Ф. Л. Варпаховский, А. С. Солодовников,
И. В. Стеллецкий

АЛГЕБРА

Группы, кольца, поля.
Бекторные и евклидовы
пространства.
Линейные отображения

Министерство просвещения РСФСР

Московский государственный заочный
педагогический институт

Ф. Л. Варпаховский, А. С. Солодовников,
И. В. Стеллецкий

АЛГЕБРА
Группы, кольца, поля. Векторные и евклидовы пространства. Линейные отображения

Учебное пособие для студентов-заочников
I курса физико-математических факультетов
педагогических институтов

МОСКВА «ПРОСВЕЩЕНИЕ» 1978

Рекомендовано к печати Главным управлением
высших и средних педагогических учебных заведений
Министерства просвещения РСФСР

Ответственный редактор *Ф. Л. Варпаховский*
Рецензенты: доктор физико-математических наук *Н. Я. Виленкин*,
доктор физико-математических наук *М. М. Глухов*,
кандидат физико-математических наук *Г. В. Дорофеев*

ИБ № 3195

АЛГЕБРА

Группы, кольца, поля. Векторные и евклидовы пространства. Линейные отображения

Редактор *Т. П. Руженская*. Художественный редактор *К. К. Федоров*. Технический редактор *Р. С. Еникеева*. Корректоры *Т. Ф. Алексина, Т. А. Кузнецова*.

Сдано в набор 04.05.77г. Подписано к печати 08.08.78г. $60\times90^1/_{16}$. Бумага тип. № 3. Гарн. Лит. Печать высокая. Усл. печ. л. 9,0. Уч.-изд. л. 8,10. Тираж 35 000 экз. Заказ № 6153. Цена 30 к.

Ордена Трудового Красного Знамени издательство «Просвещение» Государственного комитета Совета Министров РСФСР по делам издательств, полиграфии и книжной торговли. Москва, 3-й проезд Марьиной рощи, 41.

Отпечатано с матриц книжной фабрики им. М. В. Фрунзе Республиканского производственного объединения «Полиграфкнига» Госкомиздата в областной типографии управления издательств, полиграфии и книжной торговли Ивановского облисполкома, 153008, г. Иваново, ул. Типографская, 6.

В $\frac{60602—295}{103(03)—78}$ заказное

ПРЕДИСЛОВИЕ

На рубеже XIX и XX столетий алгебра претерпела важное качественное изменение, которое можно охарактеризовать как переход к изучению *абстрактных* систем объектов. До этого момента основное внимание уделялось в алгебре конкретным системам, таким как различные числовые системы, системы матриц, перестановок и т. п. Новый этап в развитии алгебры ознаменовался полным отвлечением от природы и способов построения объектов системы, и единственным предметом изучения стали *отношения* между этими объектами. Современная алгебра имеет дело просто с системами объектов, для которых определены некоторые операции и отношения, удовлетворяющие тем или иным требованиям; что именно стоит за объектами системы — матрицы, уравнения, числа и т. д.— для алгебры безразлично, важно только, чтобы заданные операции и отношения были определены и заданные требования для этих операций и отношений выполнялись.

Данная книга представляет собой по замыслу элементарное введение в теорию важнейших алгебраических систем и построена в точном соответствии с действующей программой по алгебре для педагогических институтов. Она посвящена группам и кольцам (в частности, полям), линейным пространствам и линейным отображениям.

Книга является учебником по второй части курса «Алгебра и теория чисел» и служит продолжением учебника Ф. Л. Варпаховского и А. С. Солодовникова по первой части.* Авторы сочли оправданным не ссылаться на какие-либо другие пособия, ссылки же на первую часть даются сокращенно: Алгебра, ч. I, номер страницы. В книге принят тот же способ подразделения материала, что и в первой части: главы разбиты на параграфы, а параграфы — на пункты. Вопросы и упражнения приводятся либо в конце параграфов, либо в конце отдельных пунктов. Они предназначены для самоконтроля и должны способствовать активному усвоению теории, но никоим образом не заменяют задачника. Читатель должен помнить, что только решение достаточного количества задач служит гарантией успешного овладения курсом.

Глава I написана Ф. Л. Варпаховским и И. В. Стеллецким, главы II, III и IV — А. С. Солодовниковым.

Авторы выражают искреннюю признательность рецензентам книги Н. Я. Виленкину, М. М. Глухову и Г. В. Дорофееву. Сделанные ими замечания были учтены в окончательной редакции рукописи.

---

* Варпаховский Ф. Л., Солодовников А. С. Алгебра, М. «Просвещение», 1974.

Глава I

ГРУППЫ, КОЛЬЦА, ПОЛЯ

§ 1. Операции и алгебраические системы

1. Операции. Простейшие операции над числами известны из арифметики. К ним относятся, например, операции сложения, умножения и вычитания. Общая черта, объединяющая эти арифметические операции, состоит в следующем: каждая из них любой паре чисел сопоставляет определенное третье число (соответственно сумму, произведение или разность). При этом в случае операции вычитания разность двух неравных чисел зависит не только от самих этих чисел, но и от того, какое из них является уменьшаемым, а какое — вычитаемым. Иными словами, результат операции над числами зависит, вообще говоря, не только от того, *к каким числам* применяется данная операция, но и от *порядка*, в котором эти числа берутся.

Таким образом, арифметические операции применяются к *упорядоченным* парам чисел, и всякая такая операция представляет собой отображение, соотносящее каждой упорядоченной паре чисел некоторое определенное третье число.

В первой части курса изучались операции сложения арифметических векторов и умножения квадратных матриц. Эти операции производятся не над числами, а над объектами иной природы. Вместе с тем каждую из них также можно рассматривать как отображение, а именно как отображение, сопоставляющее любой упорядоченной паре элементов некоторого множества определенный третий элемент того же множества.

По существу мы пришли к интересующему нас определению операции. С целью придать этому определению законченный и удобный вид, воспользуемся понятиями кортежа и декартова произведения. Напомним, что упорядоченный набор из n элементов $a_1, a_2,\ldots,a_n$ некоторого множества A называется кортежем длины n (обозначается символом $\langle a_1,a_2,\ldots,a_n\rangle$), а множество всех таких кортежей — n-й декартовой степенью множества A (обозначается символом A^n)*.

Введем теперь следующее основное определение:

Операцией на множестве A называется отображение, сопоставляющее каждому кортежу $\langle a_1,a_2\rangle$ из A^2** определенный элемент

---

* См.: Алгебра, ч. 1, с. 15—17.

** Иногда используется обозначение A_2, в частности в Алгебре, 4. 1.

a из A; сам элемент a называют при этом *результатом применения операции к кортежу* $\langle a_1, a_2\rangle$ или *композицией элементов* a_1, a_2.

Заметим сразу же, что в силу данного здесь определения понятие операции оказывается частным случаем понятия функции. Именно операция на множестве A представляет собой всюду определенную на A функцию двух переменных со значениями из A.

Сложение, умножение и вычитание можно рассматривать как операции на множестве $\mathbf{R}$ действительных чисел. Умножение квадратных матриц заданного порядка n представляет собой операцию на множестве всех квадратных матриц порядка n. Другими примерами служат операция векторного произведения на множестве векторов трехмерного пространства и операция возведения в степень на множестве $\mathbf{Z}^+$ целых положительных чисел.

Для обозначения операций будем пользоваться символами $\bigcirc$, $\times$ или какими-нибудь специальными символами, например знаками сложения и умножения. Результат применения операции к кортежу $\langle a_1, a_2\rangle$ будем записывать соответственно в виде $a_1 \bigcirc a_2$, $a_1 \times a_2$, $a_1 + a_2$, $a_1 a_2$.

Определенную нами операцию часто называют *двухместной* или *бинарной*, поскольку иногда приходится рассматривать и другие операции: одноместные, трехместные и т. д. Вообще, под *n-местной операцией на множестве A* понимается отображение, сопоставляющее каждому кортежу $\langle a_1, a_2, \ldots, a_n\rangle$ из A определенный элемент a из A. Скажем, операция транспонирования является одноместной операцией на множестве квадратных матриц какого-нибудь заданного порядка n — любой (одной) матрице ставится в соответствие транспонированная к ней матрица.

В дальнейшем будут изучаться почти исключительно двухместные операции и термин «операция» будет относиться только к ним. Другие случаи будут специально оговариваться.

Понятие операции допускает ряд обобщений. Одним из них как раз и является понятие n-местной операции, т. е. операции с *любым* конечным числом аргументов. Другое обобщение получается, если не требовать, чтобы результат операции, заданной на некотором множестве, принадлежал тому же самому множеству. Наконец, можно отказаться и от требования *всюду определенности* операции, т. е. считать, что отображение задано не для всех кортежей из A^n, а только для некоторых из них. Учитывая сказанное, мы сформулируем следующее общее определение операции:

Пусть A и B — какие-нибудь множества, n — целое положительное число и K — некоторое подмножество кортежей из A^n: $K \subset A^n$. *Частичной n-местной операцией на A* называется отображение, сопоставляющее каждому кортежу $\langle a_1, a_2, \ldots, a_n\rangle \in K$ определенный элемент $b \in B$.

Приведенное ранее определение получается из данного при $n = 2$: $B \subset A$ и $K = A^n$. Поэтому все операции в рассмотренных выше примерах удовлетворяют и новому определению. Вместе с тем новое определение охватывает и некоторые другие примеры. Так, операция деления на множестве $\mathbf{R}$ действительных чисел является двухместной частичной операцией; эта операция не определена, когда делителем является число 0, поэтому «область определения» K для операции деления получается удалением из $\mathbf{R}^2$ всех кортежей вида $\langle a, 0\rangle$. Операция скалярного произведения на множестве

векторов трехмерного пространства также удовлетворяет определению n-местной частичной операции; здесь каждой паре векторов сопоставляется не вектор, а действительное число, т. е. элемент другого множества.

2. Алгебраические системы. Гомоморфные и изоморфные отображения систем. Обычно в алгебре изучаются множества, на которых определены те или иные операции. Рассматриваются множества с одной, с двумя и вообще с любым конечным числом операций. Не исключается и случай, когда на множестве задано бесконечно много операций.

Введем следующее определение:

Всякое множество с заданными в нем операциями будем называть *алгебраической системой*.

Множество **R** действительных чисел с операциями умножения, сложения и вычитания; множество n-мерных арифметических векторов с операцией сложения; множество квадратных матриц заданного порядка с операциями сложения и умножения матриц — все это различные примеры алгебраических систем. Список таких примеров можно было бы легко продолжить.

Замечание. В определении алгебраической системы под операцией в соответствии с принятым соглашением понимается двухместная операция. Более широкое толкование понятия системы получается, если допустить также и произвольные n-местные операции. Алгебраической системой в этом широком смысле будет, например, множество целых положительных чисел с одноместной операцией прибавления единицы. Другой, более содержательный пример такой системы дает множество n-мерных арифметических векторов с одной (двухместной) операцией сложения векторов и бесконечным множеством одноместных операций умножения вектора на число: каждому действительному числу λ ставится в соответствие одноместная операция, которая любому вектору $\boldsymbol{a}$ сопоставляет вектор $\lambda\boldsymbol{a}$.

Одной из задач алгебры является изучение различных алгебраических систем. В частности, в этой книге будут рассмотрены некоторые наиболее важные типы таких систем: группы, кольца, поля, векторные пространства.

При изучении какой-либо алгебраической системы часто бывает удобно сравнить ее с некоторой уже известной системой — такое сравнение позволяет иногда по свойствам известной системы сделать ряд заключений о свойствах исследуемой системы. Для плодотворного сравнения двух систем необходимо только, чтобы операции в этих системах были определенным образом согласованы. Введем ряд определений.

Пусть имеются две системы: множество A с некоторыми операциями (система I) и множество A' с некоторыми операциями (система II). Будем говорить, что *задано отображение системы I на систему II*, если указано отображение множества A на множество A' и если операциям на A взаимно однозначно сопоставлены операции на A'.

Как это обычно принято, отображение множества A на множество A' будем обозначать какой-нибудь буквой, например буквой φ; при этом элемент a', соответствующий элементу a (образ эле-

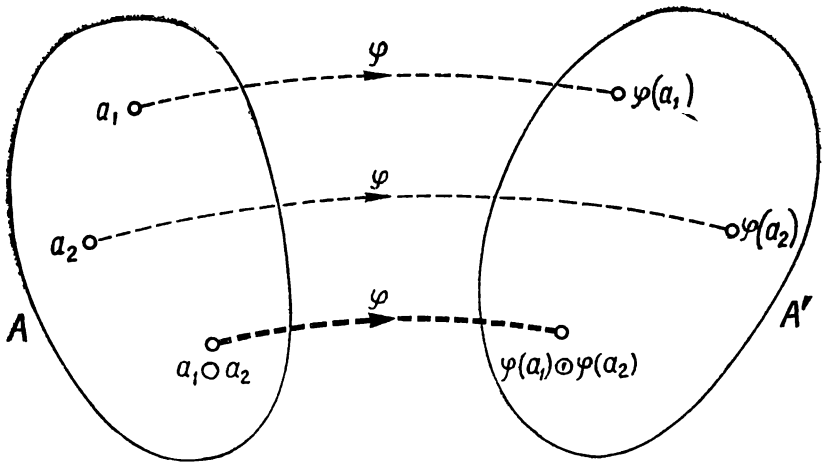

Рис. 1

мента a), обозначается символом $\varphi(a)$. Наряду с записью $a' = \varphi(a)$ пользуются записью $a \xrightarrow{\varphi} a'$ или сокращенно $a \to a'$.

Говорят, что отображение φ *сохраняет операции*, если для любых двух соответствующих друг другу операций — операции $\circ$ на A и операции $\odot$ на A' — выполняется условие:

$$\varphi(a_1 \circ a_2) = \varphi(a_1) \odot \varphi(a_2). \qquad (1)$$

Иными словами, отображение сохраняет операции, если для любых двух сопоставленных друг другу операций $\circ$ и $\odot$ из соотношений

$$a_1 \to a'_1 \qquad \text{и} \qquad a_2 \to a'_2$$

вытекает, что

$$a_1 \circ a_2 \to a'_1 \odot a'_2.$$

Содержание условия (1) можно раскрыть и несколько иначе. Пусть какие-нибудь три элемента a_1, a_2, a_3 множества A связаны соотношением

$$a_1 \circ a_2 = a_3. \qquad (2)$$

Тогда $\varphi(a_1 \circ a_2) = \varphi(a_3)$ и в силу условия (1) получаем:

$$\varphi(a_1) \odot \varphi(a_2) = \varphi(a_3). \qquad (2')$$

Таким образом, всякое равенство вида (2) сохраняется, если элементы множества A заменить в нем их образами, а операцию соответствующей ей операцией $\odot$ (отсюда, кстати, и сам термин «сохранение операций»).

Условие сохранения операций иллюстрируется схематическим рисунком 1. Линии со стрелками ведут от элементов A к их образам в A'. Поскольку образами элементов a_1, a_2 служат элементы a'_1, a'_2, то в силу условия сохранения операций образом элемента $a_1 \circ a_2$ является элемент $a'_1 \odot a'_2$ (выделенная линия на рисунке).

Отображение системы I на систему II, сохраняющее операции, называют *гомоморфным** (или *гомоморфизмом*); при этом говорят, что система II является *гомоморфным образом* системы I (или что она гомоморфна системе I).

В качестве примера рассмотрим следующие две системы: множество **Z** целых чисел с операцией сложения и множество $\{-1,1\}$ с операцией умножения. Пусть множество **Z** отображается на множество $\{-1,1\}$ по правилу: каждое четное число отображается в число 1 ($2n \to 1$), а каждое нечетное число — в число -1 ($2n + 1 \to -1$). Сопоставив друг другу операции сложения на **Z** и умножения на множестве $\{-1,1\}$, мы получим отображение первой системы на вторую. Убедимся, что это отображение сохраняет операцию. Для этого надо проверить, что если

$$a_1 \to a_1', \quad a_2 \to a_2',$$

то

$$a_1 + a_2 \to a_1' a_2'.$$

Допустим сначала, что числа a_1 и a_2 имеют одинаковую четность. Тогда их сумма четна, поэтому $a_1 + a_2 \to 1$. С другой стороны, числа a_1', a_2' имеют в этом случае одинаковые знаки, так что $a_1' a_2' = 1$ и, значит, $a_1 + a_2 \to a_1' a_2'$. Аналогично рассматривается случай, когда числа a_1, a_2 разной четности (разбор этого случая предоставляется читателю). Следовательно, построенное отображение является гомоморфизмом.

Отметим, что при гомоморфном отображении системы I на систему II некоторые утверждения о системе I сохраняют силу и для системы II. В частности, всякое равенство, связывающее элементы и операции системы I, сохраняется, если заменить эти элементы и операции соответствующими элементами и операциями системы II.

Особо важным является тот частный случай гомоморфизма, когда отображение множества A на множество A' взаимно однозначно.** Введем в связи с этим следующее определение.

Гомоморфное отображение системы I на систему II, при котором множество A первой системы отображается на множество A' второй системы взаимно однозначно, называется *изоморфным* (или *изоморфизмом*)***; о системе II говорят при этом, что она *изоморфна* системе I.

Замечание. Как известно, для взаимно однозначного отображения φ множества A на множество A' существует взаимно однозначное обратное отображение φ^{-1} (множества A' на мно-

---

* Термин «гомоморфный» означает в переводе с латинского «подобный по форме (строению, структуре)».

** Напомним, что отображение множества A на множество A' называется *взаимно однозначным*, когда *разные* элементы из A отображаются на *разные* элементы из A'.

*** Термин «изоморфный» означает в переводе с латинского «одинаковый по форме (строению, структуре)».

жество A), определяемое условием: $\varphi^{-1}(a') = a$, тогда и только тогда, когда $\varphi(a) = a'$. Нетрудно показать, что если отображение φ сохраняет операции, то и обратное отображение φ^{-1} также сохраняет операции. Действительно, пусть для произвольных элементов a'_1, a'_2 из A'

$$\varphi^{-1}(a'_1) = a_1 \text{ и } \varphi^{-1}(a'_2) = a_2.$$

Тогда

$$\varphi(a_1) = a'_1 \text{ и } \varphi(a_2) = a'_2,$$

и в силу сохранения операции при отображении φ

$$\varphi(a_1 \circ a_2) = a'_1 \odot a'_2.$$

Отсюда

$$\varphi^{-1}(a'_1 \odot a'_2) = a_1 \circ a_2 = \varphi^{-1}(a'_1) \circ \varphi^{-1}(a'_2),$$

что и требовалось доказать.

Таким образом, из существования изоморфного отображения системы I на систему II вытекает существование изоморфного отображения системы II на систему I. Следовательно, отношение изоморфизма симметрично. Учитывая это, говорят просто, что системы I и II *изоморфны*.

Рассмотрим, например, такие две системы: множество $\mathbf{R}^+$ положительных действительных чисел с операцией умножения и множество $\mathbf{R}$ всех действительных чисел с операцией сложения. Зададим отображение φ множества $\mathbf{R}^+$ на множество $\mathbf{R}$ следующим правилом: $\varphi(a) = \lg a$. Далее сопоставим друг другу операции умножения на $\mathbf{R}^+$ и сложения на $\mathbf{R}$. Отображение φ будет взаимно однозначным в силу монотонности и непрерывности логарифмической функции. Покажем, что оно сохраняет операцию. В самом деле,

$$\varphi(a_1 \cdot a_2) = \lg(a_1 \cdot a_2) = \lg a_1 + \lg a_2 = \varphi(a_1) + \varphi(a_2).$$

Таким образом, условие (1) выполнено, и рассматриваемые системы изоморфны.

Приведем еще один пример изоморфных алгебраических систем. Первую систему определим как множество $\mathbf{R}$ действительных чисел с операцией сложения, а вторую — как множество M всех матриц вида

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

(a — любое действительное число) с операцией сложения матриц. Зададим отображение φ множества $\mathbf{R}$ на множество M, полагая для любого $a \in \mathbf{R}$

$$\varphi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},$$

и сопоставим друг другу операции сложения на множествах $\mathbf{R}$ и M.

Отображение φ взаимно однозначно, поскольку разным числам соответствуют разные матрицы. Не менее очевиден факт сохранения операции:

$$\varphi(a+b)=\begin{pmatrix} a+b & 0 \\ 0 & a+b \end{pmatrix}=\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}+\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}=\varphi(a)+\varphi(b).$$

Таким образом, данные системы изоморфны.

Этот пример особенно ясно показывает, что изоморфные системы отличаются лишь такими признаками, которые связаны с *конкретной природой* элементов и операций. Во всем остальном изоморфные системы неразличимы — любое утверждение, которое формулируется только с помощью равенств, связывающих элементы и операции, истинно или ложно *одновременно* для каждой из двух изоморфных систем. Рассмотрим, например, утверждение: «В системе с одной операцией имеется такой элемент a_0, что композиция произвольного элемента a и элемента a_0 равна элементу a». Это утверждение истинно для каждой из двух систем последнего примера, поскольку

$$a+0=a \text{ и } \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}+\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

В алгебре обычно не интересуются конкретными способами задания систем и поэтому *изоморфные системы считают тождественными.*

Понятие изоморфизма мы распространим в дальнейшем на некоторые более общие системы. Относящиеся сюда определения будут сформулированы при изучении соответствующих систем.

Вопросы и упражнения

1. Даны две системы: множество $\mathbf{Z}$ целых чисел с операцией умножения и конечное множество $\{-1, 0, 1\}$ также с операцией умножения. Поставим в соответствие каждому целому положительному числу число 1, каждому отрицательному числу — число —1, числу 0 — число 0. Доказать, что построенное отображение является гомоморфизмом.

2. Доказать, что множество $\mathbf{R}$ действительных чисел с операциями сложения и умножения и множество матриц вида

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

с операциями сложения и умножения матриц являются изоморфными алгебраическими системами.

3. Показать, что система положительных чисел с операцией сложения не изоморфна системе неотрицательных чисел с операцией сложения.

§ 2. Некоторые классы операций

1. Коммутативные и ассоциативные операции. Мы рассмотрим некоторые наиболее важные классы операций, выделяя каждый класс с помощью тех или иных свойств, которыми обладают операции этого класса. Начнем со свойства *коммутативности (перестановочности)*.

Операция на множестве A называется *коммутативной*, если для любых двух элементов a_1, a_2 из A выполняется условие:

$$a_1 \circ a_2 = a_2 \circ a_1.$$

Например, операции сложения и умножения на множестве $\mathbf{R}$ коммутативны, а операция вычитания нет. Операция на множестве $\mathbf{Z}^+$ целых положительных чисел, задаваемая формулой

$$m \circ n = m^n,$$

некоммутативна (например, $3 \circ 2 = 3^2 = 9$, $2 \circ 3 = 2^3 = 8$).

Замечание. Согласно определению операция коммутативна, если условие $a_1 \circ a_2 = a_2 \circ a_1$ выполняется для *любых* двух элементов a_1, a_2. Значит, чтобы убедиться в некоммутативности операции, достаточно указать только одну пару «неперестановочных» элементов. Разумеется, какие-то другие элементы могут оказаться и перестановочными (так, в примере $4 \circ 2 = 4^2 = 2^4 = 2 \circ 4$).

Следующим важным свойством операций является свойство *ассоциативности (сочетательности)*.

Операция на множестве A называется *ассоциативной*, если для любых трех элементов a_1, a_2, a_3 из A выполняется равенство

$$(a_1 \circ a_2) \circ a_3 = a_1 \circ (a_2 \circ a_3).$$

Например, операции сложения и умножения на множестве $\mathbf{R}$ ассоциативны, тогда как операция на $\mathbf{Z}^+$, задаваемая формулой $m \circ n = m^n$, не является ассоциативной: скажем, $(2 \circ 1) \circ 3 = (2^1)^3 = 8$, а $2 \circ (1 \circ 3) = 2^{(1^3)} = 2$.

Заметим, что выражения $(a_1 \circ a_2) \circ a_3$ и $a_1 \circ (a_2 \circ a_3)$ в определении ассоциативной операции обозначают две различные «комбинации», которые можно составить из кортежа $\langle a_1, a_2, a_3 \rangle$ с помощью последовательных применений двухместной операции; другими словами, эти выражения задают два способа применения операции к кортежу длины три. Точно так же можно говорить о различных способах применения операции к кортежу любой длины больше двух. Например, для кортежа $\langle a_1, a_2, a_3, a_4 \rangle$ длины четыре получаются следующие пять способов:

$$(a_1 \circ a_2) \circ (a_3 \circ a_4);$$
$$(a_1 \circ (a_2 \circ a_3)) \circ a_4;$$
$$((a_1 \circ a_2) \circ a_3) \circ a_4;$$
$$a_1 \circ ((a_2 \circ a_3) \circ a_4);$$
$$a_1 \circ (a_2 \circ (a_3 \circ a_4)).$$

Вообще всякий способ применения операции к кортежу длины $n > 2$ задается подходящей расстановкой скобок — этим определяется процесс из ряда «шагов», где каждый шаг состоит в применении операции только к двум элементам множества.

Возникает естественный вопрос: при каком условии результаты различных применений операции к одному и тому же кортежу совпадают? Оказывается, таким условием как раз и является ассоциативность операции. Именно, справедлива следующая теорема:

Т е о р е м а. *Результаты применения ассоциативной операции к какому угодно кортежу* $\langle a_1, a_2, \ldots, a_n\rangle$ (*при* $n \geqslant 3$) *совпадают для любых двух способов расстановки скобок.*

В силу этой теоремы результат применения ассоциативной операции к кортежу $\langle a_1, a_2, \ldots, a_n\rangle$ можно обозначить просто символом $a_1 \bigcirc a_2 \bigcirc \ldots \bigcirc a_n$—, не указывая никакого конкретного способа расстановки скобок. Например, для операции сложения на множестве **R** запись $a_1 + a_2 + a_3 + a_4$ означает любую из сумм $(a_1 + (a_2 + a_3)) + a_4$, $(a_1 + a_2) + (a_3 + a_4)$ и т. д.— во всех случаях сумма будет одной и той же.

Приведем доказательство сформулированной теоремы. Будем пользоваться индукцией по n. При $n = 3$ имеется только два способа расстановки скобок, и доказываемое утверждение совпадает с требованием ассоциативности.

Пусть далее теорема верна для всех кортежей, длина которых меньше n. Докажем, что она верна и для кортежей длины n. Рассмотрим какие-нибудь два способа расстановки скобок, которые мы представим в следующем виде:

$$(a_1 \bigcirc \ldots \bigcirc a_l) \bigcirc (a_{l+1} \bigcirc \ldots \bigcirc a_n),$$
$$(a_1 \bigcirc \ldots \bigcirc a_k) \bigcirc (a_{k+1} \bigcirc \ldots \bigcirc a_n)$$

(«внутренние» скобки не указываются — их можно расставлять как угодно в силу предположения индукции).

Достаточно, очевидно, ограничиться рассмотрением случая $k \neq l$. Положим для определенности $k < l$. Тогда, снова пользуясь предположением индукции, можно представить результаты применения операции к кортежу $\langle a_1, a_2, \ldots, a_n\rangle$ по первому и второму способам, соответственно как

$$((a_1 \bigcirc \ldots \bigcirc a_k) \bigcirc (a_{k+1} \bigcirc \ldots \bigcirc a_l)) \bigcirc (a_{l+1} \bigcirc \ldots \bigcirc a_n)$$

и

$$(a_1 \bigcirc \ldots \bigcirc a_k) \bigcirc ((a_{k+1} \bigcirc \ldots \bigcirc a_l) \bigcirc (a_{l+1} \bigcirc \ldots \bigcirc a_n)).$$

Совпадение этих результатов вытекает опять-таки из требования ассоциативности. Доказательство закончено.

Вопросы и упражнения

1. Проверить, что операция матричного умножения на множестве квадратных матриц второго порядка ассоциативна, но не коммутативна.

2. Доказать, что бинарная операция на множестве **R** действительных чисел, задаваемая формулой

$$a \bigcirc b = (a + b)^2,$$

является коммутативной, но не ассоциативной.

3. Пусть $B \subset A$ и каждый элемент из A можно представить в виде композиции некоторых элементов из B. Показать, что если условие коммутативности (ассоциативности) выполняется для любых элементов из B, то операция на A будет коммутативной (ассоциативной).

2. **Нейтральные и обратные элементы. Обратимые операции.** Пусть на множестве A задана бинарная операция. Если найдется такой элемент $e \in A$, что для *любого* элемента $a \in A$ выполняются равенства:

$$e \bigcirc a = a \text{ и } a \bigcirc e = a,$$

то элемент e называется *нейтральным* относительно данной операции.

Например, число 1 является нейтральным элементом множества $\mathbf{R}$ относительно операции умножения, а нулевая матрица второго порядка — нейтральным элементом множества всех матриц второго порядка относительно операции сложения матриц. С другой стороны, множество $\mathbf{Z}^+$ целых положительных чисел не имеет нейтрального элемента относительно операции, задаваемой формулой $m \bigcirc n = m^n$, в противном случае для некоторого числа $e \in \mathbf{Z}^+$ и любого числа $a \in \mathbf{Z}^+$ выполнялись бы равенства: $m^e = m$ и $e^m = m$, что невозможно.

Эти примеры показывают, что может существовать один нейтральный элемент и что нейтрального элемента может не быть вовсе. Оказывается, что других возможностей нет, т. е. не может существовать *более одного* нейтрального элемента. В самом деле, если бы нашлось два нейтральных элемента e_1 и e_2, то получилось бы, что $e_1 \bigcirc e_2 = e_1$ (так как e_2— нейтральный элемент) и $e_1 \bigcirc e_2 = e_2$ (так как e_1— нейтральный элемент), откуда $e_1 = e_2$.

Пусть теперь множество A содержит нейтральный элемент e относительно некоторой бинарной операции. Будем говорить, что элемент b является *обратным* для элемента a, если выполняются равенства:

$$a \bigcirc b = e \text{ и } b \bigcirc a = e.$$

Из определения сразу же следует, что если элемент b является обратным для a, то элемент a будет обратным для b. Нетрудно видеть также, что нейтральный элемент e является обратным самому себе и что он не имеет никаких других обратных элементов.

Рассмотрим некоторые примеры. В случае операции умножения на множестве $\mathbf{R}$ (нейтральным элементом является число 1) обратным для любого отличного от нуля числа a будет число $a^{-1} = \frac{1}{a}$, и только оно. Число же 0 не имеет обратного (ни для какого числа b равенство $0 \cdot b = 1$ не выполняется). Если операцию умножения рассматривать только на множестве положительных действительных чисел $\mathbf{R}^+$, то все элементы будут иметь ровно по одному обратному. Множество $\mathbf{R}$ с операцией сложения (нейтральным элементом бу-

дет число 0) является системой, в которой каждый элемент a имеет ровно один обратный элемент, равный $-a$: $a + (-a) = (-a) + a = 0$. На множестве квадратных матриц второго порядка с операцией матричного умножения (нейтральным элементом будет единичная матрица) для каждой невырожденной матрицы A существует единственный обратный элемент — матрица A^{-1}, так как $AA^{-1} = A^{-1}A = E$; но никакая вырожденная матрица не обладает обратным элементом (см.: Алгебра, ч. 1, с. 121).

Итак, некоторые элементы (включая обязательно нейтральный элемент) обладают обратными, но могут существовать и элементы, не имеющие обратных. Остается выяснить вопрос: может ли какой-нибудь элемент обладать несколькими обратными? В рассмотренных примерах все элементы имели не более одного обратного, и это обстоятельство не случайно, так как справедливо следующее утверждение:

Если операция ассоциативна, то никакой элемент не может иметь более одного обратного.

Действительно, пусть два элемента b_1 и b_2 являются обратными для элемента a. Тогда $a \bigcirc b_1 = b_1 \bigcirc a = e$ и $a \bigcirc b_2 = b_2 \bigcirc a = e$. Отсюда последовательно получаем:

$$\begin{gathered} a \bigcirc b_1 = a \bigcirc b_2, \\ b_1 \bigcirc (a \bigcirc b_1) = b_1 \bigcirc (a \bigcirc b_2), \\ (b_1 \bigcirc a) \bigcirc b_1 = (b_1 \bigcirc a) \bigcirc b_2, \\ e \bigcirc b_1 = e \bigcirc b_2, \\ b_1 = b_2. \end{gathered}$$

С понятием обратного элемента тесно связано понятие обратимой операции. Операция на множестве A называется *обратимой*, если для каких угодно элементов a, b из A каждое из уравнений

$$a \bigcirc x = b$$

и

$$x \bigcirc a = b$$

имеет одно и только одно решение.

Например, операция сложения на множестве $\mathbf{R}$ всех действительных чисел (а также на множестве $\mathbf{Q}$ всех рациональных чисел или на множестве $\mathbf{Z}$ всех целых чисел) обратима, а на множестве целых неотрицательных чисел необратима (если $a > 0$, то уравнение $a + x = 0$ не имеет целого неотрицательного решения). Операция умножения обратима на множестве $\mathbf{R}^+$, но необратима на множестве $\mathbf{R}$ (ввиду неразрешимости уравнения $0 \cdot x = 1$). Операция матричного умножения на множестве квадратных матриц второго порядка необратима, так как уравнение $AX = B$ неразрешимо в случае, когда матрица A вырожденная, а матрица B невырожденная (если бы матрица C удовлетворяла этому уравнению, то определители $|AC|$ и $|B|$ были бы равны, но $|AC| = |A| \cdot |C| = 0 \cdot |C| = 0$, тогда как $|B| \neq 0$).

Следующая теорема устанавливает связь между существованием обратных элементов и обратимостью операции.

Т е о р е м а. *Ассоциативная операция на множестве A обратима тогда и только тогда, когда в A существует нейтральный элемент и для любого элемента из A существует обратный ему элемент.*

Д о к а з а т е л ь с т в о. 1. Пусть ассоциативная операция обратима. Нужно показать, что существует нейтральный элемент e и что для каждого элемента a найдется такой элемент b, который удовлетворяет равенствам: $a \circ b = b \circ a = e$.

Выберем какой-нибудь элемент $d \in A$ и рассмотрим уравнение $d \circ x = d$. Ввиду обратимости операции это уравнение имеет решение. Обозначим элемент, являющийся решением данного уравнения, через e.

Пусть далее a — произвольный элемент множества A, а элемент c является решением уравнения $x \circ d = a$. Таким образом, для элементов e и c выполняются равенства:

$$d \circ e = d \text{ и } c \circ d = a.$$

Отсюда получаем:

$$a \circ e = (c \circ d) \circ e = c \circ (d \circ e) = c \circ d = a.$$

Аналогично указывается такой элемент e', что любой элемент a из A удовлетворяет равенству

$$e' \circ a = a.$$

Но элемент e' совпадает с элементом e, так как $e' \circ e = e'$ и $e' \circ e = e$. Поэтому для всякого $a \in A$ имеют место одновременно оба равенства:

$$a \circ e = a \text{ и } e \circ a = a.$$

Следовательно, элемент e является нейтральным.

Пусть теперь a — снова какой угодно элемент из A. В силу обратимости операции уравнение $a \circ x = e$ имеет (ровно одно) решение. Обозначив это решение через b, получаем: $a \circ b = e$. Аналогично отыскивается элемент b', удовлетворяющий равенству $b' \circ a = e$. Покажем, что элемент b' совпадает с элементом b. В самом деле,

$$b' = b' \circ e = b' \circ (a \circ b) = (b' \circ a) \circ b = e \circ b = b.$$

Итак, справедливы равенства $a \circ b = e$ и $b \circ a = e$, т. е. b является обратным элементом для a. Значит, каждый элемент множества A обладает обратным.

2. Предположим теперь, что операция ассоциативна и каждый элемент из A обладает обратным. Это означает, что существует нейтральный элемент e и для всякого элемента a можно указать

единственный элемент $\tilde{a}$, такой что $a \circ \tilde{a} = e$ и $\tilde{a} \circ a = e$. Покажем, что операция обратима.

Уравнению

$$a \circ x = b$$

удовлетворяет, как легко проверить, элемент $\tilde{a} \circ b$. Обратно, если c есть какое-то решение этого уравнения, то из равенства $a \circ c = b$ получаем. $\tilde{a} \circ (a \circ c) = \tilde{a} \circ b$, откуда $c = \tilde{a} \circ b$. Таким образом, данное уравнение имеет единственное решение.

Аналогично проверяется существование и единственность решения уравнения $x \circ a = b$.

Теорема доказана.

Вопросы и упражнения

1. Обладает ли множество чисел вида $m + n\sqrt{2}$ (m и n — целые) нейтральным элементом относительно умножения? Будет ли операция умножения на этом множестве обратимой?

2 На множестве **R** действительных чисел бинарная операция задается формулой:

$$a \circ b = b.$$

Имеет ли **R** нейтральный элемент относительно этой операции? Будет ли эта операция ассоциативной?

3. Доказать, что операция матричного умножения на множестве матриц вида

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \quad (a,\ b > 0)$$

обратима.

4. Пусть A — множество всех подмножеств данного множества M. Существует ли в множестве A нейтральный элемент относительно операции пересечения подмножеств? Какие элементы будут обладать обратными?

§ 3. Группы

1. Основные определения. Примеры групп. Среди различных алгебраических систем важнейшую роль играют так называемые *группы*. Применения групп многочисленны и разнообразны как внутри самой математики, так и вне ее. Методы теории групп плодотворно используются при изучении геометрических преобразований, в теории алгебраических уравнений, в топологии, атомной физике, теории относительности, кристаллографии и во многих других разделах науки. В этой книге будут приведена лишь самые первые, элементарные сведения о группах.

Начнем с определения группы.

Непустое множество G, на котором определена ассоциативная и обратимая операция, называется *группой* (относительно этой операции).

Иными словами, множество G с ассоциативной операцией является группой, если для любых двух элементов $g_1 \in G$ и $g_2 \in G$ каждое из уравнений

$$g_1 \circ x = g_2$$

и

$$x \circ g_1 = g_2$$

имеет одно и только одно решение.

В силу теоремы, доказанной в конце предыдущего параграфа, условие обратимости операции в определении группы можно заменить следующими условиями:

1°. В множестве G существует *нейтральный* элемент, т. е. такой элемент e, что для любого $g \in G$ выполняются равенства:

$$g \circ e = g,\ e \circ g = g.$$

2°. Для каждого элемента $g \in G$ имеется *обратный* элемент f, удовлетворяющий равенствам:

$$g \circ f = e,\ f \circ g = e.$$

Обычно проще бывает проверить условия 1°, 2°, чем условие обратимости операции. Так именно мы и будем поступать в приводимых ниже примерах.

1. Множество положительных действительных чисел $\mathbf{R}^+$ образует группу относительно операции умножения. В самом деле, умножение ассоциативно, число 1 является нейтральным элементом ($1 \cdot r = r \cdot 1 = r$ для любого числа r), и для каждого числа $r > 0$ существует обратное число, равное $\frac{1}{r}\left(r \cdot \frac{1}{r} = \frac{1}{r} \cdot r = 1\right)$. Эта группа называется *мультипликативной* * *группой положительных действительных чисел.*

2. Множество $\mathbf{R}$ всех действительных чисел с операцией сложения есть группа, так как сложение ассоциативно, число 0 является нейтральным элементом ($r + 0 = 0 + r = r$ для любого числа r) и для всякого числа r обратным элементом служит противоположное ему число $-r$ (так как $r + (-r) = (-r) + r = 0$). Эта группа называется *аддитивной*** *группой действительных чисел.*

3. Арифметическое n-мерное векторное пространство является группой относительно сложения векторов. Действительно, эта операция ассоциативна, нейтральным элементом служит нулевой вектор $(0, 0, \ldots, 0)$, обратным для вектора $(a_1, a_2, \ldots, a_n)$ является вектор $(-a_1, -a_2, \ldots, -a_n)$.

Прежде чем переходить к дальнейшим примерам, сделаем несколько замечаний по поводу терминологии. Терминология мультипликативной группы положительных действительных чисел (пример 1) часто применяется в общем случае: нейтральный эле-

---

* От латинского слова multiplicatio — умножение.

** От латинского слова additio — сложение.

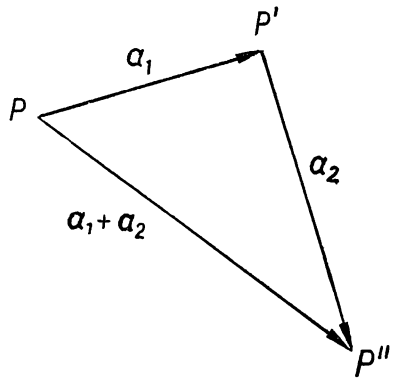

Рис. 2

мент называют *единицей* группы; элемент, обратный для g, обозначается g^{-1}; операцию называют *умножением* и результат ее применения к элементам g_1 и g_2 обозначают через g_1g_2. Это так называемая *мультипликативная* терминология. В ряде случаев более удобной представляется *аддитивная* терминология (см. пример 2): нейтральный элемент называют *нулем* группы; элемент, обратный для g, называют *противоположным* к g и обозначают через $-g$, а саму операцию называют *сложением*, обозначая композицию элементов g_1 и g_2 символом g_1+g_2. При этом всегда следует иметь в виду, что речь идет только об обозначениях и названиях; вообще говоря, множество группы не является числовым и уже поэтому групповая операция отлична от числовых операций сложения и умножения.

В дальнейшем мы будем пользоваться главным образом мультипликативной терминологией.

4. Важными примерами групп являются так называемые *группы преобразований*. Эти группы строятся следующим образом.

Пусть M — некоторое множество. Будем рассматривать всевозможные *преобразования* множества M, т. е. всевозможные взаимно однозначные отображения множества на себя. Обозначим множество всех этих преобразований через G и определим операцию умножения на G: любым двум преобразованиям g_1, g_2 сопоставим преобразование, которое получается в результате последовательного выполнения этих преобразований — сначала преобразования g_1, а затем преобразования g_2, т. е. $(g_1g_2)(x) = g_2(g_1(x))$ для всех $x \in M$.

Указанное преобразование будем называть произведением (композицией) преобразований g_1, g_2 и обозначать символом g_1g_2*. Если, например, преобразование g_1 плоскости есть сдвиг всех ее точек на вектор $\boldsymbol{a}_1$, а преобразование g_2 — сдвиг на вектор $\boldsymbol{a}_2$, то преобразование g_1g_2 будет сдвигом на вектор $\boldsymbol{a}_1+\boldsymbol{a}_2$ (рис. 2: g_1 переводит точку P в точку P', g_2 переводит точку P' в точку P'', g_1g_2 переводит точку P в точку P'').

Покажем, что множество G всех преобразований произвольного множества M есть группа относительно операции умножения преобразований. Проверим сначала, что эта операция ассоциативна. Пусть g_1, g_2, g_3 — любые три преобразования. Преобразо-

---

* В литературе часто символом g_1g_2 обозначают результат последовательного выполнения сначала операции g_2, потом g_1. В этом случае $g_1g_2(x)=g_1(g_2(x))$.

вание $g_1(g_2g_3)$ означает последовательное выполнение преобразований g_1 и g_2g_3, а преобразование g_2g_3, в свою очередь заключается в последовательном выполнении преобразований g_2 и g_3. Поэтому преобразование $g_1(g_2g_3)$ состоит в последовательном выполнении преобразований g_1, g_2, g_3:

$$(g_1(g_2g_3))(x) = g_3(g_2(g_1(x)))$$

для любого $x \in M$. То же самое верно и для преобразования $(g_1g_2)g_3$:

$$((g_1g_2)g_3)(x) = g_3(g_2(g_1(x))).$$

Следовательно,

$$g_1(g_2g_3) = (g_1g_2)g_3.$$

Обозначим через e преобразование, которое каждый элемент множества M переводит в себя (преобразование e, как иногда говорят, «оставляет на месте» все элементы из M). Очевидно, что $eg = ge = g$ для любого преобразования g, т. е. e является нейтральным элементом относительно умножения преобразований.

Пусть, далее, g — произвольное преобразование множества M. Рассмотрим преобразование $\tilde{g}$, которое определяется следующим условием: если g переводит элемент x в элемент y, то $\tilde{g}$ переводит элемент y в элемент x. Ясно, что при последовательном выполнении преобразований g и $\tilde{g}$ каждый элемент x перейдет в себя, т. е. $g\tilde{g} = e$. Аналогично $\tilde{g}g = e$. Мы получили, что для преобразования g существует обратное ему преобразование $\tilde{g}$.

Итак, доказано, что множество всех преобразований любого множества M есть группа.

5. В качестве отдельного примера выделим группу всех преобразований *конечного* множества. Преобразования n-элементного множества M условимся называть *подстановками степени* n.

Будем считать для определенности, что элементами M являются числа 1, 2,..., n, т. е. положим: $M = \{1, 2, \ldots, n\}$. Чтобы задать какое-либо преобразование этого множества, нужно для каждого числа $i \in M$ указать соответствующее ему число $\alpha_i \in M$. Поэтому всякую подстановку степени n можно задать с помощью матрицы

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix},$$

в которой под каждым числом i первой строки (состоящей из всех чисел множества M) помещается соответствующее ему число α_i. Например, матрица

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

означает подстановку, переводящую число 1 в число 2, число 2 — в число 1, число 3 — в число 3.

Ту же самую подстановку задает матрица

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

отличающаяся от предыдущей только порядком своих столбцов.

Вообще, задавая какую-либо подстановку, можно располагать числа 1, 2, ..., n в первой строке в любом порядке, тогда выбранная подстановка однозначно определяет порядок тех же чисел во второй строке. Таким образом, подстановки степени n задаются матрицами вида

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \beta_1 & \beta_2 & \dots & \beta_n \end{pmatrix},$$

где обе строки являются перестановками из чисел 1, 2,..., n. При этом две такие матрицы задают одну и ту же подстановку, если они отличаются только порядком своих столбцов.

Нетрудно подсчитать общее число подстановок степени n. Для этого зафиксируем какой-нибудь определенный порядок элементов в первой строке; например, расположим элементы первой строки в порядке их возрастания. Тогда каждая подстановка будет определяться порядком элементов второй строки. Но эти элементы можно расставить столькими различными способами, сколько имеется различных перестановок из n элементов, т. е., как известно, $n!$ способами. Так, имеется $3! = 6$ перестановок из трех элементов: (1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 2, 1), (3, 1, 2). Им отвечают 6 различных подстановок степени 3:

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

Умножение подстановок определяется общим правилом умножения преобразований (см, пример 4): произведением или композицией двух подстановок g_1 и g_2 считается подстановка, которая получается в результате последовательного выполнения сначала подстановки g_1, а затем подстановки g_2.

Пусть, например, требуется найти композицию подстановок

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ и } g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Подстановка g_1 переводит элемент 1 в элемент 2, а подстановка g_2 переводит элемент 2 снова в элемент 2. Значит, при последовательном выполнении сначала подстановки g_1, а затем подстановки g_2 элемент 1 перейдет в элемент 2, т. е. подстановка $g_1 g_2$ переведет элемент 1 в элемент 2. Аналогично элемент 2 переводится под-

становкой g_1g_2 в элемент 3, а элемент 3 — в элемент 1. Таким образом,

$$g_1g_2 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}.$$

Заметим, что порядок «сомножителей» существен. Так, например,

$$g_2g_1 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix},$$

откуда видно, что преобразования g_1g_2 и g_2g_1 различны.

Единицей (нейтральным элементом) множества подстановок является тождественная подстановка

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

а обратной для подстановки

$$\begin{pmatrix}1 & 2 & \dots & n\\ \alpha_1 & \alpha_2 & \dots & \alpha_n\end{pmatrix}$$

является подстановка

$$\begin{pmatrix}\alpha_1 & \alpha_2 & \dots & \alpha_n\\ 1 & 2 & \dots & n\end{pmatrix}.$$

Понятно также, что, будучи частным случаем операции умножения преобразований, операция умножения подстановок ассоциативна.

Итак, множество всех подстановок данной степени n является группой относительно введенной операции умножения подстановок. Эта группа называется *группой всех подстановок степени n**.

В примерах 1—3 групповая операция была коммутативной, а в случае группы подстановок степени $n > 2$ — не коммутативной. В дальнейшем группу с коммутативной операцией будем называть *коммутативной* **.

Группу, состоящую из конечного числа n элементов, называют *конечной группой порядка n*, а группу с бесконечным множеством элементов — *бесконечной*. Группы примеров 1—3 бесконечные. Группа преобразований бесконечного множества M также бесконечна, а группа подстановок степени n является конечной группой порядка $n!$.

З а д а ч а 1. Преобразование пространства, сохраняющее расстояние между любыми двумя точками, называется *движением* (перемещением); движение, оставляющее неподвижной некоторую точку, — *вращением* (поворотом) вокруг этой точки; *переносом* называется движение, при котором все точки смещаются на один и тот же вектор. Показать, что каждое из трех множеств — множество H всех

---

* Часто используется также термин *симметрическая группа степени n*.

** Коммутативную группу называют также *абелевой* — по имени норвежского математика Нильса Генрика Абеля (1802—1829).

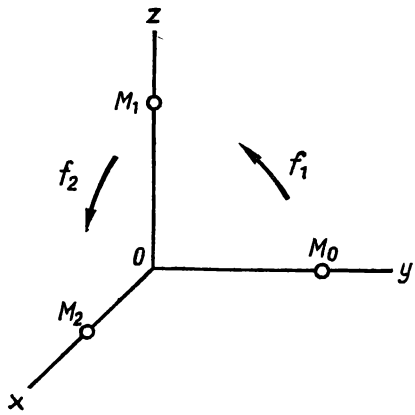

Рис. 3

переносов, множество F всех вращений и множество G всех движений — является группой относительно операции умножения преобразований и что группы F и G некоммутативны.

Р е ш е н и е. Ясно, что произведение движений g_1 и g_2 снова будет движением: если g_1 переводит точки M и N в точки M_1 и N_1, а g_2— точки M_1 и N_1 в точки M_2 и N_2, то g_1g_2 переводит точки M и N в точки M_2, N_2, но тогда из равенств $|MN| = |M_1N_1|$ и $|M_1N_1| = |M_2N_2|$ следует равенство $|MN| = |M_2N_2|$. Аналогично произведение вращений f_1, f_2 и произведение переносов h_1, h_2 будут соответственно вращением и переносом. Следовательно, умножение преобразований является операцией на каждом из множеств G, F, H, причем эта операция ассоциативна (см. пример 4).

Тождественное преобразование является одновременно движением, вращением и переносом. Поэтому каждое из множеств G, F и H содержит нейтральный элемент.

Наконец, для каждого движения g обратное преобразование g^{-1} также оказывается движением: если g^{-1} переводит точки M', N' в точки M, N, то g переводит точки M, N в точки M', N', откуда $|MN| = |M'N'|$. Аналогично для любого вращения f и любого переноса h преобразования f^{-1} и h^{-1} будут соответственно вращением и переносом. Следовательно, каждое из множеств G, F, H вместе со всяким своим элементом содержит обратный ему элемент.

Таким образом, множества G, F и H являются группами.

Докажем, что группа F некоммутативна. Пусть рассматриваются вращения вокруг некоторой точки O; проведем через точку O взаимно перпендикулярные оси Ox, Oy, Oz (рис. 3). Пусть вращение f_1 вокруг оси Ox переводит точку M_0 оси Oy в точку M_1 оси Oz, а вращение f_2 вокруг оси Oy — точку M_1 в точку M_2 оси Ox. Тогда вращение f_1f_2 переведет точку M_0 в точку M_2. Если же произвести сначала вращение f_2, а потом вращение f_1, то точка M_0 перейдет в точку M_1. Поэтому $f_1f_2 \neq f_2f_1$. Значит, группа F некоммутативна.

Группа G также некоммутативна, так как вращения f_1, f_2 являются одновременно и движениями.

С другой стороны, группа H переносов коммутативна — читатель легко убедится в этом самостоятельно.

З а д а ч а 2. Рассмотрим множество *самосовмещений* куба, понимая под самосовмещением всякое движение куба, переводящее куб в себя. Убедиться, что это множество составляет группу отно-

сительно операции умножения преобразований и найти число элементов этой группы.

Р е ш е н и е. Ясно, что произведение (т. е. последовательное выполнение) самосовмещений ассоциативно, поскольку ассоциативно умножение любых преобразований (см. пример 4 на с.18). Тождественное преобразование, оставляющее все точки куба на месте, является, очевидно, самосовмещением, и, значит, множество самосовмещений содержит нейтральный элемент Наконец, преобразование, обратное самосовмещению, также является самосовмещением. Следовательно, множество самосовмещений образует группу.

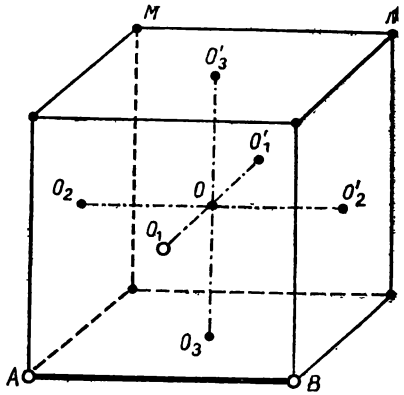

Рис. 4

Подсчитаем число элементов этой группы. Выделим какое-нибудь ребро куба AB и центр O_1 одной из примыкающих к нему граней (рис. 4). Положение куба в пространстве однозначно определяется положением его центра O и точек A, B, O_1 (так как эти точки не лежат в одной плоскости). Но центр O куба равноудален от всех его вершин и, значит, при любом самосовмещении переходит в себя. Поэтому, чтобы полностью задать самосовмещение, нужно указать, в какие точки перейдут точки A, B и O_1. Пусть M и N — любые две соседние вершины куба. Могут существовать только два самосовмещения, переводящие вершину A в M и вершину B в N,— к ребру MN примыкают две грани, и точка O_1 должна перейти в центр одной из них. Оба эти самосовмещения действительно существуют. Например, для случая, представленного на рис. 4, одно самосовмещение получается как вращение вокруг оси O_2O_2', а другое — как симметрия относительно плоскости, проходящей через ребра, параллельные ребрам AB и MN. Точно так же существует ровно два самосовмещения, переводящие вершину A в N и вершину B в M.

Итак, каждому из 12 ребер куба отвечает 4 самосовмещения. Поэтому общее число самосовмещений равно $12 \times 4 = 48$, т. е. группа самосовмещений состоит из 48 элементов.

Рекомендуем читателю убедиться, что эта группа некоммутативна (для этого можно воспользоваться доказательством некоммутативности группы вращений из предыдущей задачи).

Вопросы и упражнения

1. Показать, что числовое множество $\{-1;1\}$ является группой относительно операции умножения.

2. Показать, что множество G всех целых степеней числа $a > 0$ (т. е. множество $G = \{x : x = a^n,\ n$ — целое$\}$) есть группа относительно операции умножения.

3. Пусть L — некоторое подмножество множества M. Доказать, что множество всех преобразований множества M, переводящих каждый элемент из L в себя, является группой относительно операции умножения преобразований.

4. Будет ли группой множество всех числовых множеств относительно операции пересечения множеств?

2. Подгруппы. Пусть множество G является группой относительно некоторой бинарной операции. Подмножество H множества G, являющееся группой относительно *той же* операции, называется *подгруппой* группы G.

Из этого определения следует, что всякая группа является своей подгруппой и что множество, состоящее только из единицы группы, также будет ее подгруппой (единичная группа). Могут, однако, существовать и подгруппы, отличные от этих очевидных подгрупп.

Множество положительных рациональных чисел $\mathbf{Q}^+$ является группой относительно операции умножения и поэтому подгруппой мультипликативной группы положительных действительных чисел (см. пример 1 пункта 1). Аналогично множество целых чисел $\mathbf{Z}$, будучи группой относительно операции сложения, составляет подгруппу аддитивной группы действительных чисел (пример 2 пункта 1).

Для того чтобы установить, что непустое подмножество H группы G есть подгруппа этой группы, достаточно проверить два условия:

1°. Для любых двух элементов $h_1 \in H$, $h_2 \in H$ их композиция h_1h_2 принадлежит H.

2°. Для любого элемента $h \in H$ обратный ему элемент h^{-1} также принадлежит H.

Действительно, условие 1° означает, что операция на множестве G будет операцией также и на множестве H. Это условие называется *условием замкнутости* множества H относительно данной операции. Ассоциативность операции на H вытекает из ее ассоциативности на G. Наконец, из условий 1°, 2° следует, что H содержит нейтральный элемент e: взяв какой-либо элемент h из H, по условию 2° мы найдем в H обратный ему элемент h^{-1}, а по условию 1° получим, что нейтральный элемент $e = hh^{-1}$ также содержится в H.

Рассмотрим в качестве примера группу G всех подстановок третьей степени и выделим в ней подмножество H из подстановок

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\quad g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Легко проверяется, что $g_1g_1 = g_1$, $g_1g_2 = g_2g_1 = g_2$, $g_2g_2 = g_1$. Таким образом, попарные произведения элементов из H снова принадлежат H, т. е. условие 1° выполнено. С другой стороны, равенства $g_1g_1 = g_1$ и $g_2g_2 = g_1$ показывают, что каждый из элементов g_1, g_2

является обратным самому себе. Значит, выполнено также и условие 2°. Следовательно, подмножество H является подгруппой группы G.

Условия 1°, 2° можно заменить следующим одним условием:

3°. Для любых двух элементов $h_1 \in H$, $h_2 \in H$ элемент $h_1 h_2^{-1}$ принадлежит H.

Действительно, при выполнении условий 1°, 2° условие 3°, очевидно, также выполняется. С другой стороны, если имеет место условие 3°, то, взяв произвольный элемент $h \in H$, получим: $hh^{-1} = e \in H$. Но тогда $h^{-1} = eh^{-1} \in H$, т. е. выполнено условие 2°. Пусть теперь $h_1 \in H$ и $h_2 \in H$. Тогда $h_2^{-1} \in H$ и, следовательно, $h_1 h_2 = h_1 (h_2^{-1})^{-1} \in H$. Таким образом, из условия 3° вытекает и условие 1°.

З а д а ч а. Показать, что в случае конечного подмножества H группы G условие 2° следует из условия 1°.

Р е ш е н и е. Пусть $h \in H$. Рассмотрим бесконечную последовательность элементов:

$$h,\ h^2 = hh,\ h^3 = hhh, \ldots .$$

В силу условия 1° все элементы этой последовательности принадлежат H, а в силу конечности H какие-то два из них — h^m и h^{m+k} — должны совпадать:

$$\underbrace{hh \ldots h}_{m \text{ раз}} = \underbrace{hh \ldots h}_{m \text{ раз}} \underbrace{hh \ldots h}_{k \text{ раз}}.$$

Таким образом, $h^m = h^m h^k$, где $k \geqslant 1$. Отсюда имеем:

$$e = (h^m)^{-1} h^m = (h^m)^{-1} h^m h^k = eh^k = h^k.$$

Если $k = 1$, то $h = e$ и тогда $h^{-1} = h \in H$. Если же $k > 1$, то $e = hh^{k-1}$ и, значит, снова $h^{-1} \in H$.

Эта задача допускает и другое решение. Пусть H состоит из n элементов $h_1, h_2, \ldots, h_n$ и элемент h — какой-то один из них. Рассмотрим (конечную) последовательность произведений:

$$hh_1,\ hh_2, \ldots,\ hh_n.$$

Все эти произведения в силу 1° содержатся в H. Нетрудно проверить, что все они различны. (Например, если $hh_1 = hh_2$, то $h^{-1} hh_1 = h^{-1} hh_2$, т. е. $h_1 = h_2$.) Таким образом, в данной последовательности содержатся все элементы H, в частности элемент h. Положим для определенности $h = hh_1$. Тогда $h_1 = e$, и, значит, нейтральный элемент является одним из членов нашей последовательности. Пусть, например, $hh_n = e$. Тогда $h^{-1} = h_n$, т. е. $h^{-1} \in H$.

Вопросы и упражнения

1. Доказать, что целые числа, кратные данному числу n, образуют подгруппу группы целых чисел по сложению.

2. Найти все подгруппы группы подстановок третьей степени.

3. Показать, что множество элементов произвольной группы G, «перестановочных» со всеми элементами этой группы (т. е. таких элементов x, что для любого $g \in G$ выполняется условие $gx = xg$), является подгруппой группы G. При каком условии эта подгруппа совпадает с группой G?

4. Показать, что подмножество H группы G, удовлетворяющее условию замкнутости 1°, но не удовлетворяющее условию 2°, может не быть подгруппой группы G (рассмотреть подмножество $\mathbf{R}^+$ положительных действительных чисел множества $\mathbf{R}$ всех действительных чисел, образующих группу по сложению).

3. Отображения групп, изоморфные группы. Группы представляют собой системы с одной операцией — на них, следовательно, распространяются все понятия, связанные с отображениями систем. Исходя из общего определения гомоморфного отображения и применяя мультипликативную символику для записи операций, мы получаем следующее определение гомоморфного отображения группы.

Отображение группы G на множество G' с одной операцией называется *гомоморфным* (или *гомоморфизмом*), если это отображение сохраняет операцию, т. е. для любых элементов g_1, g_2 группы G из условий

$$g_1 \to g_1', \quad g_2 \to g_2'$$

следует, что

$$g_1 g_2 \to g_1' g_2'.$$

Множество G' с заданной на нем операцией называется при этом *гомоморфным образом* группы G.

Замечание. Чтобы не вводить дополнительных обозначений, операции в G и G' представлены здесь одинаково, т. е. обе записаны в виде произведений. Нужно, однако, помнить, что это разные операции, определенные каждая по-своему.

В пункте 2 § 1 рассматривался пример гомоморфного отображения множества целых чисел с операцией сложения на множество $\{-1, 1\}$ с операцией умножения: четные числа отображались в число 1, а нечетные — в число — 1. Так как целые числа образуют группу относительно сложения, то это отображение является на самом деле гомоморфным отображением группы.

Возникает вопрос: какие свойства операции в группе G переносятся при гомоморфизме на операцию в системе G'? Оказывается, что к таким свойствам относятся ассоциативность и обратимость; другими словами, справедлива следующая теорема.

Теорема. *Гомоморфный образ группы также является группой относительно своей операции.*

Доказательство. Пусть группа G гомоморфно отображается на множество G', и пусть при этом нейтральный элемент e группы G переходит в элемент e' множества G': $e \to e'$. Покажем, что элемент e' будет нейтральным в множестве G'. Пусть g' — произвольный элемент множества G', а элемент $g \in G$ является одним

из его прообразов: $g \to g'$. Тогда $eg \to e'g'$; но $eg = g$, поэтому $e'g' = g'$. Аналогично показывается, что $g'e' = g'$. Значит, элемент e' является нейтральным относительно операции на множестве G'.

Возьмем теперь снова произвольный элемент $g' \in G'$, и пусть по-прежнему $g \to g'$. Покажем, что для элемента g' имеется обратный. Для элемента g группы G существует обратный элемент $f \in G$. Значит,

$$gf = fg = e,$$

где e — нейтральный элемент группы G. Пусть элементу f соответствует элемент $f' \in G'$, т. е. $f \to f'$.

Тогда мы имеем:

$$g'f' = f'g' = e'.$$

Но выше было показано, что элемент e' является нейтральным, поэтому элемент f' будет обратным для g'.

Убедимся, наконец, в ассоциативности операции на множестве G'. Если g', f' и h' — любые три элемента из G' и $g \to g'$, $f \to f'$, $h \to h'$, то $(gf)h \to (g'f')h'$, а $g(fh) \to g(f'h')$. Ввиду ассоциативности операции в группе G имеет место равенство $(gf)h = g(fh)$. Значит, $(g'f')h' = g'(f'h')$, т. е. операция на множестве G' ассоциативна.

Таким образом, множество G' есть группа относительно своей операции. Теорема доказана.

Замечание. По ходу доказательства теоремы мы установили еще один важный факт:

При гомоморфизме единица группы G отображается в единицу группы G', а взаимно обратные элементы из G отображаются во взаимно обратные элементы из G'.

Итак, гомоморфный образ G' группы G снова есть группа. Если гомоморфное отображение взаимно однозначно, то оно называется *изоморфным* (или *изоморфизмом*), а группы G и G' — *изоморфными*. Как уже говорилось в п. 2 § 1, изоморфные группы отличаются только способом задания своих элементов и операций; такие группы можно считать совпадающими.

Пример изоморфных групп дают мультипликативная группа положительных действительных чисел и аддитивная группа всех действительных чисел (см. п. 2 § 1). В дальнейшем будут указаны и другие примеры.

Вопросы и упражнения

1. Доказать, что отображение любой группы G на одноэлементную группу G' сохраняет операцию, т. е. является гомоморфизмом.

2. Пусть g_0 — некоторый элемент группы G. Поставим в соответствие каждому элементу $g \in G$ снова элемент из G, равный gg_0: $g \to gg_0'$. Показать, что это соответствие задает взаимно однозначное отображение группы G на себя. Показать также, что если элемент g_0 отличен от единицы группы G, то данное отображение не будет гомоморфизмом.

3. Доказать, что если каждому элементу g группы G поставить в соответствие элемент $g_0^{-1}gg_0$ (g_0 — фиксированный элемент из G), то получится изоморфное отображение группы G на себя.

4. Циклические группы. Произвольная группа G вместе с каждым своим элементом g содержит также любые целые положительные степени этого элемента:

$$g^2 = gg,\ g^3 = ggg,\ldots,$$

а кроме того, элемент g^{-1} и его (положительные) степени:

$$(g^{-1})^2 = g^{-1}g^{-1},\ (g^{-1})^3 = g^{-1}g^{-1}g^{-1},\ldots.$$

Элементы g^{-1}, $(g^{-1})^2$, $(g^{-1})^3$,... являются, как легко проверить, обратными соответственно для элементов g, g^2, g^3,.... Их обозначают символами g^{-1}, g^{-2},g^{-3},... и называют *отрицательными степенями* элемента g. Наконец, *нулевой степенью* любого элемента $g \in G$ считают нейтральный элемент e группы G, т. е. полагают $g^0 = e$. Читателю предоставляется убедиться, что при таких соглашениях о степенях элемента g выполняются следующие привычные правила действий с показателями:

$$g^m g^n = g^{m+n},$$
$$(g^m)^n = g^{mn},$$

где m и n — произвольные целые числа.

Совокупность всех степеней элемента g образует, очевидно, коммутативную подгруппу группы G. Может случиться, что этой подгруппой исчерпывается *вся* группа G, т. е. что группа состоит в точности из элементов:

$$\ldots,\ g^{-3},\ g^{-2},\ g^{-1},\ g^0 = e,\ g^1,\ g^2,\ g^3,\ldots.$$

В связи с этим примем следующее определение.

Группа G называется *циклической*, если она состоит из всех степеней некоторого своего элемента g. Элемент g называется при этом *образующим элементом* или просто *образующей* группы, а сама группа обозначается символом (g).

Для любой циклической группы (g) имеет место одно из двух: либо все степени образующей g *различны*, либо имеются *совпадающие* степени элемента g.

В первом случае группа будет бесконечной. Примером такой группы служит группа всех целых чисел относительно сложения:

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

образующей этой группы служит число 1.

Рассмотрим теперь случай, когда какие-нибудь две степени образующей совпадают: $g^m = g^k$, где m и k — целые и $m \neq k$. В этом случае, равенство $g^m = g^k$ умножением на подходящую степень элемента g можно привести к виду $g^r = e$, где $r > 0$, а e — единица группы.

Следовательно, существует положительная степень образующей, равная единице группы. Если число n — *наименьшая* из таких степеней, то все элементы

$$e = g^0,\ g^1,\ g^2,\ldots,\ g^{n-1}$$

различны, иначе было бы $g^m = g^k$, где $0 \leqslant m < k < n$, откуда следовало бы, что $g^{k-m} = e$, причем $0 < k - m < n$, т. е. нашлась бы *меньшая* чем n положительная степень g, равная единице. С другой стороны, любая степень g^s элемента g совпадает с одним из элементов g^0, g^1, $g^2,\ldots,$ g^{n-1}: если представить целое число s в виде $nq+r$ (здесь q — частное, а r — остаток от деления s на n, так что $0 \leqslant r < n$), то получится:

$$g^s = g^{nq+r} = (g^n)^q g^r = e^q g^r = g^r.$$

Значит, элементами $g^0, g^1, g^2,\ldots, g^{n-1}$ исчерпывается вся группа G. Тем самым *группа G оказывается конечной группой порядка n.*

Пример. Все степени подстановки

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

составляют циклическую группу третьего порядка, так как

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

а все меньшие степени различны:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

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

Подстановка

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

будет образующей этой группы. Впрочем, нетрудно проверить, что для этой группы подстановка

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

также является образующей.

Аналогично множество степеней подстановки

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

является циклической группой четвертого порядка. Вообще, множество степеней подстановки

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

будет, как нетрудно проверить, циклической группой порядка n.

Из этого видно, что существуют конечные группы любого наперед заданного порядка.

В дальнейшем мы дадим полное описание всех циклических групп, а пока отметим следующий факт:

Всякая подгруппа циклической группы сама является циклической группой.

Действительно, если подгруппа H группы $G = (g)$ содержит только нулевую степень элемента g, то в H имеется только один элемент — единица e группы G (поскольку $g^0 = e$). В этом случае, очевидно, $H = (e)$.

Если же в подгруппе H содержится какая-нибудь ненулевая степень элемента g, то в ней содержится и некоторая положительная степень g, так как вместе со всяким элементом g^k в подгруппу H входит и обратный ему элемент g^{-k}. Пусть n — *наименьшая* из положительных степеней элемента g, содержащихся в H, и $h = g^n$. Покажем, что $H = (h)$, т. е. что H исчерпывается различными степенями элемента h:

$$\ldots, h^{-2}, h^{-1}, h^0 = e, h^1, h^2, \ldots .$$

Допустив противное, получим, что H содержит элемент g^s и s не делится на n. Но тогда s можно представить в виде $nq + r$, где $0 < r < n$, откуда $g^s = (g^n)^q g^r = h^q g^r$. Значит, и элемент $h^{-q}(h^q g^r) = g^r$ содержится в H, а это противоречит тому, что n — *наименьшая* из положительных степеней элемента g, содержащихся в H.

Из этого рассуждения следует, в частности, что любая подгруппа аддитивной группы $\mathbf{Z}$ целых чисел является либо единичной подгруппой $H = \{0\}$, состоящей из единственного элемента 0, либо подгруппой H_n, состоящей из чисел, кратных некоторому целому числу $n \geqslant 1$:

$$\ldots, -2n, -n, 0, n, 2n, \ldots .$$

З а д а ч а 1. Доказать, что в циклической группе порядка n с образующей g элемент g^k тогда и только тогда является образующей, когда k взаимно просто с n.

Р е ш е н и е. Допустим сначала, что числа k и n не являются взаимно простыми. Тогда у них имеется общий делитель $d > 1$, т. е. $k = k_1 d$, $n = n_1 d$. В этом случае

$$(g^k)^{n_1} = g^{kn_1} = g^{k_1 d\, n_1} = (g^n)^{k_1} = e.$$

Следовательно, среди степеней элемента g^k найдется не более n_1 различных. Но $n_1 < n$, поэтому различные степени элемента g^k не исчерпывают всей группы, состоящей из n различных элементов $g^0, g^1, \ldots, g^{n-1}$. Таким образом, элемент g^k не является образующей группы (g).

Пусть теперь числа n и k взаимно просты. Тогда элементы

$$(g^k)^0, (g^k)^1, \ldots, (g^k)^{n-1}$$

попарно различны. В самом деле, допустив, что $g^{kp} = g^{kq}$, где $p < q < n$, мы получим:

$$g^{k(q-p)} = e.$$

Ясно, однако, что с единицей совпадают только степени g, кратные n. Поэтому $k(q-p)$ делится на n, а раз k взаимно просто с n, то $q - p$ делится на n. Но это невозможно, поскольку $0 < q - p < n$. Следовательно, имеется n попарно различных степеней элемента g^k, т. е. различные степени элемента g^k исчерпывают всю группу (g). Значит, элемент g^k служит образующей этой группы.

Из доказанного утверждения вытекает, что циклическая группа порядка n имеет столько различных образующих, сколько взаимно простых с n чисел существует в последовательности 0, 1, 2,..., $n - 1$. Например, если $n = 15$, то взаимно простыми с n будут числа 1, 2, 4, 7, 8, 11, 13, 14, и в этом случае группа имеет в точности восемь различных образующих.

З а д а ч а 2. Показать, что если порядок циклической группы делится на число m, то эту группу можно гомоморфно отобразить на ее подгруппу порядка m.

Р е ш е н и е. Пусть $G = (g)$ — циклическая группа порядка n с образующей g и n делится на m: $n = km$. Степени элемента $f = g^k$

$$f^0 = e,\ f^1 = g^k,\ f^2 = g^{2k},\ \ldots,\ f^{m-1} = g^{(m-1)k}$$

все различны и $f^m = g^{mk} = e$. Поэтому элемент f является образующей циклической подгруппы порядка m группы G. Обозначим эту подгруппу через F и определим следующее отображение: каждому элементу g^s группы G сопоставим элемент f^r группы F, где r есть остаток от деления s на m. Мы получим отображение группы G на группу F, так как элементам $g^0, g^1,\ldots, g^{m-1}$ группы G будут сопоставлены соответственно элементы $f^0, f^1,\ldots, f^{m-1}$ группы F, т. е. каждый элемент группы F будет сопоставлен некоторому элементу группы G.

Покажем, что отображение сохраняет операцию. Пусть элементам g^{s_1}, g^{s_2} сопоставлены элементы f^{r_1}, f^{r_2}. Тогда $s_1 = mq_1 + r_1$ и $s_2 = mq_2 + r_2$. Положим, что $r_1 + r_2$ дает при делении на m остаток r, т. е. $r_1 + r_2 = mq + r$. Мы имеем:

$$g^{s_1}g^{s_2} = g^{s_1+s_2} = g^{mq_1+r_1+mq_2+r_2} = g^{m(q_1+q_2+q)+r}.$$

Следовательно, элементу $g^{s_1}g^{s_2}$ сопоставляется элемент f^r. Но так как $f^m = e$, то

$$f^r = (f^m)^q f^r = f^{mq+r} = f^{r_1+r_2} = f^{r_1}f^{r_2}.$$

Поэтому произведению $g^{s_1}g^{s_2}$ сопоставляется произведение $f^{r_1}f^{r_2}$. Таким образом, отображение сохраняет операцию и, значит, является гомоморфным.

Вопросы и упражнения

1. Проверить, что в циклической группе целых чисел по сложению число —1 является образующей.

2. Доказать, что группа всех подстановок третьей степени не является циклической.

3. Доказать, что для любых двух элементов g_1 и g_2 группы G порядки подгрупп (g_1g_2) и (g_2g_1) равны.

Указание Убедиться, что из равенства $(g_1g_2)^n = e$ следует равенство $(g_2g_1)^n = e$

5. Полугруппы. В ряде случаев приходится иметь дело с ассоциативными операциями, которые, однако, не обязательно обладают свойством обратимости. В связи с этим принимается следующее определение:

Непустое множество G с ассоциативной операцией называется *полугруппой* относительно этой операции.

Таким образом, группа оказывается частным случаем полугруппы — группу можно определить как полугруппу с обратимой операцией.

Не вдаваясь в подробное рассмотрение полугрупп, ограничимся несколькими примерами.

Множство **R** действительных чисел будет полугруппой относительно операции умножения, однако оно не будет группой, так как, например, уравнение $0 \cdot x = 1$ не имеет действительных решений.

В пункте 1 этого параграфа рассматривалась группа преобразований произвольного множества M. Преобразованиями считались взаимно однозначные отображения M на себя. Будем теперь говорить о произвольных однозначных отображениях множества M *в себя* (не обязательно на себя) и определять произведение таких отображений прежним правилом — как результат последовательного выполнения отображений. Тем самым мы определим операцию на множестве всех отображений, которая по-прежнему будет ассоциативной, но уже необратимой. Так, если G состоит из всех отображений трехэлементного множества $\{1, 2, 3\}$, то уравнение

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

неразрешимо в G (здесь первая из матриц означает отображение, переводящее числа 1 и 2 в число 1, а число 3 — в число 3). Действительно, если бы искомое отображение x существовало, то оно должно было бы переводить число 1 одновременно в число 1 и в число 2, что противоречит требованию однозначности отображения. Следовательно, отображения составляют полугруппу — но не группу — относительные операции умножения отображений.

Другой весьма общий пример полугруппы можно построить следующим образом: взять какой-нибудь конечный набор символов (*алфавит*) и элементами множества A считать всевозможные конечные последовательности символов этого алфавита (*слова*). При этом произведение слов α и β определяется как слово, которое

получается приписыванием справа к слову α слова β. Так, для алфавита $\{0, —, *\}$ произведением слов $\alpha = 00 —$ и $\beta = ** 00*$ будет слово $\alpha\beta = 00 —**00*$. Операция, определяемая указанным правилом, будет, очевидно, ассоциативной, но необратимой; например, для слов 000 и 00 уравнение $000x = 00$ не имеет решений.

Таким образом, множество слов некоторого алфавита является полугруппой (но не группой) относительно операции умножения слов.

§ 4. Конечные группы

1. Таблицы Кэли. В предыдущем параграфе были приведены некоторые примеры конечных групп. Теперь мы переходим к более детальному изучению таких групп. Заметим, что для полного задания какой-нибудь группы G достаточно указать, чему равны всевозможные попарные произведения $g'g''$ элементов этой группы. В случае конечной группы порядка n такое задание удобно осуществлять с помощью квадратной таблицы из n строк и n столбцов, снабженной дополнительно заглавной (верхней) строкой и заглавным (левым) столбцом. В заглавной строке записываются в некотором порядке слева направо все элементы $g_1, g_2, \ldots g_n$ группы G, а в заглавном столбце эти элементы выписываются *в том же* порядке* сверху вниз. В клетке таблицы, соответствующей элементу g_i заглавного столбца и элементу g_j заглавной строки, помещается элемент g_l, равный произведению g_ig_j. Таким образом, таблица имеет следующий вид:

Таблица 1

	g_1	. . .	g_j	. . .	g_n
g_1					
.					
g_i			g_ig_j		
.					
g_n					

* В принципе можно было бы записывать элементы группы в заглавной строке и заглавном столбце в *различном* порядке, но такие таблицы менее наглядны, и мы ими пользоваться не будем.

Такую таблицу называют *таблицей умножения* или *таблицей Кэли** группы G.

Рассмотрим, например, множество чисел $\{1, i, -1, -i\}$. Нетрудно проверить, что это множество образует (коммутативную) группу относительно операции умножения. Составим таблицу Кэли для этой группы:

Таблица 2

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Коммутативность группы выражается в том, что в любых двух клетках таблицы, симметричных относительно ее «главной диагонали» (в данной таблице две такие клетки выделены), находятся равные элементы, поскольку в этих клетках записаны произведения, отличающиеся только порядком сомножителей.

Далее, первый столбец таблицы повторяет заглавный столбец. Следовательно, заглавный элемент первого столбца является единицей группы.

В пересечении строки и столбца, озаглавленных числами i и $-i$, стоит число 1 (единица группы). Значит, числа i и $-i$ будут взаимно обратными элементами группы.

Таким образом, таблица Кэли позволяет судить о коммутативности группы, находить единицу группы и для каждого элемента — обратный ему элемент.

В пункте 4 § 3 отмечалось, что все степени подстановки

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

образуют (циклическую) группу (g). Вот как выглядит таблица Кэли для этой группы:

* Артур Кэли — английский математик (1821—1895).

Таблица 3

	g^0	g^1	g^2	g^3
g^0	g^0	g^1	g^2	g^3
g^1	g^1	g^2	g^3	g^0
g^2	g^2	g^3	g^0	g^1
g^3	g^3	g^0	g^1	g^2

Можно установить, что эта группа изоморфна группе, заданной таблицей 2, сопоставив элементам первой строки таблицы 3 соответственные элементы первой строки таблицы 2 и проверив, что полученное отображение сохраняет операцию умножения. Но так как это должно означать, что в соответственных клетках таблиц 2 и 3 находятся сопоставленные друг другу элементы, то проще поступить иначе: заменить все элементы таблицы 3 сопоставленными им элементами первой строки таблицы 2 и убедиться, что получившаяся таблица совпадает с таблицей 2.

Итак, мы видим, что изоморфными являются такие конечные группы, таблицы Кэли которых — при подходящем расположении элементов в заглавных строках — совпадают с точностью до обозначений.

Таблицу Кэли можно построить для любого конечного множества с одной операцией. Чтобы такая таблица задавала *группу*, нужно, чтобы в каждой ее строке и каждом столбце содержались *все* элементы данного множества, и притом ровно по одному разу, тогда требование обратимости операции будет выполнено. Действительно, уравнение $g'x = g''$ имеет в данном множестве столько решений, сколько раз элемент g'' входит в строку, озаглавленную элементом g'. Поэтому для однозначной разрешимости данного уравнения необходимо и достаточно, чтобы каждый элемент множества входил в эту строку ровно один раз. Проверку ассоциативности операции также можно осуществить по таблице, отыскивая произведения $(ab)c$ и $a(bc)$ для всех троек элементов множества и убеждаясь в их равенстве. Однако такая проверка, конечно, весьма громоздка, и для ее сокращения прибегают к тем или иным искусственным приемам — мы на этом не будем останавливаться.

Рассмотрим в качестве еще одного примера таблицу Кэли для группы всех подстановок третьей степени. Введем обозначения для элементов этой группы:

$$g_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad g_2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad g_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$
$$g_4=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad g_5=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\quad g_6=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

Вычисляя попарные произведения этих элементов, получаем для данной группы следующую таблицу:

Таблица 4

	g_1	g_2	g_3	g_4	g_5	g_6
g_1	g_1	g_2	g_3	g_4	g_5	g_6
g_2	g_2	g_1	g_4	g_3	g_6	g_5
g_3	g_3	g_5	g_1	g_6	g_2	g_4
g_4	g_4	g_6	g_2	g_5	g_1	g_3
g_5	g_5	g_3	g_6	g_1	g_4	g_2
g_6	g_6	g_4	g_5	g_2	g_3	g_1

По этой таблице еще раз убеждаемся в некоммутативности данной группы — произведения g_2g_4 и g_4g_2, выделенные в таблице, различны.

Вопросы и упражнения

1. Проверить правильность заполнения таблицы 4 непосредственным вычислением.

2. Найти, пользуясь таблицей 4, единицу группы и элемент, обратный для g_3.

3. Найти по таблице 4 решения уравнений $g_6x=g_2$ и $xg_6=g_2$.

2. **Теорема Кэли.** В предыдущем параграфе были рассмотрены группы подстановок. Всякая такая группа конечна и имеет порядок $n!$, где n — степень подстановок. Важность этих групп определяется тем, что их подгруппами в известном смысле исчерпываются все конечные группы. Именно справедлива следующая теорема.

Теорема Кэли. *Любая конечная группа G порядка n изоморфна некоторой подгруппе G' группы подстановок степени n.*

Доказательство. Занумеруем каким-либо образом все элементы данной группы G:

$$g_1, g_2, \ldots, g_n.$$

Пусть теперь a — произвольный элемент этой группы. Составим последовательность произведений:

$$g_1a, g_2a, \ldots, g_na. \qquad (1)$$

Все эти произведения различны — из равенства $g_ia = g_ja$ (при $i \neq j$). умножением на a^{-1} справа получалось бы равенство $g_i = g_j$. Поэтому последовательность (1) представляет собой последовательность всех элементов группы*. Значит, последовательность (1) можно записать в виде

$$g_{\alpha_1}, g_{\alpha_2}, \ldots g_{\alpha_n},$$

где $\alpha_1, \alpha_2, \ldots, \alpha_n$— некоторая *перестановка* из чисел $1,2,\ldots,n$. Поставим в соответствие элементу a подстановку

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}.$$

Таким образом, каждому элементу a группы G будет соответствовать определенная подстановка степени n. Эта подстановка переводит число k в число α_k, если произведение g_ka равно элементу g_{α_k} с номером α_k.

Убедимся, что *разным* элементам группы G будут соответствовать *разные* подстановки. Действительно, если $a \neq b$, то $g_1a \neq g_1b$; поэтому подстановки, соответствующие элементам a и b, переводят число 1 в разные числа, т. е. эти подстановки различны.

Обозначим множество из n подстановок, соответствующих элементам $g_1, g_2, \ldots, g_n$ группы G, через G'. Мы установили взаимно однозначное отображение G на G'. Покажем, что это отображение сохраняет операцию. Пусть элементам a и b соответствуют подстановки

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix} \text{ и } \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \beta_1 & \beta_2 & \ldots & \beta_n \end{pmatrix}$$

(во второй подстановке мы изменили порядок чисел в первой строке, соответственно поменяв порядок чисел второй строки,— от этого подстановка не изменится).

Убедимся, что произведению ab будет соответствовать произведение указанных подстановок, т. е. подстановка

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \beta_1 & \beta_2 & \ldots & \beta_n \end{pmatrix}.$$

---

* Внимательный читатель заметит, что последовательность (1) является столбцом таблицы Кэли группы G, соответствующим элементу a заглавной строки.

Иначе говоря, покажем, что для любого $i\,(1 \leqslant i \leqslant n)$ выполняется условие:

$$g_i\,(ab) = g_{\beta_i}.$$

Но это условие легко проверяется: из подстановок, соответствующих элементам a, b, имеем равенства $g_i a = g_{\alpha_i}$, $g_{\alpha_i} b = g_{\beta_i}$, откуда

$$g_i\,(ab) = (g_i a)\,b = g_{\alpha_i} b = g_{\beta_i}.$$

Итак, нами установлен изоморфизм группы G и некоторого множества G' подстановок с обычной операцией умножения подстановок. По основному свойству гомоморфного отображения (§ 3, пункт 3) получаем, что G' есть группа относительно операции умножения подстановок степени n. Теорема доказана.

Эту теорему нетрудно обобщить на случай бесконечных групп. Именно можно доказать, что любая бесконечная группа G изоморфна некоторой подгруппе преобразований множества G. По существу доказательство остается прежним: каждому элементу $a \in G$ сопоставляется преобразование φ_a, переводящее произвольный элемент $g \in G$ в элемент ga, и доказывается, что множество преобразований, сопоставленных всевозможным элементам из G, образует группу, изоморфную группе G.

Доказательство теоремы Кэли можно использовать для исследования вопроса о том, задает ли некоторая таблица групповую операцию на множестве G. Делается это так.

Пусть в заглавной строке таблицы стоят элементы $g_1, g_2, \ldots, g$, Убедившись, что каждый столбец содержит все эти элементы, можно сопоставить элементам $g_1, g_2, \ldots, g_n$ подстановки $p_1, p_2, \ldots, p_n$ тем способом, который применен в доказательстве теоремы Кэли. Для множества G' подстановок $p_1, p_2, \ldots, p_n$ составляется таблица умножения по правилу умножения подстановок и проверяется, что эта таблица задает группу. Для этого достаточно убедиться, что в каждой строке и каждом столбце имеются *все* элементы $p_1, p_2, \ldots, p_n$, отсюда вытекает обратимость операции, а ассоциативность умножения подстановок известна. Если условие обратимости не выполнено, то G' не группа; из доказательства теоремы Кэли следует тогда, что G также не группа. Если условие обратимости выполнено и G' — группа, то (опять-таки по доказательству теоремы Кэли) после замены в таблице подстановок элементов $p_1, p_2, \ldots, p_n$ элементами $g_1, g_2, \ldots, g_n$ должна получиться исходная таблица для G. Следовательно G будет группой в том и только в том случае, когда последний шаг проверки дает исходную таблицу для G.

Пусть, например, на множестве $G = \{g_1, g_2, g_3\}$ операция задана таблицей:

Таблица 5

	g_1	g_2	g_3
g_1	g_1	g_2	g_3
g_2	g_2	g_3	g_1
g_3	g_3	g_1	g_2

Требуется узнать, будет ли множество G группой относительно данной операции.

В каждом столбце таблицы содержатся все элементы G, следовательно элементам g_1, g_2, g_3 сопоставляются соответственно подстановки:

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Составляем таблицу умножения для этих подстановок.

Таблица 6

	p_1	p_2	p_3
p_1	p_1	p_2	p_3
p_2	p_2	p_3	p_1
p_3	p_3	p_1	p_2

В каждой строке и каждом столбце таблицы 6 имеются все подстановки p_1, p_2, p_3. Значит, данное множество подстановок есть группа. Заменяя в таблице 6 элементы p_1, p_2, p_3 элементами g_1, g_2, g_3, получим исходную таблицу 5. Следовательно, множество G является группой относительно операции, заданной таблицей 5.

Вопросы и упражнения

1. Множество чисел $g_1 = 1$, $g_2 = i$, $g_3 = -1$, $g_4 = -i$ образует группу относительно операции умножения. По способу, указанному в теореме Кэли, найти подстановку, соответствующую элементу i этой группы (см. с. 34, табл. 2).

2. Тем же способом, что и в упражнении 1, найти по таблице 4 три подстановки, соответствующие элементам g_2, g_3, g_4 группы подстановок третьей степени (см. с. 36), и убедиться, что произведение первой из них на вторую равно третьей (в согласии с тем, что по таблице $g_2 g_3 = g_4$).

§ 5. Смежные классы и фактор-группы

1. Смежные классы группы по подгруппе. Теорема Лагранжа. Пусть H_1 и H_2 — какие-нибудь два подмножества группы G. Определим произведение подмножеств H_1 и H_2 как совокупность всевозможных произведений $h_1 h_2$, где $h_1 \in H_1$, а $h_2 \in H_2$; будем обозначать это произведение символом $H_1 H_2$. Таким образом,

$$H_1 H_2 = \{x : x = h_1 h_2,\ h_1 \in H_1,\ h_2 \in H_2\}.$$

Если, например, группа G является мультипликативной группой положительных действительных чисел, H_1 — интервалом

(1,2), H_2— интервалом (2,3), то произведением H_1H_2 будет интервал (1,6). Если же в качестве H_1 взять снова интервал (1,2), а в качестве H_2— одноэлементное множество $\left\{\frac{1}{2}\right\}$, то получим, что H_1H_2 есть интервал $\left(\frac{1}{2}, 1\right)$.

Нетрудно показать, что операция умножения подмножеств группы ассоциативна: ввиду ассоциативности операции в группе G для любых трех элементов G имеет место равенство $(h_1h_2)h_3 = h_1(h_2h_3)$, а это означает, что подмножества $(H_1H_2)H_3$ и $H_1(H_2H_3)$ состоят из одних и тех же элементов, т. е. $(H_1H_2)H_3 = H_1(H_2H_3)$. Поэтому в случае произведения более чем двух подмножеств можно не указывать расстановку скобок.

Замечание. Следуя традиции, мы пользуемся здесь мультипликативной терминологией. В конкретных примерах, использующих аддитивную терминологию, предпочтительнее говорить о *сумме* подмножеств H_1 и H_2, обозначая ее символом $H_1 + H_2$. Вообще же под произведением элементов h_1 и h_2 понимается композиция этих элементов $h_1 \circ h_2$ в смысле операции на G, поэтому произведение множеств H_1, H_2 естественно было бы обозначать символом $H_1 \circ H_2$ и называть *композицией* этих множеств. Особо отметим, что определенное выше произведение множеств никоим образом нельзя смешивать с их теоретико-множественным произведением (Алгебра, ч. 1, с. 9).

Пусть теперь H — некоторая подгруппа группы G, а g — произвольный элемент этой группы. Произведение $H\{g\}$ подгруппы H и одноэлементного множества $\{g\}$ назовем *правым смежным классом элемента g по подгруппе H* и будем сокращенно обозначать символом Hg. Таким образом, правый смежный класс элемента g по подгруппе H есть множество всех элементов из H, умноженных на элемент g справа. Аналогично *левый смежный класс элемента g по подгруппе H* определяется как произведение $\{g\}H$, т. е. как совокупность всех произведений вида gh, где $h \in H$, и обозначается через gH. В случае коммутативной группы G для любых элементов g и h имеет место равенство $gh = hg$, поэтому всегда $gH = Hg$, т. е. правый и левый классы любого элемента g по любой подгруппе H совпадают и их можно не различать. Однако в случае произвольной группы, как мы увидим, левый и правый классы одного и того же элемента могут не совпадать.

Нетрудно проверить, что для любого элемента h из подгруппы H класс Hh совпадает с H. Отсюда следует, что если $\bar{g} \in Hg$, т. е. $\bar{g} = hg$, где $h \in H$, то $H\bar{g} = Hhg = Hg$. Таким образом, всякий правый класс совпадает с правым классом любого своего элемента. Аналогичное утверждение справедливо и для левых классов.

Рассмотрим примеры.

1. Пусть G — группа всех подстановок третьей степени, т. е.

$$G = \{g_1, g_2, g_3, g_4, g_5, g_6\},$$

где

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

$$g_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad g_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad g_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

На стр. 36 была дана таблица Кэли этой группы. Приведем эту таблицу еще раз:

Таблица 4

	g_1	g_2	g_3	g_4	g_5	g_6
g_1	g_1	g_2	g_3	g_4	g_5	g_6
g_2	g_2	g_1	g_4	g_3	g_6	g_5
g_3	g_3	g_5	g_1	g_6	g_2	g_4
g_4	g_4	g_6	g_2	g_5	g_1	g_3
g_5	g_5	g_3	g_6	g_1	g_4	g_2
g_6	g_6	g_4	g_5	g_2	g_3	g_1

Как мы уже видели (см. пункт 2, § 3), множество

$$H_1 = \{g_1, g_3\}$$

является подгруппой группы G. Составим правый и левый смежные классы элемента g_6 по подгруппе H_1:

$$H_1 g_6 = \{g_1 g_6,\ g_3 g_6\} = \{g_6,\ g_4\},$$
$$g_6 H_1 = \{g_6 g_1,\ g_6 g_3\} = \{g_6,\ g_5\}.$$

Таким образом, левый и правый классы элемента g_6 не совпадают. Составляя теперь правые смежные классы всех элементов группы G (для вычислений пользуемся таблицей 4), получим:

$$H_1 g_1 = \{g_1,\ g_3\},\ H_1 g_2 = \{g_2,\ g_5\},$$
$$H_1 g_3 = \{g_3,\ g_1\},\ H_1 g_4 = \{g_4,\ g_6\},$$
$$H_1 g_5 = \{g_5,\ g_2\},\ H_1 g_6 = \{g_6,\ g_4\}.$$

Отсюда видно, что различных правых смежных классов оказалось только три:

$$\{g_1,\ g_3\},\ \{g_2,\ g_5\},\ \{g_4,\ g_6\},$$

поскольку классы некоторых различных элементов, например элементов g_4 и g_6, совпадают (эти элементы входят в один и тот же класс).

2. Группа G предыдущего примера имеет, как нетрудно проверить (пользуясь таблицей 4), следующую подгруппу H_2:

$$\{g_1, g_5, g_4\}.$$

Вычисления, аналогичные вычислениям примера 1, показывают, что найдутся только два различных правых класса:

$$\{g_1, g_5, g_4\} \quad \text{и} \quad \{g_2, g_3, g_6\}.$$

Первый из них является правым смежным классом для каждого из элементов подгруппы H_2, второй — для всякого другого элемента группы G. Читателю рекомендуется проверить, что для любого элемента из G правый и левый смежные классы по подгруппе H_2 совпадают.

3. Пусть G — аддитивная группа целых чисел, а H — ее подгруппа, состоящая из чисел, кратных 4, т. е.

$$G = \{\ldots, -2, -1, 0, 1, 2, \ldots\},$$
$$H = \{\ldots, -8, -4, 0, 4, 8, \ldots\}.$$

Группа G коммутативна, поэтому правый и левый смежные классы любого элемента по подгруппе H совпадают,— можно, следовательно, говорить просто о смежном классе какого-либо элемента. Ясно, что для элементов 0,1, 2, 3 получаются следующие смежные классы:

$$H + 0 = \{\ldots, -8, -4, 0, 4, 8, \ldots\},$$
$$H + 1 = \{\ldots, -7, -3, 1, 5, 9, \ldots\},$$
$$H + 2 = \{\ldots, -6, -2, 2, 6, 10, \ldots\},$$
$$H + 3 + \{\ldots, -5, -1, 3, 7, 11, \ldots\}.$$

Поскольку любое целое число содержится в одном из классов $H + 0$, $H + 1$, $H + 2$, $H + 3$, то класс каждого элемента $g \in G$ совпадает с одним из этих классов, т. е. этими классами исчерпываются все различные смежные классы по подгруппе H.

Можно проверить, что в каждом из примеров 1—3 все *различные* правые смежные классы попарно не пересекаются и в сумме дают *всю* группу G. Иными словами, все различные правые классы образуют *разбиение** группы G. То же самое верно и для левых смежных классов. Оказывается, это обстоятельство носит общий характер, т. е. справедлива следующая теорема.

Т е о р е м а. *Какова бы ни была подгруппа H группы G, совокупность всех различных правых (левых) смежных классов по подгруппе H образует разбиение группы G.*

---

* Напомним (см.: Алгебра, ч. 1, с. 20), что совокупность непустых подмножеств множества A образует разбиение A, если эти подмножества попарно не пересекаются и их объединение совпадает с A.

Доказательство. Будем доказывать теорему для случая правых смежных классов — доказательство для левых смежных классов аналогично. Очевидно, что каждый элемент $g \in G$ принадлежит некоторому классу, а именно классу Hg (единица e группы G содержится в H, поэтому $g = eg \in Hg$). Остается показать, что различные классы не имеют общих элементов, т. е. что любые два класса, имеющие хотя бы один общий элемент, совпадают. Но это проверяется просто: если классы Hg_1 и Hg_2 содержат общий элемент $\bar{g}$, то $Hg_1 = H\bar{g}$ и $Hg_2 = H\bar{g}$, откуда $Hg_1 = Hg_2$. Теорема доказана.

Следствием доказанной теоремы является простая, но важная теорема Лагранжа:

Порядок конечной группы делится на порядок любой ее подгруппы.

Действительно, пусть конечная группа G имеет подгруппу H порядка m, состоящую из элементов $h_1, h_2, \ldots, h_m$. Для любого $g \in G$, правый класс Hg состоит из элементов $h_1g, \ldots, h_mg$, которые все различны (из $h_ig = h_jg$ следовало бы $h_i = h_j$). Таким образом, всякий правый класс содержит ровно m элементов. Пусть имеется всего $k \leqslant n$ различных правых классов. Обозначив их через Hg_1, $Hg_2, \ldots, Hg_k$, получаем по предыдущей теореме:

$$G = Hg_1 \cup Hg_2 \cup \ldots \cup Hg_k,$$

т. е. группа G, состоящая из n элементов, разбивается на k непересекающих классов, по m элементам в каждом. Отсюда $n = mk$, значит, n делится на m.

Вопросы и упражнения

1. Составить все различные смежные классы аддитивной группы целых чисел по подгруппе целых чисел, кратных шести (по образцу примера 3). Убедиться, что каждый такой класс состоит из чисел, дающих при делении на шесть один и тот же остаток.

2. Вывести из теоремы Лагранжа, что группа простого порядка не имеет подгрупп, отличных от единичной подгруппы и самой группы.

3. Могут ли какие-нибудь правые смежные классы группы G по различным подгруппам H_1 и H_2 совпадать?

2. Нормальные делители и фактор-группы. Как уже было показано, левый и правый смежные классы одного и того же элемента могут не совпадать (см. пример 1, пункта 1). Особый интерес, однако, представляет случай, когда эти классы совпадают для каждого элемента группы, как это имеет место, например, в коммутативной группе. Примем следующее определение:

Подгруппа H называется *нормальным делителем* группы G, если для всякого элемента $g \in G$ выполняется условие: $Hg = gH$.

Возвращаясь к примерам 1, 2 пункта 1, мы можем сказать теперь, что подгруппа H_1 не является, а подгруппа H_2 является нормальным делителем группы подстановок третьей степени. Подгруппа чисел, кратных 4, аддитивной группы целых чисел будет нормальным делителем группы, так как эта группа коммутативна.

Важность понятия нормального делителя определяется следующей теоремой:

Множество смежных классов группы G по нормальному делителю H образует группу относительно операции умножения классов.

Доказательство. Выше уже отмечалось, что ассоциативность умножения классов вытекает из ассоциативности групповой операции. Покажем теперь, что произведение любых двух смежных классов по нормальному делителю H является смежным классом, т. е. что умножение классов является операцией на множестве классов. Всякие два смежных класса являются смежными классами каких-то элементов g_1 и g_2, т. е. могут быть представлены как произведения Hg_1 и Hg_2. Учитывая, что H — нормальный делитель группы G, получаем:

$$(Hg_1)(Hg_2) = H(g_1H)g_2 = H(Hg_1)g_2 = H(g_1g_2)$$

(здесь используется ассоциативность умножения классов и то очевидное обстоятельство, что $HH = H$). Таким образом, произведение смежных классов Hg_1 и Hg_2 снова является смежным классом (элемента g_1g_2).

Далее, если e — единица группы G, то для класса $He = H$ и любого класса Hg имеем:

$$(Hg)H = H(Hg) = Hg.$$

Следовательно, класс $He = H$ является нейтральным элементом в множестве классов.

Наконец, для любого класса Hg класс Hg^{-1} служит обратным, так как

$$(Hg)(Hg^{-1}) = H(gg^{-1}) = He = H.$$

Итак, все требования, предъявляемые к группе, выполнены. Теорема доказана.

Замечание. Из доказательства теоремы видно, что произведение классов любых двух элементов g_1, g_2 совпадает с классом их произведения g_1g_2.

Группу смежных классов группы G по нормальному делителю H называют *фактор-группой* и обозначают символом G/H.

Таким образом, всякая группа G порождает целый ряд новых групп — каждому нормальному делителю H группы G отвечает своя фактор-группа G/H.

Фактор-группа G/H по любому нормальному делителю H представляет собой группу классов, образующих *разбиение* группы G (см. теорему на стр. 42). Мы докажем теперь, что верно и обратное утверждение:

Всякая группа классов, образующих разбиение группы G, является некоторой фактор-группой группы G.

Доказательство. Покажем, что нейтральный элемент H группы классов является подгруппой группы G. Пусть h_1 и h_2—любые элементы из H. Элемент $h_1h_2^{-1}$ принадлежит некоторому классу K

разбиения $h_1 h_2^{-1} \in K$. Тогда и элемент $h_1 \in H$ принадлежит этому классу K:

$$h_1 = (h_1 h_2^{-1})\, h_2 \in KH = K.$$

Но раз классы H и K имеют общий элемент h_1, то они совпадают. Значит, $H = K$ и $h_1 h_2^{-1} \in H$. Мы получили, что класс вместе с любыми своими элементами h_1, h_2 содержит элемент $h_1 h_2^{-1}$. Следовательно, H является подгруппой группы G (см. условие 3° на с. 25).

Убедимся теперь, что H есть нормальный делитель группы G. Пусть g — произвольный элемент группы G, и пусть элемент g принадлежит классу K, а элемент g^{-1}— классу $\tilde{K}$. Тогда класс $K\tilde{K}$; содержит единицу e группы G и поэтому совпадает с классом H: $K\tilde{K} = H$. Значит, $Kg^{-1} \subset H$ и $K \subset Hg$. С другой стороны, из равенства $HK = K$ вытекает, что $Hg \subset K$. Следовательно, $K = Hg$. Аналогично доказывается, что $K = gH$. Таким образом, для произвольного элемента $g \in G$ выполняется равенство $Hg = gH$, т.е. подгруппа H является нормальным делителем группы G.

Одновременно установлено, что всякий класс K группы классов совпадает со смежным классом Hg любого элемента $g \in K$ по нормальному делителю H. Значит, группа классов является группой смежных классов по H или фактор-группой G/H. Теорема доказана.

Для иллюстрации понятия фактор-группы вернемся к примеру 3 пункта 1, в котором множество чисел, кратных 4, составляет подгруппу H аддитивной группы G целых чисел; в силу коммутативности группы G подгруппа H является нормальным делителем этой группы. Элементами фактор-группы по этому нормальному делителю будут классы $H + 0$, $H + 1$, $H + 2$, $H + 3$, которыми исчерпываются все различные смежные классы. Нетрудно найти всевозможные попарные суммы этих классов (например, сумма классов $H + 2$ и $H + 3$ есть класс числа $2 + 3$, а так как это число попадает в класс $H + 1$, то $(H + 2) + (H + 3) = H + 1$).
В результате мы получим следующую таблицу Кэли для фактор-группы G/H:

Таблица 7

	$H+0$	$H+1$	$H+2$	$H+3$
$H+0$	$H+0$	$H+1$	$H+2$	$H+3$
$H+1$	$H+1$	$H+2$	$H+3$	$H+0$
$H+2$	$H+2$	$H+3$	$H+0$	$H+1$
$H+3$	$H+3$	$H+0$	$H+1$	$H+2$

Понятия нормального делителя и фактор-группы являются центральными понятиями теории групп и используются в важнейших ее приложениях. Например, открытое Галуа* условие разрешимости алгебраического уравнения в радикалах состоит в том, что некоторая группа G, сопоставляемая данному уравнению, должна допускать такую цепочку подгрупп G_1, G_2,..., $G_k = \{e\}$, что каждая следующая служит нормальным делителем предыдущей и все фактор-группы G/G_1, G_1/G_2,..., циклические.

Вопросы и упражнения

1. Показать, что подгруппа H группы G тогда и только тогда является нормальным делителем, когда для любого элемента $h \in H$ и любого элемента $q \in G$ элемент $q^{-1}hq$ содержится в H.

2. Показать, что единичная подгруппа группы G и сама группа G являются нормальными делителями группы G. Какими будут фактор-группы по этим подгруппам?

3. Проверить, что пересечение двух нормальных делителей группы G также будет нормальным делителем этой группы.

3. Гомоморфные образы группы. По теореме пункта 3 § 3 гомоморфный образ любой группы также является группой. С помощью понятия фактор-группы удается существенно дополнить этот результат — оказывается, всякому гомоморфному отображению группы G на группу G' отвечает изоморфное отображение группы G' на некоторую фактор-группу группы G. Иными словами, если имеется отображение группы G на группу G', сохраняющее операцию, то можно построить *взаимно однозначное* отображение группы G' на некоторую фактор-группу G/H, также сохраняющее операцию. Итак, докажем следующую теорему:

Теорема о гомоморфизме. *Если группа G' гомоморфна группе G, то группа G' изоморфна некоторой фактор-группе группы G.*

Доказательство. Пусть φ — гомоморфное отображение G на G'. По каждому элементу $g' \in G'$ составим класс всех его прообразов, т. е. класс всех тех элементов из G, который отображение φ переводит в g'. Множество всевозможных таких классов образует, как нетрудно видеть, разбиение группы G. Зададим отображение Φ группы G' на указанное множество классов, полагая, что для каждого элемента $g' \in G'$ класс $\Phi(g')$ как раз и является классом всех прообразов этого элемента. (Иными словами, $g \in \Phi(g')$ тогда и только тогда, когда $\varphi(g) = g'$.) Отображение Φ взаимно однозначно, поскольку разным элементам группы G' отвечают разные классы прообразов.

Покажем теперь, что для любых элементов g'_1, g'_2 группы G' выполняется равенство

$$\Phi(g'_1)\,\Phi(g'_2) = \Phi(g'_1 g'_2).$$

Отсюда будет следовать, что умножение классов есть операция на данном множестве классов и что отображение Φ изоморфно.

---

* Эварист Галуа (1811—1832) — французский математик. Замечательные идеи, выдвинутые Галуа, легли в основу современной теории групп.

Нужно убедиться, что каждый элемент произведения классов $\Phi(g_1')$ и $\Phi(g_2')$ принадлежит классу $\Phi(g_1'g_2')$ и обратно.

Пусть $g \in \Phi(g_1')\Phi(g_2')$. Тогда $g = g_1g_2$, причем $\varphi(g) = g_1'$ и $\varphi(g) = g_2'$. Отсюда получаем: $\varphi(g) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = g_1'g_2'$. Значит, $g \in \Phi(g_1'g_2')$.

Обратно, пусть $g \in \Phi(g_1'g_2')$. Возьмем произвольный элемент $g_2 \in \Phi(g_2')$ и представим элемент g в виде произведения элементов $\bar{g} = gg_2^{-1}$ и g_2: $g = \bar{g}g_2$. Имеем одновременно:

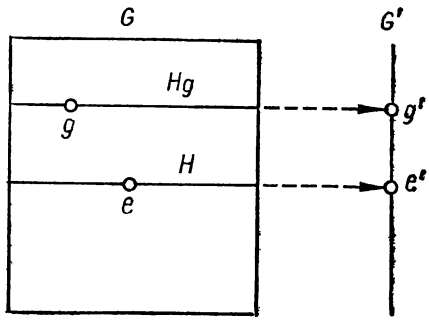

Рис. 5

$$\varphi(g) = g_1'g_2' \text{ и } \varphi(g) = \varphi(\bar{g})\varphi(g_2) = \varphi(\bar{g})g_2'.$$

Отсюда следует, что $\varphi(\bar{g}) = g_1'$, т. е. $\bar{g} \in \Phi(g_1')$. Значит,

$$g \in \Phi(g_1')\Phi(g_2').$$

Мы установили, что множество классов с операцией умножения классов изоморфно группе G'. Поэтому оно само является группой. По теореме о группе классов, образующих разбиение группы G (см. стр. 44), получаем, что группа G' изоморфна некоторой факторгруппе G/H группы G.

Теорема доказана.

Замечание. В группе G/H нормальный делитель H является нейтральным элементом. Как было показано ранее (см. стр. 27), при изоморфном отображении Φ группы G' на группу G/H нейтральный элемент e' группы G' переходит в нейтральный элемент группы G/H, т. е. $\Phi(e') = H$. Следовательно, класс H состоит из всех прообразов единицы e' группы G' при гомоморфизме φ. Этот класс называют *ядром гомоморфизма* φ. Таким образом, если группа G гомоморфно отображается на группу G', то группа G' изоморфна фактор-группе группы G/H по ядру H этого гомоморфизма.

Отметим еще, что если $\varphi(g) = g'$, то класс Hg, содержащий элемент g, совпадает с классом всех прообразов элемента g'.

Рисунок 5 наглядно иллюстрирует соответствие между G' и G/H. На этом рисунке группа G условно изображена в виде прямоугольника, а группа G' — в виде вертикального отрезка. Отображение G на G' представлено как проектирование. Различные классы группы G по подгруппе H изображаются горизонтальными отрезками; все элементы каждого такого класса отображаются в один элемент из G'. Сопоставляя каждому элементу $g' \in G'$ соответствующий горизонтальный отрезок, получаем изоморфное отображение группы G' на группу G/H.

Теорема о гомоморфизме имеет много различных приложений. Чтобы дать некоторое представление о характере этих приложений, используем теорему о гомоморфизме для описания циклических групп.

В п. 2 было показано, что фактор-группой аддитивной группы $\mathbf{Z}$ целых чисел по подгруппе H_4 чисел, кратных 4, является группа из четырех различных классов: $\{H_4+0,\ H_4+1,\ H_4+2,\ H_4+3\}$. Нетрудно проверить, что эта группа циклическая и ее образующей служит класс H_4+1. Аналогичные рассуждения показывают, что всякая фактор-группа $\mathbf{Z}/H_n$ (где H_n — подгруппа чисел, кратных числу $n \geqslant 1$) является циклической группой из n элементов — классов $H_n+0,\ H_n+1,\ldots,\ H_n+(n-1)$ — с классом H_n+1 в качестве образующей; такую группу называют обычно *группой вычетов по модулю n*.

Наконец, фактор-группа $\mathbf{Z}/H_0$, состоящая из всевозможных одноэлементных классов $\{k\}$, где k — любое целое число, изоморфна, как нетрудно видеть, самой группе $\mathbf{Z}$.

Заметим, далее, что группами $\mathbf{Z}/H_0$, $\mathbf{Z}/H_1,\ldots$, $\mathbf{Z}/H_n,\ldots$ исчерпываются в с е фактор-группы группы $\mathbf{Z}$, поскольку группами H_0, $H_1,\ldots$, $H_n,\ldots$ исчерпываются все ее подгруппы (см. пункт 4, § 3). ...

Пусть теперь $G=(g)$ — произвольная циклическая группа с образующей g. Отобразим аддитивную группу $\mathbf{Z}$ на группу G, поставив в соответствие каждому числу k из $\mathbf{Z}$ элемент g^k из G: $k \to g^k$. Такое отображение будет, очевидно, гомоморфизмом: если $k_1 \to g^{k_1}$ и $k_2 \to g^{k_2}$, то $k_1+k_2 \to g^{k_1+k_2}=g^{k_1}g^{k_2}$. Значит, по теореме о гомоморфизме группа G *изоморфна* одной из фактор-групп группы $\mathbf{Z}$, и мы приходим к следующему выводу: любая циклическая группа изоморфна одной из фактор-групп $\mathbf{Z}/H_k$. Иными словами,

Все циклические группы исчерпываются аддитивной группой целых чисел и различными группами вычетов.

В заключение этого раздела рассмотрим следующую важную задачу из геометрии.

З а д а ч а. Показать, что в группе G всех движений пространства (см. задачу на с. 21) подгруппа H параллельных переносов является нормальным делителем и что фактор-группа G/H изоморфна группе F всех вращений пространства вокруг некоторой точки.

Р е ш е н и е. Введем некоторые обозначения. Пусть в пространстве выбрана какая-нибудь точка O. Любая точка M пространства определяется тогда своим радиус-вектором $\boldsymbol{r}=\overrightarrow{OM}$, и можно поэтому отождествлять точку и ее радиус-вектор. Точку, в которую движение g преобразует точку $\boldsymbol{r}$, будем обозначать символом $g(\boldsymbol{r})$. В частности, для переноса h на вектор $\boldsymbol{a}$ и любой точки $\boldsymbol{r}$ имеем:

$$h(\boldsymbol{r})=\boldsymbol{r}+\boldsymbol{a}.$$

Из геометрии известно, что если выбрана какая-нибудь точка O в пространстве, то любое движение g можно единственным образом представить в виде произведения некоторого вращения f вокруг точки O и некоторого переноса h: $g=fh$. Поставив в соответствие движению $g=fh$ вращение f, мы получим поэтому отображение группы G на группу F. Покажем, что

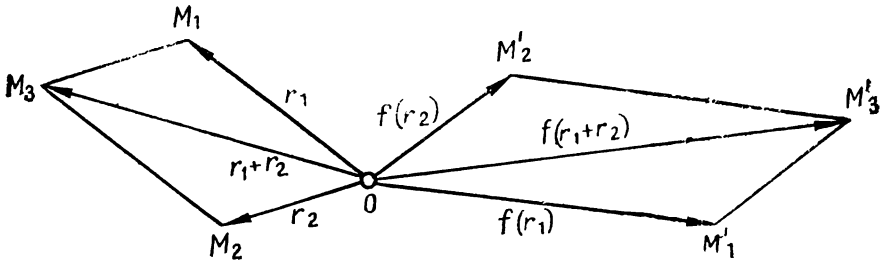

Рис. 6

построенное отображение сохраняет операцию. С этой целью установим сначала следующий вспомогательный факт: для произвольных точек r_1 и r_2 и любого вращения f выполняется условие:

$$f(r_1 + r_2) = f(r_1) + f(r_2). \tag{1}$$

Действительно, векторы r_1, r_2, $r_1 + r_2$ являются сторонами и диагональю параллелограмма с вершиной в точке O (рис. 6). Обозначим концы этих векторов соответственно через M_1, M_2, M_3. При вращении f точки M_1, M_2, M_3 перейдут в точки M_1', M_2', M_3'. Равенство пространственного четырехугольника $OM_1'M_2'M_3'$ и параллелограмма $OM_1M_2M_3$ следует из равенства их сторон и диагоналей. Поэтому четырехугольник $OM_1'M_2'M_3'$ также является параллелограммом, откуда и вытекает условие (1).

С помощью условия (1) легко доказывается, что движение hf, где h означает перенос на вектор a, равно движению $f\bar{h}$, где $\bar{h}$ есть перенос на вектор $f(a)$. В самом деле, для произвольного r

$$(hf)(r) = f(h(r)) = f(r + a) = f(r) + f(a)$$

и

$$(f\bar{h})(r) = \bar{h}(f(r)) = f(r) + f(a)$$

Пусть теперь f_1h_1 и f_2h_2 — любые два движения; им соответствуют вращения f_1 и f_2. Нужно показать, что их произведению соответствует вращение f_1f_2. Но это вытекает из того, что

$$(f_1h_1)(f_2h_2) = f_1(h_1f_2)h_2 = f_1f_2\bar{h}_1h_2.$$

Таким образом, построенное отображение является гомоморфизмом. При этом в единицу группы F переходят элементы группы H, и только они. По замечанию к теореме о гомоморфизме на с. 47 группа H представляет собой ядро данного гомоморфизма и группа F изоморфна фактор-группе G/H

Вопросы и упражнения

1. Доказать, что если конечная группа G гомоморфно отображается на конечную группу G', то порядок группы G' является делителем порядка группы G.

2. Доказать, что гомоморфный образ G' циклической группы G также является циклической группой.

§ 6. Кольца и поля

1. Определение кольца и поля. Как было показано в пункте 1 § 3, множество **R** действительных чисел является группой относительно операции сложения, причем эта группа коммутативна. Иначе говоря, операция сложения действительных чисел удовлетворяет следующим условиям (a, b, c — произвольные элементы множества **R**):

1°. $(a + b) + c = a + (b + c)$ (ассоциативность сложения);

2°. $a + b = b + a$ (коммутативность сложения);

3°. Уравнение $a + x = b$ имеет ровно одно решение для любых a и b (обратимость сложения).

Кроме того, операция сложения связана с другой операцией на **R** — операцией умножения — двумя законами дистрибутивности:

4°. $(a + b)c = ac + bc$, $a(b + c) = ab + ac$.

(правая и левая дистрибутивность умножения относительно сложения).

Наконец, операция умножения удовлетворяет условиям, аналогичным условиям 1°— 3°.

5°. $(ab)c = a(bc)$ (ассоциативность умножения);

6°. $ab = ba$ (коммутативность умножения);

7°. Уравнение $ax = b$ имеет ровно одно решение для любого $a \neq 0$ и любого b (ограниченная обратимость умножения).

Обобщая свойства множества **R**, будем рассматривать произвольное множество с двумя операциями, одну из которых условимся называть сложением, а другую — умножением. Будем применять обычную символику для обозначения этих операций и символом 0 обозначать нейтральный элемент относительно сложения.

Множество P с операциями сложения и умножения называется *кольцом*, если для любых элементов a, b, c из P выполняются свойства 1°—5°, и *полем*, если в P содержатся элементы, отличные от 0, и выполняются свойства 1°—7°.

Из приведенного определения видно, что поле является кольцом, для которого выполняются дополнительные требования 6°, 7°. Поэтому любое свойство кольца будет справедливо также для поля. Обратное, однако, неверно: свойства 6°, 7° не являются следствиями свойств 1°—5°, потому что, как мы увидим, существуют кольца, не являющиеся полями. Рассмотрим некоторые примеры.

1. Множество **Q** рациональных чисел с обычными операциями сложения и умножения является полем, поскольку суммы и произведения рациональных чисел являются снова рациональными числами, уравнение $a + x = b$ с рациональными a и b имеет единственное решение (свойство 3°), то же самое верно для уравнения $ax = b$ при $a \neq 0$ (свойство 7°), а свойства 1°, 2°, 4° — 6° выполняются для всех действительных чисел, и в частности для чисел рациональных.

2. Множество M квадратных матриц некоторого заданного порядка n является кольцом относительно операций сложения и умножения матриц, так как для этих операций свойства 1°—5° справедливы. Однако это множество при $n > 1$ не будет полем уже потому, что умножение матриц некоммутативно (нарушается свойство 6°).

3. Множество целых чисел есть кольцо относительно обычных операций умножения и сложения, но не поле, так как нарушается свойство 7°; например, уравнение $2x = 1$ не имеет целых решений.

В последнем примере, помимо требований 1°—5°, предъявляемых к кольцу, выполняется также условие 6° коммутативности умножения. Подобные системы принято называть *коммутативными кольцами.*

4. Пусть множество A состоит из чисел 0 и 1, $A = \{0,1\}$, и пусть операция сложения на A определяется правилом:

$$a + b = \begin{cases} 0, & \text{если } a = b, \\ 1, & \text{если } a \neq b, \end{cases}$$

а операция умножения — обычным образом. Легко проверить, что все свойства 1°—7° выполняются — такую проверку можно осуществить с помощью конечного перебора. В частности, для проверки свойства 7° достаточно убедиться, что уравнения $1 \cdot x = 0$ и $1x = 1$ имеют ровно по одному решению. Проверив поочередно каждое из свойств 1°—7°, получаем, что множество A с указанными операциями есть поле. Это пример так называемого *конечного поля*, т. е. поля с конечным числом элементов.

З а д а ч а 1. Рассмотрим множество C всех функций вида

$$a_0 + a_1\cos x + a_2\cos 2x + \ldots + a_n \cos nx,$$

где $a_0, a_1, a_2, \ldots, a_n$ — любая конечная последовательность действительных чисел. Выяснить, является ли множество C кольцом относительно операций сложения и умножения числовых функций.

Решить тот же вопрос для множества S всех функций вида

$$a_0 + a_1\sin x + a_2\sin 2x + \ldots + a_n \sin nx.$$

Р е ш е н и е. Суммы и произведения функций из C также являются функциями из C. Для сумм это очевидно, а для произведений следует из того, что при любых натуральных k и l справедливо тождество

$$\cos kx \cdot \cos lx = \frac{1}{2}\cos(k - l)x + \frac{1}{2}\cos(k + l)x.$$

Таким образом, сложение и умножение функций являются операциями на C.

Условиям 1°, 2°, 4°, 5° определения кольца удовлетворяют любые числовые функции, в частности функции из C. Условие 3° для множества C также выполняется, поскольку разность любых двух функций из этого множества снова принадлежит этому множеству.

Итак, множество C есть кольцо.

Однако в случае множества S вопрос решается отрицательно, так как умножение функций не будет операцией на S. Например, произведение $\sin x$ на $\sin x$ не принадлежит S, иначе мы имели бы:

$$\sin^2 x = a_0 + a_1 \sin x + \ldots + a_m \sin mx,$$

откуда следовало бы, что (отличная от нулевой) четная функция $\sin^2 x - a_0$ является одновременно и нечетной.

З а д а ч а 2. Пусть на множестве P заданы операции сложения и умножения, удовлетворяющие условиям 1°, 4°, 5° из определения кольца, и операция сложения обратима. Пусть, кроме того, в P содержится нейтральный элемент относительно операции умножения. Показать, что P является кольцом.

Р е ш е н и е. Нужно доказать, что выполняется условие 2° коммутативности сложения. Обозначим, как обычно, нейтральный элемент относительно умножения символом 1. Пользуясь законами дистрибутивности 4°, для произвольных a и b из P получаем одновременно:

$$(a + b)(1 + 1) = a(1 + 1) + b(1 + 1) = a + a + b + b,$$
$$(a + b)(1 + 1) = (a + b)1 + (a + b)1 = a + b + a + b.$$

Таким образом,

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

Отсюда следует, что

$$a + b + b = b + a + b,$$

иначе уравнение $a + x = a + b + a + b$ имело бы два решения: $a + b + b$ и $b + a + b$, что невозможно ввиду обратимости сложения. Наконец, из равенства $a + b + b = b + a + b$, пользуясь единственностью решения уравнения $x + b = b + a + b$, получаем окончательно:

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

Итак, условие 2° выполнено, и P есть кольцо.

Вопросы и упражнения

1. Почему поле не является группой относительно операции умножения?

2. Показать, что множество всех чисел вида $a + b\sqrt{3}$, где a и b — любые рациональные числа, является полем относительно обычных операций сложения и умножения чисел.

3. На множестве $\mathbf{R}$ действительных чисел с обычной операцией сложения определим операцию умножения условием: $ab = b$. Показать, что множество $\mathbf{R}$ не будет кольцом относительно данных операций.

2. Основные общие свойства колец и полей. В этом пункте будут изучены некоторые свойства колец, являющиеся следствиями

свойств 1°—4°. Такие свойства выполняются, следовательно, как для колец, так и для полей.

Напомним, что множество P, удовлетворяющее свойствам 1°—3°, является (коммутативной) группой относительно операции сложения. Будем поэтому пользоваться аддитивной терминологией. Учитывая, что противоположным элементу $-a$ будет элемент a (ибо $a + (-a) = (-a) + a = 0$), получим:

$$-(-a) = a. \tag{1}$$

Обозначим символом $b - a$ решение уравнения $a + x = b$ (это решение существует и единственно в силу свойства 2°). Элемент $b - a$ будем называть *разностью* элементов b и a. Легко проверяется, что для любых элементов a и b справедливы равенства:

$$b - a = b + (-a), \tag{2}$$

$$-(a + b) = (-a) + (-b), \tag{3}$$

$$a - a = 0. \tag{4}$$

Установим теперь некоторые дальнейшие свойства колец.

Свойство. 1. Для любых элементов a, b и c произвольного кольца P выполняются следующие равенства (дистрибутивные законы для разности):

$$a(b - c) = ab - ac, \tag{5_1}$$

$$(b - c)a = ba - ca. \tag{5_2}$$

Проверим, например, первое из этих равенств. По определению разности элемент $b - c$ есть решение уравнения $c + x = b$, т. е. справедливо равенство $c + (b - c) = b$.

Умножая это равенство слева на элемент a и пользуясь вторым из дистрибутивных законов для суммы (свойство 4°), получаем:

$$ac + a(b - c) = ab.$$

Поэтому элемент $a(b - c)$ является (единственным) решением уравнения $ac + x = ab$, т. е. совпадает с элементом $ab - ac$.

Равенство (5_2) проверяется аналогично.

Свойство 2. Для любого элемента a кольца P и элемента 0 выполняются равенства:

$$a \cdot 0 = 0, \tag{6_1}$$

$$0 \cdot a = 0. \tag{6_2}$$

(Умножение любого элемента справа или слева на нуль дает нуль, как говорят, нуль является *поглощающим* элементом.)

Для проверки свойства 2 достаточно в равенствах (5_1), (5_2) положить $b = c$.

Свойство 3. (Правило знаков.) Для любых элементов a и b кольца P выполняются равенства:

$$(-a)b = -ab, \tag{7_1}$$
$$a(-b) = -ab, \tag{7_2}$$
$$(-a)(-b) = ab \tag{7_3}$$

Докажем равенство (7_1). Элемент $-a$ является противоположным элементу a, т. е. справедливы равенства

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

Умножая эти равенства на элемент b справа, пользуясь дистрибутивностью умножения и учитывая, что по свойству 2 $0 \cdot b = 0$, получаем:

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

Отсюда видно, что элемент $(-a)b$ является противоположным элементу ab, т. е. $(-a)b = -ab$.

Равенство (7_2) проверяется аналогично, а равенство (7_3) доказывается с помощью равенств (7_1) и (7_2):

$$(-a)(-b) = -(a(-b)) = -(-ab) = ab.$$

Свойства 1—3 показывают, что в произвольных кольцах выполняются многие «привычные» законы сложения и умножения чисел. Однако существуют кольца (а иногда и поля), в которых некоторые законы операций над числами не выполняются. Известно, скажем, что сумма любого количества одинаковых отличных от нуля чисел не равна нулю. В то же время можно указать поле, в котором имеется такой элемент $a \neq 0$, что для некоторого натурального n

$$\underbrace{a + a + \cdots + a}_{n \text{ раз}} = 0.$$

Таким будет, например, поле из чисел 0 и 1 с обычной операцией умножения и операцией сложения, задаваемой равенствами: $1 + 1 = 0 + 0 = 0$, $1 + 0 = 0 + 1 = 1$ (см. пример 4 пункта 1).

Далее, известно, что если произведение двух чисел равно нулю, то хотя бы одно из этих чисел также равно нулю. Однако в некоторых кольцах это свойство нарушается. Пусть, например, на множестве $\mathbf{R}^2$ упорядоченных пар действительных чисел операции сложения и умножения задаются правилами:

$$\langle a, b\rangle + \langle c, d\rangle = \langle a + c, b + d\rangle,$$
$$\langle a, b\rangle \cdot \langle c, d\rangle = \langle ac, bd\rangle.$$

Множество $\mathbf{R}^2$ с такими операциями будет, как легко проверить, кольцом. Нулем этого кольца является пара $\langle 0,0\rangle$. При этом произведение двух отличных от нуля пар $\langle 0,1\rangle$ и $\langle 1,0\rangle$ будет равно нулю:

$$\langle 0, 1\rangle \cdot \langle 1, 0\rangle = \langle 0, 0\rangle.$$

Отличные от нуля элементы a и b, произведение которых равно нулю, принято называть *делителями нуля.*

Таким образом, в некоторых кольцах существуют делители нуля.

Вопросы и упражнения

1. Доказать равенство (5_2) по образцу доказательства равенства (5_1).

2. Доказать равенство (7_2) по образцу доказательства равенства (7_1).

3. Специфические свойства полей. В этом пункте мы рассмотрим такие свойства полей, которые справедливы не во всяком кольце.

Свойство I. В поле не существует делителей нуля: если $a \neq 0$ и $b \neq 0$, то $ab \neq 0$.

Действительно, пусть $a \neq 0$, $b \neq 0$, но $ab = 0$. Тогда уравнение $ax = 0$ имеет два различных решения: $x = b$ и $x = 0$, что противоречит пункту 7° определения поля.

Свойство II. Подмножество $P \setminus \{0\}$ ненулевых элементов поля является коммутативной группой относительно операции умножения.

Это свойство вытекает из свойства I и определения поля. Из него в свою очередь получаются такие следствия:

a) всякое поле P содержит нейтральный элемент относительно операции умножения;

b) вместе с каждым ненулевым элементом поле P содержит единственный обратный ему элемент.

Говоря об операции умножения, естественно пользоваться мультипликативной терминологией: нейтральный элемент обозначать символом 1 (и называть *единицей поля*), а обратный элемент для ненулевого элементы a — символом a^{-1} или символом $\frac{1}{a}$.

Отметим, что свойство II и его следствия не распространяются на произвольные кольца. Например, множество четных целых чисел с обычными операциями сложения и умножения является кольцом, в котором единица отсутствует.

В формулировке следующего свойства символ $\frac{b}{a}$ (где $a \neq 0$) будет означать (единственное) решение уравнения $ax = b$.

Свойство III. В любом поле P выполняются следующие равенства:

$$-a = (-1)\,a \qquad (a \text{ — любой элемент из } P); \tag{8}$$

$$\frac{b}{a} = b \cdot a^{-1} \qquad (b \text{ — любое}, \ a \neq 0); \tag{9}$$

$$\frac{1}{ab} = \frac{1}{a} \cdot \frac{1}{b} \qquad (a \neq 0, \ b \neq 0); \tag{10}$$

$$\left(\frac{b}{a}\right)^{-1} = \frac{a}{b} \qquad (a \neq 0,\ b \neq 0); \tag{11}$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad (a,\ c \text{ — любые},\ b \neq 0,\ d \neq 0) \tag{12}$$

Доказательство.

Равенство (8). Достаточно проверить, что элемент $(-1)a$ является решением уравнения $a + x = 0$:

$$a + (-1)\,a = 1 \cdot a + (-1) \cdot a = (1 + (-1))\,a = 0 \cdot a = 0.$$

(Используются последовательно свойство единицы, правая дистрибутивность кольца, свойство 2 кольца.)

Равенство (9). Нужно показать, что элемент ba^{-1} является решением уравнения $ax=b$, что проверяется непосредственной подстановкой.

Равенство (10). Имеем: $a \cdot \frac{1}{a} = 1$, $b \cdot \frac{1}{b} = 1$. Отсюда, пользуясь свойствами 5°, 6° пункта 1, получим:

$$(ab)\left(\frac{1}{a} \cdot \frac{1}{b}\right) = \left(a \cdot \frac{1}{a}\right) \cdot \left(b \cdot \frac{1}{b}\right) = 1 \cdot 1 = 1.$$

Равенство (11). По свойству (9) $\frac{b}{a} = ba^{-1}$, а по свойству (10) $(ba^{-1})^{-1} = b^{-1}(a^{-1})^{-1} = b^{-1}a$, т. е. $\left(\frac{b}{a}\right)^{-1} = b^{-1}a$. Но снова по свойству (9) $\frac{a}{b} = ab^{-1}$. Следовательно, в силу коммутативности умножения элементы $\left(\frac{b}{a}\right)^{-1}$ и $\frac{a}{b}$ совпадают.

Равенство (12). Достаточно, очевидно, проверить равенство

$$\left(\frac{a}{b} + \frac{c}{d}\right)bd = ad + bc.$$

Предоставляем эту проверку читателю.

Свойство IV. Если для некоторого целого положительного числа n выполняется равенство

$$n1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ раз}} = 0$$

(где 1 — единица поля), то и для любого элемента a поля справедливо равенство $na=0$. Обратно, если для какого-либо элемента a, отличного от нуля, выполняется равенство $na = 0$, то имеет место также и равенство $n1 = 0$.

Доказательство. Пользуясь законом дистрибутивности 4°, получаем для любого элемента a:

$$a(n1) = a\underbrace{(1+1+\cdots+1)}_{n\text{ раз}} = \underbrace{a\cdot 1 + a\cdot 1 + \cdots + a\cdot 1}_{n\text{ раз}} =$$
$$= \underbrace{a + a + \cdots + a}_{n\text{ раз}} = na.$$

Отсюда, если $n1 = 0$, то по свойству 2 колец $na = 0$. Обратно, если $na = 0$ и $a \neq 0$, то по свойству I получаем, что $n1 = 0$.

Свойство IV отражает важную особенность полей и дает повод к следующему определению:

Если существуют целые положительные числа n, для которых $n1 = 0$, то наименьшее из таких чисел называется *характеристикой* поля; в противном случае характеристикой поля считается число нуль.

Из свойства IV вытекает, что в случае поля положительной характеристики n для любого элемента a выполняется равенство $na = 0$ и что в случае поля характеристики нуль это равенство не имеет места ни для одного отличного от нуля элемента a ни при каких целых положительных n.

Конечное поле, рассмотренное в примере 4 пункта 1, имеет характеристику 2, а поле действительных чисел является полем нулевой характеристики.

Вопросы и упражнения

1. Убедиться, что кольцо квадратных матриц порядка n (см. пример 2 пункта 1) обладает (при $n > 1$) делителями нуля.

2. Почему число 1 не может быть характеристикой поля?

3. Доказать, что если характеристика поля не равна нулю, то она является простым числом.

Указание. Проверить, что для составного числа $n = n_1n_2$ и единицы поля имеет место равенство $n1 = (n_11)(n_21)$.

4. Подкольца и подполя. Понятия подкольца и подполя определяются по существу совершенно так же, как понятие подгруппы.

Подмножество L кольца K называется *подкольцом* кольца K, если L является кольцом относительно операций сложения и умножения, заданных в K.

Подмножество Q поля P называется *подполем* поля P, если Q является полем относительно операций сложения и умножения, заданных в P. Поле P называется при этом *расширением* поля Q.

Из определения подкольца следует, что L будет подкольцом кольца K, если L *замкнуто* относительно обеих операций (т. е. вместе с любыми двумя своими элементами содержит также их сумму и произведение) и если для любых a, b из L уравнение $a + x = b$ имеет (единственное) решение в L. Остальные требования, входящие в определение кольца, выполняются автоматически, так как L является подмножеством K.

Точно так же подмножество Q поля P будет его подполем, если оно замкнуто относительно каждой из двух операций на P и при любых a и b из Q оба уравнения $a + x = b$ и $ax = b$ (последнее при $a \neq 0$) имеют решения в Q.

Приведем несколько примеров. Кольцо четных целых чисел является подкольцом кольца рациональных чисел, которое в свою очередь есть подкольцо кольца действительных чисел.

Поле рациональных чисел будет подполем поля действительных чисел. При любом рациональном $a > 0$ множество всех чисел вида $r_1 + r_2\sqrt{a}$, где r_1, r_2 — любые рациональные числа, составляет поле, являющееся подполем поля действительных чисел.

В кольце M всех матриц

$$\begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix}$$

с рациональными r_1, r_2, r_3, r_4 рассмотрим подмножество L, состоящее из матриц вида

$$\begin{pmatrix} r_1 & r_2 \\ 2r_2 & r_1 \end{pmatrix}.$$

Нетрудно проверить, что это подмножество замкнуто относительно операций умножения и сложения:

$$\begin{pmatrix} r_1 & r_2 \\ 2r_2 & r_1 \end{pmatrix} + \begin{pmatrix} s_1 & s_2 \\ 2s_2 & s_1 \end{pmatrix} = \begin{pmatrix} r_1 + s_1 & r_2 + s_2 \\ 2(r_1 + s_1) & r_1 + s_1 \end{pmatrix},$$

$$\begin{pmatrix} r_1 & r_2 \\ 2r_2 & r_1 \end{pmatrix} \cdot \begin{pmatrix} s_1 & s_2 \\ 2s_2 & s_1 \end{pmatrix} = \begin{pmatrix} r_1s_1 + 2r_2s_2 & r_1s_2 + r_2s_1 \\ 2(r_2s_1 + r_1s_2) & r_1s_1 + 2r_2s_2 \end{pmatrix}.$$

Кроме того, всякое уравнение вида

$$\begin{pmatrix} r_1 & r_2 \\ 2r_2 & r_1 \end{pmatrix} + X = \begin{pmatrix} s_1 & s_2 \\ 2s_2 & s_1 \end{pmatrix}$$

имеет решение, принадлежащее L.

Следовательно, L является подкольцом кольца M.

З а д а ч а. Расширение P поля $\mathbf{Q}$ рациональных чисел, содержащее действительное число α, будем называть α-расширением. Рассмотрим множество $Q(\alpha)$ всевозможных дробей вида

$$\frac{r(\alpha)}{s(\alpha)}. \qquad (*)$$

где $r(x)$ и $s(x)$ — многочлены одного переменного с рациональными коэффициентами и $s(\alpha) \neq 0$. Показать, что $Q(\alpha)$ является α-расширением и что любое α-расширение P содержит $Q(\alpha)$.

Р е ш е н и е. Покажем, что множество $Q(\alpha)$ является полем относительно обычных операций сложения и умножения. Прежде всего суммы и произведения чисел вида (*) снова оказываются числами вида (*). Далее, свойства 1°, 2°, 4°, 5°, 6°, справедливые для любых чисел, выполняются и для чисел вида (*). Наконец,

ясно, что для произвольных чисел a и b из $Q(\alpha)$ разность $b-a$ и частное $\frac{b}{a}$ (при $a \neq 0$) принадлежат $Q(\alpha)$. Таким образом, свойства 3° и 7° также выполняются, т. е. $Q(\alpha)$ есть поле. Но все рациональные числа и число α можно представить в виде (*); например, подставляя эти числа в многочлены $r(x) = x$ и $s(x) = 1$. Поэтому $Q \subset Q(\alpha)$ и $\alpha \in Q(\alpha)$. Следовательно, $Q(\alpha)$ является α-расширением.

Пусть теперь P — любое α-расширение, и пусть $r(x)$ — какой-нибудь многочлен с рациональными коэффициентами:

$$r(x) = r_0 + r_1 x + \cdots + r_n x^n.$$

Поскольку $\alpha \in P$, $Q \subset P$ и P замкнуто относительно операций сложения и умножения, то число

$$r(\alpha) = r_0 + r_1 \alpha + \cdots + r_n \alpha^n$$

принадлежит P. Если $s(\alpha) \neq 0$, то число $\frac{1}{s(\alpha)}$ также принадлежит P. Таким образом, всякое число вида $\frac{r(\alpha)}{s(\alpha)}$ при $s(\alpha) \neq 0$ содержится в P. Следовательно, $Q(\alpha) \subset P$.

Вопросы и упражнения

1. Доказать, что множество матриц заданного порядка n, все элементы которых, расположенные ниже главной диагонали, равны нулю, является подкольцом кольца всех матриц порядка n с действительными элементами относительно операций матричного сложения и умножения.

2. Будет ли множество чисел вида $r_1 + r_2\sqrt[3]{2}$, где r_1, r_2 — рациональные числа, подполем поля действительных чисел?

3. Показать, что пересечение двух подполей поля P также является подполем этого поля.

5. Изоморфизм колец и полей. Кольца и поля являются системами с двумя операциями. На них, следовательно, распространяются понятия гомоморфного отображения и изоморфизма систем. В частности, для изоморфизма мы получаем следующее определение:

Взаимно однозначное отображение кольца (поля) K на кольцо (поле) K' называется *изоморфным* (или *изоморфизмом*), а сами кольца (поля) K и K' — *изоморфными*, если это отображение сохраняет обе операции, т. е. для любых элементов a, b из K и соответствующих им элементов a', b' из K' выполняются условия:

$$a + b \to a' + b', \quad ab \to a'b'.$$

Например, можно проверить, что кольцо, состоящее из чисел вида $r_1 + r_2\sqrt{2}$, и кольцо матриц вида

$$\begin{pmatrix} r_1 & r_2 \\ 2r_2 & r_1 \end{pmatrix}$$

(в обоих случаях r_1 и r_2— любые рациональные числа) изоморфны: чтобы построить изоморфное отображение одного кольца на другое, достаточно поставить в соответствие каждому числу $r_1 + r_2\sqrt{2}$ из первого кольца матрицу

$$\begin{pmatrix} r_1 & r_2 \\ 2r_2 & r_1 \end{pmatrix}$$

с теми же числами r_1, r_2 из второго кольца. Заметим, что поскольку первое из рассматриваемых колец есть поле, то в силу изоморфизма второе кольцо тоже является полем.

В следующем параграфе будут рассматриваться поля, на которых, помимо операций сложения и умножения, задано еще некоторое бинарное отношение. Для таких систем также можно определить понятие изоморфизма.

Поле P с бинарным отношением R считается *изоморфным* полю P' с бинарным отношением R', если существует взаимно однозначное отображение одного поля на другое, при котором для любых элементов a, b поля P и соответствующих им элементов a', b' поля P' выполняются следующие условия сохранения операций и отношения:

1°. $a + b \to a' + b'$, $ab \to a'b'$.

2°. Кортеж $\langle a, b\rangle$ принадлежит R тогда и только тогда, когда кортеж $\langle a', b'\rangle$ принадлежит R'.

Отметим, что задание бинарного отношения R на поле равносильно заданию дополнительной операции $\times$ на P, определяемой следующим образом: $a \times b$ есть 1 или 0, смотря по тому, принадлежит кортеж $\langle a, b\rangle$ отношению R или нет. Условие 2° перейдет тогда в условие сохранения этой операции.

Вопросы и упражнения

1. Сформулировать понятие гомоморфного отображения полей.

2. Доказать, что поле действительных чисел с обычными операциями сложения и умножения изоморфно полю матриц вида

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

с операциями матричного сложения и умножения.

Указание. Поставить в соответствие каждому числу a матрицу

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

§ 7. Числовые поля

1. Упорядоченные поля. На множестве R действительных чисел, кроме операций сложения и умножения, определено также некоторое бинарное отношение, называемое отношением «меньше». Принадлежность какого-либо кортежа $\langle a, b\rangle$ этому отношению принято

обозначать символом $a < b$. Сославшись на известные свойства этого отношения, мы можем теперь утверждать, что поле действительных чисел, кроме требований поля 1°—7° (см. пункт 1, § 6), удовлетворяет также следующим дополнительным требованиям:

8°. Для любых a и b имеет место одно и только одно из трех условий: $a = b$, $a < b$, $b < a$.

9°. Для любых a, b и c из $a < b$ и $b < c$ следует: $a < c$.

10°. Для любых a, b и c из $a < b$ следует: $a + c < b + c$.

11°. Для любых a, b и c из $a < b$ и $0 < c$ следует: $ac < bc$.

Свойства 8°, 9° выражают тот факт, что отношение «меньше» является отношением (простого) порядка*. Свойства 10°, 11° связывают отношение порядка с операциями сложения и умножения.

Таким образом, поле действительных чисел является упорядоченным. Нетрудно видеть, что и все подполя этого поля (например, поле рациональных чисел, поле чисел вида $r_1 + r_2\sqrt{2}$ с рациональными r_1, r_2) также будут упорядоченными. Однако далеко не всякое поле можно сделать упорядоченным — существуют поля, в которых никакое бинарное отношение не может удовлетворять всем четырем требованиям 8°—11°. Вскоре мы в этом убедимся.

Приведем некоторые свойства упорядоченных полей, являющиеся следствиями свойств 1°—11° (в ряде случаев мы опускаем доказательства, предоставляя их читателю). Принимая обычные соглашения относительно записей:

$$a > b,\ a \geqslant b,\ a \leqslant b,\ a < b < c,\ a < b \leqslant c,$$

отметим прежде всего следующие обобщения свойств 9°—11° (a, b, c, d — произвольные элементы поля):

9′. Из $a < b$ и $b \leqslant c$ следует: $a < c$.

10′. Из $a < b$ и $c \leqslant d$ следует: $a + c < b + d$.

11′. Из $0 < a < b$ и $0 < c \leqslant d$ следует: $ac < bd$.

Переходим к дальнейшим свойствам.

12°. Для единицы и нуля поля выполняется условие: $0 < 1$.

Докажем свойство 12°. Поскольку $0 \neq 1$, достаточно проверить, что не может быть $1 < 0$. Из допущения $1 < 0$ вытекало бы по свойству 10°, что $0 < -1$. Тогда по свойству 11° получилось бы, что $1(-1) < 0(-1)$, т. е. $-1 < 0$. Но условия $0 < -1$ и $-1 < 0$ не могут иметь место одновременно в силу 8°.

Из свойств 12° и 10′ вытекает следующее свойство:

13°. Для любого целого положительного m верно, что

$$m1 = \underbrace{1 + 1 + \cdots + 1}_{m \text{ раз}} > 0.$$

Свойство 13° показывает, в частности, что *характеристика всякого упорядоченного поля равна нулю.*

* См.: Алгебра, ч. 1, с. 22—24.

Из этого свойства следует также, что никакое конечное поле не может быть упорядоченным. Ведь в случае конечного поля среди элементов

$$1,\ 1+1,\ \ldots,\ 1+1+\cdots+1,\ \ldots$$

обязательно найдутся равные, а из равенства

$$\underbrace{1+1+\quad\quad+1}_{m\text{ раз}}=\underbrace{1+1+\ \ldots\ +1}_{(m+k)\text{ раз}}$$

путем m-кратного прибавления элемента -1 получится равенство

$$\underbrace{1+1+\quad\quad+1}_{k\text{ раз}}=0,$$

что противоречит свойству 13°.

14°. a) Из $a>0$ следует: $a^{-1}>0$.
b) Из $0<a<b$ следует: $0<b^{-1}<a^{-1}$.

15°. a) Если $a\neq 0$, то $a^2>0$.
b) Если либо $a\neq 0$, либо $b\neq 0$, то $a^2+b^2>0$.

16°. Из $a<b$ следует существование такого c, что $a<c<b$.

Действительно, обозначив сумму $1+1$ символом 2, имеем по свойству 13°: $2=1+1>0$; поэтому $2^{-1}>0$ (свойство 14°). Далее, $2a=a+a<a+b$ (свойство 10°). Отсюда $a=2^{-1}2a<2^{-1}\times(a+b)$ (свойство 11°). Аналогично доказывается, что $2^{-1}\times(a+b)<b$. Таким образом, для элемента $c=2^{-1}(a+b)$ имеем:

$$a<c<b.$$

Свойство 16° называют свойством *плотности* («между» любыми различными элементами поля можно «вставить» некоторый третий элемент этого поля).

Назовем теперь *модулем* (или *абсолютной величиной*) элемента a сам этот элемент, если $a>0$, и элемент $-a$ в противном случае.

Обозначая модуль a через $|a|$, отметим следующие свойства модуля.

17°. a) $|a|\geqslant 0$;
b) $|a|=|-a|$;
c) $|a+b|\leqslant|a|+|b|$;
d) $|ab|=|a|\cdot|b|$.

Вопросы и упражнения

1. Доказать свойства 9′— 11′, 14°, 15°, 17°.

2. Проверить непосредственно, что поле $\{0,1\}$ с обычной операцией умножения и операцией сложения, задаваемой равенствами $0+1=1+0=1$, $0+0=1+1=0$, не может быть упорядочено.

Указание. Показать, что в любом из случаев $0<1$, $1<0$ нарушается условие 8°.

2. Аксиоматическое определение поля действительных чисел. Как уже было сказано, наряду с полем действительных чисел упорядоченным будет и любое его подполе. Можно было бы построить и другие примеры упорядоченных полей. Чтобы выделить поле действительных чисел из класса всех упорядоченных полей, введем понятие полного упорядоченного множества.

Напомним читателю, что подмножество Q упорядоченного множества P называется *ограничением сверху*, если найдется такой элемент $p_0 \in P$, что для любого элемента $q \in Q$ выполняется условие: $q \leqslant p_0$. Элемент p_0 называется при этом *верхней границей* подмножества Q.

Упорядоченное множество P называется *полным*, если всякое ограниченное сверху подмножество Q множества P имеет *наименьшую* верхнюю границу.

Как известно из курса математического анализа, множество действительных чисел полно, а множество рациональных чисел неполно.

Полное упорядоченное поле обладает рядом важных свойств. Например, можно показать, что в таком поле разрешимо любое двучленное уравнение $x^m - a = 0$, где a — любой больший нуля элемент поля. Это справедливо не для всякого упорядоченного поля (так, уравнение $x^2 - 2 = 0$ не имеет решений в поле рациональных чисел).

Рассмотрим здесь еще одно интересное свойство полного поля, также не вытекающее из требований 1°— 11°.

Для любого $a > 0$ из полного поля P и любого другого элемента b этого поля можно указать такое натуральное n, что $na > b$ (аксиома Архимеда).

Доказательство этого свойства будем вести от противного. Предположив, что для всякого натурального m верно $ma \leqslant b$, получаем, что множество $\{ma\}$ ограничено сверху. Поэтому оно имеет наименьшую верхнюю границу c. Тогда элемент $c - a$ (который меньше c) уже не будет верхней границей этого множества, т. е. некоторый элемент ka будет больше $c - a$. Отсюда получается: $(k+1)a = ka + a > (c - a) + a = c$, что невозможно, так как c — верхняя граница множества $\{ma\}$.

Докажем, пользуясь аксиомой Архимеда, что в полном упорядоченном поле разрешимо уравнение $x^2 - a = 0$ при $a > 0$.

Рассмотрим множество A всех чисел, квадрат которых не превосходит числа a, т. е. положим:

$$A = \{x : x^2 \leqslant a\}.$$

Множество A непусто, так как, например, $0 \in A$. Кроме того, число $a + 1$ является верхней границей этого множества: если $x \in A$, то $x \leqslant a + 1$, иначе мы имели бы:

$$x^2 > (a+1)^2 = a^2 + 2a + 1 > a.$$

Следовательно, по условию полноты поля действительных чисел множество A имеет наименьшую верхнюю границу a_0, причем $a_0 \geqslant 0$ (поскольку $0 \in A$).

Покажем, что $a_0^2 - a = 0$.

Допустим $a_0^2 - a > 0$. Тогда по аксиоме Архимеда можно найти такое целое $n > 0$, что

$$n(a_0^2 - a) > 2a_0, \text{ или } a_0^2 - 2\frac{a_0}{n} > a.$$

Отсюда и из условий $a_0 \geqslant 0$, $a > 0$ следует неравенство $a_0 - \frac{1}{n} > 0$. Убедимся, что для любого $x \in A$ имеет место $x \leqslant a_0 - \frac{1}{n}$. В противном случае было бы

$$x^2 > \left(a_0 - \frac{1}{n}\right)^2 = a_0^2 - 2\frac{a_0}{n} + \frac{1}{n^2} > a.$$

Следовательно, число $a_0 - \frac{1}{n}$, меньшее a_0, является верхней границей для A, что противоречит выбору числа a_0 как наименьшей верхней границы.

Пусть теперь $a_0^2 - a < 0$. Тогда по аксиоме Архимеда можно найти такое целое $n > 0$, что

$$n(a - a_0^2) > 2a_0 + 1, \text{ или } a_0^2 + 2\frac{a_0}{n} + \frac{1}{n} < a.$$

Заменяя в последнем неравенстве число $\frac{1}{n}$ числом $\frac{1}{n^2}\left(\frac{1}{n^2} \leqslant \frac{1}{n}\right)$, получаем;

$$\left(a_0 + \frac{1}{n}\right)^2 < a.$$

Значит, число $a_0 + \frac{1}{n}$, большее a_0, является элементом A, что противоречит выбору числа a_0 как верхней границы A.

Итак, случаи $a_0^2 - a > 0$ и $a_0^2 - a < 0$ невозможны. Следовательно, $a_0^2 - a = 0$.

Весьма важный факт, связанный с полными упорядоченными полями, состоит в том, что все такие поля *совпадают* с точностью до изоморфизма. Иными словами, справедлива следующая теорема:

Любые два полных упорядоченных поля изоморфны. (Здесь изоморфизм понимается именно как изоморфизм упорядоченных полей, т. е. как взаимно однозначное отображение, сохраняющее не только операции сложения и умножения, но и бинарное отношение «меньше» (см. пункт 5, § 6).

В силу этой теоремы поле действительных чисел можно определить как *любое полное упорядоченное поле.*

В курсе математического анализа поле действительных чисел вводится путем индивидуального конструирования составляющих его элементов (и последующего определения необходимых операций и отношения).

Определяя же поле действительных чисел как полное упорядоченное поле, мы не интересуемся природой его элементов, способом задания операций и отношения порядка, а требуем только, чтобы для них выполнялись определенные требования (аксиомы). Такой аксиоматический подход находит широкие применения в различных математических теориях.

Мы не приводим здесь доказательства теоремы об изоморфизме полных упорядоченных полей, так как оно выходит за рамки этой книги.

Вопросы и упражнения

1. Доказать, что любое ограниченное снизу подмножество полного упорядоченного поля имеет наибольшую нижнюю границу.

2. Доказать, что если M_1 и M_2 — два подмножества полного упорядоченного поля и любой элемент из M_1 меньше любого элемента из M_2, то существует «разделяющий» элемент поля, который будет верхней границей для M_1 и нижней границей для M_2.

Указание. Воспользоваться ограниченностью множества M_1 и показать, что его точная верхняя граница является нижней границей для множества M_2.

3. Построение поля комплексных чисел. Как известно, уравнение $x^2 + a = 0$ не имеет решений в поле **R** действительных чисел при $a > 0$. В частности, неразрешимо уравнение $x^2 + 1 = 0$. Возникает естественный вопрос: нельзя ли построить такое расширение поля **R**, в котором содержится (хотя бы один) элемент, удовлетворяющий уравнению $x^2 + 1 = 0$. Для решения этого вопроса введем следующее определение.

Будем называть *полем комплексных чисел* любое поле **C**, для которого выполняются три условия:

a) поле **C** является расширением некоторого поля $\mathbf{R}_0$ действительных чисел;

b) некоторый элемент поля **C** удовлетворяет уравнению $x^2 + 1 = 0$, где 1 и 0 означают нейтральные элементы поля относительно умножения и сложения;

c) всякое подполе поля **C**, удовлетворяющее условиям a) и b), совпадает с полем **C**.

Элементы поля комплексных чисел будем называть *комплексными числами*.

Условия a) и b) этого определения диктуются самой постановкой задачи, что же касается условия c), то оно выделяет среди искомых расширений минимальное и, как мы увидим, в известном смысле *единственное* расширение.

Мы построим сейчас некоторое конкретное поле комплексных чисел и тем самым убедимся, что такие поля существуют.

Будем исходить из какого-нибудь поля **R** действительных чисел. В качестве множества **C** возьмем множество $\mathbf{R}^2$ всевозможных кортежей или упорядоченных пар (a, b), где $a, b \in \mathbf{R}$. Напомним, что две пары (a_1, b_1) и (a_2, b_2) считаются равными тогда и только тогда, когда $a_1 = a_2$ и $b_1 = b_2$. Определим на множестве **C** операции сложения и умножения следующим образом:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + b_1a_2).$$

Оказывается, что для этих операций выполнены все требования 1°—7° пункта 1 § 6, предъявляемые к полю. Требования 1°—3° (ассоциативность, коммутативность и обратимость сложения) проверяются непосредственно — сложение пар заключается в сложении по отдельности их первых и вторых элементов, т. е. сводится

к сложению действительных чисел, которое удовлетворяет требованиям 1°—3°. В частности, если 0 обозначает нейтральный элемент множества **R** относительно сложения чисел, то пара (0,0) будет нейтральным элементом множества **C** относительно операции сложения пар.

Проверка требований 4°—6° предоставляется читателю.

Проверим теперь требование 7° (требование ограниченной обратимости умножения). Нужно показать, что если $(a, b) \neq (0,0)$, то существует единственная пара (x, y), удовлетворяющая уравнению

$$(a, b)(x, y) = (c, d).$$

Пользуясь определением операции умножения пар, преобразуем это уравнение к виду:

$$(ax - by, ay + bx) = (c, d).$$

Последнее уравнение по определению равенства пар равносильно следующей системе двух линейных уравнений с двумя неизвестными:

$$\begin{cases} ax - by = c, \\ bx + ay = d. \end{cases}$$

Определителем этой системы является число $a^2 + b^2$. Если бы было $a^2 + b^2 = 0$, то мы имели бы: $a = 0$, $b = 0$, но по предположению $(a, b) \neq (0,0)$. Следовательно, определитель системы отличен от нуля, и система имеет *единственное* решение, легко вычисляемое по правилу Крамера:

$$x = \frac{ac + bd}{a^2 + b^2}, \quad y = \frac{ad - bc}{a^2 + b^2}.$$

Требование 7° проверено.

Заметим, что нейтральным элементом относительно умножения пар будет пара (1,0):

$$(a, b) \cdot (1, 0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a, b).$$

Итак, множество **C** с указанными операциями сложения и умножения является полем.

Теперь может быть доказана следующая основная теорема.

Теорема. *Поле* ***C*** *является полем комплексных чисел.*

Доказательство. 1. Докажем сначала, что выполнено условие а) определения поля комплексных чисел. Для этого рассмотрим подмножество $\mathbf{R}_0$ поля **C**, состоящее из пар вида $(a, 0)$. Проверим, что подмножество $\mathbf{R}_0$ с операциями сложения и умножения пар изоморфно исходному полю **R** действительных чисел. В самом деле, если поставить в соответствие каждому элементу a из **R** элемент $(a, 0)$ из $\mathbf{R}_0$:

$$a \to (a, 0),$$

то получится, очевидно, взаимно однозначное отображение **R** на $\mathbf{R}_0$.

Покажем, что это отображение сохраняет операцию умножения, т. е. что если

$$a_1 \to (a_1,\ 0),\ a_2 \to (a_2,\ 0),$$

то

$$a_1 a_2 \to (a_1,\ 0)\,(a_2,\ 0).$$

Действительно, по определению отображения произведению a_1a_2 ставится в соответствие пара $(a_1a_2,0)$, но эта пара совпадает с произведением $(a_1,\ 0)(a_2,\ 0)$ по определению умножения пар. Аналогично устанавливается, что построенное отображение сохраняет операцию сложения.

Таким образом, множество $\mathbf{R}_0$ с операциями сложения и умножения пар изоморфно полю $\mathbf{R}$ действительных чисел, и, следовательно, само является полем действительных чисел*. Значит, поле $\mathbf{C}$ можно считать расширением поля $\mathbf{R}_0$ действительных чисел.

2. Переходим к проверке условия b) определения. Учитывая, что нейтральными элементами поля $\mathbf{C}$ относительно сложения и умножения являются соответственно пары (0,0) и (1, 0), мы должны показать, что в поле $\mathbf{C}$ уравнение

$$(x,\ y)^2 + (1,\ 0) = (0,\ 0)$$

имеет решение. Пользуясь определением операций над парами, преобразуем это уравнение к виду:

$$(xx - yy + 1,\ xy + yx + 0) = (0,\ 0).$$

По определению равенства пар последнее уравнение равносильно следующей системе двух уравнений:

$$\begin{cases} x^2 - y^2 + 1 = 0, \\ 2xy = 0. \end{cases}$$

Эта система, как показывают простые выкладки, имеет ровно два решения: (0,1) и (0,—1). Тем самым условие b) проверено.

3. Проверим, наконец, условие c). Пусть подполе $\mathbf{C}_1$ поля $\mathbf{C}$ содержит поле $\mathbf{R}_0$ и какое-нибудь из решений уравнения $(x,\ y)^2 + (1,\ 0) = (0,\ 0)$. Положим для определенности, что $\mathbf{C}_1$ содержит пару (0, 1). Покажем, что $\mathbf{C}_1$ содержит любой элемент $(a,\ b)$ из $\mathbf{C}$. В самом деле, наряду с парой (0, 1) подполе $\mathbf{C}_1$ содержит пары $(a,\ 0)$ и $(b,\ 0)$, поскольку они входят в поле $\mathbf{R}_0$. Поле $\mathbf{C}_1$ замкнуто относительно операций сложения и умножения, и поэтому элемент $(a,\ 0) + (b,\ 0)\,(0,\ 1)$ принадлежит $\mathbf{C}_1$. Но

$$(a,\ 0) + (b,\ 0)\,(0,\ 1) = (a,\ 0) + (b \cdot 0 - 0 \cdot 1,\ b \cdot 1 + 0 \cdot 0) = (a,\ b).$$

---

* Предполагается, что отношение порядка определено в R_0 следующим образом: $(a_1,\ 0) < (a_2,\ 0)$ тогда и только тогда, когда $a_1 < a_2$.

Значит, $(a, b) \in \mathbf{C}_1$, т. е. подполе $\mathbf{C}_1$ поля $\mathbf{C}$ содержит каждый элемент из C, и мы получаем, что $\mathbf{C}_1 = \mathbf{C}$. Случай, когда $\mathbf{C}_1$ содержит пару $(0, -1)$, рассматривается аналогично.

Теорема доказана.

Вопросы и упражнения

1. Проверить, что для операций над парами выполняются требования 4°—6° из определения поля.

2. Показать, что отображение, построенное в первой части доказательства теоремы, сохраняет операцию сложения.

3. Как изменится третья часть доказательства теоремы, если предположить, что $\mathbf{C}_1$ содержит пару $(0, -1)$?

4. **Единственность поля комплексных чисел. Числовые поля.** Ранее уже говорилось, что любые две изоморфные системы считаются в алгебре одинаковыми. Поэтому вопрос о том, существуют ли различные поля комплексных чисел, следует ставить так: существуют ли два неизоморфных поля комплексных чисел? Отрицательный ответ на этот вопрос дает следующая теорема.

Теорема единственности. *Любые два поля комплексных чисел изоморфны.*

Доказательство. 1. Пусть некоторое поле $\mathbf{C}$ комплексных чисел содержит поле $\mathbf{R}_0$ действительных чисел и решение i уравнения $x^2 + 1 = 0$. Для элемента i имеем, следовательно: $i^2 + 1 = 0$, $i^2 = -1$. Всякий элемент вида $a + bi$, где a и b принадлежат $\mathbf{R}_0$, содержится в поле $\mathbf{C}$ в силу замкнутости $\mathbf{C}$ относительно операций сложения и умножения. Оказывается, множество всех таких элементов является *подполем* поля $\mathbf{C}$. Для доказательства нужно проверить, что это множество замкнуто относительно операций, а также требования 3° и 7° из определения поля — остальные требования, входящие в определение поля,— выполняются для любого подмножества поля $\mathbf{C}$. Замкнутость относительно операций вытекает из равенств:

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2) i,$$
$$(a_1 + b_1 i)(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2) i.$$

Решением уравнения $(a + bi) + x = c + di$ является элемент $(c - a) + (d - b)i$ из данного множества Поэтому остается проверить только свойство 7°, т. е. показать, что уравнению $(a + bi)x = c + di$ при $a + bi \neq 0$ удовлетворяет некоторый элемент вида $u + vi$, где $u, v \in \mathbf{R}_0$. Таким образом, необходимо найти такие u и v, чтобы выполнялось равенство

$$(a + bi)(u + vi) = c + di$$

или

$$(au - bv) + (bu + av) i = c + di.$$

Для этого u и v должны удовлетворять следующей системе линейных уравнений:

$$\begin{cases} au - bv = c, \\ bu + av = d. \end{cases}$$

Определитель этой системы $a^2 + b^2 \neq 0$ (иначе по свойству 15° было бы $a = b = 0$ и, значит, $a + bi = 0$). Вычисляя по правилу Крамера u и v, получаем, что в качестве искомого решения можно взять элемент

$$x = \frac{ac + bd}{a^2 + b^2} + \frac{ad - bc}{a^2 + b^2} i.$$

Итак, множество всех элементов вида $a + bi$ есть поле. Оно содержится в поле **C**, содержит все элементы $a + 0 \quad i$, т. е. поле $\mathbf{R}_0$, и элемент $0 + 1 \quad i = i$, т. е. решение уравнения $x^2 + 1 = 0$. По условию с) определения поля комплексных чисел построенное поле совпадает с полем **C**. Следовательно, любой элемент из **C** может быть представлен в виде $a + bi$, где a и b — подходящие элементы из $\mathbf{R}_0$. Такое представление единственно: допустив, что $a + bi = c + di$ и $b \neq d$, мы получим, что

$$i = \frac{c - a}{b - d},$$

а это означало бы, что в $\mathbf{R}_0$ содержится решение уравнения $x^2 + 1 = 0$. Значит, $b = d$. Но тогда и $a = c$.

2. Пусть теперь **C** и **C′** — два поля комплексных чисел, поля $\mathbf{R}_0$ и $\mathbf{R}_0'$ — содержащиеся в них поля действительных чисел, элемент i поля **C** является решением уравнения $x^2 + 1 = 0$, а элемент i' поля **C′** — решением уравнения $x^2 + 1' = 0'$. Поля $\mathbf{R}_0$ и $\mathbf{R}_0'$ изоморфны как два поля действительных чисел. Следовательно, существует изоморфное отображение поля $\mathbf{R}_0$ на поле $\mathbf{R}_0'$. Поставим в соответствие каждому элементу $a + bi$ из **C** элемент $a' + b'i'$ из **C′**, где a' и b' являются элементами поля $\mathbf{R}_0'$, соответствующими элементам a и b поля $\mathbf{R}_0$ при изоморфном отображении $\mathbf{R}_0$ на $\mathbf{R}_0'$. Мы получим, как это вытекает из части 1 доказательства, взаимно однозначное отображение **C** на **C′**.

Убедимся, что это отображение сохраняет операции. Пусть элементы $a_1 + b_1 i$ и $a_2 + b_2 i$ поля **C** отображаются соответственно в элементы $a_1' + b_1' i'$ и $a_2' + b_2' i'$ поля **C′**. Нужно доказать, что выполняется условие:

$$(a_1 + b_1 i)(a_2 + b_2 i) \to (a_1' + b_1' i')(a_2' + b_2' i'),$$

которое, очевидно, равносильно условию:

$$(a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2) i \to (a_1' a_2' - b_1' b_2') + (a_1' b_2' + b_1' a_2') i'.$$

Поэтому достаточно проверить, что при отображении $\mathbf{R}_0$ на $\mathbf{R}_0'$ имеет место:

$$(a_1a_2 - b_1b_2) \to (a_1'a_2' - b_1'b_2'),\ (a_1b_2 + b_1a_2) \to (a_1'b_2' + b_1'a_2').$$

Но это следует из того, что при отображении $\mathbf{R}_0$ на $\mathbf{R}_0'$ элементы a_1, a_2, b_1, b_2 переходят в элементы a_1', a_2', b_1', b_2' и что это отображение, будучи изоморфизмом, сохраняет операции.

Аналогично проверяется условие:

$$(a_1 + b_1i) + (a_2 + b_2i) \to (a_1' + b_1'i') + (a_2' + b_2'i').$$

Тем самым устанавливается, что отображение поля $\mathbf{C}$ на поле $\mathbf{C}'$ изоморфно. Теорема доказана.

Замечание. По ходу доказательства теоремы установлен важный факт: всякое комплексное число представимо в виде $a + bi$, где a и b — действительные числа, а $i^2 = -1$. Такая форма комплексных чисел весьма удобна и имеет широкое применение.

Теорема единственности позволяет говорить об *одном* поле комплексных чисел, так же как теорема об изоморфизме любых полных упорядоченных полей — об одном поле действительных чисел. Поле $\mathbf{C}$ комплексных чисел, следовательно, можно себе представлять как некоторое конкретное расширение какого-либо конкретного полного упорядоченного поля $\mathbf{R}_0$ (например, поля тех объектов, которые определяются как действительные числа в курсе математического анализа).

Теперь, располагая понятием поля комплексных чисел, можно определить во всей общности понятие числового поля: *числовым полем* будем называть всякое подполе поля комплексных чисел. К числовым полям, естественно, относятся все подполя поля действительных чисел, примеры которых рассматривались ранее. Однако числовые поля не обязательно должны содержаться в поле действительных чисел или содержать это поле. Например, множество чисел вида $r_1 + r_2i$, где r_1, r_2 — любые рациональные числа, а i — решение уравнения $x^2 + 1 = 0$, образует числовое поле, в которое входят не все действительные числа и которое содержит элемент i, не являющийся действительным числом.

Не вдаваясь в подробное изучение числовых полей, отметим только следующий простой факт:

Любое числовое поле содержит поле рациональных чисел.

В самом деле, всякое числовое поле P содержит числа 0 и 1 (как нейтральные элементы поля), а, значит, и число -1 (как элемент, противоположный числу 1). В силу замкнутости поля P относительно сложения в нем будут содержаться и все числа вида $1 + 1 + \ldots + 1$, $(-1) + (-1) + \ldots + (-1)$. Таким образом, в P содержатся все целые числа. Если p и q — любые целые числа и $q \neq 0$, то поле P содержит и число $\frac{p}{q}$ (как решение уравнения $qx = p$). Значит, поле P содержит *все* рациональные числа, т. е. является расширением поля рациональных чисел.

Доказанное утверждение означает, что поле рациональных чисел является *наименьшим* из числовых полей.

В заключение рассмотрим следующий вопрос. По определению поля комплексных чисел в этом поле разрешимо уравнение $x^2+1=0$. Отсюда легко вывести, что в нем разрешимо вообще любое квадратное уравнение $x^2+a_1x+a_0=0$ с комплексными (в частности, с действительными) коэффициентами. Однако справедлива, оказывается, гораздо более общая теорема:

Любое алгебраическое уравнение

$$x^n+a_{n-1}x^{n-1}+\cdots+a_0=0,$$

в котором $a_{n-1}, \ldots, a_0$ *принадлежит полю комплексных чисел, разрешимо в этом поле.*

Эту теорему называют *основной теоремой алгебры*. Ее доказательство, существенно опирающееся на соображения непрерывности, излагается в курсе математического анализа.

Вопросы и упражнения

1. Проверить подробно, что соответствие, построенное во второй части доказательства теоремы единственности, является взаимно однозначным отображением поля $\mathbf{C}$ на поле $\mathbf{C}'$.

2. Доказать, что для любых элементов a_1, a_0 поля комплексных чисел уравнение

$$x^2+a_1x+a_0=0$$

разрешимо в этом поле.

3. Показать, что поле комплексных чисел не может быть сделано упорядоченным.

Указание. Воспользоваться свойством 15° упорядоченных полей.

Глава II

ВЕКТОРНЫЕ ПРОСТРАНСТВА

Читатель уже знаком с понятием n-мерного арифметического пространства. Напомним,что это пространство представляет собой множество n-мерных арифметических векторов, т. е. строк из действительных чисел

$$(a_1, a_2,\ldots,a_n),$$

в котором определены две операции: операция сложения векторов и операция умножения вектора на действительное число. Внимательный анализ показывает, что свойства этих операций как раз и лежат в основе всей дальнейшей теории, а конкретная форма задания векторов в виде наборов действительных чисел не играет особой роли.

Если, например, в определении вектора и операций над векторами заменить действительные числа элементами произвольного поля, то мы получим дословное повторение теории арифметических пространств: свойства операций над арифметическими векторами определяются свойствами сложения и умножения в поле действительных чисел, а эти последние сохраняются в случае произвольного поля.

На самом деле можно пойти еще дальше и называть векторами любые объекты, для которых определены две операции: сложения и умножения на элементы какого-нибудь заданного поля P— с условием, что эти операции подчиняются некоторым требованиям естественного характера. Преимущества такого подхода очевидны, ибо он освобождает нас от необходимости видеть за «вектором» обязательно набор действительных чисел или каких-либо элементов и позволяет (как будет показано дальше) охватить единым понятием «вектор» объекты самой различной природы (функции, матрицы и т. п.)

§ 1. Векторное пространство над полем

1. Определение векторного пространства. Пусть P — некоторое поле. В дальнейшем для удобства формулировок элементы поля P будут называться «числами», хотя на самом деле это могут быть какие угодно объекты. Впрочем, если иметь в виду частный случай,

когда P есть числовое поле, название «числа» приобретает уже прямой смысл.

Определение. Множество L называется *векторным пространством над полем* P, если:

I) на L определена операция, называемая *сложением*: каждым двум элементам $\boldsymbol{a}$ и $\boldsymbol{b}$ из L сопоставлен некоторый третий элемент из L, обозначаемый $\boldsymbol{a}+\boldsymbol{b}$ (и называемый *суммой* элементов $\boldsymbol{a}$ и $\boldsymbol{b}$);

II) определена операция, называемая *умножением* элементов из L на числа из P: каждому элементу $\boldsymbol{a}\in L$ и каждому числу $k\in P$ сопоставлен некоторый элемент из L, обозначаемый $k\boldsymbol{a}$ (и называемый *произведением* элемента $\boldsymbol{a}$ на число k);

III) эти операции удовлетворяют следующим условиям:

1. Множество L является коммутативной группой относительно операции сложения, т. е.

1a) $\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{b}+\boldsymbol{a}$ для любых $\boldsymbol{a}$, $\boldsymbol{b}\in L$;

1b) $(\boldsymbol{a}+\boldsymbol{b})+\boldsymbol{c}=\boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{c})$ для любых $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}\in L$,

1c) в L существует такой элемент $\mathbf{0}$ (*нуль группы*), что $\boldsymbol{a}+\mathbf{0}=\boldsymbol{a}$ для любого $\boldsymbol{a}\in L$;

1d) для любого $\boldsymbol{a}\in L$ в L существует такой элемент $-\boldsymbol{a}$ (*противоположный* к $\boldsymbol{a}$ *элемент*), что $\boldsymbol{a}+(-\boldsymbol{a})=\mathbf{0}$;

2. $1\boldsymbol{a}=\boldsymbol{a}$ для любого $\boldsymbol{a}\in L$ и единицы 1 поля P;

3. $k_1(k_2\boldsymbol{a})=(k_1k_2)\boldsymbol{a}$ для любых k_2, $k_2\in P$, $\boldsymbol{a}\in L$;

4. $(k_1+k_2)\boldsymbol{a}=k_1\boldsymbol{a}+k_2\boldsymbol{a}$ для любых k_1, $k_2\in P$, $\boldsymbol{a}\in L$;

5. $k(\boldsymbol{a}+\boldsymbol{b})=k\boldsymbol{a}+k\boldsymbol{b}$ для любых $k\in P$ $\boldsymbol{a}$, $\boldsymbol{b}\in L$.

Элементы векторного пространства называются *векторами*. При этом вектор $\mathbf{0}$ называют *нулевым вектором*, а вектор $-\boldsymbol{a}$ — *противоположным вектором* (к вектору $\boldsymbol{a}$). Наравне с термином *векторное пространство* часто используется также термин *линейное пространство*.

Называя в данном определении умножение вектора на число «операцией», мы отступаем от терминологии, принятой в § 1 главы I. Действительно, термин «операция» в прежнем смысле предполагает, что каждым двум элементам *одного и того же* множества сопоставлен некоторый третий элемент. В данном же случае вектор $k\boldsymbol{a}$ сопоставляется элементам k и $\boldsymbol{a}$, взятым из *разных* множеств ($k\in P$, $\boldsymbol{a}\in L$). Тем не менее, в целях краткости, предпочтительнее отображение $P\times L$ в L также называть «операцией».

Если строго придерживаться прежней терминологии, то следовало бы говорить так: каждому $k\in P$ ставится в соответствие одноместная операция на L, которая любой элемент $\boldsymbol{a}$ из L отображает на некоторый другой элемент из L, обозначаемый символом $k\boldsymbol{a}$. При таком подходе векторное пространство оказывается системой с одной двухместной операцией и некоторым множеством одноместных операций.

Заметим, что в определении векторного пространства участвуют две различные, но одинаково обозначенные операции сложения (сложение в L и сложение в P) и умножения (умножение элементов из L на числа из P и умножение в P). Одинаковое обозначение

различных по своей природе операций обычно не приводит к путанице, поскольку из самой записи всегда бывает видно, какие операции имеются в виду. Например, в равенстве

$$(k_1 + k_2)\,\boldsymbol{a} = k_1\boldsymbol{a} + k_2\boldsymbol{a}$$

знак «+» в левой части означает сложение в P, так как k_1, $k_2 \in P$, а знак «+» в правой части означает сложение в L, так как $k_1\boldsymbol{a}$, $k_2\boldsymbol{a} \in L$.

2. Примеры векторных пространств.

1. *Арифметическое n-мерное пространство* $\mathbf{R}^n$. Это пространство изучалось подробно в первой части курса. Его элементы (векторы) представляют собой упорядоченные наборы из n действительных чисел

$$(a_1,\ a_2,\ \ldots,\ a_n) \tag{1}$$

со следующими правилами сложения таких наборов и умножения их на действительные числа:

$$(a_1,\ a_2,\ \ldots,\ a_n) + (b_1,\ b_2,\ \ldots,\ b_n) = \\ = (a_1 + a_2,\ b_1 + b_2,\ \ldots,\ a_n + b_n), \tag{2}$$

$$k\,(a_1,\ a_2,\ \ldots,\ a_n) = (ka_1,\ ka_2,\ \ldots,\ ka_n). \tag{3}$$

Согласуясь с принятым выше общим определением векторного пространства, мы можем теперь сказать, что $\mathbf{R}^n$ есть векторное пространство над полем $\mathbf{R}$ действительных чисел.

2. *Пространство P^n.* Это пространство определяется аналогично $\mathbf{R}^n$, с той лишь разницей, что действительные числа заменяются «числами» из данного поля P. Элементы пространства P^n суть строки (1), где a_1, a_2, ..., a_n — произвольные числа из P. Сложение строк и умножение их на числа из P производятся по формулам (2) и (3). Все требования, входящие в определение векторного пространства над P, очевидным образом выполняются. Следовательно, P^n есть векторное пространство над полем P.

Отметим, что особую важность представляют два частных случая: 1) когда P есть поле действительных чисел; 2) когда P есть поле комплексных чисел.

3. Пусть снова P — некоторое поле. Рассмотрим всевозможные отображения из P в P. Каждое такое отображение можно истолковывать как функцию

$$y = f(x), \tag{4}$$

определенную на множестве P и принимающую значения снова из P.

Для функций (4), естественно, вводится операция сложения. Сложить функции $f_1(x)$ и $f_2(x)$ означает построить новую функцию

$f_1(x) + f_2(x)$, значение которой при любом $x = a$ из P равно $f_1(a) + f_2(a)$. Столь же естественно определяется умножение функции $f(x)$ на число $k \in P$: полученная при этом функция $kf(x)$ при любом $x = a \in P$ принимает значение, равное $kf(a)$.

Множество всех функций (4) с указанными выше операциями сложения функций и умножения их на числа из P есть векторное пространство над P. Проверку этого факта (т. е. проверку того, что выполнены все требования 1—5, входящие в определение векторного пространства) предоставляем читателю.

4. Рассмотрим всевозможные матрицы данного типа (т. е. с данным количеством строк и столбцов):

$$\begin{pmatrix} a_{11}a_{12} & \dots & a_{1n} \\ a_{21}a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots \\ a_{m1}a_{m2} & \dots & a_{mn} \end{pmatrix}, \tag{5}$$

с элементами a_{ij} из фиксированного поля P.

Операции сложения матриц и умножения их на числа из P определим следующим образом:

$$\begin{pmatrix} a_{11}a_{12} & \dots & a_{1n} \\ a_{21}a_{22} & \dots & a_{2n} \\ & & \\ a_{m1}a_{m2} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11}b_{12} & \dots & b_{1n} \\ b_{21}b_{22} & \dots & b_{2n} \\ & & \\ b_{m1}b_{m2} & \dots & a_{mn} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11} + b_{11}a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21}a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \dots & \dots & \\ a_{m1} + b_{m1}\,a_{m2} + b_{m2} \dots & & a_{mn} + b_{mn} \end{pmatrix},$$

$$k\begin{pmatrix} a_{11}a_{12} & \dots & a_{1n} \\ a_{21}a_{22} & \dots & a_{2n} \\ \dots & & \\ a_{m1}a_{m2} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} ka_{11}ka_{12} & \dots & ka_{1n} \\ ka_{21}ka_{22} & \dots & ka_{2n} \\ \dots & & \\ ka_{m1}ka_{m2} & \dots & ka_{mn} \end{pmatrix}.$$

Легко проверяется, что все требования, входящие в определение векторного пространства, будут при этом выполнены. Мы получаем, следовательно, некоторое векторное пространство над P.

Замечание. Этот пример имеет непосредственное отношение к предыдущему примеру 3. В дальнейшем мы увидим, что каждая матрица (5) определяет некоторое отображение пространства P^n в пространство P^m. Поэтому векторное пространство последнего примера можно истолковывать как некоторое множество функций

$$y = f(x) \quad (x \in P^n,\ y \in P^m).$$

При этом оказывается, что определенным выше операциям над матрицами соответствуют сложение функций и умножение их на

числа из P, понимаемые в естественном смысле (т. е. так, как объяснено в примере 3).

3. Простейшие следствия из определения векторного пространства. Из свойств группы 1b)—1d) вытекает, как известно, *единственность* нулевого вектора. Далее, в силу тех же свойств для каждого вектора из L существует *единственный* противоположный вектор.

Покажем теперь, что число $0 \in P$ и вектор $\mathbf{0} \in L$ играют особую роль по отношению к операции умножения вектора на число, а именно:

1) $0\boldsymbol{a} = \mathbf{0}$ для любого $\boldsymbol{a} \in L$;
2) $k\mathbf{0} = \mathbf{0}$ для любого $k \in P$;
3) если $k\boldsymbol{a} = \mathbf{0}$, то или $k = 0$, или $\boldsymbol{a} = \mathbf{0}$.

Чтобы доказать 1), возьмем какое-либо число $k \in P$ и запишем, пользуясь свойством 4 определения векторного пространства, следующие равенства:

$$k\boldsymbol{a} = (k + 0)\,\boldsymbol{a} = k\boldsymbol{a} + 0\boldsymbol{a}.$$

Отсюда в силу единственности нулевого вектора, $0\boldsymbol{a} = \mathbf{0}$.

Чтобы доказать 2), возьмем какой-либо вектор $\boldsymbol{a} \in L$ и запишем на основании свойства 5 того же определения:

$$k\boldsymbol{a} = k\,(\boldsymbol{a} + \mathbf{0}) = k\boldsymbol{a} + k\mathbf{0}.$$

Отсюда, как и в предыдущем случае, $k\mathbf{0} = \mathbf{0}$.

Наконец, чтобы доказать 3), допустим, что имеет место равенство

$$k\boldsymbol{a} = \mathbf{0},$$

но при этом $k \neq 0$. Тогда, умножив обе части написанного равенства на число k^{-1}, получим:

$$k^{-1}\,(k\boldsymbol{a}) = k^{-1} \cdot \mathbf{0} = \mathbf{0}.$$

С другой стороны, в силу условий 3 и 2 определения векторного пространства

$$k^{-1}\,(k\boldsymbol{a}) = (k^{-1}k)\,\boldsymbol{a} = 1\boldsymbol{a} = \boldsymbol{a}.$$

Следовательно, $\boldsymbol{a} = \mathbf{0}$.

Установим еще несколько свойств операций над векторами:

4) $(-k)\,\boldsymbol{a} = -k\boldsymbol{a}$;
5) $k\,(-\boldsymbol{a}) = -k\boldsymbol{a}$;
6) $(k - l)\,\boldsymbol{a} = k\boldsymbol{a} - l\boldsymbol{a}$;
7) $k\,(\boldsymbol{a} - \boldsymbol{b}) = k\boldsymbol{a} - k\boldsymbol{b}$.

Свойство 4) следует из равенств:

$$k\boldsymbol{a} + (-k)\,\boldsymbol{a} = [k + (-k)]\,\boldsymbol{a} = 0\boldsymbol{a} = \mathbf{0},$$

которые показывают, что вектор $(-k)\,\boldsymbol{a}$ противоположен вектору $k\boldsymbol{a}$.

Свойство 5) доказывается аналогично:

$$k\boldsymbol{a} + k(-\boldsymbol{a}) = k[\boldsymbol{a} + (-\boldsymbol{a})] = k\boldsymbol{0} = \boldsymbol{0}.$$

Свойство 6) следует из равенств:

$$(k - l)\,\boldsymbol{a} = [k + (-l)]\,\boldsymbol{a} = k\boldsymbol{a} + (-l)\,\boldsymbol{a} = k\boldsymbol{a} - l\boldsymbol{a}.$$

Наконец, свойство 7) получается так:

$$k(\boldsymbol{a} - \boldsymbol{b}) = k[\boldsymbol{a} + (-\boldsymbol{b})] = k\boldsymbol{a} + k(-\boldsymbol{b}) = k\boldsymbol{a} - k\boldsymbol{b}.$$

4. Линейная зависимость. Для векторного пространства L над полем P вводятся те же понятия, что и для арифметических пространств. Напомним некоторые из них.

Линейной комбинацией нескольких векторов

$$\boldsymbol{a}_1,\ \boldsymbol{a}_2\ \ldots\ ,\ \boldsymbol{a}_p \tag{6}$$

из L называется любой вектор вида

$$\boldsymbol{a} = k_1\boldsymbol{a}_1 + k_2\boldsymbol{a}_2 + \cdots + k_p\boldsymbol{a}_p, \tag{7}$$

где $k_1\ k_2,\ldots,k_p$— какие-нибудь числа из поля P. При наличии равенства (7) мы говорим также, что вектор $\boldsymbol{a}$ линейно выражается через векторы (6) или что вектор $\boldsymbol{a}$ разлагается по векторам (6).

Наиболее важным является определение *линейной зависимости и независимости* системы векторов.

Система (6) называется *линейно зависимой*, если существуют такие числа $k_1,\ k_2,\ldots,\ k_p$, не равные одновременно нулю, что

$$k_1\boldsymbol{a}_1 + k_2\boldsymbol{a}_2 + \cdots + k_p\boldsymbol{a}_p = \boldsymbol{0}. \tag{8}$$

В противном случае, т. е. если равенство (8) возможно *только* в случае равенства нулю всех коэффициентов $k_1, k_2,\ldots,k_p$, система (6) называется *линейно независимой*.

Подчеркнем, что понятия линейной зависимости и линейной независимости относятся только к системам, состоящим из *конечного* числа векторов.

Перечислим ряд простых предложений, справедливых в случае векторного пространства над произвольным полем P, доказательство которых проводится дословно так же, как в случае арифметических векторов.

1. Система, состоящая из одного вектора, линейно зависима в том и только в том случае, когда этот вектор нулевой.

2. Система, состоящая более чем из одного вектора, линейно зависима тогда и только тогда, когда какой-нибудь из этих векторов линейно выражается через остальные.

3. Система, содержащая нулевой вектор, всегда линейно зависима.

4. Если некоторая часть системы (подсистема) линейно зависима, то и вся система линейно зависима.

5. Если система векторов $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_p$ линейно независима, но при добавлении к ней некоторого вектора $\boldsymbol{a}$ становится линейно зависимой, то вектор $\boldsymbol{a}$ линейно выражается через $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_p$.

Полностью сохраняет силу и доказательство теоремы, которую мы называли теоремой о двух системах векторов.

Т е о р е м а. *Пусть* $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_p$ и $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_q$ — *две системы векторов в пространстве* L, *причем* $p > q$. *Тогда, если каждый вектор первой системы линейно выражается через векторы второй системы, то первая система линейно зависима.*

Или в сжатой формулировке: если бóльшая система линейно выражается через меньшую, то бóльшая система линейно зависима.

Читателю рекомендуется восстановить доказательства всех указанных выше фактов*.

Рассмотрим теперь любую (уже не обязательно конечную) систему S векторов в пространстве L. Линейно независимую подсистему системы S будем называть *максимальной*, если добавление к ней любого нового вектора из S делает эту систему линейно зависимой. Как и в случае пространства $\mathbf{R}^n$, вводится основное понятие *базиса*:

Базисом системы S называется любая максимальная линейно независимая подсистема этой системы.

Это определение эквивалентно следующему: базисом называется линейно независимая подсистема, через которую любой вектор системы S линейно выражается. Эквивалентность следует из отмеченного выше предложения 5.

Остается в силе следующая теорема.

Т е о р е м а. *Любые два базиса системы векторов состоят из одинакового числа векторов.*

Доказательство, данное ранее для случая $\mathbf{R}^n$, дословно повторяется. А именно пусть S' и S'' — два различных базиса системы S, содержащие соответственно p и q векторов. Если бы было $p \neq q$, например $p > q$, то из теоремы о двух системах векторов следовало бы, что подсистема S' линейно зависима, что противоречит определению базиса. Отсюда $p = q$, что и требуется получить.

Из того, что сказано выше о базисах, еще вовсе не следует, что в любом векторном пространстве для каждой системы векторов существует хотя бы один базис. Вопрос о существовании базиса будет рассмотрен в следующем параграфе.

Вопросы и упражнения

1. Сохраняют ли смысл все требования, входящие в определение векторного пространства над P, если P не поле, а только кольцо?

---

* При этом следует иметь в виду, что вся теория систем линейных уравнений распространяется на тот случай, когда коэффициентами уравнений и значениями неизвестных являются элементы произвольного поля (одно из свойств систем однородных уравнений используется в доказательстве теоремы о двух системах векторов).

2. Какие из свойств векторного пространства, установленные в пункте 3, могут оказаться неверными, если P — кольцо, но не поле?

3. Является ли векторным пространством над полем $\mathbf{R}$ действительных чисел множество всех матриц вида

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

где $a, b \in \mathbf{R}$, если операции на этом множестве определены так, как в примере 4 п. 3?

4. Пусть $\boldsymbol{C}^n$ — множество всех строк $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$, где $a_1, a_2, \ldots, a_n$ принадлежат полю $\mathbf{C}$ комплексных чисел. Введем в $\boldsymbol{C}^n$ «обычную» операцию сложения (см. формулу (2)) и «необычную» операцию умножения на числа из $\mathbf{C}$, которую определим формулой

$$(x + yi) \circ \boldsymbol{a} = x\boldsymbol{a},$$

где $x\boldsymbol{a}$ есть «обычное» умножение на число (см. формулу (3)). Будет ли множество $\boldsymbol{C}^n$ с введенными таким путем операциями векторным пространством над $\mathbf{C}$?

Решить тот же вопрос в случае, когда операция умножения определяется одной из формул:

$$(x + yi) \circ \boldsymbol{a} = |x + yi|\,\boldsymbol{a},$$
$$(x + yi) \circ \boldsymbol{a} = (x - yi)\,\boldsymbol{a}.$$

§ 2. Конечномерные векторные пространства

1. Размерность. Из содержания предыдущего параграфа видно, что многие свойства арифметического векторного пространства $\mathbf{R}^n$ остаются верными в случае произвольного векторного пространства L. Однако среди свойств пространства $\mathbf{R}^n$ имеются и такие, которые без специальных оговорок не переносятся на общий случай. Главное из них состоит в том, что в пространстве $\mathbf{R}^n$ существует базис, т. е. такая система из конечного числа линейно независимых векторов, через которую любой вектор $\boldsymbol{a} \in \mathbf{R}^n$ линейно выражается.

Рассматривая произвольное векторное пространство L, мы можем оказаться перед ситуацией, когда базиса не существует. Вот простейший пример такого рода.

Пусть L — множество, элементами которого являются бесконечные последовательности

$$(a_1, a_2, a_3, \ldots)$$

действительных чисел. Сумму двух таких последовательностей и произведение последовательности на действительное число определим естественным образом:

$$(a_1, a_2, \ldots) + (b_1, b_2, \ldots) = (a_1 + b_1, a_2 + b_2, \ldots),$$
$$k(a_1, a_2, \ldots) = (ka_1, ka_2, \ldots).$$

Снабженное такими операциями, множество L становится векторным пространством над полем действительных чисел (по аналогии с $\mathbf{R}^n$ это пространство можно обозначить $\mathbf{R}^\infty$). Роль нулевого вектора в L играет последовательность

$$(0,\ 0,\ldots).$$

Если бы пространство L обладало базисом, состоящим, допустим, из n векторов, то согласно теореме о двух системах векторов любая линейно независимая система векторов в пространстве L должна была бы содержать не более чем n векторов. Между тем в пространстве L можно указать линейно независимую систему, состоящую из какого угодно числа векторов.

В самом деле, рассмотрим в пространстве L векторы:

$$\begin{aligned} \boldsymbol{e}_1 &= (1,\ 0,\ 0,\ \ldots),\\ \boldsymbol{e}_2 &= (0,\ 1,\ 0,\ \ldots),\\ \boldsymbol{e}_3 &= (0,\ 0,\ 1,\ \ldots), \end{aligned}$$

Тогда вектор

$$k_1\boldsymbol{e}_1 + k_2\boldsymbol{e}_2 + \cdots + k_m\boldsymbol{e}_m$$

представляет собой последовательность

$$(k_1,\ k_2,\ldots,k_m,\ 0,\ 0,\ldots),$$

и равенство его нулю возможно только при $k_1 = k_2 = \ldots = k_m = 0$. Это показывает, что система векторов

$$\boldsymbol{e}_1,\ \boldsymbol{e}_2,\ \ldots,\ \boldsymbol{e}_m$$

линейно независима при любом m.

Рассмотрим еще один пример бесконечномерного пространства. Пусть L — пространство всех функций $f(x)$, определенных на множестве $\mathbf{R}$ действительных чисел и принимающих действительные значения. Мы уже видели (пункт 2 § 1), что L есть векторное пространство над полем $\mathbf{R}$. Рассмотрим следующие элементы этого пространства (следующие функции):

$$1,\ x,\ x^2,\ldots,\ x^m, \tag{1}$$

где m — какое-нибудь натуральное число.

Эти элементы линейно независимы. Действительно, если бы это было не так, то нашлись бы числа $k_0, k_1, k_2,\ldots,\ k_m$ из поля $\mathbf{R}$, не равные нулю одновременно, и такие, что вектор

$$k_0 + k_1x + k_2x^2 + \cdots + k_mx^m \tag{2}$$

равен нулевому вектору пространства L. Это означает, что функция $f(x)$, выражаемая многочленом (2), *тождественно* (т.е. при

любом значении x) равна нулю, что возможно лишь, когда все коэффициенты k_0, k_1, k_2,..., k_m равны нулю*.

Итак, элементы 1, x,..., x^m пространства L линейно независимы. Это показывает, что в пространстве L существуют линейно независимые системы, состоящие из какого угодно числа векторов (ведь m — любое натуральное число). Тем самым L не допускает базиса.

Примем теперь следующее определение:

Пространство L называется *n-мерным*, если в нем существует линейно независимая система, состоящая из n векторов, а любая система с большим, чем n, числом векторов линейно зависима; число n называют при этом *размерностью* пространства L и пишут:

$$\dim L = n$$

(от английского слова *dimention* — размерность).

Векторное пространство, имеющее размерность, называется *конечномерным*.

Как показывает определение, в n-мерном пространстве не существует линейно независимой системы, содержащей более n векторов. Если в пространстве можно указать линейно независимую систему с каким угодно числом векторов, то оно называется *бесконечномерным*.

Примеры таких пространств были приведены выше.

Бесконечномерные пространства изучаются преимущественно в курсе функционального анализа. Рассматривать их дальше мы не будем.

В конечномерном пространстве L любая система векторов, содержащая хотя бы один ненулевой вектор, обязательно имеет базис.

Действительно, пусть S — такая система. Рассмотрим какой-нибудь вектор $\boldsymbol{a}_1 \neq \mathbf{0}$ из S. Если все векторы из S линейно выражаются через $\boldsymbol{a}_1$, то $\boldsymbol{a}_1$ есть базис системы S. В противном случае в системе S найдется вектор $\boldsymbol{a}_2$, образующий вместе с $\boldsymbol{a}_1$ линейно независимую подсистему. Если все векторы из S линейно выражаются через $\boldsymbol{a}_1$ и $\boldsymbol{a}_2$, то подсистема $\{\boldsymbol{a}_1, \boldsymbol{a}_2\}$ есть базис системы S. В противном случае найдется вектор $\boldsymbol{a}_3$, образующий вместе с $\boldsymbol{a}_1$, $\boldsymbol{a}_2$ линейно независимую подсистему и т. д. Продолжив этот процесс, придем после ряда шагов (не большего, чем n, где n — размерность пространства L) к подсистеме $\{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_p\}$, являющейся базисом системы S. Таким образом, существование базиса доказано.

2. Базис конечномерного векторного пространства. Понятие базиса определено для любой системы векторов пространства L. В частности можно говорить о базисе системы, состоящей из *всех* векторов пространства L. Базис всего пространства L условимся называть в дальнейшем просто *базисом*.

---

* В самом деле, если один из коэффициентов k_1, k_2,..., k_m не равен нулю, то многочлен (2) при $x \to \infty$ имеет бесконечный предел и потому не может тождественно равняться нулю. Значит, все коэффициенты k_1, k_2,..., k_m равны нулю. Но тогда и $k_0 = 0$.

Применяя к пространству L последнюю теорему из пункта 4 предыдущего параграфа, мы получаем, что все базисы пространства L состоят из одинакового числа векторов. Если учесть, что размерностью пространства L мы назвали наибольшее число линейно независимых векторов в L, то можно теперь заключить, что *число векторов в любом базисе равно* n, где n — *размерность пространства* L.

С другой стороны, в n-мерном векторном пространстве любая система из n линейно независимых векторов является базисом. Действительно, добавить к такой системе хотя бы один вектор с сохранением линейной независимости невозможно (ибо пространство n-мерное).

Задача 1. Показать, что поле **C** комплексных чисел с обычными операциями сложения этих чисел и умножения их на действительные числа является векторным пространством над полем **R** действительных чисел. Найти размерность этого пространства.

Решение. Легко проверить, что для указанных операций условия 1—5 из определения векторного пространства (см. п. 1, § 1) выполнены. Следовательно, поле **C** является векторным пространством над **R**.

В качестве одного из базисов пространства **C** можно взять пару векторов

$$1,\ i.$$

В самом деле:

1) эти векторы линейно независимы (равенство $k_1 \cdot 1 + k_2 \times i = 0$, где k_1, k_2— действительные числа, возможно только при $k_1 = k_2 = 0$);

2) любой элемент $z \in \mathbf{C}$ представим в виде $a + bi$, $(a,\ b \in \mathbf{R})$ и, следовательно, разлагается по векторам 1, i.

Из сказанного следует, что размерность **C** над **R** равна 2.

Замечание. Если рассматривать поле **C** как векторное пространство над **C** (что, конечно, возможно), то его размерность будет равна 1. Базисом в этом случае может служить любой не равный нулю элемент $z_0 \in \mathbf{C}$; любой другой элемент z разлагается по этому базису, так как $z = (zz_0^{-1})\, z_0\ (zz_0^{-1} \in \mathbf{C})$. Из этого примера видно, что одно и то же множество, рассматриваемое как линейное пространство над разными полями, может иметь различную размерность.

Задача 2. Найти базис и размерность векторного пространства L (над полем **R**), состоящего из всех матриц вида

$$\begin{pmatrix} a_{11} a_{12} \\ a_{21} a_{22} \end{pmatrix}, \tag{3}$$

где a_{11}, a_{12}, a_{21}, a_{22}— действительные числа (см. пример 4 п. 2, § 1).

Решение. В качестве базиса можно взять следующую четверку матриц:

$$e_{11} = \begin{pmatrix} 10 \\ 00 \end{pmatrix},\ e_{12} = \begin{pmatrix} 01 \\ 00 \end{pmatrix},\ e_{21} = \begin{pmatrix} 00 \\ 10 \end{pmatrix},\ e_{22} = \begin{pmatrix} 00 \\ 01 \end{pmatrix}. \tag{4}$$

Действительно, любая матрица (3) разлагается по матрицам (4):

$$\begin{pmatrix} a_{11}a_{12} \\ a_{21}a_{22} \end{pmatrix} = a_{11}e_{11} + a_{12}e_{12} + a_{21}e_{21} + a_{22}e_{22},$$

а линейная независимость матриц (4) следует из того, что равенство

$$a_{11}e_{11} + a_{12}e_{12} + a_{21}e_{21} + a_{22}e_{22} = \begin{pmatrix} 00 \\ 00 \end{pmatrix}$$

возможно только при $a_{11} = a_{12} = a_{21} = a_{22} = 0$. Таким образом, размерность пространства L равна 4.

3. Координаты вектора в данном базисе.

$$e_1, e_2, \ldots, e_n$$

— один из базисов n-мерного векторного пространства L. Любой вектор $a \in L$ должен разлагаться по базисным векторам:

$$a = a_1e_1 + a_2e_2 + \cdots + a_ne_n. \tag{5}$$

При этом такое разложение единственно. В самом деле, если бы существовало еще одно разложение

$$a = a_1'e_1 + a_2'e_2 + \cdots + a_n'e_n, \tag{6}$$

то, вычитая (6) из (5), мы получили бы:

$$(a_1 - a_1')e_1 + (a_2 - a_2')e_2 + \cdots + (a_n - a_n')e_n = 0.$$

Но в силу линейной независимости базисных векторов это возможно только при

$$a_1 = a_1', \ a_2 = a_2', \ \ldots, \ a_n = a_n'.$$

Итак, для каждого вектора $a \in L$ существует единственное разложение по базисным векторам $e_1, e_2, \ldots, e_n$. Коэффициенты $a_1, a_2, \ldots, a_n$ этого разложения будем называть *координатами вектора* a в *базисе* $e_1, e_2, \ldots, e_n$.

Покажем, что *при сложении любых векторов* a *и* b *их координаты складываются, а при умножении вектора на число все его координаты умножаются на это число.*

В самом деле, пусть наряду с (5) имеет место равенство

$$b = b_1e_1 + b_2e_2 + \cdots + b_ne_n. \tag{7}$$

Складывая (5) и (7), получаем (пользуясь соответствующими свойствами операций):

$$a + b = (a_1 + b_1)e_1 + (a_2 + b_2)e_2 + \cdots + (a_n + b_n)e_n. \tag{8}$$

Умножение же обеих частей равенства (5) на произвольное число $k \in P$ дает равенство

$$ka = (ka_1)e_1 + (ka_2)e_2 + \cdots + (ka_n)e_n. \tag{9}$$

Из равенств (8), (9) и следует наше утверждение.

4. Изоморфизм n-мерного векторного пространства над полем P и пространства P^n. Пусть L и L' — два векторных пространства над полем P. Мы скажем, что L' изоморфно L, если существует взаимно-однозначное отображение f пространства L на пространство L', при котором

$$f(\boldsymbol{a}+\boldsymbol{b}) = f(\boldsymbol{a}) + f(\boldsymbol{b}) \tag{10}$$

и

$$f(k\boldsymbol{a}) = kf(\boldsymbol{a}), \tag{11}$$

где $\boldsymbol{a}$ и $\boldsymbol{b}$ — любые векторы из L, а k — любое число из P.

Отображение, удовлетворяющее указанным условиям, называется *изоморфным* (или *изоморфизмом*).

Как уже было отмечено (см. петит на с. 73), векторное пространство над некоторым полем является системой с одной двухместной операцией и множеством одноместных операций, соответствующих всевозможным элементам данного поля. Сопоставив друг другу двухместные операции на L и L' и одноместные операции на L и L', соответствующие одному и тому же элементу поля P, мы получим, что равенства (10), (11) являются условиями сохранения всех этих операций.

Смысл условий (10) и (11) заключается в том, что отображение f сохраняет отношения, существующие между векторами из L как элементами векторного пространства. А именно условие (10) означает, что если три вектора $\boldsymbol{a}$, $\boldsymbol{b}$ и $\boldsymbol{c}$ из L связаны соотношением

$$\boldsymbol{c} = \boldsymbol{a} + \boldsymbol{b},$$

то их образы $f(\boldsymbol{a})$, $f(\boldsymbol{b})$ и $f(\boldsymbol{c})$ в L' связаны точно таким же соотношением

$$f(\boldsymbol{c}) = f(\boldsymbol{a}) + f(\boldsymbol{b});$$

аналогично условие (11) говорит о том, что если векторы $\boldsymbol{a}$ и $\boldsymbol{b}$ связаны соотношением

$$\boldsymbol{b} = k\boldsymbol{a},$$

то их образы связаны тем же соотношением

$$f(\boldsymbol{b}) = kf(\boldsymbol{a}).$$

Нетрудно показать, что если отображение f является изоморфным, то и обратное отображение f^{-1} тоже будет изоморфным (ср. с замечанием на с. 9). Следовательно, если L' изоморфно L, то и L изоморфно L', другими словами, отношение изоморфизма векторных пространств обладает свойством симметричности, и пространства L и L' называют просто *изоморфными* (друг другу).

По поводу изоморфизма векторных пространств мы можем лишь повторить то, что было сказано ранее об изоморфизме групп, полей и вообще любых алгебраических систем: два изоморфных векторных пространства с алгебраической точки зрения считаются неотличимыми.

Рассмотрим пример двух изоморфных векторных пространств. Пусть $L_{m,n}$ — векторное пространство всех матриц типа (m, n) (m строк и n столбцов). Ставя в соответствие каждой матрице $A \in L_{m,n}$ транспонированную к ней матрицу A', получим отображение f пространства $L_{m,n}$ на пространство $L_{n,m}$, которое, как нетрудно видеть, будет изоморфным: выполнение условий (10) и (11) следует из равенств $(A + B)' = A' + B'$ и $(kA)' = kA'$, проверяемых непосредственно. Таким образом, пространства $L_{m,n}$ и $L_{n,m}$ изоморфны.

Один из наиболее важных вопросов, возникающих при изучении конечномерных векторных пространств, заключается в следующем: сколько существует *различных* n-мерных векторных пространств над P? Ответ оказывается чрезвычайно простым: при данном n существует *только одно* пространство. Точнее, справедлива следующая теорема.

Теорема. *Любое n-мерное векторное пространство L над полем P изоморфно пространству P^n.*

Напомним, что через P^n мы обозначаем векторное пространство, элементами которого являются всевозможные строки

$$(a_1, a_2, \ldots, a_n)$$

чисел из P, причем сложение таких строк и умножение их на числа из P определяются так же, как в случае арифметических векторов.

Доказательство теоремы проводится в нескольких словах. Выберем в пространстве L какой-нибудь базис $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$ и сопоставим каждому вектору $\boldsymbol{a} \in L$ набор чисел $a_1, a_2, \ldots, a_n$ — координат вектора $\boldsymbol{a}$ относительно выбранного базиса. Получаемое таким образом отображение

$$\boldsymbol{a} \to (a_1, a_2, \ldots, a_n)$$

будет, как нетрудно видеть, взаимно однозначным отображением пространства L на пространство P^n. Далее, сумма любых двух векторов $\boldsymbol{a}$ и $\boldsymbol{b}$ из L отображается в сумму соответствующих им векторов из P^n, а произведение вектора $\boldsymbol{a}$ на число $k \in P$ — в произведение соответствующего вектора на то же самое число (так как при сложении двух векторов их координаты складываются, а при умножении вектора на число его координаты умножаются на это число — см. конец пункта 3). Следовательно, полученное отображение есть изоморфизм, а пространства L и P^n изоморфны. Теорема доказана.

В заключение докажем два свойства изоморфизма векторных пространств.

Пусть f — изоморфное отображение пространства L на L'.

1. *При отображении f нулевому вектору пространства L отвечает нулевой вектор пространства L'.*

В самом деле, пусть $\boldsymbol{a}$ — произвольный вектор из L. Так как отображение f является изоморфным, то можем записать:

$$f(\boldsymbol{a}) = f(\boldsymbol{a} + \boldsymbol{0}) = f(\boldsymbol{a}) + f(\boldsymbol{0}).$$

Таким образом, для произвольного вектора $a' \in L'$ справедливо равенство

$$a' = a' + f(0),$$

откуда следует, что $f(0)$ есть нулевой вектор пространства L'.

Можно рассуждать иначе. Пространства L и L' являются *группами* относительно операции сложения. Условие (10) означает, что отображение f есть гомоморфное отображение группы L на группу L'. В силу замечания на с. 27 нейтральный элемент группы L переходит при гомоморфизме в нейтральный элемент группы L', т. е. $f(0) = 0'$, где $0'$ — нулевой вектор пространства L'.

2. *Система векторов $a_1, a_2, \ldots, a_p$ в пространстве L линейно зависима в том и только в том случае, когда линейно зависима соответствующая система $f(a_1), f(a_2), \ldots, f(a_p)$ в L'.*

Действительно, пусть система $a_1, a_2, \ldots, a_p$ линейно зависима, т. е. справедливо равенство

$$k_1 a_1 + k_2 a_2 + \cdots + k_p a_p = 0,$$

где $k_1, k_2, \ldots, k_p$ — некоторые числа, не равные одновременно нулю. Имеем:

$$f(k_1 a_1 + k_2 a_2 + \cdots + k_p a_p) = \\ = k_1 f(a_1) + k_2 f(a_2) + \cdots + k_p f(a_p);$$

но, с другой стороны, $f(0) = 0'$. Следовательно,

$$k_1 f(a_1) + k_2 f(a_2) + \cdots + k_p f(a_p) = 0',$$

что и доказывает линейную зависимость системы $f(a_1), f(a_2), \ldots, f(a_p)$.

Обратно, если линейно зависима система $f(a_1), f(a_2), \ldots, f(a_p)$, то линейно зависима и система $a_1, a_2, \ldots, a_p$. Это следует из того, что отображение, обратное изоморфному, тоже является изоморфным.

3. *Размерность пространства L совпадает с размерностью L'.*

Действительно, пусть $e_1, e_2, \ldots, e_n$ — базис пространства L. Тогда из доказанного выше свойства 2 следует, что векторы $f(e_1), f(e_2), \ldots, f(e_n)$ составляют базис пространства L'. Тем самым $\dim L = \dim L'$.

5. Связь между различными базисами пространства L. Предположим, что в n-мерном векторном пространстве L (над полем P) выбраны два различных базиса:

$$e_1, e_2, \ldots, e_n \tag{12}$$

и

$$e_1', e_2', \ldots, e_n'. \tag{13}$$

Условно назовем базис (12) *первым*, а базис (13) — *вторым*.

Разлагая векторы второго базиса по векторам первого базиса, будем иметь равенства вида:

$$\left.\begin{aligned} \boldsymbol{e}_1' &= a_{11}\boldsymbol{e}_1 + a_{21}\boldsymbol{e}_2 + \cdots + a_{n1}\boldsymbol{e}_n, \\ \boldsymbol{e}_2' &= a_{12}\boldsymbol{e}_1 + a_{22}\boldsymbol{e}_2 + \cdots + a_{n2}\boldsymbol{e}_n, \\ &\cdots\cdots\cdots \\ \boldsymbol{e}_n' &= a_{1n}\boldsymbol{e}_1 + a_{2n}\boldsymbol{e}_2 + \cdots + a_{nn}\boldsymbol{e}_n. \end{aligned}\right\} \qquad (14)$$

Матрица

$$A = \begin{pmatrix} a_{11}a_{12} & \ldots & a_{1n} \\ a_{21}a_{22} & \ldots & a_{2n} \\ & & \\ a_{n1}a_{n2} & \ldots & a_{nn} \end{pmatrix},$$

столбцы которой составлены из коэффициентов разложений векторов второго базиса по векторам первого, называется *матрицей перехода от первого базиса ко второму*.

Нетрудно видеть, что матрица перехода всегда невырожденная. В самом деле, мы уже видели, что если каждому вектору

$$\boldsymbol{a} = a_1\boldsymbol{e}_1 + a_2\boldsymbol{e}_2 + \cdots + a_n\boldsymbol{e}_n$$

из L поставить в соответствие вектор

$$(a_1,\ a_2,\ \ldots,\ a_n)$$

из P^n, то получится изоморфное отображение пространства L на пространство P^n. При этом отображении векторам $\boldsymbol{e}_1'$, $\boldsymbol{e}_2'$,..., $\boldsymbol{e}_n'$ соответствуют столбцы матрицы A. Поскольку, как мы знаем, линейно независимые векторы переходят при изоморфизме снова в линейно независимые, то из линейной независимости векторов $\boldsymbol{e}_1'$, $\boldsymbol{e}_2'$,..., $\boldsymbol{e}_n'$ должна следовать линейная независимость столбцов матрицы A. Значит, матрица A невырожденная.

Полученный результат можно истолковать следующим образом. Пусть фиксирован некоторый базис (12). Тогда любому другому базису (13) отвечает невырожденная матрица A, задающая переход от (12) к (13).

Покажем теперь, что верно и обратное, а именно: если фиксирован базис (12) и взята любая невырожденная матрица A, то определенные с ее помощью (по формулам (14)) векторы $\boldsymbol{e}_1'$, $\boldsymbol{e}_2'$,..., $\boldsymbol{e}_n'$, будут составлять снова некоторый базис.

Чтобы это установить, достаточно проверить, что векторы $\boldsymbol{e}_1'$, $\boldsymbol{e}_2'$,..., $\boldsymbol{e}_n'$ линейно независимы. Но это опять-таки следует из рассмотренного выше изоморфизма пространств L и P^n. Действительно, если бы векторы $\boldsymbol{e}_1'$, $\boldsymbol{e}_2'$,..., $\boldsymbol{e}_n'$ были линейно зависимы, то это же самое относилось бы и к столбцам матрицы A; между тем матрица A по условию невырожденная.

Окончательный итог нашим рассуждениям подводит следующая теорема.

Т е о р е м а. *Пусть* $e_1, e_2 \ldots, e_n$ — *фиксированный базис пространства* L. *Тогда все без исключения базисы получаются по формулам (14), где* A — *любая невырожденная матрица.*

Заметим, что формулы (14) могут быть записаны сжато в виде некоторого матричного равенства. А именно, если ввести в рассмотрение матрицы

$$E = (e_1 e_2 \ \ldots \ e_n), \quad E' = (e_1' e_2' \ \ldots \ e_n'),$$

то вместо (14) можно записать просто:

$$E' = EA.$$

З а д а ч а 1. Векторы e_1, e_2, ..., e_n образуют базис в L. Образуют ли базис векторы

$$\begin{aligned} e_1' &= e_1, \\ e_2' &= e_1 + e_2, \\ e_3' &= e_1 + e_2 + e_3, \\ &\ldots \quad \ldots \quad \ldots \\ e_n' &= e_1 + e_2 + e_3 + \cdots + e_n? \end{aligned}$$

Р е ш е н и е. Матрица перехода в данном случае есть

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & 1 & \ldots & 1 \\ 0 & 0 & 1 & \ldots & 1 \\ & & \ldots & & \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}.$$

Эта матрица невырожденная, так как ее строки составляют лестничную систему векторов (см.: Алгебра, ч. 1, с. 79). Следовательно, векторы e_1', e_2', ..., e_n' тоже образуют базис.

З а д а ч а 2. В пространстве всех матриц

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} (a_{11}, \ a_{12}, \ a_{21}, \ a_{22} \in \mathbf{R})$$

выбрана система матриц

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix}, \begin{pmatrix} -2 & 0 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} -1 & 6 \\ 5 & 1 \end{pmatrix}. \tag{15}$$

Образует ли эта система базис данного пространства?

Р е ш е н и е. Один из базисов рассматриваемого нами пространства состоит из матриц

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

В этом базисе векторы (15) имеют координаты

$$\begin{array}{l}(\ 0,\ 1,\ 1,\ \ 0),\\ (\ 1,\ 2,\ 3,\ -1),\\ (-2,\ 0,\ 3,\ \ 2),\\ (-1,\ 6,\ 5,\ \ 1).\end{array}$$

Матрица, столбцами которой служат строки этих координат, является вырожденной, поскольку ее определитель

$$\begin{vmatrix} 0 & 1 & -2 & -1 \\ 1 & 2 & 0 & 6 \\ 1 & 3 & 3 & 5 \\ 0 & -1 & 2 & 1 \end{vmatrix},$$

как нетрудно подсчитать, равен нулю. Следовательно, матрицы (15) не образуют базиса.

6. Связь между координатами вектора в различных базисах. Решим такую задачу. Вектор $x \in L$ разложен по двум различным базисам:

$$x = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n, \tag{16}$$
$$x = x_1' e_1' + x_2' e_2' + \cdots + x_n' e_n'. \tag{17}$$

Как выражаются координаты $x_1', x_2', \ldots, x_n'$ вектора x во втором базисе через его координаты $x_1, x_2, \ldots, x_n$ в первом базисе?

Из равенства (16) находим, учитывая формулы перехода от одного базиса к другому (формулы (14)):

$$\begin{aligned} x = {} & x_1' (a_{11} e_1 + a_{21} e_2 + \cdots + a_{n1} e_n) + \\ & + x_2' (a_{12} e_1 + a_{22} e_2 + \cdots + a_{n2} e_n) + \\ & \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ & + x_n' (a_{1n} e_1 + a_{2n} e_2 + \cdots + a_{nn} e_n). \end{aligned}$$

Если в правой части этого равенства собрать воедино все члены с e_1, все члены с e_2 и т. д., то мы получим разложение вектора x по базису $e_1, e_2, \ldots, e_n$. Но такое разложение может быть только одно. Иначе говоря, суммарный коэффициент при e_i в правой части последнего равенства должен быть равен коэффициенту x_i при e_i в равенстве (16) (i — любой из номеров $1, 2, \ldots, n$). Следовательно, имеем

$$\begin{aligned} x_1 &= a_{11} x_1' + a_{12} x_2' + \cdots + a_{1n} x_n', \\ x_2 &= a_{21} x_1' + a_{22} x_2' + \cdots + a_{2n} x_n', \\ &\cdots\cdots\cdots\cdots\cdots \\ x_n &= a_{n1} x_1' + a_{n2} x_2' + \cdots + a_{nn} x_n'. \end{aligned}$$

Эти соотношения можно записать в виде одного матричного равенства. Составив матрицы из координат вектора x в первом и во втором базисе,

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \\ \\ \cdot \\ x_n \end{pmatrix}, \quad X' = \begin{pmatrix} x'_1 \\ x'_2 \\ \\ \\ \cdot \\ x'_n \end{pmatrix},$$

получим:

$$X = AX'. \tag{18}$$

Поскольку матрица A невырожденная, то существует обратная матрица A^{-1}. Умножив на нее слева обе части равенства (18), находим окончательно:

$$X' = A^{-1}X.$$

Это и есть ответ на поставленный вопрос. *Столбец координат вектора x во втором базисе получается умножением слева столбца координат в первом базисе на матрицу A^{-1}, где A — матрица перехода от первого базиса ко второму.*

Вопросы и упражнения

1. Доказать, что система векторов a_1, a_2,..., a_n в конечномерном векторном пространстве L будет базисом пространства L в том и только в том случае, если каждый вектор из L разлагается по a_1, a_2,..., a_n, и притом единственным образом.

2. Доказать, что отображение, обратное изоморфному, также является изоморфным.

3. Доказать, что при изоморфном отображении n-мерного пространства L на L' любая система векторов из L имеет тот же ранг*, что и соответствующая ей система в L'.

4. Доказать, что при $n \neq m$ пространства P^n и P^m (P — произвольное поле) не изоморфны.

5. Найти матрицу A перехода от базиса e_1, e_2, ..., e_n к базису e_n, e_{n-1},..., e_1, а также обратную ей матрицу A^{-1} и записать формулу перехода для координат.

6. Как изменится матрица перехода от одного базиса к другому, если:

a) поменять местами два вектора первого базиса;

b) поменять местами два вектора второго базиса?

---

* Напомним, что *рангом* системы векторов называется число векторов в любом базисе этой системы (см.: Алгебра, ч. 1, с. 83).

§ 3. Подпространства векторного пространства. Векторные многообразия

1. Определение подпространства. Пусть L — векторное пространство над полем P (не обязательно конечномерное). Введем следующее определение:

Подмножество K пространства L называется *подпространством* пространства L, если это подмножество замкнуто относительно операций сложения векторов и умножения вектора на число, определенных в пространстве L.

Иначе говоря, подмножество $K \subset L$ есть подпространство, если оно обладает свойствами:

1. Из $\boldsymbol{a} \in K$, $\boldsymbol{b} \in K$ следует: $\boldsymbol{a} + \boldsymbol{b} \in K$.
2. Из $\boldsymbol{a} \in K$ следует: $k\boldsymbol{a} \in K$, где k — любое число из поля $\boldsymbol{P}$.

Очевидно, отсюда вытекает, что если какие-то векторы $\boldsymbol{a}_1$, $\boldsymbol{a}_2, \ldots, \boldsymbol{a}_p$, принадлежат подпространству K, то и любая их линейная комбинация тоже принадлежит K. Это свойство можно было бы, разумеется, принять за определение подпространства.

Любое подпространство K пространства L можно рассматривать как самостоятельное векторное пространство (над полем P). Действительно, в нем определены две операции (сложения векторов и умножения вектора на число), причем свойства 2—5 этих операций, содержащиеся в определении векторного пространства, выполняются, поскольку эти операции заимствованы из пространства L. Свойство 1 также выполняется, так как вместе с вектором $\boldsymbol{a}$ подпространство K содержит векторы $0\boldsymbol{a} = 0$ и $(-1)\,\boldsymbol{a} = -\boldsymbol{a}$.

Тривиальным примером подпространства является подмножество в L, состоящее из одного лишь нулевого вектора. Это так называемое *нулевое подпространство*.

Другой тривиальный пример — все пространство L. Однако, кроме этих двух крайних случаев, могут быть и другие подпространства.

2. Подпространство как линейная оболочка нескольких векторов. Существует простой способ строить подпространства векторного пространства L. Он заключается в том, что мы берем конечное множество

$$\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_p \tag{1}$$

векторов из L и определяем подпространство K как совокупность всех линейных комбинаций векторов (1), т. е. всех векторов вида:

$$k\boldsymbol{a}_1 + k_2\boldsymbol{a}_2 + \cdots + k_p\boldsymbol{a}_p,$$

где $k_1, k_2, \ldots, k_p$ — любые числа из P.

Что такая совокупность является подпространством, проверяется совсем просто: если векторы $\boldsymbol{a}$ и $\boldsymbol{b}$ принадлежат K, то

$$\boldsymbol{a} = k_1\boldsymbol{a}_1 + k_2\boldsymbol{a}_2 + \cdots + k_p\boldsymbol{a}_p,$$
$$\boldsymbol{b} = l_1\boldsymbol{a}_1 + l_2\boldsymbol{a}_2 + \cdots + l_p\boldsymbol{a}_p.$$

Но тогда

$$\boldsymbol{a}+\boldsymbol{b}=(k_1+l_1)\,\boldsymbol{a}_1+(k_2+l_2)\,\boldsymbol{a}_2+\cdots+(k_p+l_p)\,\boldsymbol{a}_p,$$
$$k\boldsymbol{a}=(kk_1)\,\boldsymbol{a}_1+(kk_2)\,\boldsymbol{a}_2+\cdots+(kk_p)\,\boldsymbol{a}_p,$$

откуда следует, что векторы $\boldsymbol{a}+\boldsymbol{b}$ и $k\boldsymbol{a}$ также принадлежат K.

Если пространство L конечномерно, то указанным способом может быть получено *любое* подпространство в L. Действительно, если K — какое-нибудь подпространство, то, выбрав в нем базис из векторов $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_p$, мы найдем, что, во-первых, все векторы из K являются линейными комбинациями векторов $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_p$, во-вторых, что K содержит *все* такие линейные комбинации (ибо K — подпространство). Следовательно, K в точности совпадает с множеством всех линейных комбинаций векторов $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_p$.

Если подпространство K получено указанным способом из векторов (1), то мы говорим, что оно *порождено векторами (1)*, или что оно *натянуто на векторы (1)*, или что оно является *линейной оболочкой векторов* (1). Чаще всего используется последний оборот.

Наши рассуждения показывают, что в пространстве размерности n существуют подпространства любой размерности от 1 до n: подпространство размерности k, $1 \leqslant k \leqslant n$, можно получить, если взять какие-либо k линейно независимых векторов и образовать их линейную оболочку.

Нулевому подпространству мы приписываем размерность 0. Это вполне согласуется с определением размерности векторного пространства как максимального числа линейно независимых векторов данного пространства.

Проиллюстрируем понятие подпространства в случае, когда L есть трехмерное векторное пространство $\mathbf{R}^3$. Элементы этого пространства изображаются обычными геометрическими векторами, отложенными для определенности от фиксированной точки O.

Если подпространство K в $\mathbf{R}^3$ одномерно, то его базис состоит из единственного вектора $\boldsymbol{a} \neq 0$, а само K совпадает с совокупностью векторов вида $k\boldsymbol{a}$, где k — любое действительное число. Концы таких векторов заполняют некоторую прямую (рис. 7), проходящую через O (прямую вектора $\boldsymbol{a}$).

Если K — двумерное подпространство, то его базис состоит из двух неколлинеарных векторов $\boldsymbol{a}_1, \boldsymbol{a}_2$, а само K совпадает с множеством векторов вида $k_1\boldsymbol{a}_1+k_2\boldsymbol{a}_2$, где k_1, k_2 — любые действительные числа. Концы таких векторов заполняют некоторую плоскость (рис. 8), проходящую через O (плоскость векторов $\boldsymbol{a}_1, \boldsymbol{a}_2$).

Наконец, если подпространство K трехмерно, то оно совпадает со всем пространством $\mathbf{R}^3$.

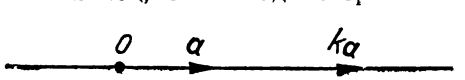

Рис. 7

3. Сумма и пересечение подпространств. Исходя из данных подпро-

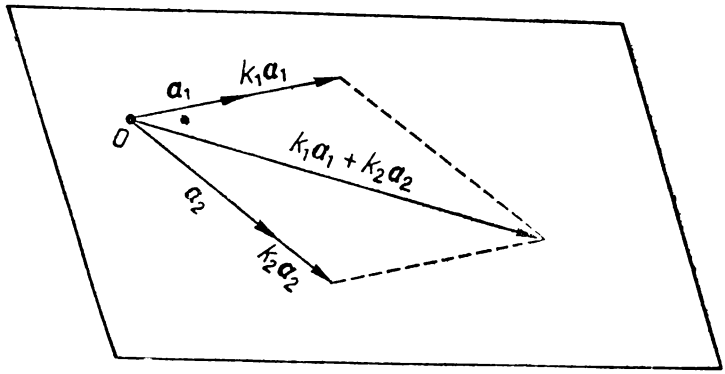

Рис. 8

странств K_1 и K_2, можно построить два новых подпространства, называемых соответственно *суммой* и *пересечением* подпространств K_1 и K_2. Сумма подпространств K_1 и K_2 определяется как множество векторов вида $\boldsymbol{a}_1 + \boldsymbol{a}_2$, где $\boldsymbol{a}_1$ — любой вектор из K_1 и $\boldsymbol{a}_2$ — любой вектор из K_2, и обозначается $K_1 + K_2$. Пересечение подпространств K_1 и K_2 определяется как множество всех векторов, принадлежащих одновременно K_1 и K_2, и обозначается $K_1 \cap K_2$.

То, что множества $K_1 + K_2$ и $K_1 \cap K_2$ являются подпространствами, проверяется просто. Пусть векторы $\boldsymbol{a}$ и $\boldsymbol{b}$ принадлежат $K_1 + K_2$, т. е.

$$\boldsymbol{a} = \boldsymbol{a}_1 + \boldsymbol{a}_2, \quad \boldsymbol{a}_1 \in K_1, \quad \boldsymbol{a}_2 \in K_2,$$
$$\boldsymbol{b} = \boldsymbol{b}_1 + \boldsymbol{b}_2, \quad \boldsymbol{b}_1 \in K_1, \quad \boldsymbol{b}_2 \in K_2.$$

Тогда

$$\boldsymbol{a} + \boldsymbol{b} = (\boldsymbol{a}_1 + \boldsymbol{a}_2) + (\boldsymbol{b}_1 + \boldsymbol{b}_2),$$
$$k\boldsymbol{a} = k\boldsymbol{a}_1 + k\boldsymbol{a}_2,$$

т. е. векторы $\boldsymbol{a} + \boldsymbol{b}$ и $k\boldsymbol{a}$ также принадлежат $K_1 + K_2$. Это доказывает, что $K_1 + K_2$ — подпространство. Аналогично, если векторы $\boldsymbol{a}$ и $\boldsymbol{b}$ принадлежат $K_1 \cap K_2$, т. е. каждый из них принадлежит как K_1, так и K_2, то сумма $\boldsymbol{a} + \boldsymbol{b}$ также принадлежит K_1 и K_2; то же самое относится и к вектору $k\boldsymbol{a}$, где k — любое число. Это доказывает, что $K_1 \cap K_2$ тоже есть подпространство.

На каждом из рисунков 9 и 10 изображены два подпространства в трехмерном векторном пространстве $\mathbf{R}^3$. Подпространства K_1 и K_2 на рис. 9 одномерны; их сумма $K_1 + K_2$ имеет размерность 2, а пересечение $K_1 \cap K_2$ — размерность 0. Подпространства K_1 и и K_2 на рис. 10 двумерны, их сумма имеет размерность 3 (она совпадает со всем пространством $\mathbf{R}^3$), а пересечение одномерно. Мы замечаем, что в обоих случаях справедливо равенство

$$\dim(K_1 + K_2) = \dim K_1 + \dim K_2 - \dim(K_1 \cap K_2) \qquad (2)$$

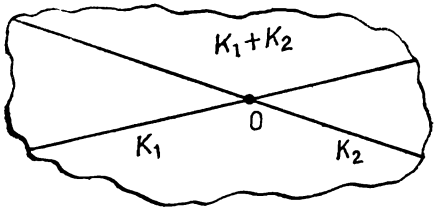

Рис. 9

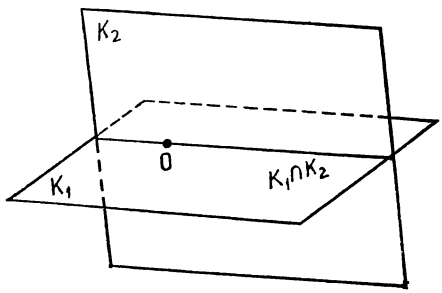

Рис. 10

— размерность суммы двух подпространств равна сумме их размерностей минус размерность их пересечения.

Теорема. *Для любых двух конечномерных подпространств K_1 и K_2 в векторном пространстве L справедлива формула* (2).

Доказательство. Выберем в подпространстве $K_1 \cap K_2$ какой-нибудь базис

$$\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_k$$

и дополним его некоторыми векторами $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_l$ до базиса K_1 и векторами $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m$ до базиса K_2. Мы полагаем, следовательно,

$$\dim(K_1 \cap K_2) = k, \quad \dim K_1 = k + l, \quad \dim K_2 = k + m.$$

Векторы подпространства $K_1 + K_2$, очевидно, линейно выражаются через векторы

$$\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_k, \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_l, \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m. \tag{3}$$

Если мы докажем, что векторы (3) линейно независимы, то отсюда будет следовать, что

$$\dim(K_1 + K_2) = k + l + m$$

и тем самым что справедлива формула (2).

Допустим, что между векторами (3) существует линейная зависимость:

$$\alpha_1\boldsymbol{a}_1 + \cdots + \alpha_k\boldsymbol{a}_k + \beta_1\boldsymbol{b}_1 + \cdots + \beta_l\boldsymbol{b}_l + \gamma_1\boldsymbol{c}_1 + \cdots + \gamma_m\boldsymbol{c}_m = \boldsymbol{0}, \tag{4}$$

где $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_l, \gamma_1, \ldots, \gamma_m$ — некоторые числа, не равные одновременно нулю. Перепишем это равенство в виде

$$\alpha_1\boldsymbol{a}_1 + \cdots + \alpha_k\boldsymbol{a}_k + \beta_1\boldsymbol{b}_1 + \cdots + \beta_l\boldsymbol{b}_l = -\gamma_1\boldsymbol{c}_1 - \cdots - \gamma_m\boldsymbol{c}_m. \tag{5}$$

Вектор

$$\alpha_1\boldsymbol{a}_1 + \cdots + \alpha_k\boldsymbol{a}_k + \beta_1\boldsymbol{b}_1 + \cdots + \beta_l\boldsymbol{b}_l \tag{6}$$

принадлежит K_1. В то же время из равенства (5) следует, что вектор (6) принадлежит и K_2; значит, он содержится в $K_1 \cap K_2$. Но в таком случае он допускает разложение по базису $K_1 \cap K_2$, т. е. по векторам $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$. Отсюда вытекает, что коэффици-

енты $\beta_1, \ldots, \beta_l$ в разложении (6) равны нулю, иначе вектор (6) имел бы два *различных* разложения по векторам базиса $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_l$. Возвращаясь к (4), находим теперь, что между векторами $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_m$ существует линейная зависимость. Но это невозможно, так как указанные векторы образуют базис в K_2. Полученное противоречие означает, что векторы (3) линейно зависимы. Теорема доказана.

4. Прямая сумма подпространств. Если пересечение $K_1 \cap K_2$ есть нулевое подпространство, то равенство (2) принимает вид:

$$\dim (K_1 + K_2) = \dim K_1 + \dim K_2.$$

В этом случае сумма $K_1 + K_2$ называется *прямой суммой*.

Для прямой суммы подпространств применяется специальное обозначение:

$$K_1 \dot{+} K_2$$

(над знаком «+» ставится точка).

Покажем, что в случае прямой суммы каждый вектор $\boldsymbol{a} \in K_1 \dot{+} K_2$ представляется в виде

$$\boldsymbol{a}_1 + \boldsymbol{a}_2 \quad (\boldsymbol{a}_1 \in K_1, \ \boldsymbol{a}_2 \in K_2) \tag{7}$$

единственным образом.

В самом деле, если бы существовали два таких представления:

$$\boldsymbol{a} = \boldsymbol{a}_1 + \boldsymbol{a}_2 \text{ и } \boldsymbol{a} = \boldsymbol{a}_1' + \boldsymbol{a}_2',$$

то, вычтя из одного равенства другое, мы получили бы:

$$\boldsymbol{a}_1 - \boldsymbol{a}_1' = -(\boldsymbol{a}_2 - \boldsymbol{a}_2').$$

Левая часть последнего равенства есть некоторый вектор из K_1, правая — вектор из K_2. Следовательно, вектор $\boldsymbol{a}_1 - \boldsymbol{a}_1' = -(\boldsymbol{a}_2 - \boldsymbol{a}_2')$ принадлежит $K_1 \cap K_2$. Но подпространство $K_1 \cap K_2$ состоит по условию из единственного вектора 0. Отсюда $\boldsymbol{a}_1 - \boldsymbol{a}_1' = \boldsymbol{0}$, $\boldsymbol{a}_2 - \boldsymbol{a}_2' = \boldsymbol{0}$, т. е.

$$\boldsymbol{a}_1 = \boldsymbol{a}_1', \ \boldsymbol{a}_2 = \boldsymbol{a}_2'.$$

Это и доказывает единственность представления $\boldsymbol{a}$ в виде (7).

Справедливо и обратное утверждение: если каждый вектор из $K_1 \dot{+} K_2$ представляется в виде (7) единственным образом, то сумма $K_1 \dot{+} K_2$ прямая. Действительно, допустим, что это не так, т. е. что подпространство $K_1 \cap K_2$ содержит ненулевой вектор $\boldsymbol{a}$. Тогда, записав

$$\boldsymbol{a} = \boldsymbol{a} + \boldsymbol{0}$$

и

$$\boldsymbol{a} = \boldsymbol{0} + \boldsymbol{a},$$

получим два различных представления вектора $\boldsymbol{a}$ в виде (7), что противоречит условию. Следовательно, $K_1 \cap K_2$ состоит только из нулевого вектора, т. е. сумма $K_1 \dot{+} K_2$ прямая.

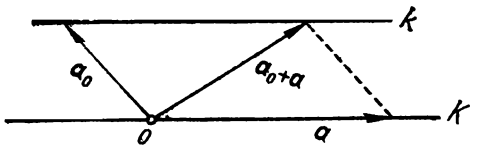

Рис. 11

Для иллюстрации укажем, что в случае подпространств K_1, K_2, изображенных на рис. 9, сумма $K_1 + K_2$ будет прямой суммой (как говорят в таких случаях, подпространства K_1 и K_2 являются *прямыми слагаемыми*). В то же время для подпространств K_1, K_2 на рис. 10 сумма $K_1 + K_2$ не прямая.

5. Векторные многообразия. Рассматривая в качестве примера трехмерное векторное пространство $\mathbf{R}^3$, мы отмечали в пункте 2, что любое одномерное пространство представляет собой совокупность векторов, концы которых расположены на прямой, проходящей через начало координат. Аналогичным образом двумерные подпространства изображаются плоскостями, также проходящими через начало координат. Но, кроме прямых и плоскостей, проходящих через начало координат, в обычном пространстве имеются еще прямые и плоскости, не проходящие через начало. Как можно охарактеризовать их с векторной точки зрения?

Пусть k — прямая в пространстве, не проходящая через начало координат O. Рассмотрим прямую, параллельную k и проходящую через O; ей отвечает одномерное подпространство K в $\mathbf{R}^3$. Выберем на прямой k некоторую точку и обозначим через $\boldsymbol{a}_0$ вектор, идущий из начала в эту точку. Из рис. 11 видно, что, складывая вектор $\boldsymbol{a}_0$ с любым вектором $\boldsymbol{a} \in K$, мы будем получать векторы, концы которых заполняют всю прямую k. Можно, следовательно, сказать, что прямая k образована концами векторов $\boldsymbol{a}_0 + \boldsymbol{a}$, где $\boldsymbol{a}$ — произвольный вектор из K. В соответствии с этим введем такое определение:

Пусть K — подпространство векторного пространства L и $\boldsymbol{a}_0$ — некоторый фиксированный вектор из L. Множество, состоящее из всех векторов вида

$$\boldsymbol{a}_0 + \boldsymbol{a},$$

где $\boldsymbol{a}$ — произвольный вектор из K, будем называть *векторным многообразием, полученным из K путем сдвига на вектор $\boldsymbol{a}_0$*. Условимся в дальнейшем это множество обозначать $\boldsymbol{a}_0 + K$. При этом подпространство K будем называть *направляющим подпространством* для многообразия $\boldsymbol{a}_0 + K$.

Разумеется, само подпространство K также является векторным многообразием (оно получается сдвигом K на нулевой вектор).

Отметим следующий факт, непосредственно вытекающий из определения многообразия $\boldsymbol{a}_0 + K$: разность любых двух векторов $\boldsymbol{x}$ и $\boldsymbol{y}$ из $\boldsymbol{a}_0 + K$ принадлежит подпространству K.

Учитывая тот факт, что по отношению к операции сложения векторов пространство L является коммутативной группой, можно сказать, что векторное многообразие, полученное сдвигом подпро-

странства K,— это *смежный класс группы L по ее подгруппе K*. Отсюда на основании общих свойств смежных классов мы делаем следующее заключение: любые два многообразия $\boldsymbol{a}_1+K$ и $\boldsymbol{a}_2+K$ либо не имеют ни одного общего вектора, либо полностью совпадают. Впрочем, это легко установить и без ссылок на свойства групп. Действительно, пусть указанные два многообразия имеют общий вектор $\boldsymbol{b}$. Тогда $\boldsymbol{a}_1-\boldsymbol{b}\in K$ и $\boldsymbol{a}_2-\boldsymbol{b}\in K$. Если теперь вместо $\boldsymbol{a}_1+K$ и $\boldsymbol{a}_2+K$ записать соответственно $\boldsymbol{b}+[(\boldsymbol{a}_1-\boldsymbol{b})+K]$ и $\boldsymbol{b}+[\boldsymbol{a}_2-\boldsymbol{b})+K]$ и учесть, что слагаемые в квадратных скобках совпадают с K, то получим, что оба многообразия совпадают с $\boldsymbol{b}+K$ и, следовательно, совпадают друг с другом.

Многообразию $\boldsymbol{a}_0+K$ приписывается *размерность*, равная размерности направляющего подпространства K.

Многообразия размерности 1 называются *прямыми*. Такое название вполне естественно, поскольку в случае пространства $\mathbb{R}^3$ одномерное многообразие состоит из векторов, концы которых заполняют некоторую прямую.

Задача 1. Показать, что:

1) два различных вектора $\boldsymbol{a}$, $\boldsymbol{b}$ принадлежат некоторой прямой, и притом единственной;

2) если три вектора $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ не принадлежат одной прямой, то существует единственное двумерное многообразие, содержащее эти векторы.

Решение. 1) Рассмотрим одномерное подпространство, порожденное (ненулевым) вектором $\boldsymbol{b}-\boldsymbol{a}$; обозначим это подпространство K. Очевидно, прямая

$$\boldsymbol{a}+K$$

содержит каждый из векторов $\boldsymbol{a}$ и $\boldsymbol{b}$ (ибо $\boldsymbol{a}=\boldsymbol{a}+0\cdot(\boldsymbol{b}-\boldsymbol{a})$, $\boldsymbol{b}=\boldsymbol{a}+1\cdot(\boldsymbol{b}-\boldsymbol{a})$).

Единственность прямой, содержащей $\boldsymbol{a}$ и $\boldsymbol{b}$, вытекает из того факта, что ее направляющее одномерное подпространство должно содержать вектор $\boldsymbol{b}-\boldsymbol{a}$ и потому должно совпадать с подпространством K. Следовательно, всякая другая прямая, содержащая $\boldsymbol{a}$ и $\boldsymbol{b}$, имеет вид $\boldsymbol{a}'+K$. Но многообразия $\boldsymbol{a}+K$ и $\boldsymbol{a}'+K$, имеющие общий вектор $\boldsymbol{a}$, совпадают.

2) Пусть теперь $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ — три вектора, не принадлежащие одной прямой. Тогда векторы $\boldsymbol{b}-\boldsymbol{a}$ и $\boldsymbol{c}-\boldsymbol{a}$ не пропорциональны: допустив, например, что $\boldsymbol{c}-\boldsymbol{a}=k(\boldsymbol{b}-\boldsymbol{a})$, получим, что векторы $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ принадлежат прямой $\boldsymbol{a}+K_1$, где K_1 порождается вектором $\boldsymbol{b}-\boldsymbol{a}$. Поэтому векторы $\boldsymbol{b}-\boldsymbol{a}$ и $\boldsymbol{c}-\boldsymbol{a}$ порождают некоторое двумерное подпространство K' (рис. 12). Рассмотрим многообразие

$$\boldsymbol{a}+K'.$$

Оно содержит, очевидно, все три вектора $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$:

$$\boldsymbol{a}=\boldsymbol{a}+0(\boldsymbol{b}-\boldsymbol{a})+0(\boldsymbol{c}-\boldsymbol{a}),$$
$$\boldsymbol{b}=\boldsymbol{a}+1(\boldsymbol{b}-\boldsymbol{a})+0(\boldsymbol{c}-\boldsymbol{a}),$$
$$\boldsymbol{c}=\boldsymbol{a}+0(\boldsymbol{b}-\boldsymbol{a})+1\cdot(\boldsymbol{c}-\boldsymbol{a}).$$

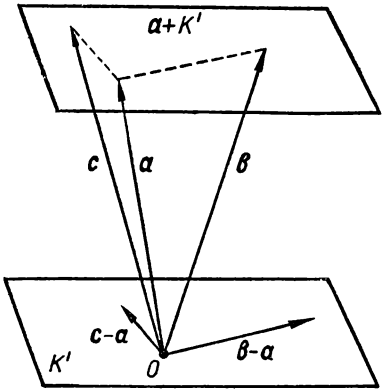

Рис. 12

То, что не существует другого двумерного многообразия, содержащего $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, доказывается просто: ведь любое такое многообразие должно иметь в качестве направляющего подпространства подпространство, содержащее векторы $\boldsymbol{b}-\boldsymbol{a}$ и $\boldsymbol{c}-\boldsymbol{a}$ и поэтому совпадающее с рассмотренным выше подпространством K'.

Задача 2. Доказать, что любые две прямые n-мерного пространства L при $n \geqslant 3$ содержатся в некотором трехмерном многообразии.

Решение. Пусть $\boldsymbol{a}_1 + K_1$ и $\boldsymbol{a}_2 + K_2$ — данные прямые. В каждом из одномерных подпространств K_1 и K_2 выберем по вектору: $\boldsymbol{b}_1 \in K_1$, $\boldsymbol{b}_2 \in K_2$, причем $\boldsymbol{b}_1 \neq 0$, $\boldsymbol{b}_2 \neq 0$. Далее рассмотрим многообразие

$$M = \boldsymbol{a}_1 + K_3,$$

где K_3 — подпространство, порожденное векторами

$$\boldsymbol{a}_2 - \boldsymbol{a}_1,\ \boldsymbol{b}_1,\ \boldsymbol{b}_2.$$

Так как $\boldsymbol{b}_1 \in K_3$, то $K_1 \subset K_3$ и, следовательно, M содержит всю прямую $\boldsymbol{a}_1 + K_1$. С другой стороны, $\boldsymbol{a}_2 + K_2 = \boldsymbol{a}_1 + (\boldsymbol{a}_2 - \boldsymbol{a}_1) + K_2$, и так как $\boldsymbol{a}_2 - \boldsymbol{a}_1 \in K_3$ и $K_2 \subset K_3$, то M содержит всю прямую K_2. Таким образом, прямые $\boldsymbol{a}_1 + K_1$ и $\boldsymbol{a}_2 + K_2$ лежат в M. Поскольку пространство K_3 порождено тремя векторами, то его размерность не превосходит 3. Если она в точности равна 3, то M есть как раз искомое многообразие. Если же окажется, что размерность M меньше 3, то, дополнив K_3 до трехмерного подпространства K' (что возможно, так как размерность всего пространства L по условию не меньше трех), получим многообразие $M' = \boldsymbol{a}_1 + K'$ размерности 3, содержащее M, а потому и обе прямые $\boldsymbol{a}_1 + K_1$, $\boldsymbol{a}_2 + K_2$.

6. Множество решений системы линейных уравнений как векторное многообразие. Рассмотрим сначала *однородную* систему линейных уравнений:

$$\left.\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= 0, \\ \cdots\quad\cdots\quad\cdots\quad\cdots & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= 0 \end{aligned}\right\} \text{(система } S_0\text{)}.$$

Все коэффициенты при неизвестных предполагаются принадлежащими данному полю P. Значения неизвестных ищутся тоже в поле P.

Каждое решение

$$(x_1, x_2, \ldots, x_n)$$

системы S_0 есть некоторый вектор пространства P^n. Обозначим множество всех решений системы S_0 через $K(S_0)$.

В первой части курса было показано (см. Алгебра, ч. 1, с. 100), что линейная комбинация нескольких решений однородной системы есть снова решение этой системы. Отсюда мы делаем теперь вывод, что *множество K (S_0) всех решений системы S_0 есть подпространство в P^n.*

Любой базис множества $K(S_0)$ мы условились ранее называть фундаментальным набором решений системы S_0. Было доказано, что число решений в фундаментальном наборе равно $n - r$, где r — ранг матрицы

$$A = \begin{pmatrix} a_{11}a_{12} \ldots a_{1n} \\ a_{21}a_{22} \ldots a_{2n} \\ \\ a_{m1}a_{m2} \ldots a_{mn} \end{pmatrix}.$$

Итак, *размерность подпространства $K(S_0)$ равна $n - r$, где n — число неизвестных, а r — ранг матрицы, составленной из коэффициентов при неизвестных в системе S_0.*

Рассмотрим теперь произвольную (но совместную) систему:

$$\left.\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2, \\ \cdot \qquad \cdot \qquad \cdot \qquad \cdot \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{array}\right\} \text{(система } S\text{)}.$$

С системой S естественно связать однородную систему S_0, полученную из S заменой свободных членов уравнений нулями. В первой части курса было показано (см. Алгебра, ч. 1, с. 97), что все решения системы S можно получить, взяв какое-либо одно решение

$$x^0 = (x_1^0, x_2^0, \ldots, x_n^0)$$

и складывая его со всевозможными решениями системы S_0. Это означает, что множество всех решений системы S есть многообразие

$$x^0 + K(S_0)$$

в пространстве P^n.

В случае, если матрица A имеет ранг n, размерность подпространства $K(S_0)$ равна 0, т. е. подпространство $K(S_0)$ нулевое. В этом случае система S будет иметь единственное решение x^0. Если же размерность $K(S_0)$ выше нуля, решений системы S будет существовать бесчисленное множество.

Вопросы и упражнения

1. Является ли подпространством пространства $\mathbf{R}^2$, рассматриваемого как множество всех радиус-векторов обычной плоскости, совокупность всех векторов с концами в первой координатной четверти?

2. Пусть L — векторное пространство всех матриц вида

$$\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix},$$

где $x_1, x_2, x_3, x_4 \in P$. Доказать, что подмножество, состоящее из всех матриц вида

$$\begin{pmatrix} x & y \\ z & -x \end{pmatrix},$$

является подпространством.

3. Всегда ли объединение двух подпространств является подпространством?

4. Какую размерность в пространстве $\mathbf{R}^5$ может иметь пересечение двух трехмерных подпространств?

5. Доказать, что сумма подпространств K_1 и K_2 тогда и только тогда будет прямой суммой, когда нулевой вектор допускает *только одно* представление в виде $\boldsymbol{a}_1 + \boldsymbol{a}_2$, где $\boldsymbol{a}_1 \in K_1$, $\boldsymbol{a}_2 \in K_2$ (это представление есть, очевидно, $\mathbf{0} + \mathbf{0}$).

6. Могут ли координаты всех векторов некоторой прямой (вообще, некоторого векторного многообразия) в пространстве $\mathbf{R}^n$ быть положительными?

7. Пусть $\boldsymbol{a}$ и $\boldsymbol{b}$ — два непропорциональных вектора и p — прямая, содержащая эти векторы (см. задачу в пункте 5). Доказать, что p состоит из всех векторов вида $k\boldsymbol{a} + l\boldsymbol{b}$, где k и l — любые числа из P, сумма которых равна 1.

8. Какова размерность векторного многообразия в $\mathbf{R}^5$, определяемого уравнением

$$x_1 + x_2 + x_3 + x_4 + x_5 = 1?$$

Глава III

ЕВКЛИДОВЫ ПРОСТРАНСТВА

В предыдущей главе были введены и изучены некоторые важные понятия, относящиеся к векторным пространствам, такие, как базис, размерность, подпространство. Однако круг понятий, связанных с обычными геометрическими векторами на плоскости или в трехмерном пространстве, значительно шире, например: каждый вектор имеет длину, два ненулевых вектора образуют определенный угол, существуют перпендикулярные векторы и т. д. Данная глава посвящается обобщению подобного рода понятий (их называют обычно *метрическими*) на случай пространства любой размерности.

На всем протяжении этой главы будут рассматриваться векторные пространства *только над полем* $\mathbf{R}$ *действительных чисел*. Читатель уже знает, что для данной размерности n существует только одно, с точностью до изоморфизма, такое пространство, а именно пространство $\mathbf{R}^n$.

§ 1. Скалярное произведение. Евклидово n-мерное пространство

1. Определение скалярного произведения. Напомним сначала некоторые сведения из курса геометрии.

Каждым двум векторам $\boldsymbol{x}$ и $\boldsymbol{y}$ в обычном трехмерном пространстве ставится в соответствие действительное число, обозначаемое $(\boldsymbol{x}, \boldsymbol{y})$ и называемое *скалярным произведением* $\boldsymbol{x}$ на $\boldsymbol{y}$. Оно определяется формулой

$$(\boldsymbol{x}, \boldsymbol{y}) = |\boldsymbol{x}| \cdot |\boldsymbol{y}| \cdot \cos\varphi, \tag{1}$$

где $|\boldsymbol{x}|$ и $|\boldsymbol{y}|$ обозначают соответственно длины векторов $\boldsymbol{x}$ и $\boldsymbol{y}$, а φ — угол между этими векторами. Доказывается, что в прямоугольной декартовой системе координат для любых двух векторов $\boldsymbol{x}$ и $\boldsymbol{y}$ справедлива формула

$$(\boldsymbol{x}, \boldsymbol{y}) = x_1y_1 + x_2y_2 + x_3y_3, \tag{2}$$

где x_1, x_2, x_3 означают координаты вектора $\boldsymbol{x}$, а y_1, y_2, y_3— координаты вектора $\boldsymbol{y}$.

Полагая в формуле (2) $\boldsymbol{x} = \boldsymbol{y}$, получаем:

$$(\boldsymbol{x}, \boldsymbol{x}) = |\boldsymbol{x}|^2,$$

откуда

$$|x| = \sqrt{(x, x)}. \tag{3}$$

Тогда из формулы (1) следует:

$$\cos\varphi = \frac{(x, y)}{\sqrt{(x, x)} \cdot \sqrt{(y, y)}}. \tag{4}$$

Таким образом, и длина вектора, и угол между векторами выражаются через скалярное произведение. Поэтому, обобщив на n-мерный случай понятие скалярного произведения, мы смогли бы длину вектора, а также угол между векторами определить с помощью формул (3) и (4).

Скалярное произведение векторов в трехмерном пространстве обладает рядом простых свойств, а именно:

1. $(x,x) \geqslant 0$, причем $(x,x) = 0$ только при $x = 0$;
2. $(x, y) = (y, x)$;
3. $(x, ky) = k(x, y)$, где k — любое действительное число;
4. $(x, y + z) = (x, y) + (x, z)$.

При любом обобщении понятия скалярного произведения желательно, чтобы свойства 1—4 сохраняли силу. Ввиду этого примем следующее определение.

Определение. Будем говорить, что в векторном пространстве L над полем действительных чисел определена операция скалярного умножения, если любой паре векторов x, $y \in L$ сопоставлено действительное число, обозначаемое (x, y) и называемое *скалярным произведением* векторов x и y, причем выполняются свойства 1—4. В этом случае говорят также, что в пространстве L *определено* (или *введено*) *скалярное произведение*.

Векторное пространство, в котором определено скалярное произведение, получает дополнительное название *евклидово* (полное название — евклидово векторное пространство).

Внимательный читатель заметит, что термин «операция» понимается здесь в широком смысле: каждой паре элементов x и y, принадлежащих множеству L, сопоставляется элемент *другого* множества — множества действительных чисел (см. петит на с. 5,6).

2. Задание скалярного произведения в конечномерном пространстве. Данное нами определение оставляет открытым вопрос: можно ли хотя бы одним способом ввести в векторном пространстве скалярное произведение? Если иметь в виду конечномерное пространство, то ответ на этот вопрос подсказывает выражение, стоящее в правой части формулы (2). А именно, выберем в n-мерном пространстве L какой-нибудь базис

$$e_1, e_2, \ldots, e_n$$

и сопоставим каждым двум векторам x и y число

$$(x, y) = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n, \tag{5}$$

где $x_1, x_2, \ldots, x_n$— это координаты вектора $\boldsymbol{x}$, а $y_1, y_2, \ldots, y_n$— координаты вектора $\boldsymbol{y}$ в выбранном базисе. Тогда, как нетрудно видеть, все свойства 1—4 будут выполнены и тем самым в L будет определено скалярное произведение.

Если выбрать другой базис

$$\boldsymbol{e}_1^*, \boldsymbol{e}_2^*, \ldots, \boldsymbol{e}_n^*$$

и сопоставить векторам $\boldsymbol{x}$ и $\boldsymbol{y}$ число

$$(\boldsymbol{x}, \boldsymbol{y})^* = x_1^* y_1^* + x_2^* y_2^* + \cdots + x_n^* y_n^*$$

(где $x_1^*, x_2^*, \ldots, x_n^*$ и $y_1^*, y_2^*, \ldots, y_n^*$ суть координаты векторов $\boldsymbol{x}$ и $\boldsymbol{y}$ в новом базисе), то, вообще говоря, равенство

$$(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{x}, \boldsymbol{y})^*$$

выполняться не будет. Отсюда становится ясно, что в n-мерном пространстве L скалярное произведение можно ввести многими различными способами.

В дальнейшем, однако, будет показано, что, как бы ни выбиралось в пространстве L скалярное произведение, обязательно найдется такой базис (и даже не один), в котором имеет место формула (5).

3. Выражение скалярного произведения в координатах. Возвращаясь к определению скалярного произведения, извлечем из основных свойств 1—4 некоторые простейшие следствия.

Прежде всего установим, что справедливы следующие два свойства, дополняющие свойства 3 и 4:

$$3'.\ (k\boldsymbol{x}, \boldsymbol{y}) = k(\boldsymbol{x}, \boldsymbol{y});$$
$$4'.\ (\boldsymbol{x} + \boldsymbol{y}, \boldsymbol{z}) = (\boldsymbol{x}, \boldsymbol{z}) + (\boldsymbol{y}, \boldsymbol{z}).$$

Свойство 3′ вытекает из цепочки равенств:

$$(k\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{y}, k\boldsymbol{x}) = k(\boldsymbol{y}, \boldsymbol{x}) = k(\boldsymbol{x}, \boldsymbol{y}),$$

в каждом из которых использовано одно из основных свойств скалярного произведения. Аналогично доказывается свойство 4′:

$$(\boldsymbol{x} + \boldsymbol{y}, \boldsymbol{z}) = (\boldsymbol{z}, \boldsymbol{x} + \boldsymbol{y}) = (\boldsymbol{z}, \boldsymbol{x}) + (\boldsymbol{z}, \boldsymbol{y}) = (\boldsymbol{x}, \boldsymbol{z}) + (\boldsymbol{y}, \boldsymbol{z}).$$

Комбинируя свойства 3 и 3′, получим:

$$3''.\ (k\boldsymbol{x}, l\boldsymbol{y}) = kl(\boldsymbol{x}, \boldsymbol{y}).$$

Далее, из 4 и 4′ сразу же следует, что

$$(\boldsymbol{x}_1 + \boldsymbol{x}_2 + \cdots + \boldsymbol{x}_p, \boldsymbol{y}_1 + \boldsymbol{y}_2 + \cdots + \boldsymbol{y}_q) = \sum_{i,j} (\boldsymbol{x}_i, \boldsymbol{y}_j),$$

т. е. скалярное умножение суммы на сумму подчиняется обычному распределительному закону: каждое слагаемое первой суммы надо умножить на каждое слагаемое второй и результаты сложить.

Отсюда, а также из свойства 3″ получается и правило умножения одной линейной комбинации на другую:

$$(k_1\boldsymbol{x}_1 + k_2\boldsymbol{x}_2 + \cdots + k_p\boldsymbol{x}_p,\ l_1\boldsymbol{y}_1 + l_2\boldsymbol{y}_2 + \cdots + l_q\boldsymbol{y}_q) = \sum_{i,j} k_i l_j (\boldsymbol{x}_i,\ \boldsymbol{y}_j). \tag{6}$$

Из этой формулы мы выведем сейчас выражение для скалярного произведения $(\boldsymbol{x}, \boldsymbol{y})$ через координаты векторов $\boldsymbol{x}$ и $\boldsymbol{y}$. Пусть в пространстве L выбран некоторый базис

$$\boldsymbol{e}_1,\ \boldsymbol{e}_2,\ \ldots,\ \boldsymbol{e}_n.$$

Рассмотрим два произвольных вектора $\boldsymbol{x}$ и $\boldsymbol{y}$. Разлагая их по базису, получим:

$$\boldsymbol{x} = x_1\boldsymbol{e}_1 + x_2\boldsymbol{e}_2 + \cdots + x_n\boldsymbol{e}_n,$$
$$\boldsymbol{y} = y_1\boldsymbol{e}_1 + y_2\boldsymbol{e}_2 + \cdots + y_n\boldsymbol{e}_n.$$

Теперь для подсчета $(\boldsymbol{x}, \boldsymbol{y})$ можно воспользоваться формулой (6). Имеем:

$$(\boldsymbol{x},\ \boldsymbol{y}) = \sum_{i,j} x_i y_j (\boldsymbol{e}_i,\ \boldsymbol{e}_j).$$

Величины

$$g_{ij} = (\boldsymbol{e}_i,\ \boldsymbol{e}_j)$$

— это постоянные числа, зависящие только от выбранного базиса. Таким образом, если фиксирован определенный базис, то для скалярного произведения получается следующее выражение:

$$(\boldsymbol{x},\ \boldsymbol{y}) = \sum_{i,j} g_{ij} x_i y_j. \tag{7}$$

4. Модуль вектора, угол между векторами, ортогональность. После того как определено скалярное произведение, такие понятия, как модуль вектора и угол между векторами, вводятся по аналогии с двумерным и трехмерным случаями:

1) *Модулем* (или *нормой*, или *длиной*) вектора $\boldsymbol{x}$ называется число

$$|\boldsymbol{x}| = \sqrt{(\boldsymbol{x},\ \boldsymbol{x})} \tag{8}$$

(величина, стоящая под знаком корня, неотрицательна в силу свойства 1 скалярного произведения).

2) *Углом* между двумя ненулевыми векторами $\boldsymbol{x}$ и $\boldsymbol{y}$ называется число φ, определяемое равенством

$$\cos\varphi = \frac{(\boldsymbol{x},\ \boldsymbol{y})}{|\boldsymbol{x}|\ |\boldsymbol{y}|} \tag{9}$$

и дополнительным условием $0 \leqslant \varphi \leqslant \pi$ (существование такого числа будет доказано ниже).

3) Векторы x и y называют *ортогональными* или *перпендикулярными* друг другу (и пишут $x \perp y$), если их скалярное произведение равно нулю.

В силу формулы (9) ненулевые векторы x и y ортогональны тогда и только тогда, когда угол φ между ними равен $\frac{\pi}{2}$ ($\cos\varphi = 0$).

Заметим еще, что *нулевой вектор ортогонален любому вектору.* Это следует из равенств:

$$(0,\ x) = (0x,\ x) = 0 \cdot (x,\ x) = 0.$$

5. **Неравенство Коши — Буняковского.** Определение модуля вектора, а также определение ортогональности двух векторов не требуют особых пояснений. Иначе обстоит дело с формулой (9), определяющей угол между ненулевыми векторами. Угол φ, косинус которого равен выражению

$$\frac{(x,\ y)}{|x|\ |y|},$$

существует тогда и только тогда, когда это выражение заключено между -1 и $+1$, т. е. когда выполняется неравенство

$$\frac{(x,\ y)^2}{|x|^2\ |y|^2} \leqslant 1,$$

которое (при $x \neq 0$ и $y \neq 0$) равносильно неравенству

$$(x,\ y)^2 \leqslant (x,\ x)\,(y,\ y). \tag{10}$$

Неравенство (10) носит название *неравенства Коши — Буняковского.* Докажем, что оно справедливо для любых двух векторов x и y.

Метод, с помощью которого доказывается неравенство (10), весьма поучителен. Пусть t — какое угодно действительное число. Подсчитаем скалярный квадрат вектора $y - tx$. Имеем:

$$(y - tx,\ y - tx) = (y,\ y) - t\,(x,\ y) - t\,(y,\ x) + t^2\,(x,\ x).$$

Мы получили равенство вида

$$(y - tx,\ y - tx) = \alpha t^2 + 2\beta t + \gamma,$$

где $\alpha = (x, x)$, $\beta = -(x, y)$, $\gamma = (y, y)$. Квадратный трехчлен* относительно t, стоящий в правой части этого равенства, при любом значении t есть число неотрицательное (ибо он равен скалярному квадрату некоторого вектора). Как известно, отсюда вытекает, что дискриминант этого трехчлена, т. е. выражение

$$\beta^2 - \alpha\gamma,$$

---

* Предполагается, что $\alpha = (x, x) \neq 0$. Достаточно рассмотреть только этот случай: если $\alpha = 0$, то $x = 0$, откуда $(x, y) = 0$; неравенство (10) принимает тогда вид $0 \leqslant 0$ и, следовательно, выполняется.

есть число неположительное. Следовательно,

$$(\boldsymbol{x},\ \boldsymbol{y})^2 - (\boldsymbol{x},\ \boldsymbol{x})\,(\boldsymbol{y},\ \boldsymbol{y}) \leqslant 0,$$

что равносильно неравенству (10).

Итак, мы доказали неравенство Коши — Буняковского и тем самым обосновали корректность определения (9).

Небезынтересно проследить, какой вид принимает неравенство Коши — Буняковского, если скалярное произведение задано (в некотором базисе) формулой (5). В этом случае мы получаем неравенство

$$(x_1y_1 + x_2y_2 + \ldots + x_ny_n)^2 \leqslant$$
$$\leqslant (x_1^2 + x_2^2 + \ldots + x_n^2)\,(y_1^2 + y_2^2 + \ldots + y_n^2),$$

которое, таким образом, справедливо для всех значений входящих в него букв.

Вопросы и упражнения

1. Вывести из свойств 1—4 скалярного произведения, что, каково бы ни было действительное число α, найдутся два вектора $\boldsymbol{x}$ и $\boldsymbol{y}$, такие, что $(\boldsymbol{x},\ \boldsymbol{y}) = \alpha$.

2. Можно ли в формуле (5) на с. 102 опустить последнее слагаемое и определить скалярное произведение формулой

$$(\boldsymbol{x},\ \boldsymbol{y}) = x_1y_1 + x_2y_2 + \ldots + x_{n-1}y_{n-1}?$$

3. Проанализировав доказательство неравенства Коши — Буняковского, показать, что равенство $(\boldsymbol{x}, \boldsymbol{y})^2 = (\boldsymbol{x}, \boldsymbol{x})\ (\boldsymbol{y}, \boldsymbol{y})$ справедливо в том и только в том случае, когда векторы $\boldsymbol{x}$ и $\boldsymbol{y}$ пропорциональны.

§ 2. Ортогональная система векторов. Ортонормированный базис

1. Ортогональная система векторов.

Определение. Система векторов

$$\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ \ldots,\ \boldsymbol{a}_p \qquad (1)$$

в евклидовом пространстве называется *ортогональной*, если векторы этой системы попарно ортогональны:

$$(\boldsymbol{a}_i,\ \boldsymbol{a}_j) = 0,$$

где i, j не превосходят p и $i \neq j$.

Очевидно, всякая подсистема ортогональной системы сама является ортогональной системой.

Возникает вопрос: сколько векторов может содержать ортогональная система? Если не требовать, чтобы каждый вектор системы был отличен от $\boldsymbol{0}$, то ответ будет гласить — любое число векторов (система $\boldsymbol{a}_1 = \boldsymbol{0}$, $\boldsymbol{a}_2 = \boldsymbol{0}, \ldots, \boldsymbol{a}_p = \boldsymbol{0}$ ортогональна при любом p). Поэтому предположим дополнительно, что все векторы системы —

ненулевые. Оказывается, что при этом условии их число не может превосходить размерности пространства. Это вытекает из следующей леммы.

Лемма. *Ортогональная система, состоящая из ненулевых векторов, всегда линейно независима.*

Доказательство. Пусть ненулевые векторы (1) образуют ортогональную систему. Предположим, рассуждая от противного, что они линейно зависимы, т. е. справедливо равенство вида

$$k_1\boldsymbol{a}_1 + k_2\boldsymbol{a}_2 + \ldots + k_p\boldsymbol{a}_p = \boldsymbol{0},$$

где среди чисел $k_1, k_2, \ldots, k_p$ имеются не равные нулю. Пусть, например, $k_1 \neq 0$. Тогда, умножив скалярно обе части последнего равенства на вектор $\boldsymbol{a}_1$, получим:

$$k_1(\boldsymbol{a}_1, \boldsymbol{a}_1) + k_2(\boldsymbol{a}_2, \boldsymbol{a}_1) + \ldots + k_p(\boldsymbol{a}_p, \boldsymbol{a}_1) = 0$$

или, если учесть, что вектор $\boldsymbol{a}_1$ ортогонален любому из векторов $\boldsymbol{a}_2, \ldots, \boldsymbol{a}_p$,

$$k_1(\boldsymbol{a}_1, \boldsymbol{a}_1) = 0.$$

Но $(\boldsymbol{a}_1, \boldsymbol{a}_1) \neq 0$, ибо $\boldsymbol{a}_1 \neq \boldsymbol{0}$. Следовательно, $k_1 = 0$. Полученное противоречие доказывает, что система (1) линейно независима.

Поскольку в n-мерном векторном пространстве любая линейно независимая система состоит не более чем из n векторов, то из доказанной леммы вытекает такое следствие:

Ортогональная система ненулевых векторов в n-мерном евклидовом пространстве состоит не более чем из n векторов.

При $n = 3$ это предложение геометрически очевидно: в обычное трехмерное пространство невозможно «вместить» более трех попарно ортогональных ненулевых векторов.

2. Существование ортогонального базиса. Мы докажем теперь, что в n-мерном евклидовом пространстве существует ортогональная система, состоящая *в точности* из n ненулевых векторов. В силу леммы предыдущего пункта такая система линейно независима и потому является базисом. Этот базис называют ортогональным. Существование ортогонального базиса основывается на следующем факте:

Для любой системы векторов n-мерного евклидова пространства с числом векторов $p < n$ найдется ненулевой вектор, ортогональный всем векторам этой системы.

Для доказательства обозначим векторы системы через $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_p$, а искомый вектор — через $\boldsymbol{x}$. Вектор $\boldsymbol{x}$ должен удовлетворять условиям:

$$(\boldsymbol{x}, \boldsymbol{a}_1) = 0, \ (\boldsymbol{x}, \boldsymbol{a}_2) = 0, \ \ldots, \ (\boldsymbol{x}, \boldsymbol{a}_p) = 0. \tag{2}$$

Выберем какой-либо базис $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$ и положим

$$\boldsymbol{x} = x_1\boldsymbol{e}_1 + x_2\boldsymbol{e}_2 + \cdots + x_n\boldsymbol{e}_n.$$

Тогда условия (2) перепишутся в виде.

$$(x_1\boldsymbol{e}_1 + x_2\boldsymbol{e}_2 + \ldots + x_n\boldsymbol{e}_n,\ \boldsymbol{a}_1) = 0,$$
$$(x_1\boldsymbol{e}_1 + x_2\boldsymbol{e}_2 + \ldots + x_n\boldsymbol{e}_n,\ \boldsymbol{a}_2) = 0,$$
$$\ldots\ldots\ldots$$
$$(x_1\boldsymbol{e}_1 + x_2\boldsymbol{e}_2 + \ldots + x_n\boldsymbol{e}_n,\ \boldsymbol{a}_p) = 0.$$

Если ввести обозначение $\alpha_{ji} = (\boldsymbol{e}_i, \boldsymbol{a}_j)$, то мы приходим к системе:

$$\alpha_{11}x_1 + \alpha_{12}x_2 + \ldots + \alpha_{1n}x_n = 0,$$
$$\alpha_{21}x_1 + \alpha_{22}x_2 + \ldots + \alpha_{2n}x_n = 0,$$
$$\ldots\ldots\ldots$$
$$\alpha_{p1}x_1 + \alpha_{p2}x_2 + \ldots + \alpha_{pn}x_n = 0.$$

Это система из p однородных уравнений с n неизвестными x_1, x_2, ..., x_n. Так как $p < n$, то система должна иметь ненулевое решение (см.: Алгебра, ч. 1, с. 57.). Следовательно, существует ненулевой вектор $\boldsymbol{x}$, удовлетворяющий условиям (2).

Из доказанного непосредственно вытекает существование ортогонального базиса. Для построения такого базиса берем произвольный вектор $\boldsymbol{a}_1 \neq \boldsymbol{0}$, затем какой-либо вектор $\boldsymbol{a}_2 \neq \boldsymbol{0}$, ортогональный $\boldsymbol{a}_1$, затем какой-либо вектор $\boldsymbol{a}_3 \neq \boldsymbol{0}$, ортогональный $\boldsymbol{a}_1$ и $\boldsymbol{a}_2$, и т. д., пока не дойдем до вектора $\boldsymbol{a}_n \neq \boldsymbol{0}$, ортогонального ранее построенным векторам $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_{n-1}$; существование каждого очередного вектора обеспечивается доказанным выше утверждением. Полученная таким путем система

$$\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ \ldots,\ \boldsymbol{a}_n$$

и будет искомым базисом.

Итак, *в n-мерном евклидовом пространстве существует ортогональный базис.*

3. Ортонормированный базис. Укажем сначала, что вектор $\boldsymbol{e}$ евклидова пространства называется *нормированным* или *единичным*, если его модуль равен 1.

Если ненулевой вектор $\boldsymbol{a}$ не является нормированным, то умножением на число $\frac{1}{|\boldsymbol{a}|}$ из него можно получить нормированный вектор $\boldsymbol{e}$:

$$\boldsymbol{e} = \frac{1}{|\boldsymbol{a}|}\boldsymbol{a}.$$

Действительно,

$$(\boldsymbol{e},\ \boldsymbol{e}) = \frac{1}{|\boldsymbol{a}|^2}(\boldsymbol{a},\ \boldsymbol{a}) = 1.$$

Переход от $\boldsymbol{a}$ к $\boldsymbol{e}$ называется *нормированием* вектора $\boldsymbol{a}$.

Определение. Базис

$$\boldsymbol{e}_1,\ \boldsymbol{e}_2,\ \ldots,\ \boldsymbol{e}_n \qquad (2)$$

евклидова пространства L называется *ортонормированным*, если:

1) этот базис ортогональный:

$$(e_i,\ e_j) = 0 \text{ при } i \neq j; \tag{3}$$

2) каждый из базисных векторов является нормированным:

$$(e_i,\ e_i) = 1. \tag{4}$$

Чтобы получить ортонормированный базис, можно взять любой ортогональный базис

$$a_1,\ a_2,\ \ldots,\ a_n$$

(как мы знаем, такой базис всегда существует) и затем каждый из его векторов нормировать:

$$e_1 = \frac{1}{|a_1|}a_1,\ e_2 = \frac{1}{|a_2|}a_2,\ \ldots,\ e_n = \frac{1}{|a_n|}a_n.$$

Скалярное произведение векторов особенно просто выражается через их координаты в ортонормированном базисе. Если

$$x = x_1e_1 + x_2e_2 + \ldots + x_ne_n,$$
$$y = y_1e_1 + y_2e_2 + \ldots + y_ne_n,$$

то перемножая x и y скалярно и учитывая (3) и (4), получаем:

$$(x,\ y) = x_1y_1 + x_2y_2 + \ldots + x_ny_n \tag{5}$$

(скалярное произведение равно сумме произведений одноименных координат). Нетрудно проверить, что и обратно, если в некотором базисе скалярное произведение выражается формулой (5), то этот базис является ортонормированным.

Заметим, что, установив существование ортонормированного базиса, мы тем самым выполнили обещание, данное в пункте 2 предыдущего параграфа: в ортонормированном базисе скалярное произведение выражается формулой (5).

4. Изоморфизм евклидовых пространств одинаковой размерности. Выше уже говорилось о том, что скалярное произведение можно ввести в n-мерном векторном пространстве многими *различными* способами. При этом, как может показаться на первый взгляд, должны получаться *разные* евклидовы пространства. Однако это не так. Мы сейчас покажем, что евклидовы пространства одной и той же размерности можно считать *одинаковыми*, поскольку такие пространства представляют собой изоморфные алгебраические системы. Предварительно сформулируем точное определение изоморфизма евклидовых пространств.

Определение. Евклидовы пространства L и L' называются *изоморфными*, если существует взаимно одновначное отображение f пространства L на пространство L', удовлетворяющее следующим условиям:

$$f(x + y) = f(x) + f(y), \tag{6}$$
$$f(kx) = kf(x), \tag{7}$$
$$(x,\ y) = (f(x),\ f(y)), \tag{8}$$

где x, y — любые элементы из L, а k — любое действительное число. Отображение f называется при этом *изоморфизмом* между пространствами L и L'.

Первые два условия данного определения, как уже говорилось раньше, являются условиями сохранения операций сложения и умножения на число; они выражают то обстоятельство, что системы L и L' изоморфны как *векторные пространства*. Третье условие можно считать условием сохранения операции скалярного умножения.

Чтобы избежать громоздких определений, мы не рассматриваем в общем виде системы с операциями типа скалярного умножения. Отметим только, что понятия гомоморфизма и изоморфизма нетрудно распространить и на такие системы, обобщив должным образом условие сохранения операций. Из этого обобщенного условия как раз и получается условие сохранения скалярного умножения в случае евклидовых пространств.

Теперь мы можем доказать следующую важную теорему.

Т е о р е м а. *Два евклидовых пространства одинаковой размерности изоморфны.*

Д о к а з а т е л ь с т в о. Пусть L и L' — два евклидовых пространства одной и той же размерности n. Выберем в L какой-нибудь ортонормированный базис

$$e_1, e_2, \ldots, e_n, \tag{9}$$

а в L' — некоторый ортонормированный базис

$$e'_1, e'_2, \ldots, e'_n. \tag{9'}$$

Определим отображение f пространства L на пространство L' следующим образом: если

$$x = x_1e_1 + x_2e_2 + \ldots + x_ne_n,$$

то

$$f(x) = x_1e'_1 + x_2e'_2 + \ldots + x_ne'_n.$$

Таким образом, вектору $x \in L$, имеющему в базисе (9) координаты $x_1, x_2, \ldots, x_n$, сопоставляется вектор $f(x) \in L'$, имеющий *точно такие же* координаты в базисе (9').

Нетрудно видеть, что отображение f есть изоморфизм между пространствами L и L'. В самом деле, для произвольных векторов x и y из L имеем:

$$x + y = (x_1 + y_1)e_1 + (x_2 + y_2)e_2 + \ldots + (x_n + y_n)e_n$$

и тем самым

$$f(x + y) = (x_1 + y_1)e'_1 + (x_2 + y_2)e'_2 + \ldots + (x_n + y_n)e'_n.$$

Следовательно,

$$f(x + y) = f(x) + f(y).$$

Аналогично доказывается, что

$$f(k\boldsymbol{x}) = kf(\boldsymbol{x}),$$

где k — любое действительное число. Итак, условия (6) и (7) определения изоморфизма выполнены.

Если теперь учесть, что базис (9) ортонормированный, то получим:

$$(\boldsymbol{x},\ \boldsymbol{y}) = x_1y_1 + x_2y_2 + \ldots + x_ny_n.$$

Но базис (9′) также ортонормированный, поэтому

$$(f(\boldsymbol{x}),\ f(\boldsymbol{y})) = x_1y_1 + x_2y_2 + \ldots + x_ny_n.$$

Следовательно,

$$(\boldsymbol{x},\ \boldsymbol{y}) = (f(\boldsymbol{x}),\ f(\boldsymbol{y})),$$

т. е. выполнено условие (8) определения изоморфизма. Теорема доказана.

С принятой в алгебре точки зрения (две изоморфные системы рассматриваются как тождественные, неразличимые) можно теперь считать, что существует *только одно* евклидово пространство данной размерности n. Это пространство обозначается дальше E^n.

Вопросы и упражнения

1. Пусть в ортогональной системе $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \ldots, \boldsymbol{a}_p$ $(p \geqslant 2)$ векторы $\boldsymbol{a}_1, \boldsymbol{a}_2$ имеют равные длины. Показать, что система $\boldsymbol{a}_1', \boldsymbol{a}_2', \boldsymbol{a}_3, \ldots, \boldsymbol{a}_p$, в которой $\boldsymbol{a}_1' = \boldsymbol{a}_1 + \boldsymbol{a}_2$, $\boldsymbol{a}_2' = \boldsymbol{a}_1 - \boldsymbol{a}_2$, также будет ортогональной.

2. Пусть векторы $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \ldots, \boldsymbol{a}_n$ $(n \geqslant 2)$ образуют ортонормированный базис. Заменим в этом базисе векторы $\boldsymbol{a}_1$ и $\boldsymbol{a}_2$ векторами

$$\boldsymbol{a}_1' = \boldsymbol{a}_1 \cos\alpha - \boldsymbol{a}_2 \sin\alpha,\quad \boldsymbol{a}_2' = \boldsymbol{a}_1 \sin\alpha + \boldsymbol{a}_2 \cos\alpha,$$

где α — любое число. Убедиться, что векторы $\boldsymbol{a}_1', \boldsymbol{a}_2', \boldsymbol{a}_3, \ldots, \boldsymbol{a}_n$ снова образуют ортонормированный базис.

3. Показать, что если векторы $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_{n-1}$ образуют в пространстве E^n линейно независимую систему, то существует только два вектора длины 1, ортогональных всем векторам этой системы.

§ 3. Ортогональное дополнение к подпространству. Процесс ортогонализации

1. Ортогональное дополнение к подпространству. Пусть K — подпространство евклидова пространства E^n. Будем говорить, что *вектор* $\boldsymbol{a}$ *ортогонален* K (и писать $\boldsymbol{a} \perp K$), если он ортогонален каждому вектору из K.

Совокупность всех векторов, ортогональных K, называется *ортогональным дополнением* K и обозначается $K^\perp$.

Покажем, что $K^\perp$ есть подпространство пространства E^n.

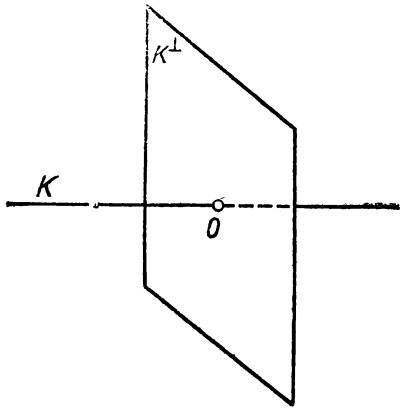

Рис. 13

В самом деле, допустим, что векторы $\boldsymbol{a}$ и $\boldsymbol{b}$ принадлежат $K^\perp$, т. е.

$$(\boldsymbol{a}, \boldsymbol{x}) = 0, \ (\boldsymbol{b}, \boldsymbol{x}) = 0 \text{ для всех } \boldsymbol{x} \in K.$$

Складывая эти равенства, получим:

$$(\boldsymbol{a} + \boldsymbol{b}, \boldsymbol{x}) = 0,$$

а умножая первое из них на произвольное число k, будем иметь:

$$(k\boldsymbol{a}, \boldsymbol{x}) = 0.$$

Это означает, что векторы $\boldsymbol{a} + \boldsymbol{b}$ и $k\boldsymbol{a}$ также принадлежат $K^\perp$. Следовательно, $K^\perp$ есть подпространство.

Пусть, например, K есть одномерное подпространство трехмерного векторного пространства. Оно изображается некоторой прямой, проходящей через начало координат (рис. 13). Ортогональное дополнение K представляет собой совокупность векторов, перпендикулярных данной прямой, поэтому $K^\perp$ изображается плоскостью, перпендикулярной данной прямой.

Нетрудно видеть, что

$$K \cap K^\perp = \{0\},$$

т. е. пересечение подпространства K с его ортогональным дополнением содержит только нулевой вектор. Действительно, если $\boldsymbol{a} \in K$ и в то же время $\boldsymbol{a} \in K^\perp$, то $(\boldsymbol{a}, \boldsymbol{a}) = 0$ и, следовательно, $\boldsymbol{a} = \boldsymbol{0}$.

Докажем теперь следующую теорему.

Теорема. *Пространство E^n есть прямая сумма любого подпространства K и его ортогонального дополнения $K^\perp$.*

Доказательство. Мы должны показать, что, во-первых, $K \cap K^\perp = \{0\}$ и, во-вторых, сумма $K + K^\perp$ совпадает с E^n. Но первое уже доказано. Поэтому остается лишь проверить, что любой вектор $\boldsymbol{v} \in E^n$ представляется в виде

$$\boldsymbol{v} = \boldsymbol{a} + \boldsymbol{b}, \text{ где } \boldsymbol{a} \in K, \ \boldsymbol{b} \in K^\perp. \tag{1}$$

Выберем в подпространстве K какой-нибудь ортогональный базис

$$\boldsymbol{a}_1, \ \boldsymbol{a}_2, \ldots, \ \boldsymbol{a}_p \tag{2}$$

Нам необходимо найти такой вектор $\boldsymbol{a} \in K$, чтобы разность $\boldsymbol{v} - \boldsymbol{a}$ была ортогональна K; тогда, обозначив эту разность через $\boldsymbol{b}$, получим искомое разложение (1).

Запишем искомый вектор $\boldsymbol{a}$ в виде

$$\boldsymbol{a} = \alpha_1 \boldsymbol{a}_1 + \alpha_2 \boldsymbol{a}_2 + \ldots + \alpha_p \boldsymbol{a}_p.$$

Числа $\alpha_1, \alpha_2, \ldots, \alpha_p$ должны быть такими, чтобы вектор

$$\boldsymbol{v} - \boldsymbol{a} = \boldsymbol{v} - \alpha_1 \boldsymbol{a}_1 - \alpha_2 \boldsymbol{a}_2 - \ldots - \alpha_p \boldsymbol{a}_p$$

был ортогонален K. Для этого необходимо и достаточно, чтобы указанный вектор был ортогонален каждому из векторов $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_p$, т. е. чтобы выполнялись равенства:

$$\begin{aligned}
&(\boldsymbol{v}, \boldsymbol{a}_1) - \alpha_1 (\boldsymbol{a}_1, \boldsymbol{a}_1) - \alpha_2 (\boldsymbol{a}_2, \boldsymbol{a}_1) - \ldots - \alpha_p (\boldsymbol{a}_p, \boldsymbol{a}_1) = 0,\\
&(\boldsymbol{v}, \boldsymbol{a}_2) - \alpha_1 (\boldsymbol{a}_1, \boldsymbol{a}_2) - \alpha_2 (\boldsymbol{a}_2, \boldsymbol{a}_2) - \ldots - \alpha_p (\boldsymbol{a}_p, \boldsymbol{a}_2) = 0,\\
&\quad\ldots\quad\ldots\quad\ldots\quad\ldots\quad\ldots\\
&(\boldsymbol{v}, \boldsymbol{a}_p) - \alpha_1 (\boldsymbol{a}_1, \boldsymbol{a}_p) - \alpha_2 (\boldsymbol{a}_2, \boldsymbol{a}_p) - \ldots - \alpha_p (\boldsymbol{a}_p, \boldsymbol{a}_p) = 0.
\end{aligned}$$

Ввиду ортогональности системы (2) эти равенства принимают вид:

$$\begin{aligned}
&(\boldsymbol{v}, \boldsymbol{a}_1) = \alpha_1 (\boldsymbol{a}_1, \boldsymbol{a}_1),\\
&(\boldsymbol{v}, \boldsymbol{a}_2) = \alpha_2 (\boldsymbol{a}_2, \boldsymbol{a}_2),\\
&\quad\ldots\quad\ldots\quad\ldots\\
&(\boldsymbol{v}, \boldsymbol{a}_p) = \alpha_p (\boldsymbol{a}_p, \boldsymbol{a}_p).
\end{aligned}$$

Отсюда однозначно определяются числа $\alpha_1, \alpha_2, \ldots, \alpha_p$, а вслед за ними и вектор $\boldsymbol{a}$:

$$\boldsymbol{a} = \frac{(\boldsymbol{v}, \boldsymbol{a}_1)}{(\boldsymbol{a}_1, \boldsymbol{a}_1)} \boldsymbol{a}_1 + \frac{(\boldsymbol{v}, \boldsymbol{a}_2)}{(\boldsymbol{a}_2, \boldsymbol{a}_2)} \boldsymbol{a}_2 + \ldots + \frac{(\boldsymbol{v}, \boldsymbol{a}_p)}{(\boldsymbol{a}_p, \boldsymbol{a}_p)} \boldsymbol{a}_p. \tag{3}$$

После того как найден вектор $\boldsymbol{a}$, полагаем: $\boldsymbol{b} = \boldsymbol{v} - \boldsymbol{a}$. Теорема доказана.

Следует еще сказать, что представление любого вектора $\boldsymbol{v} \in E^n$ в виде (1) возможно лишь *единственным* образом. Этот факт мы установили попутно, показав, что вектор $\boldsymbol{a}$ должен определяться формулой (3). Впрочем, единственность представления (1) вытекает также из общих свойств прямой суммы.

Заметим, что вектор $\boldsymbol{a}$ называется *ортогональной проекцией* вектора $\boldsymbol{v}$ на подпространство K и обозначается

$$\text{пр}_K \boldsymbol{v},$$

а вектор $\boldsymbol{b}$ — *ортогональной составляющей* $\boldsymbol{v}$ относительно K. Еще раз укажем выражение для вектора $\boldsymbol{a}$:

$$\boldsymbol{a} = \text{пр}_K \boldsymbol{v} = \frac{(\boldsymbol{v}, \boldsymbol{a}_1)}{(\boldsymbol{a}_1, \boldsymbol{a}_1)} \boldsymbol{a}_1 + \frac{(\boldsymbol{v}, \boldsymbol{a}_2)}{(\boldsymbol{a}_2, \boldsymbol{a}_2)} \boldsymbol{a}_2 + \ldots + \frac{(\boldsymbol{v}, \boldsymbol{a}_p)}{(\boldsymbol{a}_p, \boldsymbol{a}_p)} \boldsymbol{a}_p, \tag{3}$$

где $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_p$ — любой ортогональный базис подпространства K.

На рис. 14 представлено разложение вектора $\boldsymbol{v}$ на ортогональную проекцию и ортогональную составляющую для случая, когда

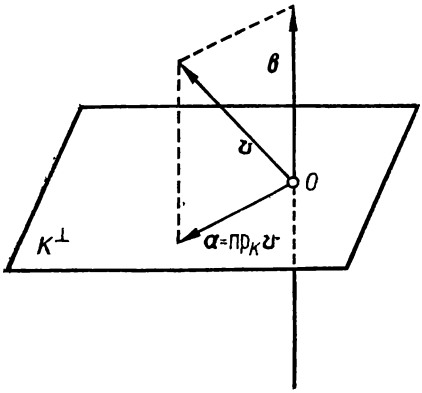

Рис. 14

K — одномерное подпространство трехмерного векторного пространства.

2. **Процесс ортогонализации.** Формула (3) показывает, что нахождение ортогональной проекции вектора $\boldsymbol{v}$ на подпространство K представляет собой весьма простую задачу, если известен какой-нибудь ортогональный базис в K. В принципе для построения ортогонального базиса можно воспользоваться методом, изложенным в пункте 2 предыдущего параграфа. Однако в практическом отношении более удобным является другой метод, носящий название *процесса ортогонализации* и позволяющий непосредственно вычислить искомый ортогональный базис

$$\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ \ldots,\ \boldsymbol{a}_p \tag{4}$$

подпространства K, лишь только известен *какой-нибудь* базис

$$\boldsymbol{b}_1,\ \boldsymbol{b}_2,\ \ldots,\ \boldsymbol{b}_p \tag{5}$$

этого подпространства.

Приведем описание этого метода. Подпространство, натянутое на первые i векторов системы (5), обозначим через K_i (очевидно, размерность K_i равна i, причем K_p есть все K). Искомые векторы $\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ldots,\ \boldsymbol{a}_p$ будем строить так, чтобы

$$\begin{aligned}
&\boldsymbol{a}_1 \in K_1,\\
&\boldsymbol{a}_2 \in K_2,\ \text{причем } \boldsymbol{a}_2 \perp K_1,\\
&\boldsymbol{a}_3 \in K_3,\ \text{причем } \boldsymbol{a}_3 \perp K_2,\\
&\quad\ldots\qquad\qquad\ldots\\
&\boldsymbol{a}_p \in K_p,\ \text{причем } \boldsymbol{a}_p \perp K_{p-1}.
\end{aligned}$$

Для этой цели положим:

$$\left.\begin{aligned}
\boldsymbol{a}_1 &= \boldsymbol{b}_1,\\
\boldsymbol{a}_2 &= \boldsymbol{b}_2 - \mathrm{пр}_{K_1}\boldsymbol{b}_2,\\
\boldsymbol{a}_3 &= \boldsymbol{b}_3 - \mathrm{пр}_{K_2}\boldsymbol{b}_3,\\
&\ldots\qquad\ldots\\
\boldsymbol{a}_p &= \boldsymbol{b}_p - \mathrm{пр}_{K_{p-1}}\boldsymbol{b}_p.
\end{aligned}\right\} \tag{6}$$

Так как в формуле $\boldsymbol{a}_i = \boldsymbol{b}_i - \mathrm{пр}_{K_{i-1}}\boldsymbol{b}_i$ оба слагаемых правой части принадлежат K_i (второе даже принадлежит K_{i-1}), то $\boldsymbol{a}_i \in K_i$; так как при этом $\boldsymbol{a}_i$ есть ортогональная составляющая $\boldsymbol{b}_i$ относительно K_{i-1}, то $\boldsymbol{a}_i \perp K_{i-1}$. Учитывая, что

$$\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ \ldots,\ \boldsymbol{a}_{i-1} \in K_{i-1} \text{ и } \boldsymbol{a}_i \perp K_{i-1},$$

мы видим, что вектор $\boldsymbol{a}_i$ ортогонален каждому из векторов $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_{i-1}$. Очевидно, это означает, что построенная система $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_p$ является ортогональной. Заметим еще, что каждый из векторов $\boldsymbol{a}_i$ отличен от $\mathbf{0}$: для $\boldsymbol{a}_1$ это очевидно, что же касается $\boldsymbol{a}_i$ при $i > 1$, то равенство $\boldsymbol{a}_i = \mathbf{0}$ означало бы, что $\boldsymbol{b}_i = \text{пр}_{K_{i-1}}\boldsymbol{b}_i$ и, следовательно, $\boldsymbol{b}_i \in K_{i-1}$, что невозможно.

Итак, в подпространстве K_p мы построили систему из ненулевых попарно ортогональных векторов $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_p$. Так как размерность K_p равна p, то построенная система является искомым ортогональным базисом в K_p.

Остается еще сказать, что нахождение векторов $\boldsymbol{a}_1$, $\boldsymbol{a}_2$,..., $\boldsymbol{a}_p$ по формулам (6) практически не является сложной задачей. Действительно, используя формулу (3) для проекции вектора на подпространство, мы можем записать (при $i > 1$):

$$\boldsymbol{a}_i = \boldsymbol{b}_i - \frac{(\boldsymbol{b}_i, \boldsymbol{a}_1)}{(\boldsymbol{a}_1, \boldsymbol{a}_1)}\boldsymbol{a}_1 - \frac{(\boldsymbol{b}_i, \boldsymbol{a}_2)}{(\boldsymbol{a}_2, \boldsymbol{a}_2)}\boldsymbol{a}_2 - \ldots - \frac{(\boldsymbol{b}_i, \boldsymbol{a}_{i-1})}{(\boldsymbol{a}_{i-1}, \boldsymbol{a}_{i-1})}\boldsymbol{a}_{i-1}.$$

Это равенство позволяет, если уже построены векторы $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_{i-1}$, найти очередной вектор $\boldsymbol{a}_i$.

Рассмотрим теперь некоторые задачи. Условимся предварительно о следующем: в приводимых ниже задачах запись

$$\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$$

будет означать, что числа a_1, a_2, ..., a_n являются координатами вектора $\boldsymbol{a}$ в некотором фиксированном *ортонормированном* базисе. Поэтому если $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ и $\boldsymbol{b} = (b_1, b_2, \ldots, b_n)$, то

$$(\boldsymbol{a}, \boldsymbol{b}) = a_1b_1 + a_2b_2 + \ldots + a_nb_n. \tag{7}$$

Задача 1. Методом ортогонализации построить ортогональный базис подпространства, порожденного векторами:

$$\boldsymbol{b}_1 = (2, -2, -2, 2),$$
$$\boldsymbol{b}_2 = (3, -1, -1, 3),$$
$$\boldsymbol{b}_3 = (2, -2, 0, 4).$$

Решение. Прежде всего отметим, что нет необходимости специально проверять, будут ли векторы $\boldsymbol{b}_1$, $\boldsymbol{b}_2$, $\boldsymbol{b}_3$ линейно независимы. Эта проверка осуществится сама собой, поскольку все три вектора $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, $\boldsymbol{a}_3$, которые мы получим в процессе ортогонализации, окажутся не равными $\mathbf{0}$.

Методом ортогонализации находим последовательно:

$$\boldsymbol{a}_1 = \boldsymbol{b}_1 = (2, -2, -2, 2),$$
$$\boldsymbol{a}_2 = \boldsymbol{b}_2 - \frac{(\boldsymbol{b}_2, \boldsymbol{a}_1)}{(\boldsymbol{a}_1, \boldsymbol{a}_1)}\boldsymbol{a}_1 = \boldsymbol{b}_2 - \frac{16}{16}\boldsymbol{a}_1 = (1, 1, 1, 1),$$
$$\boldsymbol{a}_3 = \boldsymbol{b}_3 - \frac{(\boldsymbol{b}_3, \boldsymbol{a}_1)}{(\boldsymbol{a}_1, \boldsymbol{a}_1)}\boldsymbol{a}_1 - \frac{(\boldsymbol{b}_3, \boldsymbol{a}_2)}{(\boldsymbol{a}_2, \boldsymbol{a}_2)} = \boldsymbol{b}_3 - \frac{16}{16}\boldsymbol{a}_1 - \frac{4}{4}\boldsymbol{a}_2 = (-1, -1, 1, 1).$$

Для вычисления скалярных произведений мы пользовались, конечно, формулой (7), например:

$$(\boldsymbol{b}_3,\ \boldsymbol{a}_1) = 2 \cdot 2 + (-2) \cdot (-2) + 0 \cdot (-2) + 4 \cdot 2 = 16.$$

Задача 2. Подпространство K состоит из векторов $\boldsymbol{x} = (x_1, x_2, x_3, x_4)$, координаты которых удовлетворяют системе уравнений:

$$\left.\begin{aligned} 3x_1 - x_2 - x_3 + x_4 &= 0, \\ x_1 + 2x_2 - x_3 - x_4 &= 0. \end{aligned}\right\}$$

Построить ортогональный базис подпространства K, а также найти для вектора

$$\boldsymbol{v} = (8,\ -5,\ 7,\ -10)$$

его ортогональную проекцию на K.

Решение. Решая данную систему, находим:

$$x_3 = \frac{1}{2} x_2 + 2x_1,$$
$$x_4 = \frac{3}{2} x_2 - x_1.$$

Отсюда получаем один из фундаментальных наборов решений (один из базисов K):

$$\boldsymbol{b}_1 = (1,\ 0,\ 2,\ -1),$$
$$\boldsymbol{b}_2 = (0,\ 2,\ 1,\ 3).$$

Ортогонализируем систему векторов $\boldsymbol{b}_1$, $\boldsymbol{b}_2$:

$$\boldsymbol{a}_1 = \boldsymbol{b}_1 = (1,\ 0,\ 2,\ -1),$$
$$\boldsymbol{a}_2 = \boldsymbol{b}_2 - \frac{(\boldsymbol{b}_2,\ \boldsymbol{a}_1)}{(\boldsymbol{a}_1,\ \boldsymbol{a}_1)} \boldsymbol{a}_1 = \boldsymbol{b}_2 - \frac{(-1)}{6} \boldsymbol{b}_1 = \left(\frac{1}{6},\ 2,\ \frac{4}{3},\ \frac{17}{6}\right) =$$
$$= \frac{1}{6}(1,\ 12,\ 8,\ 17).$$

Для нахождения $\text{пр}_K \boldsymbol{v}$ пользуемся формулой (3):

$$\text{пр}_K \boldsymbol{v} = \frac{(\boldsymbol{v},\ \boldsymbol{a}_1)}{(\boldsymbol{a}_1,\ \boldsymbol{a}_1)} \boldsymbol{a}_1 + \frac{(\boldsymbol{v},\ \boldsymbol{a}_2)}{(\boldsymbol{a}_2,\ \boldsymbol{a}_2)} \boldsymbol{a}_2 = \frac{32}{6} \boldsymbol{a}_1 + \frac{\frac{1}{6}(-166)}{\frac{1}{36} \cdot 498} \boldsymbol{a}_2 =$$
$$= (5,\ -4,\ 8,\ -11).$$

Задача 3. Найти ортогональную проекцию вектора

$$\boldsymbol{v} = (5,\ 2,\ -2,\ 2)$$

на подпространство K, порожденное векторами:

$$\boldsymbol{b}_1 = (2,\ 1,\ 1,\ -1),$$
$$\boldsymbol{b}_2 = (1,\ 1,\ 3,\ 0).$$

Р е ш е н и е. Искомую проекцию можно было бы спределить тем же методом, что и в предыдущей задаче. Мы, однако, будем исходить непосредственно из определения ортогональной проекции на подпространство. Наша цель — найти такой вектор $\boldsymbol{a} \in K$:

$$\boldsymbol{a} = \beta_1 \boldsymbol{b}_1 + \beta_2 \boldsymbol{b}_2,$$

чтобы разность $\boldsymbol{v} - \boldsymbol{a}$ была ортогональна векторам $\boldsymbol{b}_1$, $\boldsymbol{b}_2$, т. е. чтобы было

$$(\boldsymbol{v}, \boldsymbol{b}_1) - \beta_1 (\boldsymbol{b}_1, \boldsymbol{b}_1) - \beta_2 (\boldsymbol{b}_2, \boldsymbol{b}_1) = 0,$$
$$(\boldsymbol{v}, \boldsymbol{b}_2) - \beta_1 (\boldsymbol{b}_1, \boldsymbol{b}_2) - \beta_2 (\boldsymbol{b}_2, \boldsymbol{b}_2) = 0.$$

Вычисляя все скалярные произведения, приходим к таким соотношениям:

$$8 - 7\beta_1 - 6\beta_2 = 0,$$
$$1 - 6\beta_1 - 11\beta_2 = 0.$$

Это система двух уравнений с двумя неизвестными β_1, β_2. Решая ее, находим:

$$\beta_1 = 2, \quad \beta_2 = -1.$$

Следовательно,

$$\boldsymbol{a} = \text{пр}_K \boldsymbol{v} = 2\boldsymbol{b}_1 - \boldsymbol{b}_2 = (3, 1, -1, -2).$$

З а д а ч а 4. Найти ортогональное дополнение $K^\perp$ к подпространству K, порожденному векторами:

$$\boldsymbol{a}_1 = (1, 1, 0, -3, -1),$$
$$\boldsymbol{a}_2 = (1, -1, 2, -1, 0).$$

Р е ш е н и е. Вектор

$$\boldsymbol{x} = (x_1, x_2, x_3, x_4, x_5)$$

принадлежит подпространству $K^\perp$ в том и только в том случае, если $(\boldsymbol{x}, \boldsymbol{a}_1) = 0$ и $(\boldsymbol{x}, \boldsymbol{a}_2) = 0$, т. е.

$$1 \cdot x_1 + 1 \cdot x_2 + 0 \cdot x_3 + (-3) \cdot x_4 + (-1) \cdot x_5 = 0,$$
$$1 \cdot x_1 + (-1) \cdot x_2 + 2 \cdot x_3 + (-1) \cdot x_4 + 0 \cdot x_5 = 0.$$

Решая полученную систему уравнений, находим:

$$x_1 = -x_3 + 2x_4 + \frac{1}{2} x_5,$$

$$x_2 = x_3 + x_4 + \frac{1}{2} x_5.$$

В качестве базиса $K^\perp$ можно взять любой фундаментальный набор решений, например:

$$\boldsymbol{b}_1 = (-1, 1, 1, 0, 0),$$
$$\boldsymbol{b}_2 = (2, 1, 0, 1, 0),$$
$$\boldsymbol{b}_3 = \left(\frac{1}{2}, \frac{1}{2}, 0, 0, 1\right).$$

Задача 5. Найти ортогональное дополнение к подпространству K, заданному однородной системой уравнений:

$$\left.\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= 0, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= 0, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= 0. \end{aligned}\right\} \tag{8}$$

Решение. Положим:

$$\begin{aligned} \boldsymbol{a}_1 &= (a_{11}, \ a_{12}, \ \ldots, \ a_{1n}), \\ \boldsymbol{a}_2 &= (a_{21}, \ a_{22}, \ \ldots, \ a_{2n}), \\ &\cdot \qquad\qquad \cdot \\ \boldsymbol{a}_m &= (a_{m1}, \ a_{m2}, \ \ldots, \ a_{mn}), \end{aligned}$$

а также

$$\boldsymbol{a} = (x_1, \ x_2, \ \ldots, \ x_n).$$

Тогда система (8) перепишется следующим образом:

$$\left.\begin{aligned} (\boldsymbol{x}, \ \boldsymbol{a}_1) &= 0, \\ (\boldsymbol{x}, \ \boldsymbol{a}_2) &= 0, \\ \cdot \quad \cdot \quad \cdot \\ (\boldsymbol{x}, \ \boldsymbol{a}_m) &= 0. \end{aligned}\right\}$$

Эти соотношения показывают, что векторы $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_m$ ортогональны любому вектору $\boldsymbol{x} \in K$. Следовательно, эти векторы принадлежат $K^\perp$. Покажем, что $K^\perp$ есть в точности линейная оболочка векторов $\boldsymbol{a}_1$, $\boldsymbol{a}_2$,..., $\boldsymbol{a}_m$.

В самом деле, пусть вектор

$$\boldsymbol{a} = (a_1, \ a_2, \ldots, \ a_n)$$

принадлежит $K^\perp$. Это значит, что он ортогонален любому вектору $\boldsymbol{x} \in K$, т. е.

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0, \tag{9}$$

каково бы ни было решение $(x_1, \ x_2, \ \ldots, \ x_n)$ системы (8). Отсюда вытекает, что уравнение (9) является следствием системы (8). Но известно (см.: Алгебра, ч. 1, с. 55—56), что любое уравнение, являющееся следствием совместной системы, представимо в виде линейной комбинации уравнений этой системы. Поэтому вектор $\boldsymbol{a}$ является линейной комбинацией векторов $\boldsymbol{a}_1$, $\boldsymbol{a}_2$,... $\boldsymbol{a}_m$, что и доказывает принадлежность $\boldsymbol{a}$ линейной оболочке векторов $\boldsymbol{a}_1$, $\boldsymbol{a}_2$,... ..., $\boldsymbol{a}_n$.

Вопросы и упражнения

1. Условимся называть подпространства K_1 и K_2 *ортогональными* (друг другу), если каждый вектор из K_1 ортогонален каждому

вектору из K_2. Доказать, что если K_1 и K_2 ортогональны, то $K_1 \cap K_2 = \{0\}$.

2. Доказать теорему пункта 1 другим способом, дополнив систему (2) некоторыми векторами $\boldsymbol{a}_{p+1}$, $\boldsymbol{a}_{p+2}, \ldots$, $\boldsymbol{a}_n$, до ортогонального базиса пространства E^n и показав, что подпространство $K^\perp$ порождается векторами $\boldsymbol{a}_{p+1}$, $\boldsymbol{a}_{p+2}, \ldots$, $\boldsymbol{a}_n$.

3. Показать, что ортогональная проекция каждого вектора векторного многообразия $\boldsymbol{a}_0 + K$ на пространство $K^\perp$ совпадает с ортогональной проекцией на $K^\perp$ вектора a_0.

Глава IV

ЛИНЕЙНЫЕ ОТОБРАЖЕНИЯ

§ 1. Понятие линейного отображения. Связь между линейными отображениями и матрицами

1. Определение линейного отображения. Примеры. Центральным понятием этой главы является понятие линейного отображения.

Определение. Пусть L и L' — два векторных пространства над полем P. Отображение φ пространства L в пространство L' называется *линейным*, если оно удовлетворяет следующим условиям:

1. $\varphi(\boldsymbol{x}_1 + \boldsymbol{x}_2) = \varphi(\boldsymbol{x}_1) + \varphi(\boldsymbol{x}_2)$,
2. $\varphi(k\boldsymbol{x}) = k\varphi(\boldsymbol{x})$,

где $\boldsymbol{x}_1$, $\boldsymbol{x}_2$ и $\boldsymbol{x}$ — любые векторы из L и k — любое число из P.

Условие 1 данного определения является условием сохранения операции сложения. Но, как мы знаем, пространства L и L' представляют собой *группы* относительно операции сложения. Следовательно, линейное отображение является, в частности, *гомоморфизмом* группы L в группу L'.

Выше было сказано (см. с. 74 и 85), что векторное пространство над каким-либо полем можно считать системой с одной двухместной операцией (сложением) и множеством одноместных операций, соответствующих всевозможным числам из данного поля, а условие 2 — условием сохранения всех одноместных операций. Рассматривая пространства L и L' как системы с указанными операциями, мы получаем, что условия 1 и 2 означают сохранение *всех* этих операций при отображении φ. Таким образом, линейное отображение оказывается просто *гомоморфизмом* системы L в систему L'.

Из условий 1 и 2 легко следует, что действие линейного отображения φ на линейную комбинацию нескольких векторов подчиняется формуле

$$\varphi(k_1\boldsymbol{x}_1 + k_2\boldsymbol{x}_2 + \cdots + k_p\boldsymbol{x}_p) = \\ = k_1\varphi(\boldsymbol{x}_1) + k_2\varphi(\boldsymbol{x}_2) + \cdots + k_p\varphi(\boldsymbol{x}_p),$$

а также что нулевой вектор пространства L переходит при линейном отображении в нулевой вектор пространства L':

$$\varphi(\mathbf{0}) = \mathbf{0}'.$$

Приведем некоторые примеры линейных отображений.

1. Пусть L и L' — какие-то векторные пространства. Отображение φ, которое каждый вектор $\boldsymbol{x}$ из L переводит в нулевой вектор из L':

$$\varphi(\boldsymbol{x}) = \mathbf{0}' \quad (\boldsymbol{x} \in L),$$

будет, очевидно, линейным. Оно называется *нулевым отображением* L в L'. В частности, можно говорить о нулевом отображении пространства L в себя.

2. Тождественное отображение пространства L в себя, т. е. отображение, заданное формулой

$$\varphi(\boldsymbol{x}) = \boldsymbol{x} \quad (\boldsymbol{x} \in L),$$

является линейным.

3. Пусть L — n-мерное векторное пространство с базисом $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ и $\boldsymbol{b}$ — фиксированный вектор из векторного пространства L'. Разлагая произвольный вектор $\boldsymbol{x} \in L$ по векторам базиса:

$$\boldsymbol{x} = x_1\boldsymbol{a}_1 + x_2\boldsymbol{a}_2 + \cdots + x_n\boldsymbol{a}_n,$$

положим:

$$\varphi(\boldsymbol{x}) = x_1\boldsymbol{b}.$$

Мы получили отображение φ пространства L в пространство L', которое, как легко проверить, будет линейным.

4. Пусть L — конечномерное векторное пространство и

$$L = L_1 + L_2$$

— разложение L в прямую сумму двух подпространств L_1 и L_2. Каждый вектор $\boldsymbol{x} \in L$ допускает единственное представление в виде

$$\boldsymbol{x} = \boldsymbol{x}_1 + \boldsymbol{x}_2,$$

где $\boldsymbol{x}_1 \in L_1$ $\boldsymbol{x} \in L_2$. Определим отображение φ пространства L в себя формулой

$$\varphi(\boldsymbol{x}) = \boldsymbol{x}_1.$$

Проверка условий 1 и 2 показывает, что это отображение будет линейным. Оно называется *отображением проектирования на подпространство* L_1 (при данном выборе подпространств L_1 и L_2).

5. Множество всех матриц типа (m, n) (m строк и n столбцов) с элементами из поля P является линейным пространством над P относительно операций сложения матриц и умножения матриц на числа из P. Обозначим это пространство $L_{m,n}$. Поставим в соответствие каждой матрице $A \in L_{m,n}$ транспонированную к ней матрицу A' (имеющую n строк и m столбцов). Мы получим отображение пространства $L_{m,n}$ в $L_{n,m}$, которое будет линейным, так как

$$(A + B)' = A' + B' \text{ и } (kA)' = kA'.$$

6. Рассмотрим пространство всех многочленов от одной переменной x и определим операции сложения многочленов и умножения их на действительные числа обычным образом. Поставив в соответствие каждому многочлену его производную, мы получим, очевидно, линейное отображение пространства многочленов в себя. Это пространство является подпространством пространства всех функций действительной переменной x (см. пример 3 на с. 74).

Данный пример можно обобщить, заменяя многочлены произвольными функциями, бесконечно дифференцируемыми на всей числовой оси.

2. Запись линейного отображения в координатах. Матрица линейного отображения. Начиная с этого пункта, мы будем предполагать, что оба пространства L и L', фигурирующие в определении линейного отображения, являются конечномерными. Это предположение позволяет свести изучение линейных отображений к изучению матриц.

Пусть n и m — размерности пространств L и L' соответственно:

$$\dim L = n, \ \dim L' = m.$$

Выберем какие-нибудь базисы: базис

$$\boldsymbol{a}_1, \ \boldsymbol{a}_2, \ \ldots, \ \boldsymbol{a}_n \tag{1}$$

в пространстве L и базис

$$\boldsymbol{b}_1, \ \boldsymbol{b}_2, \ \ldots, \ \boldsymbol{b}_m \tag{2}$$

в пространстве L'. Пусть φ — линейное отображение L в L'. Рассмотрим произвольный вектор $\boldsymbol{x}$ из L и его образ $\boldsymbol{y} = \varphi(\boldsymbol{x})$ при отображении φ ($\boldsymbol{y} \in L'$). Разложим векторы $\boldsymbol{x}$ и $\boldsymbol{y}$ по базисам (1) и (2) соответственно:

$$\boldsymbol{x} = x_1\boldsymbol{a}_1 + x_2\boldsymbol{a}_2 + \cdots + x_n\boldsymbol{a}_n, \tag{3}$$

$$\boldsymbol{y} = y_1\boldsymbol{b}_1 + y_2\boldsymbol{b}_2 + \cdots + y_m\boldsymbol{b}_m. \tag{4}$$

Наша цель — найти выражения для $y_1, y_2, \ldots, y_m$ через $x_1, x_2, \ldots, x_m$.

В силу линейности отображения φ из равенства (3) следует равенство

$$\boldsymbol{y} = \varphi(\boldsymbol{x}) = x_1\varphi(\boldsymbol{a}_1) + x_2\varphi(\boldsymbol{a}_2) + \cdots + x_n\varphi(\boldsymbol{a}_n). \tag{5}$$

Векторы

$$\varphi(\boldsymbol{a}_1), \ \varphi(\boldsymbol{a}_2), \ \ldots, \ \varphi(\boldsymbol{a}_n)$$

представляют собой элементы пространства L'; поэтому каждый из них может быть разложен по базису $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_m$.

Запишем эти разложения в следующем виде:

$$\begin{aligned}
\varphi(\boldsymbol{a}_1) &= \alpha_{11}\boldsymbol{b}_1 + \alpha_{21}\boldsymbol{b}_2 + \cdots + \alpha_{m1}\boldsymbol{b}_m,\\
\varphi(\boldsymbol{a}_2) &= \alpha_{12}\boldsymbol{b}_1 + \alpha_{22}\boldsymbol{a}_2 + \cdots + \alpha_{m2}\boldsymbol{b}_m,\\
&\cdots\cdots\cdots\cdots\\
\varphi(\boldsymbol{a}_n) &= \alpha_{1n}\boldsymbol{b}_1 + \alpha_{2n}\boldsymbol{b}_2 + \cdots + \varphi_{mn}\boldsymbol{b}_m
\end{aligned} \qquad (6)$$

(обращаем внимание читателя на тот факт, что коэффициенты в разложении вектора $\varphi(\boldsymbol{a}_i)$ обозначены α_{1i}, α_{2i}, ..., α_{mi}, а не α_{i1}, α_{i2}, ..., α_{im}). Если в равенство (5) вместо $\varphi(\boldsymbol{a}_1)$, ..., $\varphi(\boldsymbol{a}_n)$ подставить эти разложения, то получим:

$$\begin{aligned}
\boldsymbol{y} = {} & x_1(\alpha_{11}\boldsymbol{b}_1 + \alpha_{21}\boldsymbol{b}_2 + \cdots + \alpha_{m1}\boldsymbol{b}_m) +\\
& + x_2(\alpha_{12}\boldsymbol{b}_1 + \alpha_{22}\boldsymbol{b}_2 + \cdots + \alpha_{m2}\boldsymbol{b}_m) +\\
& \cdots\cdots\cdots\cdots\\
& + x_n(\alpha_{1n}\boldsymbol{b}_1 + \alpha_{2n}\boldsymbol{b}_2 + \cdots + \alpha_{mn}\boldsymbol{b}_m)
\end{aligned}$$

или, собирая отдельно члены с $\boldsymbol{b}_1$, $\boldsymbol{b}_2$, ..., $\boldsymbol{b}_m$,

$$\begin{aligned}
\boldsymbol{y} = {} & (\alpha_{11}x_1 + \alpha_{12}x_2 + \cdots + \alpha_{1n}x_n)\,\boldsymbol{b}_1 +\\
& + (\alpha_{21}x_1 + \alpha_{22}x_2 + \cdots + \alpha_{2n}x_n)\,\boldsymbol{b}_2 +\\
& \cdots\cdots\cdots\cdots\\
& + (\alpha_{m1}x_1 + \alpha_{m2}x_2 + \cdots + \alpha_{mn}x_n)\boldsymbol{b}_m.
\end{aligned}$$

Сравнивая это представление вектора $\boldsymbol{y}$ с (4) и учитывая единственность разложения по базису, приходим к искомым формулам:

$$\begin{aligned}
y_1 &= \alpha_{11}x_1 + \alpha_{12}x_2 + \cdots + \alpha_{1n}x_n,\\
y_2 &= \alpha_{21}x_1 + \alpha_{22}x_2 + \cdots + \alpha_{2n}x_n,\\
&\cdots\cdots\cdots\\
y_m &= \alpha_{m1}x_1 + \alpha_{m2}x_2 + \cdots + \alpha_{mn}x_n.
\end{aligned} \qquad (7)$$

Заметим, что формулы (7) получены нами из формул (6) (в предположении линейности отображения φ). Но и формулы (6) в свою очередь легко выводятся из формул (7): подставляя в (6) координаты вектора $\boldsymbol{a}_i$ в базисе (1) (т. е. единицу вместо x_i и нуль в остальных случаях), находим, что координатами вектора $\varphi(\boldsymbol{a}_i)$ в базисе (2) будут числа α_{1i}, α_{2i}, ..., α_{mi} и, значит, $\varphi(\boldsymbol{a}_i) = \alpha_{1i}\boldsymbol{b}_1 + \alpha_{2i}\boldsymbol{b}_2 + \cdots + \alpha_{mi}\boldsymbol{b}_m$.

Говорят, что формулы (7) дают *запись линейного отображения в координатах.*

Если ввести теперь в рассмотрение матрицу

$$A = \begin{pmatrix} \alpha_{11}\alpha_{12} \ldots \alpha_{1n} \\ \alpha_{21}\alpha_{22} \ldots \alpha_{2n} \\ \\ \alpha_{m1}\alpha_{m2} \ldots \alpha_{mn} \end{pmatrix},$$

а также матрицы

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \\ \cdot \\ x_n \end{pmatrix}, \quad Y = \begin{pmatrix} y_1 \\ y_2 \\ \\ \cdot \\ y_m \end{pmatrix},$$

то формулы (6) можно записать в виде одного матричного равенства

$$(\varphi(\boldsymbol{a}_1)\,\varphi(\boldsymbol{a}_2)\,\ldots\,\varphi(\boldsymbol{a}_n)) = (\boldsymbol{b}_1\boldsymbol{b}_2\,\ldots\,\boldsymbol{b}_m)\,A, \tag{8}$$

а формулы (7) — в виде матричного равенства

$$Y = AX. \tag{9}$$

Мы показали, следовательно, что *произвольному линейному отображению* φ n-мерного пространства L в m-мерное пространство L' при фиксированных базисах (1) и (2) соответственно в L и L' *отвечает определенная матрица* A из m строк и n столбцов, такая, что координаты любого вектора $x \in L$ в базисе (1) и его образа $\varphi(x) \in L'$ в базисе (2) — связаны равенством (9). При этом для образов векторов базиса (1) и векторов базиса (2) выполняется равенство (8).

Обратно, если задана произвольная матрица A типа (m, n), то существует линейное отображение (пространства L в L'), которому отвечает — в указанном выше смысле — эта матрица. Действительно, определив отображение L в L' формулой (9), легко убеждаемся в его линейности: для координатных столбцов X_1, X_2, X любых трех векторов из L выполняются равенства:

$$A(X_1 + X_2) = AX_1 + AX_2 \text{ и } A(kX) = k(AX).$$

Итак, фиксируя базисы в пространствах L и L', мы получили взаимно однозначное соответствие между множеством всех линейных отображений L в L' и множеством всех матриц типа (m, n): каждому линейному отображению φ отвечает матрица A, для которой одновременно выполняются соотношения (8) и (9). Эта матрица A называется *матрицей линейного отображения* φ (при данном выборе базисов в L и L').

З а д а ч а. Пусть N — фиксированное натуральное число, а L_N и L_{N-1} — пространства всех многочленов с действительными коэффициентами степени не выше N и $N - 1$ соответственно. Пусть в пространстве L_N выбран базис

$$1,\ x,\ x^2,\ \ldots,\ x^N, \tag{10}$$

а в пространстве L_{N-1} — базис

$$1,\ x,\ x^2,\ \ldots,\ x^{N-1}. \tag{11}$$

Отображение L_N в L_{N-1} задано следующим образом: каждому многочлену из L_N ставится в соответствие его производная.

Найти матрицу этого отображения при указанном выборе базисов.

Р е ш е н и е. Нетрудно видеть, что заданное отображение действительно является линейным. Для определения матрицы этого отображения заметим, что многочлен

$$f(x) = a_1 + a_2 x + a_3 x^2 + \cdots + a_{N+1} x^N$$

пространства L_N имеет в базисе (10) координаты

$$a_1,\ a_2,\ a_3,\ \ldots\ ,\ a_{N+1},$$

а его образ

$$f'(x) = a_2 + 2a_3 x + 3a_4 x^2 + \cdots + N a_{N+1} x^{N-1},$$

принадлежащий пространству L_{N-1}, имеет в базисе (11) координаты

$$a_2,\ 2a_3,\ 3a_4,\ \ldots\ ,\ N a_{N+1}.$$

Если координаты образа обозначить через $b_1, b_2, b_3, \ldots, b_N$, то можно, следовательно, записать:

$$\begin{aligned} b_1 &= a_2, \\ b_2 &= 2a_3, \\ b_3 &= 3a_4, \\ &\vdots \\ b_N &= N a_{N+1}. \end{aligned}$$

Значит, искомая матрица отображения имеет следующий вид:

$$\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 2 & \ldots & 0 & 0 \\ \cdot & \cdot & \cdot & & \cdot & \cdot \\ 0 & 0 & 0 & & 0 & N \end{pmatrix}.$$

В этой матрице N строк и $N+1$ столбцов; все элементы ее равны нулю, кроме $\alpha_{12} = 1$, $\alpha_{23} = 2$, ... , $\alpha_{N,\,N+1} = N$.

3. Взаимно однозначные линейные отображения. Мы разберем теперь тот частный случай, когда линейное отображение φ является *взаимно однозначным* отображением пространства L на L'. Согласно определению, данному на с. 84, такое отображение называется *изоморфным*.

Взаимная однозначность отображения должна, естественно, каким-то образом отражаться на матрице этого отображения. Прежде всего заметим, что матрица должна быть квадратной, поскольку размерности изоморфных пространств L и L' совпадают (см. с. 86). Докажем теперь следующее утверждение:

Пусть в пространствах L и L', имеющих одну и ту же размерность n, выбрано по базису. Для того, чтобы квадратная матрица A порядка n определяла (при данном выборе базисов) взаимно одно-

значное отображение L на L', необходимо и достаточно, чтобы матрица A была невырожденной.

Доказательство. Пусть отображение, отвечающее матрице A, взаимно однозначно. Докажем, что матрица A — невырожденная.

Допустим, рассуждая от противного, что матрица A вырожденная. Рассмотрим уравнение

$$AX = 0,$$

которое равносильно (в координатной записи) системе n однородных линейных уравнений с n неизвестными. Из первой части курса (см: Алгебра, ч. 1, с. 152) известно, что такая система при условии вырожденности матрицы A обязательно имеет ненулевое решение. Другими словами, найдется вектор $\boldsymbol{x} \neq 0$, такой, что $\varphi(\boldsymbol{x}) = 0'$. Это противоречит взаимной однозначности отображения φ (два различных вектора 0 и $\boldsymbol{x}$ не могут отображаться в один и тот же вектор $0'$). Следовательно, матрица A невырожденная.

Предположим теперь, что A — невырожденная матрица; покажем тогда, что соответствующее ей отображение φ является взаимно однозначным.

Для этого необходимо проверить, что уравнение

$$\varphi(\boldsymbol{x}) = \boldsymbol{y}$$

при любом фиксированном векторе $\boldsymbol{y} \in L'$ имеет одно и только одно решение $\boldsymbol{x} \in L$, т. е., что матричное уравнение

$$AX = Y$$

однозначно разрешимо при любом Y. Но последнее уравнение в координатной записи равносильно системе из n уравнений с n неизвестными; поэтому для завершения доказательства достаточно заметить, что в силу невырожденности матрицы A указанная система имеет одно и только одно решение.

Взаимно однозначное отображение пространства L на пространство L' называется *невырожденным*. Таким образом, в применении к линейным отображениям термин «невырожденный» означает то же самое, что «изоморфный». Доказанное выше утверждение можно теперь пересказать в следующих словах: *невырожденным линейным отображениям отвечают невырожденные матрицы, и обратно.*

Если линейное отображение φ (пространства L в L') является взаимно однозначным, то для него существует обратное отображение φ^{-1} (пространства L' в L). Это отображение тоже будет линейным, так как отображение, обратное изоморфному, в свою очередь изоморфно. Возникает естественный вопрос: как связаны матрицы отображений φ и φ^{-1}? Ответом на него служит следующее предложение:

Если взаимно однозначному отображению φ при некотором выборе базисов в L и L' отвечает матрица A, то обратному отображению отвечает (при том же выборе базисов) обратная матрица A^{-1}.

Или, выражаясь короче, *обратному отображению отвечает обратная матрица.*

Доказательство весьма просто. Из соотношения (9), учитывая, что матрица A невырожденная и, следовательно, имеет обратную, находим:

$$X = A^{-1}Y.$$

Это соотношение показывает, что матрица отображения φ^{-1} есть A^{-1}.

4. Связь между умножением линейных отображений и умножением матриц. В первой части курса (см.: Алгебра, ч. 1, с. 116) рассматривались операция умножения матриц. Мы покажем сейчас, что эта операция тесно связана с операцией умножения линейных отображений.

Напомним сначала, что понимается под умножением отображений.

Пусть имеются три множества, которые мы обозначим соответственно L, L' и L''. Пусть, далее, заданы два отображения: отображение φ множества L в L' и отображение ψ множества L' в L''.

Тогда можно построить отображение множества L в L'', обозначаемое $\varphi\psi$ и определяемое как результат последовательного выполнения отображений φ и ψ:

$$\varphi\psi(x) = \psi(\varphi(x)) \quad (x \in L) \tag{12}$$

(к элементу x применяется φ, затем к полученному элементу применяется ψ). Отображение $\varphi\psi$ называют при этом произведением отображений φ и ψ.

Допустим, что все три множества L, L', L'' являются векторными пространствами (над некоторым полем P), а заданные отображения φ и ψ— линейными отображениями. Покажем, что тогда и отображение $\varphi\psi$ будет снова *линейным*.

Действительно, каковы бы ни были два вектора $\boldsymbol{x}_1$ и $\boldsymbol{x}_2$ из L, имеем:

$$\varphi\psi(\boldsymbol{x}_1 + \boldsymbol{x}_2) = \psi(\varphi(\boldsymbol{x}_1 + \boldsymbol{x}_2)) = \psi(\varphi(\boldsymbol{x}_1) + \varphi(\boldsymbol{x}_2)) = \\ = \psi(\varphi(\boldsymbol{x}_1)) + \psi(\varphi(\boldsymbol{x}_2));$$

следовательно,

$$\varphi\psi(\boldsymbol{x}_1 + \boldsymbol{x}_2) = \varphi\psi(\boldsymbol{x}_1) + \varphi\psi(\boldsymbol{x}_2).$$

Это равенство показывает, что отображение $\varphi\psi$ удовлетворяет первому условию линейности. Второе условие проверяется столь же просто:

$$\varphi\psi(k\boldsymbol{x}) = \psi(\varphi k\boldsymbol{x})) = \psi(k\varphi(\boldsymbol{x})) = k\psi(\varphi(\boldsymbol{x}))$$

и тем самым

$$\varphi\psi(k\boldsymbol{x}) = k\varphi\psi(\boldsymbol{x}).$$

Итак, отображение $\varphi\psi$ снова линейное.

Обозначим размерности пространств L, L' и L'' соответственно через n, m и k:

$$\dim L = n,\ \dim L' = m,\ \dim L'' = k.$$

Пусть в каждом из пространств L, L', L'' фиксирован некоторый базис, тогда отображению φ будет соответствовать некоторая матрица A типа (m, n), отображению ψ — матрица B типа (k, m) и отображению $\varphi\psi$ — матрица C типа (k, n). Как связаны между собой эти матрицы? Оказывается, что

$$C = BA, \tag{13}$$

т. е. матрица, отвечающая произведению отображений φ и ψ, *равна произведению матрицы отображения* ψ *на матрицу отображения* φ*.

Докажем это предложение. Пусть вектор $\boldsymbol{x}$ при отображении φ переходит в $\boldsymbol{y}$, а вектор $\boldsymbol{y}$ под действием ψ переходит в $\boldsymbol{z}$. Тогда

$$Y = AX \tag{14}$$

и

$$Z = BY, \tag{15}$$

где X, Y и Z — столбцы из координат векторов $\boldsymbol{x}$, $\boldsymbol{y}$ и $\boldsymbol{z}$ соответственно. Подставляя в равенство (15) вместо Y его выражение (14), получим:

$$Z = BAX,$$

откуда видно, что матрица отображения $\varphi\psi$ есть BA. Тем самым формула (13) доказана.

Вопросы и упражнения

1. Почему из линейности отображения φ следует, что $\varphi(\mathbf{0}) = \mathbf{0}'$?

2. Доказать линейность отображений, указанных в примерах 1 — 6 пункта 1.

3. Какая матрица будет отвечать отображению, рассмотренному в примере 5 пункта 1, если базис в каждом из пространств $L_{m,n}$, $L_{n,m}$ выбрать состоящим из матриц, в которых один из элементов равен 1, а остальные 0?

4. Почему в примере 6 пункта 1 многочлены нельзя заменить просто дифференцируемыми функциями?

5. Какие из отображений, рассмотренных в пункте 1, являются взаимно однозначными?

---

* Как уже отмечалось, отображение, получающееся при последовательном выполнении φ и ψ, обозначается $\psi\varphi$ (а не $\varphi\psi$, как у нас) и называется произведением ψ на φ. В этом случае произведению линейных отображений соответствует произведение их матриц *в том же самом*, а не в обратном порядке.

§ 2. Ранг и дефект линейного отображения

1. Ядро и область значений линейного отображения. Пусть φ — линейное отображение пространства L в пространство L'. Рассмотрим какое-нибудь множество M в L. Как и в случае произвольных отображений, *образом* множества M при отображении φ считается совокупность образов всех векторов из M, т. е. множество

$$\{\boldsymbol{y}:\ \boldsymbol{y}=\varphi(\boldsymbol{x}),\ \boldsymbol{x}\in M\}$$

(образ M содержится, очевидно, в L'). Аналогично, если M' множество в L', то его *полным прообразом* при отображении φ называется совокупность прообразов всех векторов из M'; полный прообраз M' есть, следовательно, множество

$$\{\boldsymbol{x}:\varphi(\boldsymbol{x})=\boldsymbol{y},\ \boldsymbol{y}\in M'\},$$

являющееся подмножеством пространства L (если ни один вектор из L не отображается в M', то полный прообраз M' — пустое множество).

Наиболее важным является случай, когда M и M' суть подпространства. Справедлива следующая теорема.

Теорема. *Образ любого подпространства из L при линейном отображении φ есть подпространство в L'. Полный прообраз любого подпространства из L' есть подпространство в L.*

Доказательство. Пусть K — подпространство в L и K' — его образ при отображении φ. Мы должны показать, что K' также является подпространством, т. е. если $\boldsymbol{y}\in K'$ и $\boldsymbol{y}_2\in K'$, то и $\boldsymbol{y}_1+\boldsymbol{y}_2\in K'$, а также если $\boldsymbol{y}\in K'$, то и $k\boldsymbol{y}\in K'$ для любого числа k.

Имеем:

$$\boldsymbol{y}_1=\varphi(\boldsymbol{x}_1),\ \boldsymbol{y}_2=\varphi(\boldsymbol{x}_2),$$

где $\boldsymbol{x}_1$ и $\boldsymbol{x}_2$ — некоторые векторы из K. Но тогда

$$\boldsymbol{y}_1+\boldsymbol{y}_2=\varphi(\boldsymbol{x}_1)+\varphi(\boldsymbol{x}_2)=\varphi(\boldsymbol{x}_1+\boldsymbol{x}_2);$$

следовательно, вектор $\boldsymbol{y}_1+\boldsymbol{y}_2$ тоже принадлежит K'. Далее, если $\boldsymbol{y}\in K'$, то $\boldsymbol{y}=\varphi(\boldsymbol{x})$, где $\boldsymbol{x}\in K$. Но тогда $k\boldsymbol{y}=k\varphi(\boldsymbol{x})=\varphi(k\boldsymbol{x})$, и так как $k\boldsymbol{x}\in K$ (ведь K — подпространство), то $k\boldsymbol{y}\in K'$.

Доказательство того, что полный прообраз любого подпространства из L' есть подпространство в L, проводится столь же просто; мы предоставляем это доказательство читателю.

При изучении линейного отображения L в L' особую роль играют два подпространства: образ всего пространства L (это некоторое подпространство в L') и полный прообраз нулевого подпространства (т. е. нулевого вектора) из L' (это некоторое подпространство в L).

Полный прообраз нулевого вектора называется *ядром* линейного отображения φ и обозначается символом $\ker\varphi$ (от английского слова *kernel* — ядро, сердцевина):

Образ всего пространства L называется *областью значений* данного отображения.

Например, ядро тождественного отображения пространства L есть нулевое подпространство в L, а область значений есть все L. В случае нулевого отображения пространства L в пространство L' ядром является все данное пространство L, а областью значений — нулевое подпространство в L'.

2. Ранг и дефект линейного отображения. С каждым линейным отображением можно связать два целых неотрицательных числа, являющихся важнейшими характеристиками этого отображения — так называемые ранг и дефект отображения.

Дефектом линейного отображения называется размерность его ядра.

Рангом линейного отображения называется размерность его области значений.

Существует простая связь между рангом и дефектом линейного отображения.

Теорема. *Сумма ранга и дефекта линейного отображения пространства L в L' равна размерности пространства L.*

Доказательство. Пусть r — ранг отображения φ и d — его дефект. Нам нужно показать, что

$$n = d + r, \tag{1}$$

где n — размерность пространства L.

Обозначим через A ядро отображения φ и через B' — его область значений. Как мы уже знаем, A является подпространством в L, а B — подпространством в L'.

Выберем в пространстве L подпространство B такое, что L является прямой суммой A и B:

$$L = A + B. \tag{2}$$

Для этого можно, например, выбрав какой-нибудь базис $e_1, e_2, \ldots, e_p$ подпространства A, дополнить его некоторыми векторами $e_{p+1}, e_{p+2}, \ldots, e_n$ до базиса всего пространства и в качестве B взять подпространство, порождаемое указанными векторами $e_{p+1}, e_{p+2}, \ldots, e_n$.

Отображение φ каждый вектор из B переводит в вектор из B'; следовательно, φ можно рассматривать и как отображение B в B'. Обозначим это отображение через φ_B (оно отличается от φ тем, что действует на подпространстве B, в то время как φ действует на всем пространстве L). Если мы докажем, что отображение φ_B является взаимно однозначным, то отсюда будет следовать (см. с. 125), что $\dim B = \dim B'$; тогда, пользуясь (2), получим:

$$\dim L = \dim A + \dim B = \dim A + \dim B',$$

что эквивалентно равенству (1). Итак, остается доказать, что φ_B— взаимно однозначное отображение B на B'.

Пусть $\boldsymbol{y}$ — произвольный вектор из B'. Покажем, что уравнение

$$\varphi_B(\boldsymbol{x}) = \boldsymbol{y} \tag{3}$$

имеет единственное решение $\boldsymbol{x} \in B$.

Для этого заметим, что уравнение $\varphi(\boldsymbol{x}) = \boldsymbol{y}$ обязательно имеет решение: ведь вектор $\boldsymbol{y}$ принадлежит области значений отображения φ. Пусть $\boldsymbol{x}^0$ — одно из таких решений. Представим вектор $\boldsymbol{x}^0$ в виде суммы

$$\boldsymbol{x}^0 = \boldsymbol{x}_A + \boldsymbol{x}_B,$$

где $\boldsymbol{x}_A \in A$, $\boldsymbol{x}_B \subset B$. Тогда

$$\boldsymbol{y} = \varphi(\boldsymbol{x}^0) = \varphi(\boldsymbol{x}_A) + \varphi(\boldsymbol{x}_B) = \varphi(\boldsymbol{x}_B),$$

откуда следует, что вектор $\boldsymbol{x}_B$ является решением уравнения (3).

Покажем, что других решений уравнение (3) иметь не может. Если бы наряду с $\boldsymbol{x}_B$ существовало еще одно решение $\boldsymbol{x}'_B$, то из равенств $\varphi(\boldsymbol{x}_B) = \boldsymbol{y}$, $\varphi(\boldsymbol{x}'_B) = \boldsymbol{y}$ мы получили бы: $\varphi(\boldsymbol{x}_B - \boldsymbol{x}'_B) = \boldsymbol{0}'$, т. е. $\boldsymbol{x}_B - \boldsymbol{x}'_B \in A$. Но это невозможно: ненулевой вектор $\boldsymbol{x}_B - \boldsymbol{x}'_B$ не может принадлежать одновременно B и A (по определению прямой суммы пересечение $A \cap B$ состоит только из нулевого вектора).

Теорема доказана.

3. Совпадение ранга линейного отображения с рангом его матрицы.

Т е о р е м а. *Ранг матрицы линейного отображения при произвольном выборе базисов в пространствах L и L' равен рангу самого отображения.*

Д о к а з а т е л ь с т в о. Пусть $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ — базис пространства L и $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_m$ — базис пространства L'. Так как область значений отображения φ представляет собой подпространство, порожденное векторами

$$\varphi(\boldsymbol{a}_1), \varphi(\boldsymbol{a}_2), \ldots, \varphi(\boldsymbol{a}_n) \tag{4}$$

(ибо любой вектор $\boldsymbol{x}$ из L разлагается по $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$, следовательно, его образ разлагается по $\varphi(\boldsymbol{a})$, $\varphi(\boldsymbol{a}_2), \ldots, \varphi(\boldsymbol{a}_n)$), то ранг отображения φ равен рангу указанной системы векторов. Но ранг любой системы векторов совпадает с рангом матрицы, составленной из координатных строк этих векторов в заданном базисе. Для системы (4) такой матрицей является матрица A', транспонированная к матрице A отображения φ (см. формулы (6) и определение матрицы отображения φ в пункте 2 § 1). Теперь остается лишь заметить, что ранги матриц A и A' всегда совпадают (см.: Алгебра, ч. 1, с. 91).

Вопросы и упражнения

1. Что представляют собой ядра и области значений отображений, рассмотренных в примерах 3, 4 пункта 1 § 1 и в задаче пункта 2 § 1? Чему равны ранги и дефекты указанных отображений?

2. Доказать, что отображение φ пространства L в L' взаимно однозначно тогда и только тогда, когда $d = 0$ и $n = n'$ (где $n = \dim L$, $n' = \dim L'$ и d — дефект φ).

§ 3. Линейное отображение пространства в себя

В этом параграфе (а также в следующих за ним) будет рассмотрен тот наиболее часто встречающийся случай, когда линейное отображение φ задано как отображение пространства L *в себя*. Тогда, очевидно, нет необходимости в выборе *двух различных* базисов, к одному из которых мы относили бы произвольный вектор $\boldsymbol{x} \in L$, а к другому — его образ $\boldsymbol{y} = \varphi(\boldsymbol{x})$ — достаточно *одного* базиса.

Итак, мы фиксируем в пространстве L базис

$$\boldsymbol{a}_1, \ \boldsymbol{a}_2, \ \ldots, \ \boldsymbol{a}_n, \tag{1}$$

по которому разлагаем как исходный вектор $\boldsymbol{x}$, так и его образ $\boldsymbol{y} = \varphi(\boldsymbol{x})$. Тогда линейному отображению φ будет отвечать некоторая матрица A типа (n, n) (т. е. квадратная матрица порядка n), такая, что одновременно выполняются соотношения:

$$(\varphi(\boldsymbol{a}_1)\, \varphi(\boldsymbol{a}_2) \ \ldots \ \varphi(\boldsymbol{a}_n)) = (\boldsymbol{a}_1 \boldsymbol{a}_2 \ \ldots \ \boldsymbol{a}_n) A \tag{2}$$

и

$$Y = AX, \tag{3}$$

где X есть столбец координат произвольного вектора $\boldsymbol{x}$ в базисе (1), а Y — столбец координат вектора $\boldsymbol{y} = \varphi(\boldsymbol{x})$ (образа вектора $\boldsymbol{x}$) *в том же* базисе (1). Матрица A называется при этом *матрицей отображения* φ *в базисе* (1).

Предположим теперь, что от базиса (1) мы переходим в пространстве L к новому базису

$$\boldsymbol{a}_1^*, \ \boldsymbol{a}_2^*, \ \ldots, \ \boldsymbol{a}_n^*. \tag{4}$$

В новом базисе отображению φ отвечает новая матрица A^*. Возникает вопрос: как связаны между собой матрицы A и A^*? Мы покажем, что справедлива формула

$$A^* = P^{-1} A P, \tag{5}$$

где

$$P = \begin{pmatrix} p_{11} p_{12} & \ldots & p_{1n} \\ p_{21} p_{22} & \ldots & p_{2n} \\ \ldots & \ldots & \ldots \\ p_{n1} p_{n2} & & p_{nn} \end{pmatrix}$$

есть матрица перехода от исходного базиса (1) к новому базису (4).

Для доказательства формулы (5) разложим произвольный вектор $\boldsymbol{x} \in L$ по базисам (1) и (4):

$$\boldsymbol{x} = x_1\boldsymbol{a}_1 + x_2\boldsymbol{a}_2 + \cdots + x_n\boldsymbol{a}_n,$$
$$\boldsymbol{x} = x_1^*\boldsymbol{a}_1^* + x_2^*\boldsymbol{a}_2^* + \cdots x_n^*\boldsymbol{a}_n^*.$$

Мы знаем (см. с. 90), что между старыми и новыми координатами вектора $\boldsymbol{x}$ существует следующая связь:

$$X = PX^*, \tag{6}$$

где X обозначает столбец из старых, а X^* — столбец из новых координат:

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \\ \cdot \\ x_n \end{pmatrix}, \quad X^* = \begin{pmatrix} x_1^* \\ x_2^* \\ \\ \cdot \\ x_n^* \end{pmatrix}$$

Точно такая же связь имеется и между старыми и новыми координатами вектора $\boldsymbol{y} = \varphi(\boldsymbol{x})$:

$$Y = PY^*. \tag{7}$$

Пользуясь соотношениями (3), (6) и (7), установим теперь связь между X^* и Y^*. Учитывая невырожденность матрицы перехода P, получаем последовательно:

$$Y^* = P^{-1}Y = P^{-1}AX = P^{-1}APX^*;$$

отсюда следует, что матрицей отображения φ в базисе (4) будет матрица

$$A = P^{-1}AP,$$

что и требовалось доказать.

Замечание. Матрица B называется *подобной* матрице C, если существует такая невырожденная матрица T, что выполняется равенство

$$B = T^{-1}CT.$$

Если матрица B подобна матрице C, то и матрица C подобна матрице B, так как из последнего равенства вытекает равенство

$$C = S^{-1}BS,$$

где $S = T^{-1}$. Другими словами, отношение подобия является симметричным. Поэтому можно говорить просто о *двух подобных друг другу матрицах* B и C.

Из формулы (5) мы можем теперь вывести такое заключение: *матрицы, отвечающие данному линейному отображению в двух различных базисах, подобны друг другу.*

Вопросы и упражнения

1. Определить с помощью матрицы перехода, как изменится матрица линейного отображения, если поменять местами какие-нибудь два (скажем, первый и второй) базисных вектора. Решить тот же вопрос непосредственно, исходя из формул (3), задающих отображение в координатах.

2. Доказать, что подобные матрицы имеют равные определители.

3. Пусть T — фиксированная невырожденная матрица порядка n. Сопоставим каждой матрице A порядка n матрицу $A' = T^{-1}AT$. Убедиться, что при этом получается изоморфное отображение кольца всех квадратных матриц порядка n на себя.

§ 4. Инвариантные подпространства. Собственные векторы и собственные значения линейного отображения

1. Инвариантные подпространства. Пусть L — векторное пространство над полем P и φ — линейное отображение L в себя. Рассмотрим произвольное подпространство K пространства L. Образ этого подпространства при отображении φ, как было доказано, также является подпространством. Обозначим это подпространство $\varphi(K)$. Особый интерес представляет случай, когда $\varphi(K)$ содержится в K, т. е. когда образ произвольного вектора $\boldsymbol{x}$ из K снова принадлежит K. В связи с этим вводится понятие *инвариантного подпространства.*

Подпространство K называется *инвариантным подпространством* относительно отображения φ, если $\varphi(K) \subset K$.

Тривиальным примером инвариантного подпространства является нулевое подпространство; его инвариантность следует из равенства

$$\varphi(0) = 0.$$

Все пространство L тоже является, конечно, инвариантным подпространством. Однако, кроме этих крайних случаев, возможны и другие инвариантные подпространства.

2. Собственные векторы и собственные значения. Характеристическое уравнение. Особенно важны инвариантные подпространства размерности 1. Если K — одно из таких подпространств и $\boldsymbol{x}$ — какой-нибудь ненулевой вектор из K, то

$$\varphi(\boldsymbol{x}) = \lambda \boldsymbol{x}, \tag{1}$$

поскольку вектор $\varphi(\boldsymbol{x})$ должен снова принадлежать K. Обратно, если какой-нибудь ненулевой вектор $\boldsymbol{x}$ удовлетворяет условию (1), то порожденное им одномерное подпространство K будет инва-

риантно относительно φ. Действительно, любой вектор из K имеет вид $c\boldsymbol{x}\,(c \in P)$, но

$$\varphi(c\boldsymbol{x}) = c\varphi(\boldsymbol{x}) = c(\lambda\boldsymbol{x}) = \lambda(c\boldsymbol{x}),$$

т. е.

$$\varphi(c\boldsymbol{x}) \in K.$$

Дадим следующее важное определение:

Если для вектора $\boldsymbol{x} \neq 0$ выполняется равенство (1), то этот вектор называется *собственным вектором* отображения φ, а число λ — *собственным значением*. При этом говорят, что собственный вектор $\boldsymbol{x}$ *отвечает* (соответствует, принадлежит) собственному значению λ.

Пусть, например, отображение φ трехмерного векторного пространства задано в некотором базисе $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, $\boldsymbol{a}_3$ формулой

$$\varphi(\boldsymbol{x}) = x_1\boldsymbol{a}_1,$$

где

$$\boldsymbol{x} = x_1\boldsymbol{a}_1 + x_2\boldsymbol{a}_2 + x_3\boldsymbol{a}_3$$

— разложение вектора $\boldsymbol{x}$ относительно данного базиса (как говорят иногда, φ есть проектирование на $\boldsymbol{a}_1$ параллельно $\boldsymbol{a}_2$, $\boldsymbol{a}_3$). Тогда любой вектор вида $x_1\boldsymbol{a}_1$, где $x_1 \neq 0$, будет собственным вектором, отвечающим собственному значению 1:

$$\varphi(x_1\boldsymbol{a}_1) = x_1\boldsymbol{a}_1.$$

В то же время каждый вектор вида $x_2\boldsymbol{a}_2 + x_3\boldsymbol{a}_3$, где числа x_2 и x_3 не равны нулю одновременно, будет собственным вектором, отвечающим собственному значению 0:

$$\varphi(x_2\boldsymbol{a}_2 + x_3\boldsymbol{a}_3) = 0 = 0 \cdot (x_2\boldsymbol{a}_2 + x_3\boldsymbol{a}_3).$$

Собственные векторы и собственные значения играют весьма существенную роль при исследовании структуры линейного отображения. Поэтому естественным является вопрос о способе их нахождения. Такой способ будет указан ниже.

Предположим, что зафиксирован некоторый базис $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ пространства L и что отображение φ задано в этом базисе матрицей

$$A = \begin{pmatrix} \alpha_{11}\alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21}\alpha_{22} & \ldots & \alpha_{2n} \\ \cdot & \cdots & \\ \alpha_{n1}\alpha_{n2} & \ldots & \alpha_{nn} \end{pmatrix}.$$

Если, как обычно, координаты вектора $\boldsymbol{x}$ обозначить $x_1, x_2, \ldots, x_n$, то векторное равенство (1) будет равносильно следующим n соотношениям:

$$\begin{aligned} \alpha_{11}x_1 + \alpha_{12}x_2 + \cdots + \alpha_{1n}x_n &= \lambda x_1, \\ \alpha_{21}x_1 + \alpha_{22}x_2 + \cdots + \alpha_{2n}x_n &= \lambda x_2, \\ \cdot \quad\quad \cdot \quad\quad \cdot \quad\quad & \cdot \\ \alpha_{n1}x_1 + \alpha_{n2}x_2 + \cdots + \alpha_{nn}x_n &= \lambda x_n. \end{aligned}$$

После приведения подобных членов получаем:

$$\left.\begin{array}{rcl} (\alpha_{11}-\lambda)x_1+\alpha_{12}x_2 & +\cdots+ & \alpha_{1n}x_n=0,\\ \alpha_{21}x_1+(\alpha_{22}-\lambda)x_2 & +\cdots+ & \alpha_{2n}x_n=0,\\ \cdot\quad\cdot & \cdot\quad\cdot\quad\cdot & \cdot\quad\cdot\quad\cdot\\ \alpha_{n1}x_1+\alpha_{n2}x_2 & +\cdots & (\alpha_{nn}-\lambda)x_n=0. \end{array}\right\} \qquad (2)$$

Рассматривая данную систему равенств как систему из n линейных однородных уравнений с n неизвестными $x_1, x_2, \ldots, x_n$, мы можем теперь сказать, что координаты любого собственного вектора, отвечающего собственному значению λ, удовлетворяют системе (2). Следовательно, для всякого собственного значения λ система (2) должна допускать *ненулевое* решение. Отсюда вытекает, что определитель этой системы должен быть равен нулю. Таким образом, любое собственное значение λ должно удовлетворять условию:

$$\begin{vmatrix} \alpha_{11}-\lambda & \alpha_{12} & \ldots & \alpha_{1n}\\ \alpha_{21} & \alpha_{22}-\lambda & \ldots & \alpha_{2n}\\ \cdot & \cdot & \cdot & \cdot\\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn}-\lambda \end{vmatrix} = 0. \qquad (3)$$

Обратно, если какое-то число λ из поля P удовлетворяет этому условию, то это число является собственным значением: действительно, тогда система (2) будет иметь ненулевое решение $x_1, x_2, \ldots x_n$, т. е. найдется ненулевой вектор $\boldsymbol{x}$, такой, что $\varphi(\boldsymbol{x}) = \lambda\boldsymbol{x}$.

Раскрывая определитель, стоящий в левой части равенства (3), мы получим, очевидно, многочлен n-й степени относительно λ. Следовательно, условие (3) представляет собой алгебраическое уравнение n-й степени относительно λ. Это уравнение называется *характеристическим уравнением матрицы* A.

Итак, *собственными значениями отображения* φ *являются те и только те числа* λ *из поля* P, *которые служат корнями характеристического уравнения* (3). *Для любого собственного значения* λ *соответствующие ему собственные векторы* $\boldsymbol{x}$ *составляют множество всех ненулевых решений системы* (2).

Возвращаясь к характеристическому уравнению (3), заметим, что определитель в левой части (3) является определителем матрицы $A - \lambda E$, где E — единичная матрица порядка n. Поэтому характеристическое уравнение можно представить в следующей матричной записи:

$$|A - \lambda E| = 0. \qquad (4)$$

Пользуясь формой (4) характеристического уравнения, легко доказать следующее предложение: *если матрицы* A *и* A' *подобны, то их характеристические уравнения совпадают.* Действительно, по определению подобия матриц найдется такая невырожденная матрица T, что

$$A' = T^{-1}AT.$$

Отсюда получаем:

$$|A' - \lambda E| = |T^{-1}AT - T^{-1}(\lambda E)T| = |T^{-1}(A - \lambda E)T| =$$
$$= |T^{-1}| \cdot |A - \lambda E| \cdot |T| = |A - \lambda E|.$$

Мы воспользовались в процессе преобразований теоремой об определителе произведения нескольких матриц, из которой, в частности, следует, что $|T^{-1}| \cdot |T| = |E| = 1$.

Так как при переходе от данного базиса к другому матрица отображения заменяется подобной матрицей (см. § 3), то из только что доказанного предложения вытекает, что характеристическое уравнение матрицы линейного отображения не меняется при переходе к новому базису. В связи с этим мы можем просто говорить о *характеристическом уравнении отображения*, не указывая конкретно матрицы, которой это отображение задается в том или ином базисе.

Задача. Пусть отображение трехмерного пространства L над полем $\mathbf{R}$ действительных чисел задано в некотором базисе матрицей

$$\begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}.$$

Найти собственные векторы и собственные значения этого отображения.

Решение. Характеристическое уравнение в данном случае имеет вид:

$$\begin{vmatrix} -\lambda & 1 & 0 \\ -4 & 4-\lambda & 0 \\ -2 & 1 & 2-\lambda \end{vmatrix} = 0,$$

или (после вычисления определителя)

$$-(\lambda - 2)^3 = 0.$$

Отсюда находим единственное собственное значение $\lambda_1 = 2$, после чего записываем систему (2):

$$\left.\begin{aligned} -2x_1 + x_2 &= 0, \\ -4x_1 + 2x_2 &= 0, \\ -2x_1 + x_2 &= 0. \end{aligned}\right\}$$

Решая ее, получаем: $x_2 = 2x_1 + 0x_3$. Фундаментальный набор состоит из решений (1, 2, 0) и (0, 0, 1), а общее решение записывается в виде

$$c_1(1, 2, 0) + c_2(0, 0, 1). \qquad (5)$$

Итак, данное отображение имеет единственное собственное значение $\lambda_1 = 2$, а отвечающие ему собственные векторы получаются

из выражения (5) при всевозможных действительных значениях c_1 и c_2, не равных одновременно нулю.

3. Собственные подпространства. Пусть λ — собственное значение отображения φ. Обозначим через $K(\lambda)$ множество *всех* векторов $\boldsymbol{x} \in L$, удовлетворяющих условию (1):

$$\varphi(\boldsymbol{x}) = \lambda \boldsymbol{x}.$$

Это множество состоит из всех собственных векторов, отвечающих λ, и вектора **0**. Покажем, что $K(\lambda)$ *является подпространством.*

Если векторы $\boldsymbol{a}$ и $\boldsymbol{b}$ принадлежат $K(\lambda)$, то

$$\varphi(\boldsymbol{a}) = \lambda \boldsymbol{a} \text{ и } \varphi(\boldsymbol{b}) = \lambda \boldsymbol{b},$$

откуда следует:

$$\varphi(\boldsymbol{a} + \boldsymbol{b}) = \varphi(\boldsymbol{a}) + \varphi(\boldsymbol{b}) = \lambda \boldsymbol{a} + \lambda \boldsymbol{b} = \lambda(\boldsymbol{a} + \boldsymbol{b}),$$

т. е. вектор $\boldsymbol{a} + \boldsymbol{b}$ тоже принадлежит $K(\lambda)$. Далее, если k — какое-нибудь число из P, то

$$\varphi(k\boldsymbol{a}) = k\varphi(\boldsymbol{a}) = k\lambda \boldsymbol{a} = \lambda(k\boldsymbol{a}),$$

т. е. вектор $c\boldsymbol{a}$ снова принадлежит $K(\lambda)$. Этим доказано, что $K(\lambda)$— подпространство.

Подпространство $K(\lambda)$ называется *собственным подпространством*, отвечающим собственному значению λ.

В примере, рассмотренном в пункте 2 (прсектирование на $\boldsymbol{a}_1$ параллельно $\boldsymbol{a}_2$, $\boldsymbol{a}_3$), отображение φ имело два собственных значения: 1 и 0. Для первого из них собственное подпространство есть одномерное подпространство, порожденное вектором $\boldsymbol{a}_1$, для второго — двумерное подпространство, порожденное $\boldsymbol{a}_2$ и $\boldsymbol{a}_3$.

4. Условие приводимости матрицы линейного отображения к диагональной форме. Линейное отображение может быть задано разными способами. Одна из возможных форм задания — с помощью матрицы, отвечающей отображению в том или другом базисе. Все свойства отображения можно в принципе «извлечь» из его матрицы. Естественно ожидать, что, чем проще матрица данного отображения, тем легче изучать свойства этого отображения.

Один из наиболее простых классов матриц составляют так называемые *диагональные матрицы*, т. е. квадратные матрицы вида:

$$\begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix} \tag{6}$$

(все элементы вне главной диагонали равны нулю). Представляет интерес следующая задача: охарактеризовать линейные отображения, матрицы которых при некотором выборе базиса являются диагональными. Относительно таких отображений принято гово-

рить, что их матрицы *приводятся к диагональной форме*. В этом пункте мы выясним, при каких условиях матрица отображения приводится к диагональной форме.

Пусть отображение φ имеет в базисе $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ диагональную матрицу (6). По определению матрицы отображения (см. формулу (2) § 3) имеем:

$$(\varphi(\boldsymbol{a}_1)\,\varphi(\boldsymbol{a}_2)\,\ldots\,\varphi(\boldsymbol{a}_n)) = (\boldsymbol{a}_1\boldsymbol{a}_2\,\ldots\,\boldsymbol{a}_n)\begin{pmatrix}\lambda_1 & 0 & \ldots & 0\\ 0 & \lambda_2 & \ldots & 0\\ \ldots & \ldots & \ldots & \ldots\\ 0 & 0 & \ldots & \lambda_n\end{pmatrix}, \qquad (7)$$

что равносильно равенствам:

$$\varphi(\boldsymbol{a}_1) = \lambda_1\boldsymbol{a}_1,\ \varphi(\boldsymbol{a}_2) = \lambda\boldsymbol{a}_2,\ \ldots\ ,\ \varphi(\boldsymbol{a}_n) = \lambda\boldsymbol{a}_n. \qquad (7')$$

Но равенства (7′) означают, что базис $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ состоит из собственных векторов отображения φ.

Обратно, если какой-либо базис $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ состоит из собственных векторов отображения φ, то выполняются равенства (7′), а значит, и равенство (7). Следовательно, матрица отображения φ в этом базисе диагональная.

Итак, *матрица отображения φ в некотором базисе тогда и только тогда является диагональной, когда этот базис состоит из собственных векторов отображения* φ.

Для отображения φ, заданного в n-мерном векторном пространстве L, вопрос о приводимости матрицы φ к диагональной форме сводится, таким образом, к следующему: найдется ли в пространстве L система из n линейно независимых собственных векторов отображения φ? Чтобы научиться решать этот вопрос, докажем предварительно две леммы.

Лемма 1. *Собственные векторы, отвечающие попарно различным собственным значениям, линейно независимы.*

Мы должны показать, что если $\lambda_1, \lambda_2, \ldots, \lambda_s$ — попарно различные собственные значения отображения φ и $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_s$ — отвечающие им собственные векторы, то система $\{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_s\}$ линейно независима.

Пусть $s = 1$, т. е. задан единственный собственный вектор $\boldsymbol{a}_1$. Линейная независимость системы $\{\boldsymbol{a}_1\}$ следует из того, что согласно определению собственного вектора, $\boldsymbol{a}_1 \neq \boldsymbol{0}$.

Допустим, что для системы, состоящей из $s-1$ собственных векторов, утверждение леммы справедливо; докажем тогда, что оно будет верно и для системы из s собственных векторов.

Рассуждая от противного, допустим, что векторы $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_s$ линейно зависимы:

$$c_1\boldsymbol{a}_1 + c_2\boldsymbol{a}_2 + \ldots + c_s\boldsymbol{a}_s = \boldsymbol{0}, \qquad (8)$$

где числа $c_1, c_2, \ldots, c_s$ не равны нулю одновременно. Для определенности будем считать $c_1 \neq 0$. Применив к обеим частям ра-

венства (8) отображение φ, получим:

$$\lambda_1 c_1 \boldsymbol{a}_1 + \lambda_2 c_2 \boldsymbol{a}_2 + \ldots + \lambda_s c_s \boldsymbol{a}_s = 0. \tag{9}$$

Если теперь умножить обе части равенства (8) на λ_1 и вычесть полученное равенство из (9), то будем иметь:

$$(\lambda_2 - \lambda_1) c_2 \boldsymbol{a}_2 + (\lambda_3 - \lambda_1) c_3 \boldsymbol{a}_3 + \ldots + (\lambda_s - \lambda_1) c_s \boldsymbol{a}_s = 0.$$

По предположению индукции система векторов $\boldsymbol{a}_2, \boldsymbol{a}_3, \ldots, \boldsymbol{a}_s$ линейно независима, поэтому все коэффициенты в полученном соотношении должны быть равны нулю:

$$(\lambda_2 - \lambda_1) c_2 = 0, \ (\lambda_3 - \lambda_1) c_3 = 0, \ \ldots, \ (\lambda_s - \lambda_1) c_s = 0.$$

Но все разности $\lambda_i - \lambda_1 \ (i > 1)$ отличны от нуля (ведь числа $\lambda_1, \lambda_2, \ldots, \lambda_s$ по условию попарно различны). Следовательно, $c_2 = 0, \ldots, c_s = 0$. Тогда из равенства (8) следует: $c_1 = 0$, что противоречит сделанному предположению. Лемма доказана.

Лемма 2. *Сумма размерностей всех собственных подпространств не превосходит размерности пространства L.*

Мы должны показать, что если $\lambda_1, \lambda_2, \ldots, \lambda_p$ — все попарно различные собственные значения и $K(\lambda_1), K(\lambda_2), \ldots, K(\lambda_p)$ — отвечающие им собственные подпространства, то

$$n_1 + n_2 + \ldots + n_p \leqslant n, \tag{10}$$

где $n_1, n_2, \ldots, n_p$ — размерности соответственно подпространств $K(\lambda_1), K(\lambda_2), \ldots, K(\lambda_p)$, а n — размерность пространства L.

Выберем в каждом подпространстве $K(\lambda_i)$ $(1 \leqslant i \leqslant p)$ какой-нибудь базис

$$\boldsymbol{a}_1^i, \ \boldsymbol{a}_2^i, \ \ldots, \ \boldsymbol{a}_{n_i}^i.$$

Объединив векторы всех этих базисов, получим систему S, состоящую из $n_1 + n_2 + \ldots + n_p$ векторов. Если мы докажем, что система S линейно независима, то отсюда будет следовать неравенство (10).

Допустим, рассуждая от противного, что система S линейно зависима. Это означает, что существуют такие числа α_j^i, неравные одновременно нулю, для которых справедливо соотношение

$$\alpha_1^1 \boldsymbol{a}_1^1 + \alpha_2^1 \boldsymbol{a}_2^1 + \ldots + \alpha_{n_1}^1 \boldsymbol{a}_{n_1}^1 + \ldots + \alpha_1^p \boldsymbol{a}_1^p + \alpha_2^p \boldsymbol{a}_2^p + \ldots \alpha_{n_p}^p \boldsymbol{a}_{n_p}^p = 0. \tag{11}$$

Положим

$$\alpha_1^1 \boldsymbol{a}_1^1 + \alpha_2^1 \boldsymbol{a}_2^1 + \ldots + \alpha_{n_1}^1 \boldsymbol{a}_{n_1}^1 = \boldsymbol{a}^1,$$

. . . . . .

$$\alpha_1^p \boldsymbol{a}_1^p + \alpha_2^p \boldsymbol{a}_2^p + \ldots + \alpha_{n_p}^p \boldsymbol{a}_{n_p}^p = \boldsymbol{a}^p.$$

Тогда из (11) получим соотношение

$$\boldsymbol{a}^1 + \ldots + \boldsymbol{a}^p = 0. \tag{12}$$

Если бы хоть один из векторов $\boldsymbol{a}^1,\ldots,\boldsymbol{a}^p$ был отличен от нуля, то равенство (12) противоречило бы лемме 1. Следовательно, каждый из этих векторов равен нулю. Отсюда, в свою очередь, вытекает, что все коэффициенты α_j^i равны нулю. Мы пришли к противоречию. Лемма доказана.

Теперь мы в состоянии сформулировать и доказать теорему, дающую необходимые и достаточные условия приводимости матрицы линейного отображения к диагональной форме.

Теорема. *Пусть* $\lambda_1, \lambda_2,\ldots,\lambda_p$ *— все попарно различные собственные значения отображения* φ *и* $K(\lambda_1)$, $K(\lambda_2),\ldots,$ $K(\lambda_p)$ *— отвечающие им собственные подпространства. Матрица отображения* φ *приводится к диагональной форме тогда и только тогда, когда сумма размерностей всех собственных подпространств равна размерности пространства* L*:*

$$\dim K(\lambda_1) + \dim K(\lambda_2) + \ldots + \dim K(\lambda_p) = \dim L. \qquad (13)$$

Доказательство. Пусть матрица отображения приводится к диагональной форме. Тогда отображение имеет n линейно независимых собственных векторов. Каждый из этих векторов отвечает одному из собственных значений $\lambda_1, \lambda_2,\ldots,\lambda_p$.

Пусть собственному значению $\lambda_i (1 \leqslant i \leqslant p)$ отвечает k_i из указанных n векторов. Следовательно,

$$k_1 + k_2 + \ldots + k_p = n.$$

С другой стороны, ясно, что размерность каждого пространства $K(\lambda_i)$ будет больше или равна k_i:

$$\dim K(\lambda_i) \geqslant k_i.$$

Отсюда вытекает, что

$$\dim K(\lambda_1) + \dim K(\lambda_2) + \ldots + \dim K(\lambda_p) \geqslant n.$$

Из этого неравенства и леммы 2 получаем равенство (13).

Обратно, пусть выполнено равенство (13). Тогда, выбрав базис в каждом из подпространств $K(\lambda_1)$, $K(\lambda_2),\ldots,$ $K(\lambda_p)$ и объединив эти базисы в одну систему, мы получим (см. доказательство леммы 2) n линейно независимых собственных векторов. Это означает, что матрица отображения приводится к диагональной форме.

Следствие. *Если отображение* φ *имеет* n *попарно различных собственных значений, то его матрица приводится к диагональной форме.*

Действительно, в этом случае сумма размерностей всех собственных подпространств заведомо не меньше, чем n. Значит, эта сумма в точности равна n.

Задача. В трехмерном пространстве над полем действительных чисел отображение φ задано в некотором базисе матрицей

$$\begin{pmatrix} -1 & 3 & -1 \\ -3 & 5 & -1 \\ -3 & 3 & 1 \end{pmatrix}.$$

Выяснить, приводится ли матрица отображения φ к диагональной форме.

Решение. Характеристическое уравнение

$$\begin{vmatrix} -1-\lambda & 3 & -1 \\ -3 & 5-\lambda & -1 \\ -3 & 3 & 1-\lambda \end{vmatrix} = 0,$$

как нетрудно подсчитать, преобразуется к виду:

$$(2-\lambda)^2 (1-\lambda) = 0.$$

Следовательно, отображение φ имеет только два различных собственных значения: $\lambda_1 = 1$ и $\lambda_2 = 2$.

Для собственных векторов, отвечающих $\lambda_1 = 1$, имеем следующую систему уравнений:

$$\left.\begin{aligned} -2x_1 + 3x_2 - x_3 &= 0, \\ -3x_1 + 4x_2 - x_3 &= 0, \\ -3x_1 + 3x_2 &= 0. \end{aligned}\right\}$$

Фундаментальный набор решений состоит из одного вектора $\boldsymbol{a}_1$; можно взять, например, $\boldsymbol{a}_1 = (1, 1, 1)$.

Для $\lambda_2 = 2$ имеем следующую систему:

$$\left.\begin{aligned} -3x_1 + 3x_2 - x_3 &= 0, \\ -3x_1 + 3x_2 - x_3 &= 0, \\ -3x_1 + 3x_2 - x_3 &= 0. \end{aligned}\right\}$$

Фундаментальный набор состоит из двух векторов, например: $\boldsymbol{a}_2 = (1, 1, 0)$ и $\boldsymbol{a}_3 = (0, 1, 3)$. Таким образом, имеем: $\dim K(1) = 1$ и $\dim K(2) = 2$; сумма указанных размерностей равна 3. В базисе $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3$ матрица отображения φ диагональная и имеет вид:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Вопросы и упражнения

1. Пусть L — двумерное векторное пространство над полем $\mathbf{R}$ действительных чисел (пространство векторов обычной плоскости). Найти собственные векторы и собственные значения для каждого из следующих отображений φ:

а) φ — симметрия относительно оси, проходящей через начало;

б) φ — поворот на угол α вокруг начала (обратить внимание на случаи: $\alpha = 0$ и $\alpha = \pi$).

Составить для каждого из этих отображений характеристическое уравнение.

2. Пусть L — векторное пространство матриц вида

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

с элементами из поля $\mathbf{R}$. Найти собственные векторы и собственные значения отображения φ, ставящего в соответствие каждой матрице A указанного вида транспонированную к ней матрицу A'.

3. Найти размерности собственных подпространств для отображения φ из предыдущего примера 2. Приводится ли матрица этого отображения к диагональной форме; если да, то к какой?

ОГЛАВЛЕНИЕ

Предисловие 3

Глава I. **Группы, кольца, поля.** 4
§ 1. Операции и алгебраические системы . . . . . —
§ 2. Некоторые классы операций 11
§ 3. Группы 16
§ 4. Конечные группы 33
§ 5. Смежные классы и фактор-группы 39
§ 6. Кольца и поля 50
§ 7. Числовые поля 60

Глава II. **Векторные пространства.** 72
§ 1. Векторное пространство над полем . . . . . —
§ 2. Конечномерные векторные пространства 79
§ 3. Подпространства векторного пространства. Векторные многообразия 91

Глава III. **Евклидовы пространства** 101
§ 1. Скалярное произведение. Евклидово n-мерное пространство . . . . . —
§ 2. Ортогональная система векторов. Ортонормированный базис 106
§ 3. Ортогональное дополнение к подпространству. Процесс ортогонализации 111

Глава IV. **Линейные отображения** 120
§ 1. Понятие линейного отображения. Связь между линейными отображениями и матрицами . . . . . —
§ 2. Ранг и дефект линейного отображения 129
§ 3. Линейное отображение пространства в себя 132
§ 4. Инвариантные подпространства. Собственные векторы и собственные значения линейного отображения 134