определения порядка элемента a?

2. Доказать, что в каждом из следующих случаев отображение является эпиморфизмом, найти его ядро и сравнить полученные результаты с решением задачи 1 из раздела 4.2.

а. Аддитивная группа комплексных чисел отображена на аддитивную группу вещественных чисел так, что каждому комплексному числу поставлена в соответствие его мнимая часть: $a+bi\to b$.

б. Мультипликативная группа отличных от нуля комплексных чисел отображена на группу комплексных чисел с модулем, равным 1, так, что каждому комплексному числу поставлено в соответствие комплексное число с тем же аргументом, но с модулем, равным 1:

$$r(\cos\varphi+i\sin\varphi)\to\cos\varphi+i\sin\varphi.$$

в. Мультипликативная группа отличных от нуля комплексных чисел отображена на мультипликативную группу положительных вещественных чисел так, что каждому комплексному числу поставлен в соответствие его модуль:

$$a+bi\to\sqrt{a^2+b^2}.$$

г. Группа преобразований подобия отображена на мультипликативную группу положительных вещественных чисел так, что каждому преобра-

зованию поставлено в соответствие число, показывающее, во сколько раз преобразование изменяет длину отрезка.

3. Пусть $G = A \times B$. Доказать, что $\varphi : a \to (a, e)$ — мономорфизм, а $\psi : (a, b) \to b$ — эпиморфизм ($\varphi : A \to G$; $\psi : G \to B$).

Проверить также, что $\operatorname{Im} \varphi = \operatorname{Ker} \psi$.

4. Пусть N и M — такие нормальные делители группы G, что M содержится в N, и пусть H — произвольная подгруппа группы G. Доказать, что соответствие $hM \to hN$, где h пробегает все элементы подгруппы H, — гомоморфизм, отображающий фактор-группу $\{H, M\}/M$ в фактор-группу $\{H, N\}/N$. Какой изоморфизм возникает при этом в силу теоремы о гомоморфизмах?

5. Рассмотрим предыдущую задачу в двух частных случаях, когда $M = \{e\}$ и когда $H = G$. (Эти случаи называются теоремами Нётер об изоморфизмах.)

Первая теорема об изоморфизмах:

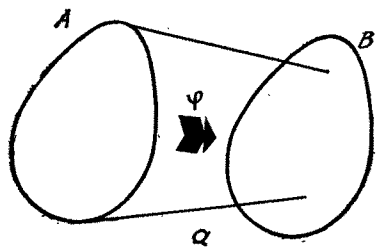
$$H/H \cap N \cong \{H, N\}/N.$$

Вторая теорема об изоморфизмах:

$$(G/M)/(N/M) \cong G/N.$$

5.3. Операции, осуществляемые гомоморфизмами

До сих пор мы рассматривали гомоморфизмы как особый класс функций, как некоторую разновидность отображений. Но в тех случаях, когда речь идет об отображениях множества в себя, удобно рассматривать операции, осуществляемые гомоморфизмами. Каждая такая операция представляет собой определенный набор функций. Ранее нам уже приходилось последовательно выполнять отображения, одно из которых не было отображением множества на себя (набор таких отображений составил гомоморфизм $\varphi : G \to G'$). Поскольку такие наборы отображений позволяют более наглядно записать «структуру» гомоморфизмов,



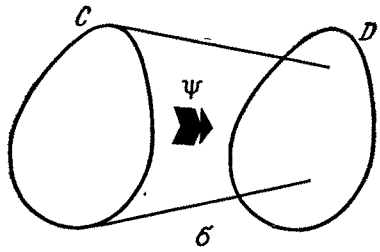


Рис. 48

то операции, осуществляемые гомоморфизмами, целесообразно рассмотреть в общем виде.

Начнем с двух отображений (рис. 48):

$$\varphi : A \to B \text{ и } \psi : C \to D.$$

Непосредственно ясно, что отображение ψ можно выполнять вслед за отображением φ лишь в том случае, если множества B и C совпадают.

Те, кому кажется, будто достаточно ограничиться более слабым условием и потребовать, чтобы образы элементов множества A содержались в множестве C, заблуждаются. Предположения о том, что элементы множества B принадлежат множеству C, недостаточно для того, чтобы отображение ψ можно было выполнять вслед за отображением φ. Действительно, полное описание последовательного выполнения двух отображений должно было бы включать и вспомогательное отображение, переводящее множество B в множество C. Следовательно, «в нерерыве» между двумя отображениями необходимо выполнить третье, вспомогательное, отображение множества B на множество C.

Но если $B = C$, то последовательное выполнение двух отображений

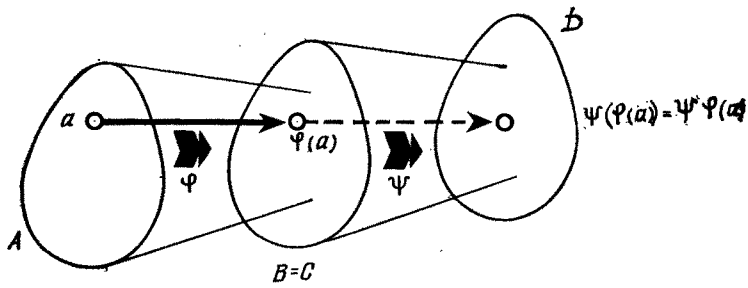


Рис. 49

становится вполне определимым и сводится к следующему:

$\psi\varphi : a \to \psi(\varphi(a))$ при любом $a \in A$.

Ясно, что, выполнив одно за другим отображения φ и ψ, мы получим некоторое новое отображение $\psi\varphi : A \to D$, которое называется произведением отображений φ и ψ (рис. 49).

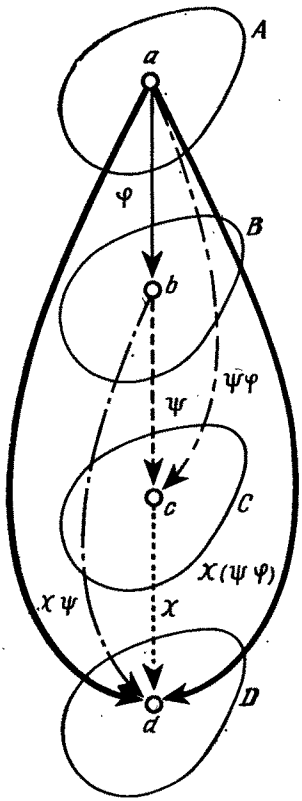


Рис. 50

Отображение $\psi\varphi : A \to D$ называется произведением отображений φ и ψ.

Нетрудно видеть, что умножение отображений ассоциативно. Это утверждение надлежит понимать в следующем смысле: если какое-нибудь из произведений $\chi(\psi\varphi)$ и $(\chi\psi)\varphi$ существует, то другое произведение отображений также выполнимо и совпадает с первым. Действительно, существование любого произведения означает, что можно задать отображения

$$\varphi : A \to B;\ \psi : B \to C;\ \chi : C \to D.$$

Но тогда, как уже неоднократно было показано, $\chi(\psi\varphi) = (\chi\psi)\varphi$ (рис. 50).

Для гомоморфизмов справедливы следующие утверждения:

Если произведение $\psi\varphi$ гомоморфизмов φ и ψ существует, то это — гомоморфизм. Если оба сомножителя φ и ψ — мономорфизмы, эпиморфизмы или изоморфизмы, то и произведение $\psi\varphi$ — соответственно мономорфизм, эпиморфизм или изоморфизм.

Прежде всего докажем утверждение относительно гомоморфизмов. По существу необходимо лишь доказать, что произведение гомоморфизмов $\psi\varphi$ сохранят групповую операцию. Гомоморфизм φ сохраняет групповую операцию, поэтому $\varphi(ab) = \varphi(a)\varphi(b)$. Но гомоморфизм ψ также сохраняет групповую операцию, откуда $\psi(\varphi(a)\varphi(b)) = \psi(\varphi(a))\ \psi(\varphi(b))$. Взятые вместе, эти соотношения и означают, что произведение $\psi\varphi$ гомоморфизмов сохраняет групповую операцию.

Если φ и ψ — мономорфизмы, то выберем элементы a и b, для которых $\psi(\varphi(a)) = \psi(\varphi(b))$. Так как ψ — мономорфизм, то

из равенства $\psi(\varphi(a)) = \psi(\varphi(b))$ следует, что $\varphi(a) = \varphi(b)$. В свою очередь равенство $\varphi(a) = \varphi(b)$ означает, что $a = b$, поскольку φ — мономорфизм. Итак, $\psi\varphi$ — мономорфизм.

Если φ и ψ — эпиморфизмы, то для любого элемента c найдется такой элемент b, что $c = \psi(b)$, а для элемента b найдется элемент a, переходящий в b под действием эпиморфизма φ: $b = \varphi(a)$, то есть выполняется соотношение $c = \psi(\varphi(a))$. Следовательно, $\psi\varphi$ — эпиморфизм.

Если оба сомножителя φ и ψ — изоморфизмы, то каждый из них является одновременно мономорфизмом и эпиморфизмом. Следовательно, произведение $\psi\varphi$ также сочетает в себе все свойства мономорфизма и эпиморфизма, а это и означает, что $\psi\varphi$ — изоморфизм.

Среди гомоморфизмов встречаются и гомоморфные отображения групп в себя. Такие гомоморфизмы называются эндоморфизмами.

В частном случае, когда эндоморфизм сводится к изоморфному отображению группы на себя, он называется автоморфизмом.

Наиболее частным случаем автоморфизма, в котором каждый элемент группы переходит в себя, является тождественное отображение. (Разумеется, существует не одно, а много тождественных отображений. У каждой группы оно «свое».)

Тождественное отображение выделяется среди прочих «сильным сходством» с единичным элементом. Тождественное отображение i группы G — это такой однозначно определенный гомоморфизм $i : G \to G$, для которого $i\varphi = \varphi$ при любом гомоморфизме $\varphi : A \to G$ и $\psi i = \psi$ при любом гомоморфизме $\psi : G \to B$.

ЗАДАЧИ

1. Доказать, что для всякого гомоморфизма φ существует такой эпиморфизм χ и такой мономорфизм ψ, для которых $\varphi = \psi\chi$.

2. Доказать, что на мономорфизм можно сокращать слева, а на эпиморфизм — справа, то есть, если φ — мономорфизм и $\varphi\alpha = \varphi\beta$, то $\alpha = \beta$, а если ψ — эпиморфизм и $\gamma\psi = \delta\psi$, то $\gamma = \delta$.

3. Доказать, что гомоморфизм φ является изоморфизмом в том и только в том случае, если существует обратный гомоморфизм, то есть такой гомоморфизм ψ, для которого $\varphi\psi$ и $\psi\varphi$ — тождественные отображения.

4. Доказать следующие утверждения:

а) если $\beta\alpha$ — мономорфизм, то α — мономорфизм;

б) если $\beta\alpha$ — эпиморфизм, то β — эпиморфизм.

5. Пусть $G = A \times B$. Доказать, что существуют гомоморфизмы $\alpha : A \to G$ и $\beta : G \to B$, для которых $\beta\alpha$ — тождественное отображение.

6. Предположим, что для групп A и B существуют гомоморфизмы $\alpha : A \to G$ и $\beta : B \to G$, для которых $\beta\alpha$ — тождественное отображение. Доказать, что, если $\operatorname{Im}\alpha$ — нормальный делитель группы G, то существует такая группа G, для которой $G \cong A \times B$.

6

Полугруппы и автоматы

6.1. Полугруппа, полугруппа с единицей, группа

При рассмотрении подгрупп мы упоминали о группе однозначных отображений данного множества на себя. Было показано, что такая группа всегда содержит подгруппу, состоящую из *всех* взаимно-однозначных отображений множества на себя. Как показало рассмотрение гомоморфизмов, не только взаимно-однозначные, но и все отображения играют в алгебре важную роль. Сопоставляя эти два факта, нетрудно понять, что изучение *всех* отображений множества на себя — задача, заслуживающая внимания.

Любые два отображения одного и того же множества на себя можно выполнять последовательно, поэтому они образуют полугруппу (в предыдущем разделе мы показали, что, если «умножение» отображений имеет смысл, то оно ассоциативно.)

Все отображения множества на себя образуют полугруппу, которая

называется полугруппой отображений данного множества.

Любая совокупность отображений множества на себя, если она полугруппа, непременно является либо подполугруппой, либо подгруппой полугруппы всех отображений множества на себя. Но этим сведения о полугруппе отображений далеко не исчерпываются. В рассмотренных нами примерах единичным элементом групп всегда было тождественное отображение и оно же было единицей полугруппы отображений. Единичный элемент содержат очень многие важные подполугруппы полугруппы всех отображений множества на себя. Это означает, что о подполугруппах с единицей полугруппы с единицей приходится говорить довольно много.

При рассмотрении подгрупп мы подчеркивали, что так называются подмножества, каждое из которых является группой относительно операции, определенной на исходной группе. Нетрудно видеть, что в подгруппе единичный элемент и элемент, обратный данному, совпадает с единичным элементом и элементом, обратным данному, всей группы. В случае полугрупп все обстоит иначе.

Рассмотрим числа 0 и 1. Они образуют полугруппу по умножению, поскольку любое произведение, составленное из нулей или единиц, равно либо 0, либо 1. Эта полугруппа с единицей: единичным элементом служит число 1. Число 0 образует подполугруппу всей полугруппы, так как произведение нулей всегда равно 0. Но в «нулевой» подполугруппе содержится и «своя» единица — число 0. Ясно, что единичный элемент «нулевой» подполугруппы отличен от единичного элемента исходной полугруппы.

Следовательно, если мы хотим, чтобы и в случае полугрупп единица подполугруппы совпадала с единицей всей полугруппы (в приведенных выше важных примерах дело обстояло именно так), то отнюдь не достаточно предположить, что полугруппа с единицей должна содержать подполугруппы с единицей. Не существует ли какого-нибудь «регулярного» способа, позволяющего определять, принадлежит ли данной подполугруппе единичный элемент всей полугруппы?

В случае подгрупп «общность» единичного элемента подгруппы и всей группы следует из того, что операция, определенная на исходной группе, продолжает оставаться групповой операцией и при переходе к подгруппе. Следовательно, если бы нам удалось каким-то образом получить единичный элемент всей полугруппы, произведя над элементами подполугруппы некую операцию, относительно которой подполугруппа «замкнута», то единичный элемент заведомо принадлежал бы интересующей нас подполугруппе. Таким образом, ответ содержится в самом поставленном вопросе: необходимо задать операцию, которая всегда порождает единичный элемент полугруппы.

Полугруппу можно рассматривать как пару $\langle S;\ f\rangle$, где S — (непустое) множество, а f — операция, удовлетворяющая условию $f(a,\ f(b,\ c)) = f(f(a,\ b),\ c)$. Полугруппа с единицей — это тройка $\langle S;\ f,\ e\rangle$, где $\langle S;\ f\rangle$ — полугруппа, а операция e удовлетворяет условию $f(e,\ a) = f(a,\ e) = a$.

Такая запись позволяет дать новое определение группы. Действительно, группу можно рассматривать как полугруппу с единицей, в которой для каждого элемента существует обратный элемент. Следовательно, группа — это четверка $\langle S;\ f,\ e,\ i\rangle$, где $\langle S;\ f,\ e\rangle$ — полугруппа с единицей, а операция i удовлетворяет условию $f(i(a),\ a) = f(a,\ i(a)) = e$.

Разумеется, такое определение группы приводит к новым определениям подгрупп и гомоморфизмов.

При рассмотрении подгрупп мы убедились в том, что единичный элемент группы принадлежит всем подгруппам и каждая подгруппа вместе с любым своим элементом содержит и обратный ему элемент. Изучая гомо-

морфизмы, мы установили, что всякий гомоморфизм переводит единичный элемент исходной группы в единичный элемент той группы, в которую отображается исходная, и образ элемента, обратного данному, совпадает с элементом «новой» группы, обратным образу данного элемента исходной группы. Следовательно, независимо от того, каких определений мы будем придерживаться, подгруппы и гомоморфизмы будут одними и теми же.

Но для чего в таком случае понадобилось определять группы столь сложным образом? Ясно, что выбрать можно любое из определений. Вопрос состоит лишь в том, почему мы ввели второй, «сложный», вариант определения. «В защиту» его приведем два соображения. Во-первых, сложный способ определения групп позволяет отделить условия, утверждающие *существование* того или иного объекта (единичного элемента или элемента, обратного данному), от условий, требующих *выполнения* какого-нибудь тождества (что оказывается весьма полезным во многих случаях). Во-вторых, если существование какого-нибудь элемента обеспечено «рецептом» его получения, то существование такого элемента становится более «зримым» и «осязаемым»: ведь мы можем не только утверждать, что тот или иной элемент существует, но и указывать, как его «сотворить».

Операции в определении группы перечислены в следующем порядке: f, e и i. С операцией f все обстоит как нельзя лучше. Это функция «двух переменных»: любым двум элементам a и b она ставит в соответствие некоторый элемент $f(a, b)$ (называемый произведением элементов a и b). Не возникает никаких осложнений и с операцией i: ее можно рассматривать как функцию «одного переменного», которая каждому элементу a ставит в соответствие элемент $i(a)$ (представляющий собой не что иное, как элемент, обратный элементу a). А как следует понимать операцию e? О ней известно лишь, что она... ставит в соответствие единичный элемент. Но чему сопоставлен единичный элемент, заранее неизвестно, поскольку определение группы об этом «умалчивает». Тем не менее такой тип соответствия отнюдь не нов. Мы встречались с ним и ранее при рассмотрении функций, принимающих одно и то же значение — постоянных, или констант. Если функция двух переменных не зависит от одной из них, то мы говорим, что она зависит лишь от другой переменной, то есть является функцией не двух , а одного переменного. По аналогии с этим функцию одного переменного, не зависящую от своего аргумента, можно назвать функцией «нуля переменных». Следовательно, функция нуля переменных — это не что иное, как константы.

Итак, полугруппы определены одной двухместной операцией, полугруппы с единицей — одной двухместной и одной нульместной операциями и, наконец, группы — одной двухместной, одной одноместной и одной нульместной операциями. Кроме того, во всех трех случаях должны выполняться определенные тождества.

В качестве упражнения докажем, что эндоморфизмы группы G образуют подполугруппу полугруппы отображений множества G (в данном случае полугруппу отображений множества G и полугруппу эндоморфизмов группы G мы рассматриваем как полугруппы с единицей).

Чтобы получить подполугруппу, необходимо лишь убедиться в том, что произведение двух сохраняющих групповую операцию отображений также сохраняет групповую операцию. Ясно, что эндоморфизмы обладают этим свойством. Единица полугруппы всех отображений множества G на себя принадлежит полугруппе эндоморфизмов, так как тождественное отображение сохраняет групповую операцию.

Аналогичным образом можно доказать, что эндоморфизмы группы $G = A \times B$, отображающие все элементы группы G на элементы вида (a, e), образуют подполугруппу полугруппы всех эндоморфизмов (входящей в качестве подполугруппы в полугруппу всех отображений множества G на себя). (Это утверждение

перестает быть верным, если интересующие нас полугруппы и полугруппу эндоморфизмов группы G рассматривать как полугруппы с единицей.)

Ясно, что произведение двух эндоморфизмов, отображающих элементы группы G на элементы вида (a,e), обладает тем же свойством. Полугруппа этих специальных эндоморфизмов содержит единицу: единичным элементом служит отображение, переводящее элемент (a, b) группы G в элемент (a, e). Но поскольку, как нетрудно видеть, элемент (a, e) не совпадает с единицей полугруппы всех эндоморфизмов, то полугруппа частных эндоморфизмов, рассматриваемая как полугруппа с единицей, не является подполугруппой полугруппы всех эндоморфизмов.

6.2. Свободные полугруппы с единицей

В приведенных выше примерах все полугруппы имели весьма специальный вид: их элементы были связаны многочисленными соотношениями, рассмотрение которых не входило в нашу задачу. Таково, например, множество целых чисел, на котором задана операция сложения: помимо ассоциативности сложение целых чисел обладает и коммутативностью. Чтобы не затемнять существо дела, мы рассмотрим операцию умножения на полугруппах, элементы которых связаны только соотношениями, используемыми при выводе свойств самого умножения (например, соотношениями, вытекающими из ассоциативности умножения).

Поскольку в наиболее важных случаях нам встречаются полугруппы с единицей, то в дальнейшем мы ограничимся рассмотрением полугруппы с единицей.

Если x — произвольный элемент рассматриваемой полугруппы, то эта же полугруппа заведомо содержит элемент e (единичный элемент) и элементы $x, x^2, x^3, \ldots, x^n, \ldots$. Некоторые из них могут совпадать, но если это особо не оговорено, то все элементы должны быть различными. Известен пример (полугруппа неотрицательных целых чисел по сложению), в котором все эти элементы действительно различны.

Если рассматриваемая полугруппа содержит еще один элемент y (отличный от $e, x, x^2, \ldots, x^n, \ldots$), то она содержит и много других элементов, например таких:

$$y, yx, yx^2, \ldots, xy, x^2y, \ldots \quad y^2x, y^2x^2, \ldots,$$

или еще более «сложных»:

$$x^2yx^4y^3x, \quad xyxyxyxy^5, \quad y^7x^4y^7x^4y^7x^4 \text{ и т.д.}$$

Можно ли в некоторых случаях без особого труда установить, что два элемента совпадают? Например, элемент x^2yx совпадает с элементом x^2yx, так как оба элемента «выглядят» одинаково. Но все элементы полугруппы записаны по-разному, и, следовательно, по их «внешнему виду» мы не можем решить, совпадают они или различны.

Можно представить себе (хотя это и не верно), что между элементами всегда имеется какое-то весьма сложное соотношение, носящее характер закона. Такую «неожиданную связь» мы продемонстрируем на примере. (Поскольку в полугруппах соотношения между элементами не возникают «самопроизвольно», мы приведем пример из области групп.)

Пусть a, b, c, d, x, y, u, v — элементы некоторой группы. Предположим, что они удовлетворяют следующим равенствам: $ax = by$, $au = bv$ и $cx = dy$.

Формально равенство $cu = dv$ не следует из этих трех равенств (и в случае полугрупп оно выполняется далеко не всегда), но если воспользоваться обратными элементами, то вывод равенства $cu = dv$ не составит особого труда. Действительно, из системы трех исходных равенств мы получим:

$$b^{-1}a = yx^{-1}, \quad b^{-1}a = vu^{-1}$$

и

$$d^{-1}c = yx^{-1},$$

то есть

$$d^{-1}c = yx^{-1} = b^{-1}a = vu^{-1},$$

а из соотношения $d^{-1}c = vu^{-1}$ следует, что $cu = dv$.

Возвращаясь к полугруппе, мы хотели бы доказать, что «различные по форме» элементы всегда различны. Разумеется, если операция уже задана, то наша задача невыполнима. Поэтому мы поступим наоборот: сначала выпишем различные по «внешнему виду» элементы, затем докажем, что они различны, и лишь после всего этого зададим операцию. Если нам «повезет», мы получим полугруппу. Если же нас постигнет неудача, то никакой полугруппы получить не удастся. (Сейчас наш опыт будет успешным, но в других случаях — когда речь идет не о полугруппе — аналогичный метод не всегда приводит к желаемому результату.)

Итак, выберем произвольные элементы и назовем их *буквами*, поскольку буквами они и обозначены. (В действительности эти элементы представляют собой не что иное, как буквы некоторого *алфавита*.) Если отказаться от особого обозначения для операции возведения в степень, то речь пойдет о том, имеет ли смысл тот или иной набор букв, записанных одна за другой в определенном порядке. Такие наборы называются *словами*. Среди слов, разумеется, будут встречаться и «однобуквенные», состоящие из одной-единственной буквы. Более того, в число слов входит и так называемое «*пустое слово*», не содержащее ни одной буквы. Два слова называются равными, если они состоят из одних и тех же букв, порядок которых совпадает. (Говоря о совпадении порядка букв в словах, мы имеем в виду следующее. Слова xxy и xyx различны: хотя они и состоят из одних и тех же букв и хотя в каждом из них после буквы x идет буква y, в первом слове на втором месте стоит буква x, а во втором слове — буква y.)

Слова, составленные из букв заданного алфавита, будут элементами полугруппы. Необходимо еще задать операцию. Определим произведение двух слов как новое слово, которое получится, если к первому слову приписать второе. (Если одно из слов пусто, то от приписывания его к другому слову или другого слова к нему другое слово не изменяется.) Например,

(полу)·(группа)=(полугруппа).

Осталось доказать лишь, что введенная нами операция умножения слов ассоциативна. Ясно, что безразлично, в каком порядке выписывать слова-сомножители: сначала первые два и к их произведению приписать третье или же сначала первое слово и к нему приписать произведение второго и третьего слов. Точное доказательство ассоциативности более громоздко, но по существу следует той же схеме (с использованием полной индукции).

Ясно, что пустое слово играет в полугруппе роль единичного элемента.

Заметим, наконец, что построенная полугруппа не содержит ни одной подполугруппы, отличной от нее самой, в которую входили бы все буквы алфавита, поскольку в противном случае, образуя соответствующее произведение букв, можно было бы получить любое слово.

Именно поэтому буквы исходного алфавита порождают полугруппу и называются системой образующих полугруппы. Поскольку между буквами нет никаких соотношений, то алфавит называется *системой свободных образующих*, а построенная из букв полугруппа — *свободной полугруппой с единицей*.

Напомним об одном характерном свойстве свободных полугрупп: для любой свободной полугруппы всегда можно найти однозначно определенный гомоморфизм полугруппы, переводящий ее в заданную полугруппу, причем так, что образующие элементы под действием гомоморфизма переходят в зараиее указанные элементы заданной полугруппы.

ЗАДАЧИ

1. Полугруппы отображений каких множеств содержат подполугруппу, изоморфную свободной по-

лугруппе, порожденной одним элементом?

2. Доказать, что любую группу, порождаемую системой образующих, состоящей из k элементов, можно получить как гомоморфный образ свободной полугруппы, порожденной $2k$ элементами.

6.3. Алгебраическая теория автоматов

Полугруппы, главным образом свободные полугруппы, весьма тесно связаны с одним из современных разделов алгебры — с алгебраической теорией автоматов.

Разумеется, мы лишены возможности сколько-нибудь подробно изложить столь сложный круг вопросов и ограничимся лишь тем, что покажем, каким образом автоматы связаны с алгеброй и, в частности, с полугруппами.

Автоматом обычно называют устройство, самостоятельно выполняющее свои функции. Разумеется, сам автомат «не сознает», какие действия он должен производить; свои функции автомат выполняет, подчиняясь командам извне. Например, торговый автомат выдает необходимый товар лишь в том случае, если в него опустить монету соответствующего достоинства или специальный жетон. Однако и этого еще не достаточно: усилия покупателя окажутся напрасными, если внутри автомата исчяк запас товара. Таким образом, функционирование автомата определяется двумя факторами. Одним из факторов служит команда, подаваемая автомату извне; этот фактор называется *сигналом на входе*. Другим фактором является мгновенное «качество» автомата, которое называется его *внутренним состоянием* или, кратко, *состоянием*. При заданном внутреннем состоянии автомат однозначно реагирует на заданный сигнал на входе. Как именно реагирует автомат? Его реакции могут быть различными. Каждую отдельную реакцию принято называть *сигналом на выходе*. Например, сигналом на выходе торгового автомата может быть либо товар, выданный покупателю, либо сигнал о том, что автомат пуст. Но если присмотреться внимательнее, то можно заметить, что происходит и нечто другое. Например, если внутри автомата находилась одна-единственная шоколадка, то после того, как автомат выдаст ее покупателю, в нем не останется ни одной шоколадки. Следовательно, в дальнейшем автомат не сможет выдавать шоколадки: одновременно с сигналом на выходе изменяется и состояние автомата.

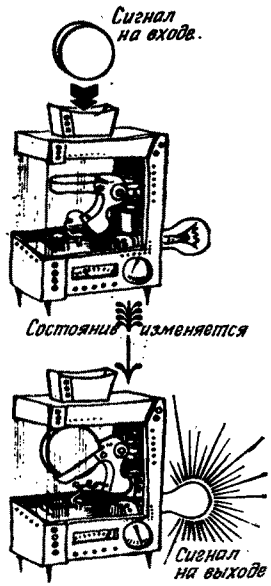


Рис. 51

Функционирование такого торгового автомата схематически показано на рис. 51.

Собирательное понятие «автомат» включает в себя необычайно много самых различных устройств. К числу автоматов, разумеется, относятся и все электронные вычислительные машины. Но и обычная пишущая машинка — тоже автомат (рис. 52).

Автоматом (в силу данного выше определения) можно считать и любое живое существо, а значит, и человека, хотя описать сколько-нибудь

Рис. 52

просто сигналы на входе, внутренние состояния и сигналы на выходе живых автоматов невозможно.

Если учесть, что «спектр» автоматов чрезвычайно широк, то не приходится удивляться, что об автоматах «вообще» можно сказать сравнительно мало. Именно поэтому удобно рассматривать определенные классы автоматов. Одна из задач, которые мы ставим, приступая к изучению автомата того или иного класса, состоит в выяснении простейшей структуры автомата, способного выполнять определенные функции.

Чтобы задать автомат, прежде всего необходимо указать три множества:

множество сигналов на входе X,
множество состояний A,
множество сигналов на выходе Y.

Но это еще не все: необходимо также задать две функции (при желании их можно рассматривать как операции). Одна из функций каждому сигналу на входе и каждому внутреннему состоянию ставит в соответствие некоторое внутреннее состояние, а другая — каждому сигналу на входе и каждому внутреннему состоянию ставит в соответствие определенный сигнал на выходе:

$$f(x, a) \in A, \quad g(x, a) \in Y,$$

где $x \in X$, $a \in A$.

Функционирование автомата схематически показано на рис. 53.

Итак, автомат можно определить как пятерку $\langle X, A, Y, f, g \rangle$, где первые три места заняты множествами, а остальные два — функциями.

Но функционирование автомата отнюдь не исчерпывается реагированием на отдельные сигналы, на вход автомата может поступать и серия сигналов, идущих один за другим. Пусть, например, автомат находится во внутреннем состоянии a, и на его вход поступает сначала сигнал x_1, а затем сигнал x_2. После поступления сигнала x_1 автомат переходит в новое внутреннее состояние $f(x_1, a)$, а на выходе «выдает» сигнал $g(x_1, a)$. Следующий сигнал на входе x_2 «застает» автомат во внутреннем состоянии $f(x_1, a)$ и переводит его в состояние $f(x_2, f(x_1, a))$. Сигнал на выходе также изменяется и переходит в $g(x_2, f(x_1, a))$.

Как показывают аналогичные рассуждения, если автомат первоначально находится во внутреннем состоянии a и на вход поступают сигналы x_1, x_2, x_3, то автомат перейдет из состояния a в конечное состояние $f(x_3, f(x_2, f(x_1, a)))$, а на выходе последовательно появятся сигналы $g(x_1, a)$, $g(x_2, f(x_1, a))$, $g(x_3, f(x_2, f(x_1, a)))$.

Обозначив сигналы на выходе через y_1, y_2, y_3, мы установим следующее соответствие между сигналами на входе и на выходе автомата:

сигналы на входе	сигналы на выходе
x_1	y_1
x_1x_2	y_1y_2
$x_1x_2x_3$	$y_1y_2y_3$

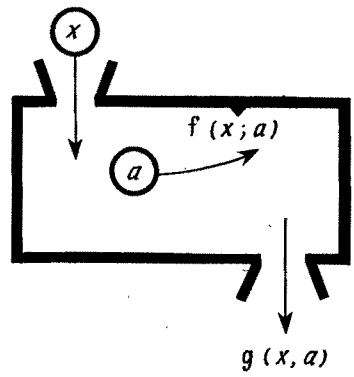


Рис. 53

Разумеется, это соответствие отнюдь не означает, что, если автомат находится в состоянии a и на вход поступает сигнал x_2, то на выходе появляется сигнал y_2, а если на вход подается сигнал x_3, то на выходе возникает сигнал y_3, поскольку сигнал на выходе зависит не только от сигнала на входе, но и от внутреннего состояния автомата, а состояния $a_1 = f(x_1, a)$ и $a_2 = f(x_2, a_1)$, вообще говоря, отличаются от исходного.

Итак, функционирование автомата можно изучать, описывая не только его реакцию на отдельные сигналы, подаваемые на вход, но и на серии сигналов. Это и позволяет подходить к сигналам на входе как к образующим свободной полугруппы. Сигналы на выходе также можно рассматривать как образующие свободной полугруппы.

Таким образом, свободные полугруппы позволяют сравнительно просто описывать работу автоматов.

7.

Представления групп

Идея рассматривать группы «вообще», абстрактно, возникла при изучении конкретных групп. Именно переход к абстрактным группам позволил подробно исследовать групповые операции. Лишь таким способом удалось избавиться от конкретных свойств, не существенных для решения общих проблем и даже затрудняющих их понимание.

Но сколь ни широки возможности, открываемые переходом от конкретных групп к абстрактным, все же и они ограничены. Не следует думать, будто в «устройстве» конкретных групп мы сможем разбираться лишь до тех пор, пока соответствующие абстрактные группы будут не слишком велики. Кроме того, определенные типы конкретных групп всегда обладают особыми, только им присущими свойствами, упрощающими и облегчающими описание групп. Было бы хорошо использовать такие группы для описания других групп. Например, очень удобно описывать группу подстановок — результаты при этом получаются весьма наглядными.

Но существует поистине неисчерпаемое множество групп, элементы которых не являются подстановками. Неужели при описании столь обширного класса групп непременно требуется отказаться от упрощений, которых удается достичь при описании группы подстановок? К счастью, столь ощутимой потери удается избежать: понятие изоморфизма позволяет преодолеть трудности, возникающие при описании групп. Напомним, что с точки зрения алгебры изоморфные группы не считаются различными. Следовательно, при описании любой группы мы могли бы воспользоваться всеми преимуществами группы подстановок, если бы нам удалось лишь доказать, что интересующая нас группа изоморфна некоторой подгруппе группы подстановок. О группе, изоморфной подгруппе группы подстановок, говорят, что она *представлена подстановками*.

Пусть S_H — группа всех подстановок множества H (групповая операция входит в обозначение S_H).

Говорят, что группа $\langle G; f\rangle$ представлена подстановками множества H, если существует мономорфизм $\varphi\colon \langle G; f\rangle \to S_H$.

Теорема Кэли. *Всякую группу можно представить подстановками.*

Для доказательства теоремы Кэли прежде всего необходимо подобрать множество H, а затем для каждого элемента заданной группы найти соответствующую ему подстановку элементов множества H.

Если задана только группа $\langle G; f\rangle$, то известно лишь одно множество: множество G. Задача: для каждого элемента g множества G найти соответствующую ему подстановку элементов того же множества. (Соответствие между элементами и подстановками зависит от групповой операции.)

Проще всего такую подстановку можно получить, записав под произвольным элементом x группы G элемент xg.

Прежде всего необходимо убедиться в том, что предложенный нами алгоритм действительно порождает подстановку. То, что при заданном g и соответствующим образом выбранном x можно получить любой элемент a группы G, следует из разрешимости уравнений $xg = a$ для группы. То, что при отображении $x \to xg$ различные элементы переходят в различные, следует из закона сокращения.

Если P_g — подстановка, поставленная указанным выше способом в соответствие элементу g, то она имеет следующий вид:

$$P_g = \begin{pmatrix} \dots x \dots \\ \dots xg \dots \end{pmatrix}.$$

Пусть φ: $g \to P_g$ — отображение, переводящее элементы группы $\langle G; / \rangle$ в группу S_G. Для доказательства теоремы Кэли требуется установить, что φ переводит различные элементы g в различные подстановки и, кроме того, сохраняет групповую операцию.

Пусть g и h — различные элементы группы G. Подстановка P_g переводит единичный элемент e в элемент $eg = g$, а подстановка P_h — в элемент $eh = h$. Так как элементы g и h различны, то и подстановки P_g и P_h различны.

Осталось доказать, что отображение φ сохраняет групповую операцию. Для этого необходимо проверить, что подстановка P_{gh}, соответствующая произведению gh, совпадает с произведением подстановок $P_g P_h$.

Подстановка P_{gh} переводит произвольный элемент x группы G в элемент $x(gh)$. Произведение подстановок $P_g P_h$ означает, что сначала производится подстановка P_g, а затем подстановка P_h. Первая подстановка переводит x в xg, а вторая переводит xg в $(xg)h$. Поскольку групповая операция ассоциативна, то $x(gh)$ совпадает с $(xg)h$, что и требовалось доказать.

Заметим, что представления играют весьма важную роль во всей математике. Позднее нам еще предстанется случай встретиться с ними.

ЗАДАЧИ

1. Что можно сказать о разложении подстановок, представляющих элементы конечной группы, в произведение циклов? Что изменится, если от конечных групп перейти к бесконечным?

2. Что произойдет, если элементу g группы G поставить в соответствие подстановку Q_g, переводящую элемент x в элемент gx?

3. Как следует видоизменить теорему Кэли для полугрупп? Какая проблема при этом возникает и для каких полугрупп она отпадает?

Глава вторая

Кольца, тела и векторные пространства

1.

Кольца и тела

1.1. Целые числа и многочлены

В конце предыдущей главы мы узнали, что группы можно получать, задавая на множествах несколько операций. Но множества с несколькими операциями возникали в математике и раньше, причем более «естественно», чем в случае групп, и первым из таких множеств было множество целых чисел.

На множестве целых чисел существует две наиболее часто используемые, наиболее важные и наиболее «естественные» операции: сложение и умножение. Каждую из этих операций в отдельности мы уже рассматривали и знаем, что целые числа образуют (коммутативную) группу по сложению и (также коммутативную) полугруппу по умножению. Но известно также, что на множестве целых чисел операция сложения связана с операцией умножения законом дистрибутивности, то есть для любых трех целых чисел a, b и c выполняется соотношение $(a + b)c = ac + bc$.

Тому, кто захочет более точно определить свойства операций сложения и умножения, необходимо найти «какой-нибудь» объект, на котором заданы две операции, удовлетворяющие (быть может, неявно) определенным тождествам. Коммутативность умножения не всегда следует из этих тождеств, поскольку существуют важные примеры, в которых умножение обладает всеми свойствами, кроме коммутативности.

Объекты с двумя заданными на них операциями, удовлетворяющими этим условиям, называются *кольцами*. Если операция умножения коммутативна, то говорят, что *кольцо коммутативно*. Рассмотрим сначала несколько примеров.

ПРИМЕРЫ

1. К о л ь ц о ч е т н ы х ч и с е л. На множестве четных чисел обычно принято рассматривать сложение и умножение. Из предыдущей главы известно, что четные числа образуют группу по сложению. По умножению они образуют полугруппу, так как произведение двух четных чисел — число четное, а умножение ассоциативно. Поскольку сложение и умножение четных чисел связаны законом дистрибутивности (так как этот закон выполняется для любых трех четных чисел), то мы действительно

получаем кольцо, причем, как очевидно, коммутативное кольцо.

2. Кольцо рациональных чисел. О рациональных числах известно, что они образуют группу по сложению и полугруппу по умножению. Поскольку на множестве рациональных чисел сложение и умножение связаны законом дистрибутивности, то мы получаем (коммутативное) кольцо.

3. Кольцо вещественных чисел.

4. Кольцо комплексных чисел. В обоих случаях рассуждения, доказывающие, что мы действительно получаем кольцо, проводятся так же, как и в случае рациональных чисел.

5. Кольцо многочленов с целочисленными коэффициентами.

Выражения вида $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$, где $a_0, a_1, a_2, \ldots, a_n$ — целые числа, называются многочленами с целочисленными коэффициентами.

Задание операций на множестве многочленов существенно упрощается, если члены многочлена записать в обратном порядке: $f(x) = a_0 + a_1 x + a_n x^n$ и, кроме того, не обращать внимания на степень многочлена.

Говорят, что многочлен $f(x)$ совпадает с многочленом

$$g(x) = b_0 + b_1 x + \cdots + b_k x^k,$$

если равенства $b_0 = a_0$, $b_1 = a_1$, ... выполняются до тех пор, покуда существуют как коэффициенты b_i, так и коэффициенты a_i; если же какой-нибудь из коэффициентов a_i или b_i не существует, то коэффициент другого многочлена с тем же номером либо также не существует, либо равен нулю. (Например, многочлены $2 + 3x$ и $2 + 3x + 0x^2$ совпадают.)

Суммой $h(x) = f(x) + g(x)$ многочленов $f(x)$ и $g(x)$ называется многочлен

$$h(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n.$$

(Предполагается, что $n \geqslant k$, и в многочлене $g(x)$ «отсутствующие» коэффициенты заменены нулями.)

Относительно определенной таким образом операции сложения многочлены образуют коммутативную группу, поскольку при любом x^i может стоять произвольное целое число, а целые числа образуют кольцо.

Произведением $k(x) = f(x)g(x)$ многочленов $f(x)$ и $g(x)$ называется многочлен

$$k(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots + a_n b_k x^{n+k}.$$

Можно доказать, что введенная нами операция умножения многочленов ассоциативна. Следовательно, многочлены образуют полугруппу, и эта полугруппа коммутативна. Мы не будем приводить подробное доказательство этого утверждения, поскольку оно довольно громоздко и требует использования полной индукции. По тем же причинам мы не будем останавливаться и на доказательстве дистрибутивности. Скажем лишь, что заданные на множестве многочленов с целочисленными коэффициентами операции сложения и умножения связаны законом дистрибутивности. Следовательно, многочлены с целочисленными коэффициентами образуют коммутативное кольцо.

6. Кольцо многочленов с рациональными коэффициентами.

7. Кольцо многочленов с вещественными коэффициентами.

8. Кольцо многочленов с комплексными коэффициентами.

Во всех трех примерах 6—8 доказательство того, что соответствующие множества многочленов являются кольцами, проводится так же, как в случае многочленов с целочисленными коэффициентами.

9. Рассмотрим пары вещественных чисел (a, b). [Пары (a, b) и (c, d) бу-

дем считать равными в том и только в том случае, если $a = c$ и $b = d$.] Определим сложение пар при помощи тождества $(a, b) + (c, d) = (a + c, b + d)$, а умножение — при помощи тождества $(a, b)\ (c, d) = (ac, bd)$.

Пары вещественных чисел образуют коммутативную группу относительно заданной на них операции сложения. Это следует из того, что операция сложения совпадает с операцией сложения, определенной на прямом произведении двух вещественных прямых. (Аналогичные рассуждения применимы и к операции умножения, если воспользоваться не вводившимся ранее, но вполне разумным понятием прямого произведения полугрупп.) Умножение пар ассоциативно, поскольку операция, производимая над каждой компонентой пар, ассоциативна. По той же причине умножение пар вещественных чисел коммутативно.

Дистрибутивность нетрудно проверить при помощи несложных выкладок: с одной стороны, $[(a, b) + (c, d)](e, f) = (a + c, b + d) \cdot (e, f) = ([a + c]e, [b + d]f)$, а с другой стороны, $(a, b)\ (e, f) + (c, d)\ (e, f) = (ae, bf) + (ce, df) = (ae + ce, bf + df)$. Элементы, стоящие в правых частях последних равенств, совпадают в силу дистрибутивности сложения чисел по умножению.

Итак, доказано, что пары вещественных чисел образуют коммутативное кольцо.

10. Рассмотрим тройки вещественных чисел (a, b, x). (Две тройки считаются равными, если их соответствующие компоненты равны.) Определим сложение троек тождеством $(a, b, x) + (c, d, y) = (a + c, b + d, x + y)$, а умножение — тождеством $(a, b, x)\ (c, d, y) = (ac, bd, xy)$.

Если ограничиться рассмотрением лишь двух первых компонент, то получится коммутативное кольцо, изученное в предыдущем примере. Следовательно, нам остается лишь доказать, что третьи компоненты троек, стоящих в левых и правых частях соответствующих тождеств, всегда равны.

С операцией сложения никаких трудностей не возникает, поскольку множество троек вещественных чисел с заданной на нем операцией сложения можно рассматривать как прямое произведение трех аддитивных групп вещественных чисел. При умножении третья компонента произведения $[(a, b, x)\ (c, d, y)]\ (e, f, u)$ равна $acu + f(ay + dx)$, а третья компонента произведения $(a, b, x)\ [(c, d, y)\ (e, f, u)]$ равна $a(cu + fy) + dfx$. Нетрудно видеть, что обе компоненты совпадают. Заметим, что умножение троек вещественных чисел не коммутативно, так как третья компонента $cx + by$ произведения $(c, d, y)\ (a, b, x)$, вообще говоря, не совпадает с $ay + dx$.

Все это вместе приводит к появлению двух законов дистрибутивности. В зависимости от того, с какой стороны — справа или слева — разрешается умножать почленно сумму, говорят о «правом» или о «левом» законе дистрибутивности. Выясним, выполняется ли для сложения троек какой-нибудь закон дистрибутивности и, если выполняется, то какой именно? Третья компонента произведения $[(a, b, x) + (c, d, y)](e, f, u)$ равна $(a + c)u + f(x + y)$; третья компонента суммы произведений $(a, b, x)(e, f, u) + (c, d, y)(e, f, u)$ равна $(au + fx) + (cu + fy)$. Нетрудно видеть, что обе компоненты совпадают. Следовательно, сложение троек дистрибутивно справа.

Третья компонента произведения $(e, f, u)[(a, b, x) + (c, d, y)]$ равна $e(x + y) + (b + d)u$, третья компонента суммы произведений $(e, f, u)\ (a, b, x) + (e, f, u)(c, d, y)$ равна $(ex + bu) + (ey + du)$. В этом случае обе компоненты совпадают. Следовательно, сложение троек дистрибутивно не только справа, но и слева. Итак, тройки вещественных чисел образуют кольцо, но кольцо не коммутативное.

Кольцом называется тройка $\langle R;\ f,\ g\rangle$, где R — некоторое множество, $\langle R;\ f\rangle$ — коммутативная группа, $\langle R;\ g\rangle$ — полугруппа, и для любых трех элементов a, b и c множества R операции f и g связаны соотношениями

$$g(f(a,\ b),\ c) = f(g(a,\ c),\ g(b,\ c))$$

и

$$g(c,\ f(a,\ b)) = f(g(c,\ a),\ g(c,\ b)).$$

Операция f задает в кольце «сложение», а операция g — «умножение» (поэтому операцию f часто обозначают, как обычное сложение чисел, знаком $+$, а операцию g — точкой).

Рассмотрим теперь подробно, каким требованиям должно удовлетворять кольцо. Подчеркнем еще раз, что в определение кольца входят оба закона дистрибутивности.

Прежде всего, на множестве R должны быть заданы две операции: сложение и умножение. Обе операции должны быть ассоциативны:

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

и $(ab)\,c = a\,(bc)$.

Относительно операции сложения в кольце должен существовать единичный элемент, называемый нулем кольца и обозначаемый 0. Если a — произвольный элемент кольца, то $a + 0 = a$. Операция сложения должна быть коммутативной: $a + b = b + a$. Для каждого элемента в кольце должен существовать обратный элемент (относительно операции сложения), называемый также противоположным; элемент, противоположный элементу a, принято обозначать $(-a)$. Он удовлетворяет соотношению $a + (-a) = 0$.

Наконец, операции сложения и умножения должны быть связаны двумя законами дистрибутивности:

$$(a + b)\,c = ac + bc$$

и $c\,(a + b) = ca + cb$.

(Оба тождества должны выполняться для любых элементов a, b и c множества R.)

Заданная в кольце операция сложения, разумеется, обладает всеми свойствами групповой операции в коммутативной группе.

Сумму элементов b и $(-a)$ часто обозначают $b - a$.

Докажем, что нуль кольца является «нулевым элементом» для операции умножения, то есть при умножении на него любого элемента кольца всегда получается нуль кольца. (Аналогичное свойство числа 0 известно; мы же выведем это свойство нулевого элемента из аксиом кольца.)

Так как соотношение $b = b + 0$ выполняется для любого элемента b кольца, то для всех элементов a кольца справедливо соотношение $ab = a(b + 0)$, откуда в силу левого закона дистрибутивности получаем $ab = ab + a0$. Поскольку элементы кольца образуют аддитивную группу (относительно заданной в кольце операции сложения), то отбрасывая (или «вычитая») члены ab из правой и левой частей последнего равенства, получаем, что $0 = a0$ для любого элемента a кольца. (Аналогичным образом можно доказать, что для любого элемента a кольца выполняется соотношение $0a = 0$.)

Из полученных тождеств следует *правило знаков*, хорошо известное для чисел.

Используя уже доказанные свойства сложения, выведем из соотношения $0 = b + (-b)$ новое соотношение $0 = a0 = a(b + (-b)) = ab + a(-b)$, выполняющееся для любых элементов a и b кольца. Так как элемент, противоположный любому элементу кольца, однозначно определен, то элемент $a(-b)$ может быть только противоположным элементу ab, то есть совпадать с элементом $-(ab)$. Аналогичным образом можно убедиться в правильности соотношения $(-a)b = -(ab)$. Сравнивая выведенные соотношения, получаем $(-a)(-b) = -(a(-b)) = -((-a)b)$, что совпадает с ab, так как любой элемент совпадает с элементом, противоположным противоположному.

Полученные соотношения позволяют без труда доказать, что $a(b-c) = ab - ac$ и $(b - c)a = ba - ca$. Столь же легко доказывается дистрибутивность и при большем числе слагаемых, даже если некоторые из них входят со знаком минус. (Разумеется, при раскрытии скобок с «отрицательными» слагаемыми надлежит пользоваться правилом знаков.)

В общем случае свойства колец существенно отличаются от свойств

кольца целых чисел. Из примера 10 ясно, что $(0, b, x)\ (c, 0, y) = (0,0,0)$ и что это произведение — нуль кольца троек вещественных чисел.

Два элемента кольца, произведение которых равно нулю, хотя каждый из сомножителей отличен от нуля, называются *делителями нуля*. Если кольцо не содержит делителей нуля, то оно называется *кольцом без делителя нуля*.

Наиболее «естественные» кольца, такие, как кольцо целых чисел или кольцо многочленов, не содержат делителей нуля и коммутативны.

Чтобы подчеркнуть сходство коммутативных колец без делителей нуля с кольцом целых чисел, их принято называть областями целостности.

Термин «коммутативное кольцо» означает, что умножение в кольце коммутативно. Аналогичным образом любое другое определение, стоящее перед словом «кольцо», также характеризует какое-то свойство операции умножения в кольце (поскольку другая операция в кольце — сложение — обладает максимальным запасом «хороших» свойств). Так, единичным элементом, или единицей, кольца называется элемент e, для которого соотношение $ea = ae = a$ выполняется при любом элементе a кольца. (Если выполняется соотношение $ea = a$, то e называется *левой* единицей. Если же выполняется соотношение $ae = a$, то e — *правая* единица кольца.)

Если в кольце есть единица, то оно называется кольцом с единицей.

Если для элемента a кольца найдется такой элемент b, что $ba = e$, то b называется *левым обратным* элементом для элемента a. Аналогичным образом определяется и *правый обратный* элемент.

Если b — левый, а c — правый обратный элемент для элемента a, то, поскольку $b = be = b(ac) = (ba)c = ec = c$, элементы b и c совпадают. Эта же цепочка равенств показывает, что элемент b (или c) определен однозначно. В таких случаях говорят, что существует элемент, обратный элементу a, и обозначают его a^{-1}.

Наиболее важными среди полугрупп были такие, в которых для каждого элемента существовал обратный элемент: полугруппы, обладавшие этим свойством, оказались группами. Было бы очень интересно найти кольца с аналогичным свойством. Итак, рассмотрим кольцо с единицей e. Если для всех элементов кольца существуют обратные элементы, то нуль кольца также обладает обратным элементом, который мы обозначим b. Следовательно, должно выполняться соотношение $b0 = e$. Но произведение $b0$, как известно, совпадает с 0, поэтому равенство $b0 = e$ может выполняться только в том случае, если $e = 0$. Но тогда для произвольного элемента a кольца получаем $a = ae = a0 = 0$. Следовательно, кольцо с интересующим нас свойством содержит лишь один элемент — нуль.

Кольцо, в котором для всех элементов существуют обратные, состоит только из нуля и называется нулевым кольцом.

Итак, если мы не хотим ограничиться рассмотрением столь бессодержательного случая, то от существования обратных элементов для всех элементов кольца придется отказаться. Более того, придется отказаться и от существования обратных элементов для делителей нуля. Действительно, если $ab = 0$ и $ca = e$, то, поскольку $0 = c0 = c(ab) = eb = b$, «второй» сомножитель равен нулю. («Первым» мы считаем сомножитель, для которого в кольце существует обратный элемент, в данном случае — элемент a.) Кольца, в которых для всех отличных от нуля элементов существуют обратные, называются *телами*. Как мы только что убедились, в телах не существует делителей нуля.

Кольца, в которых для всех отличных от нуля элементов существуют обратные, называются *телами*. Тела не содержат делителей нуля.

Если тело коммутативно, то оно

заведомо является областью целостности (то есть коммутативным кольцом без делителей нуля).

(Сравнительно недавно в специальной литературе тела было принято называть коммутативными телами, а если коммутативность не предполагалась, то тела назывались косыми.)

Та (заметим, немаловажная) роль, которую среди полугрупп играют группы, среди колец отведена телам. Действительно, тела — это кольца, в которых «для стольких элементов существуют обратные элементы, сколько вообще можно себе представить». Тело не является группой относительно операции умножения, поскольку обратные элементы существуют только для элементов, отличных от нуля. Именно поэтому все элементы, отличные от нуля, удобно рассмотреть особо.

Если кольцо является телом, то оно не содержит делителей нуля, то есть произведение любых двух отличных от нуля элементов кольца также отлично от нуля. Это означает (поскольку операция умножения ассоциативна), что отличные от нуля элементы тела образуют полугруппу по умножению. Так как тело содержит единичный элемент и элемент, обратный отличному от нуля элементу, отличен от нуля (поскольку элемент, обратный обратному, существует), то элементы тела, отличные от нуля, образуют группу по умножению. Наоборот, если отличные от нуля элементы кольца образуют группу по умножению, то единичный элемент этой группы совпадает с единицей кольца (так как $0e = e0 = 0$) и для всех элементов, отличных от нуля, существуют обратные. Следовательно, такое кольцо является телом.

Рассмотрим несколько примеров тел.

ПРИМЕРЫ

1. Тело рациональных чисел. О рациональных числах уже известно, что они образуют кольцо. Мы хотим удостовериться в том, что это кольцо является телом. Для этого требуется доказать, что для всех отличных от нуля рациональных чисел существуют обратные числа (в множестве рациональных чисел!). Но это очевидно, так как известно, что всякое рациональное число можно представить в виде a/b (a и b — целые числа) и если оно отлично от нуля, то $a \neq 0$ и поэтому существует такое рациональное число b/a, для которого $(a/b)\,(b/a) = 1$. (Очень важно, чтобы обратный элемент принадлежал тому же кольцу, которому принадлежит исходный элемент. Например, целые числа не образуют тела, хотя для любого отличного от нуля целого числа и существует обратное, но, как правило, оно не целое.)

2. Тело вещественных чисел. Вещественные числа образуют кольцо потому, что для любого отличного от нуля вещественного числа в множестве вещественных чисел существует обратное. («Строгое» доказательство этого утверждения было бы весьма громоздким, поскольку мы не дали точного определения того, что следует понимать под вещественным числом.)

3. Тело комплексных чисел. О комплексных числах уже известно, что они образуют кольцо. Докажем, что это кольцо является телом, то есть что для всякого отличного от нуля комплексного числа $a + bi$ найдется комплексное число $x + yi$, которое при умножении на $a + bi$ даст 1. (Поскольку умножение комплексных чисел коммутативно, то безразлично, с какой стороны умножать $x + yi$ на $a + bi$ — справа или слева). Умножив $x + yi$ на $a + bi$, получим систему из двух линейных уравнений, допускающую единственное решение: $x = a/(a^2 + b^2)$, $y = (-b)/(a^2 + b^2)$. Прежде всего заметим, что оба числа x и y действительно существуют: знаменатель дробей отличен от нуля (в противном случае чис-

ла a и b и, следовательно, $a + bi$ были бы равны 0). Вычислив произведение

$$(a + bi)(x + yi) = (ax - by) + (ay + bx)i$$

и подставив вместо x и y найденные значения, получим

$$ax - by = \frac{a^2 - (-b^2)}{a^2 + b^2} \text{ и}$$

$$ay + bx = \frac{a(-b) + ba}{a^2 + b^2}.$$

Следовательно, произведение действительно равно $1 + 0i$, то есть 1.

4. Тело чисел вида $a + b\sqrt{2}$ (a и b — рациональные числа). Поскольку речь идет о числах, то все тождества выполняются. Необходимо лишь проследить за тем, чтобы операции сложения и умножения не выводили из рассматриваемого множества. Соотношения $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$; $-(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2}$ и $0 = 0 + 0\sqrt{2}$ показывают, что числа вида $a + b\sqrt{2}$ образуют группу по сложению (здесь мы используем известное свойство рациональных чисел — то, что они образуют группу по сложению). Рассмотрим теперь произведение двух таких чисел:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + bd \cdot 2 = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

Так как числа $ac + 2bd$ и $ad + bc$ рациональны, то произведение имеет тот же вид, что и сомножители. Следовательно, числа вида $a + b\sqrt{2}$ с рациональными a и b образуют кольцо. Осталось лишь доказать, что для чисел такого вида, отличных от нуля, всегда существуют обратные числа (также представимые в виде $a + b\sqrt{2}$ с рациональными a и b). Коэффициенты числа, обратного числу $a + b\sqrt{2}$, мы найдем, решив систему двух линейных уравнений с двумя неизвестными. Единственное решение имеет вид

$$(a + b\sqrt{2})^{-1} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

Как показывает прямая проверка, это число действительно обратно числу $a + b\sqrt{2}$, но необходимо еще поразмыслить над тем, «существует» ли число $(a + b\sqrt{2})^{-1}$, то есть не обращается ли знаменатель в нуль. Но если бы знаменатель обращался в нуль, то выполнялось бы равенство $a^2 - 2b^2 = 0$, а это означало бы, что $\sqrt{2}$ — рациональное число. Поскольку число $\sqrt{2}$ иррационально, то число $(a + b\sqrt{2})^{-1}$ «существует».

Если кольцо не содержит делителей нуля, то это еще не означает, что оно является телом. Например, в кольце целых чисел делителей нуля нет, но это кольцо все же не тело (например, в нем не существует числа, обратного числу 2). Кольцо многочленов также не содержит делителей нуля.

Доказать это можно следующим образом. Рассмотрим многочлен $f(x) = a_0 + a_1x + \ldots + a_nx^n$ и предположим, что $a_n \neq 0$. (Такое предположение всегда допустимо, если только речь не идет о многочлене, тождественно равном нулю.) Такой многочлен называется *многочленом n-й степени*, а a_n — *коэффициентом при старшем члене*. Если $g(x) = b_0 + b_1x + \ldots + b_kx^k$ — многочлен k-й степени (следовательно, b_k — коэффициент при старшем члене), то произведение многочленов $f(x)$ и $g(x)$ имеет вид $a_0b_0 + \ldots + a_nb_kx^{n+k}$. Это многочлен $(n + k)$-й степени, а коэффициент при его старшем члене равен a_nb_k. Поскольку $a_nb_k \neq 0$, то мы действительно получаем многочлен степени $n + k$, и, следовательно, произведение любых двух многочленов, тождественно не равных нулю, также тождественно не равно нулю.

«Сходство» между кольцом целых чисел и кольцом многочленов отнюдь не исчерпывается тем, что оба кольца не содержат делителей нуля. Известно, что любое целое число можно (по существу единственным

способом) представить в виде произведения простых чисел. Решение алгебраических уравнений высоких степеней весьма упрощается тем, что многочлены допускают аналогичное разложение. Всякий многочлен (например, с рациональными коэффициентами) можно представить в виде произведения неразложимых далее многочленов (также с рациональными коэффициентами), причем это разложение в определенном смысле единственно. Известно, что для любых двух целых чисел существует наибольший общий делитель: аналогичное утверждение справедливо и для любых двух многочленов. Известно также, что в множестве целых чисел деление без остатка может оказаться невыполнимой операцией, но всегда выполнимо деление с остатком. Аналогичное утверждение можно доказать и для многочленов. Все это свидетельствует о том, насколько интересно рассматривать кольца целых чисел и многочленов, обладающие столь необычайным «сходством».

ЗАДАЧИ

1. На множестве многочленов задана следующая операция: если $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, то $f(x) \circ g(x) = a_0 + a_1g(x) + a_2 \times (g(x))^2 + \ldots + a_n(g(x))^n$. Доказать, что относительно сложения и заданной операции (рассматриваемой как умножение в кольце) многочлены образуют «почти» кольцо, то есть обе операции удовлетворяют всем условиям, за исключением левого закона дистрибутивности. Какой вывод можно сделать на основании приведенного примера?

2. Доказать, что, если кольцо содержит не более трех элементов, то оно коммутативно.

3. Построить пример кольца с четырьмя элементами, которое не коммутативно.

4. На множестве пар комплексных чисел заданы следующие операции: $(a, b) + (c, d) = (a + c, b + d)$; $(a, b)(c, d) = ac - b\overline{d}, ad - b\overline{c})$. Доказать, что при этом получается не коммутативное тело ($\overline{d}$ и $\overline{c}$ означают числа, комплексно сопряженные с числами d и c).

5. Доказать, что, если на элементах произвольной коммутативной (аддитивной) группы задать операцию, сопоставляющую любым двум элементам нуль (то есть единичный элемент группы), то получится кольцо. (Это кольцо называется *аннуляторным кольцом*.)

1.2. Разложение на простые множители

Продолжим рассмотрение целых чисел и многочленов. Мы уже упоминали о том, что многие свойства кольца целых чисел и кольца многочленов аналогичны. К наиболее важным общим свойствам относятся разложение целых чисел в произведение простых чисел и разложение многочленов в произведение неразложимых множителей. Докажем, что оба разложения следуют из осуществимости операции «деление с остатком» на множествах целых чисел и многочленов. Разумеется, мы не будем проводить отдельно два доказательства, а покажем, что, если в кольце осуществимо «деление с остатком», то его элементы в определенном смысле допускают разложение на простые множители.

Прежде всего поясним, что такое деление с остатком. Каким образом можно убедиться в том, что оно осуществимо в множестве целых чисел? Трудность заключается в том, что, если производить деление не только положительных, а любых целых чисел, то делитель не обязательно будет положительным. Предположим, что целое число a требуется разделить на целое число b. Если $b = 0$, то все кратные числа b также равны нулю, и поэтому остаток всегда равен a. Следовательно, при $b = 0$ ни о каком делении с остатком говорить нельзя. Рассмотрим теперь случай, когда $b \neq 0$. Отложим на числовой

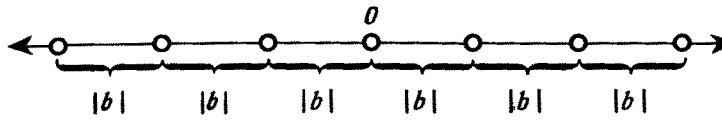


Рис. 54

оси вправо и влево от точки 0 числа, кратные числу b (рис. 54).

Длина каждого отрезка не обязательно равна b: можно лишь утверждать, что она равна $|b|$ (абсолютной величине числа b). Точка, соответствующая числу a, находится где-то на числовой оси между двумя последовательными кратными числа b. Предположим, что qb — наибольшее из кратных чисел b, не превосходящих числа a. (Число q может быть отрицательным и даже нулем.)

На рис. 55 разность $a - qb$ либо равна нулю, либо положительна, но меньше $|b|$. Обозначив разность $a - qb$ через r, мы сможем сформулировать результат наших рассуждений следующим образом:

для любого целого числа a и отличного от нуля целого числа b всегда найдутся такие целые числа q и r, что

$$a = qb + r, \qquad 0 \leqslant r < |b|.$$

Перейдем теперь к делению с остатком многочленов. Для этой операции небезразлично, какие коэффициенты у многочленов, поскольку, например, для многочленов с целочисленными коэффициентами деление с остатком выполнимо не всегда. (Для выполнимости операции «деление с остатком» необходимо лишь, чтобы коэффициенты многочленов были элементами какого-нибудь коммутативного тела.) В случае многочленов мы не можем сказать, что один многочлен меньше другого. Единственный показатель, по которому мы в каком-то смысле можем судить о «величине» многочлена, — это степень многочлена. Покажем на примере, что степень многочлена действительно служит мерой «величины» многочлена.

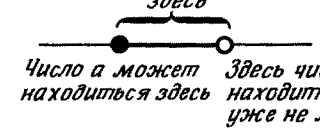


Рис. 55.

Пример выбран так, что оба многочлена имеют целочисленные коэффициенты и коэффициент при старшем члене делителя (при наивысшей степени x) равен 1.

Мы рассмотрим довольно частый случай деления с остатком многочленов. Но добиться, чтобы коэффициент при старшем члене многочлена-делителя был равен 1, можно всегда. Действительно, если заданы два многочлена $f(x)$ и $g(x)$ (первый многочлен требуется разделить на второй), а коэффициент при старшем члене многочлена $g(x)$ равен c, то от исходных многочленов $f(x)$ и $g(x)$ можно перейти к многочленам $f^*(x)$ и $g^*(x)$, выбранным так, что $f(x) = cf^*(x)$ и $g(x) = cg^*(x)$. Частное от деления многочлена $f^*(x)$ на многочлен $g^*(x)$ будет таким же, как частное от деления многочлена $f(x)$ на многочлен $g(x)$, но остатки от деления исходных многочленов и многочленов со звездочкой будут различными из-за деления на коэффициент при старшем члене делителя. Если $f^*(x) = q(x) \cdot g^*(x) + r^*(x)$, то, умножив обе части равенства на c, получим: $f(x) = q(x)g(x) + r(x)$, где $r(x) = cr^*(x)$. Так как при умножении на число, отличное от нуля, степень многочлена не изменяется, то все соотношения между степенями, выполняющиеся для одного равенства, остаются в силе и при переходе к другому равенству. Пользуясь этим, мы в дальнейшем, чтобы не усложнять вычислений, будем выбирать делитель с коэффициентом при старшем члене, равным 1.

Итак, пусть заданы два многочлена

$$f(x) = 3x^5 - 2x^4 + x^3 - x^2 + 5 \text{ и}$$

$$g(x) = x^3 - 3x^2 + 2x - 3.$$

(Мы записали первыми старшие члены многочленов потому, что такая запись более удобна при выполнении деления.) Прежде всего разделим старший член делимого на старший

член делителя: $3x^5 : x^3 = 3x^2$. Умножим частное на $g(x)$ и полученное произведение вычтем из многочлена $f(x)$:

$$f_1(x) = f(x) - 3x^2 g(x) =$$
$$= (3x^5 - 2x^4 + x^3 - x^2 + 5) -$$
$$- (3x^5 - 3x^4 + 6x^3 - 9x^2) =$$
$$= x^4 - 5x^3 + 8x^2 + 5.$$

Повторим все с самого начала, заменив многочлен $f(x)$ многочленом $f_1(x)$. От деления старших членов мы получим $x^4 : x^3 = x$, поэтому

$$f_2(x) = f_1(x) - xg(x) =$$
$$= (x^4 - 5x^3 + 8x^2 + 5) -$$
$$- (x^4 - x^3 + 2x^2 - 3x) =$$
$$= -4x^3 + 6x^3 + 3x + 5.$$

Проделаем все действия еще раз. Так как $(-4x^3) : x^3 = -4$, то

$$f_3(x) = f_2(x) - (-4) g(x) =$$
$$= (-4x^3 + 6x^2 + 3x + 5) -$$
$$- (-4x^3 + 4x^2 - 8x + 12) =$$
$$= 10x^2 + 11x - 7.$$

Подставляя в это соотношение полученные выражения для $f_2(x)$ и $f_1(x)$, получаем

$$10x^2 + 11x - 7 = f_3(x) - (-4) g(x) =$$
$$= (f_1(x) - xg(x)) - (-4) g(x) =$$
$$= f_1(x) - (x - 4) g(x) =$$
$$= (f(x) - (3x^2) g(x)) - (x - 4) g(x) =$$
$$= f(x) - (3x^2 + x - 4) g(x),$$

откуда

$$f(x) = (3x^2 + x - 4) g(x) +$$
$$+ (10x^2 + 11x - 7),$$

или, если ввести обозначения $q(x) = 3x^3 + x - 4$ и $r(x) = 10x^2 + 11x - 7$,

$$f(x) = q(x) g(x) + r(x),$$

где степень многочлена $r(x)$ меньше степени многочлена $g(x)$. Ясно, что проделанные нами операции всегда выполнимы, поскольку деление продолжается до тех пор, пока не получится многочлен, степень которого меньше степени делителя $g(x)$, или многочлен, тождественно равный нулю.

Для любого многочлена $f(x)$ и не обращающегося тождественно в нуль многочлена $g(x)$ существуют такие многочлены $q(x)$ и $r(x)$, что

$$f(x) = q(x) g(x) + r(x),$$

где степень многочлена $r(x)$ меньше степени многочлена $g(x)$ или $r(x) \equiv 0$.

(Запись $r(x) \equiv 0$ означает не алгебраическое уравнение, а многочлен $r(x)$, все коэффициенты которого равны нулю.)

Евклидовы кольца. Попытаемся теперь обобщить полученные результаты, распространив их на другие кольца. Выполняя деление с остатком в кольце целых чисел и в кольце многочленов, мы находили остатки, которые в каком-то смысле были меньше делителя. В каком именно смысле надлежит понимать «величину» делителя и остатка, можно определить при помощи функции, заданной на элементах кольца. Поскольку многочлен, тождественно равный нулю, «не имеет» степени, то эту функцию целесообразно рассматривать только на элементах кольца, отличных от нуля. Каждому элементу a кольца, отличному от нуля, поставим в соответствие значение функции $\varphi(a)$, которое в обоих рассмотренных нами случаях (для кольца целых чисел и кольца многочленов) могло быть только неотрицательным. Поэтому в дальнейшем мы будем рассматривать области целостности с единицей, в которых любому отличному от нуля элементу a поставлено в соответствие неотрицательное число $\varphi(a)$, и для любых элементов a и b кольца (если $b \neq 0$) можно найти такие элементы q и r кольца, что

$$a = qb + r,$$

причем либо $r = 0$, либо $\varphi(r) < \varphi(b)$. Деление с остатком позволяет осуществить так называемый *алгоритм Евклида* (по крайней мере воспользоваться этим алгоритмом для нахождения общего делителя), поэтому рассмотренные нами кольца называются *евклидовыми кольцами*.

Как было показано, целые числа или многочлены с рациональными коэффициентами образуют евклидовы кольца. Коммутативные тела также являются евклидовыми кольцами. Действительно, если всем отличным от нуля элементам поставить в соответствие единицу, то при $b \neq 0$ получим: $a = (a/b)b + 0$, что и доказывает наше утверждение.

Если мы хотим доказать, что во всяком евклидовом кольце существует наибольший общий делитель и элементы допускают однозначно определенное разложение на простые множители, то введенным нами понятиям необходимо дать самые общие определения. Более того, кое-какие понятия необходимо определить и «про запас» — они понадобятся нам в дальнейшем для доказательств.

Прежде всего следует пояснить, что означают такие понятия, как делимость, делитель и кратное для произвольного евклидова кольца. Делимость по существу означает выполнимость деления. Но обычно операция деления известна, тогда как для колец такое допущение в общем случае неверно. Именно поэтому для колец делимость удобно определить «с конца» — по результату деления. Выполнив деления, мы получаем частное, которое при умножении на делитель дает делимое. Это можно сформулировать и в общем случае.

Элемент b области целостности называется делителем элемента a области целостности, если в области целостности найдется такой элемент c, для которого $a = bc$, элемент a называется кратным элемента b.

Такое определение позволяет говорить о делимости и в том случае, когда деление невыполнимо. Например, на нуль делить нельзя. Тем не менее можно утверждать, что нуль является делителем нуля (или делит нуль), так как, например, при $c = 1$ выполняется соотношение $0 = 0 \cdot 1$. Символ $b|a$ означает, что b — делитель элемента a (b делит a). Теперь уже не представляет особого труда ввести для произвольного кольца понятие общего делителя.

Общим делителем двух или большего числа элементов кольца называется такой элемент, который делит каждый из этих элементов.

Даже располагая определением общего делителя, ввести для произвольного кольца понятие «наибольший общий делитель» не так-то просто. Легко найти наибольший общий делитель нескольких чисел. В случае многочленов трудность можно обойти, выбрав делитель наибольшей степени, но для прочих колец вопрос о том, какой из общих делителей следует назвать наибольшим, остается открытым. Среди элементов произвольного кольца нет ни бóльших, ни меньших. Чтобы понять, как же все-таки определить наибольший общий делитель для элементов произвольного кольца, рассмотрим чуть более внимательно решение задачи о нахождении наибольшего общего делителя двух чисел, например 24 и 60. Выпишем их общие делители: 2, 3, 4, 6, 12. Наибольший из них равен 12. Нетрудно заметить, что число 12 не только наибольший общий делитель, но и кратно всем делителям, а это уже такое свойство, о котором можно говорить и в общем случае.

Элемент $d = (a, b)$ называется наибольшим общим делителем элементов a и b кольца, если:

а) d — общий делитель элементов a и b;

б) d — кратное всех делителей элементов a и b.

Но еще не известно, соответствует ли этому определению наибольший общий делитель целых чисел. Покажем, что во всяком евклидовом кольце для любых двух элементов существует наибольший общий делитель.

Кроме того, мы убедимся в том, что в любом кольце наибольший общий делитель d элементов a и b можно представить в виде $d = ax + by$, где x и y — некоторые элементы кольца. (Мы доказываем это свойство наибольшего общего делителя потому, что оно необычайно важно для дальнейшего.)

Начнем с рассмотрения элементов кольца, представимых в виде $ax + by$. Мы не будем доказывать, что наибольший общий делитель элементов a и b существует и его можно представить в виде $ax + by$, а вместо этого докажем, что наибольший общий делитель находится среди элементов вида $ax + by$.

Пусть $H(a, b)$ — множество элементов кольца, представимых в виде $ax + by$. Это множество обладает следующими свойствами:

1) разность любых двух элементов множества $H(a, b)$ принадлежит множеству $H(a, b)$;

2) произведение любого элемента множества $H(a, b)$ и произвольного элемента кольца всегда принадлежит множеству $H(a, b)$;

3) элементы a и b принадлежат множеству $H(a, b)$.

Доказательство всех трех утверждений сводится к несложным выкладкам. Тождество $(ax + by) - (au + bv) = a(x - u) + b(y - v)$ выполняется при любых элементах x, y, u и v кольца. Но $a(x - u) + b(y - v)$ заведомо принадлежит множеству $H(a, b)$, так как $x - u$ и $y - v$ — элементы кольца. Чтобы доказать второе утверждение, рассмотрим какие-нибудь элементы x, y и u. Для них выполняется тождество $(ax + by)u = a(xu) + b(yu)$, из которого и следует наше второе утверждение. Наконец, третье утверждение мы докажем, выбрав специальным образом элементы кольца. При $x = e$ и $y = 0$ получаем $ax + by = ae + b0 = a + 0 = a$. При $x = 0$ и $y = e$ аналогичное тождество имеет вид $ax + by = a0 + be = 0 + b = b$. Следовательно, a и b принадлежат множеству $H(a, b)$.

Докажем теперь, что множество $H(a, b)$ состоит лишь из элементов, кратных d. Это утверждение очевидно, если в множестве $H(a, b)$ нет других элементов, кроме нуля, так как все элементы, кратные нулю, совпадают с нулем. Если в множестве $H(a, b)$ есть и другие элементы помимо нуля, то каждому из них (поскольку кольцо евклидово) можно поставить в соответствие некоторое неотрицательное целое число.

Выберем в множестве $H(a, b)$ элемент d, которому поставлено в соответствие наименьшее [для элементов множества $H(a, b)$] неотрицательное целое число. Иначе говоря, если d_1 — произвольный элемент множества $H(a, b)$, которому соответствует неотрицательное целое число $\varphi(d_1)$, то $\varphi(d_1)$ по крайней мере не меньше, чем $\varphi(d)$. [Такой элемент d в множестве $H(a, b)$ действительно существует, поскольку в любом подмножестве неотрицательных целых чисел всегда имеется наименьшее число. Никакие другие свойства целых чисел в приводимом нами доказательстве не используются.] Пусть c — произвольный элемент множества $H(a, b)$. Поскольку $d \neq 0$, то для элементов d и c в кольце найдутся такие элементы q и r, что $c = qd + r$ и либо $r = 0$, либо $\varphi(r) < \varphi(d)$. Если r — элемент множества $H(a, b)$, то неравенство $\varphi(r) < \varphi(d)$ выполняться не может. Но принадлежит ли r множеству $H(a, b)$? Разрешив равенство $c = qd + r$ относительно r, получим: $r = c - qd$. Так как $d \in H(a, b)$, то по свойству 2 $qd \in H(a, b)$. Кроме того, поскольку $c \in H(ab)$, то по свойству 1 $r = qd \in H(a, b)$. Но неравенство $\varphi(r) < \varphi(d)$ не может выполняться в силу выбора элемента d. Это означает, что $r = 0$, то есть $c = qd$. Следовательно, любой элемент множества, $H(a, b)$ действительно кратен элементу d. Утверждение о том, что все кратные элемента d принадлежат множеству $H(a, b)$, следует из свойства 2 множества $H(a, b)$.

Сопоставляя полученный результат со свойством 3 множества $H(a, b)$, мы заключаем, что d — общий делитель элементов a и b. Более того, справедливо даже более сильное утверждение: d — наибольший общий делитель элементов a и b. Для доказательства этого утверждения необходимо лишь убедиться в том, что элемент d кратен всем общим делителям элементов a и b.

Действительно, если $c|a$ и $c|b$ (то есть если существуют такие элементы u и v кольца, что $a = cu$ и $b = cv$), то действовать можно следующим образом. Поскольку $d \in H(a, b)$, то найдутся такие элементы t и s кольца, что $d = at + bs$. Подставляя в это соотношение $a = cu$ и $b = cv$, получаем

$$d = at + bs = (cu)\,t + (cv)\,s = cut + cvs = \\ = c\,(ut + vs).$$

Правая часть последнего равенства означает, что элемент d кратен элементу c. Именно это и требовалось доказать.

Далее следовало бы доказать, что наибольший общий делитель однозначно определен, но от этого шага мы воздержимся. Более того, если придерживаться приведенного выше определения, то наибольший общий делитель не будет однозначно определенным, даже если говорить о кольце целых чисел: действительно, вместе с d всеми свойствами наибольшего общего делителя обладает и число $-d$. Аналогичное утверждение справедливо и относительно кольца многочленов с рациональными коэффициентами, в котором наибольший общий делитель сохраняет свои свойства при умножении на любое рациональное число. Итак, наибольшие общие делители двух элементов кольца неотличимы, ни один из них ничем не выделен по сравнению с другим. Следовательно, необходимо выяснить, как связаны между собой наибольшие общие делители элементов и кольца. По определению все они делят друг друга, поэтому неудивительно, что в тех случаях, когда речь идет о делимости, наибольшие общие делители ничем не отличаются один от другого. Если каждый из двух элементов коммутативного кольца делит другой, то такие элементы называются *ассоциированными*.

Элементы a и b кольца называются ассоциированными, если в кольце существуют такие элементы u и v, что $a = bu$ и $b = av$.

Из определения следует, что $a = bu = (av)u = a(vu)$, откуда $a(e - vu) = a - avu = 0$. Так как кольцо не содержит делителей нуля, то (если $a \neq 0$) $e = vu$. Следовательно, u и v — делители единичного элемента.

Делители единичного элемента кольца называются единицами.

Например, в кольце целых чисел существуют две единицы: $+1$ и -1, в кольце многочленов единицами являются рациональные числа. Следовательно, если два элемента кольца ассоциированы, то каждый из них отличается от другого множителем, равным единице. Наоборот, если один элемент кольца равен другому элементу кольца, умноженному на единицу, то эти элементы ассоциированы.

Действительно, если $a = bu$ и u — единица (то есть если в кольце существует такой элемент v, что $uv = e$), то, поскольку $av = (bu)v = be = b$, элементы a и b ассоциированы.

С точки зрения делимости произведение не изменится, если умножить его на единицу или заменить любой из сомножителей ассоциированным с ним элементом. Поэтому разложение любого элемента кольца можно получить, записав его в виде произведения, содержащего на одну единицу больше, чем прежде. Но такое разложение не позволяет «упростить» элемент, поскольку каждый сомножитель ассоциирован с исходным.

Элемент кольца, отличный от единичного и допускающий лишь такие разложения в произведение двух элементов, в которые одним из сомножителей входит единичный элемент кольца, называется *неразложимым*.

В кольце целых чисел неразложимыми элементами являются простые числа. Поэтому теореме об однозначном разложении на простые множители всякого (отличного от 1) натурального числа в случае произвольного кольца соответствует следующее утверждение: «Всякий (отличный от единицы) элемент можно представить в виде произведения неразложимых элементов». Но в данном случае нам необходимо другое свойство простых чисел — так называемое свойство простоты. Для евклидовых колец оба свойства — неразложимость и простота — совпадают, но в общем случае эти два свойства не совпадают. Именно поэтому они и получили различные названия.

Элемент p области целостности называется простым элементом, если он делит любое произведение тогда и только тогда, когда является делителем одного из сомножителей.

Докажем, что в евклидовом кольце элемент прост в том и только в том случае, если он неразложим.

«В одну сторону» это утверждение доказывается без труда. Действительно, если q — простой элемент, то рассмотрим разложение $q = ab$. Его, разумеется, можно представить в виде $qe = ab$. Следовательно, q — делитель произведения ab. По свойству простоты отсюда следует, что q — делитель какого-то из сомножителей, например элемента a, то есть $a = qu$. Но тогда элементы a и q делят друг друга и поэтому ассоциированы, в силу чего b — единица. Это означает, что элемент q допускает разложение в произведение двух сомножителей лишь в том случае, если один из сомножителей — единица, то есть элемент q неразложим. Предположим теперь, что элемент p неразложим и делит произведение ab. Кроме того, пусть d — наибольший общий делитель элементов p и a. Так как d — делитель неразложимого элемента p, то d либо единичный элемент, либо элемент, ассоциированный с p. В последнем случае p заведомо делит a, так как d — делитель элемента a (как общий делитель элементов p и a), а p — делитель элемента d (поскольку d — элемент, ассоциированный с p). Если же d совпадает с единичным элементом, то наибольший общий делитель элементов q и p делит ассоциированный с ним единичный элемент. Следовательно, по определению множества $H(p, a)$, существуют такие элементы x и y кольца, что $px + qa = e$. Умножая это соотношение на b, получаем $pxb + qab = b$. Первое слагаемое в левой части, очевидно, делится на p. Второе слагаемое делится на p по предположению. Следовательно, сумма обоих слагаемых, то есть b, также делится на p. Итак, мы доказали, что, если $p|ab$, то либо $p|a$, либо $p|b$. Это и означает, что p — простой элемент.

После того как мы установили, что для евклидовых колец понятия «простой элемент» и «неразложимый элемент» совпадают, для завершения доказательства теоремы об однозначном разложении произвольного элемента на простые множители остается сделать немного: во-первых, доказать, что такое разложение возможно, и, во-вторых, доказать его единственность. Осуществимость разложения можно сформулировать следующим образом: *в евклидовом кольце всякий элемент, отличный от единичного, можно представить в виде произведения (конечного числа) простых элементов.*

Пусть a — произвольный элемент кольца. Если a — простой элемент, то, представив его в виде «произведения», состоящего из одного-единственного сомножителя, получим разложение на простые множители $a = a$. Если a — не простой элемент (и, кроме того, отличен от единицы и от нуля), то существует разложение $a = bc$, в котором ни один из элементов b и c не является единицей кольца. Если элементы b и c разложимы, то продолжим разложение до тех пор, пока не получим произведение, состоящее только из неразложимых сомножителей. Неприятность могла бы возникнуть лишь в том случае, если бы разложение никогда не завершалось, то есть не обрывалось бы ни на каком шаге. Это означало бы, что в разложении $a = b_1c_1$ один из двух сомножителей, например b_1, в свою очередь допускал бы разложение (если оба сомножителя b_1 и c_1 неразложимы, то разложение исходного элемента a закончено). Элемент b_1 можно было бы представить в виде $b_1 = b_2c_2$, где ни один из сомножителей b_2 и c_2 не является единицей кольца, и какой-то из них, например b_2, допускал бы дальнейшее разложение. Выполнив его, мы получили бы $b_2 = b_3c_3$ и т. д.

Покажем, что разложение любого элемента кольца не может продолжаться неограниченно долго, то есть что после конечного числа шагов какой-нибудь из двух сомножителей, возникающих при разложении очередного элемента, непременно должен совпасть с единичным элементом кольца.

Предположим, что это не так. Пусть H — множество элементов кольца, кратных какому-нибудь из элементов b_i. Ясно, что, если в кольце есть хотя бы один такой элемент, то, умножив его на любой элемент кольца, мы снова получим элемент, кратный какому-то из элементов b_i. С другой стороны, разность двух элементов, каждый из которых кратен какому-то из элементов b_i, также принадлежит множеству H. Например, если $u = b_1x$ и $v = b_3y$, то [так как $b_1 = b_2c_2 = (b_3c_3)c_2$] $u - v = b_3(c_3c_2x) - b_3y = b_3(c_3c_2x - y)$, то есть разность $u - v$ кратна элементу b_3. Аналогичным образом можно доказать, что разность любых двух элементов множества H также кратна какому-то из элементов b_i. Следовательно, множество H обладает двумя свойствами множества H (a, b), определяемого наибольшим общим делителем d элементов a и b, а относительно множества H (a, b) доказано, что оно состоит из эле-

ментов, кратных одному и тому же элементу. Таким образом, элементы множества H кратны некоторому фиксированному элементу d кольца. Поскольку каждый элемент множества H кратен какому-нибудь из элементов b_i, то элемент d, как показано выше, можно представить в виде $d=b_n t$ при некотором индексе n. С другой стороны, элемент b_{n+1} кратен какому-то из элементов b_i (в действительности — единичному элементу) и, следовательно, как элемент множества H его можно представить в виде $b_{n+1}=ds$ (t и s — единицы кольца). Поскольку $b_{n+1}=ds=b_n ts=b_{n+1}c_{n+1}ts$, то $e=c_{n+1}ts$. Следовательно, c_{n+1} вопреки предположению является единицей кольца.

Всякий элемент евклидова кольца (отличный от нуля и единицы) можно разложить в произведение простых элементов.

Прежде чем приступать к доказательству однозначности разложения, необходимо точно сформулировать, как следует понимать однозначность. Известно, что в каждом разложении (вследствие коммутативности) сомножители можно подвергать любым подстановкам. Следовательно, разложения, отличающиеся лишь порядком сомножителей, нельзя считать различными. Мы уже упоминали о том, что от замены сомножителей ассоциированными с ними элементами произведение по существу не изменяется. Более того, может случиться, что при такой замене произведение вообще остается неизменным. Так происходит в том случае, если соответствующее произведение единиц совпадает с единичным элементом кольца. Следовательно, разложения, отличающиеся тем, что какие-то из сомножителей заменены ассоциированными элементами, также нельзя считать различными. Эти замечания показывают, как следует понимать однозначность разложения.

Два разложения называются по существу тождественными, если они отличаются только порядком сомножителей и делителями единицы, то есть если множители, входящие в одно разложение, можно поставить во взаимно-однозначное соответствие с множителями другого разложения так, что соответствующие друг другу сомножители окажутся ассоциированными.

Два разложения называются по существу тождественными, если они отличаются только порядком сомножителей и сомножителями, равными делителям единицы.

Итак, мы приходим к следующему утверждению: *всякий элемент евклидова кольца, отличный от нуля и единицы, допускает однозначное разложение в произведение простых элементов.*

В том, что всякий элемент евклидова кольца можно разложить в произведение простых элементов, мы уже убедились. Остается доказать, что такое разложение однозначно определено. Предположим, что

$$p_1 \cdot p_2 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot \ldots \cdot q_k$$

— два разложения на простые множители одного и того же элемента. Так как p_1 — делитель левой части равенства, то этот же элемент делит и произведение, стоящее в правой части. Поскольку p_1 — простой элемент, то это означает, что p_1 делит один из множителей, входящих в произведение $q_1 \cdot q_2 \cdot \ldots \cdot q_k$. От изменения порядка сомножителей разложение не изменяется, поэтому, не ограничивая общности, можно предположить, что p_1 — делитель элемента q_1. Из соотношения $q_1 = p_1 u$ следует, что u — единица. Действительно, так как q — простой элемент, то он неразложим, а p_1 — не единица. Поскольку мы рассматриваем кольцо без делителей нуля, то на p_1 можно сократить, и мы приходим к равенству

$$p_2 \cdot \ldots \cdot p_n = (uq_2) \cdot \ldots \cdot q_k.$$

Продолжая сокращать на p_2, p_3 и т. д., мы в конце концов «исчерпаем» все простые элементы в правой или в левой части исходного равенства. Но простые элементы должны одновременно «иссякнуть» и в другой части равенства, поскольку произведение простых чисел не может быть равно единице. Следовательно, число простых множителей в правой и левой частях исходного равенства одинаково, а простые элементы, на которые мы производили сокращения, ассоциированы. Они не обязательно должны совпадать с простыми элементами, входившими в исходные разложения (например, после первого шага в правой части возник множитель uq_2, который не обязательно тождествен множителю q_2), но могут отличаться лишь «коэффициентами», равными единицам, и поэтому ассоциированы.

ЗАДАЧИ

Доказать следующие утверждения.

1. Числа вида $a + bi$ (a и b — целые числа, $i = \sqrt{-1}$) образуют кольцо. Это кольцо евклидово (функция φ определена соотношением $\varphi(a + bi) = a^2 + b^2$).

2. Многочлены с целочисленными коэффициентами образуют область целостности. В этом кольце наибольший общий делитель многочленов $2x$ и x^2 не представим в таком виде, в каком представимы наибольшие общие делители элементов евклидова кольца.

3. Числа $a + b\sqrt{-5}$ (a и b — целые числа) образуют кольцо. Числа 2 и $1 + \sqrt{-5}$ не имеют наибольшего общего делителя (представимого в таком виде, в каком можно представить наибольшие общие делители элементов евклидова кольца). Числа 2 и $1 + \sqrt{-5}$ неразложимы, но они не простые. Каждое из разложений $6 = 2 \cdot 3$ и $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ содержит неразложимые множители, но оба разложения существенно различны.

2

Векторные пространства и модули

2.1. Свойства векторов и элементов

Подобно тому как теория групп родилась из рассмотрения подстановок, изучение алгебры векторов в геометрии привело к созданию весьма важного алгебраического понятия.

Прежде всего выясним, что можно сказать о векторах вообще и о векторах на плоскости в частности. Векторами называются «направленные величины». Следуя этому «определению», векторы можно изображать в виде стрелок, имеющих различную длину и различное направление. Вектор считается заданным, если известны его длина и направление. Если два вектора имеют одинаковую длину и одинаковое направление, то они считаются равными (рис. 56).

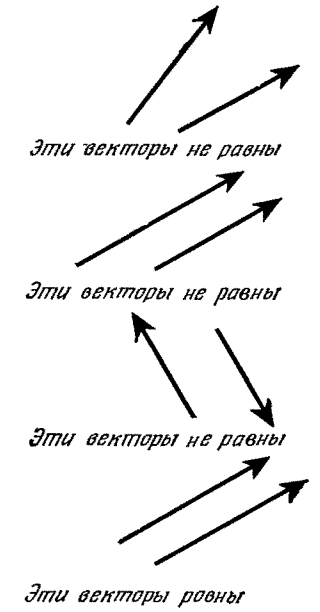


Рис. 56.

Направление векторов включает в себя и «положение» их на плоскости. Мы говорим, что направление двух векторов совпадает, если векторы параллельны и «наконечники стрел» указывают в одну сторону.

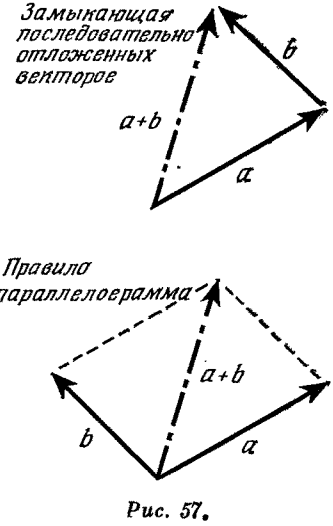


Рис. 57.

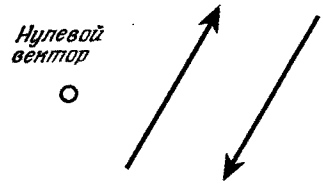


Рис. 58.

Если векторы рассматривать с точки зрения алгебры, то необходимо исследовать, какие операции и как можно производить над ними. Известна операция сложения векторов: сумма векторов a и b определяется либо как замыкающая последовательно отложенных векторов, либо по правилу параллелограмма (рис. 57).

Пользуясь введенным выше понятием равенства векторов, нетрудно показать, что оба определения суммы векторов приводят к одному и тому же результату. Из первого определения следует, что сложение векторов ассоциативно, из второго — что оно коммутативно. (Построить замыкающую последовательно отложенных векторов можно и в том случае, если два вектора-слагаемых параллельны и их нельзя дополнить до параллелограмма.) Итак, сложение векторов — операция ассоциативная и коммутативная, то есть векторы образуют (коммутативную) полугруппу относительно сложения. Всякий раз, когда нам встречается полугруппа, полезно выяснить, не является ли она группой относительно той же операции. Прежде всего следует решить, существует ли единичный элемент, то есть (поскольку операцией является сложение) существует ли «нуль-вектор». Нетрудно видеть, что быть нулевым вектор может лишь в том случае, если он не имеет ни длины, ни направления. Хотя такой вектор нельзя «нарисовать», все же можно сказать, что всеми свойствами нулевого вектора обладает вектор, стянутый в точку. Затем надлежит выяснить, для каждого ли элемента полугруппы существует обратный элемент, то есть для каждого ли вектора на плоскости найдется вектор, дающий в сумме с ним нулевой вектор. Нетрудно видеть, что вектор, обратный данному, имеет одинаковую с ним длину и противоположное направление (рис 58). О таком векторе говорят, что он равен исходному вектору, взятому со знаком минус, и называют его *противоположным* (исходному) вектором.

Итак, мы установили, что векторы на плоскости образуют коммутативную группу относительно сложения векторов. Это означает, что любое утверждение, доказанное относительно коммутативных групп, справедливо относительно векторов на плоскости.

Над векторами на плоскости можно производить не только сложение, но и другую операцию, а именно умножение на число. Умножить вектор на вещественное число λ означает «растянуть» вектор в λ раз. Разумеется, о растяжении можно говорить лишь в том случае, если $\lambda > 1$. При $\lambda = 1$ вектор остается неизменным, а если число λ меньше единицы, но положительно, то вектор сжимается. Направление вектора во всех этих случаях не изменяется.

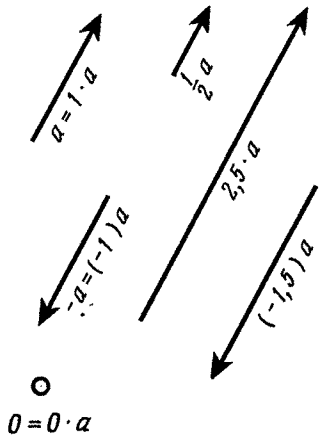


Рис. 59.

Если же число λ отрицательно, то направление вектора изменяется на противоположное (рис. 59).

Но нам не достаточно знать, как умножать векторы на числа. Чтобы эту операцию можно было использовать в вычислениях, необходимо выяснить, каким тождествам она удовлетворяет.

Мы приведем наиболее важные тождества без доказательств. Нетрудно проверить, что они действительно выполняются во всех случаях.

Если λ и μ — вещественные числа, a и b — векторы, то выполняются следующие тождества:

$$(\lambda + \mu)\, a = \lambda a + \mu a,$$

$$\lambda (a + b) = \lambda a + \lambda b,$$

$$(\lambda\mu)\, a = \lambda (\mu a), \quad 1 \cdot a = a.$$

Запомнить эти тождества весьма просто: два первых тождества выражают дистрибутивность, а третье — ассоциативность.

Последнее из приведенных нами тождеств очевидно. Оно необходимо по следующим соображениям. Если мы хотим в дальнейшем рассматривать операции сложения векторов и умножения векторов на числа с общих алгебраических позиций, то, разумеется, нам нельзя упоминать о том, что означает любая операция (этого мы не знаем), поскольку разрешается лишь указывать, каким тождествам она удовлетворяет. Если бы последнее тождество не входило в число «обязательных», то можно было бы утверждать, что произведение числа и вектора всегда равно нулевому вектору. Все остальные тождества при этом также были бы выполнены. Следовательно, последнее тождество необходимо, чтобы исключить из рассмотрения такие «бессодержательные» случаи.

Скаляры. После этих предварительных замечаний перейдем к определению общего понятия, соответствующего векторам. Прежде всего заметим, что при рассмотрении векторов нам встречаются два множества: множество векторов и множество вещественных чисел (числа, чтобы подчеркнуть их отличия от векторов, при этом принято называть *скалярами*).

Векторное пространство. На множестве векторов задано сложение, относительно которого векторы образуют группу. О скалярах (множестве вещественных чисел) известно, что они образуют тело. Связь между скалярами и векторами выражается в том, что их можно умножать (скаляр на вектор), и в результате получается вектор. Умножение вектора на скаляр и операции, заданные на множествах векторов и скаляров, удовлетворяют приведенным выше тождествам. Во всех таких случаях говорят, что мы имеем дело с *векторным пространством* над соответствующим телом.

Прежде всего рассмотрим несколько примеров векторных пространств.

ПРИМЕРЫ

1. Векторы в трехмерном пространстве над телом вещественных чисел. Определения операции сложения и умножения на число для векторов в трехмерном пространстве остаются такими же, как и для векторов на плоскости. Поэтому и тождества для этих операций выглядят так же, как и для векторов на плоскости.

2. Векторы, параллельные заданному вектору, над телом вещественных чисел. Сумма и разность векторов, параллельных заданному вектору, также параллельна заданному вектору. При умножении векторов на вещественное число параллельность не нарушается. Необходимость в проверке тождеств отпадает, поскольку для векторов на плоскости все тождества выполнены.

3. Четверки вещественных чисел над телом вещественных чисел, на которых операции заданы следующим образом:

а) $(a, b, c, d) = (x, y, u, v)$

означает, что $a = x$, $b = y$, $c = u$, $d = v$;

б) $(a, b, c, d) + (x, y, u, v) =$

$= (a + x,\ b + y,\ c + u,\ d + v)$;

в) $a(x, y, u, v) = (ax, ay, au, av)$.

Относительно сложения четверки образуют прямую сумму четырех аддитивных групп вещественных чисел, то есть коммутативную группу.

Произведение вещественного числа и четверки есть некоторая четверка. В том, что операция умножения четверки на вещественное число удовлетворяет соответствующим тождествам, можно убедиться следующим образом. Выпишем соотношения

$$(a + b)(x, y, u, v) =$$
$$= ((a + b)x, (a + b)y, (a + b)u,$$
$$(a + b)v)$$

и

$$a(x, y, u, v) + b(x, y, u, v) =$$
$$= (ax + bx, ay + by, au + bu,$$
$$av + bv).$$

Равенство соответствующих компонент в правых частях этих соотношений следует из дистрибутивности сложения вещественных чисел.

Выпишем далее соотношения

$$a[(x_1, x_2, x_3, x_4) + (y_1, y_2, y_3, y_4)] =$$
$$= (a(x_1 + y_1), a(x_2 + y_2),$$
$$a(x_3 + y_3), a(x_4 + y_4))$$

и

$$a(x_1, x_2, x_3, x_4) + a(y_1, y_2, y_3, y_4) =$$
$$= (ax_1 + ay_1, ax_2 + ay_2, ax_3 + ay_3,$$
$$ax_4 + ay_4).$$

И в этом случае соответствующие компоненты равны в силу дистрибутивности сложения вещественных чисел.

Следующая пара соотношений имеет вид

$$(ab)(x, y, u, v) = ((ab)x, (ab)y,$$
$$(ab)u, (ab)v)$$

и

$$a[b(x, y, u, v)] = (a(bx), a(by),$$
$$a(bu), a(bv)).$$

Соответствующие компоненты в правых частях равны в силу ассоциативности умножения вещественных чисел. Наконец, последнее тождество выполняется, так как

$$1 \cdot (a, b, c, d) = (1 \cdot a, 1 \cdot b, 1 \cdot c, 1 \cdot d) =$$
$$= (a, b, c, d).$$

4. Наборы из n вещественных чисел над телом вещественных чисел относительно операций, заданных в предыдущем примере. Доказательство проводится так же, как и в предыдущем примере. Необходимо лишь иметь в виду, что число компонент равно не 4, а n (впрочем, это не приводит ни к каким «осложнениям», так как соответствующие тождества для наборов из n чисел выполняются в том и только в том случае, если они выполняются для каждой компоненты в отдельности, то есть не зависят от числа компонент).

5. Бесконечные последовательности вещественных чисел над телом вещественных чисел. Две числовые последовательности $a_1, a_2, \ldots, a_n, \ldots$ и $b_1, b_2, \ldots, b_n, \ldots$ считаются равными, если $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_n = b_n$, $\ldots$. Суммой последовательностей $a_1, a_2, \ldots, a_n, \ldots$ и $b_1, b_2, \ldots, b_n, \ldots$ называется последовательность $(a_1 + b_1), (a_2 + b_2), \ldots, (a_n + b_n), \ldots$, а произведением последовательности $a_1, a_2, \ldots, a_n, \ldots$ и числа b — последовательность $ba_1, ba_2, \ldots, ba_n, \ldots$. (Бесконечные числовые последовательности и производимые над ними операции играют важную роль в математическом анализе.)

Доказательство тождеств по существу не отличается от доказательств, приведенных в двух предыдущих примерах. Действительно, из определения равенства двух последовательностей следует, что все тождества надлежит проверять покомпонентно.

6. Многочлены с вещественными коэффи-

циентами над телом вещественных чисел. Операция сложения определена как сложение многочленов, операция умножения на число — как почленное умножение на число.

Как известно, многочлены образуют коммутативную группу относительно сложения многочленов. Произведение многочлена и вещественного числа надлежит понимать в смысле тождества

$$c(a_0 + a_1x + \cdots + a_nx^n) = \\ = ca_0 + ca_1x + \cdots + ca_nx^n.$$

7. Многочлены от многих переменных с вещественными коэффициентами над телом вещественных чисел. Операции сложения и умножения на вещественное число определены как сложение многочленов и почленное умножение их на вещественное число.

Многочлены от многих переменных с вещественными коэффициентами образуют коммутативную группу. Если умножение на вещественное число определить как частный случай умножения многочленов, когда один из сомножителей вырождается в постоянную, то первые два из доказываемых тождеств следуют из дистрибутивности, а третье — из ассоциативности умножения многочленов. Последнее тождество также выполнено, поскольку многочлен, тождественно равный 1, является единичным элементом в кольце многочленов.

8. Векторное пространство над телом вещественных чисел образуют и вещественнозначные функции, если операции определены следующим образом: $h(x) = f(x) + g(x)$ — функция, принимающая в точке c значение $f(c) + g(c)$, а $a \cdot f(x)$ — функция, принимающая в точке c значение $a \cdot f(c)$.

Поскольку сложение чисел коммутативно и ассоциативно, то сложение функций обладает теми же свойствами. Нулевым элементом относительно сложения служит функция, всюду равная нулю, а функцией, противоположной функции $f(x)$, — функция, принимающая в точке c значение $-f(c)$. Произведение вещественнозначной функции и вещественного числа всегда принадлежит множеству вещественнозначных функций. Остается проверить, выполняются ли соответствующие тождества. Функция $(a + b) \cdot f(x)$ принимает в точке c значение $(a + b) \cdot f(c) = a \cdot f(c) + b \cdot f(c)$. Это — не что иное, как значение, принимаемое в точке c функцией $a \cdot f(x) + b \cdot f(x)$. Функция $a(f(x) + g(x))$ принимает в точке c значение $a(f(c) + g(c)) = a \cdot f(c) + a \cdot g(c)$, совпадающее со значением функции $a \cdot f(x) + a \cdot g(x)$ в точке c. Функция $(ab) \cdot f(x)$, как и функция $a(b \cdot f(x))$, принимает в точке c значение, равное $abf(c)$, а значение функции $1 \cdot f(x)$ в точке c совпадает со значением функции $f(x)$.

9. Векторное пространство над телом вещественных чисел образуют комплексные числа, если операцию сложения определить как сложение комплексных чисел, а умножение на вещественные числа — как частный случай умножения комплексных чисел.

Как показано выше, комплексные числа образуют относительно сложения коммутативную группу. Умножение комплексных чисел всегда порождает комплексное число, то есть не выводит из множества комплексных чисел. Тождества, которые требуется доказать, в множестве комплексных чисел переходят в законы дистрибутивности и ассоциативности, а последнее тождество означает, что число 1 «исполняет роль» единичного элемента в кольце комплексных чисел.

10. Вещественные числа образуют векторное пространство над телом рациональных чисел, ес-

ли операция сложения определена как сложение вещественных чисел, а умножение на рациональное число — как умножение вещественных чисел.

Доказательство проводится так же, как и прежде, и опирается на то, что тело вещественных чисел содержит тело рациональных чисел.

Итак, векторное пространство по существу можно рассматривать как две «пятерки», каждая из которых состоит из множества и четырех двухместных операций. Две двухместные операции вместе с одним из множеств образуют тело (разумеется, для этого еще должны выполняться соответствующие тождества), одно множество с одной операцией образуют коммутативную группу и еще одной операцией является умножение вектора на скаляр. Чтобы всякий раз не перечислять все элементы двух пятерок (поскольку теперь понятия группы и тела можно считать известными), достаточно рассматривать лишь «тройку», состоящую из одной группы, одного тела и одной операции умножения на скаляр. Такой подход позволяет дать строгое определение векторного пространства.

Коммутативная группа M называется векторным пространством над коммутативным телом Γ, если задана операция, ставящая каждому $\alpha \in \Gamma$ и $a \in M$ в соответствие некоторый элемент из M, обозначаемый αa. Эта операция обладает следующими свойствами:

$$(\alpha + \beta)\, a = \alpha a + \beta a;$$

$$\alpha\,(a + b) = \alpha a + \alpha b;$$

$$(\alpha\beta)\, a = \alpha\,(\beta a);$$

$$1 \cdot a = a.$$

Элементы M называются векторами, а элементы Γ — скалярами.

Во всех примерах тело Γ состояло из чисел. Но почти все полученные результаты остаются в силе и для любых других тел. Наиболее важны те тела, которые чаще всего встречаются на практике, и среди них — тело вещественных и тело комплексных чисел. Векторные поля над телом рациональных чисел приведены скорее как иллюстрация общего принципа. Встречаются также и векторные пространства над конечными телами и, в частности, над телами, состоящими всего лишь из двух элементов.

Рассмотрим теперь некоторые «детали» векторных пространств и докажем их важные свойства.

Нулевые элементы существуют и среди скаляров, и среди векторов, но они различны. (Например, если речь идет о четверках вещественных чисел, то скалярным нулевым элементом является число 0, а нулевым вектором — четверка (0, 0, 0, 0).) Тем не менее и нулевой скаляр, и нулевой вектор обладают одним свойством числа 0: если один из сомножителей равен нулю, то произведение также равно нулю.

Пусть α — произвольный скаляр, а u — любой вектор. Тогда для нулевого скаляра и нулевого вектора справедливы следующие соотношения:

$$u = 1 \cdot u = (0 + 1) \cdot u = 0 \cdot u + 1 \cdot u = 0 \cdot u + u;$$

$$\alpha \cdot u = \alpha\,(0 + u) = \alpha \cdot 0 + \alpha \cdot u.$$

Из группового свойства сложения векторов следует, что операция, обратная сложению, — вычитание — определена, и, следовательно, $0 \cdot u$ и $\alpha \cdot 0$ — нулевой вектор.

Векторные пространства обладают свойством, аналогичным свойствам колец без делителей нуля, например кольца целых чисел: элемент αu может быть нулевым вектором лишь в том случае, если либо α — нулевой скаляр, либо u — нулевой вектор. Действительно, если $\alpha u = 0$ и $\alpha \neq 0$, то (поскольку существует скаляр α^{-1}) выполняется соотношение

$$0 = \alpha^{-1} 0 = \alpha^{-1}(\alpha u) = (\alpha^{-1}\alpha)\, u = u,$$

то есть $u = 0$.

При вычислениях, производимых с векторами, вектор, противоположный данному, удобно записывать в виде исходного вектора, умноженного на скаляр (-1). Как показывает соотношение

$$u + (-1)u = 1 \cdot u + (-1) \cdot u =$$
$$= (1 + (-1)) \cdot u = 0 \cdot u = 0,$$

вектор $(-1) \cdot u$ действительно совпадает с вектором, противоположным вектору u.

Последнее замечание весьма «приятно», поскольку позволяет исключить вычитание векторов: достаточно заменить в каждой разности уменьшаемое вектором, умноженным на соответствующий скаляр, и свести вычитание к сложению произведений векторов и скаляров. Тем самым мы получаем общий способ строить из заданных векторов новые: составление сумм из заданных векторов, умноженных на скаляры. Возможность представления векторов в виде сумм *скалярных кратных* заданных векторов принадлежит к числу наиболее важных свойств векторов. Такие суммы называются *линейными комбинациями векторов*.

Линейной комбинацией векторов $u_1, u_2, \ldots, u_n$ называется выражение вида

$$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n,$$

где $\alpha_1, \alpha_2, \ldots, \alpha_n$ — произвольные скаляры.

Если все скаляры, входящие в линейную комбинацию, равны нулю, то и сама линейная комбинация порождает нулевой вектор. Такая линейная комбинация называется *тривиальной*.

Нулевой вектор могут порождать не только тривиальные линейные комбинации. Например,

$$5 \cdot (1, 2, -3) + 4 \cdot (2, -3, 5) +$$
$$+ 1 \cdot (-4, 5, 1) + (-3) \cdot (3, 1, 2) =$$
$$= (5, 10, -15) + (8, -12, 20) +$$
$$+ (-4, 5, 1) + (-9, -3, -6) =$$
$$= (-5 + 8 - 4 - 9, \ 10 - 12 + 5 - 3,$$
$$-15 + 20 + 1 - 6) = (0, 0, 0).$$

Составив из заданных векторов линейные комбинации, мы можем составить линейные комбинации из вновь полученных векторов, затем линейные комбинации линейных комбинаций новых векторов и т. д. О важности линейных комбинаций свидетельствует и то, что, начиная со второго шага, мы будем получать выражения одного и того же вида, какие бы линейные комбинации линейных комбинаций ни составляли. Это означает, что *любая линейная комбинация линейных комбинаций заданных векторов является линейной комбинацией исходных векторов*. Например,

$$\lambda (\alpha_1 a + \beta_1 b) + \mu (\alpha_2 a + \beta_2 b) +$$
$$+ \nu (\alpha_3 a + \beta_3 b) = (\lambda\alpha_1 + \mu\alpha_2 + \nu\alpha_3) a +$$
$$+ (\lambda\beta_1 + \mu\beta_2 + \nu\beta_3) b.$$

Аналогичным образом это утверждение можно доказать и при любом другом большем или меньшем числе заданных векторов. (Разумеется, строгое доказательство для общего случая потребовало бы использования полной индукции.)

Из полученного нами результата следует, что ни сложение, ни вычитание, ни умножение на скаляры не выводит из множества линейных комбинаций заданных векторов. Поскольку соответствующие тождества выполняются во всем векторном пространстве, то они выполняются и для линейных комбинаций заданных векторов.

Итак, мы получили подмножество векторного пространства, элементы которого образуют векторное пространство относительно операций, заданных в исходном векторном пространстве. Подмножества такого типа соответствуют подгруппам группы и по аналогии с геометрией называются *подпространствами*.

Подмножество N векторного прост-

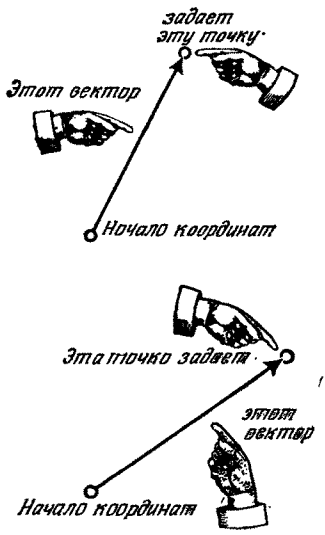


Рис. 60.

ранства M называется подпространством векторного пространства, если оно является векторным пространством относительно операций, заданных в M.

Рассмотрим несколько примеров подпространств.

ПРИМЕРЫ

1. Нулевое пространство и все пространство. Так как $\mathbf{0} + \mathbf{0} = \alpha\mathbf{0} = \mathbf{0}$, то подмножество, состоящее только из нулевого вектора, всегда является подпространством, а поскольку нулевой вектор принадлежит всем подпространствам, то подмножество, состоящее только из нулевого вектора, — «наименьшее» из всех подпространств. С другой стороны, множество всех векторов также можно считать подпространством, поскольку по определению оно является векторным пространством относительно заданных операций. Нулевое подпространство и все пространство называются *тривиальными подпространствами*. Все остальные подпространства называются *истинными подпространствами*.

2. Подпространства векторов в трехмерном пространстве. Поскольку под действием параллельного переноса векторы переходят в тождественные им векторы, то удобно считать, что все векторы отложены от некоторой фиксированной точки (то есть из каждого семейства одинаково направленных, равных по длине и параллельных векторов выбрать по одному «представителю»). Эта точка называется началом координат. Все векторы можно однозначно задать, указав их концы, а любую точку пространства рассматривать как конец некоторого вектора. Тем самым устанавливается взаимно-однозначное соответствие между векторами и точками в трехмерном пространстве (рис. 60).

Это соответствие удобно тем, что позволяет вместо множеств векторов рассматривать гораздо более наглядные множества точек.

Если подпространство состоит из одного-единственного элемента — нулевого вектора, то соответствующее ему множество точек содержит только начало координат.

Если в подпространстве существует вектор a, отличный от нулевого, то этому же подпространству принадлежат и все скалярные кратные вектора a. Нетрудно видеть, что они образуют подпространство, поскольку являются линейными комбинациями вектора a. Все эти векторы параллельны вектору a. Длина их может быть произвольной, а направление либо совпадает с направлением вектора a, либо противоположно ему. Следовательно, концы скалярных кратных вектора a располагаются на прямой, проходящей через конец вектора a и начало координат. Если множество концов векторов, образующих подпространство, мы условимся для кратности называть просто подпространством, то результат наших рассуждений можно сформулировать следующим образом. Подпространствами, заведомо превосходящими по «запасу» элементов нулевое подпространство, состоящее только из начала координат, слу-

жат прямые, проходящие через начало координат. Все истинные подпространства состоят из таких прямых, и каждая прямая, проходящая через начало координат, сама является истинным подпространством.

Предположим теперь, что подпространство содержит по крайней мере две различные прямые, проходящие через начало координат. Это означает, что помимо вектора a подпространству принадлежит вектор b, не представимый в виде произведения вектора a и скаляра. Тогда наше подпространство содержит все векторы вида $\alpha a + b$. Их концы лежат на прямой, параллельной вектору a и проходящей через конец вектора b (рис. 61).

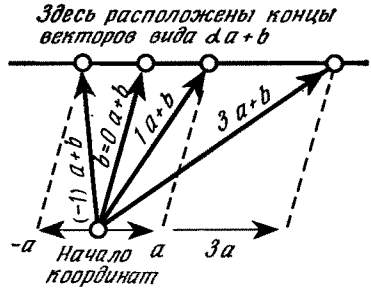


Рис. 61.

Таким образом, все точки прямой, заполненной концами векторов $\alpha a + b$, принадлежат нашему подпространству. Следовательно, этому подпространству принадлежат и все точки прямых, проведенных через концы векторов $\alpha a + b$ и начало координат. Выбрав подходящий скаляр α, мы сможем «дотянуться» вектором до любой точки плоскости и провести через нее прямую, проходящую через начало координат. Так как концы векторов $\alpha a + b$ принадлежат нашему подпространству, то отсюда следует, что ему принадлежат и все точки плоскости. С другой стороны, ясно, что векторы, лежащие в одной плоскости, образуют подпространство. Итак, вслед за прямыми, проходящими через начало координат, мы получаем в качестве подпространств плоскости, проходящие через начало координат.

Из приведенных выше рассуждений следует, что если две прямые (проходящие через начало координат) принадлежат некоторому подпространству, то вся плоскость, натянутая на эти прямые, принадлежит тому же подпространству. Если рассматриваемое пространство помимо плоскости содержит еще одну точку (то есть вектор c, не представимый в виде линейной комбинации введенных ранее векторов a и b), то, как показывают геометрические соображения, аналогичные приведенным выше, нашему подпространству принадлежат все точки трехмерного пространства (рис. 62). Итак, полный перечень подпространств трехмерного пространства включает в себя:

1) начало координат;

2) прямые, проходящие через начало координат;

3) плоскости, проходящие через начало координат;

4) все пространство.

3. Четверки чисел вида $(a, b, 0, 0)$ образуют подпространство в векторном пространстве четверок вещественных чисел.

Достаточно доказать, что линейная комбинация четверок вида $(a, b, 0, 0)$ имеет такой же вид. Имеем

$$c(a, b, 0, 0) + d(x, y, 0, 0) =$$
$$= (ca + dx, cb + dy, 0, 0).$$

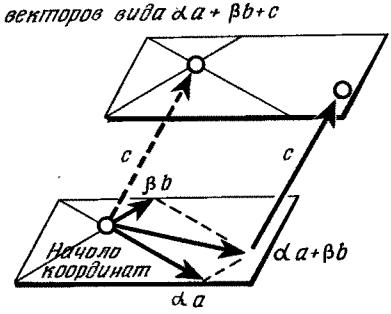


Рис. 62.

4. Четверки чисел (a, b, c, d), для которых $a + b + c + d = 0$, образуют подпространство векторного пространства всех четверок.

Образуем опять линейную комбинацию. Если $a + b + c + d = 0$ и $x + y + u + v = 0$, то $p(a, b, c, d) + q(x, y, u, v) = (pa + qx, pb + qy, pc + qu, pd + qv)$ и для последней четверки выполняется соотношение $pa + qx + pb + qy + pc + du + pd + qv = p(a + b + c + d) + q(x + y + u + v) = 0 + 0 = 0$, что и доказывает наше утверждение.

5. Числовые последовательности, у которых все члены, начиная с некоторого, равны нулю, образуют подпространство в векторном пространстве вещественных числовых последовательностей.

Ясно, что в сумме двух таких последовательностей, начиная с некоторого места, все члены также равны нулю; таким местом будет место, с которого члены обеих последовательностей равны нулю. Ясно также, что, если такую последовательность умножить на скаляр, то в произведении все члены заведомо равны нулю, начиная с того же места, что и в исходной последовательности. (Если последовательность умножить на 0, то нули в произведении могут начаться с «более близкого» места, чем в исходной последовательности.)

Относительно связи между подпространствами и линейными комбинациями мы уже установили, что линейные комбинации заданных векторов всегда образуют подпространство векторного пространства. «Полное обращение» этого утверждения неверно. Тем не менее, как нетрудно понять, всякое подпространство обладает следующим свойством: вместе с любыми принадлежащими ему векторами оно содержит и все их линейные комбинации. Действительно, если какие-то векторы принадлежат подпространству, то тому же подпространству должны принадлежать (по самому определению подпространства) и векторы, отличающиеся от них скалярными множителями, и их суммы.

ЗАДАЧИ

1. Доказать, что четверки чисел (x, y, u, v), для которых выполняются соотношения $2x - 3y + 5u + v = 0$ и $-3x + 2y + v = 0$, образуют подпространство векторного пространства всех четверок чисел.

2. Доказать, что так называемые ограниченные последовательности образуют подпространство векторного пространства бесконечных последовательностей. (Последовательность называется ограниченной, если ее члены по абсолютной величине меньше некоторого числа, зависящего лишь от выбора последовательности.)

3. Доказать, что последовательности, у которых сумма квадратов их членов ограничена числом, зависящим лишь от выбора последовательности (независимо от того, сколько членов последовательности входит в сумму), образуют подпространство векторного пространства всех ограниченных последовательностей.

4. Доказать, что многочлены от k переменных с вещественными коэффициентами образуют подпространство векторного пространства многочленов от n переменных с вещественными коэффициентами при $k \leqslant n$.

5. Доказать, что многочлены от n переменных степени не выше 1 образуют подпространство векторного пространства многочленов от n переменных с вещественными коэффициентами.

6. Доказать, что в векторном пространстве многочленов от n переменных степени не выше 1 с вещественными коэффициентами многочлены, имеющие своими корнями заданные наборы из n чисел, образуют подпространство.

2.2. Подпространство, порожденное векторами, линейная зависимость, размерность

Как известно, общие элементы подгрупп одной группы образуют отдельную подгруппу. Аналогичное утверждение справедливо и относительно подпространств.

Рассмотрим подпространства N_1, N_2, ... векторного пространства M. Обозначим через $\bigcap(N_i)$ множество их общих элементов (если число подпространств конечно, например равно 2, то множество их элементов можно обозначить $N_1 \bigcap N_2$ или аналогичным выражением, содержащим соответствующее число членов). Пусть u и v — элементы множества $N = \bigcap(N_i)$. Тогда оба элемента принадлежат каждому из подпространств N_i, и поэтому любая линейная комбинация $\alpha u + \beta v$ также принадлежит каждому из подпространств N_i, а значит, и множеству N. Нулевой вектор также принадлежит множеству N, поскольку его содержит каждое из подпространств N_i. Следовательно, необходимо лишь доказать, что множество N вместе с любым числом векторов содержит и их линейные комбинации. Впрочем, можно сослаться на то, что доказательство этого утверждения для произвольного числа векторов проводится так же, как и для двух векторов.

Небезынтересно отметить, что по существу наше утверждение уже доказано. Действительно, если какое-то подмножество векторного пространства содержит нулевой вектор (и, следовательно, не пусто) и вместе с любыми двумя векторами u и v ему принадлежит произвольная линейная комбинация $\alpha u + \beta v$, то это подмножество является подпространством. Действительно, полагая $\alpha = \beta = 1$ и $\beta = 0$, мы убеждаемся, что наше подмножество содержит векторы $u + v$ и αu. По определению это и означает, что перед нами подпространство.

Используя доказанное свойство подпространств, рассмотрим общую часть подпространств, содержащих каждый из заранее заданных векторов. (Согласно доказанному общая часть представляет собой подпространство, содержащее все заданные векторы.)

Общая часть подпространств, каждое из которых содержит все заранее заданные векторы, называется подпространством, порожденным заданными векторами.

Подпространство, порожденное векторами u_1, u_2, ..., u_n, ..., обозначим

$$\{u_1, u_2, \ldots, u_n, \ldots\}.$$

Ясно, что подпространство, порожденное векторами u_1, u_2, ..., u_n, ..., содержит все линейные комбинации этих векторов. Но, с другой стороны, линейные комбинации этих векторов образуют подпространство (и в том случае, если векторов u_1, u_2, ..., u_n, ... бесконечно много, поскольку в каждую линейную комбинацию входит лишь конечное число векторов, а как построить линейную комбинацию даже очень большого, но конечного числа векторов известно).

Подпространство, порожденное векторами u_1, u_2, ..., u_n, ..., состоит из линейных комбинаций этих векторов. Если оно совпадает со всем векторным пространством, то множество векторов u_1, u_2, ..., u_n, ... называется *системой образующих*.

Например, в трехмерном пространстве система образующих состоит из любых трех векторов, не лежащих в одной плоскости, в двумерном пространстве (на плоскости) — из любых двух непараллельных векторов.

Заметим, что, *присоединив к системе образующих новый вектор (или новые векторы), мы опять получим систему образующих*, поскольку и до расширения исходной системы образующих она не принадлежала ни одному истинному подпространству.

Элементами подпространства, порожденного заданными векторами, как мы убедились, являются векторы, представимые в виде линейных комбинаций заданных векторов. Поскольку элементы подпространства линейно выражаются через заданные векторы, то говорят, что они *линейно зависят* от заданных векторов.

Вектор v называется линейно зависимым от векторов u_1, u_2, ..., u_n, если его можно представить в виде линейной комбинации векторов u_1, u_2, ...

..., u_n. Вектор v называется линейно независимым от векторов $u_1, u_2, \ldots$ ..., u_n, если ни одна линейная комбинация этих векторов не совпадает с вектором v.

Поскольку линейные комбинации заданных векторов являются элементами порожденного этими векторами подпространства, то линейную зависимость можно выразить следующим образом:

вектор v линейно зависит от векторов $u_1, u_2, \ldots, u_n$, если $v \in \{u_1, u_2, \ldots, u_n\}$,

вектор v не зависит линейно от векторов $u_1, u_2, \ldots, u_n$, если $v \notin \{u_1, u_2, \ldots, u_n\}$.

Рассмотрим несколько элементарных свойств линейной зависимости.

а) Нулевой вектор линейно зависит от любого множества векторов.

Это утверждение просто означает, что нулевой вектор принадлежит любому подпространству векториого пространства.

б) Всякий вектор линейно зависит от любого содержащего его множества векторов.

Это утверждение очевидно. Оно означает, что подпространство, порожденное заданными векторами, содержит каждый из них.

в) Если вектор w линейно зависит от векторов $v_1, v_2, \ldots, v_k$, а каждый из этих векторов линейно зависит от векторов $u_1, u_2, \ldots, u_n$, то вектор w линейно зависит от векторов $u_1, u_2, \ldots, u_n$.

В правильности этого утверждения можно убедиться без особого труда. Если w — элемент подпространства, порожденного векторами $v_1, v_2, \ldots, v_k$, то w принадлежит любому подпространству, содержащему каждый из векторов $v_1, v_2, \ldots, v_k$. Но по предположению $\{u_1, u_2, \ldots, u_n\}$ — такое подпространство. Следовательно, вектор w линейно зависит от векторов $u_1, u_2, \ldots, u_n$, что и требовалось доказать.

В связи с линейной зависимостью возникает весьма важный вопрос об «экономии». Предположим, что в некотором векторном пространстве существует система образующих, состоящая из трех элементов (таково, например, трехмерное пространство). Но представим себе, что из-за какой-то «оплошности» нам удалось построить только систему образующих, содержащую помимо трех исходных векторов еще два дополнительных. (Известно, что, если к системе образующих присоединить новые векторы, то расширенный набор векторов также будет системой образующих.) Это нежелательно по многим причинам, хотя бы потому, что расширенная система образующих содержит лишние элементы. Два новых вектора можно исключить, поскольку они линейно зависят от трех остальных образующих. Действительно, справедливы следующие два утверждения:

1) каждый из пяти построенных векторов линейно зависит от трех исходных векторов (два вектора — по предположению, а три исходных вектора — по свойству (б) линейной зависимости);

2) все векторы линейно зависят от пяти построенных векторов (по предположению эти пять векторов составляют систему образующих векторного пространства).

Если утверждения (1) и (2) записать подряд (каждый из пяти построенных векторов линейно зависит от трех исходных векторов; все векторы линейно зависят от пяти построенных векторов), то из этих посылок в силу свойства (в) линейной зависимости следует, что «все векторы линейно зависят от трех исходных векторов», то есть три исходных вектора служат системой образующих векторного пространства.

В приведенном выше рассуждении нигде не использовалось то, что «три исходных вектора» — это «те самые» заданные векторы: выбрав любую другую тройку векторов (но непременно из пяти векторов расширенной системы образующих!), мы пришли бы к тому же заключению.

Окончательный результат наших рассуждений можно сформулировать следующим образом: если в системе образующих один из векторов линейно зависит от остальных, то, вычеркнув его, мы снова получим сис-

тему образующих. Следовательно, если некоторую систему образующих требуется по возможности «сократить», то необходимо выяснить, не найдется ли среди ее элементов таких, которые линейно зависели бы от остальных.

Аналогичный вопрос возникает не только для систем образующих, но и для любой системы векторов, порождающих подпространство (для подпространства, рассматриваемого как «самостоятельное» векторное пространство, порождающую его систему векторов допустимо считать системой образующих). «Хорошей» считается такая система векторов, которая не содержит ни одного вектора, линейно зависимого от остальных элементов системы. Два типа систем векторов — «хорошие» и «плохие» — получили особые названия.

Если в системе векторов $u_1, u_2, \ldots, u_n$ существует вектор, линейно зависимый от остальных элементов системы, то такая система векторов называется *линейно зависимой* (или, кратко, зависимой). Если же система не содержит линейно зависимых векторов, то она называется *линейно независимой*.

Если система векторов линейно зависима, то, вычеркнув из нее те векторы, которые линейно зависят от остальных, мы получим систему векторов, порождающую то же подпространство, что и исходная система. При этом новая система векторов может оказаться как линейно зависимой, так и линейно независимой. Это означает, что, вычеркнув из линейно зависимой системы принадлежащий ей вектор, мы можем получить как линейно зависимую, так и линейно независимую систему. Если же система линейно независима, то, вычеркнув из нее любой вектор, мы снова получим линейно независимую систему. Действительно, если после вычеркивания вектора какой-нибудь из векторов «укороченной» системы линейно зависел от остальных векторов, то та же линейная зависимость связывала бы векторы и в исходной системе, что невозможно, так как исходная система линейно независима.

(Интересно отметить, что в случае линейно независимых систем мы сталкиваемся с ситуацией, обратной той, с которой встретились при рассмотрении системы образующих: там присоединение нового вектора не изменяло характера системы.)

Установить описанным выше способом, является ли данная система векторов линейно зависимой или линейно независимой, было бы делом весьма сложным и трудоемким. Было бы чрезвычайно неудобно, если бы мы могли утверждать, что ни один вектор системы не зависит линейно от других ее векторов, лишь перебрав все векторы системы. Именно поэтому возникла мысль найти признак линейной независимости, позволяющий отвечать на вопрос о том, зависит ли данный вектор линейно от остальных векторов системы или нет, «сразу», не рассматривая каждый элемент системы в отдельности.

Система векторов линейно независима в том и только в том случае, если в ней нулевой вектор представим лишь в виде тривиальной линейной комбинации.

Сформулируем признак линейной независимости системы векторов более подробно.

Предположим, что заданы векторы $u_1, u_2, \ldots, u_n$. Если найдутся такие скаляры $\alpha_1, \alpha_2, \ldots, \alpha_n$, из которых по крайней мере один отличен от нуля, что

$$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n = 0,$$

то система векторов $u_1, u_2, \ldots, u_n$ линейно зависима. Если же линейная комбинация $\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_n u_n$ совпадает с нулевым вектором лишь в том случае, если все скаляры $\alpha_1, \alpha_2, \ldots, \alpha_n$ равны нулю, то система векторов $u_1, u_2, \ldots, u_n$ линейно независима.

Доказать это утверждение можно следующим образом.

Если векторы $u_1, u_2, \ldots, u_n$ линейно зависимы, то по определению среди них су-

ществует такой вектор, который линейно зависит от остальных. Пусть это будет, например, вектор u_1. Его можно представить в виде линейной комбинации

$$u_1 = \beta_2 u_2 + \cdots + \beta_n u_n,$$

или (если вектор, противоположный вектору u_1, записать в виде скалярного кратного вектора u_1)

$$(-1)\, u_1 + \beta_2 u_2 + \cdots + \beta_n u_n = 0.$$

Итак, нулевой вектор можно представить в виде линейной комбинации векторов $u_1, u_2, \ldots, u_n$. Эта линейная комбинация заведомо нетривиальна, так как первый скаляр -1 отличен от нуля.

Наоборот, если существует нетривиальная линейная комбинация векторов $u_1, u_2, \ldots, u_n$, совпадающая с нулевым вектором $\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_n u_n = 0$, то по крайней мере один из скаляров $\alpha_1, \alpha_2, \ldots, \alpha_n$ отличен от нуля. Не ограничивая общности, можно предположить, что, например, $\alpha_1 \neq 0$. Перевеся член $\alpha_1 u_1$ в другую часть равенства и умножив на α^{-1} (α^{-1} существует, так как $\alpha_1 \neq 0$), получим

$$u_1 = \left(-\frac{\alpha_2}{\alpha_1}\right) u_2 + \cdots + \left(-\frac{\alpha_n}{\alpha_1}\right) u_n.$$

Это и означает, что вектор u_1 линейно зависит от остальных заданных векторов.

В трехмерном пространстве любые три вектора, не лежащие в одной плоскости, линейно независимы, но геометрия относительного расположения векторов носит довольно сложный характер. С точки зрения геометрии гораздо более простым является случай, когда система состоит из трех попарно ортогональных векторов единичной длины. Вполне возможно, что при решении каких-то математических задач предпочтение следует отдавать не каким-нибудь «более удобным» в том или ином смысле системам векторов. Разумеется, с алгебраической точки зрения вопрос о том, какая из линейно независимых систем лучше, лишен смысла. (Как мы убедимся в дальнейшем, с алгебраической точки зрения все линейно независимые системы «равноправны»). Таким образом, проблема «усовершенствования» линейно независимой системы векторов в алгебре не возникает, но вопрос о том, каким образом одну систему линейно независимых векторов можно преобразовать в другую, носит вполне алгебраический характер. Следовательно, каждое «усовершенствование», вносимое в заданную линейно независимую систему векторов, надлежит оценивать особо и лишь затем решать, удалось ли «улучшить» исходную систему.

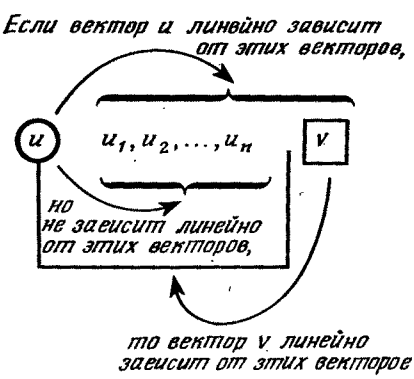


Рис. 63.

В данный момент нас интересует вопрос о том, каким образом одну линейно независимую систему векторов можно преобразовать в другую. В рассмотренном выше случае трехмерного пространства обе системы — исходная (любые три вектора, не лежащие в одной плоскости) и конечная (три попарно ортогональных вектора единичной длины) — содержали одинаковое число векторов. К такому преобразованию мы придем, заменяя векторы исходной системы по одному до тех пор, пока шаг за шагом не заменим все «старые» векторы на «новые». Поэтому прежде всего необходимо выяснить, в каких случаях один вектор допустимо заменять другим. Ответ на этот вопрос гласит:

если вектор u линейно зависит от векторов $u_1, u_2, \ldots, u_n, v$, но не зависит линейно от векторов $u_1, u_2, \ldots, u_n$, то вектор v линейно зависит от векторов $u_1, u_2, \ldots, u_n, u$ (рис. 63).

Доказательство этого утверждения весьма просто. Если вектор u линейно зависит от векторов $u_1, u_2, \ldots, u_n, v$, то его можно представить в виде

$$u = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n + \beta v.$$

В этой линейной комбинации скаляр β не может быть отличен от нуля, поскольку в противном случае вектор u зависел бы линейно от векторов $u_1, u_2, \ldots, u_n$. Следовательно, существует скаляр β^{-1}. Умножая на него и перенося векторы $\alpha_1 u_1$, $\alpha_2 u_2, \ldots$, $\alpha_n u_n$ в другую часть равенства, получаем

$$v = \left(\frac{1}{\beta}\right) u + \left(-\frac{\alpha_1}{\beta}\right) u_1 + \\ + \left(-\frac{\alpha_2}{\beta}\right) u_2 + \cdots + \left(-\frac{\alpha_n}{\beta}\right) u_n.$$

что и требовалось доказать.

При рассмотрении систем образующих было показано, что, присоединив к системе новые векторы, мы снова придем к системе образующих. Изучая линейно независимые системы «опытным путем», мы обнаружили, что при исключении из системы отдельных векторов возникает новая линейно независимая система. Возникает «подозрение», что линейно независимые системы «у́же», а системы образующих — «шире».

В обоснованности подобных сомнений можно убедиться, если подойти к задаче с «противоположной стороны». Действительно, присоединив к системе образующих новый вектор, линейно зависимый от остальных векторов системы, мы не сможем получить линейно независимую систему векторов. Вычеркнув из линейно независимой системы векторов любой вектор (линейно независимый от остальных векторов), мы не сможем получить систему образующих.

В любом векторном пространстве ни одна линейно независимая система векторов не может содержать больше элементов, чем любая система образующих.

В определенном смысле аналогичное утверждение остается в силе и в том случае, если линейно независимая система содержит бесконечно много элементов. Нас же теперь интересуют только линейно независимые системы, состоящие из конечного числа элементов. Если система образующих содержит бесконечно много элементов, то, разумеется, она заведомо «шире» любой конечной линейно независимой системы. Следовательно, необходимо рассмотреть лишь такой случай, когда и линейно независимая система векторов, и система образующих состоят из конечного числа элементов.

Пусть $a_1, a_2, \ldots, a_n$ — система образующих векторного пространства, а $b_1, b_2, \ldots, b_k$ — система линейно независимых векторов в том же векторном пространстве. Требуется доказать, что $k \leqslant n$. Для этого достаточно убедиться в том, что в данной системе образующих найдется k векторов, образующих линейно независимую систему. (Отсюда, в частности, будет следовать, что данная система образующих заведомо содержит k векторов.)

В процессе доказательства мы покажем, что из линейно независимой системы можно вычеркнуть вектор (если только все векторы линейно независимой системы не принадлежат системе образующих) и заменить его вектором из системы образующих так, чтобы получившаяся система снова была линейно независимой. Для простоты, не ограничивая общности, предположим, что, если в линейно независимой системе имеются векторы, не принадлежащие системе образующих, то они «идут первыми». Будем считать, что элементы системы образующих расположены в «удобном» (хотя и заранее неизвестном) порядке, при котором элемент, пригодный для замены очередного вычеркнутого вектора, всегда идет «следующим». Итак, пусть $b_1, b_2, \ldots, b_k$ — векторы линейно независимой системы, а $a_1, a_2, \ldots, a_n$ — векторы системы образующих. Вычеркнем вектор b_1 и заменим его вектором a_1. Выполнив это преобразование, мы получим линейно независимую систему, а система образующих при этом не изменится. Вычеркнем затем вектор b_2 и заменим его вектором a_2. Вновь полученная система векторов также линейно независима, а систе-

ма образующих и на этот раз остается без изменений. Продолжая эти преобразования, мы после конечного числа шагов «исчерпаем» векторы b и получим линейно независимую систему, состоящую из k векторов системы образующих.

Линейно независимая система — Система образующих

$b_1,\ b_2,\ \ldots,\ b_k;\qquad a_1,\ a_2,\ \ldots,\ a_n$

Вычеркнув этот вектор и заменив его этим вектором, мы получим новую линейно независимую систему, а система образующих останется прежней:

Система образующих

$b_2,\ \ldots,\ b_k;\quad a_1,\ a_2,\ \ldots,\ a_n$

Линейно независимая система

Повторив преобразование еще раз, мы придем к следующим системам:

Система образующих

$\ldots,\ b_k,\quad a_1,\ a_2,\ \ldots,\ a_n$

Линейно независимая система

Докажем, что сделанные «шаги» ведут к доказательству нашего утверждения. Вычеркнем из линейно независимой системы какой-нибудь вектор, например b_1. Прежде всего докажем, что в системе образующих найдется вектор, который не зависит линейно от системы векторов $b_2,\ldots,b_k$.

Если такого вектора в системе образующих не было, то

все векторы a_i зависели бы линейно от векторов $b_2,\ b_3,\ldots,b_k$. (1)

Но поскольку $a_1,\ a_2,\ldots,a_n$ — система образующих, то

вектор b_1 линейно зависит от векторов $a_1,\ a_2,\ldots,a_n$. (2)

Из этих двух утверждений и свойства (в) линейной зависимости следовало бы, что вектор b_1 линейно зависит от векторов $b_2,\ldots,b_k$. Но тогда система векторов $b_1,\ b_2,\ldots,b_k$ вопреки предположению была бы линейно независимой.

Следовательно, один из элементов системы образующих (если таких элементов несколько, то любой из них), например a_1, не зависит линейно от векторов $b_2,\ldots,b_k$.

Это означает, что векторы $b_2,\ldots,b_k,\ a_1$ образуют линейно независимую систему. Действительно, если бы система векторов $b_2,\ldots,b_k,\ a_1$ была бы линейно зависимой, то некоторая нетривиальная линейная комбинация векторов $b_2,\ldots,b_k,\ a_1$ была бы равна нулевому вектору. В этой линейной комбинации элемент, кратный вектору a_1, содержал бы скаляр, отличный от нуля, независимо от того, с какими скалярами входят в линейную комбинацию члены, кратные векторам $b_2,\ldots,b_k$. Но это невозможно, так как вектор a_1 линейно независим от векторов $b_2,\ldots,b_k$.

В векторных пространствах особо важную роль играют такие системы векторов, которые «не слишком малы и не слишком велики», то есть системы образующих, обладающие еще одним, дополнительным свойством: линейной независимостью. Такие системы образующих называются базисами.

Линейно независимая система образующих векторного пространства называется *базисом*.

Разумеется, нельзя утверждать заранее, что во всяком векторном пространстве существует базис, но можно доказать соответствующую теорему. В общем случае для выполнения этой задачи нам понадобилось бы большое число математических понятий, и поэтому мы проведем доказательство лишь для частного случая, когда в векторном пространстве существует конечная система образующих.

Может случиться, что, вычеркнув из системы образующих какой-нибудь элемент, мы вновь получим систему образующих. Если это так, то будем вычеркивать из исходной системы образующих элементы до тех пор, пока это возможно. Поскольку на каждом шаге мы получаем систему образующих, то и оставшиеся элементы также составляют систему образующих. Нетрудно убедиться в том, что эта система линейно независима. Действительно, если бы, например, вектор u_1 линейно зависел от остальных векторов, то по свойству (в) линейной зависимости все элементы векторного пространства линейно зависели бы от векторов $u_2,\ldots,u_n$, то есть векторы $u_2,\ldots,u_n$ были бы системой образующих векторного пространства и, следовательно вычеркивание векторов нельзя было бы завершить по достижении системы образующих $u_1,\ u_2,\ldots,u_n$.

Базис векторного пространства «выделен» среди линейно независимых систем и систем образующих в следующем смысле.

Если в векторном пространстве

существует базис, состоящий из n элементов, то:

1) любая линейно независимая система в этом векторном пространстве содержит не более n элементов;

2) любая система образующих в этом векторном пространстве содержит не менее n элементов;

3) любой другой базис в этом векторном пространстве содержит равно n элементов.

Базис векторного пространства можно рассматривать как систему образующих, содержащую n элементов. Так как число элементов в линейно яезависимой системе векторов не превышает числа элементов в системе образующих, то утверждение (1) можно считать доказанным. Доказательство утверждения (2) мы получим, если будем рассматривать базис как линейно независимую систему векторов. Наконец, утверждение (3) следует из того, что базис как линейно независимая система образующих по утверждению (1) содержит не более, а по утверждению (2) не менее n элементов.

Следующая теорема позволяет понять, почему в векторных пространствах базисы играют столь важную роль:

в произвольном векторном пространстве всякий вектор можно однозначно представить в виде линейной комбинации векторов любого базиса; наоборот, если всякий вектор можно однозначно представить в виде линейной комбинации векторов некоторой системы, то эта система образует базис векторного пространства.

Заранее известно, что система векторов является системой образующих векторного пространства лишь в том случае, если всякий вектор можно представить в виде линейной комбинации векторов системы. Следовательно, достаточно доказать, что система векторов линейно независима лишь в том случае, если всякий вектор, представимый в виде линейной комбинации ее векторов, можно линейно выразить через эти векторы только одним способом.

Прежде чем приступать к доказательству, вспомним одно из приводившихся выше определений линейной независимости: система векторов линейно независима в том и только в том случае, если нулевой вектор однозначно представим в виде линейной комбинации векторов системы (то есть если только тривиальная линейная комбинация равна нулевому вектору). Следовательно, утверждение, которое нам предстоит доказать, можно сформулировать так: *один* заданный вектор допускает однозначное представление в виде линейной комбинации векторов системы в том и только в том случае, если *все* векторы однозначно представимы в виде линейных комбинаций векторов этой системы.

Одна часть последнего утверждения очевидна: если все векторы однозначно представимы в виде линейных комбинаций заданных векторов, то и нулевой вектор обладает тем же свойством. Поскольку тривиальная линейная комбинация порождает нулевой вектор, то никакая другая линейная комбинация не может быть нулевым вектором. Это и означает, что заданная система векторов линейно независима.

Предположим теперь, что вектор v можно представить в виде линейной комбинации линейно независимых векторов $u_1, u_2, \ldots, u_n$ двумя различными способами:

$$v = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n =$$
$$= \beta_1 u_1 + \beta_2 u_2 + \cdots + \beta_n u_n.$$

Отсюда следует, что вектор $0 = u - v$ допускает представление в виде линейной комбинации

$$0 = (\alpha_1 - \beta_1) u_1 + (\alpha_2 - \beta_2) u_2 + \cdots$$
$$\ldots (\alpha_n - \beta_n) u_n.$$

Поскольку векторы $u_1, u_2, \ldots, u_n$ линейно независимы, эта линейная комбинация может быть только тривиальной, то есть все «коэффициенты» равны нулю. Это означает, что $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2, \ldots, \alpha_n = \beta_n$, то есть представление любого вектора в виде линейной комбинации заданных векторов однозначно.

Приведем теперь несколько примеров базисов.

ПРИМЕРЫ

1. Векторы на плоскости и в трехмерном пространстве. В множестве векторов на плоскости базис образуют

любые два непараллельных вектора. Поскольку векторы базиса не параллельны, то ни один из них не является скалярным кратным другого и поэтому они линейно независимы. Так как всякий вектор на плоскости можно представить в виде линейной комбинации этих векторов, то их можно рассматривать как систему образующих. В трехмерном пространстве базисом служат любые три вектора, не лежащие в одной плоскости.

2. Векторное пространство четверок вещественных чисел. Базис образуют четверки (1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0) и (0, 0, 0, 1). Их линейная комбинация получается по «рецепту»:

$$a(1, 0, 0, 0) + b(0, 1, 0, 0) + c(0, 0, 1, 0) + d(0, 0, 0, 1) = (a, b, c, d).$$

Поскольку в правой части равенства может стоять любая четверка вещественных чисел, то заданный набор четверок можно рассматривать как систему образующих. Вектор, стоящий в правой части равенства, может быть нулевым лишь в том случае, если $a = b = c = d = 0$, а это и означает, что векторы (1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0) и (0, 0, 0,1) линейно независимы.

3. Векторное пространство комплексных чисел над телом вещественных чисел. Базис образуют комплексные числа 1, i, так как любой вектор допускает однозначное представление в виде $a \cdot 1 + b \cdot i = a + bi$.

4. Многочлены с вещественными коэффициентами. Базис образуют многочлены $1, x, x^2, \ldots, x^n, \ldots$. В этом базисе бесконечно много элементов, но, как нетрудно видеть, всякий многочлен можно однозначно представить в виде линейной комбинации элементов базиса.

5. Вещественные числа над телом рациональных чисел. Можно показать, что базис существует и в этом случае, но как выписать его в явном виде, мы не знаем.

В первом примере было показано, что на плоскости (как принято называть двумерное векторное пространство) базис состоит из двух, а в трехмерном пространстве — из трех элементов. Аналогичным образом можно определить и n-мерное векторное пространство.

Векторное пространство называется n-мерным, если в нем существует базис, содержащий n элементов.

Поскольку число элементов базиса однозначно определено, то размерность векторного пространства также однозначно определена. Однако не следует забывать и о том, от чего зависит размерность: над каким телом рассматривается векторное пространство. Например, тело комплексных чисел над телом вещественных чисел образует двумерное векторное пространство, а над телом комплексных чисел (то есть над самим собой) — одномерное векторное пространство.

Векторные пространства, в которых ни при каком целом n не существует базиса, содержащего n элементов, называются *бесконечномерными*.

Следуя общему определению, мы должны были бы назвать нульмерным векторное пространство, базис которого содержит «нуль элементов». Разумеется, такое «определение» было бы бессмысленным. По аналогии (и многим другим соображениям) векторное пространство, содержащее только нулевой вектор, называется *нульмерным*.

Заметим также, что векторное пространство одномерно в том и только в том случае, если оно состоит из скалярных кратных одного (отличного от нулевого) вектора.

ЗАДАЧИ

1. Выяснить, какие из приводимых ниже утверждений совпада-

ют и какие различны по содержанию:

а) в векторном пространстве не существует линейно независимой системы из k элементов;

б) в векторном пространстве существует линейно независимая система из k элементов;

в) в векторном пространстве существует линейно независимая система из k элементов, но не существует линейно независимой системы из $k + 1$ элементов;

г) в векторном пространстве существует линейно независимая система из k элементов, но не существует линейно независимой системы более чем из k элементов;

д) в векторном пространстве не существует системы образующих из k элементов;

е) в векторном пространстве существует система образующих из k элементов;

ж) в векторном пространстве существует система образующих из k элементов, но не существует системы образующих из $k - 1$ элементов;

з) в векторном пространстве существует система образующих из k элементов, но не существует системы образующих менее чем из k элементов;

и) размерность векторного пространства не меньше k;

к) размерность векторного пространства равна k;

л) размерность векторного пространства не больше k.

2. Доказать, что в векторном пространстве все системы образующих содержат некоторый базис.

3. Доказать, что в n-мерном векторном пространстве всякую линейно независимую систему векторов можно дополнить до базиса.

4. Доказать, что, если все элементы линейно независимой системы векторов принадлежат некоторой системе образующих, то в этой системе образующих можно выделить подмножество, которое содержит рассматриваемую линейно независимую систему векторов и является базисом.

2.3. Изоморфизм и прямая сумма векторных пространств

Изоморфизм — наиболее важное понятие в теории векторных пространств, как, впрочем, и в теории групп и полугрупп. С алгебраической точки зрения изоморфные векторные пространства невозможно отличить, поскольку изоморфизм векторных пространств означает, что операции действуют в них «одинаково». С другой стороны, нам вовсе не требуется различать изоморфные векторные пространства потому, что результаты получаются гораздо проще, если отвлечься от конкретных особенностей операций и элементов.

О том, что векторные пространства изоморфны, можно говорить лишь в случае, если они заданы над одним и тем же телом. (Строго говоря, достаточно потребовать, чтобы тела, над которыми заданы векторные пространства, были изоморфными. Но поскольку с алгебраической точки зрения изоморфные тела ничем не отличаются, то для простоты мы сразу же будем считать, что они совпадают.) Под изоморфизмом векторных пространств понимают взаимно-однозначное соответствие между ними, сохраняющее операцию.

Векторные пространства M_1 и M_2 над телом Γ называются изоморфными ($M_1 \cong M_2$), если существует такое взаимно-однозначное соответствие

$$\varphi : M_1 \to M_2,$$

что при любом скаляре α из Γ и любых векторах u и v из M_1

$$\varphi(\alpha u) = \alpha \cdot \varphi(u)$$

и

$$\varphi(u + v) = \varphi(u) + \varphi(v).$$

Перечисление всех неизоморфных групп (или скорее полугрупп) — задача весьма трудная, но в случае векторных пространств она имеет простой ответ:

два векторных пространства конечной размерности изоморфны в том

и только в том случае, если их размерности совпадают. (Если два векторных пространства изоморфны, то достаточно предположить, что одно из них имеет конечную размерность, отсюда уже следует, что и другое векторное пространство также конечномерно.)

По существу изоморфизм означает, что векторные пространства над заданным телом характеризуются одним числом: размерностью пространства.

Предположим, что $\varphi\colon M_1 \to M_2$ — изоморфизм. Так как число элементов в базисе совпадает с размерностью векторного пространства, то достаточно показать, что изоморфизм φ переводит базис векторного пространства M_1 в базис векторного пространства M_2. Докажем это утверждение, разбив его на две части: сначала докажем, что φ переводит линейно независимые векторы в линейно независимые, а затем, что φ отображает систему образующих в систему образующих.

Пусть $u_1, u_2,\ldots,u_n$ — система линейно независимых векторов в M_1. Предположим, что при соответствующим образом подобранных скалярах выполняется соотношение $\alpha_1\varphi(u_1) + \alpha_2\varphi(u_2) + \ldots + \alpha\varphi(u_n) = 0$. Поскольку изоморфизм φ сохраняет операции, то из этого соотношения следует, что $\varphi(\alpha_1u_1 + \alpha_2u_2 + \ldots + \alpha_nu_n) = 0$. Таким образом, изоморфизм векторных пространств означает, что векторные пространства изоморфны как коммутативные группы. Но тогда образом нулевого элемента из M_1 при изоморфизме φ может быть только нулевой элемент из M_2, то есть $\alpha_1u_1 + \alpha_2u_2 + \ldots + \alpha_nu_n = 0$. Так как векторы $u_1, u_2,\ldots, u_n$ линейно независимы, то последнее соотношение может выполняться только в том случае, если каждый из скаляров равен нулю, а это в свою очередь означает, что векторы $\varphi(u_1), \varphi(u_2),\ldots,\varphi(u_n)$ линейно независимы.

Пусть $v_1, v_2,\ldots,v_k$ — система образующих векторного пространства M_1, y — произвольно выбранный вектор из M_2. Поскольку между векторными пространствами M_1 и M_2 изоморфизм φ устанавливает взаимно-однозначное соответствие, то вектор y — образ некоторого вектора x из M_1, иначе говоря, его можно представить в виде $y = \varphi(x)$. Запишем x в виде линейной комбинации образующих: $x = \beta_1v_1 + \beta_2v_2 + \ldots + \beta_kv_k$. В силу сохранения операций этому соотношению для векторов из M_1 соответствует соотношение $y = \varphi(x) = \beta_1\varphi(v_1) + \beta_2\varphi(v_2) + \ldots + \beta_k\varphi(v_k)$ для векторов из M_2, которое означает, что $\varphi(v_1), \varphi(v_2),\ldots, \varphi(v_k)$ — система образующих в векторном пространстве M_2.

Для доказательства обратного утверждения рассмотрим n-мерные векторные пространства M_1 и M_2. В каждом из этих пространств существует базис из n элементов. Пусть векторы $u_1, u_2,\ldots,u_n$ образуют базис в M_1, а векторы $v_1, v_2,\ldots,v_n$ — базис в M_2. Ясно, что отображение $\varphi\colon M_1 \to M_2$ действует следующим образом:

$$\varphi(\alpha_1u_1 + \alpha_2u_2 + \cdots + \alpha_nu_n) =$$

$$= \alpha_1v_1 + \alpha_2v_2 + \cdots + \alpha_nv_n.$$

1. Прежде всего необходимо убедиться в том, что φ — отображение векторного пространства M_1 на векторное пространство M_2. Поскольку базис в M_1 известен, то каждый вектор из M_1 можно представить в виде линейной комбинации векторов $u_1, u_2,..,u_n$. Следовательно, о каждом векторе из M_1 можно утверждать, что φ отображает его в некоторый вектор из M_2.

2. Если мы возьмем два различных вектора из M_1, то им соответствуют две различные линейные комбинации. Образы этих комбинаций также представляют собой две различные линейные комбинации векторов $v_1, v_2,\ldots,v_n$. Но поскольку базис в M_2 состоит из линейно независимых векторон, то две различные линейные комбинации векторов $v_1, v_2,\ldots,v_n$ порождают различные векторы из M_2. Итак, при отображении φ различные векторы из M_1 переходят в различные векторы из M_2.

3. Поскольку в пространстве M_2 имеется система образующих, то любой вектор из M_2 можно представить в виде линейной комбинации векторов $v_1, v_2,\ldots,v_n$ и, следовательно, рассматривать как образ соответствующей линейной комбинации векторов $u_1, u_2,\ldots,u_n$ из M_1.

4. Сохранение операций следует из того, что в обоих векторных пространствах сложение и умножение на скаляр производится покомпонентно.

Итак, «удачно выбрав» n-мерное векторное пространство, мы могли бы понять «устройство» всех n-мерных векторных пространств. Одним из «благодарных» объектов для изучения n-мерных векторных пространств может служить векторное пространство наборов из n элементов.

Пусть Γ — некоторое тело. Составим из его элементов наборы

$$(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Нетрудно видеть, что такие наборы образуют векторное пространство, если операции сложения и умножения на скаляр производить покомпонентно.

Докажем, что векторное пространство наборов из n элементов тела Γ n-мерно. Для этого необходимо доказать, что базис пространства состоит из n элементов. Проверим, что наборы

$$(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots$$
$$\ldots, (0, 0, \ldots, 1)$$

образуют базис нашего векторного пространства. Действительно, так как

$$\alpha_1(1, 0, \ldots, 0) + \alpha_2(0, 1, \ldots, 0) + \cdots$$
$$\cdots + \alpha_n(0, 0, \ldots, 1) = (\alpha_1, \alpha_2, \ldots, \alpha_n),$$

то каждый вектор однозначно представим в виде линейной комбинации n наборов (1, 0,...,0), (0, 1,...,0),..., (0, 0,...,1). Это и означает, что векторное пространство наборов из n элементов тела Γ n-мерно.

Некоторые подпространства построенного нами n-мерного векторного пространства допускают необычайно простое описание. Рассмотрим, например, векторное пространство пятерок вещественных чисел. Его одномерными подпространствами являются векторы вида (a, 0, 0, 0, 0), (0, a, 0, 0, 0), и т. д., то есть пятерки чисел, у которых все координаты, кроме одной, равны нулю. Двумерные подпространства образуют векторы, у которых две координаты могут принимать любые вещественные значения. К их числу относятся, например, векторы (a, b, 0, 0, 0) и (0, a, 0, 0, b). Каждое из таких подпространств определяет другое подпространство, состоящее из векторов, у которых нули расставлены там, где у векторов исходного подпространства их не было. Так, подпространство векторов (0, a, 0, 0, b) «дополняет» подпространство векторов (c, 0, d, e, 0). Тем самым мы получаем возможность разложить все векторное пространство в сумму двух дополняющих друг друга подпространств (рис. 64).

При рассмотрении групп аналогичное разложение мы называли прямым произведением подгрупп. Аналогичным образом можно интерпретировать это понятие и в данном случае. Правда, применительно к векторным пространствам (по вполне понятным причинам) чаще говорят о прямой сумме подпространств, поскольку групповой операцией в векторных пространствах является сложение. (Заметим, кстати, что в случае коммутативных групп прямое произведение принято называть прямой суммой.)

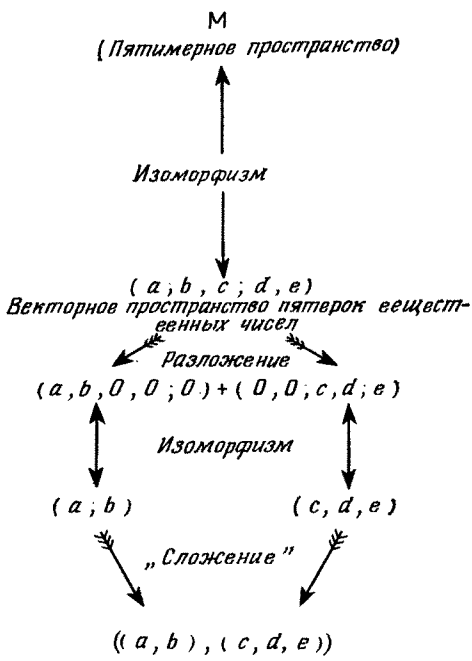


Рис. 64.

Прямой суммой $M_1 + M_2$ векторных пространств M_1 и M_2 над одним и тем же телом Γ называется множество пар (u, v) элементов, на котором операции сложения и умножения на скаляр определены следующим образом:

$$(u_1, v_1) + (u_2, v_2) =$$
$$= (u_1 + u_2, v_1 + v_2)$$

и

$$\alpha(u, v) = (\alpha u, \alpha v),$$

где α — произвольный скаляр из тела Γ, u, u_1 и u_2 — элементы мно-

жества M_1, v, v_1 и v_2 — элементы множества M_2.

Тождества, которым должна удовлетворять операция сложения, можно не проверять: ведь если отвлечься от умножения на скаляры и рассматривать только операцию сложения, то мы получим «прямое произведение» соответствующих векторных пространств как коммутативных групп. Проверим, все ли тождества выполняются для умножения на скаляр:

$$(\alpha+\beta)(u, v) = ((\alpha+\beta)u,\ (\alpha+\beta)v) =$$
$$= (\alpha u + \beta u, \alpha v + \beta v) = (\alpha u, \alpha v) +$$
$$+ (\beta u, \beta v) = \alpha(u, v) + \beta(u, v);$$

$$\alpha[(u_1, v_1) + (u_2, v_2)] =$$
$$= (\alpha u_1 + \alpha u_2, \alpha v_1 + \alpha v_2) =$$
$$= (\alpha u_1, \alpha v_1) + (\alpha u_2, \alpha v_2) =$$
$$= \alpha(u_1, v_1) + \alpha(u_2, v_2);$$

$$(\alpha\beta)(u, v) = ((\alpha\beta)u, (\alpha\beta)v) =$$
$$= (\alpha(\beta u), \alpha(\beta v)) = \alpha(\beta u, \beta v) =$$
$$= \alpha[\beta(u, v)];$$

$$1 \cdot (u, v) = (1 \cdot u, 1 \cdot v) = (u, v).$$

Таким образом, и для умножения на скаляр все тождества выполнены.

Прежде чем привести определение прямой суммы векторных пространств, мы «разложили» заданное векторное пространство на два подпространства и из них построили прямую сумму. Если векторное пространство допускает разложение на два подпространства, то такую операцию можно производить и в общем случае.

Итак, если U и V — подпространства векторного пространства M и

$$1)\ \{U, V\} = M, \quad 2)\ U \cap V = \{0\},$$

то соответствие φ: $(u, v) \to u + v$ изоморфно отображает прямую сумму U + V на векторное пространство M. Изоморфизм φ отображает на подпространство U векторы $(u, 0)$, а на подпространство V — векторы $(0, v)$ и только их.

Однозначность отображения φ следует из представления векторного пространства M в виде прямой суммы подпространств U и V. Если образы элементов (u_1, v_1) и (u_2, v_2) совпадают (то есть если $u_1 + v_1 = u_2 + v_2$), то $u_1 - u_2 = v_2 - v_1$. Элемент, стоящий в левой части последнего равенства, принадлежит подпространству U, элемент, стоящий в правой части равенства, принадлежит подпространству V. По предположению подпространства U и V имеют единственный общий элемент — нулевой вектор. Следовательно, $u_1 = u_2$ и $v_1 = v_2$. Итак, доказано, что образы различных элементов при отображении φ различны.

Образы всех элементов при отображении φ имеют вид $u + v$, где $u \in U$ и $v \in V$. Ясно, что всякий элемент векторного пространства M, представимый в таком виде, имеет прообраз, или, что то же, служит образом некоторого элемеита прямой суммы подпространств U + V. Значит, если каждый элемент векторного пространства M нам удастся представить в виде $u + v$, то тем самым будет доказано, что у всех элементов M существуют прообразы при отображении φ. Более того, достаточно доказать, что элементы векторного пространства M, представимые в виде $u + v$, образуют подпространство, содержащее каждое из подпространств U и V. Действительно, ведь отсюда следовало бы, что каждый элемент векторного пространства M содержится в таком подпространстве, так как M (в силу соотношения $M = \{V, U\}$) — единственное подпространство, которому принадлежит U и V. В том, что элементы векторного пространства M, представимые в виде $u + v$, образуют подпространство, нас убеждают соотношения

$$(u_1 + v_1) + (u_2 + v_2) =$$
$$= (u_1 + u_2) + (v_1 + v_2)$$

и

$$\alpha(u + v) = \alpha u + \alpha v$$

(так как U и V — подпространства, то $u_1 + u_2$ и αu принадлежат U, а $v_1 + v_2$ и αv принадлежат V).

Наконец, сохранение операций следует из соотношений

$$\varphi[(u_1, v_1) + (u_2, v_2)] = \varphi((u_1 + u_2,$$
$$v_1 + v_2)) = (u_1 + u_2) + (v_1 + v_2) =$$
$$= (u_1 + v_1) + (u_2 + v_2) =$$
$$= \varphi((u_1, v_1)) + \varphi((u_2, v_2))$$

и

$$\varphi[\alpha(u, v)] = \varphi((\alpha u, \alpha v)) = \alpha u + \alpha v =$$
$$= \alpha(u + v) = \alpha\varphi((u + v)).$$

В этом случае говорят, что векторное пространство M — прямая сумма подпространств U и V.

Между двумя приведенными выше определениями прямой суммы *по существу* нет различия, хотя с точки

зрения логики они не тождественны. Чисто внешне они отличаются тем, что в одном из них говорится о пространствах, а в другом о подпространствах. Но если по каким-нибудь соображениям желательно особо подчеркнуть различие между двумя определениями прямой суммы и указать, какое из них имеется в виду, то в первом случае говорят о *внешней прямой сумме*, а во втором случае (когда речь идет о подпространствах) — о *внутренней прямой сумме*.

Чтобы наглядно представить себе прямую сумму, рассмотрим трехмерное пространство. Как известно, его подпространства можно изображать в виде геометрических «фигур», проходящих через начало координат. Условия, при которых прямая сумма двух подпространств совпадает со всем пространством, сводятся к следующему:

1) каждое из подпространств дополняет другое до всего пространства;

2) подпространства не имеют других общих элементов, кроме начала координат. Две прямые, проходящие через начало координат, не имеют (если они не совпадают) других общих точек, кроме начала координат, но не дополняют друг друга до трехмерного пространства. Две плоскости (если они не совпадают) дополняют друг друга до всего пространства, но пересекаются по прямой. Плоскость и прямая (не лежащая в плоскости) образуют «благоприятную комбинацию»: они имеют только одну общую точку и дополняют друг друга до всего пространства. Если плоскость фиксирована, то прямую можно выбирать произвольно, лишь бы она не лежала в плоскости. Если фиксирована прямая, то плоскость можно проводить как угодно, лишь бы она не проходила через прямую. И в том и в другом случае прямая сумма плоскости и прямой совпадает со всем пространством. Как показывает этот пример, если одно из слагаемых прямой суммы задано, то второе слагаемое определяется не однозначно. Другие примеры неоднозначного восстановления второго слагаемого прямой суммы по заданному подпространству можно построить, рассматривая пятерки вещественных чисел.

ЗАДАЧИ

1. Доказать что при изоморфизме линейно независимая система векторов переходит в линейно независимую систему векторов, а система образующих — в систему образующих.

2. Доказать, что, если φ — такое сохраняющее операции сложения и умножения на скаляр отображение, которое переводит линейно независимую систему векторов в линейно независимую систему векторов и систему образующих в систему образующих, то φ — изоморфизм.

3. Пусть φ — отображение, сохраняющее операции сложения и умножения на скаляр. Какое из двух входящих в определение изоморфизма условий (образы различных элементов не совпадают; у каждого элемента векторного пространства, на которое отображается исходное пространство, существует прообраз) эквивалентно утверждению о том, что φ переводит линейно независимую систему векторов в линейно независимую систему векторов, и какое — утверждению о том, что

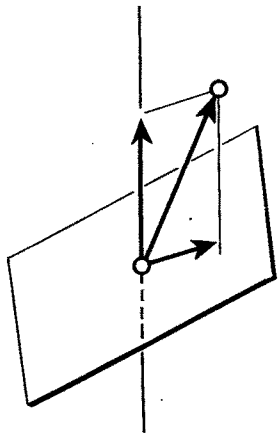


Рис. 65.

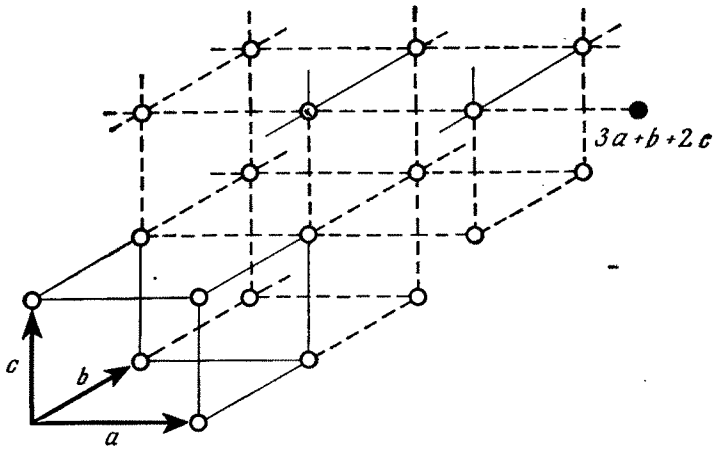


Рис. 66.

φ переводит систему образующих в систему образующих?

4. Доказать, что размерность прямой суммы равна сумме размерностей слагаемых.

5. Привести пример векторного пространства, представимого в виде прямой суммы любых двух из трех заданных подпространств (рис. 65).

2.4. Модули

В векторных пространствах скаляры по предположению образуют (коммутативное) тело. Однако столь богатой «структурой» запас скаляров обладает далеко не всегда. Рассмотрим, например, комплексные числа $a + bi$ с целыми a и b. При умножении такого комплексного числа на целое число получается комплексное число того же вида (с целой вещественной и мнимой частью), чего нельзя с уверенностью сказать в том случае, когда умножение производится на дробное число. Другим примером «почти векторного пространства» (коммутативной группы над множеством скаляров, наделенным более «бедной» структурой, чем тело) могут служить линейные комбинации с целочисленными коэффициентами любых трех векторов трехмерного пространства, не лежащих в одной плоскости. Концы векторов, представимых в виде таких линейных комбинаций, задают в пространстве так называемую точечную решетку (рис. 66). Точечные решетки встречаются при рассмотрении некоторых геометрических фигур.

Помимо частных примеров, математиков интересовал и общий вопрос: что можно сказать об аддитивной группе над множеством скаляров, в котором невыполнима операция деления? Стремясь получить на свой вопрос достаточно общий ответ, математики рассмотрели случай, когда скаляры образуют не тело, а всего лишь кольцо (коммутативность не предполагается), и назвали новый «объект» ***модулем над кольцом.***

Коммутативная (аддитивная) группа M называется модулем над кольцом R, если операция αu определена для всех $\alpha \in R$ и $u \in M$ так, что $\alpha u \in M$ и

$$(\alpha + \beta)\, u = \alpha u + \beta u;$$
$$\alpha\,(u + v) = \alpha u + \alpha v;$$
$$(\alpha\beta)\, u = \alpha\,(\beta u),$$

где α, $\beta \in R$ и u, $v \in M$.

Строго говоря, приведенное выше определение относится к *левому R-модулю. Правый R-модуль* получится в том случае, если элементы модуля умножать на элементы кольца R справа. Различие между левым и правым R-модулем далеко не формально, потому что, хотя левый R-

модуль можно обозначить как правый, при этом вместо третьего тождества, приведенного в определении модуля, должно выполняться тождество $(\alpha\beta)u = \beta(\alpha u)$. Разумеется, если кольцо R коммутативно, то левый R-модуль совпадает с правым R-модулем. Но встречаются и такие кольца, которые «слева» выглядят совсем иначе, чем «справа».

Если кольцо содержит единичный элемент, то предполагается (но не всегда!), что $1 \cdot u = u$. (В действительности этот вопрос не имеет особого значения: если R — кольцо с единицей, то R-модуль можно разложить в прямую сумму (определяемую так же, как и прямая сумма векторных пространств) двух модулей, в одном из которых выполняется соотношение $1 \cdot u = u$, а в другом умножение на скаляр переводит любой элемент в 0, после чего рассматривать каждое из «прямых слагаемых» отдельно.)

Наиболее существенное различие между модулями и векторными пространствами состоит в том, что существование нетривиальной линейной комбинации двух элементов модуля еще не означает линейную зависимость одного элемента от другого. Например, если для каких-нибудь элементов u и v модуля над кольцом целых чисел $2u + 3v = 0$ (в правой части стоит нулевой элемент модуля), то отсюда не следует, что u «линейно зависит» от v, поскольку мы не можем разрешить линейную комбинацию $2u + 3v = 0$ относительно u, разделив «коэффициенты» на 2.

Второе существенное различие между модулями и векторными пространствами заключается в том, что среди модулей нет «наименьших» (аналогов одномерных векторных пространств). Пусть, например, модуль над кольцом целых чисел состоит из скалярных кратных одного элемента u. Выбирая скалярные кратные элементов $2u$, $4u$, $8u$, ..., мы будем получать «все меньшие и меньшие» подмодули (определить подмодуль можно по аналогии с определением подпространства).

Если сравнить определения модулей и векторных пространств с определениями полугрупп, групп, колец и тел, то можно заметить, что они относятся к двум типам определений, между которыми имеется существенное различие: в определения модуля и векторного пространства входит одна «внешняя» операция.

Но при рассмотрении большого числа однотипных систем (так называемых «алгебраических структур» — полугрупп и групп и т. д.) множество весьма важных и полезных результатов удается получить, если операции заданы «внутренним образом». Такие результаты «не чувствительны» к тому, какие именно операции заданы на множестве, и не зависят от числа мест («переменных») в операции, а определяются только тем, сколько операций задано на множестве. Более того, и последнее в каком-то смысле несущественно, поскольку доказательства остаются в силе и в том случае, если число операций неограниченно возрастает.

Учитывая все преимущества «внутреннего» рассмотрения, мы хотим сейчас определить векторные пространства и модули при помощи не «внешних», а «внутренних» операций. Сделать это можно следующим образом. Вместо элементов фиксированного кольца рассмотрим одноместную операцию, представляющую собой не что иное, как умножение на заданный элемент. Тождества, приведенные во «внешних» определениях векторного пространства и кольца, позволяют нам установить соответствующие тождества для операций.

После того как эта программа будет выполнена, мы сможем дать точное определение того, что такое модуль над заданным кольцом R.

Модулем над кольцом R называется система

$$\langle M; g, i, n, \ldots, f_\alpha, \ldots \rangle,$$

где M — некоторое множество, g —

двухместная операция (сложение), i — одноместная операция (сопоставляющая каждому элементу противоположный, то есть обратный относительно операции g элемент), n — нульместная операция (задающая нулевой элемент кольца); кроме того, каждому элементу α соответствует такая одноместная операция f_α, что:

1) $\langle M; g, i, n\rangle$ — *коммутативная группа;*

2) $f_{\alpha+\beta}(u) = g(f_\alpha(u), f_\beta(u))$,

$f_\alpha(g(u, v)) = g(f_\alpha(u), f_\alpha(v))$,

$f_{\alpha\beta}(u) = f_\alpha(f_\beta(u))$.

Следует обратить внимание на одно весьма важное обстоятельство: в случае векторных пространств (как и в случае модулей) изоморфизм и подпространство (подмодуль) означают одно и то же независимо от того, какому из двух определений — «внутреннему» или «внешнему» — мы отдадим предпочтение. Действительно, в одном случае сохранение операций относится к сложению и умножению на скаляр, в другом — к каждой из операций, входящих в определение, в отдельности. Следовательно, мы всегда можем воспользоваться тем определением, которое более удобно.

ЗАДАЧИ

1. Пусть R — произвольное кольцо. Построить из пар (α, β) элементов кольца R ($\alpha \in R$, $\beta \in R$) множество, которое было бы одновременно левым и правым R-модулем.

2. Доказать, что в двустороннем R-модуле ни один элемент не может быть левым скалярным кратным другого элемента без того, чтобы не быть правым скалярным кратным того же элемента.

3

Однородные линейные отображения

3.1. Гомоморфизм векторных пространств

Гомоморфизмом векторных пространств (по аналогии с гомоморфизмом групп) мы называем однозначное отображение, сохраняющее операции. Во многих приложениях интерес представляют главным образом конечномерные векторные пространства. Поэтому в дальнейшем, если нет особых оговорок, мы под векторным пространством всегда будем подразумевать конечномерное векторное пространство. Не боясь «тяжелых последствий», мы можем на время вообще забыть о бесконечномерных векторных пространствах, поскольку значительная часть понятий и методов, излагаемых ниже для конечномерных векторных пространств, без труда переносится на бесконечномерный случай.

Гомоморфизмы векторных пространств (по причинам, которые станут понятными в дальнейшем) принято называть *однородными линейными отображениями.*

Пусть $\mathbf{M}_1$ и $\mathbf{M}_2$ — векторные пространства над телом Γ. Отображение

$$\mathbf{A} : \mathbf{M}_1 \to \mathbf{M}_2$$

называется однородным линейным отображением, если:

1) для любых элементов u и v из $\mathbf{M}_1$

$$\mathbf{A}(u + v) = \mathbf{A}(u) + \mathbf{A}(v);$$

2) для любых λ из Γ и u из $\mathbf{M}_1$

$$\mathbf{A}(\lambda u) = \lambda \mathbf{A}(u).$$

Наше знакомство с однородными линейными отображениями мы начнем с нескольких примеров, которые рассмотрим в наиболее легко обозримом случае, когда оба векторных пространства $\mathbf{M}_1$ и $\mathbf{M}_2$ являются плоскостями, а Γ — телом вещественных чисел.

ПРИМЕРЫ

1. Нулевое отображение и тождественное отображение. Пусть $\mathbf{O}$ — нулевое отображение, ставящее в соответствие любому вектору нулевой вектор. Так как каждый из векторов $\mathbf{O}(u+v)$, $\mathbf{O}(u)$, $\mathbf{O}(v)$, $\mathbf{O}(\lambda u)$ совпадает с нулевым вектором, то оба соотношения, входящих в определение однородного линейного отображения, выполняются.

Пусть $\mathbf{I}$ — тождественное отображение, то есть отображение, переводящее любой вектор в самого себя: $\mathbf{I}(u) = u$. Ясно, что для $\mathbf{I}$ оба соотношения также выполняются, поскольку $u + v = u + v$, $\lambda u = \lambda u$.

2. Отражение относительно начала координат (рис. 67). Отражение относительно начала координат переводит каждый вектор u в вектор $-u$. Следовательно, в этом случае мы имеем дело с отображением $\mathbf{A}(u) = -u$, для которого

$$\mathbf{A}(u+v) = -(u+v) = -u+(-v) = \mathbf{A}(u) + \mathbf{A}(v)$$

и

$$\mathbf{A}(\lambda u) = -(\lambda u) = \lambda(-u) = \lambda \mathbf{A}(u).$$

Таким образом, $\mathbf{A}$ — однородное линейное отображение.

3. Отражение относительно прямой, проходящей через начало координат (рис. 68).

Пусть u — вектор, направленный вдоль заданной прямой, а v — вектор, ортогональный вектору u (ни

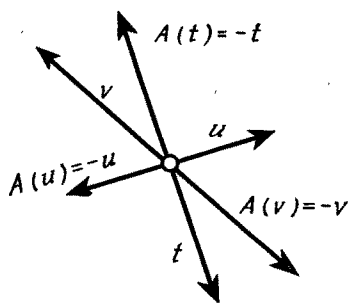


Рис. 67.

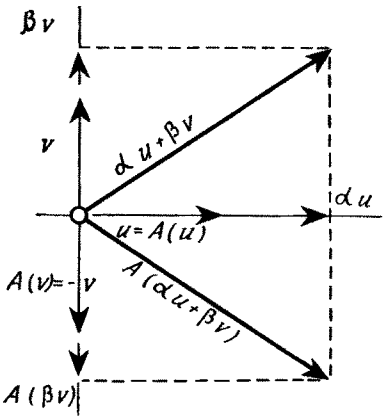


Рис. 68.

один из векторов u и v не должен быть нулевым вектором). При отражении относительно заданной прямой вектор u и все его скалярные кратные переходят в себя, а вектор v и все его скалярные кратные переходят в противоположные векторы. Следовательно, при отражении относительно заданной прямой линейная комбинация $\alpha u + \beta v$ переходит в $\alpha u - \beta v$, и мы получаем отображение $\mathbf{A}(\alpha u + \beta v) = \alpha u - \beta v$. Поскольку для этого отображения

$$\mathbf{A}((\alpha u + \beta v) + (\gamma u + \delta v)) =$$
$$= \mathbf{A}((\alpha+\gamma)u + (\beta+\delta)v) =$$
$$= (\alpha+\gamma)u - (\beta+\delta)v =$$
$$= (\alpha u - \beta v) + (\gamma u - \delta v) =$$
$$= \mathbf{A}(\alpha u + \beta v) + \mathbf{A}(\gamma u + \delta v)$$

и

$$\mathbf{A}(\lambda(\alpha u + \beta v)) = \mathbf{A}(\lambda\alpha u + \lambda\beta v) =$$
$$= \lambda\alpha u - \lambda\beta v = \lambda(\alpha u - \beta v) =$$
$$= \lambda \mathbf{A}(\alpha u + \beta v),$$

то $\mathbf{A}$ — однородное линейное отображение (любой вектор на плоскости однозначно представим в виде линейной комбинации векторов u и v).

4. Растяжение (сжатие) от центра (рис. 69). Умножив все векторы u, исходящие из начала координат на скаляр α, мы получим

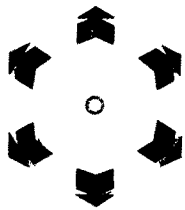


Рис. 69.

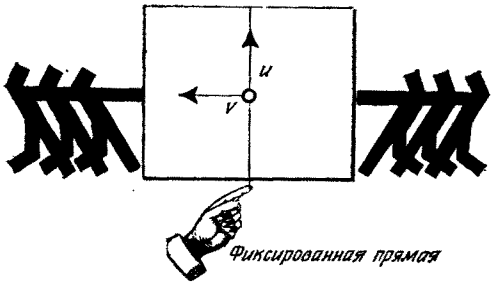


Рис. 70.

векторы αu. При $\alpha > 1$ преобразование действительно является растяжением. При $\alpha = 1$ мы получаем тождественное отображение. Если скаляр α меньше единицы, но положителен, то отображение уместнее называть сжатием. При $\alpha = 0$ мы получаем нулевое отображение. Если $\alpha = -1$, то отображение переходит в отражение относительно начала координат. При прочих отрицательных значениях α соответствующее растяжение (или сжатие) сопровождается отражением относительно начала координат. Отображение $\mathbf{A}(u) = \lambda u$ действительно является однородным линейным отображением, так как

$$\mathbf{A}(u+v) = \alpha(u+v) = \alpha u + \alpha v = \\ = \mathbf{A}(u) + \mathbf{A}(v)$$

и

$$\mathbf{A}(\lambda u) = \alpha(\lambda u) = \lambda(\alpha u) = \lambda \mathbf{A}(u).$$

5. Растяжение в направлении, перпендикулярном фиксированной прямой, проходящей через начало координат (рис. 70). Этому отображению можно придать «физический смысл», если представить себе, что плоскость резиновая и одинаково растянута в обе стороны от заданной прямой. Чтобы мы могли дать математическое описание этого отображения плоскости, введем вектор u, параллельный заданной прямой и отложенный от начала координат, и вектор v, ортогональный вектору u. Поскольку векторы u и v образуют на плоскости базис, то любой вектор можно однозначно представить в виде линейной комбинации $\alpha u + \beta v$. В направлении заданной прямой растяжение не происходит, оно сказывается только в направлении, перпендикулярном заданной прямой. Следовательно, мы получаем отображение плоскости на себя $\mathbf{A}(\alpha u + (\beta v) = \alpha u + \mu \beta v$. Нетрудно видеть, что $\mathbf{A}$ — однородное линейное отображение.

6. Поперечный сдвиг. О поперечном сдвиге мы говорим в том случае, если две равные по величине, но противоположно направленные силы (например, лезвия ножниц) стремятся сдвинуть один слой тела относительно другого. Один такой слой остается на месте, а соседние слои смещаются относительно него (рис. 71). В физике обычно рассматривают такой сдвиг, когда дальние слои испытывают бóльшие смещения, чем ближние. Математически такой поперечный сдвиг можно описать следующим образом: $\mathbf{A}(\alpha u + \beta v) = (\alpha + \mu \beta)u + \beta v$. Нетрудно проверить, что $\mathbf{A}$ — однородное линейное отображение (рис. 72).

7. Поворот. Рассмотрим поворот на 90° в положительном направлении (против часовой стрелки) вокруг начала координат (рис. 73). При таком отображении плоскости на се-

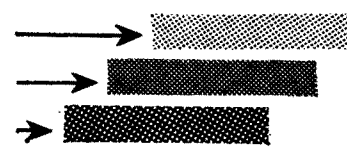


Рис. 71.

бя произвольно выбранный (но отличный от нулевого) вектор u переходит в ортогональный ему вектор v, имеющий такую же длину, как и вектор u. Если вектор v в свою очередь повернуть на 90° против часовой стрелки, то он перейдет в вектор, имеющий ту же длину, что и вектор u, но противоположное направление, то есть в вектор $-u$. Следовательно, записав произвольно выбранный вектор плоскости в виде линейной комбинации $\alpha u + \beta v$ и подвергнув его повороту на 90° вокруг начала координат против часовой стрелки, мы получим вектор, представимый в виде той же линейной комбинации, в которой вектор u заменен вектором v, а вектор v — вектором $-u$. Следовательно, поворот на 90° в положительном направлении вокруг начала координат порождает отображение плоскости на себя $\mathbf{F}(\alpha u + \beta v) = \alpha v - \beta u$. Нетрудно проверить, что $\mathbf{F}$ — однородное линейное преобразование (рис. 73).

Рассмотрим теперь поворот вокруг начала координат на 120° в положительном направлении (рис. 74). При таком повороте произвольно взятый вектор u переходит в вектор v, имеющий ту же длину, что и вектор u, но образующий с u угол в 120°. При повторном повороте вектор u переходит в вектор, противоположный вектору $u + v$. Следовательно, повернутый вектор v расположен относительно вектора $-(u + v)$ так же, как исходный вектор u относительно вектора v. Это означает, что поворот вокруг начала координат на 120° в положительном направлении порождает отображение плоскости на себя $\mathbf{F}(\alpha u + \beta v) = \alpha v + (-\beta)(u + v) = (-\beta)u + (\alpha - \beta)v$. Нетрудно видеть, что и в этом случае мы получаем однородное линейное отображение.

8. Ортогональная проекция. Опустим перпендикуляры из точек плоскости на прямую, проходящую через начало координат. Если u — (отличный от нулевого)

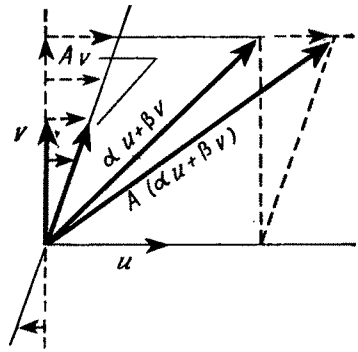


Рис. 72.

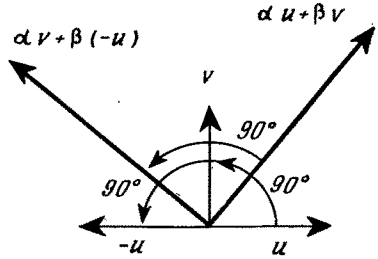


Рис. 73.

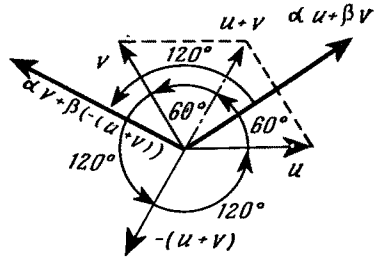


Рис. 74.

вектор, параллельный выбранной прямой, а v — вектор, ортогональный ей, то образ любого вектора на плоскости при ортогональной проекции совпадает с его составляющей в направлении вектора u: $\mathbf{V}(\alpha u + \beta v) = \alpha u$. Нетрудно видеть, что $\mathbf{V}$ — однородное линейное отображение.

В рассмотренных нами примерах основное место занимало доказательство того, что в каждом случае мы

действительно имеем дело с однородным линейным отображением. Эту трудность можно было бы обойти, если бы мы умели распознавать «с первого взгляда» те из отображений, которые являются однородными линейными отображениями.

Прежде всего необходимо выяснить, что следует знать об отображении для того, чтобы его заведомо можно было отнести к однородным линейным отображениям. Предположим, что $A : M_1 \to M_2$ — заданное однородное линейное отображение. Пусть $u_1, u_2, \ldots, u_n$ — базис векторного пространства M_1. Любой вектор из M_1 можно однозначно представить в виде линейной комбинации векторов $u_1, u_2, \ldots, u_n$. Но если $u = \alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_n u_n$, то нетрудно определить, во что переходит под действием однородного линейного отображения A вектор u. Действительно, так как A сохраняет операции, то

$$A(u) = \alpha_1 A(u_1) + \alpha_2 A(u_2) + \cdots + \alpha_n A(u_n).$$

Это означает, что *любое однородное линейное отображение однозначно определено, если заданы образы векторов базиса.*

Естественно задать вопрос: насколько «произвольно» можно задавать образы базисных векторов. Ответ на этот вопрос гласит: *образы элементов базиса можно задавать совершенно произвольно; всегда существует такое однородное линейное отображение, которое переводит векторы исходного базиса в заранее указанные векторы.*

Для доказательства этого утверждения помимо базиса $u_1, u_2, \ldots, u_n$ в векторном пространстве M_1 зададим в M_2 произвольную систему векторов $v_1, v_2, \ldots, v_n$. Докажем, что существует однозначно определенное однородное линейное отображение: $B : M_1 \to M_2$, переводящее векторы u_i в векторы v_i. Нетрудно показать, что такое однородное линейное отображение единственно. Действительно, поскольку B сохраняет операции, то под действием этого отображения произвольный вектор

$$u = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$$

из M_1 переходит в вектор

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$

из M_2. Итак, остается доказать, что B — однородное линейное отображение. Прежде всего докажем, что каждый вектор из M_1 под действием B переходит в некоторый вектор из M_2. Это утверждение следует из того, что каждый вектор из M_1 можно представить в виде линейной комбинации векторов $u_1, u_2, \ldots, u_n$, образующих базис в M_1. Докажем, далее, что B сохраняет операции. Это утверждение следует из того, что

$$B(\lambda u) = B(\lambda\alpha_1 u_1 + \lambda\alpha_2 u_2 + \cdots + \lambda\alpha_n u_n) =$$
$$= \lambda\alpha_1 v_1 + \lambda\alpha_2 v_2 + \cdots + \lambda\alpha_n v_n =$$
$$= \lambda(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n) = \lambda v = \lambda B(u)$$

и, кроме того, если $u' = \beta_1 u_1 + \beta_2 u_2 + \ldots + \beta_n u_n$, то

$$B(u + u') = B((\alpha_1 + \beta_1) u_1 +$$
$$+ (\alpha_2 + \beta_2) u_2 + \cdots + (\alpha_n + \beta_n) u_n) =$$
$$= (\alpha_1 + \beta_1) v_1 + (\alpha_2 + \beta_2) v_2 + \ldots$$
$$\cdots + (\alpha_n + \beta_n) v_n = (\alpha_1 v_1 +$$
$$+ \alpha_2 v_2 + \cdots + \alpha_n v_n) + (\beta_1 v_1 + \beta_2 v_2 + \cdots$$
$$\ldots + \beta_n v_n) = B(u) + B(u').$$

(Это доказательство можно рассматривать как своего рода «унификацию» доказательств сохранения операций, приведенных в каждом из рассмотренных нами примеров в отдельности.)

Попытаемся теперь выяснить, почему однородным линейным отображениям в математике придается столь важное значение. По существу однородные линейные отображения представляют собой не что иное, как функции, ставящие в соответствие векторам векторы. Чтобы рассматривать такие функции, необходимо ввести «сокращенные обозначения», позволяющие записывать громоздкие выкладки в удобообозримом виде и тем значительно облегчающие их. Если воспользоваться изоморфизмом векторных пространств одинаковой размерности, то произвольное n-мерное векторное пространство можно изоморфно отобразить на векторное пространство наборов из n чисел. При этом функции, отображающие вектор в вектор, «скроются» за целым набором функций многих независимых переменных.

Если оба векторных пространства

(«область определения» и «область значений» однородного линейного отображения) одномерны, то речь идет о функции, ставящей в соответствие «вектору» (ξ) «вектор» (η). Поскольку соответствие между «векторами» задано однородным линейным отображением, то $(\eta) = A((\xi)) = A(\xi(1)) = \xi A((1))$. Но если отображение A переводит вектор (1) в вектор $(\alpha) = \alpha(1)$, то A можно представить в виде $\eta \cdot (1) = \xi\alpha \cdot (1)$. Зависимость между η и ξ ($\eta = \xi\alpha$) здесь однозначна (α — фиксированное вещественное число). Соотношение $\eta = \xi\alpha$ — это линейная функция без свободного (постоянного) члена, которую обычно называют однородной линейной функцией. Если A отображает двумерное векторное пространство на одномерное векторное пространство, то $(\eta) = A((\xi_1, \xi_2))$. Предположим, что $A((1, 0)) = \alpha(1)$, $A((0, 1) = \beta(1)$. Так как A — однородное линейное отображение, то мы получаем однородную линейную функцию двух независимых переменных $\eta = \alpha\xi_1 + \beta\xi_2$. Если же, например, A отображает двумерное векторное пространство на двумерное векторное пространство, то аналогичные рассуждения приводят к двум однородным линейным функциям двух независимых переменных $\eta_1 = \alpha\xi_1 + \beta\xi_2$ и $\eta_2 = \gamma\xi_1 + \delta\xi_2$.

Эти примеры показывают, что однородные линейные отображения можно рассматривать как частный случай наборов, состоящих из нескольких функций многих независимых переменных. Однородные линейные отображения не просто принадлежат множеству функций многих независимых переменных, но и служат в этом множестве своеобразным «эталоном», позволяя «измерять», насколько изменяется по величине и направлению «зависимый» вектор, когда «независимый» вектор изменяется в заданном направлении. Именно поэтому линейным однородным отображениям в математике придают столь большое значение.

Рассмотрим теперь однородные линейные отображения с алгебраической точки зрения.

Однородные линейные отображения являются гомоморфизмами групп. Следовательно, мы можем говорить о ядре и образе отображения.

Итак, пусть $A : M_1 \to M_2$ — однородное линейное отображение.

1. Элементы $A(u)$ векторного пространства M_2 образуют подпространство, которое называется образом отображения A и обозначается Im A.

2. Элементы u векторного пространства M_1, для которых $A(u) = 0$, образуют подпространство, называемое ядром отображения A и обозначаемое Ker A.

Оба утверждения легко поддаются проверке. Если $v_1 = A(u_1)$ и $v_2 = A(u_2)$, то $\alpha v_1 + \beta v_2 = \alpha A(u_1) + \beta A(u_2) = A(\alpha u_1 + \beta u_2)$, что доказывает первое утверждение. Если $A(u_1) = A(u_2) = 0$, то $A(\alpha u_1 + \beta u_2) = \alpha A(u_1) + \beta A(u_2) = 0$, поэтому Ker A — подпространство векторного пространства M_1.

Векторные пространства Im A и Ker A не вполне «независимы»: их размерности связаны соотношением

$$\dim(\mathrm{Im}\,A) + \dim(\mathrm{Ker}\,A) = \dim(M_1),$$

где dim (M) означает размерность векторного пространства M. (Эта теорема следует из аналогии с доказанной для групп теоремой о гомоморфизмах.)

Теорему о связи размерностей Im A и Ker A можно доказать следующим образом.

Пусть $u_1, u_2, \ldots, u_n$ — базис векторного пространства Ker A. Во всем векторном пространстве M_1 векторы $u_1, u_2, \ldots, u_n$ образуют линейно независимую систему, поэтому ее можно дополнить некоторыми векторами $v_1, v_2, \ldots, v_k$ до базиса векторного пространства M_1. Отсюда, разумеется, следует, что векторы $v_1, v_2, \ldots, v_k$ образуют в M_1 линейно независимую систему. Эта система порождает подпространство N (с базисом $v_1, v_2, \ldots, v_n$), и, объединяя N с Ker A, получаем: $M_1 = \{\mathrm{Ker}\,A, N\}$. Поскольку линейная комбинация векторов $u_1, u_2, \ldots, u_n$ может совпадать с линейной комбинацией векторов $v_1, v_2, \ldots, v_k$ лишь в том случае, если обе линейные комби-

нации тривиальны (обе системы векторов линейно независимы), то $\mathrm{Ker}\,\mathbf{A} \cap \mathbf{N} = \{0\}$. Следовательно, векторное пространство $\mathbf{M}_1$ разлагается в прямую сумму подпространств $\mathrm{Ker}\,\mathbf{A}$ и N. Размерность векторного пространства $\mathbf{M}_1$, равная $n + k$ (напомним, что векторы $u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_k$ образуют базис в $\mathbf{M}_1$), совпадает с суммой размерностей подпространств $\mathrm{Ker}\,\mathbf{A}$ и N:

$$\dim(\mathbf{N}) + \dim(\mathrm{Ker}\,\mathbf{A}) = \dim(\mathbf{M}_1).$$

Для доказательства исходного равенства необходимо убедиться в том, что размерность подпространства N совпадает с размерностью образа отображения A. Но вместо того, чтобы доказывать непосредственно равенство размерностей подпространств N и $\mathrm{Im}\mathbf{A}$, мы докажем эквивалентное утверждение, а именно что подпространства N и $\mathrm{Im}\mathbf{A}$ изоморфны. Действительно, подпространство N можно отобразить на подпространство $\mathrm{Im}\mathbf{A}$ (переход $\mathbf{N} \to \mathrm{Im}\mathbf{A}$ осуществляет отображение A). Так как A — однородное линейное отображение векторного пространства $\mathbf{M}_1$ на $\mathrm{Im}\mathbf{A}$, то A можно рассматривать и как однородное линейное отображение на подпространстве N. Необходимо лишь доказать, что различные элементы из N имеют различные образы и что для каждого элемента из $\mathrm{Im}\mathbf{A}$ в N можно указать прообраз. Тем самым будет доказано, что подпространства N и $\mathrm{Im}\mathbf{A}$ изоморфны.

Если образы каких-то двух элементов из N совпадают, то разность этих элементов под действием однородного линейного отображения A переходит в нулевой вектор пространства $\mathbf{M}_2$. Но всякий вектор из $\mathbf{M}_1$, образ которого совпадает с нулевым вектором из $\mathbf{M}_2$, принадлежит ядру отображении A, а так как $\mathrm{Ker}\,\mathbf{A}$ и N имеют единственный общий элемент — нулевой вектор из $\mathbf{M}_1$, то разность двух выбранных нами векторов равна нулевому вектору из $\mathbf{M}_1$, и эти векторы совпадают. Итак, действуя на N, отображение A переводит различные векторы в различные.

Рассмотрим теперь произвольный элемент образа отображения A. По определению образа отображения, для каждого вектора $\mathbf{A}(u)$ подпространства $\mathrm{Im}\mathbf{A}$ в векторном пространстве $\mathbf{M}_1$ существует прообраз u. Записав его в виде линейной комбинации векторов базиса $u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_k$, получим

$$u = \underbrace{(\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n)}_{u'} + \underbrace{(\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n)}_{v}.$$

Поскольку $u' \in \mathrm{Ker}\,\mathbf{A}$, $v \in \mathbf{N}$, то $\mathbf{A}(u) = \mathbf{A}(u' + u) = \mathbf{A}(u') + \mathbf{A}(u) = \mathbf{A}(v)$. Следовательно, элемент $\mathbf{A}(u)$ можно рассматривать как образ элемента $v \in \mathbf{N}$.

ЗАДАЧИ

1. Найти следующие однородные линейные отображения трехмерного пространства в себя:

а) отражение относительно начала координат;

б) отражение относительно прямой, проходящей через начало координат;

в) отражение относительно плоскости, проходящей через начало координат;

г) ортогональную проекцию на плоскость, проходящую через начало координат;

д) ортогональную проекцию на прямую, проходящую через начало координат.

2. В примерах однородных линейных преобразований из задачи 1 найти ядро и образ преобразования.

3. Доказать, что следующие отображения являются однородными линейными отображениями, и найти ядра и образы этих отображений.

а) Отображение векторного пространства наборов из n чисел, ставящее в соответствие каждому набору его первую компоненту.

б) Отображение векторного пространства многочленов степени не выше n, ставящее в соответствие каждому многочлену $f(x)$ его значение $f(a)$, где a — фиксированное вещественное число.

в) Отображение комплексных чисел как векторного пространства над телом вещественных чисел, ставящее в соответствие комплексному числу $a + bi$ его мнимую часть b.

3.2. Операции над однородными линейными отображениями

Однородные линейные отображения как частный случай отображений обладают всеми их свойствами, которые были установлены нами ранее.

Два однородных линейных отображения называются совпадающими, или равными, если они оба переводят одно и то же векторное пространство в одно и то же векторное

пространство, то есть если

$$\mathbf{A}: M_1 \to M_2 \text{ и } \mathbf{B}: M_1 \to M_2,$$

причем так, что образы всех векторов исходного пространства при обоих отображениях совпадают, то есть для любого $u \in M_1$

$$\mathbf{A}(u) = \mathbf{B}(u).$$

Для однородных линейных преобразований можно определить операцию умножения.

Относительно произведения двух однородных линейных преобразований заранее известно, что оно является отображением, поскольку это установлено для произведения любых отображений. Следовательно, необходимо лишь доказать, что произведение двух однородных линейных преобразований сохраняет операции.

Это доказательство проводится следующим образом:

$$\mathbf{BA}(\lambda u) = \mathbf{B}(\mathbf{A}(\lambda u)) = \mathbf{B}(\lambda \mathbf{A}(u)) =$$
$$= \lambda \mathbf{B}(\mathbf{A}(u)) = \lambda \mathbf{BA}(u)$$

и

$$\mathbf{BA}(u+v) = \mathbf{B}(\mathbf{A}(u+v)) = \mathbf{B}(\mathbf{A}(u) +$$
$$+ \mathbf{A}(v)) = \mathbf{B}(\mathbf{A}(u)) + \mathbf{B}(\mathbf{A}(v)) =$$
$$= \mathbf{BA}(u) + \mathbf{BA}(v).$$

Относительно умножения однородных линейных преобразований известно, что оно ассоциативно, поскольку ассоциативность умножения доказана для произвольных отображений.

Если $\mathbf{A}: M_1 \to M_2$ и $\mathbf{B}: M_2 \to M_3$ — два однородных линейных преобразования, то их произведение надлежит понимать следующим образом: при любом $u \in M_1$

$$\mathbf{BA}(u) \quad \mathbf{B}(\mathbf{A}(u)).$$

Но над однородными линейными отображениями (в некоторых случаях) можно производить и другие операции. Если однородные линейные отображения рассматривать как функции, то отсюда следует, что все операции, производимые над функциями, применимы и к однородным линейным отображениям. Как известно, для функций операции сложения и умножения определены так, что при любых значениях аргументов функция, получаемая в результате выполнения операции, принимает значение, равное соответственно сумме или произведению значений, принимаемых при тех же значениях аргументов функциями-слагаемыми или функциями-сомножителями. Мы можем поступать так, поскольку знаем, как находить произведение и сумму значений функций, то есть чисел. Если же функции принимают векторные значения, то умножать их, как числа, невозможно, и остается лишь одна «знакомая» операция — сложение. Сумму двух однородных линейных отображений определим как такое однородное линейное отображение $\mathbf{A} + \mathbf{B}$, которое при любом «аргументе» u принимает значение, совпадающее с суммой векторов $\mathbf{A}(u)$ и $\mathbf{B}(u)$. Оба слагаемых $\mathbf{A}$ и $\mathbf{B}$, во-первых, должны быть заданы на одном и том же векторном пространстве, или, что то же, отображать одно и то же векторное пространство. Во-вторых, для того чтобы векторы $\mathbf{A}(u)$ и $\mathbf{B}(u)$ можно было суммировать, они должны принадлежать одному и тому же векторному пространству.

Если $\mathbf{A}: M_1 \to M_2$ и $\mathbf{B}: M_1 \to M_2$ — однородные линейные отображения, то их суммой называется такое отображение

$$(\mathbf{A} + \mathbf{B}): M_1 \to M_2,$$

что при любом $u \in M_1$

$$(\mathbf{A} + \mathbf{B})(u) \quad \mathbf{A}(u) + \mathbf{B}(u).$$

Докажем, что отображение $\mathbf{A} + \mathbf{B}$ сохраняет операции. Доказательство проведем для каждой операции в отдельности. Поскольку доказательства приводимого ниже типа встречаются весьма часто, мы разобьем их для большей ясности на три этапа.

Начнем с доказательства сохранения сложения.

1. Воспользуемся определением суммы отображений:

$$(\mathbf{A} + \mathbf{B})(u+v) = \mathbf{A}(u+v) + \mathbf{B}(u+v).$$

2. Для каждого из отображений $\mathbf{A}$ и $\mathbf{B}$ воспользуемся тем тождеством, кото-

рое требуется доказать для их суммы $\mathbf{A}+\mathbf{B}$:

$$\mathbf{A}(u+v)+\mathbf{B}(u+v)=\mathbf{A}(u)+\mathbf{A}(v)+$$
$$+\mathbf{B}(u)+\mathbf{B}(v)=\mathbf{A}(u)+\mathbf{B}(u)+$$
$$+\mathbf{A}(v)+\mathbf{B}(v).$$

3. Снова воспользуемся определением суммы отображения:

$$\mathbf{A}(u)+\mathbf{B}(u)+\mathbf{A}(v)+\mathbf{B}(v)=(\mathbf{A}+\mathbf{B})(u)+$$
$$+(\mathbf{A}+\mathbf{B})(v).$$

Той же схемы будем придерживаться и при проверке второго тождества:

1) $(\mathbf{A}+\mathbf{B})(\lambda u)=\mathbf{A}(\lambda u)+\mathbf{B}(\lambda u)$;

2) $\mathbf{A}(\lambda u)+\mathbf{B}(\lambda u)=\lambda\mathbf{A}(u)+\lambda\mathbf{B}(u)=$
$$=\lambda(\mathbf{A}(u)+\mathbf{B}(u));$$

3) $\lambda(\mathbf{A}(u)+\mathbf{B}(u))=\lambda((\mathbf{A}+\mathbf{B})(u))$.

Произведение линейных отображений невозможно определить как произведение функций, поскольку векторы нельзя умножать, как числа. Но по аналогии с умножением вектора на скаляр можно попытаться определить умножение линейного отображения на скаляр.

Если $\mathbf{A}:\mathrm{M}_1\to\mathrm{M}_2$ — линейное отображение, то линейным отображением $\alpha\mathbf{A}:\mathrm{M}_1\to\mathrm{M}_2$ называется такое отображение, что $(\alpha\mathbf{A})(u)=\alpha(\mathbf{A}(u))$.

Покажем, что $\alpha\mathbf{A}$ действительно является линейным отображением (на первом и последнем шаге в каждой цепочке равенств мы используем определение отображения $\alpha\mathbf{A}$):

$$(\alpha\mathbf{A})(u+v)=\alpha(\mathbf{A}(u+v))=$$
$$=\alpha(\mathbf{A}(u)+\mathbf{A}(v))=\alpha(\mathbf{A}(u))+$$
$$+(\mathbf{A}(v))=(\alpha\mathbf{A})(u)+(\alpha\mathbf{A})(v)$$

и

$$(\alpha\mathbf{A})(\lambda u)=\alpha(\mathbf{A}(\lambda u))=\alpha(\lambda(\mathbf{A}(u)))=$$
$$=\lambda(\alpha(\mathbf{A}(u)))=\lambda((\alpha\mathbf{A})(u)).$$

Итак, приведенные выше определения показывают, что для однородных линейных отображений изредка можно определить произведение, иногда сумму и во всех случаях — произведение любого однородного линейного преобразования и произвольно выбранного скаляра. Однако от определения операций до их конкретного выполнения — путь немалый. Для того чтобы мы могли проделать над отображениями те или иные операции, необходимо знать, какие тождества помогут нам выполнить соответствующие операции.

К рассмотрению этих тождеств мы сейчас и приступаем. Поскольку операции над однородными линейными отображениями выполнимы далеко не всегда, необходимо в каждом случае проверять, осуществима ли интересующая нас операция. Мы не будем всякий раз контролировать выполнимость операции, поскольку такая проверка удлинила бы и без того громоздкие выкладки, и рассмотрим лишь случаи, в которых намеченные операции заведомо выполнимы. Умножением однородных линейных отображений на себя мы заниматься не будем, поскольку ранее было доказано, что возведение отображений в степень ассоциативно.

1. Сложение. а) *Ассоциативность сложения.* Во-первых, $[\mathbf{A}+(\mathbf{B}+\mathbf{C})](u)=\mathbf{A}(u)+(\mathbf{B}+\mathbf{C})(u)=\mathbf{A}(u)+[\mathbf{B}(u)+\mathbf{C}(u)]$, во-вторых, $[(\mathbf{A}+\mathbf{B})+\mathbf{C}](u)=(\mathbf{A}+\mathbf{B})(u)\times\mathbf{C}(u)=[\mathbf{A}(u)+\mathbf{B}(u)]+\mathbf{C}(u)$. Так как сложение в векторных пространствах ассоциативно, то каждое из отображений $\mathbf{A}+(\mathbf{B}+\mathbf{C})$ и $(\mathbf{A}+\mathbf{B})+\mathbf{C}$, действуя на любой вектор, переводит его в один и тот же вектор-образ. Следовательно, однородные линейные отображения $\mathbf{A}+(\mathbf{B}+\mathbf{C})$ и $(\mathbf{A}+\mathbf{B})+\mathbf{C}$ совпадают.

б) *Коммутативность сложения.* Так как сложение в векторных пространствах коммутативно, то $(\mathbf{A}+\mathbf{B})(u)=\mathbf{A}(u)+\mathbf{B}(u)=\mathbf{B}(u)+\mathbf{A}(u)=(\mathbf{B}+\mathbf{A})(u)$, что и доказывает наше утверждение.

в) *Существование нулевого отображения* $\mathbf{O}$. Пусть $\mathbf{A}:\mathrm{M}_1\to\mathrm{M}_2$ — однородное линейное отображение. Обозначим через $\mathbf{O}$ такое отображение, которое каждый вектор из M_1 переводит в нулевой вектор из M_2.

Так как соотношение $(\mathbf{O} + \mathbf{A})(u) = \mathbf{O}(u) + \mathbf{A}(u) = \mathbf{0} + \mathbf{A}(u) = \mathbf{A}(u)$ выполняется при любом $u \in M_1$, то $\mathbf{O} + \mathbf{A} = \mathbf{A}$. Правда, мы еще не доказали, что введенное нами отображение $\mathbf{O}$ однородно и линейно. Но это действительно так, поскольку обе части тождеств, входящих в определение однородного линейного отображения для $\mathbf{O}$, равны нулевому вектору.

Следует иметь в виду, что для каждой пары векторных пространств существует «свое», только ей присущее нулевое отображение $\mathbf{O}$. Введение единого обозначения для различных отображений не приводит к какой-либо путанице, поскольку в сумму нулевого и любого другого однородного линейного отображения $\mathbf{A}$ всегда входит нулевое отображение того векторного пространства M_1, на котором определено второе слагаемое $\mathbf{A}$, и это нулевое отображение переводит векторное пространство M_1 в нулевой вектор векторного пространства M_2, содержащего образ векторного пространства M_1 относительно второго слагаемого суммы преобразований.

г) *Существование противоположного отображения.* Если $\mathbf{A} : M_1 \to M_2$ — однородное линейное отображение, то отображением $(-\mathbf{A}) : M_1 \to M_2$ называется отображение $(-\mathbf{A})(u) = (-\mathbf{A})(u)$. Оно «противоположно» исходному отображению $\mathbf{A}$, так как $((-\mathbf{A}) + \mathbf{A})(u) = (-\mathbf{A})(u) + \mathbf{A}(u) = -\mathbf{A}(u) + \mathbf{A}(u) = 0$ (поскольку $-\mathbf{A} + \mathbf{A} = \mathbf{O}$). Необходимо еще доказать, что отображение $-\mathbf{A}$ обладает всеми свойствами однородного линейного отображения. Вместо того чтобы проводить соответствующие выкладки, достаточно ограничиться следующим замечанием: тождества, входящие в определение однородного линейного отображения, выполняются для отображения $-\mathbf{A}$, поскольку получаются из соответствующих тождеств для отображения $\mathbf{A}$ при замене знаков в правой и левой частях на противоположные.

Итак, из тождеств, выполняющихся для суммы отображений, следует, что *однородные линейные отображения векторного пространства* M_1 *в векторное пространство* M_2 *образуют коммутативную группу по сложению.*

2. Умножение на скаляры. Для этой операции мы докажем лишь одно тождество: $(\alpha\beta)\mathbf{A} = \alpha(\beta\mathbf{A})$. Выбрав произвольный вектор (по определению отображение $\gamma\mathbf{A}$ задано на том же векторном пространстве, что и отображение $\mathbf{A}$), получим: $((\alpha\beta)\mathbf{A})(u) = (\alpha\beta)(\mathbf{A}(u)) = \alpha(\beta(\mathbf{A}(u))) = \alpha((\beta\mathbf{A})(u)) = (\alpha(\beta\mathbf{A}))(u)$.

3. Тождества для сложения однородных линейных отображений и умножения их на скаляры.

а) $(\alpha + \beta)\mathbf{A} = \alpha\mathbf{A} + \beta\mathbf{A}$.

Докажем, что образы любого вектора u при действии отображений $(\alpha + \beta)\mathbf{A}$ и $\alpha\mathbf{A} + \beta\mathbf{A}$ совпадают: $((\alpha + \beta)\mathbf{A})(u) = (\alpha + \beta)(\mathbf{A}(u)) = \alpha(\mathbf{A}(u)) + \beta(\mathbf{A}(u)) = (\alpha\mathbf{A})(u) + (\beta\mathbf{A})(u) = (\alpha\mathbf{A} + \beta\mathbf{A})(u)$.

б) $\alpha(\mathbf{A} + \mathbf{B}) = \alpha\mathbf{A} + \alpha\mathbf{B}$.

Утверждение следует из того, что $(\alpha(\mathbf{A} + \mathbf{B}))(u) = \alpha((\mathbf{A} + \mathbf{B})(u)) = \alpha(\mathbf{A}(u) + \mathbf{B}(u)) = \alpha(\mathbf{A}(u)) + \alpha(\mathbf{B}(u)) = (\alpha\mathbf{A})(u) + (\alpha\mathbf{B})(u) = (\alpha\mathbf{A} + \alpha\mathbf{B})(u)$.

Сравнив доказанные тождества с тождествами, входящими в определение векторного пространства, нетрудно заметить, что

однородные линейные отображения векторного пространства M_1 в векторное пространство M_2 с заданными на них операциями сложения и умножения на скаляр образуют векторное пространство, обозначаемое

$$\mathrm{Hom}(M_1, M_2).$$

Три буквы Hom, входящие в это обозначение, — сокращение от слова «гомоморфизм», поскольку в данном случае речь действительно идет о

гомоморфизмах. Можно показать, что аналогичные результаты получаются как для абелевых групп, так и для модулей.

4. Тождества для сложения и умножения однородных линейных отображений.

а) *Левый закон дистрибутивности.* Требуется доказать, что отображения $\mathbf{A}(\mathbf{B}+\mathbf{C})$ и $\mathbf{AB}+\mathbf{AC}$ переводят любой вектор u в один и тот же вектор. Действительно, $(\mathbf{A}(\mathbf{B}+\mathbf{C}))(u) = \mathbf{A}((\mathbf{B}+\mathbf{C})(u)) = \mathbf{A}(\mathbf{B}(u)+\mathbf{C}(u)) = \mathbf{A}(\mathbf{B}(u))+\mathbf{A}(\mathbf{C}(u)) = (\mathbf{AB})(u)+(\mathbf{AC})(u) = (\mathbf{AB}+\mathbf{AC})(u)$.

б) *Правый закон дистрибутивности.* Требуется доказать тождество $(\mathbf{B}+\mathbf{C})\mathbf{A} = \mathbf{BA}+\mathbf{CA}$. **A**, **B** и **C** означают здесь, вообще говоря, другие отображения, чем в (а). Выбрав произвольный вектор u, получим $((\mathbf{B}+\mathbf{C})\mathbf{A})(u) = (\mathbf{B}+\mathbf{C})\times(\mathbf{A}(u)) = \mathbf{B}(\mathbf{A}(u))+\mathbf{C}(\mathbf{A}(u)) = (\mathbf{BA})(u)+(\mathbf{CA})(u) = (\mathbf{BA}+\mathbf{CA})(u)$.

(Известно, что один из двух законов дистрибутивности может выполняться даже в том случае, если другой закон дистрибутивности утрачивает силу. Для однородных линейных отображений выполняются оба закона дистрибутивности, но доказывать каждый из них необходимо особо, поскольку они выражают различные свойства операций.)

Сопоставляя тождества для сложения и умножения однородных линейных отображений, можно заметить, что они совпадают с тождествами, входящими в определение кольца. Как известно, если операции в кольце выполнимы без каких бы то ни было ограничений, то для любых двух элементов кольца существует сумма и произведение. Сложение двух однородных линейных отображений выполнимо в том случае, если каждое из отображений-слагаемых переводит заданное векторное пространство M_1 в одно и то же векторное пространство M_2. Что же касается умножения (последовательного выполнения) двух однородных линейных отображений, то эта операция осуществима лишь в том случае, если векторные пространства M_1 и M_2 совпадают. Но в этом случае выполнимы обе операции — и сложение, и умножение отображений.

Однородные линейные отображения векторного пространства M на себя образуют кольцо относительно заданных выше операций сложения и умножения отображений. Элементы этого кольца называются линейными преобразованиями векторного пространства M.

5. Тождества для умножения линейных преобразований и умножения линейных преобразований на скаляр. Имеется два таких тождества. Мы выпишем их «подряд», в виде одной цепочки соотношений: $\alpha(\mathbf{AB}) = (\alpha\mathbf{A})\mathbf{B} = \mathbf{A}(\alpha\mathbf{B})$, но докажем каждое из тождеств в отдельности:

$$\text{а)}\ ((\alpha\mathbf{A})\mathbf{B})(u) = (\alpha\mathbf{A})(\mathbf{B}(u)) = \alpha(\mathbf{A}(\mathbf{B}(u))) = \alpha(\mathbf{AB})(u) = (\alpha(\mathbf{AB}))(u);$$

$$\text{б)}\ (\mathbf{A}(\alpha\mathbf{B}))(u) = \mathbf{A}((\alpha\mathbf{B})(u)) = \mathbf{A}(\alpha(\mathbf{B}(u))) = \alpha(\mathbf{A}(\mathbf{B}(u))) = (\alpha(\mathbf{AB}))(u).$$

ЗАДАЧИ

1. Доказать, что соотношение $1\cdot\mathbf{A} = \mathbf{A}$ выполняется для любого линейного преобразования **A**.

2. Доказать, что линейные преобразования образуют кольцо с единицей.

3. Доказать, что для линейного преобразования **A** следующие утверждения эквивалентны:

а) для **A** существует левое обратное преобразование;

б) для **A** существует правое обратное преобразование;

в) **A** переводит различные элементы векторного пространства в различные;

г) каждый элемент векторного пространства служит образом какого-

то элемента того же векторного пространства.

Такие преобразования называются *невырожденными*.

4. Доказать, что для линейного преобразования $\mathbf{A}$ следующие утверждения эквивалентны:

а) существует отличное от $\mathbf{O}$ линейное преобразование $\mathbf{B}$, удовлетворяющее соотношению $\mathbf{BA} = \mathbf{O}$;

б) существует отличное от $\mathbf{O}$ линейное преобразование $\mathbf{C}$, удовлетворяющее соотношению $\mathbf{AC} = \mathbf{O}$;

в) $\mathbf{A}$ не является невырожденным преобразованием.

Такие преобразования называются *вырожденными*.

5. Доказать, что, если линейное преобразование $\mathbf{P}$ удовлетворяет соотношению $\mathbf{P}^2 = \mathbf{P}$, то векторное пространство M, отображение которого на себя задано преобразованием $\mathbf{P}$, можно разложить в прямую сумму подпространств $\operatorname{Ker}\mathbf{P}$ и $\operatorname{Im}\mathbf{P}$.

6. Доказать, что линейное преобразование удовлетворяет условию $\mathbf{N}^2 = \mathbf{O}$ в том и только в том случае, если векторное пространство $\operatorname{Im}\mathbf{N}$ содержится в $\operatorname{Ker}\mathbf{N}$, то есть если $\operatorname{Im}\mathbf{N} \subseteq \operatorname{Ker}\mathbf{N}$.

7. Найти размерность векторного пространства $\operatorname{Hom}(M_1, M_2)$.

3.3. Матрицы

При задании операций над однородными линейными преобразованиями или при рассмотрении тождеств, которым должны удовлетворять эти операции, краткие и вместе с тем более «емкие» (по сравнению с применявшимися в предыдущих разделах) обозначения отображений были бы весьма кстати. Действительно, при изучении чисто алгебраических вопросов имеет значение лишь то, какие операции заданы и каким тождествам они удовлетворяют. Но если при решении какой-то конкретной, практической задачи необходимо выполнить те или иные операции, то однородные линейные отображения удобнее описывать каким-нибудь числом или набором чисел и по известным исходным значениям параметров определять значения, характеризующие конечный результат выполнения операций.

Чтобы задать однородное линейное отображение, попытаемся выяснить, какими параметрами характеризуются векторы. Весьма простое описание допускают векторы на плоскости. Действительно, всякий вектор на плоскости однозначно определяется заданием его конца, если его начало совмещено с началом координат. Следовательно, для задания вектора на плоскости необходимы те числа, которые характеризуют положение точки на плоскости, а их мы без труда определим, введя на плоскости систему координат (рис. 75).

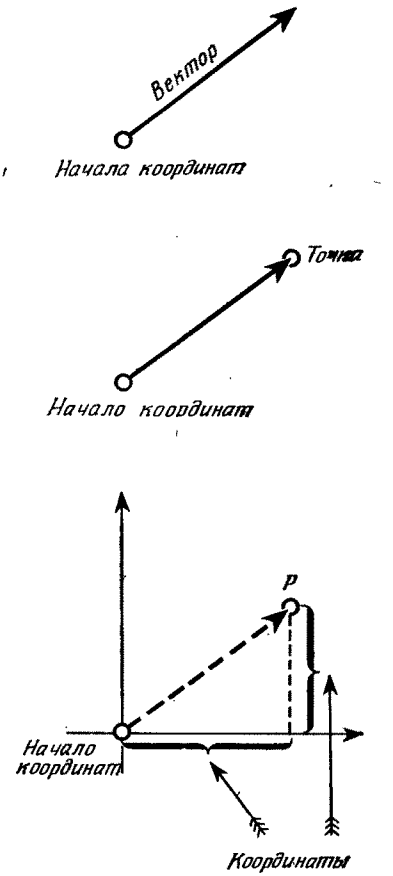
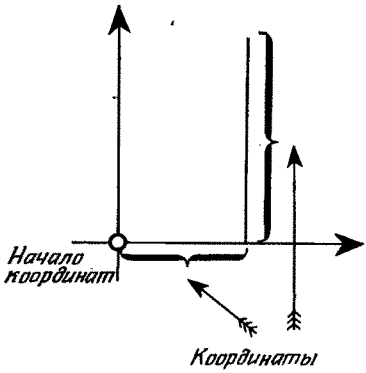
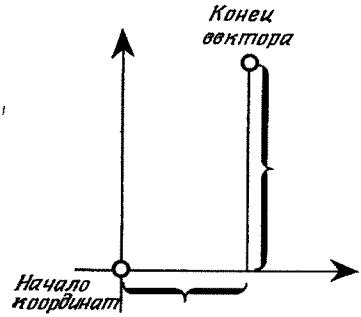


Рис. 75.

Аналогичным образом можно определять положение точек не только на плоскости, но и в пространстве. Существенного (принципиального) различия между этими двумя случаями нет.

Но уже в связи с введением координат на плоскости возникает один вопрос: какую систему координат выбрать?





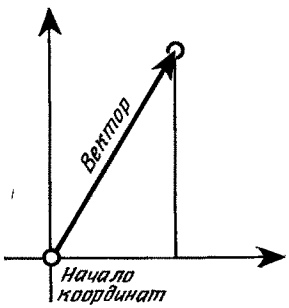
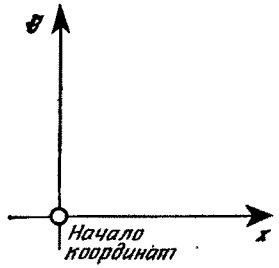


Рис. 76.



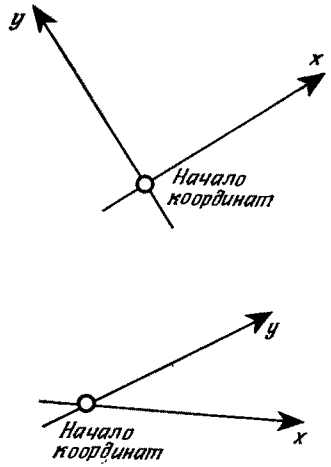


Рис. 77.

На плоскости «решающий шаг» еще кое-как можно было бы сделать, например объявить «наилучшей» прямоугольную систему координат, оси которой взаимно перпендикулярны, а координатные линии параллельны линиям обреза этой страницы (рис. 76). Прямому углу между осями координат или параллельности прямых на плоскости можно придать вполне наглядный смысл, хотя это еще не свидетельствует о превосходстве введенной системы координат перед другими (рис. 77). Несравненно труднее придать наглядный смысл аналогичным понятиям, если размерность векторного пространства больше трех, а если речь идет о векторных пространствах не над вещественными числами, то задача становится безнадежной.

Следовательно, нам не остается ничего другого, как смириться с

мыслью, что *вводить можно любые системы координат*. Важно лишь, чтобы, выбрав какую-нибудь одну систему координат, мы придерживались ее, пока не завершим вычисления: ведь одни и те же числа в различных системах координат определяют различные векторы.

В системе координат (x, y) пара чисел $(x = 2, y = 3)$ задает вектор u, а в системе координат (x', y') та же пара чисел $(x' = 2, y' = 3)$ определяет вектор u' (рис. 78). Векторы u и u' не совпадают.

Итак, мы установили, что ни одной системе координат невозможно отдать предпочтение, но, коль скоро система координат выбрана, необходимо ее зафиксировать.

Но какой смысл имеют координаты вектора в произвольной системе координат? Во всяком векторном пространстве помимо векторов имеются еще и скаляры. Если бы мы научились выражать координаты вектора через скаляры, то тем самым нам удалось бы придать смысл и координатам вектора в произвольной системе координат.

На плоскости запись вектора в координатах можно рассматривать, как представление вектора в виде суммы двух векторов. Направления векторов-слагаемых фиксированы, а длины изменяются в зависимости от вектора-суммы. Если вдоль каждой из координатных осей выбрать по единичному вектору, то координаты любого вектора на плоскости будут показывать, с какими коэффициентами выбранные единичные векторы входят в линейную комбинацию, совпадающую с этим вектором. Но два ортогональных вектора на плоскости можно рассматривать как базис, так как любой вектор на плоскости можно представить в виде их линейной комбинации.

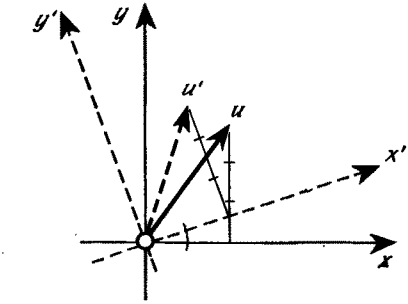


Рис. 78.

Аналогичным образом можно поступать и в других случаях, поскольку базис существует в любом конечномерном векторном пространстве.

Координаты вектора принято записывать либо одну под другой в виде столбца, либо в виде строки. (Обе формы записи по существу ничем не отличаются, но над столбцами более удобно производить выкладки. Если бы произведение однородных линейных отображений следовало понимать не как $(\mathbf{AB})(u) = \mathbf{A}(\mathbf{B}(u))$, а как $(\mathbf{AB})(u) = \mathbf{B}(\mathbf{A}(u))$, то такую запись легче было бы читать «с конца»: $(u)(\mathbf{AB}) = ((u)\mathbf{A})\mathbf{B}$, и действия было бы удобнее производить над векторами-строками.) Итак, *в заданном базисе* вектор u имеет координаты

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$ Это принято записывать так: $$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}.$$

Кратко координаты вектора u в заданном базисе обозначаются $[u]$.

Пусть $e_1, e_2, \ldots, e_n$ — фиксированный базис в n-мерном векторном пространстве M над телом Γ. Если вектор $u \in \mathrm{M}$ можно представить в виде линейной комбинации $u = \alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n$, то скаляры $\alpha_1, \alpha_2, \ldots, \alpha_n$ называются координатами вектора u в базисе $e_1, e_2, \ldots, e_n$.

Если речь идет не об одном векторе, а о нескольких векторах, имеющих различную размерность, то в обозначении вектора указывают не только координаты, но и размерность: $[u]_n$ означает координаты n-мерного вектора u.

Рассмотрим, например, элементы e и f базиса двумерного векторного пространства над телом вещественных чисел

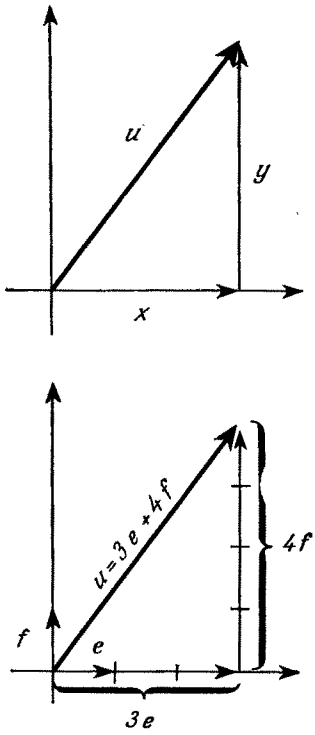


Рис. 79.

(рис. 79). Векторы $g = e + f$ и $h = e - f$ образуют другой базис того же векторного пространства. Действительно, так как $e = \frac{1}{2}(g + h)$, $f = \frac{1}{2}(g - h)$, то векторы g и h можно рассматривать как систему образующих, а поскольку эта система состоит из двух элементов, то она является базисом. Вектор $u = 4e + 6f$ имеет в базисе (e, f) координаты $\begin{bmatrix}4\\6\end{bmatrix}$ (рис. 80), а в базисе (g, h) — координаты $\begin{bmatrix}5\\-1\end{bmatrix}$ (рис. 81), так как $u = 4e + 6f =$

Рис. 80.

Рис. 81.

$= 4 \cdot (\frac{1}{2}(g + h)) + 6 (\frac{1}{2} \cdot (g - h)) = 2(g + h) + 3(g - h) = 5g - h$. Вектор v, имеющий в базисе (g, h) координаты $\begin{bmatrix}4\\6\end{bmatrix}$, отличен от вектора u (рис. 82), так как $v = 4g + 6h = 4(e + f) + 6(e - f) = 10e - 2f$.

Если в некотором базисе всем векторам сопоставить их координаты, то соответствие между векторами и координатами будет взаимно-однозначным (рис. 80). Более того, если операции над столбцами производить так же, как над наборами из n чи-

Рис. 82.

сел, то есть покомпонентно, то соответствие между векторами и координатами будет изоморфизмом. Чтобы убедиться в этом, рассмотрим, как производятся над «столбцами» операции сложения и умножения на скаляр:

$$\begin{bmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{bmatrix}+\begin{bmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{bmatrix}=\begin{bmatrix}\alpha_1+\beta_1\\ \alpha_2+\beta_2\\ \vdots\\ \alpha_n+\beta_n\end{bmatrix};$$

$$\lambda\cdot\begin{bmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{bmatrix}=\begin{bmatrix}\lambda\alpha_1\\ \lambda\alpha_2\\ \vdots\\ \lambda\alpha_n\end{bmatrix}.$$

Следовательно, если $u = \alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n$ и $v = \beta_1 e_1 + \beta_2 e_2 + \ldots + \beta_n e_n$, то $u + v = (\alpha_1 + \beta_1) e_1 + (\alpha_2 + \beta_2) e_2 + \ldots + (\alpha_n + \beta_n) e_n$ и, кроме того, $\lambda u = (\lambda\alpha_1) e_1 + (\lambda\alpha_2) e_2 + \ldots + (\lambda\alpha_n) e_n$, что и доказывает наше утверждение. Полученный нами результат можно «сформулировать» более кратко: $[u + v] = [u] + [v]$ и $[\lambda u] = \lambda[u]$.

Если этими соотношениями воспользоваться достаточное число раз, то координаты линейной комбинации векторов можно представить в виде линейной комбинации координат заданных векторов:

$$[\lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_n u_n] = \lambda_1[u_1] + \lambda_2[u_2] + \cdots + \lambda_n[u_n].$$

Перейдем теперь к описанию однородных линейных отображений. Пусть $\mathbf{A} : \mathrm{M}_1 \to \mathrm{M}_2$ — однородное линейное отображение. Как известно, любое однородное линейное отображение однозначно определено, если задано, во что оно переводит элементы базиса. Более того, было показано, что, какие бы элементы векторного пространства мы ни выбрали, всегда можно найти однородное линейное отображение, переводящее в них элементы базиса. Прежде всего зададим в векторном пространстве M_1 какой-нибудь базис, например состоящий из векторов $e_1, e_2, \ldots, e_n$. Если этот базис *фиксирован*, то любое однородное линейное отображение можно однозначно определить, указав образы базисных элементов $\mathbf{A}(e_1), \mathbf{A}(e_2), \ldots, \mathbf{A}(e_n)$. Поскольку эти образы также являются векторами, то их также можно описывать при помощи координат, но для этого в векторном пространстве M_2, которому принадлежат векторы $\mathbf{A}(e_1), \mathbf{A}(e_2), \ldots, \mathbf{A}(e_n)$, необходимо задать и фиксировать какой-нибудь базис. Пусть $f_1, f_2, \ldots, f_n$ — векторы, образующие базис в M_2. В этом базисе образы векторов $e_1, e_2, \ldots, e_n$, составляющих базис в векторном пространстве M_1, имеют координаты $[\mathbf{A}(e_1)], [\mathbf{A}(e_2)], \ldots, [\mathbf{A}(e_n)]$.

Попытаемся теперь действовать в обратном порядке. Если координаты $[\mathbf{A}(e_1)], [\mathbf{A}(e_2)], \ldots, [\mathbf{A}(e_n)]$ заданы, то тем самым в векторном пространстве M_2 однозначно определены n векторов (так как в векторном пространстве M_2 имеется фиксированный базис). Поскольку в векторном пространстве M_1 также есть фиксированный базис, то, какие бы n векторов в M_2 мы ни задали, всегда найдется такое однородное линейное отображение (и притом только одно), которое переводит элементы заданного базиса из M_1 в эти n векторов из M_2. Следовательно, задав в векторном пространстве M_2 (с фиксированным базисом!) координаты $[\mathbf{A}(e_1)], [\mathbf{A}(e_2)], \ldots, [\mathbf{A}(e_n)]$, мы однозначно определим однородное линейное отображение.

Запишем теперь координаты векторов, в которые переходят под действием этого отображения элементы базиса векторного пространства M_1. Нам понадобится двойная нумерация: один индекс поможет нам отличать координаты данного вектора, а другой укажет порядковые номера векторов. Следовательно, координаты векторов-образов элементов базиса векторного пространства M_1 зависят *от двух индексов. Первый индекс указывает порядковый номер базисного вектора, о котором идет речь, а второй индекс нумерует координаты его образа.* Итак, координаты век-

торов, в которые однородное линейное отображение $\mathbf{A}$ переводит элементы $e_1, e_2, \ldots, e_n$ базиса векторного пространства M_1, можно записать в виде

$$[\mathbf{A}(e_1)] = \begin{bmatrix} a_{11} \\ a_{12} \\ \vdots \\ a_{1n} \end{bmatrix};$$

$$[\mathbf{A}(e_2)] = \begin{bmatrix} a_{21} \\ a_{22} \\ \vdots \\ a_{2n} \end{bmatrix}; \ldots$$

$$\ldots; [\mathbf{A}(e_n)] = \begin{bmatrix} a_{n1} \\ a_{n2} \\ \vdots \\ a_{nn} \end{bmatrix}.$$

Необходимо произвести еще две проверки. Во-первых, мы должны убедиться в том, что если задано однородное линейное отображение векторного пространства M_1 в векторное пространство M_2, то (при фиксированных базисах в M_1 и M_2!) оно однозначно определяет набор $n \times k$ координат, выписанных выше. Во-вторых, требуется доказать, что, если задано $n \times k$ скаляров, упорядоченных по двум индексам, то они (также при фиксированных базисах в M_1 и M_2!) однозначно определяют однородное линейное отображение.

Числа или какие-нибудь другие элементы, записанные в определенном порядке, называются *матрицей*.

Разумеется, если речь идет о векторных пространствах над телом вещественных чисел, то элементы матрицы являются вещественными числами. Разумеется, элементы могут быть расположены в любом порядке, важно лишь, чтобы он оставался неизменным.

Если элементы расположены в виде прямоугольника, то говорят, что они образуют прямоугольную матрицу. Следовательно, однородное линейное отображение $\mathbf{A}$ в заданных базисах можно записать в виде прямоугольной матрицы:

$$|\mathbf{A}| = \begin{bmatrix} a_{11} & a_{21} & \ldots & a_{n1} \\ a_{12} & a_{22} & \ldots & a_{n2} \\ \vdots & \vdots & & \vdots \\ a_{1k} & a_{2k} & \ldots & a_{nk} \end{bmatrix}.$$

В этой связи необходимо заметить следующее: *для линейных преобразований* векторные пространства M_1 и M_2 совпадают. В принципе и в этом случае следовало бы задавать два базиса: один базис — для записи образов векторов, другой — для записи координат, но оба базиса удобно отождествлять и *вместо двух базисов рассматривать лишь один*.

Приведем теперь несколько примеров однородных линейных отображений, записанных в виде матриц.

ПРИМЕРЫ

1. Некоторые линейные преобразования плоскости. (Мы рассмотрим лишь те линейные преобразования, которые были перечислены выше, как примеры однородных линейных отображений.)

а) Отражение относительно прямой.

Для любых не параллельных векторов u, v на плоскости линейное преобразование $\mathbf{A}$, действующее так, что $\mathbf{A}(u) = -u$ и $\mathbf{A}(v) = -v$, определяет некоторую матрицу. Представив образ вектора u в виде $(-1)\cdot u + 0\cdot v$, мы получим первый столбец матрицы $\begin{pmatrix} -1 \\ 2 \end{pmatrix}$. Записав образ вектора v в виде линейной комбинации $0\cdot u + (-1)\cdot v$, мы найдем второй столбец матрицы $\begin{pmatrix} 0 \\ -1 \end{pmatrix}$. Итак, $[\mathbf{A}] = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$.

б) Отражение относительно прямой, проходящей через начало координат.

Если u — вектор, направленный вдоль прямой, а v — вектор, ортогональный вектору u, то преобразование $\mathbf{A}$ действует так, что $\mathbf{A}(u) = u$, а $\mathbf{A}(v) = -v$. Образ вектора u можно представить в виде линейной ком-

бинации $1 \cdot u + 0 \cdot v$, а образ вектора v — в виде линейной комбинации $0 \cdot u + (-1) \cdot v$. Следовательно, матрица линейного преобразования $\mathbf{A}$ состоит из двух столбцов $\binom{1}{0}$ и $\binom{0}{-1}$, то есть $[\mathbf{A}] = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

в) Растяжение от центра.

В качестве базиса на плоскости можно выбрать любые два непараллельных вектора u и v. Линейное преобразование $\mathbf{A}$ состоит в растяжении всех векторов в α раз, поэтому $\mathbf{A}(u) = \alpha \cdot u + 0 \cdot v$, $\mathbf{A}(v) = 0 \cdot u + \alpha \cdot v$ и, следовательно, $[\mathbf{A}] = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$.

г) Растяжение в направлении, перпендикулярном прямой, проходящей через начало координат.

Если «коэффициент растяжения» равен α, u — вектор, направленный вдоль прямой, а v — вектор, ортогональный прямой, то линейное преобразование $\mathbf{A}$ действует так, что $\mathbf{A}(u) = 1 \cdot u + 0 \cdot v$, $\mathbf{A}(v) = 0 \cdot u + \alpha \cdot v$ и, таким образом, $[\mathbf{A}] = \begin{bmatrix} 1 & 0 \\ 0 & \alpha \end{bmatrix}$.

д) Поперечный сдвиг.

Если u — вектор, указывающий направление сдвига, а v — вектор, ортогональный вектору u, то поперечный сдвиг порождает линейное преобразование $\mathbf{A}(u) = u$, $\mathbf{A}(v) = v + \mu u$ с матрицей $[\mathbf{A}] = \begin{bmatrix} 1 & \mu \\ 0 & 1 \end{bmatrix}$. (Заметим, что это первая матрица, в которой элементы в «правом верхнем углу» не симметричны элементам в «левом нижнем углу» относительно так называемой главной диагонали.)

е) Поворот.

Если $\mathbf{F}$ — поворот вокруг начала координат на 90° в положительном направлении, а u, v — такие ортогональные векторы, что $\mathbf{F}(u) = v$, $\mathbf{F}(v) = -u$, то $[\mathbf{F}] = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Если $\mathbf{F}$ — поворот вокруг начала координат на 120° в положительном направлении и $v = \mathbf{F}(u)$, то $\mathbf{F}(v) = -u + (-1) \cdot v$ и $[\mathbf{F}] = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$. Следует иметь в виду, что при описании поворота на 120° мы воспользовались базисом, весьма точно «подогнанным» к преобразованию, но порождающим несколько непривычную систему координат. Если бы вектор v получался из вектора u при повороте вокруг начала координат на 90° в положительном направлении, то в этом базисе, как нетрудно проверить, линейному преобразованию, соответствующему повороту вокруг начала координат на 120° в положительном направлении, соответствовала бы матрица

$$\begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}.$$

ж) Ортогональная проекция.

В базисе u, v, приведенном в примере 8, ортогональная проекция порождает линейное преобразование $\mathbf{V}(u) = u$, $\mathbf{V}(v) = 0$. Следовательно, его матрица имеет вид $[\mathbf{V}] = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.

2. Тождественное линейное преобразование векторного пространства. Если $u_1, u_2, \ldots, u_n$ — произвольный базис, то тождественное линейное преобразование действует так, что $\mathbf{I}(u_1) = u_1$, $\mathbf{I}(u_2) = u_2$, ..., $\mathbf{I}(u_n) = u_n$. Это означает, что в матрице $\mathbf{I}$ (независимо от базиса) в первом столбце первый элемент равен единице, а остальные — нулю, во втором столбце на втором месте стоит единица, а все остальные элементы равны нулю, и, наконец, в последнем столбце на последнем месте стоит единица, а на всех предыдущих — нули. Те места, на которых стоят единицы, называются *главной диагональю* матрицы. Разумеется, главной диагональю обладают лишь матрицы, в которых число столбцов совпадает с числом элементов в столбцах. Такие матрицы называются *квадратными*.

3. Нулевое отображение $\mathbf{O}$. Если при отображении n-мерного векторного пространства $\mathbf{M}_1$

в k-мерное векторное пространство M_2 каждый вектор из M_1 переходит в нулевой вектор из M_2, то при любом выборе базиса в M_1 всем его элементам будет соответствовать нулевой вектор в M_2. Следовательно, матрица нулевого отображения **O** содержит n столбцов, в каждом из которых все k элементов равны нулю. Таким образом, независимо от выбора базиса все элементы матрицы нулевого отображения **O** всегда равны нулю.

Если матрица однородного линейного отображения известна, то, зная координаты исходного вектора, можно найти координаты его образа при отображении. Предполагается, что исходный вектор и однородное линейное отображение заданы в одном и том же базисе. Тогда образ вектора задан во «втором» базисе однородного линейного отображения.

Пусть $\mathbf{A} : M_1 \to M_2$ — однородное линейное отображение, e_1, e_2,... ..., e_n — базис векторного пространства M_1, а f_1, f_2, ..., f_k — базис векторного пространства M_2. Если $u = \xi_1 e_1 + \xi_2 e_2 + \ldots + \xi_n e_n$ — исходный вектор, то $v = \mathbf{A}(u) = \xi_1 \mathbf{A}(e_1) + \xi_2 \mathbf{A}(e_2) + \ldots + \xi_n \mathbf{A}(e_n)$ — образ вектора v при отображении **A**. Координаты вектора v можно найти, зная координаты векторов $\mathbf{A}(e_i)$:

$$[v] = \xi_1 [\mathbf{A}(e_1)] + \xi_2 [\mathbf{A}(e_2)] + \ldots + \xi_n [\mathbf{A}(e_n)].$$

Первую координату вектора v мы найдем, взяв первые координаты векторов $\mathbf{A}(e_1)$, $\mathbf{A}(e_2)$,...,$\mathbf{A}(e_n)$, умножив их на ξ_1, ξ_2,..., ξ_n (координату вектора $\mathbf{A}(e_i)$ на ξ_i) и сложив полученные произведения. Аналогичным образом можно найти вторую координату вектора v (необходимо лишь вместо первых координат векторов $\mathbf{A}(e_1)$, $\mathbf{A}(e_2)$,...,$\mathbf{A}(e_n)$ взять их вторые координаты). Продолжая вычисления, мы, наконец, найдем k-ю координату вектора v (проделав соответствующие действия над k-ми координатами векторов ($\mathbf{A}(e_1)$, $\mathbf{A}(e_2)$,.. $\mathbf{A}(e_n)$.

Выясним, нельзя ли алгоритм отыскания координат вектора v сформулировать проще. Внимательно рассмотрев всю последовательность действий, нетрудно заметить, что для вычисления первой координаты вектора v необходимо учитывать только первые координаты векторов $\mathbf{A}(e_i)$. Эти координаты образуют первую *строку* матрицы [A]. Аналогичным образом при вычислении второй координаты вектора v нам понадобится лишь вторая строка матрицы однородного линейного отображения **A**, а при вычислении k-й координаты вектора v — лишь k-я строка той же матрицы.

Рассмотрим элементы первой строки матрицы [A], понадобившиеся при вычислении первой координаты вектора v: α_{11}, α_{21}, ..., α_{n1}. Первая координата вектора v равна сумме $\alpha_{11}\xi_1 + \alpha_{21}\xi_2 + \ldots + \alpha_{n1}\xi_n$. В аналогичном виде представимы и другие координаты вектора v. Единственное отличие от первой координаты состоит в том, что второй индекс элементов матрицы [A] равен не единице, а натуральному числу, заключенному между 2 и k.

Рассмотрим, как образуются такие суммы. Пусть заданы строка и столбец, содержащие одно и то же число элементов. Умножим первый элемент строки на первый элемент столбца, второй элемент строки — на второй элемент столбца и т. д., последний элемент строки умножим на последний элемент столбца, а произведения сложим.

Полученная сумма называется *произведением выбранных нами строки и столбца*. Координаты вектора $\mathbf{A}(v)$ можно описать в терминах произведений строк и столбцов следующим образом: умножив каждую строку матрицы [A] на координаты вектора v, записанные в виде столбца, получим соответствующую координату вектора-образа $\mathbf{A}(v)$.

Произведение строки и столбца

$$[\alpha_1, \alpha_2, \ldots, \alpha_n] \begin{bmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{bmatrix} = \alpha_1\xi_1 + \alpha_2\xi_2 + \ldots + \alpha_n\xi_n.$$

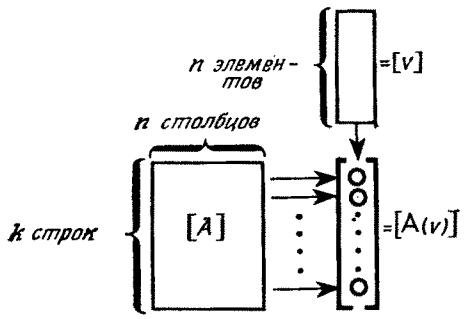


Рис. 83.

На рис. 83 произведения строк и столбца отмечены кружками и располагаются на пересечении прямых, указанных стрелками.

Рассмотрим теперь, как выглядят «в переводе» на язык матриц операции, производимые над однородными линейными отображениями.

1. Произведение матрицы на скаляр.

Матрицу $[\lambda A]$ определим по аналогии с матрицей $[A]$. Если $e_1, e_2, \ldots, e_n$ — соответствующий базис, то матрица $[A]$ состоит из столбцов $[A(e_1)]$, $[A(e_2)]$, ..., $[A(e_n)]$, а столбцы матрицы $[\lambda A]$ имеют вид $[\lambda A(e_1)] = \lambda[A(e_1)]$, $[\lambda A(e_2)] = \lambda[A(e_2)]$, ..., $[\lambda A(e_n)] = \lambda[A(e_n)]$.

Это означает, что матрица $[\lambda A]$ получается из матрицы $[A]$ при умножении всех элементов матрицы $[A]$ на λ.

Удобно принять следующее определение: чтобы найти произведение матрицы на скаляр, все элементы матрицы следует умножить на скаляр.

Такое определение позволяет утверждать, что скалярное кратное матрицы равно произведению матрицы на скаляр. Более точно наш результат можно было бы сформулировать следующим образом: скалярное кратное матрицы и произведение матрицы на скаляр удовлетворяют соотношению $[\lambda A] = \lambda[A]$.

2. Сумма матриц.

Говоря о сложении однородных линейных отображений $\mathbf{A}$ и $\mathbf{B}$, мы подразумеваем, что отображение $\mathbf{A} + \mathbf{B}$ существует. По определению матрицы $[A]$ ее j-й столбец состоит из координат вектора $\mathbf{A}(e_j)$, то есть равен $[\mathbf{A}(e_j)]$. Аналогично j-й столбец матрицы $[\mathbf{B}]$ равен $[\mathbf{B}(e_j)]$. Используя уже известные соотношения, получаем, что j-й столбец матрицы $[\mathbf{A} + \mathbf{B}]$ равен $[(\mathbf{A} + \mathbf{B})(e_j)] = [\mathbf{A}(e_j) + \mathbf{B}(e_j)] = [\mathbf{A}(e_j)] + [\mathbf{B}(e_j)]$. Это означает, что j-й столбец матрицы $[\mathbf{A} + \mathbf{B}]$ совпадает с суммой j-х столбцов матриц $[A]$ и $[B]$. (Сумму столбцов мы получим, сложив покомпонентно столбцы-слагаемые.) Следовательно, каждый элемент матрицы $[\mathbf{A} + \mathbf{B}]$ можно найти, вычислив сумму элементов матриц $[A]$ и $[B]$, стоящих «на том же месте]».

Итак, сумму матриц разумно *определить* следующим образом.

Пусть заданы две матрицы с одинаковым числом строк и столбцов. Их суммой называется матрица, в которой j-й элемент i-й строки (то

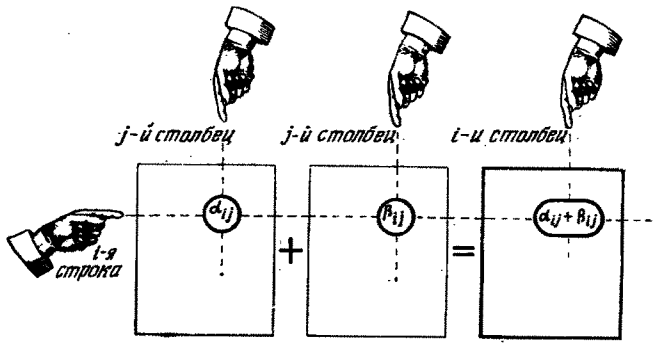


Рис. 84.

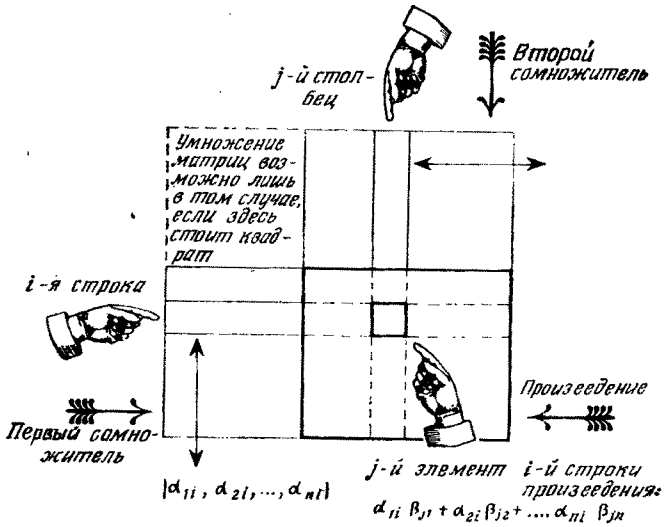


Рис. 85.

есть элемент, стоящий на пересечении i-й строки и j-го столбца) равен сумме j-х элементов i-х строк матриц-слагаемых (рис. 84).

Суммой двух матриц называется матрица, в которой элемент, стоящий на пересечении i-й строки и j-го столбца, равен сумме элементов, стоящих на пересечении i-х строк и j-х столбцов в матрицах-слагаемых.

При таком определении выполняется соотношение $[A + B] = [A] + [B]$.

3. Произведение матриц.

Введем операцию умножения матриц. Ее определение желательно выбрать так, чтобы матрица произведения двух однородных линейных отображений совпадала с произведением матриц, соответствующих отображениям-сомножителям.

Предположим, что заданы однородные линейные отображения A: $M_2 \to M_3$ и B: $M_1 \to M_2$ и существует однородное линейное отображение AB: $M_1 \to M_3$. Если мы хотим записать матрицы отображений, то во всех трех векторных пространствах M_1, M_2 и M_3 необходимо указать базисы. Конкретно нас будет интересовать только базис в M_1. Пусть $e_1, e_2, \ldots, e_n$ — элементы этого базиса. Найти j-й элемент i-й строки матрицы [AB] означает то же самое, что и найти i-й элемент ее j-го столбца. Но j-й столбец матрицы [AB] мы получим без труда. Это — не что иное, как столбец $[AB(e_j)]$. Выясним, как он связан с матрицей [A]. Для этого столбец $[AB(e_j)]$ удобно представить в виде $[A(B(e_j))]$. Из этой записи следует, что i-й элемент столбца $[AB(e_j)]$ мы получим, умножив i-ю строку матрицы [A] на столбец, состоящий из координат вектора $B(e_j)$. Но вектор $B(e_j)$ — это не что иное, как j-й столбец матрицы [B] (рис. 85).

Итак, можно утверждать, что элемент матрицы [AB], стоящий на пересечении i-й строки и j-го столбца, совпадает с произведением i-й строки матрицы [A] и j-го столбца матрицы [B].

Следовательно, произведение матрицы разумно определить так: если число строк первой матрицы равно числу столбцов второй матрицы, то, перемножив их (именно в том порядке, в котором матрицы перенумерованы!), мы получим матрицу, в которой j-й элемент i-й строки совпадает с произведением i-й строки первой матрицы и j-го столбца второй матрицы.

Произведением двух матриц называется матрица, у которой j-й элемент i-й строки совпадает с произведением i-й строки первой матрицы и j-го столбца второй матрицы.

При таком определении соотношение $[AB] = [A][B]$, как нетрудно видеть, выполняется.

ЗАДАЧИ

1. Указать те из перечисленных ниже матриц, для которых операция сложения имеет смысл:

0) $[1 \quad 3 \quad -2]$;

1) $\begin{bmatrix} 4 & 0 & 3 \\ 2 & -3 & 4 \end{bmatrix}$;

2) $\begin{bmatrix} -3 & -2 & 17 \\ 15 & -7 & -1 \\ 4 & 5 & 0 \end{bmatrix}$;

3) $\begin{bmatrix} 3 & -1 & 5 \\ -2 & 3 & -4 \end{bmatrix}$;

4) $[5 \quad -3 \quad 4]$;

5) $\begin{bmatrix} 3 \\ -5 \\ 11 \end{bmatrix}$;

6) $\begin{bmatrix} 4 & -11 \\ -3 & 0 \\ -1 & 7 \end{bmatrix}$;

7) $\begin{bmatrix} -7 & 13 & 41 \\ 13 & -1 & 0 \\ 0 & -5 & 13 \end{bmatrix}$;

8) $\begin{bmatrix} -4 & 13 \\ 7 & -2 \\ 1 & -1 \end{bmatrix}$;

9) $\begin{bmatrix} 2 \\ 7 \\ -2 \end{bmatrix}$.

2. Указать те из перечисленных в предыдущей задаче матриц, которые можно умножать одну на другую.

3. Доказать, что для любого линейного преобразования плоскости либо существует базис, в котором матрица преобразования имеет вид $\begin{bmatrix} 0 & a \\ b & c \end{bmatrix}$, либо во всяком базисе матрица преобразования имеет вид $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$.

4. Пусть в некотором базисе матрица линейного преобразования $\mathbf{A}$ плоскости имеет вид $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ и, кроме того, $p = a + d$ и $q = ad - bc$. Доказать, что $\mathbf{A}^2 - p \cdot \mathbf{A} + q \cdot \mathbf{I} = \mathbf{O}$.

4

Группы и кольца

4.1. Представление групп матрицами

Решая задачи о линейных преобразованиях, мы выяснили, при каких условиях для данного линейного преобразования существует обратное линейное преобразование. Поскольку преобразование, обратное произведению преобразований, совпадает с произведением (взятых в обратном порядке) обратных преобразований, то невырожденные (то есть такие, для которых существуют обратные) преобразования образуют группу по умножению. Такие линейные преобразования можно представить (если задан базис) квадратными матрицами. Следовательно, те квадратные матрицы, для которых существуют обратные, образуют группу относительно операции умножения матриц. Такие матрицы в дальнейшем мы будем называть невырожденными.

Вычисления с матрицами производятся сравнительно просто и совершенно «автоматически». Именно поэтому групповые операции проще изучать на группах, состоящих из матриц. Подобно тому как элементы групп мы некогда заменяли подстановками, теперь же их можно попытаться заменить матрицами. Точнее говоря, речь идет об установлении следующего соответствия между элементами групп и матрицами.

Если существует мономорфизм φ, *отображающий данную группу* G *в мультипликативную группу невырожденных матриц* $n \times n$, *то говорят, что группа* G *представима матрицами* $n \times n$, *а гомоморфизм* φ *называется представлением группы* G *матрицами* $n \times n$.

Заметим, что когда говорят о представлениях групп (имеющих весьма важное значение), то о φ известно лишь, что это — гомоморфизм. Те представления, в которых φ — мономорфизм, обычно на-

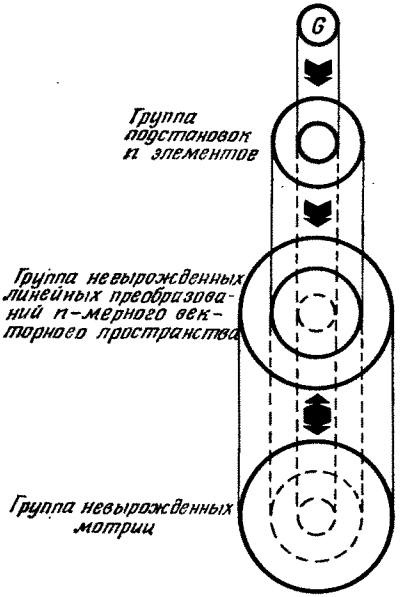


Рис. 86.

зываются «*точными представлениями*». Поскольку мы будем в дальнейшем рассматривать только такие представления, то условимся для краткости называть их просто представлениями и опускать слово «точные».

Докажем, что всякую группу n-го порядка можно представить матрицами $n \times n$.

Для доказательства этого утверждения весьма полезной оказывается теорема Кэли, согласно которой группа, содержащая n элементов, изоморфна некоторой подгруппе группы всех подстановок n элементов. Используя теорему Кэли, достаточно было бы доказать, что всякая группа подстановок изоморфна некоторой подгруппе невырожденных матриц $n \times n$. Тогда исходная группа была бы изоморфна некоторой подгруппе группы матриц, поскольку, если группа изоморфна какой-нибудь подгруппе любой из подгрупп, то она тем самым изоморфна и подгруппе всей группы (рис. 86).

Но от матриц $n \times n$ мы могли бы перейти к линейным преобразованиям n-мерного векторного пространства, поэтому достаточно рассмотреть мономорфизм φ, ставящий в соответствие каждой подстановке некоторое невырожденное линейное преобразование n-мерного линейного пространства.

Пусть $e_1, e_2, \ldots, e_n$ — базис заданного n-мерного векторного пространства. Не ограничивая общности, можно считать, что любая подстановка n элементов действует именно на векторах $e_1, e_2, \ldots, e_n$. Каждому элементу базиса e_i поставим в соответствие тот элемент базиса e_j, в который вектор e_i переходит под действием рассматриваемой подстановки. Но коль скоро для каждого элемента базиса известен его образ, то тем самым однозначно определено однородное линейное отображение, переводящее векторы e_i в их образы относительно подстановки.

Однозначное соответствие между подстановками и однородными линейными отображениями допускает более точное описание. Пусть P — произвольная подстановка базисных векторов $e_1, e_2, \ldots, e_n$. Подстановке P соответствует линейное преобразование A_P, для которого при всех $i \leqslant n$ выполняются условия $A_P(e_i) = P(e_i)$. Покажем, что φ: $P \to A_P$ — мономорфизм, отображающий группу подстановок в группу невырожденных линейных преобразований.

Прежде всего заметим, что φ — отображение, поскольку образы базисных векторов относительно подстановки P однозначно определяют линейное преобразование A_P. Ясно, что различным подстановкам соответствуют различные линейные преобразования. Действительно, два линейных преобразования, соответствующих различным подстановкам, не могут совпадать хотя бы потому, что среди элементов базиса заведомо найдется по крайней мере один вектор, переходящий под действием этих преобразований в различные векторы. Не представляет особого труда и доказательство того, что φ сохраняет операции. Линейное преобразование A_{PQ}, соответствующее произведению подстановок PQ, переводит базисный вектор e_i в базисный вектор $A_{PQ}(e_i) = PQ(e_i)$. С другой стороны, произведение линейных преобразований A_P и A_Q, соответствующих подстановкам P и Q, переводит базисный вектор e_i в вектор $A_P A_Q(e_i) = A_P(Q(e_i)) = P(Q(e_i))$. Нетрудно видеть, что вектор $P(Q(e_i))$ совпадает с вектором $PQ(e_i)$.

Остается еще доказать, что все линейные преобразования, соответствующие подстановкам, невырожденны. Убедиться в этом нетрудно. Действительно, каждая подстановка отображает базис на базис. Таким образом, при линейном преобразовании все элементы базиса оказываются образами каких-то элементов базиса. Следовательно, образ преобразования содержит

все элементы базиса и поэтому совпадает со всем векторным пространством. Но именно это и означает, что преобразование невырожденно.

В качестве примера найдем представление группы подстановок третьего порядка матрицами 3×3. Тождественная подстановка переводит все элементы в самих себя. Следовательно, соответствующее ей линейное преобразование также отображает все элементы в себя, то есть является тождественным. Подстановка (123) переводит e_1 в e_2, поэтому и соответствующее ей линейное преобразование отображает вектор e_1 в вектор e_2. Следовательно, в первом столбце матрицы этого преобразования на втором месте стоит единица ($e_2 = 1 \cdot e_2$), а на всех остальных местах — нули (коэффициенты образа вектора e_1 при всех остальных базисных векторах равны нулю). Та же подстановка (123) переводит e_2 в e_3, поэтому соответствующее ей линейное преобразование отображает вектор e_2 в вектор e_3. Это означает, что во втором столбце матрицы преобразования на третьем месте стоит единица, а на всех остальных местах — нули. Наконец, как показывают аналогичные рассуждения, в третьем столбце матрицы преобразования первый элемент равен единице, а два остальных — нулю. Пользуясь тем же методом, найдем матрицы преобразований, соответствующих всем шести подстановкам трех элементов:

$$\text{тождественная подстановка} \leftrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

$$(123) \leftrightarrow \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix};$$

$$(132) \leftrightarrow \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}; \quad (12) \leftrightarrow \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

$$(13) \leftrightarrow \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}; \quad (23) \leftrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

В общем случае в таком представлении матрицы содержат «слишком много» строк (и столбцов). Нередко группу удается представить матрицами с меньшим числом элементов. Имеются основания полагать, что каким-нибудь другим способом число «абсолютно необходимых элементов» удастся еще более понизить. (Такое действительно возможно, поскольку каждая из матриц содержит много элементов, равных нулю, а они «не идут в счет» при выполнении операций.) Следовательно, занимаясь поисками представлений групп, важно строить матрицы с наименьшим из возможных числом элементов.

Например, для представления группы второго порядка не обязательно обращаться к матрицам 2×2. Представление этой группы можно построить, поставив в соответствие образующему элементу число -1. Этот элемент имеет порядок, равный 2, и мы получаем представление группы «матрицами» 1×1. Чтобы получить представление группы третьего порядка, не обязательно брать матрицы 3×3. Действительно, матрица $\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$ в кубе совпадает с единичной матрицей $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Следовательно, сопоставив образующему элементу группы матрицу $\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$, мы получим представление группы третьего порядка матрицами 2×2.

Если образующему элементу группы третьего порядка поставить в соответствие комплексное число z, куб которого равен 1 ($z = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$), то получится представление группы «матрицами» 1×1. Этот пример показывает, что «величина» представления зависит от того, над каким телом рассматривать матрицы. (Ясно, что построить представление группы третьего порядка вещественными числами нам бы не удалось, так как не существует отличного от единицы вещественного числа, куб которого был бы равен единице.)

ЗАДАЧИ

1. Доказать, что все группы четвертого порядка можно представить матрицами 2×2.

2. Доказать, что группу пятого порядка можно представить матрицами 2×2, причем образующему элементу будет соответствовать матрица $\begin{bmatrix} 0 & 1 \\ 1 & a \end{bmatrix}$.

3. Доказать, что любую (конечную) циклическую группу можно представить матрицами 2×2 с вещественными элементами.

4.2. Групповые алгебры

При рассмотрении представлений групп матрицами мы сталкиваемся с весьма интересной ситуацией. Если группа изоморфна некоторой подгруппе матриц, то с алгебраической точки зрения она неотличима от этой подгруппы матриц, тождественна ей. Но на множестве матриц помимо групповой операции (умножения матриц) определены еще операции умножения матриц на скаляры и сложения. Это позволяет придать смысл таким понятиям, как произведение элемента группы и скаляра или сумма двух элементов группы. Разумеется, результат выполнения дополнительных (по отношению к групповой операции — умножению) операций не обязательно должен принадлежать группе и в большинстве случаев не принадлежит ей. Дополнительные операции, как правило, «выводят» из группы. «Незамкнутость» группы относительно сложения элементов и умножения их на скаляры означает, что, перебирая произведения элементов группы и скаляров и образуя из них всеми возможными способами суммы, мы получаем элементы более широкого (по сравнению с исходной группой) кольца.

Матрицы «неудобны» лишь тем, что определенные «линейные комбинации» элементов группы иногда совпадают с одним из элементов группы. В том, что такие случаи могут представиться, нас убеждает, например, группа невырожденных матриц. Если возврат к элементам исходной группы желательно исключить, то операции сложения элементов группы и умножения их на скаляры целесообразно рассматривать, минуя представление групп матрицами. Схема получения «новых» элементов, неоднократно опробованная нами в других случаях, сводится к следующему.

Сосредоточим внимание не на результатах выполнения операций, а на «конструировании» новых элементов. Нас будут интересовать элементы, которые не могут не возникать под действием дополнительных операций. «Синтезируя» новые элементы, мы ограничимся только самым необходимым, то есть будем продолжать пополнение их запаса лишь до тех пор, пока не получим из новых элементов элемент, встречавшийся нам ранее. На множестве построенных элементов дополнительные операции определены, поскольку они заведомо порождают лишь «допустимые» элементы (предполагается, что при построении новых элементов мы строго придерживались правил и нигде не ошибались). Описанная выше схема применима к произвольным группам, но мы рассмотрим ее лишь для конечных групп.

Если G — конечная группа с элементами $g_1, g_2, \ldots, g_n$, то одна операция (умножение) на G уже задана. Мы хотим, кроме групповой операции, ввести на G умножение на элементы некоторого тела Γ и сложение произведений элементов из G и из Γ, то есть образовать элементы вида $\alpha_1 g_1 + \alpha_2 g_2 + \ldots + \alpha_n g_n$, где $\alpha_1, \alpha_2, \ldots, \alpha_n$ — элементы тела Γ. Если бы такие «суммы произведений» были определены, то в силу дистрибутивности и ассоциативности групповой операции в G мы могли бы не только умножать их на скаляры и производить сложение, но и умножать одну «линейную комбинацию» элементов группы G на другую, оставаясь во множестве «сумм произве-

дений» элементов из G и элементов из Γ. Именно поэтому, дойдя до «линейных комбинаций», мы обрываем построение «новых» элементов. Итак, рассмотрим элементы вида $\alpha_1 g_1 + \alpha_2 g_2 + \ldots + \alpha_n g_n$, где $g_i \in G$, $\alpha_i \in \Gamma$. Множество всех таких элементов (не только «готовых», но и тех, которые можно получить, применяя к уже построенным элементам операции умножения на скаляр и сложения) обозначим (Γ; G). Будем пока считать, что элементы множества (Γ; G) заданы.

(Строго говоря, мы не можем ставить между элементами из (Γ; G) знак «плюс», поскольку это не сложение: операция сложения на (Γ; G) *еще не определена*. Тем не менее мы обозначаем неизвестную операцию как сложение именно потому, что *хотим*, чтобы она была сложением. Выбор знака «плюс» для обозначения этой операции выражает наши «чаяния».)

Введем на элементах множества (Γ; G) операции. Сначала выясним, какие операции нам следовало бы задать на (Γ; G), а затем — как это можно сделать. Речь идет о трех операциях: об умножении на скаляры, о сложении и об умножении элементов. Эти операции нам *хотелось бы* определить так, чтобы выполнялось как можно больше «хороших тождеств». С учетом наших «пожеланий» операции целесообразно задать следующим образом (более того, это — единственный способ задать операции умножения на скаляр, сложения и умножения элементов с соблюдением максимального числа тождеств).

Если $u = \alpha_1 g_1 + \alpha_2 g_2 + \ldots + \alpha_n g_n \in (\Gamma; G)$ и $\lambda \in \Gamma$, то пусть $\lambda u = (\lambda\alpha_1) g_1 + (\lambda\alpha_2) g_2 + \ldots + (\lambda\alpha_n) g_n$. Если множество ($\Gamma$; G) содержит помимо u еще один элемент $v = \beta_1 g_1 + \beta_2 g_2 + \ldots + \beta_n g_n$, то пусть $(u + v) = (\alpha_1 + \beta_1) g_1 + (\alpha_2 + \beta_2) g_2 + \ldots + (\alpha_n + \beta_n) g_n$. Труднее определить произведение двух элементов множества (Γ; G), поскольку групповая операция (умножение) в G не задана конкретно. Именно поэтому целесообразно ввести следующее определение. Образуем все выражения вида $\alpha_i \beta_j g_i g_j$. Рассмотрим те члены, в которых произведение $g_i g_j$ совпадает с фиксированным элементом g_k группы G. Коэффициенты при элементе g_k группы G будут произведениями вида $\alpha_i \beta_j$. (Разумеется, такие выражения, как «коэффициенты», «члены» и «выражения», мы употребляем здесь лишь в переносном смысле.)

Итак, операции на множестве (Γ; G) определены. Следовательно, «принципиальные» трудности преодолены. Но остались еще трудности «практические», связанные с доказательством тождеств, которым удовлетворяют введенные нами операции. «Нетрудно видеть», что большинство тождеств выполняются. Тем не менее строгое доказательство тождеств достаточно сложно, поскольку они должны относиться не к конкретному, заранее заданному числу членов, а к выражениям, содержащим любое число членов. Именно поэтому мы не будем приводить здесь доказательства тождеств, а ограничимся лишь тем, что перечислим их. Ясно, что, задав на множестве (Γ; G) умножение на скаляры и сложение, мы получим векторное пространство. Операция умножения элементов определена так, что умножение дистрибутивно относительно сложения как слева, так и справа. Пользуясь этим свойством умножения, а также ассоциативностью группового умножения, можно доказать, что умножение элементов из (Γ; G) ассоциативно. Аналогичным образом можно убедиться в том, что выполняется тождество $\lambda(u \cdot v) = (\lambda u)v = u(\lambda v)$.

Наконец, необходимо проверить, удалось ли нам получить то, что хотелось. Сделать это можно следующим образом. Для каждого элемента g_i группы G рассмотрим тот элемент u_i множества (Γ; G), в который g_i входит с коэффициентом, равным единице, а остальные элементы группы G — с коэффициентами, равными нулю. Элементы u_i образуют группу по

умножению, а соответствие $u_i \longleftrightarrow g_i$ устанавливает изоморфизм этой группы и группы G. С другой стороны, для элементов u_i выполняется соотношение

$$(\alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_n g_n) = \\ = \alpha_1 \cdot u_1 + \alpha_2 \cdot u_2 + \cdots + \alpha_n \cdot u_n.$$

Для таких равенств умножение справа на скаляр совпадает с введенной нами операцией умножения на скаляр, а сложение — с определенной на (F; G) операцией сложения. Следовательно, множество (F; G) состоит если не из линейных комбинаций элементов группы G, то из линейных комбинаций элементов группы, изоморфной группе G. Поскольку обе группы изоморфны, то «в сущности» речь идет о линейных комбинациях, образованных из элементов заданной группы.

Множество (F; G) с тремя заданными на нем операциями (группового умножения, умножения элементов группы G на скаляры из F и сложения элементов из G) называется групповой алгеброй группы G над телом F.

Три операции, входящие в определение групповой алгебры, мы умеем выполнять на множестве линейных преобразований векторного пространства, или, что то же, на множестве матриц $n \times n$. Кроме того, в этом случае выполняются все необходимые тождества. Множество (F; G), на котором три операции, входящие в определение групповой алгебры, удовлетворяют полному набору тождеств, называется *алгеброй*.

Кольцо A называется алгеброй над телом F, если аддитивная группа A является векторным пространством над F и, кроме того, при любом $\lambda \in F$ и любых элементах u и v из A выполняется тождество $\lambda(uv) = (\lambda u)v = u(\lambda v)$.

Нетрудно доказать следующее. Если в алгебре, рассматриваемой как векторное пространство, задан базис и определено умножение для элементов базиса, то операцию умножения можно однозначно определить для любых двух элементов алгебры. Поэтому при проверке ассоциативности умножения достаточно убедиться в том, что на элементах базиса умножение ассоциативно. Таким образом, ассоциативность умножения в групповой алгебре является прямым следствием ассоциативности умножения в группе.

Рассмотрим несколько важных примеров алгебр.

ПРИМЕРЫ

1. Полугрупповая алгебра. Если «формальные линейные комбинации» с коэффициентами из заданного тела составить не из элементов группы, а из элементов полугруппы, то на множестве таких линейных комбинаций можно задать такие же операции, какие определены в групповой алгебре. Тождества для операций также выполняются, поскольку умножение в полугруппе ассоциативно.

Относительно полугрупповых алгебр нам бы хотелось сделать два замечания.

Во-первых, построение полугрупповой (групповой) алгебры можно начать с бесконечной полугруппы (группы). Разумеется, в этом случае «линейные комбинации» надлежит определить так, чтобы они содержали лишь конечное число членов. Но зато для таких «укорочеиных» линейных комбиниаций выполнимы все заданные на алгебре операции и остаются в силе соответствующие тождества.

Во-вторых, полугрупповую алгебру можно рассматривать как свободную алгебру над заданной полугруппой. Произведения элементов свободной полугруппы не удовлетворяли никаким другим тождествам, кроме «самых необходимых». Аналогично обстоит дело и с полугрупповыми алгебрами. Между элементами полугрупповой алгебры нет никаких зависимостей, кроме той, что они образуют полугруппу по умножению. (Иначе говоря, сложение и умножение на скаляры не порождают «новых» зависимостей между элементами подгруппы. Действительно, элементы полугруппы должны быть линейно независимыми и (если они порождают «все») образовывать базис полугрупповой алгебры. Но именно так мы и строили полугрупповую алгебру.)

2. Кольцо многочленов. Пусть свободная полугруппа с единицей порождена одним элементом x. Тогда элементы полугруппы имеют вид: 1 (единичный элемент), x, x^2, ...

..., x^n, ... Элементами полугрупповой алгебры, построенной на этой полугруппе, будут «линейные комбинации» $\lambda_0 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_n x^n$ с «коэффициентами» из некоторого заданного тела. Так мы получаем многочлены с коэффициентами из заданного тела, поскольку операции, заданные на элементах полугрупповой алгебры, в этом случае совпадают с операциями, производимыми над многочленами. Это обстоятельство позволяет нам рассматривать кольцо многочленов как свободную алгебру свободной полугруппы, порожденной одним элементом, над заданным телом.

Аналогичный метод применим в алгебраических «конструкциях» и в том случае, если «коэффициенты» принадлежат не телу, а кольцу, и позволяет определить многочлены с коэффициентами из заданного кольца.

3. Комплексные числа. Пусть e и i — элементы базиса двухмерного векторного пространства над вещественными числами. Операцию умножения этих элементов зададим следующим образом:

$$e \cdot e = e, \quad e \cdot i = i \cdot e = i,$$
$$i \cdot i = (-1)e.$$

Поскольку e «ведет себя» как единичный элемент, то ассоциативность умножения необходимо проверить лишь для случая, когда все три сомножителя равны i, а в этом случае умножение ассоциативно. Следовательно, мы получаем алгебру, которая (как кольцо) изоморфна телу комплексных чисел.

4. Кватернионы. Пусть e, i, j и k — элементы базиса четырехмерного векторного пространства над телом вещественных чисел. Умножение зададим следующим образом:

$$e \cdot e = e, \; e \cdot i = i \cdot e = i, \quad e \cdot j = j \cdot e = j,$$
$$e \cdot k = k \cdot e = k;$$
$$i \cdot j = k, \; j \cdot k = i, \; k \cdot i = j;$$
$$j \cdot i = (-1) \cdot k, \; k \cdot j = (-1) \cdot i,$$
$$i \cdot k = (-1) \cdot j;$$
$$i \cdot i = j \cdot j = k \cdot k = (-1) \cdot e.$$

Нетрудно видеть, что такое умножение ассоциативно. Следовательно, мы получаем алгебру. Более того, можно доказать, что это — алгебра с делением (делить справа и слева можно на любой элемент, отличный от нуля). Следовательно, мы получаем некоммутативное тело. Оно называется телом кватернионов.

Заметим, что помимо тела кватернионов существуют лишь два примера такого рода. Что именно кроется за этим несколько туманным выражением, точно сформулировал Фробениус.

Теорема Фробениуса.

Пусть A — алгебра над телом вещественных чисел, удовлетворяющая следующим условиям:

1) как векторное пространство A конечномерна;

2) как кольцо A не содержит делителей нуля.

Тогда алгебра A изоморфна либо телу вещественных чисел, либо телу комплексных чисел, либо телу кватернионов.

Интересно заметить, что примеров *неассоциативных* алгебр (в которых умножение не предполагается ассоциативным) можно привести сколь угодно много. Многочисленность неассоциативных алгебр имеет под собой две причины. Одна из причин внешняя: ясно, что в различных областях математики (не только в алгебре!) встречается великое множество алгебр с неассоциативным умножением. Другая причина — внутренняя. При рассмотрении операции умножения возникает естественное условие дистрибутивности, позволяющее одновременно рассматривать все алгебры «над» данным векторным пространством (то есть алгебры, совпадающие с данным векторным пространством, если «забыть» об умножении), но из них нельзя «отсеять» алгебры с неассоциативным умножением.

ЗАДАЧИ

1. Доказать, что матрицы $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ с вещественными элементами образуют над телом вещественных чисел алгебру, изоморфную телу комплексных чисел.

2. Доказать, что матрицы

$$\begin{bmatrix} a & -b & -c & d \\ b & a & -d & -c \\ c & d & a & b \\ -d & c & -b & a \end{bmatrix}$$

образуют над телом вещественных чисел алгебру, изоморфную телу кватернионов.

3. Доказать, что всякий гомоморфизм, действующий из группы G_1 в группу G_2, можно продолжить до гомоморфизма, действующего из групповой алгебры $(\Gamma; G_1)$ в групповую алгебру $(\Gamma; G_2)$, который является одновременно гомоморфизмом колец и гомоморфизмом векторных пространств.

Глава третья

Структуры, булевы алгебры

1

Структуры и операции над множествами

1.1. Операции над частями одного множества

Содержание предыдущих глав дает наглядное представление об отличительных особенностях абстрактной алгебры. Мы видели, что абстрактная алгебра занимается изучением операций и различных способов их задания. Встречавшиеся нам до сих пор операции по существу не отличались от того, что можно было бы ожидать от «естественных» операций. Вместе с тем ясно, что действия, производимые над операциями, не зависели от того, были ли эти операции обычными или «экзотическими». В дальнейшем речь пойдет об операциях, существенно отличающихся от тех, с которыми нам приходилось иметь дело до сих пор.

В математике весьма фундаментальную роль играют множества. Множество — это нечто такое, о чем известно лишь, что оно состоит из элементов. Поскольку в математике элементы всегда наделены определенными свойствами, то обычно эти свойства позволяют отличать элементы одного множества от элементов другого множества. Но нередко встречаются и такие случаи, когда элементы одного множества наделены не одним, а несколькими свойствами, а рассмотрению подлежат элементы, обладающие какими-то или даже всеми заданными свойствами. Иногда бывает необходимо найти элементы множества, принадлежащие по крайней мере одному из заданных множеств (содержащиеся в заданных множествах). Иначе говоря, возникает необходимость из элементов одних множеств строить другие множества. Это означает, что над множествами можно производить операции. В простейшем случае операции производятся лишь над двумя множествами. (Впрочем, как нетрудно видеть, общий случай легко сводится к простейшему, разумеется, при условии, что соответствующие операции придется неоднократно повторить.) Если имеются два множества (или любое большее число множеств), то их можно рассматривать как части некоторого «большого» множества. Поэтому в дальнейшем мы будем говорить о частях одного множества и о производимых над ними операциях.

Пусть A и B — подмножества множества H.

Пересечением, или общей частью, подмножеств A и B называется множество $A \cap B$, состоящее из тех и только тех элементов множества H, которые принадлежат каждому из подмножеств A и B.

Объединением подмножеств A и B

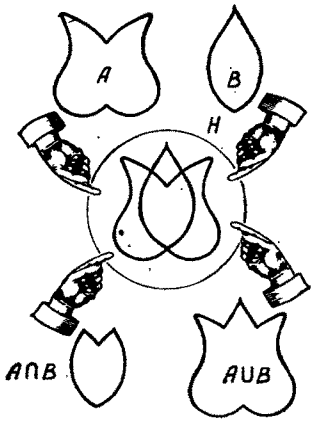


Рис. 87.

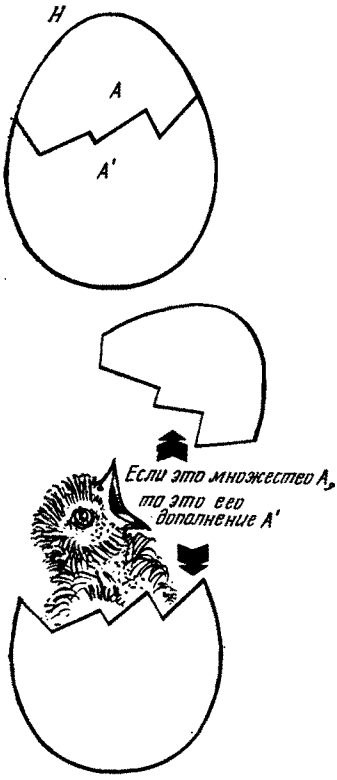


Рис. 88.

называется множество $A \cup B$, состоящее из тех и только тех элементов множества H, которые принадлежат хотя бы одному из подмножеств A или B (рис. 87).

Дополнением множества A называется множество A' тех и только тех элементов множества H, которые не принадлежат множеству A (рис. 88).

Уместно заметить, что два подмножества одного множества считаются равными, если состоят из одних и тех же элементов. (Таким образом, подмножество не зависит от того, каким способом задано оно и каким — элементы.) Следовательно, чтобы задать подмножество, необходимо указать его элементы или по крайней мере сообщить, каким способом их можно было бы отличить.

Если два подмножества не имеют общих элементов, то не существует такого подмножества, которое было бы пересечением данных подмножеств. Такое исключение было бы весьма неудобным и причинило бы немало хлопот, чем значительно затруднило бы описание производимых над множествами операций. Именно поэтому считается, что существует однозначно определенное подмножество, не содержащее ни одного элемента. (То, что оно однозначно определено, видно из определения этого подмножества, поскольку оно не может иметь одинаковых элементов ни с одним другим подмножеством, кроме «однотипного» с ним «пустого» подмножества.) Такое подмножество называется *пустым множеством*. Если два подмножества не имеют общих элементов, то говорят, их пересечение пусто, или — пустое множество.

Единообразия в рассмотрении подмножеств можно достичь, добавив ко всему множеству еще один элемент. Для большей ясности будем считать, что этот элемент — слово, а именно слово «пустое». Условимся считать наш дополнительный элемент принадлежащим всем подмножествам «большого» множества. Какие бы подмножества мы ни выбрали, они окажутся такими же, как и прежде, только после перечисления элементов каждого из них нам придется добавить: «И еще один элемент, а именно слово „пустое“». Если пересечение двух подмножеств до пополнения множества было пусто, то и после пополнения пересечение этих подмножеств будет «пустым множеством» —

в том смысле, что оно будет содержать только слово «пустое».

Включив в рассмотрение пустое множество, мы получаем возможность утверждать, что пересечение любых двух подмножеств существует и объединение любых двух подмножеств также существует. Для каждого подмножества существует дополнение, поскольку теперь все множество H также обладает дополнением: пустым множеством.

В дальнейшем мы будем обозначать пустое множество через O, а все множество через E. Выясним, какие тождества можно установить для операций над множествами. Рассмотрим сначала только тождества, относящиеся к операциям объединения и пересечения множеств, причем тождества для обеих операций будем выписывать одновременно. Первые тождества имеют следующий вид:

1а) $A \cap A = A$; 1б) $A \cup A = A$.

(Эти два тождества называются *законами идемпотентности*.)

Оба тождества очевидны. Первое из них утверждает, что множеству A принадлежат те и только те элементы, которые принадлежат множеству A *и* множеству A. Согласно второму тождеству, множеству A принадлежат те и только те элементы, которые принадлежат множеству A *или* множеству A. Вторая пара тождеств имеет следующий вид:

2а) $A \cap B = B \cap A$; 2б) $A \cup B = B \cup A$.

(Взятие пересечения и объединения — коммутативные операции.) Эти два тождества самоочевидны, так как ни в определении пересечения, ни в определении объединения ничего не говорится о порядке подмножеств. Третья пара тождеств имеет следующий вид:

3а) $(A \cap B) \cap C = A \cap (B \cap C)$;

3б) $(A \cup B) \cup C = A \cup (B \cup C)$.

(Эти два тождества означают, что взятые пересечения и объединения — ассоциативные операции.)

Обратимся к доказательствам тождеств 3а и 3б. Рассмотрим множества, стоящие в левой и в правой частях первого тождества. Они образованы элементами, принадлежащими каждому из подмножеств A, B и C (и только такими элементами). Рассмотрим множества, стоящие в левой и в правой частях второго тождества. Они образованы элементами, принадлежащими по крайней мере одному из подмножеств — A, B и C (и только такими элементами).

Следующие тождества, которые необходимо рассмотреть, выражают законы дистрибутивности. Возникает вопрос, какая из двух операций «похожа» на сложение и какая «напоминает» умножение. Поскольку на этот вопрос невозможно ответить со всей определенностью, до сих пор (по крайней мере в принципе) различают два закона дистрибутивности. В рассматриваемом нами случае удивительным образом выполняются оба закона:

4а) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$;

4б) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

Эти два тождества доказываются так же, как и предыдущие. В обоих случаях необходимо убедиться в том, что подмножества, стоящие в левой и в правой частях тождества, образованы одними и теми же элементами. Доказательство проводится в два этапа. Сначала мы показываем, что одно из подмножеств содержится в другом, а затем убеждаемся в том, что все элементы второго подмножества принадлежат первому подмножеству. Поскольку оба этапа доказательства для обоих тождеств протекают аналогично, мы сначала закончим первые этапы доказательства для тождеств 4а и 4б, а затем перейдем ко вторым этапам.

Первый этап доказательства основан на использовании лишь свойства «вхождения», или «включения», одного подмножества в другое, и в нем ни словом не упоминается об элементах подмножеств. Напомним, что объединение двух подмножеств A и B представляет собой наименьшее из подмножеств, содержащих оба подмножества A и B, а пересечение подмножеств A и B — наибольшее из подмножеств, входящих в каждое из подмно-

жеств A и B (и, кроме того, подмножество любого подмножества является подмножеством исходного множества).

Поскольку подмножество $A \cap B$ принадлежит и подмножеству A, и подмножеству B, то оно принадлежит и подмножествам $A \cup C$ и $B \cup C$, каждое из которых содержит и A, и B, и, следовательно, входит в пересечение $(A \cup C) \cap (B \cup C)$. Последнее утверждение справедливо и относительно подмножества C, так как его содержит и подмножество $A \cup C$, и подмножество $B \cup C$. Это означает, что объединение подмножеств $A \cap B$ и C принадлежит подмножеству $(A \cup C) \cap (B \cup C)$, так как каждое из подмножеств $A \cap B$ и C в отдельности содержится в $(A \cup C) \cap (B \cup C)$. Итак,

$$(A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C).$$

Подмножество $A \cup B$ содержит и подмножество A, и подмножество B и поэтому включает в себя каждое из подмножеств $A \cap C$ и $B \cap C$, а следовательно, и их объединение $(A \cap C) \cup (B \cap C)$. Подмножество C входит в объединение $(A \cap C) \cup (B \cap C)$, так как содержится в подмножествах $A \cap C$ и $B \cap C$. Это означает, что пересечение подмножеств $A \cup B$ и C содержит подмножество $(A \cap C) \cup (B \cap C)$. Итак,

$$(A \cup B) \cap C \supseteq (A \cap C) \cup (B \cap C).$$

Докажем теперь, что всякий элемент x подмножества $(A \cup C) \cap (B \cup C)$ принадлежит подмножеству $(A \cap B) \cup C$. Если элемент x принадлежит подмножеству C, то он принадлежит и подмножеству $(A \cap B) \cup C$ (поскольку оно содержит подмножество C). Следовательно, в дальнейшем, не ограничивая общности, можно предполагать, что x не является элементом множества C. Поскольку x принадлежит подмножеству $(A \cup C) \cap (B \cup C)$, то x входит в каждое из подмножеств $A \cup C$ и $B \cup C$. Так как x по предположению не принадлежит подмножеству C, то это может быть лишь в том случае, если x принадлежит каждому из подмножеств A и B в отдельности и, следовательно, их пересечению $A \cap B$. Итак, x принадлежит либо подмножеству C, либо подмножеству $A \cap B$, то есть входит в объединение $(A \cap B) \cup C$.

По определению пересечения и объединения подмножеств произвольный элемент y подмножества $(A \cup B) \cap C$ принадлежит подмножеству C, а также по крайней мере одному из подмножеств A или B (а может быть, и обоим подмножествам A и B). Если y — элемент множества A, то y принадлежит пересечению $A \cap C$, а если y — элемент подмножества B, то y принадлежит пересечению $B \cap C$. И в том и в другом случае y принадлежит объединению этих подмножеств $(A \cap C) \cup (B \cap C)$, что и требовалось доказать.

Еще одна пара важных тождеств показывает, что при взятии объединения мы получаем бо́льшие, а при взятии пересечения — меньшие подмножества.

5а) $(A \cap B) \cup A = A$;

5б) $(A \cup B) \cap A = A$.

(Эти тождества называются *законами поглощения*. Действительно, независимо от того, возьмем ли мы сначала пересечение подмножества B с подмножеством A, а затем — объединение подмножеств $A \cap B$ и A, или сначала образуем объединение подмножеств A и B, а затем — пересечение подмножеств $A \cup B$ и A, подмножество B «поглощается».)

Оба тождества очевидны.

Перейдем теперь к тождествам, относящимся к дополнениям подмножеств. Дополнение дополнения любого подмножества совпадает с исходным множеством:

6) $(A')' = A$.

Тождества между переходом к дополнению и взятием объединения или пересечения подмножеств имеют следующий вид:

7а) $(A \cap B)' = A' \cup B'$;

7б) $(A \cup B)' = A' \cap B'$.

Элемент x принадлежит подмножеству $(A \cap B)'$ в том и только в том случае, если он не принадлежит подмножеству $A \cap B$. В свою очередь, если x не принадлежит подмножеству $A \cap B$, то он не входит по крайней мере в одно из подмножеств A и B. Но если элемент x не принадлежит A, то он принадлежит A', а если x не принадлежит B, то он принадлежит B'. По крайней мере одно из этих условий заведомо выполняется, а это в означает, что x принадлежит $A' \cup B'$.

Элемент y принадлежит подмножеству $(A \cup B)'$ в том и только в том случае, если он не принадлежит ни подмножеству A, ни подмножеству B. Иначе говоря, элемент y должен входить как в A', так и в B', а это означает, что в $A' \cap B'$ входят те и только те элементы, которые принадлежат $(A \cup B)'$.

После того как мы достаточно освоились в алгебре, нетрудно проверить, что помимо взятия объединения и пересечения подмножеств существуют еще две нуль-местные операции: O и E (пустое множество и «все» множество). Нуль-местные операции связаны с двухместными следующими тождествами:

8а) $O \cap A = O$; 8б) $E \cup A = E$;

8в) $E \cap A = A$; 8г) $O \cup A = A$.

Каждое из этих тождеств очевидно и не требует доказательства.

Наконец, с переходом к дополнению нуль-местные операции связаны следующими (столь же очевидными) тождествами:

9а) $O' = E$; 9б) $E' = O$;

10а) $A \cap A' = O$; 10б) $A \cup A' = E$.

Аналогичные операции можно задать на подпространствах векторного пространства. Общая часть, или пересечение, двух пространств, как было показано выше, всегда является подпространством. Теоретико-множественное объединение двух подпространств не является подпространством, но существует «наименьшее» подпространство, содержащее два заданных подпространства, а именно подпространство, порожденное двумя заданными подпространствами. Пустому множеству соответствует подпространство, состоящее из нулевого вектора, а всему множеству—все векторное пространство. Но понятия, аналогичного теоретико-множественному дополнению, в векторном пространстве не существует: дополнение подпространства не является подпространством. Впрочем, это не причиняет никаких хлопот, поскольку объединение двух подпространств надлежит понимать не в теоретико-множественном смысле, а как объединение образующих элементов двух подпространств. Дополнение подмножества A — это подмножество, пересечение которого с подмножеством A пусто, а объединение с подмножеством A совпадает со всем пространством. Соответственно дополнением подпространства B векторного пространства мы называем подпространство, пересечение которого с подпространством B пусто, а объединение с подпространством B порождает все векторное пространство. Это означает, что все векторное пространство представимо в виде прямой суммы двух подпространств. Но для любого данного подпространства можно найти такое подпространство, которое в прямой сумме с ним образует все векторное пространство. Трудность состоит лишь в том, что второе слагаемое в прямой сумме определено не однозначно, и поэтому нельзя сказать, какое подпространство будет дополнением данного подпространства. Выясним, наконец, выполняются ли для векторных пространств аналоги тождеств, перечисленных выше для операций взятия теоретико-множественного пересечения и объединения.

Нетрудно видеть, что три первые пары тождеств выполняются. От доказательств соответствующих теоретико-множественных тождеств отличается только доказательство ассоциативности объединения, но и оно не представляет особой трудности (в правой и в левой частях доказываемого тождества стоят подпространства, порожденные тремя подпространствами).

Первая половина доказательства четвертой пары тождеств дословно воспроизводит доказательство их теоретико-множественных аналогов, поскольку для векторного пространства пересечение подпространств A и B остается наибольшим из подпространств, принадлежащих каждому из подпространств A и B, а подпространство, порожденное подпространствами A и B (аналог теоретико-множественного объединения) — наименьшим из подпространств, содержащих подпространства A и B.

Но провести вторую половину доказательства для векторного пространства оказывается невозможно, поскольку правая часть «тождеств» не равна левой, в чем нас убеждает следующий контрпример. Пусть $A = \{u\}$, $B = \{v\}$ и $C = \{u + v\}$, где u и v — два непараллельных вектора на плоскости. Тогда $A \cap B = \{O\}$, $(A \cap B) \cup C = \{u + v\}$ и, кроме того, так как $A \cup C = B \cup C = \{u, v\}$, то $(A \cup C) \cap (B \cup C) = \{u, v\}$. Э о означает, что часть аналога тождества 4а для векторных про-

странств содержится в правой части, не совпадая с ней. Можно также доказать, что в левой части аналога тождества 4б для векторных пространств стоит подпространство $\{u + v\}$, а в правой части — подпространство $\{O\}$, поэтому правая часть содержится в левой, не совпадая с ней.

Как показывают достаточно многочисленные примеры, при определенных условиях (если одно из подпространств A и B, например подпространство A, содержит подпространство C) законы дистрибутивности остаются в силе и для векторных пространств.

Действительно, если $A \cup C = A$ и $A \cap C = C$, то оба тождества переходят в одно: $(A \cap B) \cup C = A \cap (B \cup C)$. Докажем его. Так же как и при доказательстве дистрибутивности теоретико-множественного пересечения относительно объединения, непосредственно видно, что $(A \cap B) \cup C \subseteq A \cap (B \cup C)$ (разумеется, если $A \supseteq C$). Рассмотрим элемент x подпространства $A \cap (B \cup C)$. С одной стороны, x принадлежит подпространству A, с другой стороны, его можно представить в виде $x = b + c$, где b — вектор из B, а c — вектор из C. Поскольку $C \subseteq A$, то из принадлежности c подпространству C следует, что $c \in A$ и элемент $b = x - c$ принадлежит подпространству A как разность двух элементов из A. Это означает, что элемент x представим в виде суммы элемента из $A \cap B$ (а именно b) и элемента из C, то есть принадлежит подпространству $(A \cap B) \cup C$.

Нетрудно видеть, что для векторных пространств выполняются аналоги тождеств 5а и 5б, а тождества 6 и 7 не имеют смысла. Аналоги тождеств 8 очевидны, а остальные тождества утрачивают смысл.

В качестве еще одного примера рассмотрим все подгруппы одной группы. Пересечение в этом случае совпадает с теоретико-множественным пересечением, так как множество общих элементов двух подгрупп само также является подгруппой. Объединение двух подгрупп A и B надлежит понимать как подгруппу, порожденную подгруппами A и B, поскольку это — наименьшая из подгрупп, содержащих и A, и B. Хорошего аналога теоретико-множественного дополнения для групп, так же как и для векторных пространств, не существует, причем для групп ситуация еще более «безнадежна». Действительно, в случае векторных пространств существовало несколько подпространств, каждое из которых обладало всеми свойствами дополнения. В случае групп нет ни одной подгруппы, которую можно было бы считать «кандидатом» в дополнение.

Выясним, как обстоит дело с тождествами. Что касается законов дистрибутивности, то ясно, что те тождества, которые выполняются для векторных пространств, остаются в силе и для групп. Более того, можно доказать, что «первая половина» законов дистрибутивности верна для групп, а «вторая половина» отказывает в таких же частных случаях, как и для векторных пространств. Рассмотрим, например, следующие подгруппы группы подстановок цифр 1, 2, 3 и 4:

подгруппа A с элементами (12)(34), (13)(24), (14)(23) и тождественной подстановкой;

подгруппа B с элементами (123), (132) и тождественной подстановкой;

подгруппа C, состоящая из подстановки (12)(34) и тождественной подстановки.

Ясно, что подгруппа A содержит подгруппу C. Подгруппа $A \cap B$ состоит только из единичного элемента и, следовательно, $(A \cap B) \cup C = C$. Но, с другой стороны, подгруппе $B \cup C$ принадлежит, например, элемент (132)(12)(34)(123) = (14)(23). Следовательно, этот элемент входит и в подгруппу $A \cap (B \cup C)$, которая, таким образом, содержит элемент, не принадлежащий подгруппе $(A \cap B) \cup C$. Это означает, что подгруппы $A \cap (B \cup C)$ и $(A \cap B) \cup C$ не совпадают.

ЗАДАЧИ

1. Рассмотрим подмножества неотрицательных целых чисел, состоящие из конечного (может быть, равного нулю) числа элементов. Какие из операций над множествами можно задать на этих подмножествах? Какие

тождества будут при этом выполняться?

2. Рассмотрим подмножества, получающиеся из множества всех отрицательных чисел при выбрасывании конечных подмножеств элементов. Какие из операций над множествами можно задать на этих подмножествах? Какие тождества будут при этом выполняться?

3. Рассмотрим подмножества целых чисел, состоящие из конечного набора положительных целых чисел и всех отрицательных целых чисел, за исключением конечного подмножества. Какие из операций над множествами можно задать на этих подмножествах? Какие тождества будут при этом выполняться?

4. Доказать, что для подгрупп коммутативной группы выполняются такие же тождества, как и для векторных пространств.

5. Доказать, что для нормальных делителей группы выполняются такие же тождества, как и для векторных пространств.

1.2. Структуры, специальные структуры

В предыдущих примерах мы рассмотрели случаи, когда производились две операции: объединения и пересечения. (Среди задач предыдущего раздела встречались и такие, которые не содержали аналогов пустого множества O или «всеобъемлющего» множества E; понятие дополнения встречалось лишь в первом из этих случаев.) Во всех примерах неизменно выполнялись все тождества, за исключением законов дистрибутивности 4а и 4б. В таких случаях множества (наделенные операциями объединения и пересечения) принято называть структурами. По доказанному все подмножества любого множества, все подпространства любого векторного пространства и все подгруппы любой группы образуют структуры.

Тройка $\langle H;\ \cap,\ \cup\rangle$, где H — множество, а $\cap$ и $\cup$ — две двухместные операции, называется структурой, если выполняются следующие условия:

1) обе операции идемпотентны, то есть для любого элемента a из H

$$a \cap a = a \text{ и } a \cup a = a;$$

2) обе операции коммутативны, то есть для любых элементов a и b из H

$$a \cap b = b \cap a \text{ и } a \cup b = b \cup a;$$

3) обе операции ассоциативны, то есть для любых элементов a, b и c из H

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

и

$$(a \cup b) \cup c = a \cup (b \cup c);$$

4) выполняются оба закона поглощения, то есть для любых элементов a и b из H

$$(a \cap b) \cup a = a \text{ и } (a \cup b) \cap a = a.$$

Тройка $\langle H;\ \cap,\ \cup\rangle$ называется структурой, если выполняются следующие условия:

1) $a \cap a = a$ и $a \cup a = a$;

2 $a \cap b = b \cap a$ и $a \cup b = b \cup a$;

3) $(a \cap b) \cap c = a \cap (b \cap c)$,

$(a \cup b) \cup c = a \cup (b \cup c)$;

4) $(a \cap b) \cup a = a$ и $(a \cup b) \cap a = a$.

Два обстоятельства заслуживают особого внимания. Во-первых, законы поглощения — единственное условие, связывающее обе операции. Рассматривая структуру подмножеств произвольного множества, мы установили, что она дистрибутивна. Но если бы мы удовлетворились этим свойством, то заданные на структурах операции не были бы взаимосвязаны. В этом случае о «совместном» действии двух операций нельзя было бы почерпнуть никакой информации, кроме той, что известна о каждой из операций в отдельности. (В частности, две операции могли бы совпадать.)

Во-вторых, из двух законов поглощения (не используя других условий) следует идемпотентность операций. Интересно отметить, что в отличие от структур во всех остальных случаях (при рассмотрении групп, колец и т. д.) идемпотентность вводится специальным предположением, хотя число условий всегда стремятся по возможности сократить.

Мы привели достаточно примеров структур (операции, заданные на некоторых из них, помимо «обязательных» тождеств удовлетворяли и «дополнительным» тождествам). Можно было бы привести множество других примеров из самых различных областей математики, но для этого потребовались бы такие познания в математике, которых мы не вправе ожидать от читателя.

Приведем прежде всего несколько общих результатов, относящихся ко всем структурам. Если рассмотреть тождества 2 и 3, то можно заметить, что структуры образуют относительно обеих операций коммутативные полугруппы. Обе операции сохраняют коммутативность и ассоциативность и в том случае, когда число «сомножителей» или «слагаемых» больше двух.

Принцип двойственности

Наше второе замечание подтверждается тем, что, если в любой паре тождеств переставить символы входящих в них операций (то есть заменить объединение пересечением, а пересечение объединением), то тождества, образующие рассматриваемую пару, также «поменяются местами». Отсюда следует, что доказательство любой теоремы останется в силе, если символ каждой из двух операций заменить парным символом. Таким образом, у каждой теоремы имеется свой «двойник», отличающийся от нее лишь тем, что каждая операция заменена парной. Теорема-«двойник» истинна в том и только в том случае, если истинна исходная теорема. Именно поэтому каждую теорему доказывают вместе с ее «двойником» — так называемой *двойственной* теоремой. Это утверждение известно под названием *принципа двойственности*. В дальнейшем мы воспользуемся этим принципом при рассмотрении специальных структур в предположении, что их «специальность» двойственна, то есть что наряду с каждым дополнительным («специализирующим») условием выполняется и двойственное ему условие. Такой подход не всегда позволяет получить две теоремы, поскольку некоторые утверждения двойственны самим себе. Их принято называть *самодвойственными* утверждениями (или теоремами).

Мы уже рассмотрели несколько специальных структур. Одни из них были дистрибутивными, другие обретали дистрибутивность лишь в особых случаях. Сформулировать, чем именно выделены эти случаи, мы пока не можем, потому что в рассмотренных нами частных примерах структуры выполнялось условие, согласно которому один элемент был частью другого элемента. Аналогичное условие для структуры общего типа нам не встречалось. Тем не менее понятие дистрибутивности распространяется и на общий случай, причем ввести его можно не одним, а двумя способами в зависимости от того, какому из законов дистрибутивности отдать предпочтение. Покажем, что в действительности безразлично, какой из законов дистрибутивности будет выбран: если один из них выполняется, то выполняется и другой.

Напомним, что принцип двойственности позволяет вместо двух утверждений доказывать лишь одно, поскольку законы дистрибутивности двойственны.

Если для любых трех элементов a, b и c структуры выполняется соотношение $(a \cap b) \cup c = (a \cup c) \cap (b \cup c)$, то для любых трех элементов x, y, t той же структуры выполняется соотношение $(x \cup y) \cap t = (x \cap t) \cup (y \cap t)$.

Итак, предположим, что объединение дистрибутивно (относительно пересечения), то есть для любых трех элементов выполняется соотношение $(a \cap b) \cup c = (a \cup c) \cap (b \cup c)$. Подставляя в него $a = x$, $b = t$, $c = y \cap t$, получаем

$$(x \cap t) \cup (y \cap t) = [x \cup (y \cap t)] \cap [t \cup (y \cap t)].$$

По закону поглощения выражение, стоящее во вторых прямоугольных скобках, равно t. Элементы x и $y \cap t$ в первых прямоугольных скобках коммутируют, а поскольку по предположению объединение дистрибутивно относительно пересечения, то «содержимое» первой пары прямоугольных скобок можно представить в следующем виде:

$$x \cup (y \cap t) = (x \cup y) \cap (x \cup t).$$

Подставляя в предыдущее соотношение и используя ассоциативность, получаем

$$(x \cap t) \cup (y \cap t) = (x \cup y) \cap [(x \cup t) \cap t].$$

Элемент, стоящий в квадратных скобках, по «другому» закону поглощения равен t. Следовательно, для любых трех элементов структуры пересечение дистрибутивно (относительно объединения).

Рассмотренные нами специальные структуры отличались не только тем, что введенные на них операции удовлетворяли дополнительным тождествам. Они содержали также особые элементы и были наделены некоторыми операциями помимо взятия объединения и пересечения. Начнем с особых элементов: нуля и единицы структуры.

Если в структуре S существует такой элемент 0, для которого соотношение $0 \cap a = 0$ выполняется при любом $a \in S$, то 0 называется нулем структуры S. Если в структуре S существует такой элемент e, для которого соотношение $e \cup a = a$ выполняется при любом $a \in S$, то e называется единицей структуры S. Нуль называют также нижней, а единицу — верхней гранью.

Структуры, для которых существуют верхняя и нижняя грань, называются ограниченными.

Общее название единицы и нуля — грань — выбрано из следующих соображений. При рассмотрении структуры подмножеств произвольного множества нулем служит «ничто», или пустое подмножество, а единицей «все», или исходное множество. Все остальные подмножества заключены между этими двумя «избранными» подмножествами, причем нуль ограничивает любое подмножество «снизу», а единица — «сверху».

Прежде всего покажем, что если нуль или единица существуют, то они единственны. Пусть $0'$ — еще один нуль структуры (помимо 0). Тогда должны выполняться соотношения $0 \cap 0' = 0'$ и $0' \cap 0 = 0$. В силу коммутативности элементы 0 и $0'$ равны, то есть нуль однозначно определен. Утверждение о единственности единицы следует из принципа двойственности.

Заметим, что как нуль, так и единицу можно определить по-разному. *Элемент 0 является нулем структуры S в том и только в том случае, если соотношение $0 \cup a = a$ выполняется при любом $a \in S$. Элемент e является единицей структуры S в том и только в том случае, если соотношение $e \cap a = a$ выполняется при любом $a \in S$.* В силу принципа двойственности достаточно доказать лишь одно из двух утверждений: либо относительно единицы, либо относительно нуля. Докажем утверждение, в котором говорится о единице.

Если соотношение $e \cap a = a$ выполняется при всех $a \in S$, то $e \cup a = e \cup (e \cap a) = e$ (сначала мы подставили вместо элемента a равный ему элемент $e \cap a$, а затем воспользовались законом поглощения). Наоборот, если при всех $a \in S$ выполняется соотношение $e \cup a = a$, то (также произведя подстановку и воспользовавшись законом поглощения) мы получим $e \cap a = (e \cup a) \cap a = a$.

В приведенном выше доказательстве никак не используется ни «универсальность» соотношения $e \cap a = a$ (то, что a — произвольный элемент структуры), ни то, что речь идет о верхней и нижней грани структуры. Следовательно, полученный нами результат допускает обобщение: соотношение $a \cap b = b$ выполняется в том и только в том случае, если $a \cup b = a$.

Для элементов a и b структуры соотношение $a \cap b = b$ выполняется в

том и только в том случае, если выполняется соотношение $a \cup b = a$.

Если это утверждение понимать так, что второе соотношение следует из первого, а первое — из второго, то в силу принципа двойственности достаточно доказать лишь одно из них, так как соотношения $a \cap b = b$ и $a \cup b = a$ двойственны. Пусть $a \cap b = b$. Тогда, произведя подстановку и используя закон поглощения, получаем $a \cup b = a \cup (a \cap b) = a$.

Изучая структуры, мы сталкиваемся с такой же ситуацией, как и в случае полугрупп с единицей. Если структура обладает подструктурой и та и другая «случайно» содержат по нулю, то нуль подструктуры не обязательно должен совпадать с нулем всей структуры. Но если говорят о «структуре с нулем», то нуль любой ее «подструктуры с нулем» по определению совпадает с нулем всей структуры. Аналогичное утверждение справедливо и относительно «структуры с единицей».

Рассмотрим, наконец, понятие дополнения. Его можно определить для структур, если учесть, что пересечение любого элемента с его дополнением равно нулю, а объединение любого элемента с дополнением равно единице. Отсюда следует, что понятие дополнения имеет смысл лишь для ограниченных структур, то есть для структур, обладающих верхней и нижней гранью.

Элемент a' называется дополнением элемента a ограниченной структуры, если выполняются соотношения

$$a \cap a' = 0 \text{ и } a \cup a' = e.$$

В общем случае, как уже упоминалось, если существует одно дополнение, то может существовать и несколько дополнений. Следовательно, переход от элемента структуры к дополнению нельзя считать операцией. Но если структура дистрибутивна, то для каждого ее элемента существует не более одного дополнения. Поэтому для дистрибутивных структур взятие дополнения представляет собой «почти» операцию и называется *частичной операцией*. Термин «частичная операция» означает, что операция определена не для всех элементов структуры, но для тех элементов, для которых она определена, операция задана однозначно. Частичные операции удовлетворяют определенным тождествам. С аналогичной ситуацией нам приходилось сталкиваться при рассмотрении отображений. Различие состоит лишь в том, что на этот раз все элементы, о которых идет речь, принадлежат не двум различным множествам, а одной вполне определенной структуре.

Для любого элемента a дистрибутивной структуры существует не более одного дополнения a', для которого

1) $(a')' = a$;

2) $e' = 0$ и $0' = e$;

3) $(a \cup b)' = a' \cap b'$ и $(a \cap b)' = a' \cup b'$.

Прежде всего убедимся в том, что дополнение однозначно определено. Пусть x и y — дополнения элемента a, то есть пусть

$$a \cap x = a \cap y = 0 \text{ и } a \cup x = a \cup y = e.$$

Так как e — единичный элемент, то $x = x \cap e$, а вместо e можно подставить элемент $a \cup y$. Но пересечение дистрибутивно относительно объединения, поэтому $x = x \cap (a \cup y) = (x \cap a) \cup (x \cap y)$. Поскольку $x \cap a = 0$ и $0 \cup (x \cap y) = x \cap y$, то $x = x \cap y$. Пользуясь аналогичными рассуждениями, можно показать, что $y = y \cap x$, а так как пересечение коммутативно, то x и y совпадают и каждый из этих элементов равен $x \cap y$.

Если a' — дополнение элемента a, то из соотношений $a' \cup a = e$ и $a' \cap a = 0$ следует, что a — дополнение элемента a'. Но дополнение любого элемента структуры однозначно определено, поэтому $(a')' = a$.

Равенства $e' = 0$ и $0' = e$ нетрудно вывести из соотношений $e \cup 0 = e$ и $e \cap 0 = 0$.

Однозначная определенность дополнения существенно упрощает доказательство последнего (третьего) свойства дополнения: действительно, достаточно доказать, что $a' \cap b'$ — дополнение элемента $a \cup b$, а $a' \cup b'$ — дополнение элемента $a \cap b$.

Первое свойство позволяет еще более сократить доказательство и свести его к доказательству первого из двух утверждений, поскольку второе утверждение эквивалентно первому, только вместо a в него входит a', а вместо b — дополнение b'.

Используя дистрибутивность объединения, получаем:

$$(a \cap b) \cap (a' \cup b') = (a \cap b \cap a') \cup (a \cap b \cap b').$$

Поскольку $a \cap a' = b \cap b' = 0$ и $b \cap 0 = a \cap 0 = 0$, то в правой части стоит элемент $0 \cup 0 = 0$. Аналогичным образом находим объединение элементов $a \cap b$ и $a' \cup b'$:

$$(a \cap b) \cup (a' \cup b') = (a \cup a' \cup b') \cap (b' \cup a' \cup b') =$$
$$= (e \cup b') \cap (e \cup a') = e \cap e = e.$$

Итак $(a \cap b) \cap (a' \cup b') = 0$, $(a \cap b) \cup (a' \cup b') = e$. Это и доказывает, что каждый из элементов $a \cap b$ и $a' \cup b'$ служит дополнением другого.

Разумеется, с введением операции перехода к дополнению мы получаем структуру совсем «иного рода». Может показаться, что дополнение существует в ограниченной дистрибутивной структуре и в содержащейся в ней «полуограниченной» структуре, но эти дополнения различны. В действительности, как удается доказать, все обстоит иначе, то есть дополнение в «части» структуры совпадает с дополнением во всей структуре (подобно тому, как единичный элемент подгруппы совпадает с единичным элементом группы, а элемент, обратный данному элементу, в подгруппе остается обратным ему при «возвращении» ко всей группе).

Дистрибутивные ограниченные структуры, в которых дополнение существует для каждого элемента, приобрели необычайную известность (причем не только в математике!). Они были «первыми» подробно изученными структурами и получили особое название: булевы алгебры.

Дистрибутивные ограниченные структуры, в которых для каждого элемента существует обратный, называются *булевыми алгебрами*.

ЗАДАЧИ

1. Доказать, что идемпотентность следует из двух законов поглощения.

2. Доказать, что в дистрибутивных структурах выполняются тождества $[(a \cup c) \cap b] \cup c = (a \cup c) \cap (b \cup c)$ и $(a \cap b) \cup (a \cap c) = a \cap [b \cup (a \cap c)]$, каждое из которых следует из другого (без предположения о дистрибутивности структуры).

3. Доказать, что для любых трех элементов в дистрибутивной структуре выполняется тождество

$$(a \cap b) \cup (b \cap c) \cup (c \cap a) =$$
$$= (a \cup b) \cap (b \cup c) \cap (c \cup a).$$

1.3. Частично упорядоченные множества и структуры

В приведенных выше примерах структур мы познакомились с весьма естественным способом сравнения элементов: при выполнении операций над определенными подмножествами множества нам приходилось учитывать, что одно подмножество больше или меньше другого (или что для рассматриваемых подмножеств ни одно из «неравенств» не выполняется). Кроме того, мы встретились и с таким частным случаем, когда сами подмножества удается определить лишь при помощи сравнения. (Речь идет о достаточно важном частном случае — подпространствах векторного пространства, понятия, с необходимостью возникающего во многих разделах математики.)

Было бы интересно рассмотреть затронутые в примерах «проблемы относительной величины» элементов подробнее и, быть может, высказать некоторые общие утверждения. С вопросами относительной величины элементов множества мы впервые сталкиваемся при изучении чисел. Какие бы два (вещественных, рациональных, целых и т. д.) числа мы ни выбрали, всегда можно сказать, какое из них *меньше* и какое *больше* или что они *равны*. (Наше утверждение не относится к комплексным числам!) Множества, обладающие та-

ким свойством, называются *упорядоченными* (иногда говорят, что на множестве задано *отношение порядка*) или *вполне упорядоченными*. Разумеется, понятию упорядоченного множества необходимо дать строгое определение, то есть точно указать, какими свойствами обладает «порядок». С алгебраической точки зрения определению с большей легкостью поддается не тот случай, когда один элемент множества меньше другого, а несколько более общий случай, когда один элемент множества «не больше» другого, то есть удобнее говорить о том, что один из элементов меньше другого или равен ему.

Понятие «меньше или равен», очевидно, является не операцией, а связью, существующей (или не существующей) между элементами множества. Такие связи называются *отношениями*.

Множество называется упорядоченным, если на нем задано отношение $\leqslant$, обладающее следующими свойствами:

1) оно рефлексивно, то есть для любого элемента a множества выполняется отношение $a \leqslant a$;

2) антисимметрично, то есть если для элементов a и b множества выполняются отношения $a \leqslant b$ и $b \leqslant a$, то $a = b$;

3) транзитивно, то есть если для элементов a, b и c множества выполняются отношения $a \leqslant b$ и $b \leqslant c$, то $a \leqslant c$;

4) трихотомично, то есть для любых элементов a и b множества выполняется либо отношение $a \leqslant b$, либо отношение $b \leqslant a$.

(Во многих случаях элементы удобно записывать в обратном порядке — «обратная» запись делает доказательство более «прозрачным», при этом знак неравенства следует «повернуть» в противоположную сторону: $a \geqslant b$ означает то же самое, что и $b \leqslant a$.)

Множество называется упорядоченным, если на нем задано рефлексивное, антисимметричное, транзитивное и трихотомическое отношение.

В рассмотренных нами примерах упорядочение не было «полным»: отношение порядка не обладало трихотомичностью. Действительно, в каждом из примеров нетрудно указать подмножества, одно из которых не содержит другое. Множества такого типа называются *частично упорядоченными* или *полуупорядоченными*.

Множество называется полуупорядоченным, если на нем задано отношение $\leqslant$, обладающее следующими свойствами:

1) оно рефлексивно;
2) антисимметрично;
3) транзитивно.

Во всех примерах, рассмотренных нами перед введением в теорию структур, были определенные подмножества одного «универсального» множества, на которых было задано отношение «принадлежности». Следовательно, $A \leqslant B$ означает для подмножеств A и B, что всякий элемент подмножества A принадлежит подмножеству B. Проверим, можно ли считать, что это отношение частично упорядочивает подмножества данного множества.

Так как любой элемент подмножества A принадлежит подмножеству A, то это отношение рефлексивно. Если любой элемент подмножества A принадлежит подмножеству B, а любой элемент подмножества B принадлежит подмножеству A, то оба подмножества состоят из одних и тех же элементов и, следовательно, совпадают, в силу чего отношение антисимметрично. Наконец, если любой элемент подмножества A принадлежит подмножеству B, а любой элемент подмножества B принадлежит подмножеству C, то все элементы подмножества A принадлежат подмножеству C и отношение транзитивно.

В качестве примера частично упорядоченного множества можно было бы взять произвольное множество с заданным на нем отношением «совпадения», то есть отношением $a \leqslant b$, которое выполняется, если элементы a и b совпадают. Нетрудно видеть, что «совпадение» рефлексивно, антисимметрично и транзитивно, то есть обладает всеми свойствами отно-

шения, устанавливающего частичную упорядоченность. (Аналогичный пример можно было бы привести и с множествами, построив набор подмножеств какого-нибудь множества, ни одно из которых не содержит другого подмножества.) Производить операции над элементами нашего частично упорядоченного множества было бы невозможно, поскольку ни «пересечение», ни «объединение» элементов не определены. Чтобы операции стали выполнимыми, в общем случае необходимо уметь из любых двух элементов находить «непосредственно меньший» и «непосредственно больший». Сначала мы дадим точное определение того, какой из двух элементов «меньший» и какой «больший», а затем поясним, как следует понимать выражение «один элемент непосредственно следует за другим».

Элемент u частично упорядоченного множества называется *нижней гранью* элементов a и b, если $u \leqslant a$ и $u \leqslant b$. Элемент v называется *верхней гранью* элементов a и b, если $a \leqslant v$ и $b \leqslant v$.

Элемент x частично упорядоченного множества называется *наибольшей нижней гранью* элементов a и b, если он является их нижней гранью и для любой нижней грани u элементов a и b выполняется отношение $u \leqslant x$. Элемент y называется *наименьшей верхней гранью* элементов a и b, если он является их верхней гранью и для любой верхней грани v элементов a и b выполняется отношение $y \leqslant v$.

Введя понятия наибольшей нижней и наименьшей верхней грани, мы почти построили структуру: не оговорено лишь, что и наибольшая нижняя, и наименьшая верхняя грань элементов a и b однозначно определены. Но такая оговорка была бы совершенно излишней, потому что если для двух элементов частично упорядоченного множества существует наибольшая нижняя или наименьшая верхняя грань, то она однозначно определена.

Оба утверждения доказываются аналогично, поэтому мы приведем доказательство лишь первого из них. Если каждый из элементов x и t служит наибольшей нижней гранью элементов a и b, то $t \leqslant x$, так как x — наибольшая нижняя грань, а t — нижняя грань. Если t рассматривать как наибольшую нижнюю грань, а x как нижнюю грань, то получим отношение $x \leqslant t$. Из отношений $t \leqslant x$ и $x \leqslant t$ (в силу антисимметричности) следует, что $x = t$.

Итак, взятие наибольшей нижней и наименьшей верхней грани можно рассматривать как операции, поскольку и наибольшая нижняя, и наименьшая верхняя грань (если они существуют) однозначно определены.

Если для элементов a и b упорядоченного множества существует наибольшая нижняя (наименьшая верхняя грань), то она называется пересечением (объединением) элементов a и b. Пересечение элементов обозначается $a \cap b$, а объединение — $a \cup b$.

Если для любых двух элементов частично упорядоченного множества существует пересечение и объединение, то элементы этого множества образуют относительно операций взятия пересечения и объединения структуру.

Проверим, что нам действительно удалось построить структуру.

1. Доказательство идемпотентности: для «элементов» a и a как наибольшая нижняя, так и наименьшая верхняя грань совпадают с a, что и доказывает идемпотентность пересечения и объединения.

2. Доказательство коммутативности: так как и в определение наибольшей нижней грани, и в определение наименьшей верхней грани оба элемента входят симметрично, то $a \cap b$ совпадает с $b \cap a$, а $a \cup b$ — с $b \cup a$.

3. Для доказательства ассоциативности необходимо убедиться в том, что $(a \cap b) \cap c$ — наибольшая нижняя грань элементов a, b и c, то есть что элемент $(a \cap b) \cap c$ не больше (меньше или равен) каждого из элементов a, b и c и не меньше (больше или равен) любого из элементов, меньших или равных элементам a, b и c. Действительно, так как элемент $x = (a \cap b) \cap c$ — нижняя грань элементов $a \cap b$ и c, то $x \leqslant a \cap b$ и $x \leqslant c$. В свою очередь из отношения $x \leqslant a \cap b$ следует, что $x \leqslant a$ и $x \leqslant b$. Итак, мы установили, что выполняются три отношения: $x \leqslant a$, $x \leqslant b$ и $x \leqslant c$. Но если

$u \leqslant a$ и $u \leqslant b$, то $u \leqslant a \cap b$. Если выполняется еще и отношение $u \leqslant c$, то $u \leqslant (a \cap b) \cap c$, то есть x не меньше (больше или равен) любой из трех нижних граней.

Используя коммутативность пересечения, получаем: $a \cap (b \cap c) = (b \cap c) \cap a$. Это означает, что элемент $a \cap (b \cap c)$—наибольшая нижняя грань элементов b, c и a. Поскольку наибольшая нижняя грань однозначно определена (для трех элементов это утверждение выполняется так же, как и для двух элементов), то элементы $(a \cap b) \cap c$ и $a \cap (b \cap c)$ равны. Тем самым ассоциативность пересечения доказана.

Ассоциативность объединения доказывается аналогично.

4. Для доказательства закона поглощения воспользуемся следующими очевидными фактами: если $u \leqslant v$, то, с одной стороны, $u \cap v = u$, а с другой стороны, $u \cup v = v$. Так как $a \leqslant a \cup b$, то $a \cap (a \cup b) = a$, а поскольку $a \cap b \leqslant b$, то $(a \cap b) \cup b = b$.

Превращение частично упорядоченного множества в структуры весьма «выгодно»: оно позволяет «нарисовать» множество (о чем пойдет речь несколько ниже) и «увидеть» структуру. Вопрос состоит лишь в том, все ли структуры удастся «проявить», то есть все ли структуры можно получить из частично упорядоченных множеств изложенным выше способом. Ответ на этот вопрос утвердительный: во всех структурах можно задать частичное упорядочение так, чтобы для любых двух элементов получившегося частично упорядоченного множества существовали наибольшая нижняя и наименьшая верхняя грани, совпадающие соответственно с пересечением и с объединением этих двух элементов.

Во всякой структуре можно задать частичное упорядочение.

Чтобы доказать это утверждение, рассмотрим произвольную структуру. Если бы она уже была частично упорядоченным множеством, то отношение $a \leqslant b$ при помощи двух заданных на структуре операций можно было бы выразить двояко: как $a \cap b = a$ или как $a \cup b = b$. Действительно, оба соотношения следуют из условия $a \leqslant b$ и справедливы лишь в том случае, если это условие выполнено. Но для структур было доказано, что соотношение $a \cap b = a$ выполняется в том и только в том случае, если $a \cup b = b$. Следовательно, в структурах частичное упорядочение удобно задавать следующим образом:

отношение $a \leqslant b$ выполняется для элементов a и b структуры, если $a \cap b = a$.

Покажем, что это отношение действительно позволяет получить из структуры частично упорядоченное множество.

1. Отношение рефлексивно. Действительно, в силу идемпотентности пересечения $a \cap a = a$, а это и означает, что введенное нами отношение рефлексивно.

2. Отношение антисимметрично. Пусть $a \leqslant b$ и $b \leqslant a$. Тогда $a \cap b = a$ и $b \cap a = b$. Поскольку пересечение коммутативно, то $a = a \cap b = b \cap a = b$. Тем самым антисимметричность отношения доказана.

3. Для доказательства транзитивности предположим, что $a \leqslant b$ и $b \leqslant c$. Это означает, что $a \cap b = a$ и $b \cap c = b$. Подставляя b из последнего соотношения в первое, получаем:

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

(производя преобразования, мы воспользовались ассоциативностью пересечения и соотношением $a \cap b = a$). Полученное соотношение $a = a \cap c$ означает, что $a \leqslant c$. Следовательно, введенное нами отношение транзитивно.

Остается еще доказать, что для любых двух элементов существуют наибольшая нижняя и наименьшая верхняя грань, совпадающие к тому же соответственно с элементами $a \cap b$ и $a \cup b$. Именно это и позволяет упростить остальную часть доказательства, поскольку *известны те элементы*, относительно которых требуется доказать, что они являются наибольшей нижней и наименьшей верхней гранью.

Из тождеств, которым удовлетворяет пересечение, следует, что

$$(a \cap b) \cap a = (a \cap a) \cap b = a \cap b$$

и аналогично, что $(a \cap b) \cap b = a \cap b$. Но именно это и означает, что $a \cap b$ — нижняя грань элементов a и b. Если x — любая нижняя грань элементов a и b, то, используя соотношения $x \cap a = x \cap b = x$ и тождества для пересечения, получаем:

$$x \cap (a \cap b) = (x \cap a) \cap b = x \cap b = x.$$

Следовательно, $a \cap b$ — наибольшая нижняя грань элементов a и b. Доказательство утверждения относительно объеди-

нения несколько сложнее и значительно упростилось бы, если бы частичное упорядочение структуры можно было задать при помощи объединения. Поскольку это действительно можно сделать (так как соотношения $a \cap b = a$ и $a \cup b = b$ выполняются одновременно), то доказательство утверждения относительно объединения слово в слово (с учетом принципа двойственности) воспроизводит приведенное выше доказательство утверждения о пересечении.

Итак, доказано, что из частично упорядоченного множества (в определенных случаях) можно построить структуру, а из структуры — частично упорядоченное множество (причем именно такое, из которого можно построить структуру). Это означает, что можно поступить следующим образом: взяв некоторую структуру, построить из нее частично упорядоченное множество, а из него опять построить структуру или. выбрав какое-нибудь частично упорядоченное множество, построить из него структуру (если это возможно), а из нее опять построить частично упорядоченное множество. Заранее не предполагается, хотя это и так, что «вторичная» структура, созданная из частично упорядоченного множества, которое построено из «первичной» структуры, совпадает с первичной структурой. (Следовательно, определенные «окольным путем» операции вторичной структуры в действительности оказываются такими же, как операции в исходной структуре.) Аналогичным образом отношение, заданное на структуре, построенной из частично упорядоченного множества, совпадает с исходным отношением. (Доказательство этого утверждения, вообще говоря, не сложно: необходимо лишь произвести кое-какие выкладки. Тем не менее мы не будем приводить доказательства, поскольку оно достаточно длинно и громоздко.)

Всякую структуру можно построить из соответствующим образом выбранного частично упорядоченного множества.

Но, как было доказано выше, в любой структуре можно задать частичное упорядочение. Если структура содержит лишь конечное число элементов, то возникает конечное частично упорядоченное множество, которое можно «нарисовать». Такой подход позволяет получать «портреты» конечных структур и даже конечных частей (не обязательно подструктур) бесконечных структур.

Условимся, изображая конечное частичное множество, помещать наименьший элемент в самом низу, а бо́льшие элементы располагать выше. Поскольку одного лишь такого правила недостаточно для построения изображения, мы будем проводить линии, показывающие, какой из двух элементов больше и какой — меньше другого. При этом, разумеется, мы не станем проводить все возможные линии, поскольку неравенство «больше — меньше» достаточно указать лишь для «непосредственно следующих друг за другом» элементов, после чего уже можно без труда определять, какой из любых двух элементов больше или меньше.

Наши «правила» допускают следующую точную формулировку. *Элемент b непосредственно следует за элементом a, а элемент a непосредственно предшествует элементу b, если $a \leqslant b$, элементы a и b различны и не существует элемента x, отличного от элементов a и b, который удовлетворял бы отношениям $a \leqslant x \leqslant b$.* Если $u \leqslant v$ и элементы u и v различны, то v может непосредственно следовать за u. В противном случае найдется элемент x, отличный от u и от v и такой, что $u \leqslant x \leqslant v$. Следовательно, элемент x можно «вписать» между элементами a и b. Поскольку упорядочению подлежит конечное число элементов, то оно рано или поздно завершается. Все элементы множества оказываются внесенными в «список» $u \leqslant x_1 \leqslant x_2 \leqslant \ldots \leqslant x_n \leqslant v$, элементы u, x_1, x_2, ..., x_n, v различны и каждый элемент непосредственно следует за предыдущим. Таким образом, отношение $u \leqslant v$ означает, что существуют элементы, которые

Частично упорядоченное множество из двух элементов, между которыми имеется одно отношение

Частично упорядоченное множество из двух элементов, между которыми нет ни одного отношения

Рис. 89.

можно расположить по порядку $u \leqslant x_1 \leqslant x_2 \leqslant \ldots \leqslant x_n \leqslant v$, и каждый следующий элемент следует непосредственно за предыдущим. Поэтому достаточно знать, какие элементы и за какими следуют непосредственно. Если «непосредственное следование» обозначить прямой, идущей снизу вверх, то оно однозначно определит частичное упорядочение на множестве элементов структуры.

Рассмотрим теперь несколько «портретов» частично упорядоченных множеств. Прежде всего заметим, что «нарисовать» пустое множество невозможно, изображение множества из одного элемента не представляет интереса, поскольку в нем нет двух элементов и, следовательно, нет элемента, который непосредственно следовал бы за другим элементом.

В множестве из двух элементов между двумя элементами может существовать либо одно отношение, либо ни одного отношения. Следовательно, при рассмотрении таких множеств могут представиться два случая (рис. 89).

Возможные портреты частично упорядоченных множеств с тремя элементами показаны на рис. 90.

Рассмотрим теперь несколько структур. Пустое множество не принадлежит к числу структур (так же, как оно не принадлежит и к числу групп, но рассматривать его как частично упорядоченное множество вполне допустимо). Множество из одного элемента является структурой, поскольку для любых «двух» его элементов существует наименьшая верхняя и наибольшая нижняя грань. Единственный элемент множества является одновременно нулевым и единичным элементом структуры. Из множеств с двумя элементами к числу структур принадлежит то, между элементами которого задано отношение. Меньший элемент служит нулевым, а больший — единичным элементом структуры. В другом множестве из двух элементов не существует ни верхней, ни нижней грани для элементов.

В том множестве из трех элементов, в котором имеется три отношения, пересечением любых двух элементов служит меньший из них, а объединением — больший. Следовательно, наименьшим из трех элементов является нулевой элемент, а наибольшим — единичный элемент. В первом множестве из трех элементов с двумя отношениями для двух меньших элементов не существует нижней грани, а во втором множестве для двух бо́льших элементов не существует верхней грани. В множестве из трех элементов с одним отношением для «изолированного» элемента, рассматриваемого в паре с любым другим элементом, не существует ни общей нижней, ни общей верхней гра-

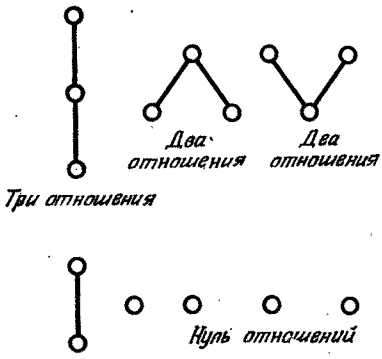


Рис. 90.

ни. Наконец, в множестве из трех элементов без отношений для любых двух элементов не существует ни общей нижней, ни общей верхней грани.

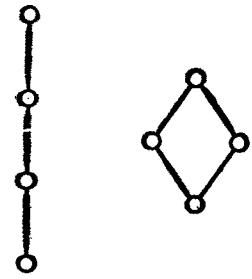
В рассмотренных нами конечных структурах всегда существовали нулевой элемент и единичный элемент. Это не случайно. Нулевой и единичный элементы существуют в любой конечной структуре.

Во всякой конечной структуре существуют нулевой и единичный элементы.

Пересечение всех элементов структуры (однозначно определенное в силу ассоциативности) не больше (то есть меньше или равно) любого элемента структуры и поэтому совпадает с нулевым элементом. Аналогично объединение всех элементов структуры совпадает с единичным элементом.

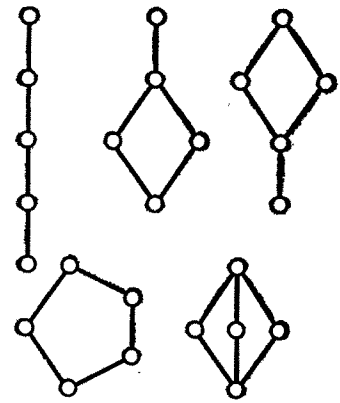
Это замечание оказывается весьма полезным при рассмотрении структур с более чем тремя элементами. Действительно, при изучении структуры с двумя элементами было как их разместить: наименьший элемент должен располагаться в самом низу, наибольший — в самом верху. Следовательно, встретив структуру из четырех элементов, мы заведомо знаем, что два других элемента должны образовывать какое-то из «двухэлементных» частично упорядоченных множеств. Существует всего два таких множества, поэтому и структуры из четырех элементов возможны в двух вариантах. Нетрудно видеть, что оба варианта существуют (рис. 91).

Аналогичные соображения применимы и к анализу структур из пяти элементов. Положение двух элементов определено заранее, а относительно трех остальных элементов известно, что они образуют частично упорядоченное множество. Поскольку существует всего пять частично упорядоченных множеств из трех элементов, то и структуры из пяти элементов возможны в пяти вариантах. Все пять типов структур существуют (рис. 92).



Диаграммы двух структур из четырех элементов

Рис. 91.



Диаграммы структур из пяти элементов

Рис. 92.

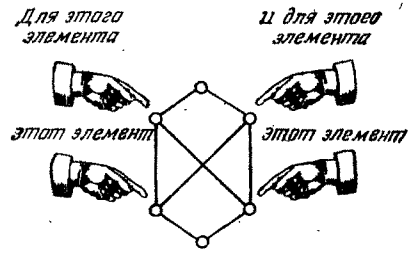


Рис. 93.

Заметим, что из некоторых частично упорядоченных множеств структура может не получиться не только из-за отсутствия верхней или нижней грани для некоторых элементов, но и из-за чрезмерного «изобилия» верхних и нижних граней.

Одна из «не состоявшихся структур» изображена на рис. 93.

Двоякие свойства структур позволяют в отдельных случаях использовать частичное упорядочение. Весьма полезны, например, свойства такого рода: «объединение малых элементов меньше, чем пересечение больших элементов». В более точной формулировке это утверждение гласит следующее:

если структура состоит из элементов $a_1, a_2, \ldots, a_n$ *и* $b_1, b_2, \ldots, b_k$ *и для любой пары* a_i, b_j *выполняется отношение* $a_i \leqslant b_j$, *то для наименьшей верхней грани* a *элементов* a_i *и наибольшей нижней грани* b *элементов* b_j *справедливо отношение* $a \leqslant b$.

По условию все элементы a_i служат верхними гранями любого элемента b_j. Следовательно, каждый из элементов b_j не меньше (больше или равен) верхней грани a элементов a_i. Но это означает, что a — нижняя грань элементов b_j и поэтому не больше (меньше или равна) наибольшей нижней грани b элементов b_j.

Приведенное выше утверждение позволяет без труда доказывать «неравенства», в которые в качестве меньшего элемента входит объединение, а в качестве большего — пересечение. Докажем, например, что закон дистрибутивности верен «в одну сторону» для любой структуры.

Пусть a, b и c — три элемента структуры. Так как $a \cap b \leqslant a$, $a \cap b \leqslant b$ и $a \leqslant a \cup c$, $b \leqslant b \cup c$, то в силу транзитивности частичного упорядочения $a \cap b \leqslant a \cup c$ и $a \cap b \leqslant b \cup c$. А поскольку ясно, что $c \leqslant a \cup c$ и $c \leqslant b \cup c$, то

$$(a \cap b) \cup c \leqslant (a \cup c) \cap (b \cup c).$$

Напомним, что это «неравенство» составляет ту «половину» закона дистрибутивности, которая была доказана без обращения к отдельным элементам. Нетрудно видеть, что необходимости в обращении к элементам подмножеств действительно не было, поскольку операции или отношения выражают лишь определенное свойство взаимосвязи между подмножествами.

Частичное упорядочение позволяет сформулировать свойство, некогда характеризовавшее подпространства векторного пространства. Еще при «первой встрече» с этим свойством мы упоминали о том, что оно присуще не только подпространствам векторного пространства, но и подгруппам коммутативной группы. В общем случае подмодули произвольного модуля образуют структуру, наделенную тем особым свойством, о котором идет речь. Такие структуры называются поэтому *модулярными* (или *дедекиндовыми*).

Что касается равенства $(a \cap b) \cup c = a \cap (b \cup c)$, входящего в определение модулярной структуры, то, заменив его «неравенством в одну сторону», мы получим отношение, выполняющееся для всех структур. Действительно, «неравенства» $a \cap b \leqslant a$, $a \cap b \leqslant b \cup c$ и $c \leqslant b \cup c$ очевидны, а отношение $a \leqslant c$ выполняется по условию, откуда и следует, что $(a \cap b) \cup c \leqslant a \cap (b \cup c)$.

Разумеется, всякая модулярная структура является одновременно и «просто» структурой. Нетрудно доказать, что всякая дистрибутивная структура модулярна. Действительно, в тождество $(a \cap b) \cup c = (a \cup c) \cap (b \cup c)$, выражающее закон дистрибутивности при $a \leqslant c$, вместо объединения $a \cup b$ можно подставить равный ему элемент a и получить соотношение, означающее, что структура модулярна.

Структура называется модулярной, если для любого элемента b и $a \geqslant c$ выполняется соотношение

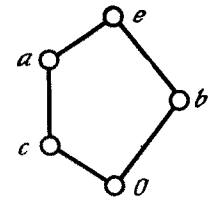
$$(a \cap b) \cup c = a \cap (b \cup c).$$

Заранее не очевидно, следует ли из модулярности дистрибутивность структуры и не будут ли все структуры модулярными. Докажем, что ответы на оба вопроса отрицательные: построим примеры, в одном из которых структура не модулярна, а в другом модулярна, но не дистрибутивна. (С примерами такого рода нам по существу приходилось встречаться и раньше, но приводимые теперь примеры необычайно важны.) На

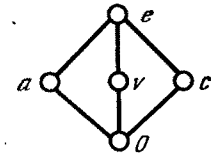
рис. 94 показаны диаграммы двух структур, одна из которых не модулярна, а другая модулярна, но не дистрибутивна.

В первом примере выполняется отношение $a \geqslant c$, но $(a \cap b) \cup c = 0 \cup c = c$, а $a \cap (b \cup c) = a \cap e = a$, а элементы c и a не равны.

Во втором примере, как нетрудно видеть, структура не дистрибутивна. Действительно, $(a \cap b) \cup c = 0 \cup c = c$, $(a \cup c) \cap (b \cup c) = e \cap e = e$, а элементы c и e различны. Во избежание путаницы в обозначениях запишем условие модулярности в следующем виде: если $u \geqslant v$, то $(u \cap t) \cup v = u \cap (t \cup v)$. При $u = v$ обе стороны равенства по закону поглощения переходят в элемент u. Если же элементы u и v различны, то либо $v = 0$, либо $u = e$. В первом случае в правой и в левой частях равенства стоит $u \cap t$, во втором — элемент $t \cup v$. И в том, и в другом случаях структура модулярна.



а) Немодулярная и недистрибутивная структура из пяти элементов



б) Модулярная, но не дистрибутивная структура из пяти элементов

Рис. 94.

ЗАДАЧИ

1. Верно ли утверждение, что структур из n элементов существует столько же, сколько частично упорядоченных множеств из $n - 2$ элементов?

2. Доказать, что для всякой структуры

$$(a \cap b) \cup (b \cap c) \cup (c \cap a) \leqslant$$
$$\leqslant (a \cup b) \cap (b \cup c) \cap (c \cup a).$$

3. Доказать, что на всяком упорядоченном множестве можно задать операции структуры и полученная структура всегда будет дистрибутивной.

2.

Соотношения между структурами

2.1. Подструктура, гомоморфизм, прямое произведение

Изучая группы, кольца и тому подобные «образования», мы говорили о «частях», напоминающих по своим свойствам «целое»: подгруппах, подкольцах и т. д. Рассматривая структуры, можно было бы попытаться ввести понятие подструктуры. Подструктурой естественно назвать подмножество элементов структуры, образующих «самостоятельную» структуру (относительно операций, заданных на исходной структуре). Излишне проверять для подструктуры тождества, которым должны удовлетворять операции, поскольку эти тождества выполняются «автоматически»: по предположению они справедливы для любых элементов исходной структуры, в том числе и тех, которые образуют подструктуру. Но условия, входящие в определение структуры, носят достаточно общий характер и лишь в исключительных случаях учитывают такие «мелочи», как существование отдельных элементов. Именно поэтому необходимо проверить, замкнута ли выбранная «часть» структуры относительно взятия объединения и пересечения.

Любое (непустое) подмножество элементов структуры называется подструктурой, если оно вместе с любыми двумя своими элементами содержит их объединение и пересечение.

Построение структур во многом

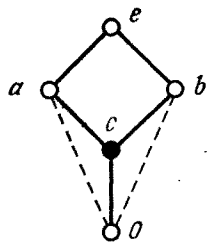


Рис. 95.

облегчалось тем, что их можно было изобразить наглядно в виде частично упорядоченных множеств. Было бы весьма «кстати», если бы и подструктуры нам удалось представить в виде соответствующих подмножеств частично упорядоченных множеств. Ясно, что любое подмножество элементов структуры (как частично упорядоченного множества) является частично упорядоченным множеством. Разумеется, далеко не каждое подмножество может быть подструктурой. Требуется ввести особое предположение о том, что получившееся частично упорядоченное множество является структурой относительно частичного упорядочения, заданного во всем множестве. Но и этого мало. Рассмотрим, например, структуру из пяти элементов, изображенную на рис. 95. Подмножество, состоящее из элементов a, b, 0 и e, образует структуру относительно частичного упорядочения, заданного на всей исходной структуре, но пересечением элементов a и b в этом подмножестве служит 0, а в исходной структуре — элемент c. Следовательно, выбранное нами подмножество из четырех элементов a, b, 0 и e не замкнуто относительно взятия пересечения.

Тем не менее частично упорядоченные множества можно с успехом использовать при изучении подструктур. Необходимо лишь следить за тем, чтобы объединения или пересечения элементов не «выпадали» из подструктуры, как в рассмотренном выше примере.

Ясно, что если в структуре выполняется какое-нибудь тождество, то оно должно выполняться и в подструктуре. Следовательно, любая подструктура дистрибутивной структуры дистрибутивна, а любая подструктура модулярной структуры модулярна. Иначе говоря, структура, содержащая любую недистрибутивную подструктуру, не дистрибутивна, а структура, содержащая любую немодулярную подструктуру, не модулярна. Среди структур из пяти элементов можно указать две недистрибутивные структуры и одну немодулярную структуру (рис. 94).

Итак, структура, содержащая подструктуру ($а$), не модулярна, а структура, содержащая как подструктуру ($а$), так и подструктуру ($б$), не дистрибутивна. Небезынтересно отметить, что оба утверждения допускают обращение: если структура не содержит подструктуру ($а$), то она модулярна, а если структура не содержит подструктуру ($б$), то она дистрибутивна. (То же можно выразить несколько иначе: если структура не дистрибутивна, то в ней существует либо подструктура ($а$), либо подструктура ($б$); если структура не модулярна, то в ней заведомо существует подструктура ($а$).)

Разумеется, если существование нулевого или единичного элемента (или существование обоих «граничных» элементов) особо оговорено или предполагается, что существуют дополнения элементов, то понятие подструктуры надлежит формулировать так, чтобы она содержала элементы, существование которых постулируется.

Гомоморфизм в случае структур можно определить как однозначное отображение, переводящее «пересечение в пересечение» и «объединение в объединение». Отсюда следует, что гомоморфизм сохраняет частичное упорядочение. Действительно, если $a \leqslant b$, то, поскольку $a \cap b = a$, при любом гомоморфизме φ выполняется соотношение $\varphi(a) = \varphi(a \cap b) = \varphi(a) \cap \varphi(b)$, а это и означает, что $\varphi(a) \leqslant \varphi(b)$. (Гомоморфизм действует из

структуры S_1 в структуру S_2, и в структурах S_1 и S_2 операции и отношения, задающие частичное упорядочение, различны. Однако если мы выберем для этих операций и отношений одинаковые обозначения, то это не приведет ни к каким недоразумениям — разумеется, при условии, что речь идет о различных множествах или о множествах, рассматриваемых как различные.) Можно ожидать, что произвольно выбранное отображение одной структуры в другую, сохраняющее частичную упорядоченность, не будет гомоморфизмом.

Гомоморфизмы структур «ведут себя» гораздо хуже, чем гомоморфизмы групп. Гомоморфизм группы G_1 в группу G_2 отображает в один и тот же элемент группы G_2 целый смежный класс группы G_1 по соответствующему нормальному делителю. Зная любой из смежных классов, можно восстановить все остальные и тем самым по существу задать гомоморфизм. В частности, если гомоморфизм отображает в один элемент группы G_2 лишь один-единственный элемент группы G_1, то под действием этого гомоморфизма различные элементы группы G_1 переходят в различные элементы группы G_2.

С гомоморфизмами структур все обстоит иначе. Один из контрпримеров «образцовому поведению» гомоморфизмов можно привести, даже если структура дистрибутивна. Рассмотрим упорядоченное множество. Если его разделить на части, простирающиеся «отсюда и досюда», и каждую часть стянуть в одну точку независимо от того, что происходит с остальными частями, то получится гомоморфизм, при котором все элементы, которые принадлежат части, тянущейся «отсюда и досюда», отображаются в одну и ту же точку.

Предположим, например, что в точку стягивается лишь одна часть множества, а все остальные остаются «в первозданном виде» (рис. 96) или, если угодно, подвергаются каким-то изменениям. Относительно полученного гомоморфизма нельзя утверждать, ни что любая часть множества, отображаемая в точку, содержит одинаковое число элементов, ни что по одной такой части можно определить все остальные.

Рис. 96.

Мы могли бы говорить о мономорфизме структур — гомоморфизме, отображающем различные элементы в различные, и об изоморфизме — взаимно-однозначном отображении структур. Изоморфные структуры можно считать одинаковыми, поскольку с алгебраической точки зрения между ними нет различий.

Наконец, на структуры можно перенести и понятие прямого произведения. Мы рассмотрим прямое произведение лишь двух структур, но все рассуждения остаются в силе и в том случае, когда число «прямых сомножителей» больше двух. Пусть A и B — две структуры. Обозначим операции, заданные в каждой из них, через $\cup$ и $\cap$. Прямым произведением $A \times B$ этих двух структур называется множество пар (a, b),

где $a \in A$, $b \in B$ и, кроме того, $(a_1, b_1) = (a_2, b_2)$ означает, что $a_1 = a_2$, $b_1 = b_2$, а операции выполняются по следующим правилам:

$$(a_1, b_1) \cup (a_2, b_2) = (a_1 \cup a_2, b_1 \cup b_2)$$

и

$$(a_1, b_1) \cap (a_2, b_2) = (a_1 \cap a_2, b_1 \cap b_2).$$

Нетрудно видеть, что мы опять получили структуру (необходимо лишь проверить все тождества).

Прямое произведение структур обладает необычными свойствами. Например, если фиксировать любой элемент b из структуры B, то множество пар (a, b) всегда образует подструктуру прямого произведения, изоморфную структуре A.

ЗАДАЧИ

1. Найти такие структуры, в которых любое подмножество является подструктурой.

2. Найти такие структуры, в которых любое подмножество, являющееся структурой относительно заданного на исходной структуре частичного упорядочения, представляет собой подструктуру исходной структуры.

3. Доказать, что любой элемент всякой структуры, содержащей не менее двух элементов, принадлежит некоторой подструктуре, отличной от всей структуры.

4. Верно ли, что пересечение подструктур одной структуры также является подструктурой?

5. Можно ли говорить о подструктуре, что она порождена определенными элементами структуры?

6. Доказать, что существует взаимно-однозначное отображение одной структуры из четырех элементов на другую, сохраняющее частичное упорядочение, но не являющееся изоморфизмом.

2.2. Идеал, примарный идеал, логические связки

При гомоморфизме структуры S_1 в структуру S_2 множество элементов из S_1, переходящих в один и тот же элемент из S_2, не может быть произвольным. Если φ — гомоморфизм структур и $\varphi(a) = \varphi(b)$, то, поскольку φ сохраняет операции, получаем (используя идемпотентность объединения и пересечения): $\varphi(a \cap b) = \varphi(a) \cap \varphi(b) = \varphi(a)$ и $\varphi(a \cup b) = \varphi(a) \cup \varphi(b) = \varphi(a)$, то есть образы объединения и пересечения элементов a и b совпадают с образом элемента a (а следовательно, и b). То же можно сформулировать несколько иначе: множество элементов из S_1, отображаемых гомоморфизмом φ в один и тот же элемент из S_2, всегда образуют подструктуру. Но эта подструктура не произвольна. Например, если структура содержит нулевой и единичный элементы, то они, очевидно, образуют подструктуру. Если эти «граничные» элементы переходят при гомоморфизме в один и тот же элемент, то их образ (в «структуре» образов) будет одновременно и нулевым, и единичным элементом, а это означает, что он будет образом всех элементов. Следовательно, о структуре, состоящей из двух элементов, не может быть и речи. В общем случае, если $a \leqslant b$ и $\varphi(a) = \varphi(b)$, то образ любого элемента x, удовлетворяющего условию $a \leqslant x \leqslant b$, будет совпадать с образом элементов a и b. Действительно, по условию $x = a \cup x$ и $x = x \cap b$, откуда $x = a \cup (x \cap b)$ и $\varphi(x) = \varphi(a) \cup (\varphi(x) \cap \varphi(b))$. Из условия $a \leqslant x \leqslant b$ и закона поглощения следует, что элемент, стоящий в правой части, совпадает с $\varphi(a)$. Подструктура, обладающая этим свойством, называется *выпуклой подструктурой*. (Заметим, что отнюдь не всякая выпуклая подструктура встречается среди множеств элементов, переходящих при гомоморфизме в один и тот же элемент.)

Особенно важную роль играют выпуклые подструктуры, которые могут отображаться при гомоморфизмах в нулевой и в единичный элементы (в тех случаях, когда исходная структура не содержит ни нулевого, ни единичного элементов).

Предположим, что к структуре добавлен новый элемент, который меньше всех остальных элементов. Отобразив новый элемент в нулевой элемент, мы получим тот же гомоморфизм, что и прежде. Если этот гомоморфизм отображает элемент a в нулевой элемент и $x \leqslant a$, то (так как $0 \leqslant x$) в силу выпуклости элемент также переходит в нулевой элемент.

Подструктура структуры, содержащая вместе с любым элементом a все элементы x, удовлетворяющие условию $x \leqslant a$, называется *идеалом структуры*.

Подструктура структуры, содержащая вместе с любым элементом a все элементы x, удовлетворяющие условию $a \leqslant x$, называется *двойственным идеалом* (рис. 97).

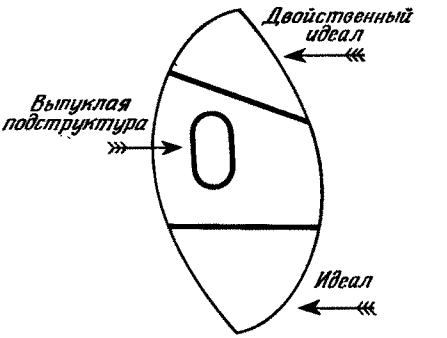


Рис. 97.

Подмножество I называется идеалом структуры H, если:

1) I замкнуто относительно объединения;

2) из $a \in I$ и $x \leqslant a$ следует, что $x \in I$ (и I не пусто).

Подмножество D называется двойственным идеалом структуры H, если:

1) D замкнуто относительно пересечения;

2) из $b \in D$ и $y \geqslant b$ следует, что $y \in D$ (и D — не вся структура).

Любой элемент структуры определяет идеал, состоящий из элементов, которые не больше его. Выберем, например, произвольный элемент c. Если $a \leqslant c$ и $b \leqslant c$, то каждый из элементов a и b служит нижней гранью для c, и поэтому $a \cup b \leqslant c$. Если $x \leqslant a$, то в силу транзитивности отношения, задающего частичное упорядочение, $x \leqslant c$, а так как $a \cap b \leqslant a$, то отсюда следует замкнутость относительно пересечения. Полученный идеал обозначим $(c)_i$. Аналогично элементы, которые не меньше элемента c, образуют двойственный идеал $(c)_d$. Можно показать, что в конечной структуре существуют идеалы только типа $(c)_i$ и двойственные идеалы только типа $(c)_d$. Следовательно, во всякой конечной структуре имеется столько идеалов и двойственных идеалов, сколько она содержит элементов (рис. 98).

Пустое множество естественно не относить к числу идеалов, но из соображений удобства пустое множество можно считать двойственным идеалом (в отличие от всей структуры, которую исключают из числа двойственных идеалов, хотя она и удовлетворяет определению).

Если в определении идеала потребовать, чтобы вместе с любым своим элементом он содержал и все меньшие элементы, то отпадет необходимость в предположении о замкнутости относительно пересечения, поскольку пересечение двух элементов не больше каждого из них. Следовательно, это (и аналогичное ему) свойство позволяют определить идеал и двойственный идеал.

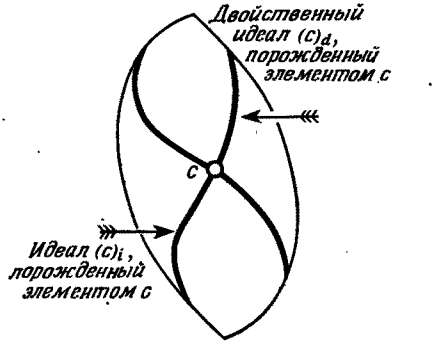


Рис. 98.

Рис. 99.

Рассматривая условия (1) и (2) в определениях идеала и двойственного идеала, нетрудно заметить, что условия (1) двойственны (условия (2) также можно считать двойственными). Действительно, разобьем структуру H на две части A и B так, чтобы они не имели общих элементов, а любой элемент из H принадлежал какой-нибудь из них. (Иначе говоря, если A и B рассматривать как подмножества структуры H, то A является дополнением для B, а B — дополнением для A.) Условие (2), входящее в определение идеала, выполняется для A в том и только в том случае, когда для B выполняется условие (2), входящее в определение двойственного идеала. Действительно, если условие (2) для A выполнено и $b \in B$, то при $y \geqslant b$ элемент y не может принадлежать подмножеству A, поскольку в противном случае A содержало бы элемент b. Следовательно, $y \in B$. Аналогично, если условие (2) выполняется для B, то $a \in A$ и при $x \leqslant a$ элемент x не может принадлежать подмножеству B, поскольку в противном случае элемент a был бы из B. Следовательно, $x \in A$.

О разбиении структуры на подмножества A и B, обладающие перечисленными выше свойствами, принято говорить как о *сечении*. Подмножество A называется *нижним*, а подмножество B — *верхним сегментом* структуры (рис. 99).

В общем случае при сечении структуры нижний сегмент не является идеалом, а верхний сегмент — двойственным идеалом. Если же нижний сегмент удовлетворяет определению идеала, а нижний сегмент — определению двойственного идеала, то говорят соответственно о *примарном идеале* и *двойственном примарном идеале*. Эти понятия играют весьма важную роль в теории структур.

Примарный идеал и двойственный примарный идеал можно получить следующим образом. Если φ — гомоморфизм структуры H в структуру из двух элементов, то под действием φ в нуль переходят элементы нижнего сегмента структуры, образующие примарный идеал, а в единичный элемент — элементы верхнего сегмента структуры при том же сечении, образующие двойственный примарный идеал.

Свойство гомоморфизма сохранять упорядочение приводит к тому, что элементы, отображаемые гомоморфизмом в нулевой и в единичной элементы, образуют соответственно нижний и верхний сегменты. Если элементы a и b принадлежат нижнему сегменту, то — так как $\varphi(a \cup b) = \varphi(a) \cup \varphi(b) = 0 \cup 0 = 0$ — объединение $a \cup b$ также принадлежит нижнему сегменту. Если же оба элемента a и b принадлежат нижнему сегменту, то — так как $\varphi(a \cap b) = \varphi(a) \cap \varphi(b) = e \cap e = e$ — и их пересечение $a \cap b$ также принадлежит верхнему сегменту. Следовательно, нижний сегмент является идеалом, а верхний — двойственным идеалом, что и требовалось доказать.

Приведенное здесь свойство полностью определяет примарный идеал. Иначе говоря, примарный идеал можно получить, лишь отображая структуру в структуру из двух элементов: примарный идеал образуют элементы, переходящие при гомоморфизме в нулевой элемент. Итак, требуется доказать, что для любого примарного идеала можно найти соответствующий гомоморфизм. Ясно, что таким гомоморфизмом может быть лишь отображение, переводящее элементы примарного идеала в нулевой элемент структуры из двух элемен-

тов, а элементы двойственного примарного идеала — в единичный элемент структуры из двух элементов (именно в этом по существу и состоит приведенное выше утверждение). Следовательно, необходимо доказать, что (однозначно определенное) отображение, о котором идет речь, представляет собой гомоморфизм.

Если элементы a и b принадлежат идеалу, то их пересечение $a \cap b$ также принадлежит идеалу (поскольку $a \cap b$ не больше элементов идеала a и b). Следовательно, $\varphi(a \cap b)$ — нулевой элемент структуры из двух элементов и $\varphi(a) \cap \varphi(b)$ — также нулевой элемент, поскольку каждый из элементов $\varphi(a)$ и $\varphi(b)$ совпадает с нулевым элементом. Если же элементы a и b принадлежат двойственному идеалу, то их объединение $a \cup b$ также принадлежит двойственному идеалу. Следовательно, каждый из элементов $\varphi(a)$, $\varphi(b)$ и $\varphi(a \cup b)$ совпадает с единичным элементом структуры из двух элементов, а это означает, что объединение первых двух из них совпадает с третьим (рис. 100).

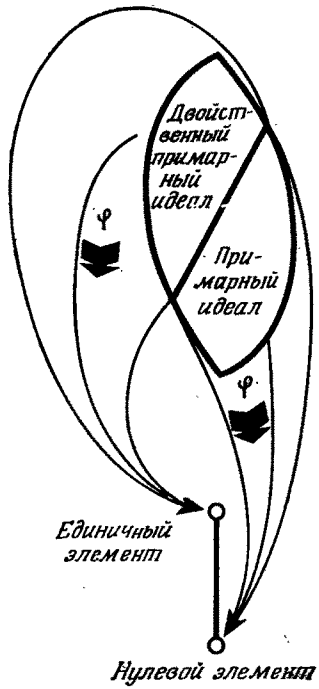


Рис. 100.

Структуры и примарные идеалы весьма тесно связаны с «формальной» логикой и посредством нее — с вычислительными машинами. Рассмотрим какие-нибудь высказывания, например «день жаркий» или «собака лает», независимо от того, истинны они или нет. (Во многих случаях определить истинно ли то или иное высказывание бывает довольно затруднительно: одно и то же высказывание может быть иногда истинным, а иногда ложным.) Из заданных высказываний образуем новые, связывая исходные высказывания союзами (называемыми логическими связками) «*и*» и «*или*». Одно из полученных «составных» высказываний «день жаркий *и* собака лает» утверждает, что оба начальных высказывания выполняются одновременно (независимо от того, выполняются ли они в действительности). Другое составное высказывание «день жаркий *или* собака лает» утверждает, что выполняется по крайней мере одно из входящих в него высказываний (а может быть, и оба высказывания).

Введенные нами «операции» над высказываниями удовлетворяют таким же тождествам, как и «настоящие» операции в структурах. Например, оба составных высказывания «день жаркий *и* день жаркий» и «день жаркий *или* день жаркий» означают, что «день жаркий» (идемпотентность). Коммутативность и ассоциативность не требуют особого доказательства, поскольку безразлично, в каком порядке мы произносим высказывания. Следующее высказывание: «(день жаркий *и* собака лает) *или* (день жаркий)» означает лишь, что «день жаркий *или* день жаркий» и, кроме того, «собака лает». Действительно, не зависит от «собачьего лая» лишь та часть составного высказывания, в которой утверждается, что «день жаркий». Следовательно, для логических связок выполняется закон поглощения. (Нетрудно понять, что выполняются оба закона поглощения.) Таким образом, высказывания образуют относительно введенных нами операций структуру, причем эта структура дистрибутивна.

Выясним теперь, что произойдет, если одни высказывания, входящие в составные высказывания, «истинны», а другие «ложны» (то есть не истинны). Рассмотрим два утверждения и обозначим их A и B. Возможны следующие случаи:

A	B	A *и* B	A *или* B
истинно	истинно	истинно	истинно
истинно	ложно	ложно	истинно
ложно	истинно	ложно	истинно
ложно	ложно	ложно	ложно

Если логическую связку *и* обозначить $\bigcap$, а логическую связку *или* обозначить $\bigcup$, то эту таблицу можно записать в следующем виде:

истинно $\bigcap$ истинно = истинно
истинно $\bigcap$ ложно = ложно
ложно $\bigcap$ истинно = ложно
ложно $\bigcap$ ложно = ложно

истинно $\bigcup$ истинно = истинно
истинно $\bigcup$ ложно = истинно
ложно $\bigcup$ истинно = истинно
ложно $\bigcup$ ложно = ложно

Такие соотношения мы получили бы для структуры из двух элементов, в которой «истинно» отождествлено с единичным элементом, а «ложно» с нулевым элементом. Иначе говоря, логическую связку *и* можно рассматривать как пересечение, а логическую связку *или* как объединение. Истинности одних и ложности других высказываний соответствует при этом гомоморфное отображение исходной структуры в структуру из двух элементов. «Ложными» называются прообразы нулевого элемента (образующие примарный идеал), «истинными» — прообразы единичного элемента (образующие двойственный примарный идеал).

Наконец, нельзя не упомянуть еще об одном результате, относящемся к идеалам структур. Если I — произвольный идеал, а u — произвольный элемент структуры, то обозначим через $\{I, u\}$ наименьший идеал, содержащий элемент u и идеал I. Нетрудно видеть, что такой идеал всегда существует, но мы все-таки докажем, что множество $\{I, u\}$ — идеал. (Собственно говоря, «интерес» представляет только случай, когда элемент u не принадлежит идеалу I, но предположение о том, что $u \notin I$, было бы излишним, так как в процессе доказательства оно не используется.)

Множеству $\{I, u\}$ принадлежат все элементы a идеала I и элемент u. Следовательно, оно содержит все объединения $a \cup u$. Кроме того, $\{I, u\}$ содержит все элементы x, для которых существует верхняя грань a из I, то есть элемент $a \in I$, удовлетворяющий «неравенству» $x \leqslant a$, так как идеал I вместе со всяким своим элементом содержит и все меньшие или равные элементы. Элементы x образуют идеал, поскольку, как нетрудно проверить, все условия, входящие в определение идеала, выполнены. Прежде всего в этот идеал входят все элементы идеала I, так как соотношение $a \leqslant a \cup u$ выполняется при любом $a \in I$. Кроме того, так как $u \leqslant a \cup u$, то идеалу, состоящему из элементов x, принадлежит и элемент u. Вместе с любым своим элементом x этот идеал содержит и все элементы, меньшие или равные x, поскольку, если $x \leqslant a \cup u$ и $y \leqslant x$, то в силу транзитивности отношения $y \leqslant a$. Наконец, если для элементов a и b идеала I выполняются соотношения $x \leqslant a \cup u$ и $y \leqslant b \cup u$, то, так как $x \cup y \leqslant (a \cup u) \cup (b \cup u) = (a \cup b) \cup (u \cup u) = (a \cup b) \cup u$, объединение $x \cup y$ также обладает требуемым свойством, поскольку элемент $a \cup b$ принадлежит идеалу I. Тем самым доказано, что элементы x, удовлетворяющие «неравенству» $x \leqslant a$, где $a \in I$, действительно образуют идеал.

Для идеалов типа $\{I, u\}$ в случае дистрибутивных структур выполняется следующее соотношение:

$$\{I, u \cap v\} = \{I, u\} \cap \{I, v\}.$$

Поскольку элемент $u \cap v$ принадлежит каждому из двух идеалов, стоящих в правой части равенства, то поэтому в любой структуре идеал $\{I, u \cap v\}$ содержится в идеале $\{I, u\} \cap \{I, v\}$ (в том, что в правой части равенства всегда стоит идеал, убедиться нетрудно, но мы не будем останавливаться на доказательстве этого утверждения, поскольку оно никак не используется в дальнейшем). Предположим, что структура дистрибутивна и x — элемент, принадлежащий $\{I, u\} \cap \{I, v\}$. Это означает, что идеал I содержит такие элементы a и b, для которых выполняется, во-первых, соотношение $x \leqslant a \cup u$

и, во-вторых, соотношение $x \leqslant b \cup u$. Так как элемент $c = a \cup b$ не меньше каждого из элементов a и b, то $x \leqslant c \cup u$ и $x \leqslant c \cup v$. Таким образом, элемент x является нижней гранью элементов $c \cup u$ и $c \cup v$, а следовательно, и их пересечения, то есть $x \leqslant (c \cup u) \cap (c \cup v)$. В силу дистрибутивности элемент, стоящий в правой части «неравенства», можно представить в виде $c \cup (u \cup v)$, а это означает, что элемент x принадлежит левой части доказываемого равенства, так как c — элемент идеала I.

ЗАДАЧИ

1. Доказать, что элементы структуры, которые не больше какого-нибудь элемента заданной выпуклой подструктуры, образуют идеал.

2. Доказать, что любую выпуклую подструктуру можно представить в виде пересечения идеала и двойственного идеала структуры.

3. Доказать, что идеал P структуры является примарным идеалом в том и только в том случае, если при $a \cap b \in P$ либо $a \in P$, либо $b \in P$.

4. Доказать, что, если для элемента структуры существует дополнение, то любой примарный идеал содержит либо элемент, либо его дополнение.

5. Доказать, что в структуре, заданной на упорядоченном множестве, всякий идеал примарный.

6. Существуют ли другие структуры, в которых всякий идеал примарный, кроме структуры из задачи 5?

7. Найти идеалы и примарные идеалы недистрибутивных структур из пяти элементов.

2.3. Представления структур

Самыми «конкретными» из всех рассмотренных нами структур были структуры, состоящие из подмножеств различных множеств, с операцией объединения, совпадавшей со взятием теоретико-множественного объединения, и операцией пересечения, совпадавшей со взятием теоретико-множественного пересечения. Казалось бы, было бы весьма полезно научиться строить представления произвольных структур при помощи структур подмножеств подобно тому, как при изучении представлений групп удобно рассматривать представления произвольных групп группами подстановок или матрицами. Для этого было бы необходимо научиться строить гомоморфизм, отображающий заданную структуру в структуру подмножеств некоторого множества так, что различные элементы исходной структуры переходят в различные подмножества (иначе говоря, подлежащий построению гомоморфизм является мономорфизмом).

Однако от подобных надежд, сколь бы привлекательными они ни казались, необходимо сразу же отказаться, поскольку структура подмножеств любого множества дистрибутивна и, следовательно, может служить представлением только дистрибутивной структуры, но зато для дистрибутивных структур задача построения представлений при помощи структуры подмножеств разрешима. Любую дистрибутивную структуру можно представить некоторой подструктурой подмножеств определенным образом выбранного множества. Точная формулировка этого утверждения известна под названием *теоремы Стоуна*.

Теорема Стоуна о представлении структур. Для любой дистрибутивной структуры существует мономорфизм, отображающий ее в структуру всех подмножеств некоторого множества, причем так, что дополнение переходит в дополнение.

Доказательство теоремы Стоуна не столь просто, как доказательство теоремы Кэли о представлении групп подстановками. Именно поэтому проследить от начала до конца весь ход рассуждений мы считаем весьма поучительным. Особенно длинен один из этапов доказательства. Чтобы не прерывать общего хода доказательства, мы рассмотрим его заранее, тем более что соответствующее утверждение, известное под названием теоремы о *сепарабельности* элементов дистрибутивной структуры, пред-

ставляет интерес и само по себе. Оно гласит:

для любых двух различных элементов дистрибутивной структуры всегда найдется гомоморфизм, при котором образы этих элементов различны.

При доказательстве сепарабельности элементов произвольной дистрибутивной структуры мы будем исходить из следующих соображений. Если I — идеал структуры, а D — двойственный идеал, не имеющий с I общих элементов, то в структуре существует такой содержащий I и не имеющий общих элементов с D идеал B, что любой идеал, бóльший B, уже имеет с D по крайней мере один общий элемент.

Для конечных структур это утверждение очевидно, поскольку идеал, содержащий I, можно выбрать столь большим, чтобы он еще не пересекался, но «был на грани пересечения» с двойственным идеалом D. Существование такого «максимального» идеала в случае бесконечной структуры заранее не очевидно, хотя можно доказать, что предположение о существовании максимального идеала не приводит к противоречию. (Допуская определенную «вольность речи», можно сказать, что идеал допускает «расширение» до тех пор, пока он не «соприкоснется» с двойственным идеалом).

Если структура дистрибутивна, то B — примарный идеал. Убедиться в этом мы сможем, доказав, что элементы структуры, не принадлежащие B, образуют двойственный примарный идеал. Непосредственно ясно, что, если какой-нибудь элемент a не принадлежит B, то и все элементы структуры, не меньшие (бóльшие или равные) a, не принадлежат B. Следовательно, необходимо лишь доказать, что, если каждый из двух элементов не принадлежит B, то их пересечение также не принадлежит B. Если элементы u и v не принадлежат B, то каждый из идеалов $\{B, u\}$ и $\{B, v\}$ больше B и поэтому имеют по крайней мере по одному общему элементу с D. Пусть x и y — общие элементы идеалов $\{B, u\}$ и $\{B, v\}$ и двойственного идеала D. Тогда $x \cap y$ также принадлежит каждому из идеалов $\{B, u\}$ и $\{B, v\}$, поскольку пересечение элементов x и y меньше любого из них. Кроме того, $x \cap y$ принадлежит D, так как D — двойственный идеал. Поскольку идеал B «еще» не имеет общих элементов с D, то идеал $\{B, u \cap v\}$ больше идеала B. Но это возможно лишь в том случае, если $u \cap v$ не принадлежит B, что и требовалось доказать.

Если теперь a и b — два различных элемента, дистрибутивной структуры, то можно рассуждать следующим образом. «Неравенства» $a \leqslant b$ и $b \leqslant a$ не могут выполняться одновременно. Предположим, что не выполняется, например, соотношение $b \leqslant a$. Это означает, что элемент b не принадлежит идеалу $(a)_i$ (состоящему из элементов x, которые удовлетворяют «неравенству» $x \leqslant a$) и что идеал $(a)_i$ не имеет общих элементов с двойственным идеалом $(b)_d$ (состоящим из элементов y, которые удовлетворяют «неравенству» $y \leqslant b$). Следовательно, по доказанному существует примарный идеал P, содержащий идеал $(a)_i$, но не имеющий общих элементов с двойственным идеалом $(b)_d$, в силу чего $a \in P$ и $b \notin P$. Таким образом, гомоморфизм, отображающий элементы примарного идеала P в нулевой элемент, а остальные элементы исходной структуры — в единичный элемент структуры из двух элементов, переводит элемент a в нулевой, а элемент b — в единичный элемент структуры из двух элементов, то есть образы элементов a и b при таком гомоморфизме различны. Итак, теорема о сепарабельности элементов дистрибутивной структуры доказана.

Построить представление, о котором говорится в теореме Стоуна, можно следующим образом. Пусть задана система подмножеств некоторого множества, выбранных так, что вместе с любыми двумя подмножествами она содержит их (теоретико-множественное) пересечение и объединение. Наша задача состоит в том, чтобы по заданным подмножествам определить «точки» всего множества. (Действительно, представление можно рассматривать как ситуацию, в которой «подмножества» уже заданы, а точки множества еще не известны»). Что можно утверждать о подмножествах, содержащих некоторую точку множества? Во-первых, теоретико-множественное пересечение двух таких подмножеств содержит выбранную точку. Кроме того, любое подмножество, которое больше подмножества, содержащего выбранную точку, обладает тем же свойством. Это означает, что подмножества, которым принадлежит выбранная точка, образуют двойственный идеал. Во-вторых, если два подмножества не содержат выбранную точку, то она не может принадлежать пересечению этих подмножеств. Кроме того, если выбранная точка не принадлежит какому-нибудь подмножеству, то

и все меньшие подмножества также не содержат ее. Это означает, что подмножества, не содержащие выбранную точку, образуют идеал. Поскольку любое подмножество либо содержит, либо не содержит выбранную точку (и точка не может одновременно принадлежать и не принадлежать одному и тому же подмножеству), то идеал и двойственный идеал нашей структуры подмножеств будут не чем иным, как нижним и верхним сегментами, порожденными сечением множества, то есть примарным идеалом и двойственным примарным идеалом. Если подмножествам, содержащим «приглянувшуюся» нам точку поставить в соответствие эту точку, а подмножествам, не содержащим ее, — пустое множество, то структура подмножеств окажется гомоморфно отображенной в структуру из двух элементов, нулевым элементом которой служит пустое множество, а единичным элементом — выбранная точка. Приведенные выше рассуждения относятся к каждой точке множества, поэтому гомоморфизмы описанного выше типа позволяют определить все точки множества. (Структура подмножеств иногда допускает несколько гомоморфизмов такого типа. «Обилие» гомоморфизмов не создает особых затруднений, поскольку определяемую подмножествами точку множества можно считать не простой, а «кратной».)

Обратим приведенные выше рассуждения. Пусть задана некоторая структура. Рассмотрим «все» гомоморфизмы, отображающие ее в «структуры из двух элементов». Это утверждение нуждается в уточнении, потому что, во-первых, если имеется один такой гомоморфизм, то задать любой другой гомоморфизм не представляет труда, так как все структуры из двух элементов изоморфны, во-вторых, не все из этих гомоморфизмов «существенно» различны, поскольку, если два гомоморфизма отображают в нулевой элемент одни и те же элементы исходной структуры, то различие в точках, служащих единичными элементами, «почти никак» не сказывается на гомоморфизмах. Учитывая это, мы будем строить для любого примарного идеала лишь один гомоморфизм, отображающий все его элементы в пустое множество, а остальные элементы исходной структуры — в «точку», то есть нулевым элементом структуры из двух элементов условимся раз и навсегда считать пустое множество, а единичный элемент называть точкой. Гомоморфизм рассматриваемого типа обозначим через φ, а единичный элемент структуры из двух элементов — через P_φ (таким образом, P_φ — точка, соответствующая гомоморфизму φ).

Итак, элементами рассматриваемого множества служат определенные выше точки, а элементам структуры соответствуют подмножества, состоящие из точек множества. Соответствие устанавливается следующим образом:

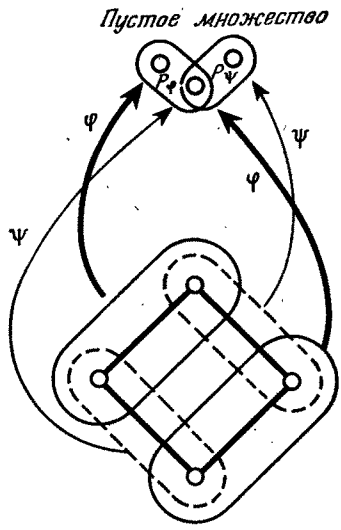


Рис. 101.

если a — произвольный элемент структуры, то ему соответствует подмножество $H(a)$, содержащее такие точки P_φ, для которых $\varphi(a) = P_\varphi$ (следовательно, если гомоморфизм ψ отображает элемент a в пустое множество, то P_ψ не принадлежит подмножеству $H(a)$ (рис. 101).

Остается лишь доказать, что мы действительно получили представление исходной структуры. Как показано выше, соответствие $a \to H(a)$ является отображением, поскольку элемент a позволяет однозначно определить точки подмножества $H(a)$.

Покажем, что при отображении $a \to H(a)$ образы различных элементов различны. Это утверждение следует из сепарабельности элементов исходной структуры (именно здесь используется дистрибутивность структуры). Действительно, если a и b — два элемента структуры, то сепарабельность означает, что существует гомоморфизм φ, отображающий, например, элемент a в нулевой элемент, а элемент b — в единичный элемент, то есть $\varphi(a) \neq P_\varphi$ и $\varphi(b) = P_\varphi$. Но тогда P_φ не принадлежит подмножеству $H(a)$, но является элементом подмножества $H(b)$. Следовательно, подмножества $H(a)$ и $H(b)$ различны.

Проверим, сохраняются ли операции.

1. Включение $P_\varphi \in H(a \cap b)$ означает, что $\varphi(a \cap b) = \varphi(a) \cap \varphi(b)$ совпадает с единичным элементом. Так может быть лишь в том случае, если каждый из эле-

ментов $\varphi(a)$ и $\varphi(b)$ совпадает с единичным элементом. Это означает, что P_φ — элемент каждого из подмножеств $H(a)$ и $H(b)$, то есть $H(a \cap b) = H(a) \cap H(b)$.

2. Включение $P_\varphi \in H(a \cup b)$ означает, что $\varphi(a \cup b) = \varphi(a) \cup \varphi(b)$ — единичный элемент. Так может быть в том и только в том случае, если по крайней мере один из элементов $\varphi(a)$ и $\varphi(b)$ совпадает с единичным элементом, то есть если P_φ — элемент по крайней мере одного из подмножеств $H(a)$ и $H(b)$.

Итак, теорема Стоуна о представлении двустрибутивных структур полностью доказана.

ЗАДАЧИ

1. Доказать, что в представлении структуры нулевому элементу (если таковой существует в исходной структуре) соответствует пустое множество.

2. Доказать, что в представлении структуры единичному элементу (если таковой существует в исходной структуре) соответствует множество, состоящее из всех точек (то есть все множество.)

3. Доказать, что, если один из двух элементов исходной структуры является дополнением другого, то и соответствующие им подмножества в представлении исходной структуры также являются дополнениями одного для другого.

Глава четвертая

Основные направления развития современной алгебры

1.

Общая алгебра, алгебраические структуры

От рассмотрения конкретно заданных групп мы перешли к изучению абстрактных групп, перестав считать различными изоморфные группы. Аналогичным образом от рассмотрения конкретных колец и структур было естественно перейти к построению общей теории колец и структур. То же самое относится и ко всем другим *алгебраическим структурам*.

Группы, кольца, тела — все это конкретные алгебраические структуры, или, точнее, типы алгебраических структур. В развитии алгебры углубленное изучение отдельных типов алгебраических структур происходило параллельно с выяснением их общих свойств. Рассмотренные нами алгебраические структуры позволяют сразу указать то общее, что их объединяет: все они представляют собой определенную «систему», состоящую из некоторого множества и заданных на нем операций.

Алгебраической структурой называется система

$$\mathfrak{A} = \langle A; f_1, f_2, \ldots, f_n, \ldots \rangle,$$

первый элемент которой представляет собой множество, а остальные элементы — заданные на этом множестве операции (то есть функции конечного числа переменных со значениями в том же множестве).

Раздел алгебры, занимающийся изучением общих свойств алгебраических структур, называется *общей алгеброй*. К «компетенции» общей алгебры относятся и обобщения понятий, уже известных на примере отдельных конкретных структур, и рассмотрение различных структур с «общих позиций». На многие вопросы, в том числе и на те, которые были затронуты выше, нам придется ограничиться лишь беглыми ответами.

В круг вопросов, относящихся к общей алгебре, входят, например, понятия *подструктуры*, *гомоморфизма* и *прямого произведения*. По существу их можно определить так же, как мы делали это до сих пор. Подструктурой называется часть структуры, замкнутая относительно заданных на ней операций, гомоморфизмом — однозначно определенное отображение, сохраняющее опера-

ции, а прямым произведением — такой «набор элементов», компонентами которого являются соответствующие алгебраические структуры, а операции выполняются покомпонентно. В этой связи возникает вопрос: можно ли операции, производимые в одной из структур, выполнять над элементами другой структуры? При ответе на этот вопрос можно исходить из того, что о гомоморфизме или прямом произведении имеет смысл говорить лишь в том случае, если алгебраические структуры принадлежат к одному и тому же типу. В свою очередь «однотипность» можно понимать как «выполнение одних и тех же операций над всеми переменными». Например, с этой точки зрения кольцо и структуру допустимо считать однотипными алгебраическими структурами, если в кольце рассматривать сложение и умножение, а в структуре—объединение и пересечение, поскольку и в том и в другом случае операции двухместны, или бинарны. (Разумеется, прямое произведение таких однотипных алгебраических структур — «новообразование» довольно причудливое и не является ни кольцом, ни структурой.) Но если в кольце относительно заданных в нем операций существуют нулевой и единичный элементы, а для каждого элемента — противоположный (обратный относительно операции сложения) ему элемент, то прямое произведение кольца и структуры оказывается таким же, как булева алгебра, так как представляет собой множество, на элементах которого заданы две нульместные, одна одноместная и две двухместные операции.

Если же мы все же захотим провести различие между прямыми однотипными алгебраическими структурами, то необходимы более тонкие соображения. Например, кольца отличаются от структур (или кольца с единицей — от булевых алгебр) тем, что заданные на них операции удовлетворяют различным условиям. В общем случае эти условия заданы в виде тождеств или равенств (выражающих коммутативность, ассоциативность или законы поглощения), но встречаются и такие условия, которые невозможно записать в виде равенств (например, в теории тел — существование обратного элемента для всех элементов, отличных от нуля; в теории структур — модулярность, задаваемая при помощи частичного упорядочения). Ясно, что возможность записать все условия в виде равенств мы оцениваем как благоприятную. В этих случаях говорят об *алгебраической структуре, заданной равенствами*. Можно доказать, что, если в некоторой структуре определенное равенство выполняется при любом выборе элементов (то есть тождественно), то оно выполняется и во всех подструктурах, гомоморфных образах структуры (множества образов всех элементов структуры при гомоморфизме) и прямых произведениях нескольких «экземпляров» структуры.

Отсюда следует, что *тела невозможно задать равенствами*, так как прямое произведение двух тел не является телом.

Более важная проблема состоит в выяснении того, когда тот или иной тип алгебраической структуры можно задать равенствами. В этом направлении получен весьма серьезный результат. Оказывается, сформулированное выше условие не только необходимо, но и достаточно для того, чтобы алгебраическую структуру можно было бы задать равенствами. Речь идет о следующем. Если структура A задана каким-то образом и доказано, что ее подструктуры, образ при гомоморфизме и прямое произведение $A \times A$ принадлежат к тому же типу, что и A, то существуют уравнения, определяющие алгебраическую структуру A.

От алгебраических структур, определяемых равенствами (и имеющих достаточно важное значение), перейдем к более широкому, но все еще четко ограниченному кругу других алгебраических структур. Прежде

всего нам бы хотелось упомянуть о структурах, в которых от операций требуется, чтобы они были не операциями, а лишь «частичными операциями», то есть были заданы не на всех элементах. В том, что такие «патологические» структуры необходимы, нас убеждает их распространенность. Действительно, с «частичной операцией» нам уже приходилось сталкиваться при рассмотрении тел, а именно с «операцией», порождающей обратные элементы, поскольку они существуют только для элементов, отличных от нуля. В подобных случаях принято говорить о *частичной алгебраической структуре*. Таким образом, тело остается алгебраической структурой, хотя ее и невозможно задать равенствами. По существу это означает, что алгебраические методы не позволяют отличить тела от «всех прочих» колец.

Перелистав книгу, нетрудно обнаружить и такие алгебраические структуры, на которых заданы «не операции» или по крайней мере «не только операции». Мы имеем в виду структуры, на которых наряду с операциями заданы отношения. Что же касается отношения, то они имеют мало общего с операциями. Рассмотрим, например, частичное упорядочение. Если множество частично упорядочено, то для любых двух элементов a и b «неравенство» $a \leqslant b$ либо выполняется, либо не выполняется, что позволяет определить отношение $\leqslant$ следующим образом.

Рассмотрим все возможные пары элементов. Для каждой пары элементов a и b выясним, удовлетворяют ли они «неравенству» или оно не выполняется. Если на этот вопрос всегда можно ответить, то тем самым «действие» отношения на элементах множества полностью описано. Следовательно, отношение можно рассматривать как некоторую функцию двух переменных, принимающую значения не из области определения, а из множества слов «истинно» и «ложно» («да» и «нет»). Такие функции называются логическими.

Если на алгебраических структурах помимо операций определены еще и алгебраические функции, то такие алгебраические структуры называются *алгебрами отношений*. Изучением алгебр отношений и других абстрактных алгебраических структур занимаются большие разделы современной алгебры. Многие из них граничат с *теорией множеств*, *теорией моделей* и *математической логикой*.

2.

Категории, гомологическая алгебра

Значительная часть современных работ по алгебре посвящена изучению «внутреннего устройства» алгебраических структур, но появились работы и другого направления, которое можно было бы охарактеризовать как «внешнее». Внимание их авторов сосредоточено в основном на таких взаимосвязях между отдельными типами алгебраических структур, которые можно установить, не определяя операции или элементы структур.

В качестве простейшего примера рассмотрим векторное пространство, например конечномерное векторное пространство над телом вещественных чисел. Если мы хотим рассмотреть сразу все возможные векторные пространства (во взаимосвязях, существующих между ними), то, очевидно, нецелесообразно рассматривать элементы каждого векторного пространства. Гораздо удобнее изучать интересующие нас векторные пространства как «единые и неделимые» *объекты*. Но для однородных линейных отображений векторные пространства не представляют единого целого, так как каждое векторное пространство (как объект) поразному связано с другими векторными пространствами. Именно поэтому при совместном рассмотрении объектов и отображений последним отводится особая роль.

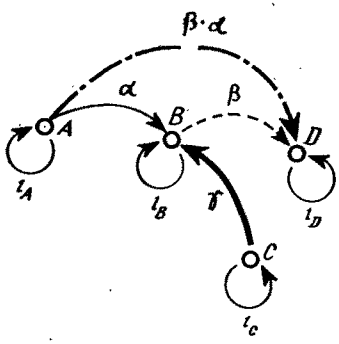
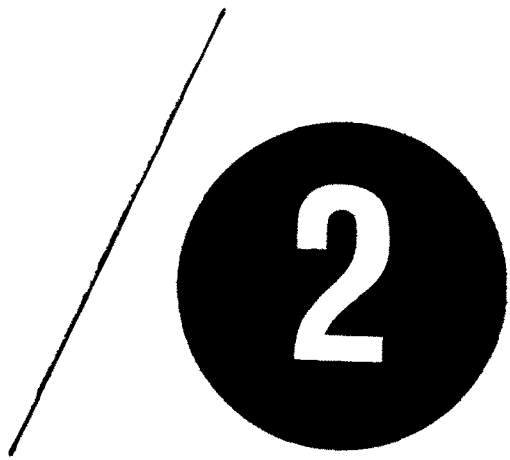


Рис. 102.

Обычно принято говорить о *совокупности объектов и отображений*. Объекты изображают в виде точек, а отображения — в виде стрелок, направленных от одной точки к другой. «Умножать» одно отображение на другое можно не всегда, а лишь в том случае, если первый сомножитель выходит из той точки, в которую входит второй сомножитель (рис. 102). Если существуют (в том или ином смысле) произведения трех сомножителей, то умножение отображений ассоциативно. Кроме того, предполагается, что для всякого объекта существует тождественное отображение, оставляющее его без изменений. Если все эти условия выполнены, то совокупность объектов и отображений называется *категорией*. Категории приобретают все более важное значение не только в алгебре, но и в других областях математики. Особенно тесно теория категорий связана с *топологией* — одним из разделов современной математики, истоки которого восходят к геометрии. В ней особо заметную роль играют категории, элементами которых являются модули над кольцами.

На стыке алгебры и топологии зародилась новая математическая дисциплина — *гомологическая алгебра*, уже снискавшая себе известность мощными методами и глубокими результатами. Она широко использует аппарат топологии и теории модулей. Бегло перечисленные нами разделы современной алгебры представляют собой «полигон», весьма пригодный для испытания и проверки результатов новых теорий.

РЕШЕНИЯ ЗАДАЧ



К главе первой

1.1

1. Если на месте каждого элемента конечного множества оказывается какой-то другой элемент того же множества, причем различные элементы переходят в различные, то и после выполнения подстановки мы будем располагать всеми элементами исходного множества. Действительно, число элементов, подвергшихся подстановке, совпадает с числом первоначально заданных элементов, поскольку ни один элемент не был замещен двумя другими элементами и, кроме того, каждый из замещающих элементов заимствован из исходного множества. Следовательно, и по завершении подстановки мы получим каждый из первоначально заданных элементов.

2. Чтобы доказать утверждение задачи, необходимо найти подстановку, перемещающую каждый из первоначально заданных элементов на какое-то место, но отводящую некоторым (в частности, одному) элементам несколько мест. (Иначе говоря, нижняя строка подстановки должна содержать все элементы верхней строки, но некоторые элементы должны встречаться несколько раз.) Этому требованию отвечает, например, подстановка $\binom{1\,2\,3\,4\,5\ldots}{1\,1\,2\,3\,4\ldots}$.

3. Если все элементы исходного множества «расписаны по местам», то ни один элемент не встречается дважды, поскольку мест имеется ровно столько, сколько элементов.

1.2

2. Если Q — подстановка, обратная тождественной подстановке I, то $QI = I$. Но так как $QI = I$, то подстановкой, обратной тождественной подстановке I, может быть только сама I. Обратная подстановка существует для любой подстановки, следовательно, она существует и для I и, как мы только что убедились, совпадает с самой тождественной подстановкой I.

3. Пусть $Q = P^{-1}$ — подстановка, обратная подстановке P, а Q^{-1} — подстановка, обратная подстановке Q. Так как $PQ = I$, а такому соотношению при заданной подстановке Q может удовлетворять только подстановка, обратная подстановке Q, то $Q^{-1} = P$. Следовательно, подстановка, обратная обратной подстановке, совпадает с исходной («прямой») подстановкой.

4. Рассмотрим произведение подстановок PQ. Известно, что подстановка, обратная подстановке PQ, существует. Достаточно найти подстановку R, удовлетворяющую соотношению $R(PQ) = I$: только она и может быть подстановкой, обратной подстановке PQ. Докажем, что $R = Q^{-1}P^{-1}$. Вычислим для этого произведение $R(PQ)$:

$$(Q^{-1}P^{-1})(PQ) = Q^{-1}(P^{-1}P)Q = Q^{-1}IQ = Q^{-1}(IQ) = Q^{-1}Q = I.$$

Итак, мы видим, что подстановка, обратная произведению подстановок, совпадает с произведением обратных подстановок. Особое внимание следует обратить на то, что порядок обратных сомножителей «обратен» порядку «прямых» сомножителей в исходном произведении подстановок и изменить его в общем случае невоз-

можно, поскольку умножение подстановок не коммутативно. Но умножение степеней P^n и P^k коммутативно, поэтому и сомножители в произведении подстановок, обратных степеням, можно переставлять, то есть $(P^nP^k)^{-1} = (P^n)^{-1}(P^k)^{-1}$. Используя это свойство степеней, можно показать, что $(P^k)^{-1} = (P^{-1})^n$.

1.3

1. Степени цикла $P = (012345)$ равны: $P^2 = (024)(135)$, $P^3 = (03)\times$ $\times(14)(25)$, $P^4 = (042)(153)$ и $P^5 =$ $= (054321)$. Из них лишь P^5 состоит из одного цикла.

2. На первом месте в циклической подстановке может стоять любой из элементов. Следовательно, если ее степень допускает разложение в произведение нескольких циклов, то эти циклы должны иметь одинаковую длину и быть независимыми. Как показывает предыдущая задача, так происходит лишь в том случае, если общий делитель показателя степени и длины исходного цикла отличны от единицы. Нетрудно понять, что все подстановки, допускающие разложение в произведение независимых циклов одинаковой длины, действительно являются степенями циклических подстановок. Одну из таких подстановок (поскольку их существует несколько) можно получить, расположив по порядку сначала первые элементы циклов, затем вторые элементы и т. д.

3. Чтобы найти произведение подстановок, проще всего разложить оба сомножителя в произведение транспозиций: $(01234) = (01)(02)(03)\times$ $\times(04)$, $(0567) = (05)(06)(07)$, откуда $(01234)(0567) = (01)(02)(03)(04)(05)\times$ $\times(06)(07) = (01234567)$.

В общем случае при умножении двух циклов, имеющих ровно один общий элемент, мы получим цикл, представимый в следующем виде: на первом месте стоит общий элемент, затем идут по порядку элементы первого сомножителя и в заключение — элементы второго сомножителя. Аналогичное утверждение справедливо и относительно произведения нескольких сомножителей.

4. Решение задачи целесообразно начать с подстановки P, не разложимой в произведение циклов. Пусть $P = \begin{pmatrix} 0\,1\,2\,3\,4\ldots \\ a\,b\,c\,d\,e\ldots \end{pmatrix}$, где a, b, c, d и e — различные элементы (ни один из которых не встречается в нижней строке вторично). Обратная подстановка имеет вид $P^{-1} = \begin{pmatrix} a\,b\,c\,d\,e\ldots \\ 0\,1\,2\,3\,4\ldots \end{pmatrix}$. Требуется найти подстановку $\begin{pmatrix} a\,b\,c\,d\,e\ldots \\ 0\,1\,2\,3\,4\ldots \end{pmatrix}(01234)\times$ $\times\begin{pmatrix} 0\,1\,2\,3\,4\ldots \\ a\,b\,c\,d\,e\ldots \end{pmatrix}$.

Подвергая исходные элементы a, b, c, d, e подстановкам

$$\begin{pmatrix} a\,b\,c\,d\,e\ldots \\ 0\,1\,2\,3\,4\ldots \end{pmatrix},$$

$$(0\,1\,2\,3\,4) \text{ и } \begin{pmatrix} 0\,1\,2\,3\,4\ldots \\ a\,b\,c\,d\,e\ldots \end{pmatrix},$$

получаем

a	0	1	b
b	1	2	c
c	2	3	d
d	3	4	e
e	4	0	a

Если взять исходный элемент u, отличный от элементов a, b, c, d, e, то под действием подстановки P^{-1} он перейдет в какой-то элемент v, отличный от 0, 1, 2, 3 и 4. Следовательно, подстановка P^{-1} переводит u в v, циклическая подстановка (01234) отображает v в v, а подстановка P «возвращает» v на исходное место, переводя его снова в u. Следовательно, произведение подстановок $\begin{pmatrix} a\,b\,c\,d\,e\ldots \\ 0\,1\,2\,3\,4\ldots \end{pmatrix}(01234)\begin{pmatrix} 0\,1\,2\,3\,4\ldots \\ a\,b\,c\,d\,e\ldots \end{pmatrix}$ оставляет все элементы, отличные от пяти перечисленных выше элементов, на месте, то есть совпадает с циклом $(abcde)$. В доказательстве нигде не была использована длина заданного цикла. Это позволяет утверждать, что, если C — цикл длины k, а P — произвольная подстановка, то $P^{-1}CP$ — цикл длины k.

Утверждение задачи допускает обобщение. Если подстановка Q разлагается в произведение независи-

мых циклов A, B и C, то можно показать, что $P^{-1}AP$, $P^{-1}BP$ и $P^{-1}CP$ — независимые циклы, произведение которых равно $P^{-1}QP$. Следовательно, подстановки Q и $P^{-1}QP$ всегда допускают однотипные разложения в произведения независимых циклов.

2.1

Задачи этого раздела просты, и решение их вряд ли вызовет какие-нибудь затруднения у читателей. Поэтому мы считаем возможным не приводить подробное решение для каждой задачи, а ограничиться лишь ответами, чтобы каждый мог проверить, не допустил ли он ошибку в своих рассуждениях. Поскольку множество элементов, над которыми производятся операции, по многим причинам может быть «не группой», мы укажем в каждом примере, обладает ли соответствующее множество чисел тем или иным групповым свойством или не обладает. Все ответы сведены в таблицу. Ассоциативность особо не отмечалась, поскольку во всех примерах заданные операции ассоциативны. Сокращенные обозначения, стоящие в первой строке, «расшифровываются» следующим образом: С — сложение (чисел), ЕС — существует единичный элемент относительно операции сложения, ОС — существует обратный элемент относительно операции сложения, У — умножение (чисел), ЕУ — существует единичный элемент относительно умножения, ОУ — существует обратный элемент относительно умножения. В каждой следующей строке приведен набор чисел (нулей и единиц), соответствующий примеру, номер которого указан слева. Единица означает утвердительный, а нуль — отрицательный ответ на вопрос о том, обладает ли то или иное множество чисел соответствующим свойством. Буквы С и У в конце каждой строки показывают, относительно какой операции — сложения или умножения — образуют группу числа, рассматриваемые в примере.

	С	ЕС	ОС	У	ЕУ	ОУ	
1	1	1	1	1	1	0	С
2	0	0	1	1	1	1	У
3	1	0	0	1	1	1	У
4	1	1	0	0	0	0	
5	1	1	1	1	1	0	С
6	0	0	1	1	1	1	У
7	0	0	1	1	1	1	У
8	0	0	1	1	0	0	
9	0	0	0	1	0	0	
10	0	0	0	1	1	1	У
11	0	0	1	1	1	1	У
12	1	1	1	1	1	0	С
13	1	1	1	1	1	0	С
14	0	0	1	1	1	1	У

2.2

1. Доказательство проводится так же, как и в случае векторов на плоскости, поскольку, если два вектора направлены в одну и ту же сторону, то и их сумма направлена в ту же сторону.

2. Доказательство утверждения задачи аналогично предыдущему.

3. Сдвиги на плоскости представляют собой движения, обладающие тем отличительным свойством, что они любой отрезок переводят в равный и параллельный отрезок. Поскольку (I) произведение двух движений, обладающих этим свойством, также наделено им, (II) движение, обратное сдвигу, также обладает отличительным свойством сдвигов, и тождественное преобразование принадлежит к числу движений, обладающих этим свойством, (III) произведение любых трех движений ассоциативно, то сдвиги на плоскости действительно образуют группу.

4. Доказать, что повороты на плоскости вокруг заданной точки образуют группу, можно так же, как было доказано утверждение предыдущей задачи. Действительно, воспользуемся тем, что повороты представляют собой движения на плоскости, обладающие тем отличительным свойст-

вом, что расстояние любой точки плоскости от центра (точки, вокруг которой производятся повороты) при повороте остается неизменным.

5. Доказать, что движения на плоскости, переводящие заданный равносторонний треугольник (квадрат) в себя, образуют группу, можно аналогично тому, как были доказаны утверждения предыдущих задач.

6. Доказать, что движения в пространстве образуют группу, можно аналогично тому, как было доказано групповое свойство движений на плоскости. Единственное отличие состоит в том, что на этот раз движения могут «выводить из плоскости».

7. Доказательство того, что преобразования подобия на плоскости образуют группу, проводится так же, как доказательство группового свойства сдвигов на плоскости. Трудность возникает лишь в связи с тем, каким образом можно дать более точную геометрическую «характеристику» преобразований подобия. Как показывают несложные геометрические соображения, преобразования подобия отличаются тем, что переводят любой треугольник в подобный треугольник.

8. Эта задача является частным случаем задачи 6, так же как задача 5— частным случаем примера 2. Поэтому доказать, что движения в пространстве, переводящие заданный тетраэдр в себя, образуют группу, можно аналогично тому, как были доказаны групповые свойства множеств в решениях предыдущих задач.

9. Пусть f — функция, удовлетворяющая условиям задачи (одной буквой мы будем обозначать функции в тех случаях, когда выписывание в явном виде аргумента излишне), а $f(\alpha)$ — значение, принимаемое функцией f в точке α (α — число, заключенное между 0 и 1). Функции, которые нас интересуют, обладают следующими свойствами:

1) $f(0) = 0$ и $f(1) = 1$;

2) если $0 \leqslant \alpha < \beta \leqslant 1$, то $0 \leqslant f(\alpha) < f(\beta) \leqslant 1$;

3) если $0 \leqslant \beta \leqslant 1$, то существует такое число α, что $0 \leqslant \alpha \leqslant 1$ и $\beta = f(\alpha)$.

Дав точное определение функций, удовлетворяющих условиям задачи, рассмотрим заданную на них операцию. Пусть f и g — функции, обладающие свойствами (1)—(3), а $f \circ g$ — их «произведение», то есть функция, которая получается при подстановке функции g в функцию f. Функцию $f \circ g$ можно определить следующим образом: в любой точке α «произведение» $f \circ g$ принимает значение $f \circ g(\alpha) = f(g(\alpha))$ (пока мы не задумываемся над тем, определено ли выражение, стоящее в правой части этого равенства).

Прежде всего покажем, что $f \circ g$ — функция допустимого типа. Так как при $0 \leqslant \alpha \leqslant 1$ значение $g(\alpha)$ удовлетворяет неравенствам $0 \leqslant g(\alpha) \leqslant 1$, то значение $f(g(\alpha))$ определено и также заключено между нулем и единицей. Следовательно, $f \circ g$ — функция, заданная на отрезке $0 \leqslant \alpha \leqslant 1$.

Проверим, обладает ли $f \circ g$ свойствами (1)—(3).

1. Пользуясь определением функции $f \circ g$, получаем: $f \circ g(0) = f(g(0)) = f(0) = 0$ и $f \circ g(1) = f(g(1)) = f(1) = 1$. Следовательно, $f \circ g$ обладает свойством (1).

2. Пусть $0 \leqslant \alpha < \beta \leqslant 1$. Так как функция g обладает свойством (2), то $0 \leqslant g(\alpha) < g(\beta) \leqslant 1$. Поскольку значения $g(\alpha)$ и $g(\beta)$ функции g удовлетворяют тем же неравенствам, что и числа α и β, а функция f обладает свойством (2), то $0 \leqslant f(g(\alpha)) < f(g(\beta)) \leqslant 1$. Следовательно, $f \circ g$ обладает свойством (2).

3. Предположим теперь, что $0 \leqslant \gamma \leqslant 1$. Так как функция f обладает свойством (3), то существует число β, удовлетворяющее неравенствам $0 \leqslant \beta \leqslant 1$ и такое, что $\gamma = f(\beta)$. Но функция g также обладает свойством (3), поэтому существует число α, удовлетворяющее неравенствам $0 \leqslant \alpha \leqslant 1$ и такое, что $\beta = g(\alpha)$. Таким образом, $\gamma = f(\beta) = f(g(\alpha))$. Следовательно, $f \circ g$ обладает свойством (3).

Итак, мы доказали, что операция подстановки не выводит из множества допустимых функций. Остается еще показать, что функции, обладающие свойствами (1)—(3), образуют группу относительно операции подстановки. Воспользуемся тем, что две функции называются равными, если они всюду принимают равные значения. (Особого внимания в определении равных функций заслуживает слово «всюду». В данном случае оно означает «на отрезке от нуля до единицы». Действительно, все остальные значения независимой переменной мы не принимаем во внимание, поскольку неизвестно, как ведут себя допустимые функции вне отрезка $[0, 1]$. Продолжив двумя различными способами одну и ту же допустимую функцию вне отрезка $[0, 1]$, мы получим две различные функции на всей числовой прямой. Тем не менее, с нашей точки зрения, эти функции различными не будут, так как во всех точках отрезка $[0, 1]$ они принимают равные значения. Поэтому приведенное выше определение равных функций необходимо понимать с оговоркой: «всюду», то есть при любых α из области определения. О значениях, принимаемых функциями вне области определения — интервала $[0, 1]$, нам ничего не известно, и мы о них говорить не будем.)

I. Для доказательства ассоциативности подстановки рассмотрим три функции: f, g и h. Если они обладают свойствами (1)—(3), то при любом α (разумеется, удовлетворяющем неравенствам $0 \leqslant \alpha \leqslant 1$) значение $\beta = h(\alpha)$ заключено между нулем и единицей, то есть $0 \leqslant \beta \leqslant 1$. То же самое можно сказать и о значении $\gamma = g(\beta)$, удовлетворяющем неравенствам $0 \leqslant \gamma \leqslant 1$, откуда в свою очередь следует, что $\delta = f(\gamma)$ удовлетворяет неравенствам $0 \leqslant \delta \leqslant 1$. Итак, с одной стороны, мы получаем цепочку равенств

$$(f \circ g)\, h(\alpha) = f \circ g(h(\alpha)) = f \circ g(\beta) = f(g(\beta)) = f(\gamma) = \delta,$$

а с другой стороны, — соотношения

$$f \circ (g \circ h)(\alpha) = f(g \circ h(\alpha)) = f(g(h(\alpha))) = f(g(\beta)) = f(\gamma) = \delta.$$

Тем самым ассоциативность подстановки доказана.

II. Нетрудно видеть, что единичным элементом служит функция, «тождественно равная независимой переменной x», то есть такая функция e, для которой при любом α выполняется соотношение $e(\alpha) = \alpha$. Разумеется, прежде всего необходимо доказать, что функция e обладает всеми свойствами единичного элемента группы. Но в этом можно убедиться прямой проверкой. Действительно, если $0 \leqslant \alpha \leqslant 1$ и $\beta = f(\alpha)$, то при $0 \leqslant \beta \leqslant 1$ получаем

$$e \circ f(\alpha) = e(f(\alpha)) = e(\beta) = \beta$$

и

$$f \circ e(\alpha) = f(e(\alpha)) = f(\alpha) = \beta.$$

Следовательно,

$$f = e \circ f = f \circ e.$$

III. Наконец, определим функцию, обратную заданной функции f. Для этого рассмотрим функцию g, которая определена следующим образом: если $\beta = f(\alpha)$, то $g(\beta) = \alpha$. Прежде всего необходимо убедиться в том, что g — действительно функция допустимого типа. Если функция f обладает свойством (3), то $g(\beta)$ существует при всех $0 \leqslant \beta \leqslant 1$. Необходимо еще проверить, что число $g(\beta)$ однозначно определено. Но если число γ отлично от α, то по свойству (2) значение $f(\gamma)$ отлично от $f(\alpha) = \beta$. Следовательно, функция f принимает значение β лишь в одной точке. Выясним теперь, обладает ли функция g всеми тремя свойствами допустимых функций.

1) Так как $f(0) = 0$ и $f(1) = 1$, то $g(0) = 0$ и $g(1) = 1$.

2) Пусть $0 \leqslant \alpha < \beta \leqslant 1$ и, кроме того, $\alpha = f(\gamma)$ и $\beta = f(\delta)$. (По свойству (3) такие γ и δ существуют и оба принадлежат отрезку $[0, 1]$.) Если $\gamma = \delta$, то $\alpha = f(\gamma) = f(\delta) = \beta$, а при $\delta < \gamma$ получаем из свойства (2) функ-

ции f, что $\beta = f(\delta) < f(\gamma) = \alpha$. И равенство $\alpha = \beta$, и неравенство $\beta < \alpha$ противоречат условию $\alpha < \beta$. Следовательно, возможен лишь случай, когда $\gamma < \delta$. Так как $\gamma = g(\alpha)$ и $\delta = g(\beta)$, то это означает, что $0 \leqslant g(\alpha) < g(\beta) \leqslant 1$.

3) Наконец, пусть $0 \leqslant \beta \leqslant 1$. Тогда для числа $\alpha = f(\beta)$, с одной стороны, выполняются неравенства $0 \leqslant \alpha \leqslant 1$, а с другой стороны, по определению функции g — соотношение $\beta = g(\alpha)$.

Осталось лишь доказать, что введенная нами функция g обратна функции f. Пусть $0 \leqslant \alpha \leqslant 1$. Тогда $g \circ f(\alpha) = g(f(\alpha)) = \alpha$, то есть $g \circ f = e$. С другой стороны, по свойству (3) допустимых функций существует такое β из отрезка $[0, 1]$, что $\alpha = f(\beta)$. Но тогда из определения функции g следует, что $\alpha = g(\beta)$, откуда $f \circ g(\alpha) = f(g(\alpha)) = f(\beta) = \alpha$, то есть $f \circ g = e$.

2.3

1. Нет, $\langle E; h\rangle$ не группа (поэтому сама форма записи $\langle E; h\rangle$ «не закона»), так как множество E не замкнуто относительно операции возведения в степень h. Действительно, возводя целое число в степень с целым показателем, мы не всегда получаем целое число (например, $2^{-1} = {}^1/_2$).

2. Нет, $\langle P; h\rangle$ не группа. Хотя множество P и замкнуто относительно операции возведения в степень h, поскольку положительное число, возведенное в степень с положительным (как, впрочем, и любым) показателем, положительно, но операция h не ассоциативна. Чтобы убедиться в этом, достаточно привести хотя бы один пример, когда ассоциативность нарушается. Так, $h(h(2,2),3) = h(2^2,3) = h(4,3) = 4^3 = 64$, а $h(2,h(2,3)) = h(2,2^3) = h(2,8) = 2^8 = 256$.

3.1

1. Приводимое ниже доказательство целиком переносится на тот случай, когда в полугруппе имеется левый единичный элемент, а для каждого элемента существует левый обратный (достаточно сослаться на «симметрию правого и левого»).

Если e — правый единичный элемент и элемент b — правый обратный для элемента a, а элемент c — правый обратный для элемента b, то

$$ba = (ba)\,e = (ba)\,(bc) = b\,(ab)\,c = (be)\,c = bc = e.$$

Следовательно, элемент b — левый обратный для элемента a. Кроме того,

$$ea = (ab)\,a = a\,(ba) = ae = a,$$

то есть e — левый единичный элемент.

2. а) Ясно, что относительно операции умножения, заданной так, что произведение всегда совпадает со вторым сомножителем, любое множество замкнуто. Следовательно, необходимо проверить лишь, ассоциативно ли такое необычное умножение. Нетрудно видеть, что оно действительно ассоциативно:

$$(ab)\,c = bc = c \quad \text{и} \quad a\,(bc) = ac = c.$$

б) В этой полугруппе левый единичный элемент не только существует, но и более того любой элемент является левым единичным элементом. Действительно, поскольку умножение определено так, что $ab = b$ для любого элемента b, то a — левый единичный элемент. А так как соотношение $ab = b$ выполняется при любом a, то каждый элемент полугруппы является левым единичным элементом.

в) Рассмотрим элемент e полугруппы, который по доказанному является левым единичным элементом. Соотношение $ae = e$ выполняется для произвольного элемента a полугруппы, а это означает, что элемент e — правый обратный для элемента a. (Небезынтересно отметить, что все элементы полугруппы обладают одним и тем же правым обратным элементом.)

3. Как показывает предыдущая задача, полугруппа в общем случае

не является группой, если в ней имеется единичный элемент «с одной стороны», а обратные элементы существуют «с другой стороны». Действительно, в полугруппе, рассмотренной в задаче 2, каждый элемент служит левым единичным элементом, в силу чего эта полугруппа (если она содержит по крайней мере два элемента) не может быть группой. Но, как показывает задача 1, если потребовать, чтобы в полугруппе единичный элемент и обратные элементы существовали «с одной и той же стороны», то полугруппа становится группой. Таковы ответы на вопросы задачи 3.

4. Если $ea = a$, то для любого элемента b группы выполняется соотношение $bea = ba$, откуда (используя закон сокращения справа) получаем: $be = b$. Это означает, что e—правый единичный элемент группы. Аналогичным образом, используя закон сокращения слева, можно убедиться в том, что e — левый единичный элемент группы. (Таким образом, утверждение задачи справедливо для полугрупп, в которых выполняются законы сокращения.)

5. Построить полугруппу, удовлетворяющую условиям задачи, можно следующим образом. Если на произвольном конечном множестве (например, на конечном множестве чисел) задать операцию $ab = b$, то будет выполняться левый закон сокращения. Действительно, если $ax = ay$, то $x = ax = ay = y$. Такая полугруппа, как показано в задаче 2, не является группой, если содержит по крайней мере два элемента.

6. Пара $\langle P; h\rangle$ полугруппой не является: в решении задачи 2 из раздела 2.3 доказано, что операция h не ассоциативна.

3.2

1. Чтобы определить порядок подстановок, возведем их в целые положительные степени: $(12)^1 = (12)$, $(12)^2$ = тождественная подстановка; $(123)^1 = (123)$, $(123)^2 = (132)$, $(123)^3$ = тождественная подстановка; $(1234)^1 = (1234)$, $(1234)^2 = (13)(24)$, $(1234)^3 = (1432)$, $(1234)^4$ = тождественная подстановка. Следовательно, порядок цикла совпадает с его длиной. Можно показать, что это утверждение справедливо и в общем случае.

2. Порядки подстановок равны 2, 3, 6 и 4. Можно доказать, что порядок подстановки равен наименьшему общему кратному длин циклов, в произведение которых разложена подстановка. (Мы не приводим подробного доказательства этого утверждения, поскольку оно весьма громоздко.)

3. Если вещественное число a имеет конечный порядок, то некоторая степень его (речь идет о «настоящей» степени, так как групповой операцией в мультипликативной группе вещественных чисел служит обычное умножение чисел) совпадает с единичным элементом группы, то есть равна 1. Но условию $a^n = 1$ из всех положительных чисел удовлетворяет только число 1, порядок которого равен 1, а из всех отрицательных чисел только число —1, порядок которого равен 2. (В общем случае только порядок единичного элемента группы равен 1.)

4. Требуется найти комплексные числа, для которых при некотором n выполняется соотношение $a^n = 1$. Этому условию удовлетворяют только так называемые комплексные корни n-й степени из единицы. Например, при $n = 4$ существуют четыре таких корня: 1, —1, i и $-i$. Порядок двух первых корней найден в предыдущей задаче, порядок двух последних корней равен 4. (Комплексные корни n-й степени из единицы располагаются на единичной окружности, описанной на комплексной плоскости вокруг точки 0, и совпадают с вершинами правильного n-угольника, вписанного в эту окружность. Иначе говоря, корни n-й степени из единицы не заполняют целиком всю единичную окружность, а лежат в точках пересечения ее с прямыми,

образующими с вещественной осью углы, кратные $2\pi/n$.)

5. Единичным элементом в группе монотонно возрастающих функций, заданных на отрезке $[0, 1]$, обращающихся при $x = 0$ в нуль, а при $x = 1$ в единицу, служит функция e, удовлетворяющая при любом $0 \leqslant \alpha \leqslant 1$ соотношению $e(\alpha) = \alpha$. Но если f — элемент группы, отличный от e, то между 0 и 1 заведомо найдется такое α, при котором $f(\alpha) \neq \alpha$. Пусть, например, $f(\alpha) > \alpha$. Тогда (так как f — монотонная функция) $f(f(\alpha)) > f(\alpha)$ и, следовательно, $\alpha < f(\alpha) < f^2(\alpha)$ (здесь $f^2(\alpha)$ означает $f(f(\alpha))$). Продолжая подставлять в f значения $f^2(\alpha)$, $f^3(\alpha)$ и т. д., получаем возрастающую числовую последовательность $\alpha, f(\alpha), f^2(\alpha), \ldots, f^n(\alpha), \ldots$. Следовательно, $f^n(\alpha)$ ни при каком n не совпадает с α, то есть равенство $f^n(\alpha) = \alpha$ исключается. Как показывают аналогичные рассуждения, функция f не может быть элементом конечного порядка и в том случае, если $f(\alpha) < \alpha$. Следовательно, в рассматриваемой группе имеется лишь один элемент конечного порядка — единичный элемент.

3.3

1. Утверждение задачи следует из того, что как сложение, так и умножение чисел коммутативно.

2. В некоммутативности группы движений на плоскости (то есть в том, что не всякие два элемента группы можно переставить, не изменив их произведения) можно убедиться, если нам удастся найти хотя бы одну пару элементов группы, произведение которых зависит от порядка сомножителей. Поскольку таких пар существует много, то перечислить все пары не представляется возможным. Мы приведем лишь простейший пример некоммутирующих движений на плоскости (вполне достаточный для доказательства некоммутативности движений на плоскости), но читатель, несомненно, сможет построить и другие примеры. Пусть A и B — две (различные) точки плоскости. Докажем, что отражения относительно точек A и B (принадлежащие к числу движений на плоскости) не коммутируют. Для этого достаточно указать хотя бы одну точку P, которая под действием произведений двух отражений (отличающихся порядком сомножителей) переходит в различные точки плоскости. Выберем точку P так, чтобы точки A, B и P (именно в этом порядке!) расположились в вершинах квадрата (рис. 103).

Отразив точку P относительно точки A, а полученную точку P_1 относительно точки B, мы получим точку P_2, изображенную на рис. 103 вверху. Отразив точку P относительно точки B, а полученную точку P_1 — относительно точки A, мы получим точку P_2, показанную на рис. 103 внизу. Нетрудно видеть, что результаты получились различными.

3. а) Пусть t — любое (может быть, наименьшее) общее кратное чисел n и k. Тогда, как известно, a^t и b^t совпадают с единичным элементом группы. Из тождества для степеней, справедливого для любой коммутативной группы, следует, что $(at)^t = a^t b^t = ee = e$. Сравнивая соотношение $(ab)^t = e$ с определением порядка элемента ab, заключаем, что $o(ab)$ делит t.

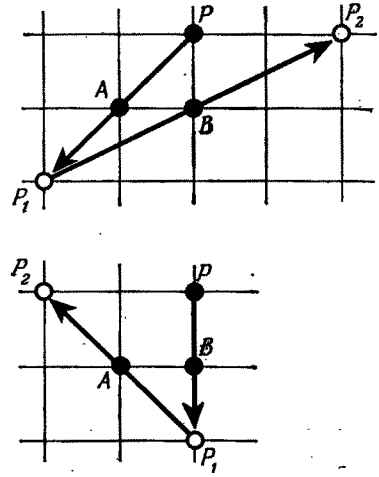


Рис. 103.

б) В рассматриваемом случае, как и всегда, порядок произведения ab делит произведение nk.

Наоборот, если $(ab)^t = e$, то $a^t b^t = e$. Возводя произведение $a^t b^t$ в n-ю и в k-ю степень, получаем

$$a^{nt}b^{nt} = e \quad \text{и} \quad a^{kt}b^{kt} = e.$$

По определению порядка элемента группы $a^n = b^k = e$, поэтому

$$b^{nt} = e \quad \text{и} \quad a^{kt} = e.$$

Так как порядок элемента b равен k, а порядок элемента a равен n, то соотношения $b^{nt} = e$ и $a^{kt} = e$ могут выполняться лишь в том случае, если k делит nt, а n делит kt. В теории чисел доказывается, что, если целое число делит произведение двух целых чисел и взаимно просто с одним из сомножителей, то оно делит другой сомножитель. Применяя эту теорему, получаем, что k делит t и n делит t. Так как k и n — взаимно простые числа, то их произведение является делителем числа t. При $t = o(ab)$ отсюда следует, что произведение nk делит ab.

Но два положительных целых числа делят друг друга лишь в том случае, если они совпадают. Следовательно, $o(ab) = nk$, что и требовалось доказать.

в) Достаточно привести пример. Из тождеств для степеней следует, что $o(a^{-1}) = o(a)$ независимо от порядка элемента a. Но порядок элемента aa^{-1} равен 1, а единица делит порядок любого элемента a.

4. Пусть a — элемент n-го порядка, а b — элемент бесконечного порядка. Тогда порядок элемента $c = ab$ не может быть конечным. Действительно, если бы порядок элемента c был равен k, то (поскольку $o(a^{-1}) = n$) из предыдущей задачи следовало бы, что порядок элемента $b = a^{-1}c$ делит наименьшее общее кратное чисел n и k, то есть вопреки исходному предположению конечен. Так как c — элемент бесконечного порядка и порядок элемента, обратного элементу b бесконечного порядка, бесконечен, то b^{-1} и c — два элемента бесконечного порядка, произведение которых a имеет конечный порядок. С другой стороны, «квадрат» (произведение на себя) элемента бесконечного порядка имеет бесконечный порядок.

(Если группа некоммутативна, то произведение двух элементов конечного порядка может иметь бесконечный порядок. Например, отражения относительно точек (см. задачу 2) являются элементами порядка 2 группы движений на плоскости, а произведение их порождает сдвиг, то есть элемент бесконечного порядка той же группы.)

4.1

1. Элементы подгруппы $\{n\}$ аддитивной группы целых чисел — это «степени» одного элемента, то есть — целые кратные числа n. Элементы подгруппы $\{-n\}$ — это целые кратные числа $-n$. Поскольку они совпадают с целыми кратными числа n (в силу равенства $(-n)k = n(-k)$), то обе циклические подгруппы $\{n\}$ и $\{-n\}$ также совпадают.

Элементами подгруппы $\{n, k\}$ аддитивной группы целых чисел служат «произведения степеней» образующих элементов, то есть числа вида $nx + ky$, где x и y — произвольные целые числа. Пусть d — наименьшее из положительных целых чисел, принадлежащих подгруппе $\{n, k\}$. Мы утверждаем, что подгруппа $\{n, k\}$ состоит из целых кратных числа d. Выберем в подгруппе $\{n, k\}$ произвольное число a. Разделив a на d, мы получим какое-то частное q и какой-то остаток r, который меньше d и положителен или равен нулю, то есть a можно представить в виде $a = qd + r$. Поскольку вместе с числами a и d подгруппе $\{n, k\}$ принадлежат и целые кратные этих чисел и суммы кратных, то подгруппа $\{n, k\}$ содержит и число $r = a + (-q)d$. Число d выбрано так, что оно является наименьшим положительным

числом в подгруппе $\{n, k\}$. Так как остаток r принадлежит подгруппе $\{n, k\}$ и меньше d, то r не может быть положительным числом. По определению остаток r либо равен нулю, либо положителен. Следовательно, остается единственная возможность: $r = 0$, а это означает, что $a = dq$. Итак, любое число, принадлежащее подгруппе $\{n, k\}$, кратно d.

Из доказанного уже следует, что подгруппа $\{n, k\}$ циклическая. Но если приведенное выше доказательство проанализировать более подробно, то нетрудно убедиться, что сама подгруппа $\{n, k\}$ в нем нигде не используется. Следовательно, *любая подгруппа аддитивной группы целых чисел циклическая.*

Выясним теперь зависимость числа d от заданных чисел n и k. Поскольку числа n и k принадлежат подгруппе $\{n, k\}$, то, как и любой другой элемент подгруппы, они делятся на d. Это означает, что d — общий делитель чисел n и k. С другой стороны, число d как элемент подгруппы $\{n, k\}$ можно записать в виде $d = nu + kv$ (где u и v — целые числа). Из этого представления числа d видно, что любое число, делящее n и k, является делителем d, то есть число d кратно любому общему делителю чисел n и k. Иначе говоря, d обладает отличительным свойством наибольшего общего делителя чисел n и k. Итак, окончательный результат наших рассуждений сводится к следующему: всякая подгруппа аддитивной группы целых чисел, порожденная любыми двумя числами, совпадает с циклической подгруппой, порожденной наибольшим общим делителем этих двух чисел.

2. Поскольку рассматривается мультипликативная группа вещественных чисел, отличных от нуля, то групповой операцией является умножение чисел, и поэтому произведение степеней элементов группы совпадает с произведением чисел. Подгруппа $\{-1\}$ состоит из степеней числа -1. Существуют всего две различные степени этого числа: 1 и -1. Следовательно, подгруппа $\{-1\}$ состоит из двух чисел: 1 и -1.

Подгруппа $\{-1, 2\}$ состоит из чисел вида $(-1)^k 2^n$, где k и n — целые числа. Поскольку среди степеней числа -1 существуют лишь два различных числа, то элементы подгруппы $\{-1, 2\}$ имеют вид 2^n, и -2^n, где n — произвольное целое число (в частности, n может быть равным нулю или отрицательным).

Подгруппа $\{1, 2, 3, 4, \ldots\}$ состоит из произведений степеней чисел 1, 2, 3, 4, ... Все эти числа положительны, поэтому подгруппа $\{1, 2, 3, 4, \ldots\}$ может содержать только положительные рациональные числа. С другой стороны, нетрудно видеть, что любое положительное рациональное число принадлежит подгруппе $\{1, 2, 3, 4, \ldots\}$, поскольку дробь k/n можно записать в виде произведения первой степени числа k и минус первой степени числа n, то есть kn^{-1}.

Подгруппа $\{1/2, 1/3, \ldots\}$ содержится в подгруппе $\{1, 2, 3, 4, \ldots\}$. Но образующие подгруппы $\{1/2, 1/3, \ldots\}$ обратны отличным от 1 образующим подгруппы $\{1, 2, 3, 4, \ldots\}$. Следовательно, образующие 2, 3, 4, ... предыдущей подгруппы принадлежат подгруппе $\{1/2, 1/3, \ldots\}$, а поскольку единичный элемент принадлежит всем подгруппам, то подгруппа $\{1/2, 1/3, \ldots\}$ содержит подгруппу $\{1, 2, 3, 4, \ldots\}$. Итак, подгруппа $\{1/2, 1/3, \ldots\}$ состоит из положительных рациональных чисел.

Все элементы подгруппы $\{-1, 2, 3, \ldots\}$ — рациональные числа. Так как эта подгруппа содержит подгруппу $\{2, 3, \ldots\}$, то ей принадлежат все положительные рациональные числа. Кроме того, она содержит число -1, а значит и все числа, получающиеся из положительных рациональных чисел, если их взять со знаком минус. Итак, подгруппа $\{-1, 2, 3, \ldots\}$ содержит все рациональные числа (и только рациональные числа).

Подгруппе, порожденной положительными числами, которые меньше единицы, могут принадлежать только положительные числа, поскольку

целые положительные числа при возведении в степень с целым показателем остаются положительными. Если a — положительное число и больше единицы, то $1/a$ — положительное число и меньше единицы. Поскольку $a = (1/a)^{-1}$, то рассматриваемая нами подгруппа содержит все отличные от единицы положительные числа. Это означает, что она содержит все положительные числа (и только их), так как единичный элемент (число 1) принадлежит всем подгруппам.

3. Покажем, что элементы (01) и (0123456) порождают всю группу подстановок элементов 0, 1, 2, 3, 4, 5 и 6. Подгруппа {(01), (0123456)} вместе с циклом (0123456) содержит и обратный цикл (6543210). Это означает, что вместе с транспозицией (01) рассматриваемая подгруппа содержит следующие транспозиции:

$$(6543210)(01)(0123456) = (12),$$
$$(6543210)(12)(0123456) = (23),$$
$$(6543210)(23)(0123456) = (34),$$
$$(6543210)(34)(0123456) = (45),$$
$$(6543210)(45)(0123456) = (56),$$
$$(6543210)(56)(0123456) = (60).$$

Комбинируя их, находим подстановки, также принадлежащие подгруппе {(01), (0123456)}:

$$(01)(12)(01) = (02),$$
$$(02)(23)(02) = (03),$$
$$(03)(34)(03) = (04),$$
$$(04)(45)(04) = (05),$$
$$(05)(56)(05) = (06).$$

Итак, мы доказали, что рассматриваемая подгруппа содержит транспозиции (01), (02), (03), (04), (05) и (06), порождающие, как известно, всю группу подстановок чисел 0, 1, 2, 3, 4, 5 и 6.

Анализируя ход рассуждений, нетрудно заметить, что по существу не используется число элементов, на которых действуют подстановки. Следовательно, наши рассуждения позволяют доказать и более общее утверждение: группу всех подстановок любого числа элементов порождают

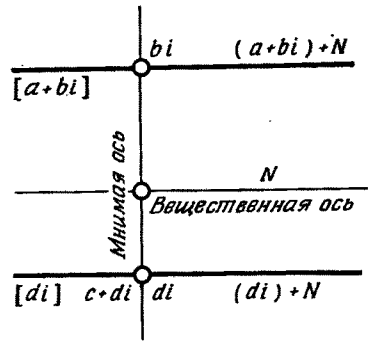


Рис. 104.

два элемента: транспозиция — например, транспозиция (01) — и цикл, в которой входят все перемещаемые при подстановках элементы, но так, что элементы, затрагиваемые транспозицией, идут подряд [в рассматриваемом примере это означает, что цикл может начинаться с цифр 0 и 1, то есть иметь вид (01...)].

4.2

1. а) В аддитивной группе G комплексных чисел смежный класс вместе с любым комплексным числом содержит и все комплексные числа, получающиеся из данного при сложении с любым числом из подгруппы N (то есть с любым вещественным числом). Это означает, что вместе с комплексным числом $a + bi$ смежный класс содержит и все комплексные числа, мнимая часть которых равна b, то есть комплексные числа вида $x + bi$, где x — произвольное вещественное число. На комплексной плоскости смежным классам соответствуют «горизонтальные» прямые, а подгруппе N — вещественная ось (рис. 104).

Чтобы задать смежный класс, необходимо указать мнимую часть (общую для всех) входящих в него комплексных чисел. Пусть $[a + bi]$ — смежный класс, которому принадлежит комплексное число $a + bi$. Вместо $a + bi$ можно взять комплексное число bi, так как

$[a + bi] = [bi]$, поскольку оба числа $a + bi$ и bi принадлежат одному смежному классу. Сложение смежных классов производится следующим образом: $[bi] + [ci] = [bi + ci] = [(b + c)i]$. [То, что при факторизации G по N получается группа (фактор-группа G/N), заранее известно, так как вещественные числа образуют подгруппу аддитивной группы комплексных чисел, которая в силу коммутативности является нормальным делителем.] Итак, сложение смежных классов происходит «так же», как сложение вещественных чисел.

На комплексной плоскости сложение «горизонтальных прямых» можно производить, сопоставляя каждой прямой вещественное число, соответствующее точке пересечения этой прямой с мнимой осью, и производя сложение полученных вещественных чисел (рис. 105).

б) Фактор-группа G/N существует, так как N — подгруппа и, разумеется, нормальный делитель. Два отличных от нуля комплексных числа принадлежат одному смежному классу, если одно из них отличается от другого вещественным множителем, так как подгруппа N состоит из положительных вещественных чисел. Если комплексные числа записаны в тригонометрической форме, то справедливо следующее утверждение: комплексные числа $r(\cos\varphi + i\sin\varphi)$

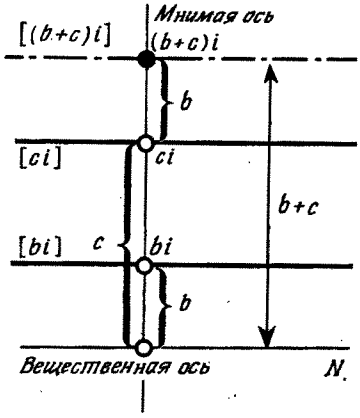


Рис. 105.

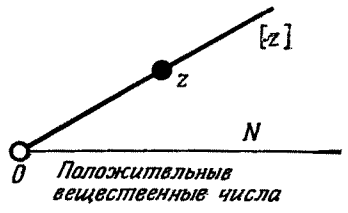


Рис. 106.

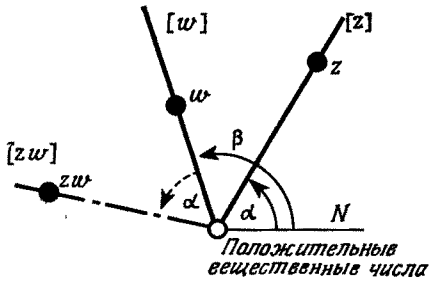


Рис. 107.

и $s(\cos\psi + i\sin\psi)$ принадлежат одному смежному классу в том и только в том случае, если их аргументы равны, то есть если $\varphi = \psi$. Пусть $[z]$ — смежный класс, которому принадлежит комплексное число z. На комплексной плоскости элементами смежного класса являются точки с одинаковым аргументом. Они заполняют луч, выходящий из начала координат (рис. 106).

Выясним теперь, что происходит при умножении двух смежных классов. Если смежный класс $[z]$ умножить на смежный класс $[w]$, то получится смежный класс $[zw]$. Как мы уже знаем, смежный класс определен в том и только в том случае, если задан общий аргумент составляющих его комплексных чисел. По теореме Муавра аргумент произведения zw равен сумме аргументов сомножителей z и w, поэтому на комплексной плоскости «умножение» лучей, исходящих из начала координат, сводится к сложению аргументов. Разумеется, важно все время следить за тем, чтобы среди комплексных чисел не было нуля, то есть производить все построения на комплексной плоскости, из

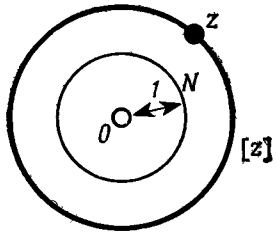


Рис. 108.

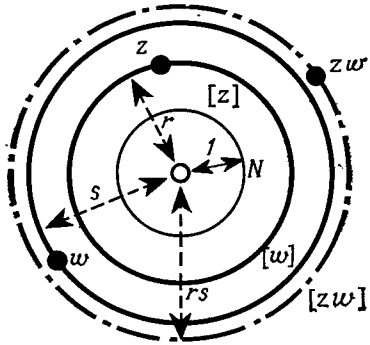


Рис. 109.

которой «выколота» точка 0 (рис. 107).

в) Фактор-группа существует и в этом случае. Для построения ее комплексные числа удобно представить в тригонометрической форме. Комплексные числа принадлежат одному смежному классу мультипликативной группы G комплексных чисел, отличных от нуля по подгруппе N комплексных чисел с модулем, равным единице, если их модули совпадают. Чтобы задать смежный класс, необходимо и достаточно задать общее значение модуля входящих в него комплексных чисел.

На комплексной плоскости числа, имеющие одинаковый модуль, заполняют окружность с центром в начале координат и радиусом, равным модулю. Следовательно, каждый смежный класс изображается в виде такой окружности, а все смежные классы — в виде концентрических окружностей (рис. 108). (Напомним, что [z] означает смежный класс, содержащий комплексное число z.)

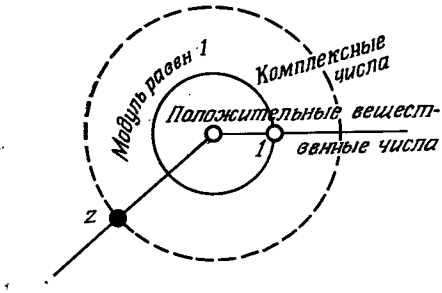


Рис. 110.

При умножении смежных классов необходимо вычислить произведение вещественных чисел, соответствующих смежным классам — сомножителям (модули комплексных чисел, принадлежащих смежным классам). Умножение смежных классов можно наглядно изобразить на комплексной плоскости. «Произведением» двух окружностей будет окружность, радиус которой равен произведению радиусов окружностей — сомножителей (рис. 109). (Все окружности описать вокруг начала координат.)

Небезынтересно отметить связь, существующую между двумя последними задачами. Нетрудно убедиться в том, что фигурирующие в них нормальные делители имеют лишь один общий элемент: число 1. Всякое комплексное число (если оно отлично от нуля) принадлежит одному из смежных классов группы G по подгруппе положительных вещественных чисел и одному из смежных классов по подгруппе комплексных чисел с модулем, равным единице, причем смежные классы по каждому из нормальных делителей группы G не имеют общих элементов. Действительно, любое отличное от нуля комплексное число однозначно определено, если заданы его модуль и аргумент (рис. 110).

Окружности и лучи задают на комплексной плоскости «сетку», используемую в так называемых полярных координатах.

г) Фактор-группа G/N существует, так как любой элемент группы порождает некоторую подгруппу, а

всякая подгруппа коммутативной группы является ее нормальным делителем. В один смежный класс с вещественным числом x попадают все вещественные числа, отличающиеся от него на целое кратное число 2π (поскольку в аддитивной группе G вещественных чисел групповой операцией является сложение). Эти числа представимы в виде $x + 2k\pi$, где k — произвольное натуральное число. (Таким образом, все решения некоторых тригонометрических уравнений принадлежат одному смежному классу группы G по $N = \{2\pi\}$.) Разумеется, в качестве нормального делителя можно было выбрать не только подгруппу $\{2\pi\}$, но и любую другую циклическую подгруппу.

д) Как было показано выше, движения образуют нормальный делитель группы преобразований подобия. Поэтому в рассматриваемом случае фактор-группа G/N существует. Выясним, как «устроены» смежные классы, из которых состоит фактор-группа. Если **T** — преобразование подобия, то смежный класс [**T**], которому оно принадлежит, состоит из преобразований **TS**, где **S** — любое движение. Ясно, что, если преобразование **T** изменяет расстояния между точками в λ раз (λ — положительное число), то и любой другой элемент из смежного класса [**T**] обладает тем же свойством.

Действительно, движение **S**, выполняемое первым, не изменяет расстояний между точками, а производимое вслед за **S** преобразование подобия **T** изменяет расстояние между любой парой точек в λ раз. Следовательно, каждый элемент из смежного класса [**T**] изменяет расстояния в том же отношении.

Верно и обратное утверждение: если два преобразования изменяют расстояния между точками в одном и том же отношении, то они принадлежат одному смежному классу.

Пусть **R** — преобразование подобия с коэффициентом подобия λ. Рассмотрим преобразование $\mathbf{S} = \mathbf{T}^{-1}\mathbf{R}$. Ясно, что **S** — преобразование подобия. Так как **T** изменяет все расстояния в λ раз, то $\mathbf{T}^{-1}$ приводит к увеличению (или уменьшению) расстояний в λ^{-1} раз. При умножении преобразований коэффициенты подобия также умножаются. Следовательно, преобразованию подобия **S** соответствует коэффициент подобия $\lambda^{-1}\lambda = 1$. Но это и означает, что **S** — движение. Таким образом, преобразование подобия **R** можно представить в виде $\mathbf{R} = \mathbf{TS}^{-1}\mathbf{R} = \mathbf{TR}$, то есть **R** принадлежит смежному классу [**T**].

Итак, мы установили, что одному смежному классу принадлежат преобразования подобия, изменяющие (увеличивающие или уменьшающие) расстояние между точками в одно и то же число раз. Произведение двух смежных классов состоит из преобразований с коэффициентом подобия, равным произведению коэффициентов подобия, соответствующих смежным классам-сомножителям. Следовательно, умножение смежных классов подчиняется тем же «правилам», что и умножение положительных вещественных чисел.

е) В этой задаче необходимо доказать, что N — нормальный делитель группы G. Какие элементы принадлежат подгруппе N? Три элемента известны: это тождественная подстановка и два образующих элемента (12)(34) и (13)(24). Произведение их дает подстановку (14)(23). Нетрудно проверить, что произведение любых двух различных подстановок из (12)(34), (13)(24) и (14)(23) совпадает с третьей подстановкой, а квадрат любой подстановки—с единичным элементом. (Пользуясь симметрией, мы можем сократить объем работы и рассмотреть лишь один из трех возможных вариантов). Итак, подгруппа N состоит из четырех элементов. Нетрудно видеть, что квадрат любого из них совпадает с единичным элементом и каждый элемент является четной подстановкой. Других элементов, обладающих этими свойствами, в группе G нет, поскольку, если квадрат элемента a совпадает с единичным элементом, то подстановка a

может быть лишь произведением двух независимых циклов. Если к тому же она четна, то и число циклов четно, то есть равно либо 0, либо 2. Пусть Q — одна из подстановок подгруппы N, отличных от единичного элемента. Тогда $(PQP^{-1})^2 = PQP^{-1}PQP^{-1} = PQQP^{-1} = PP^{-1} = I$, то есть квадрат подстановки PQP^{-1} совпадает с тождественной подстановкой (единичным элементом группы) и подстановка PQP^{-1} четна. Следовательно, подгруппа N является нормальным делителем. Группа G содержит $1 \cdot 2 \cdot 3 = 24$ элемента, а подгруппа N — только 4 элемента. Это означает, что в каждом смежном классе содержится по 4 элемента, то есть число смежных классов равно $24 : 4 = 6$. Из каких элементов состоит отдельный смежный класс? Как производить групповую операцию над смежными классами? Для полного описания того, как действует групповая операция в фактор-группе, прежде всего необходимо выбрать из каждого смежного класса по *представителю* (*элементу*), а затем, перебрав все попарные произведения, установить, что при любом выборе представителей они всегда принадлежат одним и тем же смежным классам. (В общем случае перебор элементов, представляющих смежные классы, сопряжен с большим объемом работы. Действительно, при шести представителях число попарных произведений достигает тридцати шести, и каждое из них необходимо еще умножить поочередно на все элементы нормального делителя. Разумеется, многие из произведений совпадают. В рассматриваемом случае задачу удается решить достаточно просто, не прибегая к перебору попарных произведений всех представителей.) Докажем, что элементы стационарной подгруппы числа 4 можно выбрать в качестве представителей смежных классов по нормальному делителю N. Подстановки, образующие эту стационарную подгруппу, оставляют число 4 на месте, поэтому их можно рассматривать как подстановки трех элементов. Общее число всех подстановок трех элементов равно шести. Поскольку число смежных классов также равно шести, достаточно доказать, что различные элементы стационарной подгруппы числа 4 принадлежат различным смежным классам. Пусть P и Q — элементы этой стационарной подгруппы. Требуется доказать, что, если подстановки P и Q не совпадают, то они принадлежат различным смежным классам по N. Наше утверждение можно сформулировать и иначе: если подстановки P и Q из стационарной подгруппы цифры 4 принадлежат одному смежному классу по нормальному делителю N, то они совпадают. Итак, предположим, что подстановки P и Q принадлежат одному смежному классу по нормальному делителю N, то есть что в N существует подстановка T, удовлетворяющая соотношению $Q = PT$. Разрешим это равенство относительно T: $T = P^{-1}Q$. Поскольку N—подгруппа группы G, то подстановка $P^{-1}Q$ принадлежит N (и, следовательно, оставляет на месте число 4). Но элемент $P^{-1}Q$, стоящий в правой части последнего равенства, совпадает с элементом T, стоящим в левой части того же равенства и принадлежащим подгруппе N, а из всех элементов нормального делителя N оставляет на месте число 4 только тождественная подстановка I. Следовательно, $T = I$, то есть $Q = PT = PI = P$, что и требовалось доказать.

Остается еще установить, каким образом можно умножать смежные классы. Сделать это совсем не трудно, так как элементы, представляющие смежные классы, образуют подгруппу, и поэтому произведение любых двух представителей всегда представляет какой-нибудь смежный класс. Это означает, что умножение смежных классов происходит так же, как умножение подстановок трех элементов.

2. Для большей наглядности поставим в соответствие каждой линейной функции по точке плоскости.

Функции $y = ax + b$ сопоставим точку с координатами (a, b). Поскольку для линейных функций выполняется условие $a \neq 0$, то мы будем рассматривать только такие точки плоскости, у которых первая координата отлична от нуля (рис. 111).

Элементами подгруппы H являются функции вида $y = ax$. Они образуют подгруппу, так как функция $y = x$ также имеет заданный вид, «произведение» (подстановка) функций $y = ax$ и $y = bx$ (функция $y = (ab)x$) и функция $y = a^{-1}x$, обратная функции $y = ax$, принадлежат H. Элементам подгруппы H соответствуют точки плоскости с координатами $(a, 0)$. Они лежат на одной из координатных осей. Выясним, какие точки плоскости соответствуют нормальному делителю N. (В том, что N — нормальный делитель, мы уже убедились.) Так как нормальному делителю N принадлежат линейные функции вида $y = x + c$, то им соответствуют точки плоскости с координатами $(1, c)$. Они заполняют прямую, перпендикулярную оси, соответствующей подгруппе H, и пересекающую эту ось в точке с координатами $(1, 0)$. Пересечение двух прямых, изображающих на плоскости (a, b) подгруппу H и нормальный делитель N, в одной точке означает, что эти две подгруппы имеют лишь один общий элемент. Поскольку они обе заведомо содержат единичный элемент, то общая точка может соответствовать только ему. Действительно, нетрудно видеть, что точка $(1, 0)$ соответствует функции $y = 1x + 0$ (рис. 112).

Чтобы ответить на вопрос о том, сколько общих элементов имеет левый смежный класс с правым смежным классом по подгруппе H, рассмотрим линейную функцию $y = ax + b$ с заданными коэффициентами a и b. В один левый смежный класс с ней попадают функции $y = a(tx) + b$, где t — произвольное отличное от нуля вещественное число. Таким образом, элементами одного левого смежного класса являются

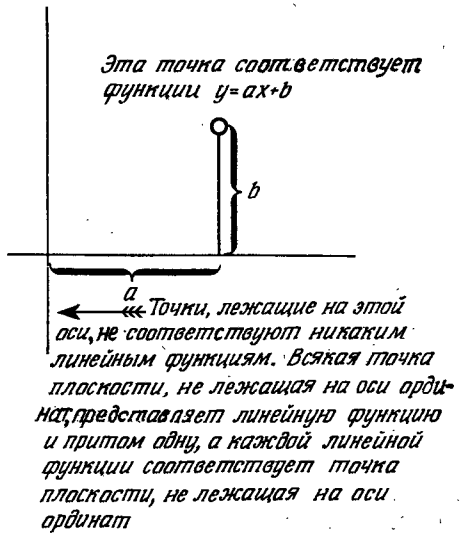


Рис. 111.

линейные функции с произвольным (отличным от нуля) вещественным коэффициентом при x, но постоянным свободным членом. Точки (a, b), соответствующие элементам смежного класса, лежат на «горизонтальных» прямых. Каждая точка такой прямой [за исключением «выброшенной» оси $(0, b)$] соответствует функции, принадлежащей одному и тому же левому смежному классу. Аналогичным образом правому смежному классу, содержащему функцию $y = ax + b$, принадлежат линейные функции вида $y = t(ax + b)$. Им соот-

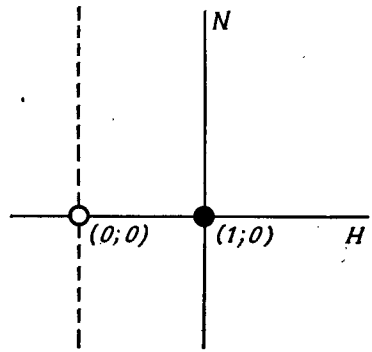


Рис. 112.

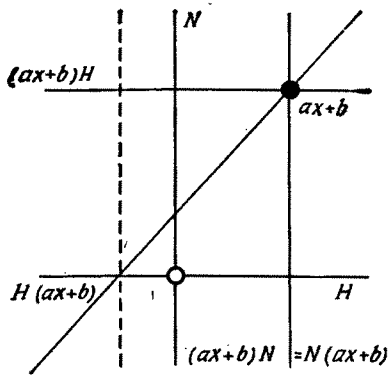


Рис. 113.

ветствуют точки плоскости с координатами (ta, tb), отношение которых (tb/ta) не зависит от выбора точки. Такие точки заполняют прямую, проходящую через начало координат. Кроме того, эта прямая проходит через точку (a, b) и, следовательно, полностью определена. Определим теперь смежные классы по подгруппе N. Поскольку N — нормальный делитель группы G, то достаточно определить смежные классы лишь с одной из сторон: либо только левые, либо только правые. В одном смежном классе с функцией $y = ax + b$ на этот раз оказываются функции вида $(ax + b) + t$, где t — произвольное вещественное число. На плоскости им соответствуют точки с координатами $(a, b + t)$, лежащие на «вертикальной» прямой, которая проходит через точку (a, b). На вопросы о том, сколько общих элементов имеют те или иные смежные классы, проще всего можно ответить, если рассмотреть соответствующие прямые и выяснить число их общих точек.

Горизонтальные прямые не имеют общих точек. Следовательно, левые смежные классы по подгруппе H не могут иметь общих элементов. Прямые, проходящие через начало координат, имеют общую точку, но она «выколота». Это означает, что и правые смежные классы по подгруппе H не имеют общих элементов. Горизонтальная прямая в общем случае имеет с прямой, проходящей через начало координат, одну общую точку (исключение составляет прямая, проходящая через начало координат и совпадающая с горизонтальной осью, с которой горизонтальные прямые не имеют общих точек). Следовательно, в общем случае левый смежный класс по подгруппе H имеет один общий элемент с правым смежным классом по той же подгруппе, если правый смежный класс не «вырождается» в подгруппу H: разумеется с этим смежным классом ни один другой левый смежный класс по подгруппе H не имеет общих элементов. Аналогичным образом можно убедиться в том, что все вертикальные прямые имеют по одной общей точке как с любой горизонтальной прямой, так и с любой прямой, проходящей через начало координат. Это означает, что соответствующие прямым смежные классы имеют по одному общему элементу (рис. 113).

Переходим к последнему вопросу задачи. Требуется найти произведения комплексов HN и NH. Иначе говоря, необходимо выяснить, какие линейные функции можно представить в виде «произведений» линейных функций $y = ax$ и $y = x + b$, то есть в виде $y = a(x + b)$ и $y = (ax) + b$. Ясно, что в виде $y = (ax) + b$ представима любая линейная функция, то есть NH совпадает со всей группой G. Если задана произвольная функция $y = ax + c$, то ее можно записать в виде $y = a(x + a^{-1}c)$, а это означает, что и HN совпадает со всей группой G.

3. Прежде чем приступать к решению задачи, изобразим наглядно группу G и подмножества H, M и N.

Из условий задачи известно, что M — подгруппа группы G, поскольку M состоит из общих элементов двух подгрупп. Следовательно, M — подгруппа в группе H, так как в H действует та же групповая операция, что и во всей группе G (рис. 114).

В предыдущей задаче мы доказали, что M — нормальный делитель группы H. Иначе говоря, если $a \in H$ и $x \in$

$\in$ M, то $axa^{-1} \in$ M. Поскольку M содержится в H, то и элемент x принадлежит подгруппе H. Но тогда (по групповому свойству) элемент axa^{-1} также принадлежит подгруппе H. Так как M содержится в нормальном делителе N, то среди прочих элементов подгруппы M нормальному делителю N принадлежит и элемент x. Следовательно, элемент axa^{-1} также принадлежит N. Таким образом, axa^{-1} — общий элемент нормального делителя N и подгруппы H, а это означает, что axa^{-1} принадлежит M.

Во второй половине приведенного выше доказательства, как нетрудно проверить, используется лишь то, что N — нормальный делитель группы G. Никаких предположений относительно свойств элемента a не делается: им может быть любой элемент группы G. Можно доказать также, что, если не только N, но и H — нормальный делитель группы G и $x \in$ M, то $axa^{-1} \in$ H при любом $a \in$ G. Это и означает, что $axa^{-1} \in$ M при любом $a \in$ G.

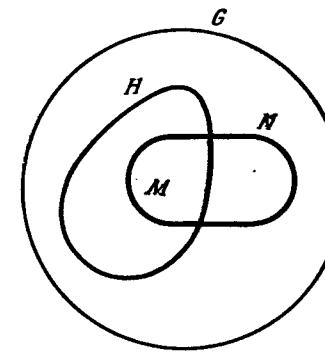


Рис. 114.

4.3

1. Пусть a — образующий элемент группы A, b — образующий элемент группы B. Тогда прямое произведение A $\times$ B состоит из пар элементов (a^i, b^j), где i и j — неотрицательные целые числа, удовлетворяющие неравенствам $i < p$, $j < q$. Поскольку при всех i и j мы получаем различные элементы, то общее число элементов в нрямом произведении A $\times$ B равно pq. Докажем, что A $\times$ $\times$ B — циклическая группа. Для этого достаточно убедиться в том, что A $\times$ B содержит элемент порядка pq и даже что A $\times$ B содержит элемент, порядок которого не меньше pq. (Элемент, у которого число различных степеней больше pq, не мог бы существовать в группе A $\times$ B, так как она содержит всего pq элементов.)

Докажем, что порядок элемента (a, b) не меньше pq. Действительно, если порядок элемента (a, b) равен d, то $(a, b)^d = (e, e)$, где e — единичные элементы в группах A и B. По определению групповой операции в прямом произведении A $\times$ B получаем: $(a, b)^d = (a^d, b^d)$. Следовательно, элемент a^d совпадает с единичным элементом группы A, а элемент b^d — с единичным элементом группы B. Это возможно лишь в том случае, если показатель степени d кратен как порядку элемента a, так и порядку элемента b, то есть числам p и q. По условию задачи, p и q — раэличные простые числа, поэтому число d может быть кратным каждому из них в том и только в том случае, если оно кратно произведению pq и поэтому не меньше pq.

2. Доказать, что порядок группы A $\times$ B равен p^2 можно так же, как был установлен порядок прямого произведения в решении предыдущей задачи. Так как $(a^i, b^j)^p = (a^{ip}, b^{jp}) = (a^{pi}, b^{pj}) = (e^i, e^j) = (e, e)$, то порядок любого элемента прямого произведения равен p. Следовательно, ни у одного из элементов прямого произведения A $\times$ B циклических групп порядка p не существует p^2 различных степеней.

3. Пусть n — порядок группы A, а k — порядок группы B. Тогда в парах элементов, образующих прямое произведение A $\times$ B, первое место можно заполнить n различными способами, а второе место k различными способами (независимо от первого). Следовательно, общее число

пар равно nk. Поскольку как первая, так и вторая «компонента» пары (то есть как элементы группы A, так и элементы группы B) выбирались каждый раз по-другому, то все полученные пары различны, и поэтому прямое произведение $A \times B$ действительно содержит nk элементов.

4. Единичный элемент прямого произведения двух групп принадлежит к числу пар, у которых на втором месте стоит единичный элемент, поскольку обе его компоненты являются единичными элементами прямых сомножителей. Произведение двух элементов рассматриваемого вида (u, e) и (v, e) равно (uv, e), то есть его вторая компонента также совпадает с единичным элементом второго сомножителя прямого произведения. Наконец, так как $(u, e)^{-1} = (u^{-1}, e)$, то и элемент, обратный элементу заданного вида, имеет вторую компоненту, равную e. Следовательно, элементы (u, e) прямого произведения двух групп, где u — произвольный элемент первого сомножителя, а e — единичный элемент второго сомножителя, образуют подгруппу. Докажем, что для этой подгруппы выполняется необходимый и достаточный признак нормального делителя. Если (a, b) — произвольный элемент прямого произведения, а элемент (u, e) принадлежит интересующей нас подгруппе, то $(a, b)(u, e)(a, b)^{-1} = (a, b) \times (u,e)(a^{-1}, b^{-1}) = (aua^{-1}, beb^{-1}) = (aua^{-1}, e)$, в силу чего $(a, b)(u, e)(a, b)^{-1}$ также принадлежит рассматриваемой подгруппе, что и требовалось доказать.

5. В один смежный класс с элементом (a, b) попадают все элементы вида $(a, b)(u, e) = (au, b)$. Их второй компонентой является фиксированный элемент b группы B. Справедливо и обратное утверждение: если вторая компонента некоторого элемента прямого произведения $A \times B$ равна b, то этот элемент принадлежит тому же смежному классу, что и элемент (a, b). Действительно, при любом $c \in A$ выполняется соотношение $(c, b) = (aa^{-1}c, be) = (a, b)(a^{-1}c, e)$, а второй сомножитель в правой части последнего равенства принадлежит нормальному делителю. Поскольку среди элементов вида (c, b) имеется ровно один элемент, у которого первая компонента совпадает с единичным элементом группы A [элемент (e, b)], то тем самым наше утверждение доказано.

5.1

1. Оба утверждения очевидны. Рефлексивность изоморфизма следует из того, что тождественное отображение принадлежит к числу изоморфизмов, а транзитивность — из того, что отображение, получающееся при последовательном выполнении двух изоморфизмов, также является изоморфизмом.

(Рефлексивность, транзитивность и симметрия изоморфизмов позволяют утверждать, что все группы допускают разбиение на непересекающиеся классы. Каждая группа принадлежит одному и только одному классу и, следовательно, однозначно определяет некоторую абстрактную группу. Все группы, принадлежащие одному классу, изоморфны. Любые две группы, принадлежащие различным классам, не изоморфны.)

2. Для доказательства коммутативности воспользуемся тем, что соответствие $(a, b) \to (b, a)$ является изоморфизмом. Перейдем к доказательству ассоциативности. Элементы прямого произведения $(A \times B) \times C$ имеют вид $((a, b), c)$ а элементами прямого произведения $A \times (B \times C)$ являются тройки $(a, (b, c))$. Ассоциативность следует из того, что соответствие $((a, b), c) \to (a, (b, c))$ является изоморфизмом.

(Прямое произведение трех групп можно было бы определить и непосредственно, как группу, элементами которой являются тройки элементов (a, b, c). Изоморфизм $((a, b), c) \to (a, b, c)$ показывает, что эта группа изоморфна прямому произведению $(A \times B) \times C$ и, следовательно, прямому произведению $A \times (B \times$

$\times$ C). Таким образом, «длинное» прямое произведение, состоящее из трех или большего числа сомножителей, всегда можно записать в виде прямого произведения прямых произведений, что гораздо удобнее, чем «прямая» запись прямого произведения многих сомножителей.)

3. Докажем, что соответствие $(a, b) \to ab$ (где $a \in A$, $b \in B$) является изоморфизмом. Поскольку равенство пар элементов влечет за собой совпадение компонент, то соответствие $(a, b) \to ab$ можно считать отображением.

Если образы пар (a_1, b_1) и (a_2, b_2) при этом отображении совпадают, то, умножив обе части равенства $a_1b_1 = a_2b_2$ слева на a_2^{-1}, а справа на b_1^{-1}, мы получим новое равенство $a_2^{-1}a_1 = b_2b_1^{-1}$. В его левой части стоит элемент, принадлежащий подгруппе A, а в правой части — элемент из подгруппы B. Поскольку эти подгруппы не имеют других общих элементов, кроме единичного элемента, то $a_2^{-1}a_1 = e$ и $b_2b_1^{-1} = e$. Умножив первое соотношение слева на a_2, а второе соотношение справа на b_1, получим: $a_1 = a_2$ и $b_1 = b_2$. Итак, мы доказали, что при отображении $(a, b) \to ab$ различные пары (a, b) переходят в различные произведения ab.

Докажем теперь, что любой элемент группы G можно представить в виде произведения ab, где $a \in A$ и $b \in B$. Так как

$$(a_1b_1)(a_2b_2) = a_1(b_1a_2)b_2 =$$
$$= a_1(a_2a_2^{-1}b_1a_2)b_2 =$$
$$= (a_1a_2)(a_2^{-1}b_1a_2b_2)$$

и

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

то произведение элементов представимо в виде произведения ab, и элементы, обратные таким элементам, также представимы в виде произведения ab (элементы $a_2^{-1}ba_2$ и $ab^{-1}a^{-1}$ принадлежат подгруппе B, поскольку B — нормальный делитель группы G). Единичный элемент допускает тривиальное разложение требуемого вида. Следовательно, произведения ab образуют группу, содержащую оба нормальных делителя A и B группы G. Произведения ab включают в себя поэтому все элементы подгруппы, порожденной нормальными делителями A и B, а поскольку эта подгруппа совпадает со всей группой G, то все элементы исходной группы G представимы в виде произведений ab. Отсюда тотчас же следует, что каждый элемент группы G является образом некоторого элемента прямого произведения нормальных делителей A и B; в элемент ab переходит при рассматриваемом отображении пара (a, b).

Необходимо еще проверить, сохраняет ли отображение $(a, b) \to ab$ групповую операцию. В прямом произведении «умножение» элементов определяется соотношением $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$. Для сохранения операции необходимо, чтобы для элементов группы G, соответствующих элементам прямого произведения, выполнялось равенство $(a_1b_1)(a_2b_2) = a_1a_2b_1b_2$. Сокращая слева на a_1, а справа на b_2, преобразуем его к виду $b_1a_2 = a_2b_1$. Итак, требуется доказать, что для любого элемента a из нормального делителя A и любого элемента b из нормального делителя B выполняется соотношение $ab = ba$, которое можно представить в виде

$$b^{-1}a^{-1}ba = e.$$

Именно его нам и предстоит доказать. Поскольку нормальные делители A и B имеют лишь один общий элемент — единичный элемент группы G, то достаточно доказать, что элемент $b^{-1}a^{-1}ba$ принадлежит как подгруппе A, так и подгруппе B. Поскольку B — нормальный делитель группы G, то он содержит элемент $a^{-1}ba$, а подгруппа A по той же причине содержит элемент $b^{-1}a^{-1}b$.

Оба элемента принадлежат B.

$$\underbrace{b^{-1}\cdot\overbrace{a^{-1}\cdot b}\cdot a}$$

Оба элемента принадлежат A.

Но A и B — подгруппы, и поэтому вместе с любыми двумя своими элементами содержат и их произведение, что и требовалось доказать.

5.2

1. Поскольку гомоморфизм сохраняет групповую операцию, то им может быть только отображение $\varphi(n) = a^n$ (n — целое число). Из тождеств для степеней одного элемента группы следует, что оно действительно является гомоморфизмом. Если φ — мономорфизм, то все степени элемента a различны, или, что то же, a — элемент бесконечного порядка. Если φ — эпиморфизм, то вся группа состоит из степеней элемента a, то есть является циклической.

Ядро гомоморфизма $\varphi(a) = a^n$ состоит из тех и только тех целых чисел k, при которых a^k совпадает с единичным элементом группы. Следовательно, порядок элемента a равен некоторому целому числу, а ядро гомоморфизма состоит из целых кратных этого числа.

2. а) Сохранение групповой операции следует из закона сложения комплексных чисел: $(a + bi) + (c + di) = (a + c) + (b + d)i$. Ясно, что при отображении $a + bi \to b$ множество образов совпадает с множеством всех вещественных чисел, то есть отображение $a + bi \to b$ является эпиморфизмом. Ядро этого эпиморфизма образуют комплексные числа, переходящие при отображении в нуль, то есть комплексные числа с нулевой мнимой частью, или вещественные числа. Следовательно, по теореме о гомоморфизмах, фактор-группа аддитивной группы комплексных чисел по аддитивной группе вещественных чисел изоморфна группе вещественных чисел.

б) Ясно, что соответствие

$$r(\cos\varphi + i\sin\varphi) \to \cos\varphi + i\sin\varphi$$

однозначно, а теорема Муавра позволяет утверждать, что оно является гомоморфизмом. Все комплексные числа с модулем 1 при отображении переходят в себя, поэтому в действительности можно говорить об эпиморфизме. Ядро гомоморфизма образуют комплексные числа с аргументом, равным 0°. Это — не что иное, как положительные вещественные числа. Следовательно, по теореме о гомоморфизмах фактор-группа мультипликативной группы отличных от нуля комплексных чисел по мультипликативной группе положительных вещественных чисел изоморфна мультипликативной группе комплексных чисел с модулем 1.

в) Ясно, что соответствие $a + bi \to \sqrt{a^2 + b^2}$ однозначно. Гомоморфизмом оно является потому, что модуль произведения совпадает с произведением модулей всех сомножителей. Поскольку каждое положительное вещественное число при гомоморфизме $a + bi \to \sqrt{a^2 + b^2}$ переходит в себя, то в действительности мы имеем дело с эпиморфизмом. Ядро этого эпиморфизма составляют комплексные числа, отображаемые в единицу, то есть те и только те комплексные числа, модуль которых равен 1. Следовательно, по теореме о гомоморфизмах, фактор-группа мультипликативной группы отличных от нуля комплексных чисел по мультипликативной группе комплексных чисел с модулем 1 изоморфна мультипликативной группе положительных вещественных чисел.

г) Поскольку преобразования подобия определены так, что число, показывающее, во сколько раз изменяется длина отрезка (коэффициент подобия), зависит только от преобразования, то мы действительно получаем отображение. В решении задачи 1д из раздела 4.2 было доказано, что при умножении преобразований подобия коэффициенты подобия также умножаются. Это означает, что рассматриваемое отображение является гомоморфизмом. Если

λ — произвольное положительное число, то соответствующее ему преобразование подобия (с коэффициентом подобия, равным λ) мы получим, рассмотрев растяжение в λ раз от какой-нибудь точки (или при $\lambda < 1$ сжатие в λ раз к какой-нибудь точке). Итак, отображение, о котором говорится в задаче, является эпиморфизмом. Ядро эпиморфизма образуют преобразования подобия, переходящие при отображении в единичный элемент мультипликативной группы положительных вещественных чисел, то есть преобразования подобия с коэффициентом подобия 1. Это — не что иное, как движения. Следовательно, по теореме о гомоморфизмах, фактор-группа преобразований подобия по группе движений изоморфна мультипликативной группе положительных вещественных чисел.

Сравнивая эту задачу с задачей 1 из раздела 4.2, можно заметить, что по существу мы повторно доказали утверждения этой задачи (придав им точную формулировку, использующую понятие гомоморфизма). Теорема о гомоморфизмах позволила существенно сократить доказательства.

3. Ясно, что φ и ψ — отображения. Из определения групповой операции в прямом произведении групп (поскольку над компонентой a производится групповая операция группы A, а над компонентой b — групповая операция группы B) следует, что φ и ψ — гомоморфизмы. При $a_1 \neq a_2$ пары (a_1, e) и (a_2, e) различны, поэтому φ — мономорфизм. Так как элемент b может быть любым элементом из группы B [например, как образ пары (e, b)], то ψ — эпиморфизм. Нетрудно видеть, что эпиморфизм ψ отображает элементы (a, e) прямого произведения G в единичный элемент группы G, а пары (a, e) образуют $\operatorname{Im}\varphi$. Следовательно, $\operatorname{Im}\varphi = \operatorname{Ker}\psi$.

4. Прежде всего необходимо установить, что соответствие $h\mathrm{M} \to h\mathrm{N}$ можно считать отображением. Это следует из того, что M содержится в N и, следовательно, hM — подмножество смежного класса hN. Поскольку любое подмножество группы, если оно содержится в некотором смежном классе по N, может быть только таким подмножеством, то hM однозначно определяет смежный класс hN. Ясно, что смежный класс hM принадлежит подгруппе {H, M}. Произведение двух таких смежных классов является одним из смежных классов hM. Смежный класс, обратный смежному классу hM, также принадлежит к числу смежных классов того же типа. Следовательно, подгруппа {H, M} исчерпывается смежными классами hM. Итак, соответствие $h\mathrm{M} \to h\mathrm{N}$ задает отображение смежных классов группы {H, M} по нормальному делителю M в некоторое множество — как показывают аналогичные рассуждения, в фактор-группу {H, N}/N.

Это отображение является гомоморфизмом, так как M и N — нормальные делители группы G и $(h_1\mathrm{M})(h_2\mathrm{M}) = (h_1h_2\mathrm{M})$, $(h_1\mathrm{N})(h_2\mathrm{N}) = (h_1h_2\mathrm{N})$. Итак, рассматриваемое отображение действительно сохраняет групповую операцию.

Чтобы мы могли применить теорему о гомоморфизмах, для полученного гомоморфизма φ необходимо определить его образ $\operatorname{Im}\varphi$ и ядро $\operatorname{Ker}\varphi$. Как показывают рассуждения, аналогичные приведенным выше, вся подгруппа {H, N} исчерпывается смежными классами hN, то есть $\operatorname{Im}\varphi = \{\mathrm{H}, \mathrm{N}\}/\mathrm{N}$.

Рассмотрим теперь ядро гомоморфизма φ. Смежный класс hM принадлежит $\operatorname{Im}\varphi$, если его прообраз при гомоморфизме — смежный класс hN — является единичным элементом фактор-группы {H, N}/N, то есть если $h\mathrm{N} = \mathrm{N}$. Но так происходит в том и только в том случае, если $h \in \mathrm{N}$. Так как элемент h по определению принадлежит подгруппе H, то ядро гомоморфизма φ образуют те смежные классы hM, для которых $h \in \mathrm{H} \cap \mathrm{N}$. (Через H $\cap$ N мы обозначили пересечение, то есть общую

часть, подгрупп H и N.) Эти смежные классы порождают подгруппу $\{H \cap N, M\}$. А поскольку элементы ядра являются смежными классами по нормальному делителю M, то ядро гомоморфизма φ совпадает с фактор-группой $\{H \cap N, M\}/M$. Отсюда по теореме о гомоморфизмах получаем

$$(\{H, M\}/M)/(\{H \cap N, M\}/M) \cong$$
$$\cong \{H, N\}/N.$$

5. Если $M = \{e\}$, то, с одной стороны, $\{H, M\} = H$ и $\{H \cap N, M\} = H \cap N$, а с другой стороны, вместо H/M можно подставить H, а вместо $H \cap N/M$ — пересечение $H \cap N$. Проделав эти преобразования, мы получим первую теорему Нётер об изоморфизмах:

$$H/H \cap N \cong \{H, N\}/N.$$

Если $H = G$, то $\{G, M\} = \{G, N\} = G$; кроме того, $G \cap N = N$ и $\{N, M\} = N$. Производя соответствующие подстановки, преобразуем приведенное выше соотношение к виду

$$(G/M)/(N/M) \cong G/N.$$

Это соотношение известно под названием второй теоремы Нётер об изоморфизмах.

Нетрудно видеть, что правая часть соотношения получена как бы при сокращении одинаковых знаменателей «дробей», стоящих в числителе и в знаменателе левой части. Первая теорема Нётер также обнаруживает общие черты с действиями, производимыми над обычными дробями. Если соотношение

$$H/H \cap N \cong \{H, N\}/N$$

прочитать справа налево, то видно, что числитель и знаменатель «дроби» можно заменять пересечением с одной и той же подгруппой. Если то же соотношение прочитать слева направо, то видно, что вместо числителя и знаменателя можно рассматривать подгруппу, порожденную числителем и нормальным делителем, которая профакторизована по нормальному делителю.

5.3

1. Воспользуемся теоремой о гомоморфизмах. Если $\varphi : A \to B$, то $\chi : a \to a \cdot \operatorname{Ker} \varphi$ и $\psi : a \cdot \operatorname{Ker} \varphi \to \varphi(a)$ при любом $a \in A$. Таким образом, χ — эпиморфизм, ψ — мономорфизм и $\varphi = \psi\chi$, что и требовалось доказать.

2. Если φ — мономорфизм и $\varphi\alpha = \varphi\beta$, то при любом x, на который можно подействовать как отображением α, так и отображением β, выполняется соотношение $\varphi\alpha(x) = \varphi\beta(x)$. Поскольку различные элементы мономорфизм φ переводит в различные элементы, то $\alpha(x) = \beta(x)$. Это и означает, что $\alpha = \beta$.

Пусть ψ — эпиморфизм и $\gamma\psi = \delta\psi$. Это равенство означает, что, если ψ отображает группу A на группу B, то как γ, так и δ отображают B в какую-то другую группу. Пусть b — произвольный элемент группы B. Так как ψ — эпиморфизм, то в группе A существует элемент a, образ которого при эпиморфизме ψ совпадает с b, то есть $b = \psi(a)$. По условию задачи, $\gamma(b) = \gamma\psi(a) = \delta\psi(a) = \delta(b)$. Так как b — произвольный элемент группы B, то $\gamma = \delta$, что и требовалось доказать.

3. То, что для любого изоморфизма φ существует обратный изоморфизм ψ, было доказано при рассмотрении изоморфизмов. Докажем обратное утверждение. Пусть $\varphi : A \to B$ — некоторый гомоморфизм, а ψ — гомоморфизм, обладающий тем свойством, что $\varphi\psi$ и $\psi\varphi$ — тождественные отображения. Гомоморфизм ψ может осуществлять только отображение $\psi : B \to A$ (в противном случае отображения $\varphi\psi$ и $\psi\varphi$ не могли бы быть тождественными). Если $\varphi(a_1) = \varphi(a_2)$, то (поскольку отображение $\psi\varphi$ любой элемент переводит в себя) $a_1 = \psi\varphi(a_1) = \psi\varphi(a_2) = a_2$. Следовательно, φ — мономорфизм. Если b — произвольный элемент группы B_2 то (поскольку отображение $\varphi\psi$ лю-

бой элемент переводит в себя) $b = \varphi\psi(b)$. Это означает, что любой элемент b группы B является образом некоторого элемента группы A при гомоморфизме φ, то есть φ — эпиморфизм. Но гомоморфизм, обладающий свойствами мономорфизма и эпиморфизма, является изоморфизмом. Следовательно, φ — изоморфизм.

4. Утверждения задачи докажем от противного. а) Если α — не мономорфизм, то существуют два различных элемента, переходящих под действием α в один и тот же элемент. Но в этом случае $\beta\alpha$ отображает те же два различных элемента в один элемент и поэтому не может быть мономорфизмом. б) Рассмотрим гомоморфизмы $\alpha : A \to B$ и $\beta : B \to C$. Если β — не эпиморфизм, то в группе C найдется элемент c, не являющийся образом ни одного из элементов группы B, то есть не представимый в виде $c = \beta(b)$. Но тогда ни один из элементов a группы A не представим в виде $\beta\alpha(a)$, поскольку $\alpha(a)$ — элемент группы B. Следовательно, $\beta\alpha$ — не эпиморфизм. В обоих случаях полученные противоречия доказывают, что исходное предположение неверно, то есть что выполняются исходные утверждения задачи.

5. Требуемым свойством обладают гомоморфизмы $\alpha : a \to (a, b)$ и $\beta : (a, b) \to a$.

6. Так как $\beta\alpha$ — тождественное отображение, а всякое тождественное отображение является мономорфизмом, то из задачи 4 следует, что α — мономорфизм. Это означает, что α изоморфно отображает группу A на $\mathrm{Im}\alpha$. Рассмотрим подгруппу $\mathrm{Ker}\,\beta$ группы G. И $\mathrm{Im}\alpha$, и $\mathrm{Ker}\,\beta$ — нормальные делители группы $G : \mathrm{Im}\alpha$ — по условию задачи, $\mathrm{Ker}\,\beta$ — как ядро гомоморфизма.

Если $g \in \mathrm{Im}\alpha \cap \mathrm{Ker}\beta$, то g можно представить в виде $g = \alpha(a)$, где a — некоторый элемент группы A, а $\beta(g)$ совпадает с единичным элементом e группы A. Таким образом, $e = \beta(g) = \beta\alpha(a)$, а поскольку $\beta\alpha$ — тождественное отображение, то $\beta\alpha(a) = a$. Следовательно, $a = e$, поэтому элемент g, являющийся образом элемента a при гомоморфизме α, совпадает с единичным элементом группы G, а $\mathrm{Im}\alpha$ и $\mathrm{Ker}\beta$ имеют единственный общий элемент — единичный элемент.

Если $g \in G$, то $\alpha\beta(g) \in G$ и для $b = g(\alpha\beta(g))^{-1}$ выполняется соотношение $\beta(b) = \beta(g)\beta\alpha\beta(g^{-1})$. Но $\beta\alpha$ — тождественное отображение, поэтому $\beta(b) = \beta(g)\beta(g^{-1}) = e$, то есть $b \in \mathrm{Ker}\beta$. Нетрудно видеть, что элемент $\alpha\beta(g)$ принадлежит $\mathrm{Im}\alpha$, а элемент g можно представить в виде $g = b \cdot \alpha\beta(g)$. Следовательно, все элементы группы G принадлежат группе, порожденной $\mathrm{Im}\alpha$ и $\mathrm{Ker}\beta$, то есть $\mathrm{Im}\,\alpha$ и $\mathrm{Ker}\,\beta$ порождают всю группу G. Из задачи 3 раздела 5.1 получаем, что в этом случае

$$G \cong \mathrm{Ker}\,\beta \times \mathrm{Im}\,\alpha \text{ и } A \cong \mathrm{Im}\,\alpha.$$

Утверждение задачи соответствует $B = \mathrm{Ker}\beta$.

6.2

1. Так как рассматриваемая полугруппа содержит бесконечно много элементов, то речь может идти лишь о множествах, допускающих бесконечно много отображений на себя. Таким свойством обладают только бесконечные множества. Это означает, что сколько бы элементов множества $a_1, a_2, \ldots, a_n, \ldots$ мы ни перебрали, всегда найдутся элементы множества, еще не названные нами. Рассмотрим отображение, которое каждый из перенумерованных нами элементов переводит в следующий элемент, а каждый из остальных элементов оставляет на месте. Степени этого отображения вместе с тождественным отображением образуют полугруппу, изоморфную свободной полугруппе, порожденной одним элементом.

2. Пусть $g_1, g_2, \ldots, g_k$ — образующие элементы группы. Выберем k образующих элементов свободной полугруппы и отобразим их на эле-

менты g_1, g_2, ..., g_k, а остальные k образующих свободной полугруппы отобразим на обратные элементы g_1^{-1}, g_2^{-1}, ..., g_k^{-1}. Гомоморфизм, осуществляющий заданное нами отображение, существует (и более того — однозначно определен). Так как любой элемент группы можно представить в виде произведения образующих элементов и элементов, обратных образующим, то вся группа является гомоморфным образом свободной полугруппы.

(Система из $2k$ образующих элементов свободной полугруппы понадобилась потому, что одна лишь операция умножения не позволяет задавать обратные элементы, поэтому, если бы существование обратных элементов не гарантировалось заранее, то его пришлось бы доказывать особо в каждом отдельном случае. Соображения подобного рода используются при построении так называемых «свободных групп». Эти группы характеризуются тем, что их образующие элементы не связаны никакими соотношениями, кроме тех, которые следуют из аксиом группы. Соответствие между образующими элементами двух групп одноэначно определяет гомоморфизм, а отличительное свойство свободных групп при гомоморфизме не нарушается.)

7

1. Если x — один из элементов цикла, то элементы цикла расположены в следующем порядке: x, xg, xg^2, ... Все эти элементы различны до тех пор, пока соответствующая степень элемента g не совпадает с единичным элементом группы. Следовательно, длина каждого цикла совпадает с порядком $o(g)$ элемента g. Поскольку (при $g \neq e$) каждый элемент группы входит в один из циклов, то общее число элементов во всех циклах равно порядку группы. Следовательно, порядок элемента является делителем порядка группы. (Мы получаем новое, весьма простое, доказательство частного случая теоремы Лагранжа.)

Если группа не конечна, то для конечных элементов g длина циклов будет по-прежнему совпадать с порядком элемента $o(g)$, а для элементов бесконечного порядка длина каждого цикла бесконечна, причем в обе стороны (в частности, число бесконечных циклов может оказаться равным 1).

2. В этом случае подстановка Q_g переводит элемент x в элемент gx, а подстановка Q_h отображает gx в $(hg)x$. Но именно в элемент $(hg)x$ элемент x переходит под действием подстановки Q_{hg}. Следовательно, соответствие $x \to gx$ не сохраняет, а «обращает» групповую операцию, поскольку образ произведения оказывается равным произведению образов, взятых в обратном порядке.

3. В случае полугрупп соответствие P_g, при котором любому элементу x сопоставляется элемент xg, вообще говоря, не является подстановкой. Соответствия P_g связаны с подстановками так же, как отображения множества в себя с взаимно-однозначными отображениями множества на себя. Относительно соответствий P_g можно показать, что, если задать на них операцию «умножения», аналогичную операции, производимой над подстановками, то P_g образуют полугруппу.

Нетрудно проверить, что соответствие $\varphi : g \to P_g$ сохраняет операцию. Тем не менее φ не является мономорфизмом, как в случае групп. Действительно, существуют полугруппы, в которых при различных g и h для всех элементов x выполняется соотношение $xg = xh$. (Такова, например, полугруппа, в которой умножение задано так, что произведение двух элементов совпадает с первым сомножителем $ab = a$.)

При доказательстве теоремы Кэли мы установили, что отображение $\varphi : g \to P_\varphi$ является мономорфизмом, использовав при этом существование единичного элемента группы. Нетрудно видеть, что если в полугруппе

существует (левый) единичный элемент, то мы также получаем мономорфизм.

Для произвольных полугрупп справедливо утверждение, аналогичное теореме Кэли, поскольку всякую полугруппу можно дополнить одним элементом так, что этот элемент будет единичным элементом расширенной полугруппы, а для полугруппы с единицей доказательство теоремы Кэли «проходит».

К главе второй

1.1

1. Все тождества относительно сложения выполнены, в этом мы убедились при рассмотрении кольца многочленов. Операция, заданная на множестве многочленов, представляет собой не что иное, как замену переменной, или подстановку. Докажем ассоциативность. Пусть $f(x)$, $g(x)$ и $h(x)$ — три многочлена и $v(x) = f(x) \circ g(x) = f(g(x))$, $u(x) = g(x) \circ h(x) = g(h(x))$. Тогда

$$f(x) \circ [g(x) \circ h(x)] = f(x) \circ u(x) = f(u(x)) = f(g(h(x))$$

и

$$[f(x) \circ g(x)] \circ h(x) = v(x) \circ h(x) = v(h(x)) = f(g(h(x))).$$

Тем самым ассоциативность операции доказана.

Если $k(x) = f(x) + g(x)$, то для любого многочлена $u(x)$ справедливо соотношение $k(u(x)) = f(u(x)) + g(u(x))$, или $(f(x) + g(x)) \circ u(x) = f(x) \circ u(x) + g(x) \circ u(x)$. Это означает, что для операции выполняется правый закон дистрибутивности. В отличие от него левый закон дистрибутивности для операции $\circ$ утрачивает силу. Например, при $f(x) = g(x) = x$ и $u(x) = x^2$

$$u(x) \circ (f(x) + g(x)) = x^2 \circ 2x = (2x)^2 = 4x^2,$$

а

$$u(x) \circ f(x) + u(x) \circ g(x) = x^2 \circ x + x^2 \circ x = x^2 + x^2 = 2x^2.$$

Этот пример показывает, что из тождеств, которым удовлетворяют заданные на элементах кольца операции, выпадает один из законов дистрибутивности. Поэтому существенно, чтобы в число условий входили оба закона дистрибутивности.

2. Одним из элементов кольца является нулевой элемент. Умножение на нуль всегда коммутативно. Если кольцо содержит только один элемент, то утверждение задачи доказано. Если в кольце имеется еще один элемент a, то существует лишь одно произведение, отличное от нуля: $a \cdot a$. Ясно, что оба входящих в него сомножителя можно переставлять местами, не изменяя произведение. Следовательно, утверждение задачи можно считать доказанным и для колец, содержащих два элемента. Если кольцо, кроме нуля, содержит элементы a и b, то элемент $a + b$ не может совпадать ни с a, ни с b (так как оба элемента a и b отличны от нуля), в силу чего $a + b = 0$. Но тогда $ab = -aa$ (так как $a(a + b) = aa + ab$ и $a(a + b) = a0 = 0$) и, кроме того, $ba = -aa$ (так как $(a + b)a = aa + ba$). Таким образом, в этом случае отличные от нуля элементы кольца удовлетворяют соотношению $ab = ba$. (Коммутативность умножения для всех других вариантов выбора двух элементов кольца следует из приведенных выше соображений.)

3. Начнем с группы по сложению, состоящей из двух элементов: чисел 0 и 1. Единичным элементом группы является число 0, поэтому $1 + 1 = 0$. Рассмотрим множество из четырех элементов: прямое произведение такой группы на себя. Оно сос-

тоит из пар (a, b), а каждая из компонент a и b может принимать любое из двух значений 0 или 1. Сложение в прямом произведении групп определено, а умножение мы зададим следующим образом:

$$(a, b)(c, d) = ((a + b)c,\ (a + b)d).$$

Прежде всего докажем ассоциативность умножения:

$$(a, b)[(c, d)(e, f)] = (a, b)((c + d)e,$$
$$(c + d)f) = ((a + b)(c + d)e,$$
$$(a + b)(c + d)f);$$
$$[(a, b)(c, d)](e, f) =$$
$$= ((a + b)c,\ (a + b)d)(e, f) =$$
$$= (((a + b)c + (a + b)d)e,$$
$$((a + b)c + (a + b)d)f).$$

Итак, умножение ассоциативно.

Аналогичным образом можно доказать и оба закона дистрибутивности.

Построенное кольцо не коммутативно, так как, например, $(1, 0)(1, 1) = (1, 1)$, а $(1, 1)(1, 0) = (0, 0)$.

4. Заданное на множестве пар комплексных чисел сложение является не чем иным, как операцией, заданной в прямом произведении аддитивной группы комплексных чисел на себя, поэтому относительно сложения пары комплексных чисел образуют группу. Как показывают прямые выкладки, умножение пар ассоциативно и дистрибутивно (выполняются оба закона дистрибутивности).

Единичным элементом кольца служит пара $(1, 0)$, элементом, обратным элементу (a, b) — пара $(\overline{a}/N, -b/N)$, где $N = a\overline{a} + b\overline{b} = |a|^2 + |b|^2$. Если $(a, b) \neq (0, 0)$, то вещественное число отлично от нуля, и поэтому на него можно делить. Следовательно, мы действительно получили тело.

Построенное тело не коммутативно. Например, $(i, 0)(0, 1) = (0 - 0, i + 0) = (0, i)$, а $(0, 1)(i, 0) = (0 - 0, 0 + (-i)) = (0, -i)$.

5. Ассоциативность и дистрибутивность следуют из того, что произведение двух и большего числа сомножителей равно нулю.

1.2

1. Поскольку речь идет о числах, то необходимость в доказательстве тождеств отпадает. Используя свойства целых чисел, получаем: $(a + bi) + (c + di) = (a + c) + (b + d)i$, $1 = 1 + 0 \cdot i$, $-(a + bi) = (-a) + (-b)i$ и $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$. Следовательно, комплексные числа $a + bi$ с целой вещественной и мнимой частью образуют кольцо.

Для упрощения выкладок заметим, что $\varphi(a + bi)$ совпадает с квадратом модуля комплексного числа $a + bi$, в силу чего значение функции φ, соответствующее произведению, равно произведению ее значений, соответствующих сомножителям. Рассмотрим сначала случай, когда делитель — положительное целое число N (равное $N + 0 \cdot i$). Выберем из заданного кольца произвольный элемент $u + vi$. Разделим на N вещественную часть u и мнимую часть v. Чтобы избавиться от слишком больших остатков от деления, видоизменим несколько процедуру деления. Если остаток от деления больше $N/2$, то увеличим частное на 1 и получим остаток, заключенный между $-N/2$ и $+N/2$. Итак, для u найдутся целые числа p и r, а для v — целые числа q и s, удовлетворяющие соотношениям $u = pN + r$ и $v = qN + s$, причем оба числа r и s заключены между $-N/2$ и $N/2$ (то есть, если x — любое из чисел r и s, то $-N/2 \leqslant x \leqslant N/2$) и

$$u + vi = (pN + r) + (qN + s)i =$$
$$= (pN + qNi) + (r + si) =$$
$$= (p + qi)N + (r + si).$$

Комплексное число $u + vi$ уже представлено в требуемом виде. Необходимо лишь доказать соответствующее неравенство:

$$\varphi(r+si)=r^2+s^2\leqslant\left(\frac{N}{2}\right)^2+\left(\frac{N}{2}\right)^2=$$

$$=\frac{N^2}{2}<N^2=N^2+0^2=\varphi(N).$$

На этом рассмотрение первого случая завершается.

Пусть теперь $a+bi$ и $c+di$ — произвольные элементы кольца, а $c+di$, кроме того, отличен от нуля. Тогда $(c+di)(c-di)=c^2+d^2=N$ — положительное целое число и $u+vi=(a+bi)(c-di)$ — элемент кольца. По доказанному выше, существуют элементы $p+qi$ и $r+si$ кольца, удовлетворяющие соотношению

$$u+vi=(p+qi)N+(r+si).$$

Это означает, что

$$(a+bi)(c-di)=$$
$$=(p+qi)(c+di)(c-di)+$$
$$+(r+si).$$

Поскольку левая часть равенства и первое слагаемое в правой части равенства делятся на $c-di$, то и второе слагаемое в правой части также делится на $c-di$, то есть его можно представить в виде $r+si=(x+yi)(c-di)$, где $x+yi$ — некоторый элемент кольца. Подставляя это выражение в равенство и сокращая обе части на отличное от нуля комплексное число, получаем:

$$a+bi=(p+qi)(c+di)+(x+yi).$$

Так как $\varphi(c-di)=N$, то

$$N^2>\varphi(r+si)=\varphi(x+yi)\varphi(c-di)=$$
$$=\varphi(x+yi)N.$$

Разделив обе части неравенства $N^2>\varphi(x+yi)N$ на N, приходим к окончательному результату: $\varphi(x+yi)<N=\varphi(c+di)$.

2. Поскольку многочлены с рациональными коэффициентами образуют область целостности, то необходимость в проверке тождеств отпадает. Остальная часть первого утверждения доказывается так же, как в решении предыдущей задачи.

Переходим ко второму утверждению. Требуется доказать, что многочлен $2x\cdot f(x)+x^2\cdot g(x)$ (где $f(x)$ и $g(x)$ — многочлены с целочисленными коэффициентами) не может быть наибольшим общим делителем многочленов $2x$ и x^2. Поскольку оба многочлена $2x$ и x^2 кратны многочлену x, то их наибольший общий делитель (если его можно представить в указанном выше виде) также кратен многочлену x. Запишем его в виде многочлена $x\cdot d(x)$. Если это — общий делитель многочленов $2x$ и x^2, то найдутся такие многочлены $u(x)$ и $v(x)$ с целочисленными коэффициентами, что $2x=x\cdot d(x)u(x)$ и $x^2=x\cdot d(x)v(x)$, или после сокращения $2=d(x)u(x)$ и $x=d(x)v(x)$. Из первого равенства видно, что многочлен $d(x)$ может быть только постоянной, а из второго равенства коэффициент при его старшем члене равен 1 или -1. Число -1 является единицей, поэтому можно предположить, что $d(x)=1$. Тогда $2x\cdot f(x)+x^2\cdot g(x)=x$, или после сокращения $2f(x)+x\cdot g(x)=1$. Ясно, что последнее равенство выполняться не может, так как свободный член первого слагаемого в его левой части четен (так как равен удвоенному свободному члену многочлена $f(x)$), а свободный член второго слагаемого равен нулю, и их сумма никак не может быть равной единице.

Из приведенного решения видно, что кольцо многочленов с целочисленными коэффициентами не может быть евклидовым кольцом, поскольку в нем «кое-чего» недостает для этого. Тем не менее элементы кольца допускают однозначное разложение на простые множители. Доказательство этого утверждения чрезвычайно громоздко и основано на использовании большого числа лемм, поэтому мы не будем приводить его здесь. Но метод доказательства (применимый не только к рассматриваемому, но и ко многим другим кольцам) заслуживает того, чтобы сказать о нем несколько слов.

Если элементы области целостнос-

ти допускают однозначное разложение на простые множители и выполняется специальное условие (кольцо должно быть нетеровым), то построив кольцо, элементами которого являются многочлены с коэффициентами из заданного кольца, мы опять получим нетерово кольцо, и его элементы будут допускать однозначное разложение на простые множители. Можно показать, что всякое евклидово кольцо является нетеровым. Следовательно, кольцо многочленов с коэффициентами из евклидова кольца также принадлежит к числу нетеровых. Тот же метод позволяет доказать, что в кольце многочленов от любого числа переменных с коэффициентами из евклидова кольца все элементы допускают однозначное разложение на простые множители.

3. Доказать, что числа $a \pm b\sqrt{-5}$ с целыми a и b образуют область целостности, можно так же, как в предыдущих задачах. Но для доказательства остальных утверждений необходимы новые соображения.

Предположим, что $a + b\sqrt{-5}$ — делитель числа $c \pm d\sqrt{-5}$. Это означает, что существует число $x \pm y\sqrt{-5}$, удовлетворяющее равенству $(a \pm b\sqrt{-5})(x \pm y\sqrt{-5}) = c \pm d\sqrt{-5}$. Модули чисел $a \pm b\sqrt{-5}$, $x \pm y\sqrt{-5}$ и $c \pm d\sqrt{-5}$ связаны между собой соотношением $(a^2 \pm 5b^2)(x^2 \pm 5y^2) = c^2 + 5d^2$. Так как все три модуля — целые числа, то отсюда следует, что $a^2 \pm 5b^2$ делит число $c^2 \pm 5d^2$. Число $a^2 \pm 5b^2$ называется *нормой* числа $a + b\sqrt{-5}$. Понятие нормы позволяет сформулировать полученный результат следующим образом: *если в заданном кольце чисел одно число делит другое, то норма делимого кратна норме делителя.* Полученный результат будет неоднократно использоваться в дальнейшем, поскольку он позволяет свести делимость элементов к делимости их норм.

Число $a \pm b\sqrt{-5}$ может быть делителем числа 2 в том и только в том случае, если $a^2 \pm 5b^2$ делит $2^2 = 4$. Аналогичное утверждение справедливо и относительно числа $1 \pm \sqrt{-5}$: число $a \pm b\sqrt{-5}$ делит его в том и только в том случае, если $a^2 + 5b^2$ делит $1^2 + 5 \cdot 1^2 = 6$. Поскольку наибольший общий делитель чисел 4 и 6 равен 2, то рассматривать необходимо только делители числа 2. Число $a^2 \pm 5b^2$ неотрицательно и поэтому равно либо 1, либо 2. При $b \neq 0$ число $a^2 \pm 5b^2$ не может быть меньше 5. Следовательно, $b = 0$. Так как квадрат целого числа не равен 2, то $a^2 = 1$. Будем считать, что $a = \pm 1$. Тогда наибольший общий делитель двух чисел 2 и $1 \pm \sqrt{-5}$ равен 1 (другой общий делитель равен -1). Предположим теперь, что

$$2(a + b\sqrt{-5}) + (1 \pm \sqrt{-5})(c + d\sqrt{-5}) = 1.$$

Раскрывая скобки и группируя члены, содержащие и не содержащие $\sqrt{-5}$, преобразуем равенство к виду

$$(2a + c \pm 5d) + (2b \pm c + d)\sqrt{-5} = 1,$$

откуда

$$2a \pm c + 5d = 1, \quad 2b \pm c + d = 0.$$

Вычитая из первого равенства второе, получаем

$$2a - 2b \pm 4d = 1,$$

что невозможно, так как единица — нечетное число.

Для доказательства неразложимости чисел 2 и $1 \pm \sqrt{-5}$ в кольце чисел $a \pm b\sqrt{-5}$ с целыми a и b воспользуемся тем же приемом. Однако на этот раз недостаточно ограничиться делителями числа 2, а придется рассмотреть делители чисел 4 и 6. Поскольку в дальнейшем нам понадобится доказать неразложимость чисел 3 и $1 - \sqrt{-5}$, рассмотрим также делители числа $3^2 = 9$. (При доказательстве неразложимости

числа $1 - \sqrt{-5}$ речь опять пойдет о делителях числа 6.) Нас будут интересовать только положительные делители: 1, 2, 3, 4, 6 и 9. Так как число -1 — единица кольца, то можно считать, что рассмотрению подлежат только делители вида $a + b\sqrt{-5}$ с $a > 0$. Если $b \geqslant 2$, то $a^2 + 5b^2 \geqslant 2$, и мы заключаем, что либо $b = 1$, либо $b = 0$. Если $b = 1$, то число $a^2 \mp 5$ может быть равно 9 (при $a = 2$) и 6 (при $a = 1$). Если же $b = 0$, то число $a^2 \mp 5$ может быть равно 9 (при $a = 3$), 4 (при $a = 2$) и 1 (при $a = 1$).

Поскольку норма произведения равна произведению норм сомножителей, то одно из двух равных по норме чисел делит другое лишь в том случае, если норма частного равна 1. Как показано выше, так бывает только в том случае, если частное равно $+1$ или -1, то есть если два числа совпадают или одно из них равно другому, взятому со знаком минус. Таким образом, из полученных выше чисел $2 \mp \sqrt{-5}$, $2 - \sqrt{-5}$, $1 \mp \sqrt{-5}$, $1 - \sqrt{-5}$, 3, 2 и 1 первые два не делят ни одно из заданных чисел, а все остальные (кроме 1) делят только себя. Следовательно, все эти числа неразложимы.

Доказательство того, что ни одно из чисел 2 и $1 \mp \sqrt{-5}$ не простое, проводится так же, как доказательство неразложимости, и сводится к несложным выкладкам.

2.1

1. Предположим, что (a, b, c, d) и (x, y, u, v) — четверки чисел, удовлетворяющие обоим соотношениям. Тогда $2(a + x) - 3(b + y) + 5(c + u) + (d + v) = (2a - 3b + 5c + d) + (2x - 3y + 5u + v) = 0 + 0 = 0$ и $-3(a + x) + 2(b + y) + (d + v) = (-3a + 2b + c) + (-3x + 2y + v) = 0 + 0 = 0$. Кроме того, $2(tx) - 3(ty) + 5(tu) + (tv) = t(2x - 3y + 5u + v) = t \cdot 0 = 0$ и $-3(tx) + 2(ty) + tv = t(-3x + 2y + v) = t \cdot 0 = 0$ при любом t. Следовательно, четверки чисел, удовлетворяющие двум приведенным в условиях задачи соотношениям, образуют подпространство в векторном пространстве всех четверок чисел.

2. Если $a_1, a_2, \ldots, a_n, \ldots$ — ограниченная последовательность, то существует такое вещественное число A, что при любом i выполняется неравенство $-A < a_i < A$. Пусть $b_1, b_2, \ldots, b_n, \ldots$ — другая ограниченная последовательность, члены которой по абсолютной величине меньше вещественного числа B, то есть при любом i удовлетворяют неравенству $-B < b_i < B$. Сумма двух последовательностей также принадлежит к числу ограниченных последовательностей, поскольку $-(A + B) < a_i + b_i < A + B$. Если все члены первой последовательности умножить на вещественное число c, то верхней гранью для членов последовательности будет число cA вместо прежней верхней грани A (если число c отрицательно, то верхней гранью будет число $-cA$; при $c = 0$ верхней гранью может служить любое положительное число, например 1).

3. Прежде всего необходимо доказать, что последовательности, у которых ограничена сумма квадратов их членов, являются ограниченными последовательностями. Пусть $a_1, a_2, \ldots, a_n, \ldots$ — одна из таких последовательностей и сумма квадратов любого числа ее членов меньше числа A (которое поэтому может быть только положительным). Выбрав любой из членов последовательности, получим: $a_i^2 < A$, то есть $-\sqrt{A} < a_i < \sqrt{A}$.

Ясно, что верхней гранью для суммы квадратов членов последовательности $ca_1, ca_2, \ldots, ca_n, \ldots$ служит число c^2A.

Найдем верхнюю грань, соответствующую сумме двух последовательностей: $a_1, a_2, \ldots, a_n, \ldots$ с верхней гранью для суммы квадратов ее членов, равной A, и $b_1, b_2, \ldots, b_n, \ldots$ с верхней гранью для суммы квадратов ее членов, равной B. Суммой двух последовательностей является после-

довательность $a_1 + b_1$, $a_2 + b_2$, ..., $a_n + b_n$, ... Выбрав любое число членов этой последовательности, образуем сумму их квадратов. Если n — номер последнего из отобранных членов, то удобнее рассматривать сумму квадратов n первых членов последовательности $(a_1 + b_1)^2 + (a_2 + b_2)^2 + \ldots + (a_n + b_n)^2$. Если бы квадрат суммы был равен сумме квадратов, то верхней гранью для $(a_1 + b_1)^2 + (a_2 + b_2)^2 + \ldots + (a_n + b_n)^2$ было бы число $A + B$. Но число $a^2 + b^2$ не может быть верхней гранью для $(a + b)^2$. Однако нетрудно показать, что число $2(a^2 + b^2)$ всегда больше (или равно) квадрата суммы $(a + b)^2$. Действительно, вычитая из первого числа второе, получаем: $2(a^2 + b^2) - (a + b)^2 = 2a^2 + 2b^2 - a^2 - 2ab - b^2 = a^2 - 2ab + b^2 = (a - b)^2$. Число $(a - b)^2$ как квадрат вещественного числа не может быть отрицательным. Следовательно, для суммы двух последовательностей сумма квадратов любого числа ее членов ограничена сверху, например, числом $2(A + B)$.

Последовательности с ограниченными суммами квадратов их членов играют важную роль в математическом анализе.

Для тех, кто знаком с понятием сходимости, заметим следующее. Последовательности каждого из перечисленных ниже типов образуют подпространство в векторных пространствах последовательностей пяти остальных типов:

а) вещественные последовательности;

б) ограниченные последовательности;

в) сходящиеся последовательности;

г) последовательности, сходящиеся к нулю;

д) последовательности с ограниченной суммой квадратов их членов;

е) последовательности, все члены которых, начиная с какого-то номера, равны нулю.

4. Утверждение следует из того, что, если многочлен умножить на число или взять сумму двух многочленов, то многочлен, который при этом получается, содержит не больше переменных, чем исходные многочлены.

5. Утверждение следует из того, что при умножении на число степень многочлена не возрастает, а степень суммы двух многочленов не выше большей из степеней слагаемых.

6. Требуется доказать, что, если многочлен $a_1x_1 + a_2x_2 + \ldots + a_nx_n$ имеет корнями n каких-то чисел, то те же числа будут корнями многочлена $(ta_1)x_1 + (ta_2)x_2 + \ldots + (ta_n)x_n$ (t — произвольное вещественное число), и если многочлены $a_1x_1 + a_2x_2 + \ldots + a_nx_n$ и $b_1x_1 + b_2x_2 + \ldots + b_nx_n$ обладают одинаковым набором n корней, то те же n чисел являются корнями многочлена $(a_1 + b_1)x_1 + (a_2 + b_2)x_2 + \ldots + (a_n + b_n)x_n$ (a_i и b_i — заданные вещественные числа). Доказательство достаточно провести для какого-нибудь одного набора из n корней, так как ни один набор не выделен. Пусть $c_1, c_2, \ldots, c_n$ — набор из n чисел, обращающих в нуль заданные многочлены. Тогда

$$(ta_1)c_1 + (ta_2)c_2 + \cdots + (ta_n)c_n = t(a_1c_1 + a_2c_2 + \cdots + a_nc_n) = t \cdot 0 = 0$$

и

$$(a_1 + b_1)c_1 + (a_2 + b_2)c_2 + \cdots \ldots (a_n + b_n)c_n = (a_1c_1 + a_2c_2 + \cdots + a_nc_n) + (b_1c_1 + b_2c_2 + \cdots + b_nc_n) = 0 + 0 = 0.$$

2.2

1. Выясним, что можно сказать в каждом случае о размерности векторного пространства. Для краткости условимся обозначать размерность dim.

а) Если в векторном пространстве не существует линейно независимой системы из k элементов, то образуем линейно независимую систему, вклю-

чив в нее максимально возможное число элементов (некоторое число линейно независимых элементов в векторном пространстве заведомо существует: их больше нуля и меньше k). Пусть $u_1, u_2, \ldots, u_m$ — линейно независимая система, содержащая максимальное число элементов. Мы знаем, во-первых, что $m < k$, и, во-вторых, что любая система из $m + 1$ элементов линейно зависима (так как m — наибольшее число элементов в линейно независимой системе). Следовательно, при любом векторе v система векторов $v, u_1, u_2, \ldots, u_m$ линейно зависима. Это возможно лишь в том случае, если вектор v линейно зависит от векторов $u_1, u_2, \ldots, u_m$. Так как v — произвольный элемент векторного пространства, то $u_1, u_2, \ldots, u_m$ — система образующих и, поскольку она линейно независима, базис векторного пространства. Следовательно, $\dim < k$. Справедливо и обратное утверждение: если $\dim < k$, то любая система из k элементов линейно зависима, в противном случае система образующих не могла бы состоять менее чем из k элементов.

б) Если в векторном пространстве ни при каком n не существует базиса из n элементов, то векторное пространство бесконечномерно. Если же при каком-то n существует базис из n элементов, то $n \geqslant k$, так как базис является системой образующих. Следовательно, неравенство $n \geqslant k$ выполняется во всех случаях. Справедливо и обратное утверждение. Если в векторном пространстве при каком-то n существует базис из n элементов и $n \geqslant k$, то существует линейно независимая система из k элементов (например, если из базиса вычеркнуть $n - k$ векторов, то оставшиеся k векторов образуют такую систему). Если же в векторном пространстве ни при каком n не существует базиса из n элементов, то при любом k в нем существует линейно независимая система из k векторов. Действительно, если бы в векторном пространстве при каком-нибудь k не существовала линейно независимая система из k векторов, то по доказанному в п. (а), это означало бы, что при каком-то $m < k$ существует базис из m элементов.

в) По доказаниому в п. (б) размерность векторного пространства в этом случае удовлетворяет неравенству $\dim \geqslant k$. По доказанному в п. (а) должно выполняться неравенство $\dim < k + 1$. Следовательно, остается единственная возможность: $\dim = k$. Разумеется, в этом случае элементы базиса из k векторов составляют линейно независимую систему из k векторов, а поскольку базис является системой образующих, то линейно независимая система из $k + 1$ векторов не существует.

г) Так же как и в предыдущем случае, можно доказать, что $\dim = k$.

д) Если в векторном пространстве ни при каком n не существует базиса из n векторов, то векторное пространство бесконечномерно. Если же при каком-то n в векторном пространстве существует базис из n элементов, то должно выполняться неравенство $n > k$. В противном случае, дополнив базис соответствующим числом элементов, мы получили бы систему из k векторов, а поскольку базис является системой образующих, то и новая система также была бы системой образующих, что по условиям задачи невозможно. Это означает, что $\dim > k$. Наоборот, если $\dim > k$ и существует базис из n элементов (то есть $\dim = n$), то система образующих из k элементов существовать не может, так как векторы базиса линейно независимы. В п. (е) мы покажем, что, если система образующих из k элементов не существует, то при некотором n существует базис из n элементов. Поэтому, если в векторном пространстве базис из n элементов не существует ни при каком n (то есть если векторное пространство бесконечномерно), то в нем не может существовать система образующих из k элементов.

е) Если в векторном пространстве существует система образующих из k

элементов, то, как было показано выше, вычеркнув из нее некоторое (может быть, равное нулю) число векторов, мы получим базис. Следовательно, в этом случае $\dim \leqslant k$. Наоборот, если $\dim \leqslant k$, то, приписав к любому базису (который одновременно является системой образующих) соответствующее число векторов, мы получим систему из k элементов. Поскольку новая система содержит систему образующих, то она также является системой образующих.

ж) По доказанному в п. (е) $\dim \leqslant k$, а по доказанному в п. (д) $\dim > k-1$. Этим неравенствам удовлетворяет только $\dim = k$. Наоборот, при $\dim = k$ любой базис является системой образующих из k элементов, а поскольку векторы базиса линейно независимы, то в этом случае в векторном пространстве не существует системы образующих из $k-1$ элементов.

з) Векторное пространство k-мерно. Доказать это можно так же, как в предыдущем случае.

Расположим все рассмотренные нами случаи в порядке возрастания размерности векторного пространства. У нас получится следующая последовательность:

1) $\dim < k$ — п. (а);
2) $\dim \leqslant k$ — п. (е) и (л);
3) $\dim = k$ — п. (в), (г), (ж), (з) и (к);
4) $\dim \geqslant k$ — п. (б) и (и);
5) $\dim > k$ — п. (д).

Любое из условий (2) [п. (е) и (л)] следует из условия (1) [п. (а)] (если одно число меньше другого, то оно не больше другого). Точно так же из условия (5) [п. (д)] следует любое из условий (4) [п. (б) и (и)]. Кроме того, любое из условий (3) влечет за собой каждое из условий (2) и (4) (если одно число равно другому, то оно не меньше и не больше другого). Наконец, интересно отметить, что, если любое из условий (2) дополнить любым из условий (4), то из их совокупности будет следовать любое из условий (3) (если одно число не больше и не меньше другого, то оно равно другому числу). В частности, если в векторном пространстве при некотором k существует линейно независимая система из k векторов и образующая система из k элементов, то должен существовать и базис из k векторов. (Более того, исходя из условий (2) и (3), можно показать, что и линейно независимая система из k векторов, и система из k образующих являются в этом случае базисами векторного пространства.)

2. Утверждение доказано дважды: при рассмотрении векторных пространств и в решении предыдущей задачи. Было показано, что, если из системы образующих вычеркивать элементы до тех пор, пока суженная система остается системой образующих, то последняя из полученных таким способом систем образующих будет линейно независимой.

3. По существу для доказательства утверждения достаточно воспользоваться тем, что в векторном пространстве существует система образующих.

Выберем в векторном пространстве любую линейно независимую систему и начнем дополнять ее векторами, следя за тем, чтобы после присоединения очередного вектора расширенная система оставалась линейно независимой. Будем расширять систему до тех пор, пока это возможно. После конечного числа шагов процесс оборвется, так как в векторном пространстве с системой образующих из n элементов ни одна линейно независимая система не может содержать более чем n векторов. Если $u_1, u_2, \ldots, u_k$—максимальная линейно независимая система векторов, то, присоединив к ней любой вектор v, мы получим линейно зависимую систему $u_1, u_2, \ldots, u_k, v$. Следовательно, существует нетривиальная линейная комбинация векторов $u_1, u_2, \ldots, u_k, v$, равная нулевому вектору. В этой линейной комбинации коэффициент при векторе v не может быть равен нулю, поскольку в противном случае

векторы $u_1, u_2, \ldots, u_k$ вопреки предположению были бы линейно зависимыми. Следовательно, вектор v линейно зависит от векторов $u_1, u_2, \ldots, u_k$. Поскольку v — произвольный элемент векторного пространства, то $u_1, u_2, \ldots, u_k$ — система образующих, а значит, и базис, так как векторы $u_1, u_2, \ldots, u_k$ линейно независимы.

4. Доказательство проводится так же, как в предыдущей задаче, только векторы линейно независимой системы взяты из системы образующих. Решение предыдущей задачи позволяет утверждать, что в векторном пространстве существует линейно независимая система векторов, которая включает в себя исходную линейно независимую систему, содержится в системе образующих и обладает тем свойством, что любой элемент системы образующих линейно зависит от ее векторов. По свойству (в) линейной зависимости отсюда следует, что каждый элемент векторного пространства линейно зависит от векторов этой системы. Следовательно, она является базисом векторного пространства.

2.3

1. Доказательство этого утверждения было приведено, когда мы показали, что размерности изоморфных векторных пространств совпадают.

2. Предположим, что φ переводит линейно независимую систему векторов в линейно независимую систему. Поскольку любой (отличный от нулевого) вектор линейно не зависит от самого себя (только в тривиальной линейной комбинации обращается в нулевой вектор), то его образ при отображении φ не может совпадать с нулевым вектором, поскольку нулевой вектор линейно зависим (существует нетривиальная линейная комбинация, переводящая нулевой вектор в нулевой вектор, например $1 \cdot 0 = 0$, где скаляр при нулевом векторе отличен от нуля). Таким образом, если $\varphi(u) = \varphi(v)$, то (поскольку φ сохраняет операции) $\varphi(u - v) = \varphi(u) - \varphi(v)$ совпадает с нулевым вектором, и поэтому $u - v = 0$, или $u = v$. Наоборот, предположим, что образы различных векторов при отображении φ различны, и рассмотрим систему линейно независимых векторов $u_1, u_2, \ldots, u_n$. Рассмотрим образ такой линейной комбинации этих векторов, которую отображение φ переводит в нулевой вектор:

$$\alpha_1\varphi(u_1) + \alpha_2\varphi(u_2) + \cdots + \alpha_n\varphi(u_n) = 0.$$

Так как φ сохраняет операции, то

$$\varphi(\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n) = 0.$$

Поскольку нулевой вектор может быть образом только нулевого вектора и по условию образы различных векторов не совпадают, то это означает, что $\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_n u_n = 0$. Но векторы $u_1, u_2, \ldots, u_n$ — линейно независимы, поэтому все скаляры $\alpha_1, \alpha_2, \ldots, \alpha_n$ равны нулю. Следовательно, образы векторов $u_1, u_2, \ldots, u_n$ при отображении φ — векторы $\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)$ — линейно независимы.

Таким образом, отображение φ переводит линейно независимую систему векторов в линейно независимую систему в том и только в том случае, если образы различных элементов не совпадают.

Предположим теперь, что отображение φ переводит систему образующих в систему образующих. Прежде всего заметим, что система образующих существует в любом векторном пространстве. Но все элементы системы образующих порождают векторное пространство и поэтому не могут принадлежать ни одному истинному подпространству.

Пусть φ отображает векторное пространство M_1 в векторное пространство M_2. Выберем в векторном пространстве M_2 произвольный элемент, а в векторном пространстве M_1 систему образующих, элементы которой обозначим u_i. (Мы не выпи-

сываем все образующие по порядку, поскольку не известно, конечно ли их число и можно ли выписать их все подряд.) Отображение φ переводит систему образующих u_i векторного пространства M_1 в систему образующих $\varphi(u_i)$ векторного пространства M_2. Следовательно, вектор $v \in M_2$ можно представить в виде линейной комбинации *конечного числа* векторов $\varphi(u_i)$ (обозначенных так, чтобы индексы векторов u_i шли по порядку):

$$v = \alpha_1\varphi(u_1) + \alpha_2\varphi(u_2) + \cdots + \alpha_n\varphi(u_n) = \varphi(\alpha_1u_1 + \alpha_2u_2 + \cdots + \alpha_nu_n)$$

(переход от линейной комбинации образов к образу линейной комбинации возможен потому, что отображение φ сохраняет операции сложения и умножения на скаляр). Полученный результат показывает, что вектор v является образом некоторого вектора из пространства M_1. Выберем в векторном пространстве M_1 систему образующих, элементы которой обозначим u_i. Требуется доказать, что элементы $\varphi(u_i)$ составляют систему образующих векторного пространства M_2. Рассмотрим произвольный вектор v из векторного пространства M_2. По предположению, этот вектор имеет прообраз в векторном пространстве M_1, то есть его можно представить в виде $v = \varphi(u)$. Так как u_i — элементы системы образующих в векторном пространстве M_1, то поэтому вектор u из M_1 можно представить в виде линейной комбинации конечного числа векторов u, то есть

$$u = \alpha_1u_1 + \alpha_2u_2 + \ldots + \alpha_nu_n,$$

откуда

$$v = \varphi(u) = \varphi(\alpha_1u_1 + \alpha_2u_2 + \cdots + \alpha_nu_n) = \alpha_1\varphi(u_1) + \alpha_2\varphi(u_2) + \cdots + \alpha_n\varphi(u_n).$$

Следовательно, вектор v можно представить в виде линейной комбинации векторов $\varphi(u_1)$, $\varphi(u_2)$, ..., $\varphi(u_n)$, то есть векторы $\varphi(u_i)$ — элементы системы образующих в векторном пространстве M_2.

(Другое доказательство см. в решении задачи 2.)

4. Разумно доказать утверждение для внутренней прямой суммы. Пусть $M = U + V$ — внутренняя прямая сумма. Требуется доказать, что, объединив линейно независимую систему векторов в подпространстве U с линейно независимой системой векторов в подпространстве V, мы получим линейно независимую систему векторов во всем векторном пространстве M, а объединив систему образующих в подпространстве U с системой образующих в подпространстве V, мы получим систему образующих во всем векторном пространстве M. Следовательно, аналогичное утверждение справедливо и относительно базисов: объединив базисы в подпространствах U и V, мы получим базис во всем векторном пространстве M. Это и означает, что размерность прямой суммы совпадает с суммой размерностей соответствующих подпространств.

Итак, пусть $u_1, u_2, \ldots, u_n$ — линейно независимая система векторов в подпространстве U, а $v_1, v_2, \ldots, v_k$ — линейно независимая система векторов в подпространстве V.

Предположим, что некоторая линейная комбинация векторов $u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_k$ равна нулевому вектору:

$$\alpha_1u_1 + \alpha_2u_2 + \cdots + \alpha_nu_n + \beta_1v_1 + \beta_2v_2 + \cdots + \beta_kv_k = 0.$$

Сумма первых n членов в левой части равна некоторому вектору u из подпространства U, а сумма n следующих членов равна некоторому вектору v из подпространства V (поскольку подпространства замкнуты относительно сложения и умножения на скаляр). Преобразуем линейную комбинацию $u + v = 0$ к виду $v = -u$, где $v \in V$ и $-u \in U$. Поскольку подпространства U и V не имеют других общих элементов, кроме ну-

левого вектора, то $u = 0$ и $v = 0$, или

$$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n = 0$$

и

$$\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_k v_k = 0.$$

Так как $u_1, u_2, \ldots, u_n$ и $v_1, v_2, \ldots, v_k$ — линейно независимые системы векторов, то обе линейные комбинации тривиальны (иначе говоря, все скаляры $\alpha_1, \alpha_2, \ldots, \alpha_n$ и $\beta_1, \beta_2, \ldots, \beta_k$ равны нулю). Тем самым линейная независимость «объединенной» системы векторов $u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_k$ доказана.

Предположим теперь, что $u_1, u_2, \ldots, u_p$ и $v_1, v_2, \ldots, v_q$ — системы образующих в подпространствах U и V. Поскольку эти два подпространства порождают все векторное пространство, то любой вектор из M можно представить в виде $u' + v'$, где $u' \in U$ и $v' \in V$. В каждом из подпространств U и V система образующих известна, поэтому при надлежащим образом выбранных скалярах векторы u' и v' можно представить в виде

$$u' = \gamma_1 u_1 + \gamma_2 u_2 + \cdots + \gamma_p u_p \text{ и}$$

$$v' = \delta_1 v_1 + \delta_2 v_2 + \cdots + \delta_q v_q.$$

Следовательно, сумма $u' + v'$ представима в виде линейной комбинации

$$u' + v' = \gamma_1 u_1 + \gamma_2 u_2 + \cdots + \gamma_p u_p + \delta_1 v_1 + \delta_2 v_2 + \cdots + \delta_q v_q.$$

Таким образом, объединив системы образующих в подпространствах U и V, мы действительно получили систему образующих во всем векторном пространстве.

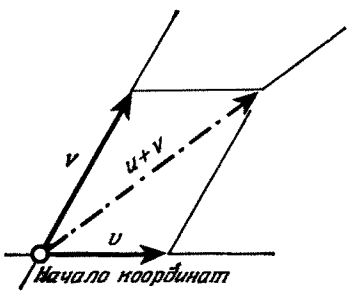


Рис. 115.

5. Чем более простым окажется наш пример, тем лучше. Разумеется, в простейшем (но не вырожденном) случае каждое из подпространств должно быть одномерным. Прямая сумма двух одномерных подпространств двумерна и, если скаляры брать из тела вещественных чисел, представляет собой плоскость в векторном пространстве. Выберем в этой плоскости два вектора u и v так, чтобы они не были параллельными. Рассмотрим любую линейную комбинацию векторов u и v, не параллельную ни одному из них, например, вектор $u + v$ (рис. 115). Ясно, что любые два из подпространств $\{u\}$, $\{v\}$ и $\{u + v\}$ не имеют общих элементов, кроме нулевого вектора, и что, кроме того, любые два из этих трех подпространств порождают всю плоскость.

Эта задача показывает, что прямую сумму нескольких подпространств было бы неудобно определить как объединение подпространств, из которых любые два не имеют общих элементов, кроме нулевого вектора. Если прямая сумма внешняя, то никаких затруднений не возникает: ее можно определить, взяв n векторных пространств (над одним и тем же телом) и образовав наборы из n элементов, i-я компонента которых является элементом i-го векторного пространства. Задав на множестве этих наборов операции, состоящие в покомпонентном сложении и умножении на скаляры (элементы тела), мы получим векторное пространство — внешнюю прямую сумму n выбранных нами векторных пространств. Если бы мы попытались перенести эту схему на внутреннюю прямую сумму, то понадобилось бы ввести дополнительное предположение о том, что заданные подпространства вместе порождают все векторное пространство и из них нельзя выбрать ни одно подпространство, которое имело бы не только с остальными под-

пространствами, но и с подпространствами, порожденными остальными подпространствами, какие-нибудь общие элементы, кроме нулевого вектора. Например, в трехмерном пространстве любые три не лежащие в одной плоскости вектора порождают подпространства, прямая сумма которых совпадает со всем пространством.

Нетрудно видеть, что, если векторное пространство раэлагается в прямую сумму подпространств, то это означает следующее: любой вектор пространства можно представить, причем однозначно, в виде суммы векторов, принадлежащих подпространствам-слагаемым.

2.4

1. Определив на множестве пар операцию сложения, как покомпонентное сложение, мы заведомо получим коммутативную группу, поскольку множество пар с такой операцией представляет собой не что иное, как прямое произведение двух коммутативных групп. Умножение на элемент γ кольца R удобно задать следующим образом: $\gamma(\alpha, \beta) = (\gamma\alpha, \gamma\beta)$ и $(\alpha, \beta)\gamma = (\alpha\gamma, \beta\gamma)$. Нетрудно проверить, что при этом выполняются все тождества как для левого, так и для правого модуля. Кроме того, справедливо тождество $(\alpha u)\beta = \alpha(u\beta)$, где α и β — элементы кольца, а u — элемент модуля. Если для модуля, который является левым и правым модулем (над одним и тем же кольцом), выполняется еще и это тождество, то он называется двусторонним модулем.

2. Пример такого модуля можно построить, если воспользоваться решением предыдущей задачи. Построенный модуль будет двусторонним модулем в смысле определения, приведенного в конце решения, но нам это понятие не понадобится.

Рассмотрим некоммутативное кольцо с единицей. Так же как в решении предыдущей задачи, построим модуль из пар (α, β) элементов этого кольца. Выберем элемент $(1, \gamma)$, где 1 — единичный, а γ — пока произвольный элемент кольца (условие, которому должен удовлетворять элемент γ, будет выведено чуть ниже). Умножив элемент $(1, \gamma)$ слева на элемент кольца α, получим элемент $(\alpha, \alpha\gamma)$, который будет «левым скалярным кратным» для элемента $(1, \gamma)$. Если элемент $(\alpha, \alpha\gamma)$ является «правым скалярным кратным» элемента $(1, \gamma)$, то его можно представить в виде $(1, \gamma)\beta = (\beta, \gamma\beta)$, где β — некоторый элемент кольца. Приравняв отдельно первые и вторые компоненты пар, получим: $\alpha = \beta$ и, следовательно, $\alpha\gamma = \gamma\beta = \gamma\alpha$. Таким образом, если элементы кольца α и γ выбраны так, что они не коммутируют, то элемент модуля $(\alpha, \alpha\gamma)$ будет левым скалярным кратным для элемента $(1, \gamma)$, но не будет правым скалярным кратным. Поскольку кольцо некоммутативно, то такие элементы α и γ всегда найдутся.

3.1

1. а) При отражении относительно начала координат все векторы переходят в противоположные. Следовательно, однородное линейное преобразование $\mathbf{A}$ в этом случае действует следующим образом: $\mathbf{A}(u) = -u$.

б) Если u — вектор, направленный вдоль прямой, то при отражении относительно прямой он переходит в себя, а все векторы, ортогональные прямой, переходят в противоположные векторы. Следовательно, если векторы v и w ортогональны вектору u и тройка векторов u, v и w порождает все векторное пространство (векторы u, v и w не лежат в одной плоскости), то $\mathbf{A}(u) = u$, $\mathbf{A}(v) = -v$, $\mathbf{A}(w) = -w$.

Это означает, что на произвольно выбранный вектор однородное линейное отображение действует следующим образом: $\mathbf{A}(\alpha u + \beta v + \gamma w) = \alpha u - \beta v - \gamma w$.

в) При отражении относительно плоскости π, проходящей через начало координат, все векторы, лежа-

щие в плоскости π, переходят в себя вместе с векторами u и v, порождающими π, а все векторы w, ортогональные плоскости π, переходят в противоположные. Следовательно, на произвольный вектор действует однородное линейное преобразование $A(\alpha u + \beta v + \gamma w) = \alpha u + \beta v - \gamma w$.

г) Однородное линейное преобразование, соответствующее ортогональной проекции на проходящую через начало координат плоскость π, можно построить так же, как в предыдущем случае — п. (в): если u и v — векторы, порождающие плоскость π, а w — вектор, ортогональный плоскости π, то на произвольный вектор действует однородное линейное преобразование $V(\alpha u + \beta v + \gamma w) = \alpha u + \beta v$.

д) Если u — вектор, направленный вдоль прямой, на которую производится ортогональное проектирование, v и w — векторы, ортогональные вектору u, и тройка векторов u, v и w порождает все векторное пространство, то $V(\alpha u + \beta v + \gamma w) = \alpha u$.

2. При нулевом отображении **O** все элементы векторного пространства переходят в нулевой вектор, поэтому $\mathrm{Ker}\,\mathbf{O}$ совпадает со всем векторным пространством, а $\mathrm{Im}\,\mathbf{O}$ состоит только из нулевого вектора. При тождественном отображении каждый элемент векторного пространства переходит в себя и ни один вектор, кроме нулевого, не переходит в нулевой вектор, поэтому $\mathrm{Ker}\,\mathbf{I} = \{0\}$, а $\mathrm{Im}\,\mathbf{I}$ совпадает со всем векторным пространством.

При отражении относительно начала координат и прямой, проходящей через начало координат, растяжении от центра, растяжении в направлении, перпендикулярном фиксированной прямой, проходящей через начало координат, поперечном сдвиге и повороте ни один вектор не переходит в нулевой вектор, кроме него самого. Следовательно, ядра всех этих линейных преобразований состоят только из нулевого вектора. Поскольку ядро как векторное пространство нульмерно, а сумма размерностей ядра и образа преобразования во всех перечисленных нами случаях равна 2, то размерность образа преобразования равна 2, то есть образом преобразования является вся плоскость.

При ортогональной проекции на прямую образ преобразования совпадает с прямой, на которую производится проектирование, а ядро преобразования — с перпендикулярной прямой.

Если от плоскости перейти к трехмерному пространству, то при отражениях относительно начала координат, а также прямой и плоскости, проходящих через начало координат, в нулевой вектор переходит только нулевой вектор, поэтому ядро преобразования состоит только из нулевого вектора. Поскольку сумма размерностей ядра и образа преобразования равна размерности всего векторного пространства, то образ преобразования трехмерен, а это означает, что он может совпадать только со всем векторным пространством.

При ортогональной проекции на плоскость π образом преобразования является плоскость π, а ядром — ортогональная ей прямая. При ортогональной проекции на прямую образом преобразования служит прямая, а ядром — ортогональная ей плоскость. (В обоих случаях сумма размерностей ядра и образа преобразования совпадает с размерностью всего пространства: $1 + 2 = 3$.)

3. а) Поскольку операции сохраняются, то их следует производить покомпонентно. Первой компонентой набора может быть любое вещественное число (если речь идет о наборах из n вещественных чисел), поэтому образ преобразования совпадает с телом всех вещественных чисел. Ядру преобразования принадлежат наборы, переходящие при преобразовании в вещественное число 0, то есть наборы, первая компонента которых равна 0.

б) Так как значение, принимае-

мое в точке $x = a$ суммой многочленов, совпадает с суммой значений, принимаемых в этой точке каждым слагаемым, а многочлен $c \cdot f(x)$ принимает значение $c \cdot f(a)$, то мы действительно получаем однородное линейное отображение. Поскольку многочлен, тождественно равный постоянной, принимает в точке $x = a$ значение, равное этой постоянной, и любому вещественному числу c можно поставить в соответствие многочлен, тождественно равный c, то образ рассматриваемого преобразования совпадает с телом всех вещественных чисел. Ядро преобразования состоит из многочленов, принимающих в точке $x = a$ значение $f(a) = 0$, то есть имеющих корень a.

в) Рассмотрим отображение, ставящее в соответствие комплексному числу $a + bi$ его мнимую часть (равную не bi, а вещественному числу b). Так как мнимая часть суммы комплексных чисел $(a + bi) + (c + di)$ совпадает с суммой мнимых частей слагаемых, а мнимая часть комплексного числа $c(a + bi)$ (c — любое вещественное число) равна умноженной на c мнимой части комплексного числа $a + bi$, то мы действительно получаем однородное линейное отображение (которое в данном случае является линейным преобразованием). Поскольку образом комплексного числа может быть любое вещественное число, то образ преобразования совпадает с телом всех вещественных чисел. Ядру преобразования принадлежат комплексные числа с мнимой частью, равной нулю, то есть опять-таки вещественные числа. Следовательно, ядро преобразования также совпадает с телом всех вещественных чисел. Таким образом, мы сталкиваемся с интересным случаем, когда ядро и образ преобразования совпадают.

3.2

1. По определению $(1 \cdot \mathbf{A})(u) = 1 \cdot (\mathbf{A}(u))$. По свойству векторных пространств $1 \cdot (\mathbf{A}(u))$ совпадает с $\mathbf{A}(u)$. Следовательно, линейные преобразования $1 \cdot \mathbf{A}$ и $\mathbf{A}$ переводят любой вектор u в один и тот же вектор, то есть равны.

2. Тождественное преобразование $\mathbf{I}$ отображает любой вектор u в себя, то есть $\mathbf{I}(u) = u$. Отсюда следует, что, во-первых, $\mathbf{A}(\mathbf{I}(u)) = \mathbf{A}(u)$ и, во-вторых (если вместо u в равенство $\mathbf{I}(u) = u$ подставить $\mathbf{A}(u)$), $\mathbf{I}(\mathbf{A}(u)) = \mathbf{A}(u)$. Полученные равенства обозначают, что $\mathbf{AI} = \mathbf{A}$ и $\mathbf{IA} = \mathbf{A}$, то есть что $\mathbf{I}$ — единичный элемент кольца линейных преобразований.

3. Если $\mathbf{BA} = \mathbf{I}$, то $\mathbf{B}(\mathbf{A}(u)) = \mathbf{I}(u) = u$ при любом векторе u. При $u \in \mathrm{Ker}\mathbf{A}$ и $\mathbf{A}(u) = 0$ получаем: $u = \mathbf{B}(\mathbf{A}(u)) = \mathbf{B}(0) = 0$, то есть ядро линейного преобразования $\mathbf{A}$ состоит только из нулевого вектора.

Если $\mathbf{AC} = \mathbf{I}$, то (поскольку $u = \mathbf{I}(u) = \mathbf{A}(\mathbf{C}(u))$) все элементы векторного пространства принадлежат образу линейного преобразования $\mathbf{A}$.

Так как сумма размерностей ядра и образа преобразования должна совпадать с размерностью векторного пространства, то в том случае, когда образ совпадает со всем векторным пространством, ядро преобразования состоит только из нулевого вектора. Поэтому условия (в) и (г) эквивалентны и каждое из них следует как из условия (а), так и из условия (б).

Если выполняется одно из условий (г) и (д), то выполняется и другое условие. Следовательно, каждый элемент векторного пространства допускает однозначное представление в виде $\mathbf{A}(u)$. Поэтому поставив вектору $\mathbf{A}(u)$ в соответствие вектор u, мы получим однозначно определенное отображение. Так как $\mathbf{A}(u) + \mathbf{A}(v) = \mathbf{A}(u + v)$ и $\alpha\mathbf{A}(u) = \mathbf{A}(\alpha u)$, то это соответствие сохраняет операции сложения и умножения на скаляры. Однородное линейное отображение $\mathbf{BA} : (u) \to u$ удовлетворяет соотношению $\mathbf{BA} = \mathbf{I}$ (так как $\mathbf{BA}(u) = u$). Кроме того, однородные линейные отображения $\mathbf{AB}$ и $\mathbf{I}$ отображают любой вектор и в один и тот же вектор из образа отображения $\mathbf{A}$

[так как $\mathbf{A}(\mathbf{B}(\mathbf{A}(u))) = \mathbf{A}(u)$]. Поскольку образ отображения $\mathbf{A}$ совпадает со всем векторным пространством, то $\mathbf{AB} = \mathbf{I}$. Иначе говоря, каждое из условий (а) и (б) следует как из условия (в), так и из условия (г).

4. Если преобразование невырожденное, то из задачи 3 следует, что для него существует левое и правое обратные преобразования, которые, разумеется, совпадают. Если $\mathbf{A}^{-1}$ — преобразование, обратное преобразованию $\mathbf{A}$, то при $\mathbf{BA} = \mathbf{O}$ и $\mathbf{AC} = \mathbf{O}$ получаем: $\mathbf{B} = \mathbf{BI} = \mathbf{BAA}^{-1} = \mathbf{OA}^{-1} = \mathbf{O}$ и $\mathbf{C} = \mathbf{IC} = \mathbf{A}^{-1}\mathbf{AC} = \mathbf{A}^{-1}\mathbf{O} = \mathbf{O}$. Это означает, что условие (в) следует как из условия (а), так и из условия (б). Если же преобразование $\mathbf{A}$ вырожденное, то его ядро содержит не только нулевой вектор, но и образ преобразования не совпадает со всем векторным пространством. Пусть $u_1, u_2, \ldots, u_r$ — базис подпространства $\mathrm{Ker}\,\mathbf{A}$ и векторы $v_1, v_2, \ldots, v_s$ дополняют его до базиса всего векторного пространства. Тогда подпространство $\mathrm{Im}\mathbf{A}$ имеет размерность s, а один из его базисов состоит из векторов $a_1 = \mathbf{A}(v_1)$, $a_2 = \mathbf{A}(v_2)$, ..., $a_s = \mathbf{A}(v_s)$. Этот базис также можно дополнить до базиса всего векторного пространства, для чего потребуется r векторов. Пусть это будут векторы $b_1, b_2, \ldots, b_r$.

Какие бы $r + s$ векторов мы ни выбрали, всегда можно найти линейное преобразование, переводящее в них векторы любого заданного базиса. Следовательно, существует такое линейное преобразование $\mathbf{B}$, что $\mathbf{B}(b_1) = u_1$, $\mathbf{B}(b_2) = u_2$, ..., $\mathbf{B}(b_r) = u_r$; $\mathbf{B}(a_1) = \mathbf{B}(a_2) = \ldots = \mathbf{B}(a_s) = 0$. Нетрудно видеть, что линейное преобразование $\mathbf{AB}$ также переводит все векторы a_i в нулевой вектор. Поскольку $u_j \in \mathrm{Ker}\mathbf{A}$, то $\mathbf{AB}(b_j) = \mathbf{A}(u_j) = 0$. Итак, линейное преобразование $\mathbf{AB}$ переводит все элементы базиса, состоящего из векторов a_i и b_j, в нулевой вектор, то есть $\mathbf{AB} = \mathbf{O}$. В то же время линейное преобразование $\mathbf{A}$, а значит и $\mathbf{BA}$, переводит в нулевой вектор каждый из векторов u_i. Кроме того, $\mathbf{B}(a_j) = 0$ по определению линейного преобразования $\mathbf{B}$, поэтому $\mathbf{BA}(v_j) = \mathbf{B}(a_j) = 0$. Следовательно, линейное преобразование $\mathbf{BA}$ переводит в нулевой вектор все элементы базиса, состоящего из векторов u_i и v_j, то есть $\mathbf{BA} = \mathbf{O}$. Так как ядро преобразования $\mathbf{A}$ состоит не только из нулевого вектора, то $r > 0$, и поэтому образ преобразования $\mathbf{B}$ содержит не только нулевой вектор. Это означает, что $\mathbf{B} \neq \mathbf{O}$. Таким образом, из условия (в) следует как условие (а), так и условие (б) (хотя, умножив любое линейное преобразование справа или слева на преобразование $\mathbf{B}$, мы получим нулевое преобразование $\mathbf{O}$).

5. Соотношение $\mathbf{P}^2(u) = \mathbf{P}(u)$, которое можно представить в виде $\mathbf{P}^2(u) - \mathbf{P}(u) = 0$, выполняется для любого вектора u. Следовательно, $\mathbf{P} \times (\mathbf{P}(u) - u) = \mathbf{P}^2(u) - \mathbf{P}(u) = 0$, то есть $\mathbf{P}(u) - u = v \in \mathrm{Ker}\,\mathbf{P}$. Но тогда $u = \mathbf{P}(u) + (-v)$, где $\mathbf{P}(u) = \mathrm{Im}\,\mathbf{P}$ и $-v \in \mathrm{Ker}\,\mathbf{P}$. Это означает, что образ и ядро линейного преобразования $\mathbf{P}$ порождают все векторное пространство. С другой стороны, если вектор v принадлежит и образу, и ядру линейного преобразования $\mathbf{P}$, то, во-первых, вектор v можно представить в виде $v = \mathbf{P}(u)$ и, во-вторых, $v = \mathbf{P}(u) = \mathbf{P}^2(u) = \mathbf{P}(\mathbf{P}(u)) = \mathbf{P}(v) = 0$ (так как $\mathbf{P}(v) = 0$). Таким образом, подпространства $\mathrm{Im}\mathbf{P}$ и $\mathrm{Ker}\,\mathbf{P}$ имеют только один общий элемент — нулевой вектор. (Последнее — или, наоборот, первое — утверждение можно было бы не доказывать: по теореме о соотношении между размерностями ядра и образа линейного преобразования достаточно было бы ограничиться доказательством лишь одного из двух утверждений, но это существенно усложнило бы доказательство.)

6. Если $\mathbf{N}^2 = \mathbf{O}$, то, поскольку соотношение $\mathbf{N}(\mathbf{N}(u)) = 0$ выполняется для любого вектора u, линейное преобразование $\mathbf{N}$ переводит в нулевой вектор все элементы своего образа. Следовательно, $\mathrm{Im}\,\mathbf{N} \subset \mathrm{Ker}\mathbf{N}$. С

другой стороны, если образ линейного отображения содержится в ядре того же изображения, то любой вектор u (поскольку $\mathbf{N}(u) = 0$) принадлежит $\operatorname{Im}\mathbf{N}$, то есть $\mathbf{N}(\mathbf{N}(u)) = 0$, а это и означает, что $\mathbf{N}^2 = \mathbf{O}$.

7. Пусть $e_1, e_2, \ldots, e_n$ — базис векторного пространства M_1, а $f_1, f_2, \ldots, f_k$ — базис векторного пространства M_2. Покажем, что базис векторного пространства $\operatorname{Hom}(M_1, M_2)$ можно получить следующим образом.

Пусть $\mathbf{A}_{ij}$ — однородное линейное отображение, переводящее вектор базиса e_i в вектор базиса f_j, а все остальные векторы заданного базиса векторного пространства M_1 — в нулевой вектор. Поскольку образы векторов базиса можно задавать совершенно произвольно, то для любой пары чисел i и j мы получаем по одному однородному линейному отображению.

Докажем, что отображения $\mathbf{A}_{ij}$ составляют систему образующих векторного пространства $\operatorname{Hom}(M_1, M_2)$. Для этого рассмотрим любое однородное линейное отображение $\mathbf{A}$ из этого пространства. Если $\mathbf{A}(e_i) = \alpha_{i1}f_1 + \alpha_{i2}f_2 + \ldots + \alpha_{ik}f_k$, то, как нетрудно видеть, отображение $\mathbf{A}$ совпадает с суммой отображений $\alpha_{ij}\mathbf{A}_{ij}$. Если же сумма отображений $\beta_{ij}\mathbf{A}_{ij}$ является нулевым отображением $\mathbf{O}$, то любой вектор базиса e_p она переводит в нулевой вектор. Это означает, что $\beta_{p1}f_1 + \beta_{p2}f_2 + \ldots + \beta_{pk}f_k = 0$. Поскольку система векторов $f_1, f_2, \ldots, f_k$ как базис линейно независима, то все коэффициенты β_{pq} должны быть равными нулю. Следовательно, отображения $\mathbf{A}_{ij}$ линейно зависимы. Как линейно независимая система образующих совокупность однородных линейных отображений $\mathbf{A}_{ij}$ является базисом. Так как этот базис состоит из nk элементов, то размерность векторного пространства $\operatorname{Hom}(M_1, M_2)$ равна nk.

3.3

1. Операцию сложения можно производить над матрицами с номерами 0 и 4 (сумма матриц равна $[6, 0, 2]$), а также 1 и 3 (сумма матриц равна матрице

$$\begin{bmatrix} 7 & -1 & 8 \\ 0 & 0 & 0 \end{bmatrix}\Bigg).$$

Кроме того, операцию сложения можно производить над матрицами 5 и 9, а также 6 и 8. Суммы матриц равны соответственно

$$\begin{bmatrix} 5 \\ 2 \\ 9 \end{bmatrix} \text{ и } \begin{bmatrix} 0 & 2 \\ 4 & -2 \\ 0 & 0 \end{bmatrix}.$$

Наконец, операцию сложения можно производить над матрицами 2 и 7. Сумма матриц равна

$$\begin{bmatrix} -10 & 11 & 58 \\ 28 & -8 & -1 \\ 4 & 0 & 13 \end{bmatrix}.$$

2. Обозначим через (i,j) произведение матриц с номерами i и j (i — номер первого сомножителя, j — номер второго сомножителя). Тогда

$$(0,5) = [1, 3, -2]\begin{bmatrix} 3 \\ -5 \\ 11 \end{bmatrix} = 1 \cdot 3 + 3(-5) + (-2)11 = -34.$$

Аналогичным образом вычисляем следующие произведения:

$$(0,2) = [34, -33, 14], \quad (0,6) = [-3, -25], \quad (0,7) = [32, 20, 15],$$

$$(0,8) = [15, 9], \quad (0,9) = [27],$$

$$(1,2) = \begin{bmatrix} 0 & 7 & 68 \\ -35 & 37 & 37 \end{bmatrix},$$

$$(1,5) = \begin{bmatrix} 45 \\ 65 \end{bmatrix},$$

$$(1,6) = \begin{bmatrix} 13 & -23 \\ 13 & 6 \end{bmatrix} \quad \text{и т. д.}$$

(Можно было бы также вычислить произведения матриц (1,7), (1,8), (1,9), (2,2), (2,5), (2,6), (2,7), (2,8), (2,9), (3,2), (3,5) — (3,9) и т. д.)

3. Если на плоскости существует такой вектор u, что векторы $v =$

$= \mathbf{A}(u)$ и u не параллельны, то в базисе, состоящем из этих векторов, линейному преобразованию $\mathbf{A}$ соответствует матрица $\begin{bmatrix} 0 & a \\ 1 & c \end{bmatrix}$, так как $\mathbf{A}(u) = 0 \cdot u + 1 \cdot v$. Если же такого вектора u на плоскости не существует, то выберем два любых непараллельных вектора и обозначим их u и v. Так как образ вектора u параллелен вектору u, а образ вектора v параллелен вектору v, то $\mathbf{A}(u) = \alpha u$, $\mathbf{A}(v) = \beta v$, где α и β — некоторые вещественные числа. При некотором γ должно выполняться равенство $\mathbf{A}(u + v) = \gamma(u + v)$, то есть $\alpha u + \beta v = \gamma u + \gamma v$. Поскольку векторы u и v линейно независимы, то $\alpha = \beta = \gamma$. Это означает, что линейное преобразование $\mathbf{A}$ представляет собой растяжение от центра, то есть во всяком базисе его матрица будет иметь вид $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$.

4. Достаточно доказать, что в заданном базисе матрица $\mathbf{A}^2 - p\mathbf{A} + q\mathbf{I}$ совпадает с нулевой матрицей (то есть все элементы матрицы равны нулю), поскольку лишь в этом случае соответствующее линейное преобразование может быть нулевым преобразованием $\mathbf{O}$. Вычисляя матрицы, соответствующие каждому слагаемому в отдельности, а затем их сумму, получаем:

$$[\mathbf{A}]^2 = \begin{bmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{bmatrix},$$

$$-p[\mathbf{A}] = \begin{bmatrix} -pa & -pb \\ -pc & -pd \end{bmatrix},$$

$$[\mathbf{A}^2 - p\mathbf{A} + q\mathbf{I}] =$$

$$= \begin{bmatrix} a^2 + bc - pa + q & ab + bd - pb + 0 \\ ac + cd - pc + 0 & bc + d^2 - pd + q \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

4.1

1. Поскольку существуют две неизоморфные группы четвертого порядка, необходимо рассмотреть два случая.

а) Все элементы группы имеют порядок 2.

Известно, что среди вещественных чисел существует лишь один элемент порядка 2 (относительно умножения), а именно: число -1. Это наводит на мысль представить элементы порядка 2 матрицами $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ или $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, так как квадрат обеих матриц совпадает с единичной матрицей $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Но если матрицы $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ и $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ принадлежат группе, то их произведение также должно быть элементом группы, и матрица $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ является элементом порядка 2. Нетрудно проверить, что при этом мы действительно получаем представление группы.

б) Циклическая группа.

Чтобы построить представление для этого случая, необходимо найти матрицу 2×2, которая была бы элементом порядка 4. В задаче 3 из раздела 3.3 было показано, что произвольному линейному преобразованию соответствует либо матрица $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ в любом базисе, либо матрица $\begin{bmatrix} 0 & a \\ 1 & b \end{bmatrix}$ в специально выбранном базисе. Поскольку соотношения между линейным преобразованием и его степенями выполняются независимо от того, в каком базисе записана матрица преобразования, то, не ограничивая общности, можно предположить, что матрица преобразования записана либо в виде $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$, либо в виде $\begin{bmatrix} 0 & a \\ 1 & b \end{bmatrix}$. Нетрудно видеть, что, если четвертая степень матрицы первого типа совпадает с единичной матрицей $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, то и квадрат той же матрицы совпадает с единичной матрицей (предполагается, что элементы матрицы принадлежат телу вещественных чисел!). Проще всего в этом можно убедиться, вычислив четвертую степень матрицы, но гораздо

лучше воспользоваться следующим способом.

Как показано в задаче 4 из раздела 3.3, рассматриваемое нами линейное преобразование A удовлетворяет соотношению $\mathbf{A}^2 = p\mathbf{A} - q\mathbf{I}$, где $p = 0 + b = b$, а $q = 0 \cdot b - 1 \cdot a = a$, то есть $\mathbf{A}^2 = b\mathbf{A} + a\mathbf{I}$. Возводя в квадрат обе части последнего равенства, получаем: $\mathbf{A}^4 = (\mathbf{A}^2)^2 = (b\mathbf{A} + a\mathbf{I})^2 = b^2\mathbf{A}^2 + 2ab\mathbf{A} + a^2\mathbf{I} = b^2(b\mathbf{A} + a\mathbf{I}) + 2ab\mathbf{A} + a^2\mathbf{I} = (b^3 + 2ab)\mathbf{A} + (b^2a + a^2)\mathbf{I}$. Поскольку преобразования A и I линейно независимы, то преобразование $\mathbf{A}^4$ может совпадать с I в том и только в том случае, если $b^3 + 2ab = 0$ и $b^2a + a^2 = 1$. Первое равенство можно представить в виде $b(b^2 + 2a) = 0$. Если $b = 0$, то из второго равенства следует, что $a = 1$ или $a = -1$. Нетрудно проверить, что матрица $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ является элементом порядка 2. Если же $b \neq 0$, то должно выполняться равенство $b^2 = -2a$. Подставляя это значение b^2 во второе равенство, получаем $-a^2 = 1$, что невозможно, так как квадрат любого вещественного числа положителен.

2. Представление группы пятого порядка матрицами 2×2 можно построить аналогично тому, как в решении предыдущей задачи были построены представления групп четвертого порядка. Известно, что все группы пятого порядка изоморфны, поэтому рассмотрению подлежит лишь один случай. Так как пятая степень матрицы $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ может совпадать с единичной матрицей лишь в том случае, если сама матрица равна единичной, то выбирать следует только матрицы второго типа. В решении предыдущей задачи было показано, что $\mathbf{A}^4 = (b^3 + 2ab)\mathbf{A} + (b^2a + a^2)\mathbf{I}$. Следовательно, $\mathbf{A}^5 = (b^3 + 2ab)\mathbf{A}^2 + (b^2a + a^2)\mathbf{A} = (b^3 + 2ab)(b\mathbf{A} + \mathbf{I}) + (b^2a + a^2)\mathbf{A} = (b^4 + 3ab^2 + a^2)\mathbf{A} + (b^3a + 2a^2b)\mathbf{I}$. Так как $\mathbf{A}^5 = \mathbf{I}$, то $b^4 + 3ab^2 + a^2 = 0$ и $b^3a + 2a^2b = 1$. [Если в первом равенстве произвести подстановку $b^2 = ca$, то оно преобразуется к виду $(c^2 + 3c + 1)a^2 = 0$. Значение $a = 0$ следует отбросить, так как оно приводит к противоречию (из второго равенства мы получили бы, что $0 = 1$), поэтому $c^2 + 3c + 1 = 0$. Из второго равенства при $b^2 = ca$ получаем $b(c + 2)a^2 = 1$. Возводя обе части этого равенства в квадрат и еще раз подставляя $b^2 = ca$, преобразуем к виду $c(c + 2)^2a^5 = 1$. А поскольку $c(c^2 + 4c + 4) = c[(c^2 + 3c + 1) + c + 3] = c(0 + c + 3) = c^2 + 3c = -1$, то матрица, соответствующая образующему элементу группы пятого порядка, принадлежит к матрицам второго типа.] При $a = -1$ из второго равенства получаем $b^3 - 2b + 1 = 0$. Это соотношение (так же как и соотношение $b^4 - 3b^2 + 1 = 0$, в которое переходит при $a = -1$ первое равенство) можно рассматривать как уравнение относительно b. Поскольку $b = 1$ — корень уравнения $b^3 - 2b + 1 = 0$ (но не удовлетворяет уравнению $b^4 - 3b^2 + 1 = 0$), то это уравнение можно преобразовать к виду $(b - 1)(b^2 + b - 1) = 0$. Каждый из корней второго множителя удовлетворяет уравнению $b^4 - 3b^2 + 1 = 0$. Следовательно, матрица, соответствующая образующему элементу группы пятого порядка, имеет вид $\begin{bmatrix} 0 & -1 \\ 1 & b \end{bmatrix}$, где $b = \frac{-1 \pm \sqrt{5}}{2}$ (пригоден любой из корней).

3. Попытка решить эту задачу при помощи простых и коротких выкладок, приведенных в решении предыдущей задачи, кажется безнадежной. Подобный «пессимизм» вполне обоснован: подход, использованный нами в решении предыдущей задачи, непригоден в общем случае не только потому, что связан с необходимостью рассмотрения бесконечного множества групп, но и потому, что весьма часто сами выкладки становятся трудно обозримыми. Гораздо удобнее воспользоваться геометрическим подходом и выяснить, существует ли

на плоскости линейное преобразование, n-я степень которого совпадает с тождественным преобразованием (а любая меньшая степень еще не совпадает с тождественным преобразованием). Перебрав все известные линейные преобразования, мы обнаружим, что таким преобразованием является поворот на $(1/h)$-ю полной окружности. Тем самым утверждение задачи доказано. В качестве примера найдем матрицу 2×2, порождающую представление циклической группы шестого порядка. (Вычисление этой матрицы по способу, примененному в предыдущей задаче, было бы сопряжено с довольно громоздкими выкладками.) Если преобразование A переводит вектор u в вектор v, то в базисе u, v первый столбец матрицы преобразования A имеет вид $\begin{bmatrix}0\\1\end{bmatrix}$. Поскольку поворот вокруг начала координат на 1/6 полной окружности, то угол между векторами u и v равен 60°. Подвергнув вектор v преобразованию A, мы переведем его в вектор $v - u$, поэтому вся матрица преобразования A в базисе u, v имеет вид $\begin{bmatrix}0&-1\\1&0\end{bmatrix}$.

Линейные преобразования позволяют представлять весьма многие группы. Например, если взять две прямые, проходящие через начало координат, то отражения относительно них порождают так называемую группу диэдра. Если угол между прямыми кратен $360°/n$ (но не кратен 360°), то группа диэдра содержит $2n$ элементов и в ней существует нормальный делитель из n элементов, который является циклической подгруппой. Если угол между прямыми таков, что ни один кратный ему угол не совпадает с целым кратным угла 360°, то группа диэдра бесконечна и также содержит (бесконечную) циклическую подгруппу. Фактор-группа группы диэдра по этой циклической подгруппе имеет порядок 2.

Представления многих интересных групп удается построить при помощи линейных преобразований трехмерного пространства.

4.2

1. Поскольку матрицы $\begin{bmatrix}a&-b\\b&a\end{bmatrix}$ составляют подмножество множества всех матриц 2×2, то все тождества, которым должны удовлетворять операции сложения и умножения, для этих матриц выполняются. Необходимо лишь доказать, что множество рассматриваемых матриц замкнуто относительно сложения и умножения. (Этот вопрос не возник бы, если бы речь шла о сложении и умножении вещественных чисел.) Замкнутость относительно умножения легко доказывается прямыми выкладками, так как

$$\begin{bmatrix}a&-b\\b&a\end{bmatrix}\cdot\begin{bmatrix}c&-d\\d&c\end{bmatrix}=$$

$$=\begin{bmatrix}ac&-bd&-ad&-bc\\ad&+bc&ac&-bd\end{bmatrix},$$

то есть произведение двух матриц имеет тот же вид, что и сомножители. Замкнутость относительно сложения очевидна.

Изоморфизм алгебры матриц и тела комплексных чисел задается отображением $\begin{bmatrix}a&-b\\b&a\end{bmatrix} \leftrightarrow a + bi$.

2. Эта задача решается так же, как и предыдущая, только вычисления становятся гораздо более громоздкими. Но существует и другой способ решения, позволяющий избежать длинных выкладок. Воспользуемся им.

Разобьем исходную матрицу двумя прямыми, проходящими через ее центр, на четыре матрицы 2×2. Матрица, стоящая в левом верхнем углу, соответствует комплексному числу $a + bi$. Рядом с ней по горизонтали стоит матрица, соответствующая комплексному числу $-(c + di)$, а под ней — матрица, соответствующая комплексному числу $c - di$. Наконец, в правом нижнем углу исходной матрицы стоит матрица, соответствующая комплексному числу $a - bi$. Если комплексные числа обозначить через $\alpha = a + bi$

и $\beta = c + di$, а комплексно сопряженные числа — через $\overline{\alpha} = a - bi$ и $\overline{\beta} = c - di$, то исходную матрицу можно записать в виде $\begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix}$. Это означает, что кватернионы можно представить матрицами с комплексными элементами так же, как комплексные числа, — матрицами с вещественными элементами. Эта аналогия весьма точна, так как вещественные числа при комплексном сопряжении переходят в себя. (Следовательно, если использовать только вещественные числа, то мы получим представление, приведенное в предыдущей задаче.)

3. Если φ — гомоморфизм и $g_1, g_2, \ldots, g_n$ — элементы группы G_1, то отображение $\alpha_1 g_1 + \alpha_2 g_2 + \ldots + \alpha_n g_n \to \alpha_1 \varphi(g_1) + \alpha_2 \varphi(g_2) + \ldots + \alpha_n \varphi(g_n)$ действительно является гомоморфизмом. (Следует иметь в виду, что элементы $\varphi(g_i)$ в общем случае не образуют базис в G_2.)

К главе третьей

1.1

1. На конечных подмножествах множества неотрицательных целых чисел можно определить объединение и пересечение, поскольку и объединение, и пересечение конечных множеств конечны (в частности, могут содержать 0 элементов). Среди подмножеств имеется наименьшее (пустое множество), но не существует наибольшего, поскольку для любого конечного подмножества можно указать содержащее его конечное подмножество. Понятие дополнения не имеет смысла для рассматриваемых подмножеств, так как дополнение конечного подмножества было бы бесконечным и, следовательно, не принадлежало бы к числу выделенных подмножеств.

Что касается тождеств, они *должны* выполняться (речь идет о тождествах, не содержащих всего множества и дополнений), и поэтому мы не будем доказывать их особо (все эти тождества справедливы для любых подмножеств любого множества).

2. На подмножествах, о которых говорится в задаче, можно задать объединение и пересечение. Действительно, если имеются два подмножества и в каждом из них до множества всех неотрицательных чисел недостает лишь конечного числа элементов, то и в пересечение не войдут лишь те неотрицательные числа, которые не принадлежат либо одному, либо другому подмножеству, и в пересечении будет отсутствовать лишь конечный набор неотрицательных чисел. (В пересечении отсутствующих чисел может оказаться меньше или самое большее столько же, сколько в обоих подмножествах, взятых вместе.) Среди подмножеств существует наибольшее (поскольку множество всех неотрицательных чисел можно рассматривать как подмножество, получающееся при выбрасывании из всего множества конечного, нулевого, набора неотрицательных чисел), но не существует наименьшего (поскольку если подмножество получено при выбрасывании конечного набора элементов из множества неотрицательных чисел, то, выбросив из него еще один элемент, мы получим подмножество, которому до множества всех неотрицательных чисел будет попрежнему недоставать лишь конечного набора элементов). Ясно, что понятие дополнения в рассматриваемом случае лишено смысла и что выполняются все тождества, в которые не входят пустое множество и дополнения.

3. Так же как и в двух предыдущих задачах, подмножества, о которых говорится в этой задаче, допускают объединение и пересечение. Ни наибольшего, ни наименьшего среди рассматриваемых подмножеств не существует, поскольку, выбросив из любого (допустимого) подмножества или присоединив к нему одно число, мы всегда получим подмножество такого же типа, как и исходное. Все тождества, содержащие только выполнимые операции, остаются в силе.

4. Необходимо лишь выяснить, выполняется ли одно тождество, а именно: если $A \supseteq C$, то $(A \cap B) \cup C = A \cap (B \cup C)$. Относительно произвольных подмножеств известно, что $(A \cap B) \cup C \subseteq A \cap (B \cup C)$. Следовательно, остается

лишь доказать, что каждый элемент подмножества $A \cap (B \cup C)$ принадлежит подмножеству $(A \cap B) \cup C$. Если элемент x принадлежит правой части доказываемого равенства, то, с одной стороны, $x \in A$, а, с другой стороны, $x \in B \cup C$. Так как группа коммутативна, то $B \cup C$ состоит из элементов вида $b \cdot c$, где $b \in B$ и $c \in C$. (Это — наиболее важное место во всем доказательстве.) Равенство $x = bc$ запишем в виде $b = xc^{-1}$. Элемент x принадлежит подгруппе A, так как по предположению $x \in A \cap (B \cup C)$. Элемент c принадлежит подгруппе A, так как $A \supseteq C$. Следовательно, подгруппа A содержит и элемент c^{-1}, а значит, и элемент $b = xc^{-1}$. Поскольку элемент b принадлежит и подгруппе B, то он входит в число элементов пересечения $A \cap B$. Отсюда мы заключаем, что элемент $x = bc$ принадлежит подгруппе, порождаемой $A \cap B$ и C, а именно это и требовалось доказать.

5. В решении предыдущей задачи мы уже упоминали о том, что наиболее важным местом во всем доказательстве было утверждение о возможности представления элементов объединения $B \cup C$ в виде произведений $b \cdot c$, где $b \in B$ и $c \in C$. Поскольку для нормальных делителей это условие выполнено, то доказательство, приведенное в решении предыдущей задачи, дословно переносится на случай нормальных делителей.

1.2

1. Подставив $b = a \cap a$ в левую часть тождества $(a \cup b) \cap a = a$, преобразуем ее к виду $[a \cup (a \cap a)] \cap a$. По второму закону поглощения выражение в квадратных скобках равно a. Следовательно, в левой части тождества стоит $a \cap a$, что и требовалось доказать.

2. Прежде всего докажем, что в дистрибутивных структурах выполняются оба тождества. Используя дистрибутивность и ассоциативность, преобразуем левую часть первого тождества к виду $(a \cap b) \cup [(c \cap b) \cup c]$. По закону поглощения выражение в квадратных скобках равно c. Используя дистрибутивность еще раз, получаем, что левая часть доказываемого тождества совпадает с его правой частью. Второе тождество следует из первого в силу принципа двойственности.

Докажем теперь (опираясь опять-таки на двойственность), что любое из тождеств следует из другого (на этот раз без предположения о дистрибутивности структуры). Для этого достаточно доказать, что одно тождество следует из другого, так как рассматриваемые тождества двойственны. Действительно, левые и правые части тождеств соответствуют друг другу, поскольку в обоих случаях являются объединениями (пересечениями). Если во второе тождество вместо элемента $a \cap c$ подставить c, а вместо элемента a — элемент $a \cup c$, то обе левые стороны совпадут, и левую сторону второго тождества можно преобразовать, используя первое тождество. (Возможно, что такое преобразование не ведет к цели, но испробовать его все же стоит.) Итак, пусть $d = a \cap c$. Тогда $a \cup d = a \cup (a \cap c) = a$ (по закону поглощения). Следовательно, в левую часть второго тождества можно подставить $a = a \cup d$ и преобразовать ее к следующему виду: $[(a \cup d) \cap b] \cup d$. Нетрудно видеть, что это выражение совпадает с левой частью первого тождества (необходимо лишь заменить c на d). Поэтому выражение $[(a \cup d) \cap b] \cup d$ совпадает с правой частью первого тождества, в котором элемент c заменен элементом d, то есть равно $(a \cup d) \cap (b \cup d)$. Но так как $a \cup d = d$, а $d = a \cap c$, то $(a \cup d) \cap (b \cup d) = a \cap [b \cup (a \cap c)]$. Тем самым доказано, что второе тождество выполняется, если выполняется первое тождество.

3. Прежде всего воспользуемся дистрибутивностью и преобразуем объединение двух первых пересечений: $(a \cap b) \cup (c \cap b) = (a \cup c) \cap b$.

Всю левую часть тождества запишем в виде $[(a \cup c) \cap b] \cup (c \cap a)$ и, воспользовавшись еще раз дистрибутивностью, представим ее в виде объединения пересечений элементов, стоящих в квадратных скобках, с элементом $c \cap a$, то есть в виде $[(a \cup c) \cup (c \cap a)] \cap [b \cup (c \cap a)]$. Выражение в первых квадратных скобках, используя ассоциативность, приведем к виду $a \cup [c \cup (c \cap a)]$. Из закона поглощения следует, что $c \cup (c \cap a) = c$, поэтому $a \cup [c \cup (c \cap a)] = a \cup c$. Выражение во вторых квадратных скобках дистрибутивность позволяет преобразовать к виду $(b \cup c) \cap (b \cup a)$. Таким образом, выражение, стоящее в левой части доказываемого тождества, совпадает с $[(a \cup c) \cap (b \cup c) \cap (b \cup a)]$, а это (в силу коммутативности и ассоциативности) — не что иное, как выражение, стоящее в правой части тождества.

Справедливо и обратное утверждение: если выполняется тождество, приведенное в задаче, то структура дистрибутивна. Для доказательства обратного утверждения прежде всего необходимо убедиться в том, что выполняются тождества, приведенные в задаче 2. Подставив в левую часть исходного тождества вместо a объединение $a \cup c$, преобразуем ее к виду $[(a \cup c) \cap b] \cup (b \cap c) \cup [c \cap (a \cup c)]$. По закону поглощения $c \cap (a \cup c) = c$, поэтому все выражение можно записать в виде $[(a \cup c) \cap b] \cup [(b \cap c) \cup c]$. Выражение $(b \cap c) \cup c$, стоящее во вторых квадратных скобках, можно упростить, используя закон поглощения $(b \cap c) \cup c = c$, после чего левая часть тождества запишется в виде $[(a \cup c) \cap b] \cup c$. Именно это выражение стоит в левой части первого тождества из задачи 2. Тот же элемент должен получиться из тождества, приведенного в задаче 3 (которое по предположению выполняется), если в его правой части элемент a заменить объединением $a \cup c$. Произведя замену, преобразуем правую часть тождества к виду $(a \cup c \cup b) \cap (b \cup c) \cap (c \cup a \cup c)$. Так как объединение идемпотентно, то $c \cup a \cup c = a \cup c$, а закон поглощения позволяет упростить выражение $[a \cup (b \cup c)] \cap (b \cup c)$, сведя его к $b \cup c$. После этих преобразований правая часть тождества принимает вид $(b \cup c) \cap (a \cup c)$. Ясно, что это выражение совпадает с правой частью первого тождества из задачи 2. Таким образом, в рассматриваемом нами случае выполняются оба тождества из задачи 2 (поскольку в решении задачи 2 было доказано, что одно из тождеств следует из другого), и в дальнейшем мы можем использовать любое из них.

Чтобы доказать дистрибутивность структуры, рассмотрим выражение $a \cap (b \cup c)$. Пользуясь законом поглощения, произведем замену $a = [a \cap (a \cup c)]$, а в выражении, стоящем в квадратных скобках, вместо первого элемента a подставим $[a \cap (a \cup b)]$. Так как пересечение ассоциативно, то полученное выражение можно преобразовать к виду

$$a \cap [(a \cup b) \cap (a \cup c) \cap (b \cup c)].$$

Сравнивая это пересечение с левой частью нашего исходного тождества, получаем:

$$a \cap (b \cup c) = a \cap [(b \cap c) \cup (a \cap c) \cup (a \cap b)].$$

Выражение $a \cap [(a \cap b) \cup (a \cap c)]$ совпадает с правой частью второго тождества из задачи 2, в которой вместо b подставили $a \cap b$. Поэтому оно должно совпадать с левой частью того же тождества, в которой элемент b заменен пересечением $a \cap b$, то есть с выражением $[(a \cap a \cap b) \cup (a \cap c)]$. Это выражение можно упростить. Так как пересечение идемпотентно, то $a \cap a \cap b = a \cap b$ и, следовательно, для $y = (a \cap b) \cup (a \cap c)$ выполняется соотношение $a \cap y = y$. Обозначив через x пересечение $b \cap c$, запишем полученное тождество в виде

$$a \cap (b \cup c) = a \cap [x \cup (a \cap c)].$$

Нетрудно видеть, что его правая часть имеет такой же вид, как и пра-

вая второго тождества из задачи 2, и, следовательно, вместо нее можно записать левую часть этого тождества, то есть выражение $[(a \cap x) \cup (a \cap y)]$. Как было показано выше, $a \cap y = y = (a \cap b) \cup (a \cap c)$, то есть в правой части нашего тождества стоит элемент $[(a \cap x) \cup (a \cap b)] \cup (a \cap c)$. Но

$$(a \cap x) \cup (a \cap b) = (a \cap b \cap c) \cup (a \cap b) = [(a \cap b) \cap c] \cup (a \cap b),$$

а по закону поглощения элемент $[(a \cap b) \cap c] \cup (a \cap b)$ совпадает с $a \cap b$. Следовательно, $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$, а это и означает, что структура дистрибутивна.

1.3

1. Нет, не верно. Утверждение было бы верно в том случае, если бы, изъяв из любой структуры граничные элементы, можно было бы получить частично упорядоченное множество, а дополнив частично упорядоченное множество граничными элементами, превратить его в структуру. Если частично упорядоченное множество содержит два или три элемента, то, приписав к нему граничные элементы, мы действительно получим структуры, содержащие соответственно четыре и пять элементов. На рис. 93 изображено частично упорядоченное множество, полученное таким способом из частично упорядоченного множества, содержавшего 4 элемента. Дополненное множество не является структурой, поскольку содержит элементы, для которых существует несколько «наибольших нижних граней». Чтобы утверждение стало верным, его необходимо видоизменить и относить не ко всем частично упорядоченным множествам, а лишь к таким, в которых никакие два элемента не могут иметь по нескольку «наибольших нижних граней». Действительно, если это условие соблюдено, то для любых двух элементов верхняя грань, если она и существует, может быть только наименьшей верхней гранью. Если такое множество дополнить граничными элементами, то те пары, для которых ранее не существовало объединения или пересечения, могут обрести недоставший элемент. Впрочем, никаких проблем, связанных с однозначностью, при этом не возникает.

2. Пересечение, стоящее в левой части, и объединение, стоящее в правой части, содержат четыре элемента, поэтому какой-то из элементов a, b и c встречается дважды. Поскольку каждое пересечение и каждое объединение связывает различные элементы, то элемент, который встречается дважды (или, если их несколько, элементы), должен (должны) один раз входить в пересечение и один раз входить в объединение. Предположим, что дважды встречается элемент a. Тогда в левой части он входит в пересечение $x \cap a$, а в правой — в объединение $y \cup a$, и $x \cap a \leqslant a \leqslant y \cup a$. Поскольку отношение $\leqslant$ транзитивно, то отсюда следует, что любое пересечение в левой части не больше (меньше или равно) любого объединения в правой части. Следовательно, объединение пересечений не больше пересечения объединений, что и требовалось доказать.

3. Прежде всего докажем, что для любых двух элементов существует наибольшая нижняя и наименьшая верхняя грань. Пусть $a \leqslant b$. Тогда элемент a является нижней гранью элементов a и b, а элемент b — их верхней гранью. Если элемент x — любая нижняя грань этих элементов, а элемент y — любая их верхняя грань, то по определению $x \leqslant a$ и $b \leqslant y$, а это означает, что a — наибольшая нижняя грань элементов a и b, а b — их наименьшая верхняя грань.

Прежде чем приступать к доказательству дистрибутивности, покажем, что для всякой структуры справедливо следующее утверждение: если $a \leqslant b$, то при любом элементе c выполняется отношение $a \cup c \leqslant b \cup c$ (и аналогично $a \cap c \leqslant b \cap c$). Действительно, так как $b \leqslant b \cup c$, $c \leqslant$

$\leqslant b \cup c$ и $a \leqslant b$, то в силу транзитивности упорядочения элемент $b \cup c$ является верхней гранью для элементов a и c, то есть не меньше их наименьшей верхней грани.

Тем самым мы доказали, что $(a \cap b) \cup c = (a \cup c) \cap (b \cup c)$. Так как исходное множество частично упорядочено, то какой-то из элементов a и b не больше другого. Поскольку эти элементы входят в правую и левую части выведенного равенства симметрично (правая и левая части тождества не изменятся, если элементы a и b переставить), то, неограничивая общности, можно предположить, например, что $a \leqslant b$. Это означает, что, во-первых, $a \cap b = a$ и, следовательно, в левой части равенства стоит элемент $a \cup c$, а, во-вторых, по доказанному $a \cup c \leqslant b \cup c$, то есть пересечение, стоящее в правой части равенства, также равно $a \cup c$. Тем самым дистрибутивность структуры доказана.

2.1

1. Если любое подмножество структуры является подструктурой, то, в частности, это можно сказать и о подмножествах, содержащих по 2 элемента. Следовательно, если a и b — различные элементы структуры то пересечение $a \cap b$ совпадает либо с a, либо с b, а это означает, что либо $a \leqslant b$, либо $b \leqslant a$. Таким образом, наша структура (как частично упорядоченное множество) заведомо упорядочена. Но структуры, получаемые из упорядоченных множеств, обладают требуемым свойством, поскольку любое подмножество вместе с двумя своими элементами содержит их объединение и пересечение: ведь и объединение, и пересечение любых двух подмножеств совпадают с одним из них.

2. Пусть a и b — два «не сравнимых» элемента структуры (то есть такие элементы, для которых не выполняется ни отношение $a \leqslant b$, ни отношение $b \leqslant a$). Если в структуре существует такой элемент x, для

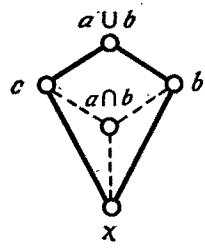


Рис. 116.

которого $x \leqslant a \cap b$, но $x \neq a \cap b$, то четыре элемента x, a, b и $a \cup b$ образуют подмножество, которое является структурой относительно объединения и пересечения, заданных в исходной структуре, но не принадлежит к числу ее подструктур, так как пересечение $a \cap b$ в исходной структуре отличается от пересечения тех же элементов в построенной структуре (рис. 116). Следовательно, в исходной структуре пересечение любых двух не сравнимых элементов может быть только нулевым элементом, а объединение — только единичным элементом структуры. Итак, возможны два случая. Если структура упорядочена как частично упорядоченное множество, то любое подмножество является подструктурой. В противном случае структура совмещает в себе несколько упорядоченных множеств, и, кроме того, мы можем присоединить к ней нулевой и единичный элементы. Итак, если некоторое подмножество частично упорядоченного множества является структурой, то она состоит либо из элементов одного упорядоченного множества (и является подструктурой исходной структуры), либо состоит из элементов по крайней мере двух упорядоченных множеств. Следовательно, если нулевой и единичный элемент принадлежат подмножеству, то оно является подструктурой исходной структуры, поскольку содержит объединение и пересечение любых двух своих не сравнимых элементов.

3. Утверждение очевидно. Действительно, любой элемент структуры сам по себе является подструктурой, так как объединение и пересечение

идемпотентны. Если структура содержит по крайней мере два элемента, то каждый из них образует подструктуру, отличную от всей структуры.

4. Нет, не верно. Из решения предыдущей задачи видно, что пересечение двух подструктур, содержащих по одному элементу, пусто. Если структура содержит по крайней мере два элемента, то такие подструктуры заведомо найдутся.

5. Можно. Из решения предыдущей задачи видно, что пересечение двух подструктур может быть пустым, но если оно не пусто, то, очевидно, само является подструктурой. Но пересечение подструктур, содержащих заданные элементы, не может быть пустым, поскольку будет содержать эти элементы. Следовательно, подструктура, порожденная заданными элементами, представляет собой не что иное, как пересечение подструктур, содержащих эти элементы.

6. Ясно, что, если отображение сохраняет частичное упорядочение, то упорядоченное множество оно может переводить только в упорядоченное множество, поэтому «вторая» структура, на которую происходит отображение, может быть только упорядоченной (рис. 117). Граничный элемент может переходить только в граничный элемент, поэтому во второй структуре по существу может быть лишь одно отображение интересующего нас типа [правда, «средние» элементы могут отображаться в «обратном» порядке (рис. 118)]. Ясно, что рассматриваемое отображение сохраняет частичное упорядочение. Оно не является гомоморфизмом (а значит, и изоморфизмом). Это следует из того, что в «первой» структуре пересечение двух не граничных элементов совпадает с нулевым элементом, а пересечение их образов не совпадает с нулевым элементом (точнее, не совпадает с образом нулевого элемента).

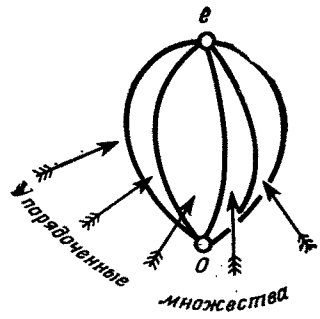


Рис. 117.

2.2

1. Если элементы x и y обладают требуемым свойством, то есть, если $x \leqslant a$ и $y \leqslant b$, где a и b — элементы выпуклой подструктуры, то $x \cup y$ также обладает этим свойством (так как $x \cup y \leqslant a \cup b$, а элемент $a \cup b$ принадлежит выпуклой подструктуре). Таким образом, свойство 1 идеала доказано.

Если $x \leqslant a$ и a — элемент выпуклой подструктуры, то при $y \leqslant x$ вследствие транзитивности отношения $\leqslant$ элемент y также будет меньше хотя бы одного элемента выпуклой подструктуры. Следовательно, свойство 2 идеала также доказано. Нетрудно заметить, что выпуклость подструктуры в доказательстве совсем не была использована.

2. Как показано в решении предыдущей задачи, заданная выпуклая подструктура содержится в идеале, состоящем из элементов структуры, которые не больше какого-нибудь из ее элементов. Аналогичным образом можно убедиться в том, что заданная выпуклая подструктура содержится

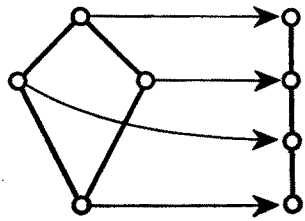


Рис. 118.

в двойственном идеале, состоящем из элементов структуры, которые не меньше какого-нибудь из ее элементов. Следовательно, заданная выпуклая подструктура содержится в пересечении того идеала и того двойственного идеала, о которых шла речь. Докажем теперь, что она совпадает с этим пересечением.

Если x — элемент идеала, то в выпуклой подструктуре найдется такой элемент a, что $x \leqslant a$. Если же элемент x принадлежит двойственному идеалу, то в выпуклой подструктуре найдется такой элемент b, что $b \leqslant x$. Поскольку выполняются оба «неравенства», то есть $b \leqslant x \leqslant a$ и оба элемента a и b, принадлежат выпуклой подструктуре, то элемент x также принадлежит ей (последнее следует из выпуклости подструктуры). Таким образом, выпуклая подструктура совпадает с пересечением идеала и двойственного идеала, о которых говорилось выше.

(Этот метод позволяет строить «выпуклую оболочку» произвольной подструктуры, то есть наименьшую выпуклую подструктуру, которая содержит ее. Для этого достаточно построить содержащий подструктуру идеал так, как это было сделано в решении задачи 1, а затем аналогичным способом построить содержащий ее двойственный идеал. Пересечение идеала и двойственного идеала и будет выпуклой оболочкой заданной подструктуры.)

3. Каждый идеал можно рассматривать как нижний сегмент, порожденный некоторым сечением структуры. Идеал будет примарным идеалом, если верхний сегмент, порожденный тем же сечением, является двойственным идеалом. Одно из необходимых для этого условий заранее выполнено, поскольку речь идет о сечении структуры. Второе условие состоит в том, что, если элементы a и b принадлежат двойственному идеалу, то он содержит и пересечение $a \cap b$. Это условие можно сформулировать и следующим образом: если пересечение $a \cap b$ не принадлежит двойственному идеалу, то он не содержит какой-нибудь из элементов a и b. Иначе говоря, если $a \cap b$ принадлежит идеалу, то в нем должен содержаться и какой-нибудь из элементов a и b. Тем самым утверждение задачи доказано.

(На свойство, о котором говорится в задаче, указывает само название «примарный идеал», то есть идеал, напоминающий по свойствам простые числа. Действительно, «структурное» сходство следующих двух утверждений весьма заметно: а) если пересечение двух элементов принадлежит примарному идеалу, то какой-нибудь из них также принадлежит примарному идеалу; б) если произведение двух чисел делится на простое число, то по крайней мере один из сомножителей делится на это простое число. Но чаще свойства примарных идеалов и простых чисел бывают связаны не «тесными родственными узами», а обнаруживают лишь отдаленное сходство. Мы не рассматриваем здесь такие свойства, поскольку не занимаемся выяснением «внешних связей» между примарными идеалами и простыми числами.)

4. Если структура содержит элемент, для которого существует дополнение, то в структуре имеются нулевой и единичный элементы. Ясно, что нулевой элемент структуры содержится во всяком идеале, потому что нулевой элемент не больше любого элемента структуры. Что же касается единичного элемента, то он по аналогичным причинам принадлежит любому двойственному идеалу (за исключением «пустого» двойственного идеала). Если некоторый элемент вместе со своим элементом принадлежит одному идеалу, то этот идеал содержит как единичный, так и нулевой элемент, поскольку вместе с любыми двумя элементами ему принадлежат их объединение и пересечение. Следовательно, такой идеал может быть только всей структурой. Аналогично, из всех двойственных идеалов только вся структура

(которую мы не относим к двойственным идеалам) могла бы содержать нулевой и единичный элементы. Следовательно, истинный примарный идеал может содержать что-нибудь одно: либо элемент, либо дополнение.

5. В решении задачи 3 условие примарности идеала сформулировано следующим образом: идеал примарен, если он вместе с пересечением двух элементов содержит какой-нибудь из них. Этому условию удовлетворяет любое подмножество из структуры, заданной на упорядоченном множестве, поскольку вместе с пересечением двух элементов оно всегда содержит один из этих элементов и этот элемент принадлежит исходному множеству.

6. Докажем, что других структур, в которых всякий идеал примарный, не существует. Пусть a и b — произвольные элементы структуры. Идеал $(a \cap b)_i$, состоящий из элементов, каждый из которых не больше пересечения $a \cap b$, содержит элемент $a \cap b$. Если этот идеал примарный, то он должен содержать какой-нибудь из элементов a и b. Не ограничивая общности (поскольку оба элемента входят в пересечение $a \cap b$ симметрично), предположим, что примарному идеалу принадлежит элемент a. Тогда по определению идеала $(a \cap b)_i$ должно выполняться соотношение $a \leqslant a \cap b$. Сравнивая его с соотношением $a \cap b \leqslant a$ и используя антисимметрию частичного упорядочения, получаем $a = a \cap b$. Но это и означает, что $a \leqslant b$. Следовательно, любые два элемента структуры допускают сравнение.

7. Напомним, что в конечной структуре любой идеал состоит из элементов, которые не больше данного элемента. Этот элемент является объединением всех элементов идеала (имеющим смысл в том случае, когда структура конечна, поскольку объединение конечного числа элементов существует), так как объединение всех элементов принадлежит идеалу и не меньше любого из его

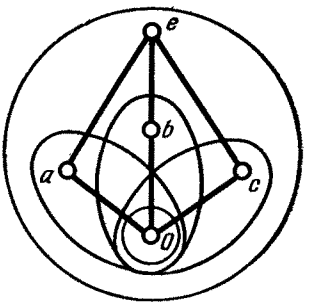


Рис. 119.

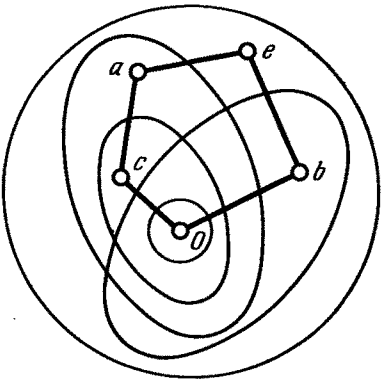


Рис. 120.

элементов. Следовательно, в каждой из двух структур, содержащих по 5 элементов, существует ровно 5 идеалов. Эти идеалы показаны на рис. 119 и 120.

Рассмотрим сначала примарные идеалы модулярной, но не дистрибутивной структуры. Обозначим элементы структуры, отличные от граничных элементов, через a, b и c. Если задан примарный идеал, то по крайней мере два из этих элементов принадлежат либо примарному идеалу, либо двойственному примарному идеалу. (Каждый элемент структуры принадлежит либо примарному идеалу, либо двойственному примарному идеалу, поэтому из трех элементов по крайней мере два должны попасть либо в примарный идеал, либо в его дополнение.) Вместе с этими двумя элементами примарному идеалу или двойственному примарному идеалу принадлежит их объ-

единение и пересечение. Поскольку объединение элементов совпадает с единичным элементом, а пересечение — с нулевым элементом, то либо все элементы структуры принадлежат примарному идеалу, либо все элементы структуры принадлежат двойственному примарному идеалу. Следовательно, существует только тривиальный примарный идеал, совпадающий со всей структурой.

Можно показать, что во второй структуре из пяти элементов существуют два примарных идеала, один из которых помимо нулевого элемента содержит элемент b, а другой — элементы a и c.

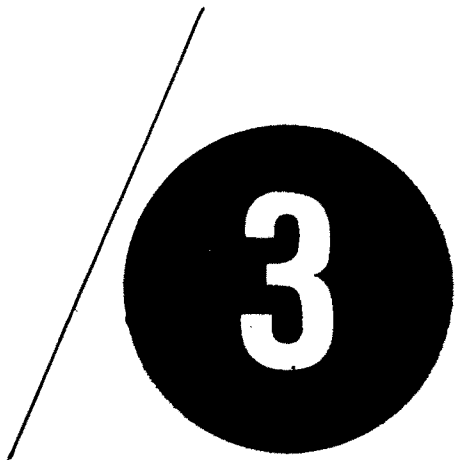
2.3

1. Образом нулевого элемента при любом гомоморфизме может быть только нулевой элемент, поэтому образ нулевого элемента принадлежит любому примарному идеалу. Следовательно, точка P_φ не будет образом нулевого элемента ни при каком гомоморфизме φ, то есть подмножество $H(0)$ не содержит ни одной точки, а это означает, что $H(0)$ —пустое множество.

2. Единичный элемент принадлежит только тривиальному примарному идеалу, поэтому ни при каком гомоморфизме φ не может отображаться в нулевой элемент, то есть $\varphi(e)$ всегда совпадает с точкой P_φ. Это означает, что все точки P_φ принадлежат подмножеству $H(e)$, то есть оно совпадает со всем множеством.

3. Как показано в решении задачи 4 из раздела 2.2, любой нетривиальный примарный идеал содержит либо элемент, либо его дополнение, но не оба. Иначе говоря, если элементы a и a' дополняют друг друга, то один из образов $\varphi(a)$ или $\varphi(a')$ совпадает с нулевым элементом. Это означает, что точка P_φ принадлежит одному и только одному из множеств $H(a)$ и $H(a')$. (Решения двух предыдущих задач позволяют доказать то же утверждение исходя из свойства гомоморфизма сохранять операции.)

КРАТКИЙ СЛОВАРЬ ТЕРМИНОВ



В этом кратком словаре собраны наиболее важные или часто встречающиеся в книге термины. (Курсивом выделены термины, смысл которых раскрывается в других статьях словаря. Число в скобках указывает номер страницы, на которой термин встречается впервые.)

Абелева группа (49). *Коммутативная группа.* (Абелевы группы названы в честь норвежского математика Нильса Хенрика Абеля.)

Абстрактная группа (43, 73). *Группа* называется абстрактной в том случае, если ни ее элементы, ни *групповая операция* не заданы конкретно. Точнее говоря, абстрактной группой называется множество групп, изоморфных данной группе.

Автомат (88). Пятерка $\langle X, A, Y; f, g\rangle$, где X — множество сигналов на входе, A — множество внутренних состояний, Y — множество сигналов на выходе, а f и g — две двухместные *операции*, из которых первая сигналу на входе и внутреннему состоянию ставит в соответствие определенное внутреннее состояние, а вторая сигналу на входе и внутреннему состоянию сопоставляет определенный сигнал на выходе.

Автоморфизм (83). *Изоморфное отображение* на себя группы (или любой *алгебраической структуры*).

Аксиомы (43). Свойства операций, налагаемые определением группы (или другой *алгебраической структуры*).

Алгебра (156). Кольцо A называется алгеброй над *телом* Γ, если A — аддитивная группа и *векторное пространство* над Γ и, кроме того, для любого λ из Γ и любых элементов u, v из A выполняются соотношения $\lambda(uv) = (\lambda u)v = u(\lambda v)$.

Алгебра отношений (193). Теория *алгебраических структур*, учитывающих наряду с операциями логические функции.

Алгебраическая структура (191). Система $\mathfrak{A} = \langle A;\ f_1,\ f_2,\ \ldots,\ f_n,\ \ldots\rangle$, где A — некоторое множество, а $f_1, f_2, \ldots, f_n, \ldots$ — *операции*, определенные на элементах этого множества.

Алгебраическая структура, определяемая равенствами (192). Алгебраическая структура, в которой *аксиомы* относительно *операций* можно задать равенствами (или тождествами).

Аннуляторное кольцо (99). *Кольцо*, в котором *произведение* любых двух элементов равно *нулевому элементу* кольца.

Ассоциативность (15). Свойство операции, состоящее в том, что для любых трех элементов $(ab)c = a(bc)$ (два элемента, стоящие рядом, означают, что над ними произведена операция).

Ассоциированный элемент (104). Два элемента кольца называются ассоциированными, если каждый из них делит другой.

Базис (122). Базисом *векторного пространства* называется *линейно независимая система*, которая одновременно является *системой образующих*.

Бесконечномерное векторное пространство (124). *Векторное пространство*, в котором содержится по крайней мере один ненулевой вектор и не существует (конечного) *базиса*.

Булева алгебра (171). *Ограниченная* и *дистрибутивная структура*, в которой для каждого элемента существует *дополнение*.

Вектор (112). Элемент *векторного пространства*.

Векторное пространство (112). Так называется *коммутативная груп-*

па М над *коммутативным телом* Γ, если любому α из Γ и любому элементу u из М соответствует некоторый элемент αu из М; для любых α, β из Γ и u, v из М выполняются соотношения $(\alpha + \beta)u = \alpha u + \beta u$, $\alpha(u + v) = \alpha u + \alpha v$, $(\alpha\beta)u = \alpha(\beta u)$ и для единичного элемента 1 из Γ и любого элемента u из М справедливо соотношение $1u = u$.

Верхняя грань (173). В *частично упорядоченном множестве* a называется верхней гранью для элементов b_1, b_2, ..., b_n, ..., если при любом индексе i выполняется отношение $b_i \leqslant a$.

Взаимно-однозначное соответствие (31). *Взаимно-однозначное отображение.*

Взаимно-однозначное отображение (54). *Отображение*, при котором каждый элемент выступает в качестве образа какого-нибудь элемента и различные элементы переходят в различные.

Внешняя прямая сумма (129). *Прямая сумма.*

Внутренняя прямая сумма (129). *Векторное пространство* называется внутренней прямой суммой двух *подпространств*, если они порождают все векторное пространство, а их пересечение состоит только из *нулевого вектора*.

Выпуклая подструктура (182). *Подструктура структуры*, содержащая вместе с любыми элементами a и b все элементы x, для которых $a \leqslant x \leqslant b$.

Главная диагональ (149). Элементы *квадратной матрицы*, стоящие на пересечениях строк и столбцов с одинаковыми номерами.

Гомологическая алгебра (194). Область современной абстрактной алгебры, смежная с топологией.

Гомоморфное отображение (76, 180, 191). Отображение одной *группы*, структуры или *алгебраической структуры* в другую, сохраняющее операции. Последнее означает, что образ результата *операции*, производимой над элементами исходного множества, можно получить, выполнив над образами элементов операцию, определенную на содержащем их множестве.

Группа (37, 84). Пара $\langle G; f \rangle$, состоящая из множества G и заданной на нем двухместной *операции* f; операция f ассоциативна, существует *единичный* элемент, и для каждого элемента из G существует *обратный*. Другое определение: четверка $\langle G; f, e, i \rangle$, состоящая из множества G, одной двухместной операции f, одной нульместной операции e и одной одноместной операции i, где f — *групповая операция*, e — обозначение единичного элемента и i — функция, сопоставляющая каждому элементу группы обратный элемент. Эти аксиомы определяют те же свойства, что и предыдущее определение группы.

Групповая алгебра (158). *Алгебра* (Γ, G) над *телом* Γ, базис которой *изоморфен группе* G по умножению.

Групповая операция (37). В группе $\langle G; f \rangle$ — это функция f, которая каждой паре элементов из G ставит в соответствие некоторый элемент из G. Если групповая операция представляет собой умножение или не имеет специального названия, то говорят о групповом умножении. Если же групповая операция представляет собой сложение, то группа называется аддитивной.

Движение (31). *Взаимно-однозначное соответствие* между точками плоскости или трехмерного пространства (*взаимно-однозначное отображение* плоскости или пространства на себя), при котором расстояние между любыми двумя точками не изменяется.

Двойственный идеал (183). *Выпуклая подструктура*, содержащая вместе с любым элементом a все элементы x, удовлетворяющие отношению $a \leqslant x$.

Двойственный примарный идеал (184). Двойственный идеал, содержащий объединение двух элементов лишь при условии, если каждый из них принадлежит ему.

Деление (40). В *группах* — решение уравнений $ax = b$ и $ya = b$.

Делитель (102). Элемент a из *области целостности* называется делителем элемента b, если в кольце существует такой элемент c, для которого $ac = b$.

Делитель нуля (96). Два отличных от нуля элемента *кольца*, произведение которых совпадает с *нулевым элементом*, называются делителями нуля.

Дистрибутивность (94). Одна *операция* (например, умножение) дистрибутивна относительно другой операции (например, сложения), если выполняются тождества $(a \dotplus b)c = ac \dotplus bc$ и $c(a \dotplus b) = ca \dotplus cb$. Если выполняется только первое тождество, то говорят, что операция дистрибутивна справа. Если выполняется только второе тождество, то операция называется дистрибутивной слева.

Дистрибутивная структура (168). *Структура*, в которой любая из двух *операций дистрибутивна* относительно другой.

Длина цикла (24). Число элементов, входящих в *цикл* (то есть число фактически перемещаемых элементов).

Дополнение (162). Дополнением подмножества A называется подмножество, *объединение* которого с подмножеством A совпадает со всем множеством, а *пересечение* пусто (*пустое множество*). Дополнением элемента *а структуры* называется такой элемент, объединение которого с элементом a совпадает с *единичным элементом*, а пересечение с *нулевым элементом* структуры.

Евклидово кольцо (101). *Область целостности с единицей*, в которой каждому элементу a, отличному от *нулевого элемента*, поставлено в соответствие неотрицательное целое число $\varphi(a)$ так, что при любом a и отличном от нулевого элемента b всегда найдутся элементы q и r, удовлетворяющие соотношениям $a = bq \dotplus r$ и либо $\varphi(r) < \varphi(b)$, либо $r = 0$.

Единицы (104). Элементы кольца, являющиеся *делителями единичного элемента*.

Единичная подгруппа (52). *Подгруппа группы*, состоящая только из *единичного элемента*.

Единичный элемент (29, 37, 96, 169). Элемент e *группы* (или *полугруппы*), для которого при любом a из группы (или полугруппы) выполняются соотношения $ea = ae = a$. Если выполняется только соотношение $ea = a$ или только соотношение $ae = a$, то e называется соответственно левым или правым единичным элементом. Единичным элементом кольца называется единичный элемент полугруппы, образуемой элементами *кольца* относительно *заданного в нем умножения*. Единичным элементом структуры называется элемент, служащий *верхней гранью* для любого другого элемента структуры.

Законы поглощения (164). Тождества $a \cup (a \cap b) = a$ и $a \cap (a \cup b) = a$ в теории структур.

Законы сокращения (41). Действуют в *полугруппе*, если для произвольных элементов из соотношений $ax = ay$ или $xa = ya$ следует, что $x = y$. Если заключение о равенстве $x = y$ можно вывести только из первого соотношения, то говорят о левом законе сокращения, а если только из второго соотношения, то о правом законе сокращения.

Замкнутость относительно операции (50). Свойство *подгрупп* (или *алгебраических подструктур*) *группы* (*алгебраической структуры*), состоящее в том, что результат операции, производимой над элементами подгруппы (подструктуры), также принадлежит подгруппе (подструктуре).

Идеал (183). *Выпуклая подструктура структуры*, содержащая вместе со всеми элементами их *нижнюю грань*.

Идемпотентность (163). Свойство двухместной *операции*, состоящее в том, что вторая степень некоторого

элемента совпадает с ним самим, то есть $aa = a$. Идемпотентностью принято называть аналогичное свойство двухместной операции и в том случае, если оно выполняется на всех элементах. Например, в *структурах* идемпотентны обе заданные на них операции: $a \cap a = a$ и $a \cup a = a$.

Изоморфное отображение (72). *Взаимно-однозначное гомоморфное отображение.*

Истинная подгруппа (52). Любая *нетривиальная подгруппа группы.*

Истинное подпространство (114). Любое *нетривиальное подпространство векторного пространства.*

Категория (194). Совокупность так называемых *объектов* и *отображений*, удовлетворяющих определенным тождествам.

Квадратная матрица (149). Прямоугольная *матрица*, в которой число столбцов совпадает с числом строк.

Кольцо (95). Тройка $\langle R; f, g\rangle$, где $\langle R; f\rangle$ — *коммутативная группа*, $\langle R; g\rangle$ — *полугруппа* и операция g *дистрибутивна* относительно операции f.

Кольцо без делителей нуля (96). *Кольцо*, не содержащее делителей нуля.

Кольцо с единицей (96). Кольцо, в котором существует *единичный элемент.*

Коммутативная группа (49). Группа с *коммутативной групповой операцией.*

Коммутативность (15). Свойство двухместной *операции*, состоящее в том, что результат применения ее к любым двум элементам не зависит от того, в каком порядке они взяты. Если ab означает, что над элементами a и b произведена операция, то в случае коммутативности $ab = ba$.

Конечная группа (52). *Группа*, содержащая конечное число элементов.

Конкретная группа (43). *Группа* с заданными элементами и *операцией.*

Координаты (145). Если элемент (вектор) *векторного пространства* представить в виде *линейной комбинации* векторов *базиса*, то входящие в эту линейную комбинацию *скаляры* называются координатами вектора в заданном базисе.

Левый R-модуль (130). Так называется *коммутативная группа* M (в которой групповая операция обозначена как сложение) над *кольцом* R, если любому α из R и любому элементу u из M можно поставить в соответствие элемент αu из M (называемый произведением α и u), причем так, что

$$(\alpha + \beta)\, u = \alpha u + \beta u;$$

$$\alpha\,(u + v) = \alpha u + \alpha v;$$

$$(\alpha\beta)\, u = \alpha\,(\beta u)$$
$$(\beta \in \mathrm{R},\ v \in \mathrm{M}).$$

Левый обратный элемент (39). Элемент b называется левым обратным для элемента a полугруппы с единицей, если произведение ba совпадает с единичным элементом полугруппы.

Левый смежный класс (60). Если H — *подгруппа группы* G и a — некоторый элемент из G, то левым смежным классом aH называется множество элементов вида ax, где $x \in$ H.

Линейная зависимость (117). Элемент *векторного пространства* линейно зависим от определенных *векторов*, если его можно представить в виде *линейной комбинации* этих векторов.

Линейная комбинация (113). Линейной комбинацией элементов *векторного пространства* называется сумма скалярных кратных этих элементов (произведений элементов и *скаляров*).

Линейная независимость (118). Элемент *векторного пространства* линейно независим от определенных векторов, если его нельзя представить в виде *линейной комбинации* этих векторов.

Линейно зависимая система

(119). Подмножество *векторного пространства*, в котором имеется *вектор*, *линейно зависящий* от других векторов.

Линейно независимая система (119). Подмножество *векторного пространства*, не содержащее *вектора*, который был бы *линейно зависим* от остальных векторов.

Линейное преобразование (142). *Однородное линейное отображение* векторного пространства на себя.

Матрица (148). Элементы, чаще всего числа, расположенные в определенном порядке, обычно в виде прямоугольника.

Модуль (130). Общее название *левых* и *правых модулей*.

Модулярная структура (178). *Структура*, в которой равенство

$$a \cap (b \cup c) = (a \cap b) \cup c$$

выполняется при $a \geqslant c$ для любого элемента b.

Мономорфизм (76). *Гомоморфное отображение*, при котором образы различных элементов различны.

Наибольшая нижняя грань (173). *Нижняя грань* двух (или большего числа) элементов *частично упорядоченного множества*, которая служит нижней гранью всех других нижних граней этих элементов.

Наибольший общий делитель (102). *Общий делитель* двух (или большего числа) элементов *области целостности*, делящийся на любой другой общий делитель этих элементов.

Наименьшая верхняя грань (173). *Верхняя грань* двух (или большего числа) элементов *частично упорядоченного множества*, которая служит *верхней гранью* всех других верхних граней этих элементов.

Невырожденная матрица (153). *Квадратная матрица*, для которой существует *обратная* (относительно умножения) матрица.

Независимые циклы (22). *Циклы*, не имеющие общих элементов.

Неразложимый элемент (104). Элемент *области целостности*, обладающей единичным элементом, который допускает разложение на два множителя лишь в том случае, если один из них равен *единице*, но сам отличен от единицы.

Нечетная подстановка (27). *Подстановка*, допускающая разложение в произведение нечетного числа *транспозиций*.

Нижняя грань (173). Нижней гранью двух (или большего числа) элементов *частично упорядоченного множества* называется элемент, который меньше этих элементов или равен им.

Нормальный делитель (63). *Подгруппа группы* называется нормальным делителем, если любой *левый смежный класс* по ней является одновременно и правым смежным классом (по ней же).

Нулевое кольцо (96). *Кольцо*, состоящее из единственного элемента — *нулевого элемента*.

Нулевой элемент (169). В *структуре* — элемент, служащий нижней гранью для любого другого элемента. В *кольце* — единичный элемент аддитивной группы.

Нульмерное векторное пространство (124). *Векторное пространство*, состоящее только из нулевого вектора.

Область целостности (96). *Коммутативное кольцо без делителей нуля*.

Обратный элемент (37, 96). *Левый обратный элемент*, который является и *правым обратным элементом*.

Общая алгебра (191). Раздел алгебры, изучающий общие свойства *алгебраических структур*.

Общий делитель (102). Общим делителем двух (или большего числа) элементов *области целостности* называется такой элемент, который *делит* каждый из этих элементов.

Объединение (173, 161). Объединением двух элементов *частично упорядоченного множества* называется их *наименьшая верхняя грань*. Объединением двух подмножеств одного множества называется подмно-

жество, состоящее из элементов множества, которые принадлежат по крайней мере одному из этих двух подмножеств.

Объект (193). Элемент *категории*.

Ограниченная структура (169). *Структура*, в которой имеется *нулевой элемент* и *единичный элемент*.

Однородное линейное отображение (132). *Отображение* $\mathbf{A}$ *векторного пространства* M_1 над телом Γ в векторное пространство M_2 над телом Γ, для которого при любых элементах u и v из M_1 и λ из Γ выполняются соотношения $\mathbf{A}(u + v) = \mathbf{A}(u) + \mathbf{A}(v)$ и $\mathbf{A}(\lambda u) = \lambda \mathbf{A}(u)$.

Операция (37). В теории *групп* или любых других *алгебраических структур* так называют функции, входящие в определение группы (или алгебраической структуры). Эти функции принимают значения из множества, входящего в определение. Операция называется n-местной (или n-арной), если соответствующая функция зависит от n переменных.

Отношение (172). Связь между элементами одного множества

Отображение (53). Об отображении одного множества в другое говорят в том случае, если каждому элементу первого множества поставлен в соответствие какой-нибудь вполне определенный элемент второго множества. Следовательно, отображение по существу представляет собой функцию. (Это не определение, а лишь пояснение к тому, что такое отображение. В действительности же отображение принадлежит к числу фундаментальных неопределяемых понятий математики.)

Отображение (194). Элемент *категории*.

Пересечение (56, 161). Пересечением *подгрупп* или вообще подмножеств называется подмножество, состоящее из тех и только тех элементов, которые принадлежат каждому из рассматриваемых подмножеств.

Пересечение (165, 173). Пересечение двух (или большего числа) элементов *частично упорядоченного множества* совпадает *с наибольшей нижней гранью* этих элементов.

Перестановка (12). Запись элементов в определенном порядке.

Подгруппа (50). Подмножество *группы*, элементы которого образуют группу относительно исходной *групповой операции*.

Подгруппа, порожденная заданными элементами (57). Наименьшая из *подгрупп*, содержащих заданные элементы.

Подпространство (113). Подмножество векторного пространства, замкнутое относительно операций, заданных во всем векторном пространстве.

Подпространство, порожденное заданными векторами (117). Наименьшее из *подпространств*, содержащих заданные векторы.

Подстановка (13). Любое изменение порядка, в котором расположены элементы.

Подструктура (179). Подмножество *структуры*, которое является структурой относительно операций, заданных на исходной структуре.

Подструктура алгебраическая (191). Подмножество *алгебраической структуры*, замкнутое относительно каждой из операций.

Полугруппа (39). Пара $\langle F; f \rangle$, где f — двухместная *ассоциативная операция*, заданная на множестве F.

Полугруппа отображений (83). Множество *отображений*, элементы которого образуют полугруппу относительно операции *умножения отображений*.

Полугруппа с единицей (84). Полугруппа, в которой существует выделенный относительно *операции единичный элемент*.

Порядок группы (58). Если группа конечна, то ее порядок равен числу элементов группы. В противном случае порядок группы бесконечен.

Порядок элемента (48). Если существуют положительные *степени* элемента группы, совпадающие

с *единичным элементом*, то порядок элемента равен наименьшему из показателей таких степеней. В противном случае порядок элемента группы бесконечен.

Пустое множество (162). Множество, по определению не содержащее ни одного элемента.

Правый R-модуль (130). Понятие, аналогичное левому R-модулю и отличающееся лишь тем, что элементы модуля умножаются на элементы кольца R не слева, а справа.

Правый обратный элемент (39). Элемент *с полугруппы с единицей* называется правым обратным для элемента a, если произведение ac совпадает с *единичным элементом* полугруппы.

Правый смежный класс (60). Если H — *подгруппа* и a — элемент *группы* G, то правым смежным классом Ha называется множество элементов из G вида ax, где $x \in H$.

Представление матрицами (153). *Мономорфизм группы* в группу *невырожденных матриц* с заданным числом элементов.

Представление подстановками (90). *Мономорфизм группы* в группу *подстановок* определенных элементов.

Примарный идеал (184). Идеал в *структуре*, который содержит *пересечение* двух элементов лишь в том случае, если ему принадлежит каждый из этих элементов.

Принцип двойственности (168). Принцип, согласно которому в теории *структур* из любого истинного утверждения при замене *пересечения* объединением, а *объединения* — пересечением получается истинное утверждение.

Произведение комплексов (65). Для подмножеств A и B *полугруппы* произведением комплексов называется множество элементов, представимых в виде ab, где $a \in A$ и $b \in B$.

Произведение отображений (82). Результат последовательного выполнения отображений. Первым, выполняется отображение, входящее в произведение вторым сомножителем. (Порядок выполнения отображений-сомножителей устанавливается определением произведения и может быть обратным.)

Простой элемент (105). Элемент *области целостности*, который делит произведение лишь в том случае, если делит один из сомножителей.

Прямая сумма (127). *Прямое произведение векторных пространств* или *абелевых групп*.

Прямое произведение (170, 181). Прямым произведением групп, структур или других *алгебраических структур* называется конструкция, позволяющая получать группы, структуры или алгебраические структуры. Элементы прямого произведения составляются из элементов исходных структур, а операции выполняются покомпонентно.

Размерность (124). Если *векторное пространство* состоит только из нулевого вектора, то его размерность равна нулю (оно *нульмерно*). Если же векторное пространство состоит не только из нулевого вектора и в нем существует конечный *базис*, то размерность векторного пространства равна числу элементов базиса. Во всех остальных случаях векторное пространство бесконечномерно.

Свободная полугруппа с единицей (87). Полугруппа, состоящая из слов — наборов свободных образующих и пустого слова с *операцией*, состоящей в приписывании одного слова к другому.

Свободная система образующих (87). Заранее заданная система образующих *свободной полугруппы с единицей*, между которыми в *полугруппе* нет никаких соотношений, кроме тех, которые следуют из *аксиом*, определяющих полугруппу.

Сепарабельность (187). Свойство *дистрибутивных структур*, состоящее в том, что для любых двух элементов можно указать *примарный идеал*, содержащий лишь один из них.

Система образующих (57, 117). Подмножество *группы* (или *векторного*

пространства), элементы которого порождают *подгруппу* (или *подпространство*), совпадающее со всей группой (всем векторным пространством).

Скаляр (112). В случае *векторного пространства* заданными *телом* скалярами называются элементы тела.

Сложение в кольце (95). *Операция* в кольце, относительно которой элементы кольца образуют *коммутативную группу*.

Степень (24). В теории *групп* или *полугрупп* степенью называется произведение, в которое сомножителями входят либо данный элемент, либо обратный ему элемент, либо единичный элемент.

Структура (167). Тройка $\langle H; \cap, \cup \rangle$, где $\cup$ и $\cap$ — заданные на множестве H *идемпотентные*, *коммутативные* и *ассоциативные* двухместные операции, для которых выполняются *законы поглощения*.

Тело (96). *Кольцо*, в котором для всех элементов, отличных от *нулевого*, существуют *обратные элементы*.

Теорема Лагранжа (61). Теорема, утверждающая, что *порядок подгруппы конечной группы* является делителем порядка группы.

Теорема Кэли (90). Теорема, утверждающая, что всякую *группу* можно *представить* при помощи *подстановок*.

Теорема Стоуна (187). Теорема, утверждающая, что для всякой дистрибутивной структуры существует *мономорфизм*, отображающий эту структуру в множество всех ее подмножеств и переводящий *дополнение* в дополнение.

Тождественное отображение (55). *Отображение*, при котором каждый элемент множества переходит в себя.

Тождественная подстановка (17). *Подстановка*, при которой каждый элемент переходит в себя.

Тождественное преобразование (33). *Движение*, при котором каждый элемент переходит в себя.

Транспозиция (25). *Цикл длины* 2.

Тривиальная подгруппа (52). *Подгруппа группы* называется тривиальной, если она либо состоит только из *единичного элемента*, либо совпадает со всей группой.

Тривиальное подпространство (114). Подпространство векторного пространства называется тривиальным, если оно либо состоит только из нулевого вектора, либо совпадает со всем *векторным пространством*.

Тривиальная линейная комбинация (113). *Линейная комбинация* элементов *векторного пространства*, в которую все векторы входят умноженными на нулевой *скаляр*.

Умножение (15). Общее название *операции* в *группах* или *полугруппах*.

Умножение в кольце (95). *Операция* в *кольце*, относительно которой элементы кольца образуют *полугруппу*.

Упорядоченное множество (172). Множество, на котором определено *отношение* $\leqslant$. Это отношение порядка рефлексивно ($a \leqslant a$), антисимметрично (если $a \leqslant b$ и $b \leqslant a$, то $a = b$), трихотомично (для любых двух элементов a и b заведомо выполняется одно из отношений $a \leqslant b$ или $b \leqslant a$) и транзитивно (если $a \leqslant b$ и $b \leqslant c$, то $a \leqslant c$).

Фактор-группа (67). *Группа*, образуемая (*левыми*) *смежными классами* по *нормальному делителю* относительно умножения комплексов (см. *произведение комплексов*.)

Цикл (22). Циклическая подстановка.

Циклическая группа (58). Группа, *система образующих* которой состоит из одного элемента.

Циклическая подстановка (22). Подстановка, переводящая каждый из записанных в подходящем порядке элементов в следующий, а последний элемент — в первый.

Частичная алгебраическая структура (193). *Алгебраическая структура*, на которой определена частичная операция.

Частичная операция (170). Операция, определенная не на всех элементах (парах элементов) мно-

жества, входящего в *алгебраическую структуру*.

Частично упорядоченное множество (172). Множество, на котором задано отношение $\leqslant$, не обладающее в отличие от *упорядоченного множества* свойством трихотомичности.

Четная подстановка (27). *Подстановка*, допускающая разложение в четное число *транспозиций*.

Элемент бесконечного порядка (48). Элемент *группы* или *полугруппы* с единицей, все *степени* которого различны.

Элемент группы (37). Элементом группы $\langle G; f \rangle$ называется элемент множества G.

Эндоморфизм (83). *Гомоморфное отображение* группы (или любой другой *алгебраической структуры*) на себя.

Эпиморфизм (76). Гомоморфное отображение *группы* G_1 (или любой другой *алгебраической структуры* S_1) в группу G_2 (в алгебраическую структуру S_2), при котором для каждого элемента из G_2 (из S_2) существует прообраз.

Э. Фрид

ЭЛЕМЕНТАРНОЕ ВВЕДЕНИЕ
В АБСТРАКТНУЮ АЛГЕБРУ

Научный редактор А. Г. Белевцева
Мл. научный редактор Л. И. Леонова
Художник Л. М. Муратова
Художественный редактор Л. Е. Безрученков
Технический редактор В. П. Сизова
Корректор Н. И. Варанова

ИБ № 1633

Сдано в набор 10.01.79. Подписано и печати 14.08.79. Формат $70\times100^1/_{16}$. Бумага кн.-журн. Гарнитура обыкновенная. Печать высокая. Объем 8,25 бум. л. Усл. печ. л. 21,45. Уч.-изд. л. 21,20. Изд. № 12/9868. Тираж 75.000 экз. Зак. 35. Цена 1 р.50 к.

Издательство «Мир»
Москва, 1-й Рижский пер., 2.

Ярославский полиграфкомбинат Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. 150014. Ярославль, ул. Свободы, 97.