Л. А. СКОРНЯКОВ

ЭЛЕМЕНТЫ АЛГЕБРЫ

Л. А. СКОРНЯКОВ

ЭЛЕМЕНТЫ АЛГЕБРЫ

ИЗДАНИЕ ВТОРОЕ, ПЕРЕРАБОТАННОЕ

Допущено Министерством высшего
и среднего специального образования СССР
в качестве учебного пособия
для физико-математических специальных вузов

МОСКВА «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
1986

ББК 22.14
С44
УДК 512 (075.8)

С к о р н я к о в Л. А. **Элементы алгебры**: Учеб. пособие для вузов.—2-е изд.— М.: Наука. Гл. ред. физ.-мат. лит., 1986.— 240 с.

В основу учебного пособия положен курс лекций по высшей алгебре, читавшийся в течение ряда лет на механико-математическом факультете и отделении структурной лингвистики филологического факультета Московского университета.

В книге содержатся следующие разделы: матрицы и системы линейных уравнений, элементы общей алгебры, представления конечных групп. При этом учение о системах линейных уравнений излагается без использования понятия линейной зависимости, а изложение теории представлений конечных групп имеет теоретико-кольцевую направленность. Уделено внимание и упражнениям, помогающим овладеть изложенными в пособии понятиями.

1-е издание выходило в 1980 г.

Для студентов младших курсов университетов и педагогических институтов.

Р е ц е н з е н т
доктор физико-математических наук профессор *З. И. Боревич*

Лев Анатольевич Скорняков

ЭЛЕМЕНТЫ АЛГЕБРЫ

Редактор *Ф. И. Кизнер*
Художественный редактор *Т. Н. Кольченко*
Технический редактор *Е. В. Морозова*
Корректор *Н. Б. Румянцева*

ИБ № 12923

Сдано в набор 09.04.86. Подписано к печати 27.08.86.
Формат 84×108/32. Бумага тип. № 2.
Гарнитура обыкновенная. Печать высокая.
Усл. печ. л. 12,6. Усл. кр.-отт. 12,92. Уч.-изд. л. 13,13.
Тираж 21000 экз. Заказ № 2453. Цена 45 коп.

Ордена Трудового Красного Знамени издательство «Наука»
Главная редакция физико-математической литературы
117071 Москва В-71, Ленинский проспект, 15

2-я типография издательства «Наука»
121099 Москва Г-99, Шубинский пер., 6.

С $\frac{1702030000-173}{053(02)-86}$ 66-86

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ КО ВТОРОМУ ИЗДАНИЮ

Наиболее фундаментальное изменение по сравнению с первым изданием состоит в том, что ряд результатов, не зависящих от теории представлений, перенесен из главы IV в главу II, где вместе с теоремой о строении конечно порожденных абелевых групп они составили новый параграф. Здесь же дано прямое доказательство разрешимости p-групп и групп порядка pq, а также намечено доказательство простоты группы SO (3). Остальные изменения сводятся к улучшению деталей изложения.

По техническим причинам в настоящем издании не удалось привести список литературы для дальнейшего изучения общей алгебры. В качестве первого чтения здесь может быть рекомендована книга автора «Элементы общей алгебры» (М.: Наука, 1983), где имеются и необходимые литературные указания. Изложение учения о системах линейных уравнений, более элементарное, чем в настоящем пособии, можно найти в брошюре автора «Системы линейных уравнений» (М.: Наука, 1986).

ПРЕДИСЛОВИЕ К ПЕРВОМУ ИЗДАНИЮ

Настоящее учебное пособие ставит своей целью познакомить читателя с основами алгебры. Здесь излагается общая теория линейных уравнений (включая теорию определителей и алгебру матриц), элементы общей алгебры (а именно простейшие свойства полугрупп, групп, колец, модулей и структур (решеток)) и основы теории представлений конечных групп, включая необходимые факты из теории линейных пространств и полупростых конечномерных алгебр. При этом основы теории линейных пространств излагаются как частный случай теории правых модулей над кольцом. Разумеется, читатели, изучившие линейные пространства по каким-либо другим источникам, могут пропустить § 1 главы III. В главах III и IV не используются результаты § 7 главы II. С другой стороны, в этих главах необходимы некоторые сведения из теории многочленов, не затрагиваемой в настоящем пособии. В этих случаях даны точные ссылки на соответствующие места из учебников А. Г. Куроша и А. И. Кострикина *). С расчетом на студентов младших курсов в пособие не включены результаты, в доказательствах которых используется трансфинитная индукция или лемма Куратовского — Цорна. Именно поэтому речь идет о конечномерных алгебрах, а не о кольцах с условием минимальности. Сознавая архаичность такого изложения, можно утешать себя мыслью, что оно дает лишний повод для использования теории линейных пространств.

Настоящее пособие, хотя и имеет в виду университетский курс алгебры, не может заменить существующие руководства и не претендует на это. Однако оно дает возможность преподающим и изучающим алгебру познакомиться с изложением материала, отличающимся от предлагаемого упоминавшимися выше учебниками А. Г. Куроша

*) Курош А. Г. Курс высшей алгебры.— 11-е изд.— М.: Наука, 1975; Кострикин А. И. Введение в алгебру.— М.: Наука, 1977.

и А. И. Кострикина. Именно, в главе I излагается учение о системах линейных уравнений без использования понятия линейной зависимости, а в главе IV предлагается изложение теории представлений, имеющее теоретико-кольцевую направленность.

Автор глубоко благодарен З. И. Боревичу, А. В. Михалеву, А. П. Мишиной и Р. А. Шмидту, прочитавшим рукопись и сделавшим ряд полезных замечаний, а также Т. А. Гуровой за большую помощь при оформлении рукописи.

ГЛАВА I

СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ

Задачей настоящей главы является разработка методов, позволяющих исследовать и решать системы линейных уравнений. Аппаратом для этого служат матрицы и определители, изучаемые в этой главе.

§ 1. Матрицы и их элементарные преобразования

Понятие *n-мерной строки* действительных чисел является неопределяемым. Если дана строка $(a_1, \ldots, a_n)$ *), то числа a_i называются ее *координатами* или *компонентами*. Строки $(a_1, \ldots, a_m)$ и $(b_1, \ldots, b_n)$ считаются *равными*, если $m = n$ и $a_i = b_i$ для всех i.

На множестве n-мерных строк действительных чисел можно определить сложение и умножение на действительное число λ по следующим правилам:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

и

$$\lambda (a_1, \ldots, a_n) = (\lambda a_1, \ldots, \lambda a_n).$$

Строка, состоящая из одних нулей, называется *нулевой* и обозначается через 0. Легко проверяется справедливость следующих свойств:

$$a + b = b + a, \qquad \lambda (a + b) = \lambda a + \lambda b,$$
$$(a + b) + c = a + (b + c), \qquad (\lambda + \mu) a = \lambda a + \mu a,$$
$$a + 0 = 0 + a = a, \qquad (\lambda\mu) a = \lambda (\mu a),$$

уравнение $a + x = 0$ разрешимо для любой строки a, $\qquad 1a = a$

(здесь a, b, c — строки, а λ и μ — числа) **).

*) Употребляются такие термины «строка длины n», «n-мерный вектор» и «кортеж длины n» над множеством действительных чисел.

**) Обратим внимание на то, что во втором равенстве правого столбца знак $+$ в его левой и правой частях имеет различный смысл: слева он означает сложение чисел, а справа — сложение строк. Различный смысл имеет и подразумеваемый символ умножения в третьем равенстве этого столбца: $\lambda\mu$ означает произведение чисел, а в остальных случаях мы имеем дело с умножением строки на число.

Докажем, например, равенство $\lambda(a + b) = \lambda a + \lambda b$. С этой целью заметим, что i-ми координатами строк, стоящих в левой и правой частях этого равенства, являются $\lambda(a_i + b_i)$ и $\lambda a_i + \lambda b_i$ соответственно и их совпадение вытекает из справедливости закона дистрибутивности для действительных чисел.

Таблицу, представляющую собой несколько n-мерных строк, записанных одна под другой, называют *матрицей*. Матрица

$$A = \begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{Vmatrix}$$

содержит m строк и n столбцов. Будем говорить также, что она имеет *размер* $m \times n$. Строка является матрицей размера $1 \times n$. Столбец можно рассматривать как матрицу размера $m \times 1$. Матрицу размера $n \times n$ называют *квадратной матрицей порядка* n. Матрица, состоящая из нулевых строк, называется *нулевой* и обозначается O, а матрица

$$E = \begin{Vmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{Vmatrix}$$

— *единичной*. Подчеркнем, что для каждого числа n существует своя единичная матрица порядка n, а для каждого размера $m \times n$ — своя нулевая матрица. Две матрицы считаются *равными*, если они имеют одинаковые размеры и их элементы, стоящие на соответствующих местах, совпадают.

В дальнейшем элементы матрицы, обозначенной некоторой большой буквой (скажем, A), будем, как правило, без специальных оговорок обозначать соответствующей малой буквой с индексами (в нашем случае a_{ij}), обозначающими номер строки и столбца соответственно.

Ступенчатой называется матрица A, обладающая следующими свойствами:

(1) Если i-я строка нулевая, то $(i + 1)$-я строка также нулевая.

(2) Если первые ненулевые элементы i-й и $(i + 1)$-й строк располагаются в столбцах с номерами k_i и k_{i+1} соответственно, то

$$k_i < k_{i+1}.$$

Наглядно эти свойства означают, что ниже нулевой строки могут располагаться лишь нулевые строки, а все элементы, располагающиеся влево и вниз от первого ненулевого элемента какой-либо строки, являются нулями. Происхождение названия нетрудно объяснить, рассматривая, например, ступенчатую матрицу

$$\begin{Vmatrix} 0 & 1 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{Vmatrix},$$

где $k_1 = 2$, $k_2 = 4$ и $k_3 = 5$.

Под преобразованием матрицы понимается переход от одной матрицы к другой, осуществленный по определенным правилам. Будем рассматривать следующие преобразования, называемые *элементарными преобразованиями строк*:

Элементарное преобразование первого типа — перемена местами двух строк матрицы.

Элементарное преобразование второго типа — прибавление к какой-либо строке матрицы другой ее строки, умноженной на некоторое число.

Аналогично определяются *элементарные преобразования столбцов.*

Иногда оказывается полезным

Элементарное преобразование третьего типа — умножение некоторой строки на отличное от нуля число.

Решающую роль для построения нужной нам теории играет следующий факт.

Т е о р е м а 1. *Всякую матрицу конечным числом элементарных преобразований строк можно превратить в ступенчатую матрицу.*

Д о к а з а т е л ь с т в о. Проведем доказательство индукцией по числу строк матрицы. Если имеется всего одна строка, то матрица уже ступенчатая, ибо оба условия, входящие в определение ступенчатой матрицы, выполнены тривиальным образом (ввиду отсутствия второй строки). Пусть теперь матрица A содержит m строк, где $m \geqslant 2$. Предположим, что матрицу с числом строк, меньшим m, можно привести к ступенчатому виду. Если $A = 0$, то она ступенчатая. Если A ненулевая, то в ней есть хоть один ненулевой элемент. Ненулевой элемент располагает-

ся в какой-то строке. Значит, в нашей матрице есть ненулевые строки. Выберем ту, в которой первый ненулевой элемент располагается в столбце с наименьшим номером, скажем, с номером k_1. Применив преобразование первого типа, перенесем эту строку на первое место. Тогда матрица примет вид

$$\begin{Vmatrix} 0 & \dots & 0 & b_{1k_1} & \dots \\ 0 & \dots & 0 & b_{2k_1} & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & b_{mk_1} & \dots \end{Vmatrix},$$

причем $b_{1k_1} \neq 0$. Теперь будем применять преобразования второго типа: ко второй строке прибавим первую, умноженную на $-\frac{b_{2k_1}}{b_{1k_1}}$, к третьей строке — первую, умноженную на $-\frac{b_{3k_1}}{b_{1k_1}}$, и т. д. После применения $m - 1$ таких элементарных преобразований добьемся того, что в k_1-м столбце всюду, кроме первой строки, будут нули:

$$C = \begin{Vmatrix} 0 & \dots & 0 & b_{1k_1} & \dots \\ 0 & \dots & 0 & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots \end{Vmatrix}.$$

Отбросим первую строку. Оставшаяся матрица имеет $m - 1$ строку. По индуктивному предположению ее можно привести к ступенчатому виду:

$$G = \begin{Vmatrix} 0 & \dots & 0 & 0 & \multirow{3}{*}{D} \\ \dots & \dots & \dots & \dots & \\ 0 & \dots & 0 & 0 & \end{Vmatrix}.$$

Пусть первые ненулевые элементы строк ступенчатой матрицы G располагаются в столбцах с номерами $k_2, \dots, k_r$. Тогда $k_2 < \dots < k_r$ по определению ступенчатой матрицы. Но осуществляя элементарные преобразования уменьшенной матрицы, можно считать, что мы делаем элементарные преобразования матрицы C, не использующие первой строки. Поскольку при выполнении этих элементарных преобразований нули, стоявшие в первых k_1 столбцах матрицы C, не могли исчезнуть, то $k_1 <$

$< k_2$. Таким образом, мы получили матрицу

$$H = \left\| \begin{array}{cccc|c} 0 & \dots & 0 & b_{1k_1} & \dots \\ 0 & \dots & 0 & 0 & \\ \dots & \dots & \dots & \dots & D \\ 0 & \dots & 0 & 0 & \end{array} \right\|,$$

удовлетворяющую условию (2) из определения ступенчатой матрицы. Если же в H имеется нулевая строка, то она не совпадает с первой строкой, так как $b_{1k_1} \neq 0$ и, значит, лежит в матрице G. Но G ступенчатая. Следовательно, ниже нулевой строки лежат только нулевые строки. Таким образом, H — ступенчатая матрица.

Теорема 2. *Если от матрицы A к матрице B можно перейти конечным числом элементарных преобразований строк, то и от B к A также можно перейти конечным числом элементарных преобразований строк.*

Доказательство. Если для перехода от A к B использовано одно элементарное преобразование первого типа, то утверждение очевидно. Допустим, что от A к B перешли, используя одно элементарное преобразование второго типа, т. е. (i-я строка в B) = (i-я строка в A) + λ (j-я строка в A), а каждая из остальных строк матрицы B совпадает с соответствующей строкой матрицы A. Таким образом, $b_{ik} = a_{ik} + \lambda a_{jk}$ и $b_{jk} = a_{jk}$ для каждого номера k. Если теперь к i-й строке матрицы B прибавить ее j-ю строку, умноженную на $-\lambda$, то в получившейся после этого матрице на месте (i, k) окажется элемент

$$b_{ik} + (-\lambda)\, b_{jk} = (a_{ik} + \lambda a_{jk}) + (-\lambda a_{jk}) = a_{ik}.$$

Поскольку элементы получившейся матрицы, расположенные в строках, отличных от i-й, совпадают с соответствующими элементами матрицы A, то и вся она совпадает с A, так что справедливость теоремы в случае применения одного элементарного преобразования полностью доказана. Допустим теперь, что переход от A к B осуществлен с использованием t элементарных преобразований, где $t > 1$. Обозначим через C матрицу, возникшую после применения первого из этих элементарных преобразований. Тогда от C к B перешли, используя $t - 1$ элементарное преобразование. В силу индуктивного предположения, используя элементарные преобразования, можно перейти от B к C, а как установлено в начале доказательства, точно так же можно перейти и от C к A.

Таким образом, применение элементарных преобразований позволяет перейти от B к A, что и требовалось.

Полученные результаты дают возможность предложить метод решения любой системы линейных уравнений вида

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m. \end{cases}$$

Эта система однозначно определяется матрицей

$$\bar{A} = \left\| \begin{array}{cccc|c} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{array} \right\|,$$

которая называется *расширенной матрицей системы*. Матрица, стоящая левее вертикальной черты, называется *матрицей системы*.

Строка $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ считается *решением* выписанной выше системы, если для всех i справедливы числовые равенства

$$a_{i1}\alpha_1 + a_{i2}\alpha_2 + \ldots + a_{in}\alpha_n = b_i.$$

Две системы линейных уравнений называются *эквивалентными*, если всякое решение первой системы является решением второй системы и наоборот. Поэтому вместо данной системы можно решать ей эквивалентную.

Т е о р е м а 3. *Если от матрицы $\bar{A}$ к матрице $\bar{B}$ можно перейти конечным числом элементарных преобразований строк, то соответствующие системы линейных уравнений эквивалентны.*

Предварительно докажем следующую лемму.

Л е м м а. *Если от матрицы $\bar{A}$ к матрице $\bar{B}$ можно перейти конечным числом элементарных преобразований строк, то всякое решение системы, соответствующей матрице $\bar{A}$, служит решением системы, соответствующей матрице $\bar{B}$.*

Ясно, что лемму достаточно доказать для случая, когда применяется одно элементарное преобразование, ибо переход к общему случаю легко осуществляется индукцией. Если применено элементарное преобразование первого типа, т. е. переставлены местами строки, наши уравнения только меняются местами. Конечно, старые решения

по-прежнему будут им удовлетворять. При элементарных преобразованиях второго типа к i-й строке прибавляем j-ю строку, умноженную на λ. Следовательно, i-я строка матрицы $\bar{B}$ имеет вид

$$(a_{i1} + \lambda a_{j1}, \ldots, a_{in} + \lambda a_{jn} \mid b_i + \lambda b_j).$$

Пусть $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ — решение системы с матрицей $\bar{A}$, т. е. решение каждого из ее уравнений. Будет ли оно решением системы с матрицей B? Сомнение может вызвать только i-е уравнение этой системы. Но

$$(a_{i1} + \lambda a_{j1})\,\alpha_1 + \ldots + (a_{in} + \lambda a_{jn})\,\alpha_n =$$
$$= (a_{i1}\alpha_1 + \ldots + a_{in}\alpha_n) + \lambda\,(a_{j1}\alpha_1 + \ldots + a_{jn}\alpha_n) =$$
$$= b_i + \lambda b_j.$$

Переходя к доказательству теоремы, заметим, что согласно лемме каждое решение системы $\bar{A}$ (т. е. системы, соответствующей матрице $\bar{A}$) служит решением системы $\bar{B}$. С другой стороны, в силу теоремы 2 от матрицы $\bar{B}$ к матрице $\bar{A}$ можно перейти с помощью элементарных преобразований. Следовательно, применив лемму еще раз, видим, что каждое решение системы $\bar{B}$ служит решением системы $\bar{A}$. Таким образом, эти системы эквивалентны.

Теперь ясно, что для нахождения решений любой системы линейных уравнений достаточно уметь находить решения ступенчатой системы (т. е. системы, матрица которой является ступенчатой), так как любую матрицу можно привести к ступенчатому виду, а после элементарных преобразований получается эквивалентная система уравнений.

Пусть нам дана ступенчатая матрица, соответствующая системе m линейных уравнений с n неизвестными. Возможны следующие два случая.

I. Существует строка, в которой первый ненулевой элемент находится на последнем месте.

II. Такой строки нет.

В первом случае соответствующая система уравнений содержит уравнение вида $0 \cdot x_1 + \ldots + 0 \cdot x_n = b$, где $b \neq 0$. Ясно, что никакой набор значений x_i не может удовлетворять этому уравнению, а тем более всем уравнениям системы. Значит, система уравнений не имеет решений *).

*) Про систему, не имеющую решений, говорят, что она *несовместна*.

Для анализа второго случая допустим, что рассматриваемая ступенчатая матрица содержит r ненулевых строк и что первые ненулевые элементы этих строк располагаются в столбцах с номерами $k_1, \ldots, k_r$. По определению ступенчатой матрицы

$$1 \leqslant k_1 < k_2 < \ldots < k_r \leqslant n.$$

Неизвестные $x_{k_1}, \ldots, x_{k_r}$ назовем *главными*, а все остальные (если они есть) — *свободными*. Кроме того, отбросим уравнения, соответствующие нулевым строкам, что, как легко видеть, приведет к системе, эквивалентной исходной.

Допустим сначала, что свободных неизвестных нет. Тогда

$$r = n,\ k_1 = 1,\ k_2 = 2, \ldots, k_n = n$$

и рассматриваемая система имеет вид

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1\,n-1}x_{n-1} + a_{1n}x_n = b_1, \\ a_{22}x_2 + \ldots + a_{2\,n-1}x_{n-1} + a_{2n}x_n = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n-1\,n-1}x_{n-1} + a_{n-1\,n}x_n = b_{n-1}, \\ a_{nn}x_n = b_n, \end{cases}$$

причем $a_{11}, a_{22}, \ldots, a_{nn}$ отличны от нуля. Поскольку $a_{nn} \neq 0$, из последнего уравнения однозначно определяется x_n. После этого предпоследнее уравнение позволяет однозначно определить x_{n-1} и т. д. Таким образом, в выделенном случае рассматриваемая система имеет единственное решение.

Предположим теперь, что свободные неизвестные есть. В этом случае обозначим через L_i сумму свободных неизвестных, умноженных на стоящие перед нами коэффициенты i-го уравнения, и, перенося свободные неизвестные в правую часть, придем к системе

$$\begin{cases} a_{1k_1}x_{k_1} + a_{1k_2}x_{k_2} + \ldots + a_{1k_r}x_{k_r} = b_1 - L_1, \\ a_{2k_2}x_{k_2} + \ldots + a_{2k_r}x_{k_r} = b_2 - L_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{rk_r}x_{k_r} = b_r - L_r, \end{cases}$$

где коэффициенты $a_{1k_1}, a_{2k_2}, \ldots, a_{rk_r}$ отличны от нуля.

Как и выше, мы можем последовательно определять $x_{k_r}, x_{k_{r-1}}$ и т. д., если придадим свободным неизвестным какие-либо определенные значения. При этом главные

неизвестные определяются однозначно. Придавая свободным неизвестным всевозможные значения, мы найдем все решения данной системы, т. е. решим ее. Поскольку свободным неизвестным можно придавать различные значения, система в рассматриваемом случае имеет более одного решения.

Система линейных уравнений называется *однородной*, если все ее правые части равны нулю. Однородная система всегда имеет решение, например нулевую строку. Поэтому интересно выяснить, когда имеются и ненулевые решения.

Теорема 4. *Если число уравнений однородной системы линейных уравнений меньше числа неизвестных, то она имеет хотя бы одно ненулевое решение.*

Доказательство. Приведем данную однородную систему к ступенчатому виду. Разумеется, она останется однородной. Ясно, что число главных неизвестных не может превысить числа строк. Следовательно, существуют свободные неизвестные, что обеспечивает существование ненулевых решений.

Таким образом, мы располагаем методом, позволяющим решить любую систему линейных уравнений, т. е. или установить, что она не имеет решений, или указать ее единственное решение, или, выбрав свободные неизвестные, выразить через них остальные *). Однако остается неясным, не зависит ли число свободных неизвестных от способа решения. Более того, даже в случае, если такой зависимости нет, остается открытым вопрос: существует ли для данного набора неизвестных способ решения, при котором именно эти неизвестные окажутся свободными? Например, если $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ — решение системы

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 4, \\ x_1 + x_2 - x_3 + x_4 = 2, \end{cases}$$

то $\alpha_3 = 1$, т. е. неизвестное x_3 ни при каком способе решения не может оказаться свободным.

Решить эти вопросы позволяет теория, развиваемая в последующих параграфах этой главы (см. также конец § 1 гл. III). Отметим, что изучаемые в этих параграфах понятия находят широкое применение и в других вопросах, как внутриматематических, так и прикладных.

---

*) Этот метод часто называют методом Гаусса или методом последовательного исключения неизвестных.

Упражнения

1. Доказать, что элементарными преобразованиями строк и столбцов любую матрицу можно привести к диагональному виду (матрица D называется *диагональной*, если $d_{ij} = 0$ при $i \neq j$). Привести пример, показывающий, что существуют матрицы, которые нельзя привести к диагональному виду элементарными преобразованиями только строк.

2. Доказать, что, присоединяя к расширенной матрице системы линейных уравнений нулевую строку, мы получим систему линейных уравнений, эквивалентную исходной.

3. Говорят, что строка a является *линейной комбинацией* строк $a_1, \ldots, a_m$, если $a = \lambda_1 a_1 + \ldots + \lambda_m a_m$ для некоторых чисел $\lambda_1, \ldots, \lambda_m$. Доказать, что, отбросив строку расширенной матрицы системы линейных уравнений, являющуюся линейной комбинацией остальных, мы получим систему линейных уравнений, эквивалентную исходной. Использовать этот результат для решения упражнения 2.

4. Доказать, что система линейных уравнений однородна тогда и только тогда, когда нулевая строка является ее решением.

5. Сформулировать и доказать условия на элементы расширенной матрицы системы линейных уравнений с n неизвестными, необходимые и достаточные для того, чтобы всякая строка длины n служила решением этой системы.

6. Доказать аналог теоремы 2 для элементарных преобразований третьего типа, а аналоги теорем 1 и 2 — для элементарных преобразований столбцов.

7. Может ли система линейных уравнений с действительными коэффициентами иметь в точности два различных решения?

8. Доказать утверждение: если матрица B получена из матрицы A конечным числом элементарных преобразований строк, то каждая строка матрицы B является линейной комбинацией строк матрицы A. Указание: провести индукцию по числу использованных преобразований.

9. Показать, что первые ненулевые элементы строк ступенчатых матриц, полученных конечным числом элементарных преобразований строк из одной и той же матрицы, располагаются в одних и тех же столбцах. Указание: использовать упражнение 8.

§ 2. Определители

Отображение F множества квадратных матриц порядка n в множество действительных чисел называется *определителем*, если оно удовлетворяет следующим условиям.

I. Если матрица A имеет две одинаковые строки, то $F(A) = 0$.

II.

$$F\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ a'_{i1} + a''_{i1} & a'_{i2} + a''_{i2} & \ldots & a'_{in} + a''_{in} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} =$$

$$= F\left(\begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a'_{i1} & a'_{i2} & \dots & a'_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{Vmatrix}\right) + F\left(\begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a''_{i1} & a''_{i2} & \dots & a''_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{Vmatrix}\right)$$

(другими словами, если некоторая строка матрицы представлена в виде суммы двух строк, то определитель этой матрицы *) равен сумме определителей двух матриц, полученных из данной заменой строки, являющейся суммой двух строк, ее слагаемыми).

III.

$$F\left(\begin{Vmatrix} a_{11} & a_{12} & \dots a_{1n} \\ \dots & \dots & \dots \\ \lambda a_{i1} & \lambda a_{i2} & \dots \lambda a_{in} \\ \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots a_{nn} \end{Vmatrix}\right) = \lambda F\left(\begin{Vmatrix} a_{11} & a_{12} & \dots a_{1n} \\ \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots a_{in} \\ \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots a_{nn} \end{Vmatrix}\right)$$

(другими словами, числовой множитель, относящийся к строке, можно выносить за знак определителя).

IV.

$$F\left(\begin{Vmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{Vmatrix}\right) = 1.$$

Подчеркнем, что вопрос о существовании и единственности определителя пока остается для нас открытым. Однако всякое отображение F, удовлетворяющее условиям I—IV, должно обладать также следующими свойствами:

1. Если матрица A содержит нулевую строку, то $F(A) = 0$.

2. Если от матрицы A к матрице B можно перейти с помощью одного элементарного преобразования первого типа, то $F(B) = -F(A)$.

3. Если от матрицы A к матрице B можно перейти с помощью одного элементарного преобразования второго типа, то $F(B) = F(A)$.

4. Если S — ступенчатая матрица порядка n, то $F(S) = s_{11} \dots s_{nn}$, где в соответствии с нашим соглашением s_{ij} — элемент матрицы S, стоящий на пересечении i-й строки и j-го столбца.

*) Говоря «определитель матрицы A», мы имеем в виду число, соответствующее матрице A при отображении F.

Доказательство. 1. Учитывая III, имеем

$$F(A) = F\begin{pmatrix} \cdots\cdots \\ 0\ \ 0\ \ \ldots\ 0 \\ \cdots\cdots \end{pmatrix} = 0 \cdot F(A) = 0.$$

2. Предположим, что при переходе от A к B переменены местами i-я и j-я строка. Рассмотрим вспомогательную матрицу C, в которой в i-й и в j-й строках стоит сумма i-й и j-й строк матрицы A. Согласно условию I, $F(C) = 0$. Так как i-я строка выражена в виде суммы двух строк, то, вводя обозначение $\bar{a}_k = (a_{k1}, \ldots, a_{kn})$ и воспользовавшись условием II, напишем

$$0 = F(C) = F\begin{pmatrix} \cdots\cdots \\ \bar{a}_i \\ \cdots\cdots \\ \bar{a}_i + \bar{a}_j \\ \cdots\cdots \end{pmatrix}_{\substack{i \\ \\ j}} + F\begin{pmatrix} \cdots\cdots \\ \bar{a}_j \\ \cdots\cdots \\ \bar{a}_i + \bar{a}_j \\ \cdots\cdots \end{pmatrix}_{\substack{i \\ \\ j}}.$$

Во вновь полученных матрицах j-е строки представлены в виде суммы двух строк. Можно еще раз воспользоваться условием II:

$$0 = F\begin{pmatrix} \cdots \\ \bar{a}_i \\ \cdots \\ \bar{a}_i \\ \cdots \end{pmatrix}_{\substack{i \\ \\ j}} + F\begin{pmatrix} \cdots \\ \bar{a}_i \\ \cdots \\ \bar{a}_j \\ \cdots \end{pmatrix}_{\substack{i \\ \\ j}} +$$

$$+ F\begin{pmatrix} \cdots \\ \bar{a}_j \\ \cdots \\ \bar{a}_i \\ \cdots \end{pmatrix}_{\substack{i \\ \\ j}} + F\begin{pmatrix} \cdots \\ \bar{a}_j \\ \cdots \\ \bar{a}_j \\ \cdots \end{pmatrix}_{\substack{i \\ \\ j}}.$$

Отсюда с помощью условия I получим

$$0 = F(A) + F(B).$$

Следовательно,

$$F(A) = -F(B),$$

что и требовалось доказать.

3. Допустим, что матрица B получена из A прибавлением к i-й строке матрицы A ее j-й строки, умноженной на λ. Используя условия II и III и обозначения $\bar{a}_k =$

$= (a_{k1}, \ldots a_{kn})$, получаем

$$F(B) = F\left(\begin{Vmatrix} \cdot & \cdot & \cdot \\ \bar{a}_i + \lambda \bar{a}_j & & \\ \cdot & \cdot & \cdot \\ \bar{a}_j & & \\ \cdot & \cdot & \cdot \end{Vmatrix}\right) =$$

$$= F\left(\begin{Vmatrix} \cdot & \cdot & \cdot \\ \bar{a}_i & & \\ \cdot & \cdot & \cdot \\ \bar{a}_j & & \\ \cdot & \cdot & \cdot \end{Vmatrix}\right) + \lambda F\left(\begin{Vmatrix} \cdot & \cdot & \cdot \\ \bar{a}_j & & \\ \cdot & \cdot & \cdot \\ \bar{a}_j & & \\ \cdot & \cdot & \cdot \end{Vmatrix}\right) = F(A) + \lambda F\left(\begin{Vmatrix} \cdot & \cdot & \cdot \\ \bar{a}_j & & \\ \cdot & \cdot & \cdot \\ \bar{a}_j & & \\ \cdot & \cdot & \cdot \end{Vmatrix}\right).$$

Последняя матрица содержит две одинаковые строки. Значит, по условию 1 последнее слагаемое обращается в нуль, откуда $F(B) = F(A)$.

4. Пусть A — ступенчатая матрица. Если она содержит нулевую строку, то, с одной стороны, $F(A) = 0$ по свойству 1, а с другой — хотя бы одно из чисел $a_{11}, a_{22}, \ldots$ $\ldots, a_{nn}$ равно нулю, чем и доказывается справедливость свойства 4 в рассматриваемом случае. При отсутствии в матрице A нулевых строк она имеет вид

$$A = \begin{Vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ 0 & a_{22} & \ldots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & a_{nn} \end{Vmatrix},$$

где $a_{11}, a_{22}, \ldots, a_{nn} \neq 0$ (так как равенство $a_{ii} = 0$ заведомо ведет к появлению нулевой строки). Такая матрица называется *треугольной*. Прибавив к первой строке матрицы A ее последнюю строку, умноженную на $-\frac{a_{1n}}{a_{nn}}$, ко второй — последнюю строку, умноженную на $-\frac{a_{2n}}{a_{nn}}$, и т. д., добьемся того, что все элементы последнего столбца, кроме a_{nn}, обратятся в нуль. При этом элементы остальных столбцов останутся без изменения. Далее, прибавив к первой, второй и последующим строкам получившейся матрицы ее предпоследнюю строку, умноженную на подходящие числа, превратим в нули все элементы предпоследнего столбца, кроме $a_{n-1\,n-1}$. Аналогично поступая с третьим от конца столбцом и т. д., придем к

матрице

$$B = \begin{Vmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{Vmatrix}.$$

Используя свойства 3, III и IV, получаем

$$F(A) = F(B) = a_{11}a_{22} \dots a_{nn}F(E) = a_{11}a_{22} \dots a_{nn}.$$

Теорема 1 (теорема единственности). *Существует не более одной функции, удовлетворяющей условиям* I—IV.

Доказательство. Предположим, что есть две такие функции F и G. Надо доказать, что $F = G$, т. е. установить, что $F(A) = G(A)$ для любой матрицы A. В силу теоремы 1 из § 1, матрицу A можно привести к ступенчатому виду S конечным числом элементарных преобразований. Допустим, что при этом использовано k элементарных преобразований первого типа. Ввиду свойств 2, 3 и 4

$$F(A) = (-1)^k F(S) = (-1)^k s_{11}s_{22} \dots s_{nn}.$$

Поскольку те же самые соображения справедливы и для функции G, а матрица A была приведена к ступенчатому виду независимо от функций, то

$$G(A) = (-1)^k G(S) = (-1)^k s_{11}s_{22} \dots s_{nn},$$

т. е. $F(A) = G(A)$.

Теорема 2 (теорема существования). *Функция F, удовлетворяющая условиям* I—IV, *существует.*

Доказательство. Установим справедливость следующего утверждения, равносильного утверждению теоремы 2.

Для всякого натурального n существует функция F, отображающая множество квадратных матриц порядка n в множество действительных чисел и удовлетворяющая условиям I—IV.

Из него, очевидно, вытекает справедливость теоремы 2. Но такая формулировка позволяет провести индукцию по n. Для матриц первого порядка достаточно положить $F(a) = a$. Предположим, что высказанное утверждение справедливо для матриц, порядок которых меньше n. Возьмем произвольную матрицу порядка n:

$$A = \begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{Vmatrix}.$$

Матрицу, полученную из матрицы A вычеркиванием i-й строки и j-го столбца, назовем *подматрицей* матрицы A и будем обозначать через M_{ij}^{A}, а если ясно, о какой матрице A идет речь, то через M_{ij}. В силу индуктивного предположения для каждой из этих подматриц определено число $F(M_{ij})$, которое называется *минором* или, точнее, *дополнительным минором элемента* a_{ij}. Число $A_{ij} = (-1)^{i+j}F(M_{ij})$ назовем *алгебраическим дополнением* элемента a_{ij} в матрице A. Положим

$$F_i(A) = a_{1i}A_{1i} + a_{2i}A_{2i} + \ldots + a_{ni}A_{ni}$$

(пока можно ожидать, что $F_1, F_2, \ldots, F_n$ — различные функции!). Теперь зафиксируем i (т. е. номер столбца) и положим $F = F_i$. Убедимся, что функция F удовлетворяет условиям I—IV.

I. Пусть s-я и t-я строки матрицы A совпадают. Тогда во всех минорах M_{ri}, кроме M_{si} и M_{ti}, встречаются одинаковые строки. Поэтому, учитывая индуктивное предположение, имеем

$$F(A) = a_{si}A_{si} + a_{ti}A_{ti} = \\ = a_{si}(-1)^{s+i}F(M_{si}) + a_{ti}(-1)^{t+i}F(M_{ti}).$$

Допустим для определенности, что $s < t$. Тогда t-я строка матрицы A (с выброшенной координатой a_{ti}), равная ее s-й строке (с выброшенной координатой a_{si}), в матрице M_{si} располагается на $(t-1)$-м месте. Та же самая строка встречается и в матрице M_{ti}, но располагается в ней на s-м месте. Все остальные строки матриц M_{si} и M_{ti} одни и те же и располагаются в одном и том же порядке. Таким образом, для того чтобы матрицу M_{ti} превратить в матрицу M_{si}, достаточно передвинуть ее s-ю строку на $(t-1)$-е место, не меняя взаимного расположения остальных строк. Для этого придется $t-1-s$ раз менять местами соседние строки матрицы. В силу свойства 2

$$F(M_{si}) = (-1)^{t-1-s}F(M_{ti}),$$

откуда

$$F(A) = a_{si}[(-1)^{s+i+t-1-s}F(M_{ti}) + (-1)^{t+i}F(M_{ti})] = \\ = a_{si}(-1)^{i+t}(-F(M_{ti}) + F(M_{ti})) = 0.$$

II. Положим

$$A=\begin{Vmatrix} a_{11} & & a_{12} & & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a'_{s1}+a''_{s1} & & a'_{s2}+a''_{s2} & \dots & a'_{sn}+a''_{sn} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & & a_{n2} & \dots & a_{nn} \end{Vmatrix},$$

$$A'=\begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a'_{s1} & a'_{s2} & \dots & a'_{sn} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{Vmatrix} \quad \text{и} \quad A''=\begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a''_{s1} & a''_{s2} & \dots & a''_{sn} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{Vmatrix}.$$

Далее обозначим через A_{kl}, A'_{kl} и A''_{kl} алгебраические дополнения элемента, стоящего на месте (k, l) в матрицах A, A' и A'' соответственно. Аналогичные обозначения будем применять и для подматриц. Заметим, что $A_{si} = A'_{si} = A''_{si}$, так как при вычеркивании s-й строки во всех трех случаях остается одна и та же подматрица. Если же $t \neq s$, то, в силу индуктивного предположения и условия II, имеем

$$A_{ti} = (-1)^{t+i} F(M_{ti}) =$$
$$= (-1)^{t+i} (F(M'_{ti}) + F(M''_{ti})) = A'_{ti} + A''_{ti}.$$

Поэтому

$$F(A) = a_{1i}A_{1i} + \dots + (a'_{si} + a''_{si}) A_{si} + \dots + a_{ni}A_{ni} =$$
$$= a_{1i}(A'_{1i} + A''_{1i}) + \dots + (a'_{si} + a''_{si}) A_{si} + \dots$$
$$\dots + a_{ni}(A'_{ni} + A''_{ni}) = (a_{1i}A'_{1i} + \dots + a'_{si}A'_{si} + \dots$$
$$\dots + a_{ni}A'_{ni}) + (a_{1i}A''_{1i} + \dots + a''_{si}A''_{si} + \dots$$
$$\dots + a_{ni}A''_{ni}) = F(A') + F(A'').$$

III. Пусть

$$A=\begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{s1} & a_{s2} & \dots & a_{sn} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{Vmatrix} \quad \text{и} \quad A'=\begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ \lambda a_{s1} & \lambda a_{s2} & \dots & \lambda a_{sn} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{Vmatrix}.$$

Обозначения A_{kl}, A'_{kl}, M_{kl} и M'_{kl} будем использовать в том же смысле, как и выше. Тогда, учитывая индуктив-

ное предположение и условие III, получим

$$A'_{li} = \begin{cases} A_{si}, & \text{если } l = s, \\ \lambda A_{li}, & \text{если } l \neq s. \end{cases}$$

Поэтому

$$F(A') = a_{1i}A'_{1i} + \ldots + (\lambda a_{si})\,A'_{si} + \ldots + a_{ni}A'_{ni} =$$
$$= a_{1i}(\lambda A_{1i}) + \ldots + (\lambda a_{si})\,A_{si} + \ldots + a_{ni}(\lambda A_{ni}) =$$
$$= \lambda(a_{1i}A_{1i} + \ldots + a_{si}A_{si} + \ldots + a_{ni}A_{ni}) = \lambda F(A).$$

IV. Учитывая индуктивное предположение, имеем

$$F\left(\begin{Vmatrix} 1 & 0 \ldots 0 \\ 0 & 1 \ldots 0 \\ \cdot & \cdot \ldots \cdot \\ 0 & 0 \ldots 1 \end{Vmatrix}\right) = a_{11}A_{11} = 1 \cdot 1 = 1.$$

Таким образом, каждая из функций F_i удовлетворяет условиям I—IV, т. е. является определителем. Этим заканчивается доказательство теоремы 2.

Из теорем 1 и 2 вытекает, что каждой матрице A соответствует вполне определенное число $F(A)$, которое будем называть *определителем матрицы* A и обозначать через $|A|$.

Поскольку согласно теореме 1 для функций F_i, рассматривавшихся при доказательстве теоремы 2, имеем $F_1 = F_2 = \ldots = F_n$, нами заодно доказана

Т е о р е м а 3 (теорема о разложении по столбцу).

$$|A| = a_{1i}A_{1i} + \ldots + a_{ni}A_{ni}.$$

Если дана матрица $A = \| a_{ij} \|$, то условимся обозначать через A^* матрицу, определяемую условиями $a^*_{ij} = a_{ji}$. Про эту матрицу будем говорить, что она получена из матрицы A *транспонированием*. Заметим, что строки матрицы A служат столбцами матрицы A^*, а столбцы — строками.

Условимся обозначать через I*, II* и т. д. условия I, II и т. д., в которых слово «строка» заменено на «столбец». Аналогичный смысл имеют свойства 1*, 2* и т. д. Убедимся, что определитель удовлетворяет условиям I*—III* и обладает свойствами 1*—3*.

I*. Проведем доказательство индукцией по порядку матрицы. Если он равен 1, то утверждение тривиально, а для матрицы второго порядка оно проверяется непосредственным подсчетом. Если кроме двух равных столбцов имеется хотя бы еще один, то разложим определи-

тель по этому столбцу и рассмотрим алгебраические дополнения его элементов. В каждой из соответствующих подматриц остались одинаковые столбцы. Определители этих подматриц, будучи определителями порядка $n-1$, равны нулю по индуктивному предположению. Но тогда и сами алгебраические дополнения равны 0, а значит, равен нулю и определитель.

Справедливость условий II* и III* сразу следует из теоремы о разложении по столбцу.

Что касается свойств 1*—3*, то они могут быть выведены из условий I*—III* дословным повторением рассуждений, использованных при выведении свойств 1—3 из условий I—IV.

Теорема 4 (теорема о транспонировании). $|A^*| = |A|$.

Доказательство. Положим $F(A) = |A^*|$. Определенное таким образом отображение F удовлетворяет условиям I—III, поскольку эти свойства отображения F относительно строк матрицы A превращаются в условия I*—III* для определителя матрицы A^*, которые, как уже установлено, справедливы. Кроме того, $F(E) = |E^*| = |E| = 1$. В силу теоремы единственности, отображение F совпадает с определителем, т. е.

$$|A^*| = F(A) = |A|.$$

Теорема 5 (теорема о разложении по строке).

$$|A| = a_{i1}A_{i1} + \ldots + a_{in}A_{in}.$$

Доказательство. Заметим, что подматрица M^*_{ij} матрицы A^*, полученная удалением i-й строки и j-го столбца, может быть получена транспонированием подматрицы M_{ji} матрицы A, полученной удалением j-й строки и i-го столбца. В силу теоремы 4, $|M^*_{ij}| = |M_{ji}|$. Используя теоремы 3 и 4, получаем

$$\begin{aligned}|A| = |A^*| &= a^*_{1i}(-1)^{1+i}|M^*_{1i}| + \ldots \\ \ldots + a^*_{ni}(-1)^{n+i}|M^*_{ni}| &= a_{i1}(-1)^{1+i}|M_{i1}| + \ldots \\ \ldots + a_{in}(-1)^{n+i}|M_{in}| &= a_{i1}A_{i1} + \ldots + a_{in}A_{in}.\end{aligned}$$

Теорема 6 (теорема об умножении на чужие алгебраические дополнения). *Если* $i \neq j$, *то* $a_{i1}A_{j1} + \ldots + a_{in}A_{jn} = 0$ *и* $a_{1i}A_{1j} + \ldots + a_{ni}A_{nj} = 0$.

Доказательство. Достаточно заметить, что первая из сумм совпадает с разложением по j-й строке оп-

ределителя *), в котором все строки матрицы A, кроме j-й, оставлены без изменения, а вместо j-й подставлена i-я. Но такой определитель имеет две одинаковые строки и, следовательно, равен нулю по свойству I. Второе соотношение доказывается аналогично.

Теорема 7 (об определителе с нулями в правом верхнем углу). *Если A и B — квадратные матрицы, то*

$$\left|\begin{array}{c|c} A & O \\ \hline C & B \end{array}\right| = |A|\,|B|.$$

Доказательство. Обозначим через k порядок матрицы A и будем вести индукцию по числу k. Если $k = 1$, то, разложив по первой строке, получим

$$\left|\begin{array}{c|ccc} a_{11} & 0 & \dots & 0 \\ \hline a_{21} & & & \\ \vdots & & B & \\ a_{n1} & & & \end{array}\right| = a_{11}|B|,$$

что и требовалось. В общем случае, разложив определитель

$$\Delta = \left|\begin{array}{c|c} A & O \\ \hline C & B \end{array}\right|$$

по первой строке, получим

$$\Delta = a_{11}A_{11}^{\Delta} + \dots + a_{1k}A_{1k}^{\Delta},$$

где A_{is}^{Δ} означает алгебраическое дополнение элемента a_{is} в определителе Δ. Аналогично используются обозначения M_{is}^{Δ}, A_{is}^{A}, M_{is}^{A}. Имеем

$$A_{1s}^{\Delta} = (-1)^{1+s}\,|M_{1s}^{\Delta}|, \text{ где } s = 1, 2, \dots, k.$$

Правый верхний угол матрицы M_{1s}^{Δ} заполнен нулями, причем порядок матрицы, стоящей в ее левом верхнем углу, равен $k - 1$. Применив индуктивное предположение, получим

$$|M_{1s}^{\Delta}| = |M_{1s}^{A}|\,|B|.$$

*) Говоря о строках, столбцах или элементах определителя, мы имеем в виду строки, столбцы и элементы рассматриваемой матрицы.

Отсюда

$$A_{1s}^{\Delta} = (-1)^{1+s} \mid M_{1s}^{\Delta} \mid = (-1)^{1+s} \mid M_{1s}^{A} \mid \mid B \mid = A_{1s}^{A} \mid B \mid.$$

Поэтому

$$\Delta = a_{11}A_{11}^{A} \mid B \mid + a_{12}A_{12}^{A} \mid B \mid + \ldots + a_{1k}A_{1k}^{A} \mid B \mid = \\ = \mid A \mid \mid B \mid.$$

Остановимся еще на одном способе вычисления определителя. Используя разложение по первой строке, можно записать

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

и

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12}\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13}\begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix} = \\ = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - \\ - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}.$$

Таким образом, для определителей второго и третьего порядка существуют формулы, выражающие их через элементы соответствующих матриц *). Убедимся, что подобные формулы имеют место для определителей любого порядка. С этой целью рассмотрим отображение σ множества чисел $\{1, 2, \ldots, n\}$ на себя, при котором различные числа переходят в различные (т. е. если $i \neq j$, то $\sigma(i) \neq \sigma(j)$). Такое отображение называется *подстановкой* на множестве $\{1, 2, \ldots, n\}$. Подстановки σ и τ на множестве $\{1, 2, \ldots, n\}$ считаются *равными*, если $\sigma(i) = \tau(i)$ для каждого i. Подстановку σ удобно записывать в виде таблицы

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Число

$$\operatorname{sgn}\sigma = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j} = \\ = \frac{(\sigma(1) - \sigma(2)) \ldots (\sigma(1) - \sigma(n))\,(\sigma(2) - \sigma(3)) \ldots (\sigma(n-1) - \sigma(n))}{(1-2) \ldots (1-n)\,(2-3) \ldots (2-n) \ldots ((n-1) - n)}$$

*) Для запоминания этих формул удобно следующее геометрическое представление: «положительные» произведения получаются, если идти по стрелкам, изображенным на рис. 1, а «отрицательные» — на рис. 2.

называется *знаком подстановки*. Легко заметить, что абсолютная величина как числителя, так и знаменателя выписанной дроби равна $1!\,2!\,\ldots\,(n-1)!$. Следовательно, знак подстановки может быть равен 1 или -1. В первом случае подстановка называется *четной*, а во вто-

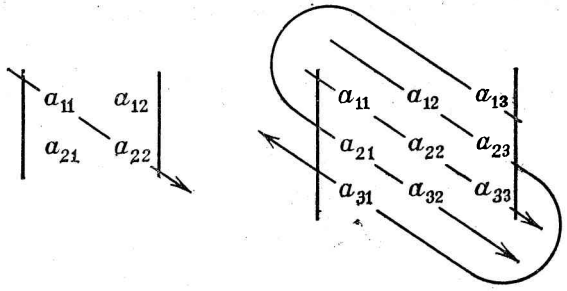


Рис. 1

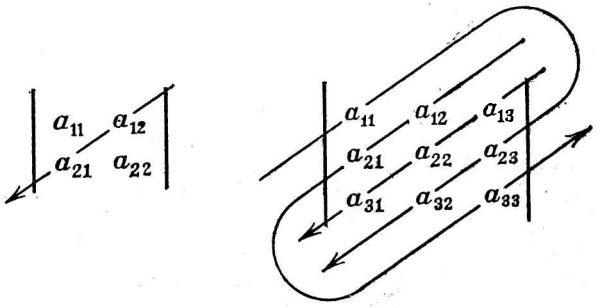


Рис. 2

ром — *нечетной*. Например, если σ задается таблицей

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

то

$$\operatorname{sgn}\sigma = \frac{3\cdot 1\cdot 2\cdot(-2)\,(-1)\cdot 1}{(-1)\,(-2)\,(-3)\,(-1)\,(-2)\,(-1)} = 1,$$

т. е. эта подстановка четная.

Скажем, что подстановки σ и τ *отличаются на транспозицию* (i, j), если

$$\sigma(k) = \begin{cases} \tau(k), & \text{если } k \neq i, j, \\ \tau(j), & \text{если } k = i, \\ \tau(i), & \text{если } k = j. \end{cases}$$

При записи этих подстановок в виде таблицы нетрудно заметить, что одна из них получается из другой переменой местами чисел, стоящих на i-м и j-м местах нижней строки.

Теорема 8. *Если подстановки* σ *и* τ *отличаются на транспозицию* (i, j), *то* $\operatorname{sgn}\sigma = -\operatorname{sgn}\tau$.

Доказательство. Группируя сомножители, получим

$$\operatorname{sgn}\sigma = \prod_{\substack{1\leqslant k<l\leqslant n\\ k\neq i,\ j\\ l\neq i,\ j}} \frac{\sigma(k)-\sigma(l)}{k-l}\cdot\prod_{\substack{1\leqslant k\leqslant n\\ k\neq i,\ j}}\left(\frac{\sigma(i)-\sigma(k)}{i-k}\cdot\frac{\sigma(j)-\sigma(k)}{j-k}\right)\cdot$$

$$\cdot\frac{\sigma(i)-\sigma(j)}{i-j} = \prod_{\substack{1\leqslant k<l\leqslant n\\ k\neq i,\ j\\ l\neq i,\ j}} \frac{\tau(k)-\tau(l)}{k-l}\cdot$$

$$\cdot\prod_{\substack{1\leqslant k\leqslant n\\ k\neq i,\ j}}\left(\frac{\tau(j)-\tau(k)}{i-k}\cdot\frac{\tau(i)-\tau(k)}{j-k}\right)\cdot\frac{\tau(j)-\tau(i)}{i-j} =$$

$$= \prod_{\substack{1\leqslant k<l\leqslant n\\ k\neq i,\ j\\ l\neq i,\ j}} \frac{\tau(k)-\tau(l)}{k-l}\cdot\prod_{\substack{1\leqslant k\leqslant n\\ k\neq i,\ j}}\left(\frac{\tau(j)-\tau(k)}{j-k}\cdot\frac{\tau(i)-\tau(k)}{i-k}\right)\cdot$$

$$\cdot\frac{\tau(i)-\tau(j)}{i-j}\cdot(-1) = (-1)\operatorname{sgn}\tau.$$

Возможен (и обычно используется) несколько иной подход к определению четности подстановки. Именно: говорят, что пара $(\sigma(i), \sigma(j))$, где σ — подстановка на множестве $\{1, 2, \ldots, n\}$ и $i<j$, образует инверсию, если $\sigma(i)>\sigma(j)$. После этого четность подстановки определяется как четность числа инверсий в ней. Убедимся, что это определение совпадает с нашим. В самом деле, пара $(\sigma(i), \sigma(j))$ образует инверсию тогда и только тогда, когда

$$\frac{\sigma(i)-\sigma(j)}{i-j}<0,$$

и, следовательно, $\operatorname{sgn}\sigma = (-1)^t$, где t — число инверсий в подстановке σ.

Теорема 9. $|A| = \sum_{\sigma}\operatorname{sgn}\sigma\, a_{1\sigma(1)}\ldots a_{n\sigma(n)}$, *где* σ *пробегает все подстановки на множестве чисел* $\{1, 2, \ldots, n\}$.

Доказательство. Рассмотрим функцию

$$F(A) = \sum_{\sigma}\operatorname{sgn}\sigma\, a_{1\sigma(1)}\ldots a_{n\sigma(n)}$$

и убедимся, что она удовлетворяет условиям I—IV. Тогда из теоремы о единственности определителя будем иметь $F(A) = |A|$, что и требуется. Начнем с проверки последнего условия.

IV. Пусть $A = E$. Если подстановка $\sigma \neq \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$, то $\sigma(i) \neq i$ для некоторого i. Поэтому произведение $a_{1\sigma(1)} \dots a_{n\sigma(n)}$ содержит элемент $a_{i\sigma(i)} = 0$ и, следовательно, равно нулю. Значит, остается только одно слагаемое, т. е.

$$F(A) = \operatorname{sgn} \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} a_{11} a_{22} \dots a_{nn} = 1.$$

III. Если матрица A' получена из A умножением s-й строки на λ, то

$$F(A') = \sum_{\sigma} \operatorname{sgn} \sigma \, a_{1\sigma(1)} \dots (\lambda a_{s\sigma(s)}) \dots a_{n\sigma(n)} =$$

$$= \lambda \sum_{\sigma} \operatorname{sgn} \sigma \, a_{1\sigma(1)} \dots a_{s\sigma(s)} \dots a_{n\sigma(n)} = \lambda F(A).$$

II. Если A, A' и A'' имеют тот же смысл, что и на с. 22, то

$$F(A) = \sum_{\sigma} \operatorname{sgn} \sigma \, a_{1\sigma(1)} \dots (a'_{s\sigma(s)} + a''_{s\sigma(s)}) \dots a_{n\sigma(n)} =$$

$$= \sum_{\sigma} \operatorname{sgn} \sigma \, a_{1\sigma(1)} \dots a'_{s\sigma(s)} \dots a_{n\sigma(n)} +$$

$$+ \sum_{\sigma} \operatorname{sgn} \sigma \, a_{1\sigma(1)} \dots a''_{s\sigma(s)} \dots a_{n\sigma(n)} = F(A') + F(A'').$$

I. Допустим, что s-я строка матрицы A совпадает с t-й, причем $s < t$. Возьмем четную подстановку

$$\begin{pmatrix} 1 & \dots & s & \dots & t & \dots & n \\ \sigma(1) & \dots & \sigma(s) & \dots & \sigma(t) & \dots & \sigma(n) \end{pmatrix}.$$

Этой подстановке соответствует произведение

$$a_{1\sigma(1)} \dots a_{s\sigma(s)} \dots a_{t\sigma(t)} \dots a_{n\sigma(n)}. \qquad (*)$$

Рассмотрим подстановку τ, полученную из σ применением транспозиции (s, t). Согласно теореме 8, подстановка τ нечетная и, следовательно, ей соответствует произведение

$$-a_{1\tau(1)} \dots a_{s\tau(s)} \dots a_{t\tau(t)} \dots a_{n\tau(n)}. \qquad (**)$$

Согласно определению транспозиции, $\sigma(i) = \tau(i)$, если $i \neq s$, t, $\sigma(s) = \tau(t)$ и $\sigma(t) = \tau(s)$. Отсюда, поскольку s-я строка матрицы A равна ее t-й строке, имеем $a_{i\sigma(i)} = a_{i\tau(i)}$, если $i \neq s$, t, $a_{s\sigma(s)} = a_{t\sigma(s)} = a_{t\tau(t)}$ и $a_{t\sigma(t)} = a_{s\sigma(t)} = a_{s\tau(s)}$. Следовательно, произведения (*) и (**) отличаются только знаком. Поэтому их сумма равна нулю. Допустим, что таким образом перебраны все четные

подстановки. Если сумма

$$\sum_{\sigma} \operatorname{sgn} \sigma \, a_{1\sigma(1)} \ldots a_{n\sigma(n)}$$

отлична от нуля, то должна остаться нерассмотренной какая-то нечетная подстановка. Но применив к ней транспозицию (s, t), придем к нерассмотренной четной подстановке. Полученное противоречие завершает доказательство.

Упражнения

1. Если F и G — две функции со свойствами I — III и $G(A) \neq 0$ для некоторой матрицы A, то существует такое число λ, что $F(X) = \lambda G(X)$ для любой матрицы X.

2. Определитель матрицы A равен нулю тогда и только тогда, когда хотя бы одна из ее строк (или столбцов) является линейной комбинацией остальных.

3. Если A — матрица нечетного порядка и $A^* = -A$ (через $-A$ обозначена матрица, полученная из A изменением знака всех ее элементов на противоположный), то $|A| = 0$.

4. Сформулировать и доказать для определителя свойство столбцов, аналогичное свойству 4 для строк.

5. Какова связь между определителями матрицы A и матрицы, полученной из строк (столбцов) матрицы A, расположенных в обратном порядке (т. е. первая строка (столбец) ставится на последнее место, вторая — на предпоследнее и т. д.)?

6. Чему равен определитель, у которого сумма строк с четными номерами равна сумме строк с нечетными номерами?

7. Доказать, что существует $n!$ различных подстановок на множестве $\{1, 2, \ldots, n\}$. Указание: провести индукцию по n.

8. Чему равно произведение знаков всех подстановок на множестве $\{1, 2, \ldots, n\}$?

§ 3. Алгебра матриц

Если в матрице A отметить какие-нибудь k строк и k столбцов, то элементы, стоящие на пересечении отмеченных строк и столбцов, образуют квадратную матрицу порядка k — *подматрицу* матрицы A. Определитель каждой из таких матриц называется *минором* порядка k матрицы A. Таким образом, миноры, о которых говорилось в § 2, оказываются минорами порядка $n - 1$ в смысле данного определения. Наивысший порядок отличных от нуля миноров матрицы A называется ее *рангом*. Разумеется, ранг матрицы размера $m \times n$ не превосходит наименьшего из чисел m и n. Заметим, что у нулевой матрицы ненулевых миноров нет. Поэтому ее ранг естественно положить равным нулю.

Теорема 1. *Ранг ступенчатой матрицы равен числу ее ненулевых строк.*

Доказательство. Пусть ступенчатая матрица A содержит r ненулевых строк. Тогда, отметив ненулевые строки и столбцы, в которых располагаются первые ненулевые элементы этих строк, получим треугольную матрицу. Ее определитель равен произведению диагональных элементов, отличных от нуля, и, следовательно, отличен от нуля, так что матрица A содержит ненулевой минор порядка r. Всякий же минор большего порядка содержит нулевую строку и поэтому обращается в нуль. Таким образом, ранг$A = r$.

Теорема 2. ранг A = ранг A^*.

Доказательство. Пусть ранг $A = r$. Рассмотрим в матрице A^* произвольный минор порядка $s > r$. Пусть он является определителем подматрицы M. Тогда M^* — подматрица матрицы A^*. Поскольку ее порядок больше r, то минор $|M^*| = 0$, а значит, и $|M| = 0$ (см. теорему 4 из § 2). Таким образом, все миноры матрицы A^*, порядок которых больше r, обращаются в нуль. Следовательно, ранг $A^* \leqslant r =$ ранг A. Это же неравенство для матрицы A^* дает ранг $A =$ ранг $A^{**} \leqslant$ ранг A^*. Таким образом, ранг $A^* \leqslant$ ранг $A \leqslant$ ранг A^*, т. е. ранг $A =$ ранг A^*.

Теорема 3. *Ранг матрицы не меняется при элементарных преобразованиях строк (столбцов).*

Сначала будет доказана

Лемма. *Если от матрицы A к матрице B можно перейти конечным числом элементарных преобразований строк, то* ранг $B \leqslant$ ранг A.

Доказательство леммы будем вести индукцией по числу примененных элементарных преобразований. Допустим, что использовано только одно элементарное преобразование. Пусть ранг $A = r$. Для доказательства леммы достаточно убедиться, что всякий минор $|M|$ матрицы B порядка, большего чем r, равен нулю. Если от матрицы A к матрице B перешли переменой местами двух строк, то подматрица M либо совпадает с некоторой подматрицей M' матрицы A, порядок которой больше чем r, либо отличается от такой подматрицы M' только порядком строк. Поскольку ранг $A = r$, то $|M'| = 0$, а значит, $|M| = \pm |M'| = 0$. Допустим теперь, что переход к матрице B осуществлен прибавлением к i-й строке матрицы A ее j-й строки, умноженной на λ. Возможны три случая: 1) i-я строка не проходит через под-

матрицу M; 2) как i-я, так и j-я строки проходят через подматрицу M; 3) i-я строка проходит через подматрицу M, а j-я не проходит. В первом случае подматрица M совпадает с соответствующей подматрицей матрицы A и, следовательно, $|M| = 0$. Во втором случае имеем

$$|M| = \begin{vmatrix} \cdots\cdots\cdots\cdots \\ a_{ik_1} + \lambda a_{jk_1} \cdots a_{ik_s} + \lambda a_{jk_s} \\ \cdots\cdots\cdots\cdots \\ a_{jk_1} \cdots a_{jk_s} \\ \cdots\cdots\cdots\cdots \end{vmatrix} = \begin{vmatrix} \cdots\cdots \\ a_{ik_1} \cdots a_{ik_s} \\ \cdots\cdots \\ a_{jk_1} \cdots a_{jk_s} \\ \cdots\cdots \end{vmatrix} = 0,$$

ибо последний определитель является минором матрицы A. В третьем случае запишем

$$|M| = \begin{vmatrix} \cdots\cdots\cdots\cdots \\ a_{ik_1} + \lambda a_{jk_1} \cdots a_{ik_s} + \lambda a_{jk_s} \\ \cdots\cdots\cdots\cdots \end{vmatrix} =$$

$$= \begin{vmatrix} \cdots\cdots \\ a_{ik_1} \cdots a_{ik_s} \\ \cdots\cdots \end{vmatrix} + \lambda \begin{vmatrix} \cdots\cdots \\ a_{jk_1} \cdots a_{jk_s} \\ \cdots\cdots \end{vmatrix}.$$

Но первый из этих определителей является минором матрицы A, а второй лишь порядком строк отличается от некоторого минора матрицы A. Следовательно, оба этих определителя равны нулю, откуда $|M| = 0$. Таким образом, для случая, когда использовано лишь одно элементарное преобразование, лемма доказана. Допустим, что использовано m преобразований. Пусть C — матрица, полученная после осуществления $m - 1$ преобразования. Учитывая индуктивное предположение, имеем

$$\text{ранг } B \leqslant \text{ранг } C \leqslant \text{ранг } A,$$

что и требовалось.

Доказательство теоремы. Допустим, что от матрицы A к матрице B перешли конечным числом элементарных преобразований строк. Ввиду леммы ранг $B \leqslant$ $\leqslant$ ранг A. Но если элементарные преобразования позволяют перейти от A к B, то, согласно теореме 2 из § 1, от B к A также можно перейти конечным числом элементарных преобразований. Еще раз применяя лемму, получаем, что ранг $A \leqslant$ ранг B. Нужное равенство сразу следует из полученных неравенств. Справедливость теоремы для столбцов легко вывести из теоремы 2.

Теорема 4 (теорема Кронекера—Капелли). *Система линейных уравнений совместна* (*т. е. имеет решение*)

тогда и только тогда, когда ранг матрицы системы равен рангу ее расширенной матрицы.

Доказательство. Поскольку, согласно теоремам 1 и 3 из § 1, от каждой системы линейных уравнений можно перейти к эквивалентной ей ступенчатой системе, а ранги матрицы системы и ее расширенной матрицы, в силу теоремы 3, при этом меняться не будут, то достаточно установить справедливость теоремы 4 для ступенчатой системы. Для ступенчатой же системы, в силу теоремы 1, ранги матрицы системы и ее расширенной матрицы равны тогда и только тогда, когда эти матрицы имеют одинаковое число ненулевых строк, или, что то же самое, тогда и только тогда, когда первый ненулевой элемент последней ненулевой строки расширенной матрицы не располагается в столбце свободных членов. Из анализа ступенчатой системы, проведенного в § 1, известно, что это имеет место тогда и только тогда, когда система совместна.

Теорема 5. *Совместная система линейных уравнений от n неизвестных с матрицей A имеет единственное решение тогда и только тогда, когда* ранг $A = n$.

Доказательство. В силу теорем 1 и 3 ранг $A = n$ тогда и только тогда, когда данная система приводится к треугольному виду (т. е. к системе с треугольной матрицей). С другой стороны, ступенчатая система имеет единственное решение в том и только том случае, когда она треугольна.

Следствие. *Однородная система n линейных уравнений с n неизвестными обладает ненулевыми решениями тогда и только тогда, когда определитель этой системы равен нулю.*

Когда в § 1 мы говорили о главных и свободных неизвестных, эти понятия зависели от способа приведения расширенной матрицы системы к ступенчатому виду. Для решения задач, обсуждавшихся в конце § 1, необходимо иметь определение, зависящее лишь от данной системы линейных уравнений. С этой целью, если дана система линейных уравнений относительно неизвестных $x_1, \ldots, x_n$, условимся говорить, что неизвестные $x_{i_1}, \ldots, x_{i_k}$ *можно объявить главными*, если при любом задании остальных неизвестных значения этих неизвестных определяются однозначно. Про эти остальные неизвестные будем говорить, что их *можно объявить свободными*. Подчеркнем, что в последних двух фразах определяются термины «можно объявить главными» и «можно объявить свободными», а не понятия «главное неизвестное»

и «свободное неизвестное». Неизвестные становятся главными или свободными лишь после того, как мы, реализуя имеющуюся возможность, объявим их таковыми. Ясно, что главные и свободные неизвестные в смысле, определенном в § 1, можно объявить такими и в смысле нового определения.

Центральным результатом нашей теории является

Теорема 6. *Пусть имеется совместная система m линейных уравнений с n неизвестными, $\bar{A}$ — расширенная матрица этой системы и ранг $\bar{A} = r$. Тогда неизвестные $x_{i_1}, \ldots, x_{i_k}$ можно объявить главными в том и только том случае, когда $k = r$ и в столбцах матрицы $\bar{A}$ с номерами $i_1, \ldots, i_k$ располагается ненулевой минор порядка r.*

Доказательство. Допустим, что $k = r$ и что в столбцах с указанными номерами располагается ненулевой минор порядка r. Тогда ранг матрицы

$$\begin{Vmatrix} a_{1i_1} & a_{1i_2} & \ldots & a_{1i_r} \\ a_{2i_1} & a_{2i_2} & \ldots & a_{2i_r} \\ \ldots & \ldots & \ldots & \ldots \\ a_{mi_1} & a_{mi_2} & \ldots & a_{mi_r} \end{Vmatrix}$$

размера $m \times r$ равен r. В силу теорем 1 и 3, приведя эту матрицу к ступенчатому виду, получим матрицу

$$\begin{Vmatrix} b_{1i_1} & b_{1i_2} & \ldots & b_{1i_r} \\ 0 & b_{2i_2} & \ldots & b_{2i_r} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & b_{ri_r} \\ 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 \end{Vmatrix},$$

где $b_{1i_1}, b_{2i_2}, \ldots, b_{ri_r} \neq 0$. Применив те же самые элементарные преобразования к матрице $\bar{A}$, получим матрицу

$$\bar{B} = \left\| \begin{array}{ccccccc|c} \ldots & b_{1i_1} & \ldots & b_{1i_2} & \ldots & b_{1i_r} & \ldots & c_1 \\ \ldots & 0 & \ldots & b_{2i_2} & \ldots & b_{2i_r} & \ldots & c_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & 0 & \ldots & 0 & \ldots & b_{ri_r} & \ldots & c_r \\ \ldots & 0 & \ldots & 0 & \ldots & 0 & \ldots & c_{r+1} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & 0 & \ldots & 0 & \ldots & 0 & \ldots & c_m \end{array} \right\|.$$

Подчеркнем, что эта запись не означает, что все строки матрицы $\bar{B}$, начиная с $(r+1)$-й, нулевые: в столбах с номерами, отличными от $i_1, i_2, \ldots, i_r$, могут встретиться ненулевые элементы, стоящие в этих строках. Однако на самом деле все строки матрицы $\bar{B}$, начиная с $(r+1)$-й, нулевые. Действительно, допустим, что это не так, т. е. $b_{pq} \neq 0$ для некоторых p и q, где $r+1 \leqslant p \leqslant m$. Конечно, $q \neq i_1, \ldots, i_r$. Однако может случиться, что $q = n+1$, т. е. $b_{pq} = c_p$. Пусть M — минор матрицы $\bar{B}$ порядка $r+1$, расположенный в строках с номерами $1, 2, \ldots, r$, p и столбцах с номерами $i_1, \ldots, i_r, q$. Переставляя, если нужно, столбцы этого минора, получим

$$M = \pm \begin{vmatrix} b_{1i_1} & b_{1i_2} & \ldots & b_{1i_r} & b_{1q} \\ 0 & b_{2i_2} & \ldots & b_{2i_r} & b_{2q} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & b_{ri_r} & b_{rq} \\ 0 & 0 & \ldots & 0 & b_{pq} \end{vmatrix} = \pm b_{1i_1} \ldots b_{ri_r} b_{pq} \neq 0.$$

Но тогда

$$\text{ранг } \bar{A} = \text{ранг } \bar{B} \geqslant r+1,$$

что противоречит условию. Таким образом, система линейных уравнений, соответствующая матрице $\bar{B}$, эквивалентна исходной системе и содержит r уравнений, не считая уравнений вида $0x_1 + \ldots + 0x_n = 0$. Придавая неизвестным, отличным от $x_{i_1}, \ldots, x_{i_r}$, произвольные значения и перенося их в правую часть, легко убедиться, что неизвестные $x_{i_1}, \ldots, x_{i_r}$ однозначно определяются одно за другим, начиная с последнего. Таким образом, их можно объявить главными.

Допустим теперь, что неизвестные $x_{i_1}, \ldots, x_{i_k}$ можно объявить главными. Положив остальные неизвестные равными нулю, придем к системе

$$\begin{cases} a_{1i_1}x_{i_1} + \ldots + a_{1i_k}x_{i_k} = b_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{mi_1}x_{i_1} + \ldots + a_{mi_k}x_{i_k} = b_m. \end{cases} \qquad (*)$$

имеющей единственное решение. В силу теоремы 5, ранг матрицы этой системы равен k. Следовательно, $k \leqslant r$ и в столбцах $i_1, \ldots, i_k$ располагается ненулевой минор порядка k. Допустим, что $k < r$. Заметим, что система $(*)$ приводится к треугольному виду, и применим к исходной системе те же самые элементарные преобразования. Тогда

расширенная матрица системы приобретает вид

$$\left\|\begin{array}{ccccccccc|c}
\dots & b_{1i_1} & \dots & b_{1i_2} & \dots & b_{1i_k} & \dots & & & c_1 \\
\dots & 0 & \dots & b_{2i_2} & \dots & b_{2i_k} & \dots & & & c_2 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & & & \dots \\
\dots & 0 & \dots & 0 & \dots & b_{ri_k} & \dots & & & c_r \\
\dots & 0 & \dots & 0 & \dots & 0 & \dots & & & c_{r+1} \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & & & \dots \\
\dots & 0 & \dots & 0 & \dots & 0 & \dots & & & c_m
\end{array}\right\|$$

В силу теоремы Кронекера — Капелли, ранг матрицы системы равен $r > k$. Поэтому среди строк $(b_{i1}, \dots, b_{in})$, где $k < i \leqslant m$, есть ненулевые. Следовательно, найдется $b_{pq} \neq 0$, где $p > k$. Если теперь положить равными нулю все неизвестные с номерами, отличными от $i_1, \dots, i_k, q$, то получим $x_q = c_p/b_{pq}$. Следовательно, x_q не может быть взят произвольным, что противоречит возможности объявить $x_{i_1}, \dots, x_{i_k}$ главными неизвестными. Следовательно, $k = r$, чем и завершается доказательство.

Пример. В системе

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 4, \\ x_1 + x_2 - x_3 + x_4 = 2 \end{cases}$$

главными можно объявить следующие пары неизвестных: (x_1, x_3), (x_2, x_3), (x_3, x_4). Пары же (x_1, x_2), (x_1, x_4) и (x_2, x_4) объявить главными нельзя.

Пусть даны матрица A размера $m \times n$ и матрица B размера $n \times p$. Другими словами, число столбцов матрицы A равно числу строк матрицы B. *Произведением* AB матриц A и B называется матрица C размера $m \times p$, элементы которой вычисляются по следующему правилу:

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \quad (i = 1, \dots, m;\ j = 1, \dots, p).$$

Подчеркнем, что в соответствии с этим определением (и в отличие от чисел) произведение двух матриц существует не всегда. Целесообразность предложенного определения подтверждается дальнейшим развитием теории, излагаемой в настоящем параграфе и в гл. III. Попутно заметим, что рассмотрение произведения матриц оказывается полезным во многих вопросах теоретической и прикладной математики.

Теорема 7. $(AB)C = A(BC)$ и $(AB)^* = B^*A^*$ (написанные равенства означают, в частности, что правая и левая части каждого из них существуют одновременно).

Доказательство. Сначала убеждаемся, что из существования левой части каждого из этих равенств следует существование правой и наоборот. Например, если существует произведение $(AB)C$, то матрицы A и B имеют размеры $m \times n$ и $n \times p$ соответственно. Но тогда AB имеет размеры $m \times p$, откуда вытекает, что матрица C должна иметь размеры $p \times q$. После этого ясно, что произведение BC существует и имеет размеры $n \times q$. Но тогда существует и произведение $A(BC)$. При этом как $(AB)C$, так и $A(BC)$ имеют размеры $m \times q$. Далее полагаем $U = AB$, $V = BC$, $S = (AB)C$, $T = A(BC)$ и убеждаемся, что

$$s_{ij} = \sum_{l=1}^{p} u_{il}c_{lj} = \sum_{l=1}^{p}\sum_{k=1}^{n} a_{ik}b_{kl}c_{lj} = \sum_{k=1}^{n}\sum_{l=1}^{p} a_{ik}b_{kl}c_{lj} =$$

$$= \sum_{k=1}^{n} a_{ik}\left(\sum_{l=1}^{p} b_{kl}c_{lj}\right) = \sum_{k=1}^{n} a_{ik}v_{kj} = t_{ij}.$$

Этим доказано первое равенство. Для доказательства второго положим $C = AB$ и $D = B^*A^*$. Как и выше, нетрудно убедиться, что произведение $D = B^*A^*$ существует и что матрицы C и D имеют одинаковые размеры. Кроме того,

$$c^*_{ij} = c_{ji} = \sum_{k=1}^{n} a_{jk}b_{ki} = \sum_{k=1}^{n} a^*_{kj}b^*_{ik} = \sum_{k=1}^{n} b^*_{ik}a^*_{kj} = d_{ij},$$

что и требовалось.

Хотя для произведения нескольких чисел и употреблялась запись $a_1 \ldots a_n$, она, строго говоря, бессмысленна, ибо определено лишь произведение двух чисел. Да и, в самом деле, для того, чтобы вычислить это произведение, мы всегда (правда, мысленно) расставляли скобки. Употребление же приведенной выше записи объясняется тем, что результат вычисления не зависит от расстановки скобок. Докажем аналогичный результат для матриц, что даст нам возможность использовать запись $A_1 \ldots A_n$ без скобок.

Теорема 8. *Пусть произведение матриц*

$$K = A_1(A_2(\ldots(A_{n-1}A_n)\ldots))$$

существует. Тогда произведение $A_1 \ldots A_n$ *существует при любой расстановке скобок, сводящей вычисление к вы-*

числению произведений, содержащих лишь два сомножителя, и всякий раз равно K.

Доказательство. Произведение одного или двух сомножителей скобок не содержит, и потому справедливость доказываемой теоремы тривиальна. Для трех сомножителей это утверждение совпадает с первой частью теоремы 7. Допустим, что теорема доказана, если число сомножителей меньше n. Рассмотрим произведение $A_1 \ldots A_n$ с некоторой расстановкой скобок. Выделяя скобки, соответствующие последнему умножению, имеем следующие варианты:

$$B_1 = A_1 (A_2 \ldots A_n),$$
$$B_2 = (A_1 A_2)(A_3 \ldots A_n),$$
$$\ldots\ldots\ldots\ldots$$
$$B_{n-1} = (A_1 \ldots A_{n-1}) A_n.$$

Разумеется, предполагается, что внутри данных скобок задана некоторая расстановка скобок. Ясно, что $B_1 = K$, ибо в силу индуктивного предположения произведение $A_2 \ldots A_n$ от расстановки скобок не зависит. Допустим, что доказаны равенства

$$K = B_1 = \ldots = B_{i-1}.$$

Тогда

$$\begin{aligned} B_{i-1} &= (A_1 \ldots A_{i-1})(A_i A_{i+1} \ldots A_n) = \\ &= (A_1 \ldots A_{i-1})(A_i (A_{i+1} \ldots A_n)) = \\ &= ((A_1 \ldots A_{i-1}) A_i)(A_{i+1} \ldots A_n) = \\ &= (A_1 \ldots A_i)(A_{i+1} \ldots A_n) = B_i \end{aligned}$$

в силу теоремы 7 и индуктивного предположения. Продолжая этот процесс, убедимся, что

$$K = B_1 = \ldots = B_{n-1}.$$

А это и требовалось.

Теорема 9. *Умножение матрицы A слева (справа) на диагональную матрицу*

$$D = \begin{Vmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & d_n \end{Vmatrix}$$

равносильно умножению строк (столбцов) матрицы A на элементы $d_1, d_2, \ldots, d_n$ соответственно.

Доказательство. Если $DA = C$, то

$$c_{ij} = \sum_{k=1}^{n} d_{ik}a_{kj} = d_{ii}a_{ij} = d_i a_{ij}$$

для каждого i. Утверждение, касающееся столбцов, доказывается аналогично.

Следствие. *Если*

$$E = \begin{Vmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{Vmatrix},$$

то $AE = A$ *и* $EB = B$ *всякий раз, когда умножение возможно.*

Следствие объясняет, почему матрица E была названа единичной.

Назовем *элементарными* матрицы, полученные из матрицы E применением одного элементарного преобразования. Это будут матрицы вида

$$S(i,j) = \begin{array}{c} \\ i \\ \\ j \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccc} & & & i & & j & \\ \end{array} \\ \begin{Vmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & 0 & & 1 & \\ & & & & 1 & & \\ & & & 1 & & 0 & \\ & & & & & & 1 \end{Vmatrix} \end{array}, \qquad T(i,j,\lambda) = \begin{array}{c} \\ i \\ \\ j \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccc} & & i & & j \\ \end{array} \\ \begin{Vmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & \dots & \lambda \\ & & \dots & \ddots & \dots \\ & & 0 & \dots & 1 \end{Vmatrix} \end{array}$$

Формально эти матрицы могут быть описаны так:

$$s_{pq} = \begin{cases} 1, & \text{если } p = q \neq i, j, \\ 1, & \text{если } p = i,\ q = j \text{ или } p = j,\ q = i, \\ 0 & \text{в остальных случаях;} \end{cases}$$

$$t_{pq} = \begin{cases} 1, & \text{если } p = q, \\ \lambda, & \text{если } p = i,\ q = j, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Примерами элементарных матриц служат

$$S(2,4) = \begin{Vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{Vmatrix} \text{ и } T(2,4,\lambda) = \begin{Vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & \lambda & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{Vmatrix}.$$

Теорема 10. *Умножение матрицы A на матрицу $S(i, j)$ слева (справа) равносильно перемене местами i-й и j-й строк (i-го и j-го столбцов).*

Доказательство. Положив $C = S(i, j)A$, будем иметь

$$c_{pq} = \sum_k s_{pk}a_{kq} = \begin{cases} s_{ij}a_{jq} = a_{jq}, & \text{если } p = i, \\ s_{ji}a_{iq} = a_{iq}, & \text{если } p = j, \\ s_{pp}a_{pq} = a_{pq}, & \text{если } p \neq i, j. \end{cases}$$

Утверждение, касающееся столбцов, доказывается аналогично.

Теорема 11. *Умножение матрицы A на матрицу $T(i, j, \lambda)$ слева (справа) равносильно прибавлению к i-й строке (j-му столбцу) матрицы A ее j-й строки (i-го столбца), умноженной на λ.*

Доказательство. Положив $C = T(i, j, \lambda)A$, будем иметь

$$c_{pq} = \sum_k t_{pk}a_{kq} = \begin{cases} t_{ii}a_{iq} + t_{ij}a_{jq} = a_{iq} + \lambda a_{jq}, & \text{если } p = i, \\ t_{pp}a_{pq} \qquad\qquad = a_{pq}, & \text{если } p \neq i. \end{cases}$$

Утверждение, касающееся столбцов, доказывается аналогично.

Таким образом, применение элементарных преобразований к строкам матрицы равносильно ее умножению слева на элементарные матрицы.

Теорема 12. *Ранг произведения не превосходит рангов сомножителей.*

Доказательство. Допустим, что матрица A имеет размеры $m \times n$, а B — размеры $n \times p$. Докажем сначала, что (ранг AB) $\leqslant$ (ранг A). Это очевидно, если (ранг A) $= m$, ибо матрица AB имеет размеры $m \times p$. Если же (ранг A) $= r < m$, то приведем матрицу A к ступенчатому виду S, используя элементарные преобразования строк. Ввиду теорем 8, 10 и 11 можем записать

$$S = U_1 \ldots U_k A,$$

где $U_1, \ldots, U_k$ — элементарные матрицы. Но тогда

$$SB = U_1 \ldots U_k AB,$$

и теоремы 10 и 11 позволяют заключить, что от матрицы AB к матрице SB можно перейти, осуществляя элементарные преобразования строк. В силу теоремы 3

$$\text{ранг } SB = \text{ранг } AB.$$

Далее, из теорем 1 и 3 вытекает, что все строки матрицы S, начиная с $(r+1)$-й, нулевые. Простой подсчет показывает, что то же самое верно и для строк матрицы SB. Следовательно,

$$\text{ранг } AB = \text{ранг } SB \leqslant r = \text{ранг } A.$$

Теперь, учитывая теоремы 2 и 7, а также доказанное неравенство, получаем

$$\text{ранг } AB = \text{ранг } (AB)^* = \text{ранг } B^*A^* \leqslant \text{ранг } B^* = \text{ранг } B.$$

Теорема 13. *Если A — квадратная матрица порядка n и $|A| \neq 0$, то существует одна и только одна матрица B такая, что $AB = BA = E$.*

Доказательство. Как известно, производя элементарные преобразования над строками, можно от матрицы A перейти к некоторой диагональной матрице D (см. рассуждения, использованные при доказательстве свойства 4 на с. 19). Ввиду теорем 10 и 11

$$D = U_1 \ldots U_k A,$$

где $U_1, \ldots, U_k$ — элементарные матрицы. С другой стороны, согласно теореме 3, имеем

$$\text{ранг } D = \text{ранг } A = n,$$

т. е. $|D| \neq 0$. Следовательно,

$$D = \begin{Vmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & d_n \end{Vmatrix},$$

где все d_i отличны от 0. Положим

$$U = \begin{Vmatrix} d_1^{-1} & 0 & \ldots & 0 \\ 0 & d_2^{-1} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & d_n^{-1} \end{Vmatrix}$$

и $B = UU_1 \ldots U_k$. Учитывая теорему 8, получим

$$BA = UU_1 \ldots U_k A = UD = E.$$

Но $|A^*| \neq 0$. В силу доказанного

$$CA^* = E$$

для некоторой матрицы C. Ввиду теоремы 7

$$AC^* = (CA^*)^* = E^* = E,$$

Отсюда

$$B = BE = BAC^* = EC^* = C^*,$$

т. е.

$$AB = E = BA.$$

Если $AX = E = XA$ для какой-нибудь матрицы X, то

$$X = XE = XAB = EB = B,$$

чем доказывается единственность матрицы B.

Матрица B, рассмотренная в теореме 13, называется *обратной* *) для матрицы A и обозначается через A^{-1}.

Заметим, что в качестве A^{-1} можно взять матрицу

$$B = \begin{Vmatrix} \frac{A_{11}}{|A|} & \frac{A_{21}}{|A|} & \cdots & \frac{A_{n1}}{|A|} \\ \frac{A_{12}}{|A|} & \frac{A_{22}}{|A|} & \cdots & \frac{A_{n2}}{|A|} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{A_{1n}}{|A|} & \frac{A_{2n}}{|A|} & \cdots & \frac{A_{nn}}{|A|} \end{Vmatrix},$$

где через A_{ij} обозначено алгебраическое дополнение элемента a_{ij} в матрице A. Действительно, если $C = AB$ и $D = BA$, то, учитывая теоремы 3, 5 и 6 из § 2, получаем

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} = \frac{1}{|A|} \sum_{k=1}^{n} a_{ik} A_{jk} = \begin{cases} 1, & \text{если } i = j, \\ 0, & \text{если } i \neq j, \end{cases}$$

и

$$d_{ij} = \sum_{k=1}^{n} b_{ik} a_{kj} = \frac{1}{|A|} \sum_{k=1}^{n} A_{ki} a_{kj} = \begin{cases} 1, & \text{если } i = j, \\ 0, & \text{если } i \neq j. \end{cases}$$

Таким образом, $C = D = E$, т. е. $B = A^{-1}$. Этим еще раз доказано существование обратной для всякой матрицы с ненулевым определителем.

Рассуждения, приведенные при доказательстве теоремы 13, можно использовать и для получения еще одного способа вычисления обратной матрицы. Действительно, мы имеем равенство

$$UU_1 \ldots U_k A = E.$$

---

*) Матрицу, определитель которой отличен от нуля (равен нулю), обычно называют *невырожденной* (*вырожденной*). Поэтому теорему 13 можно сформулировать так: *каждая невырожденная матрица имеет обратную, и притом только одну.* Устанавливаемому ниже следствию теоремы 14 можно придать такую форму: *вырожденная матрица не имеет обратной.*

Умножая его справа на A^{-1}, получим

$$UU_1 \ldots U_k E = A^{-1}.$$

Это равенство показывает, что для вычисления матрицы A^{-1} достаточно применить к матрице E те же элементарные преобразования, которые применялись к матрице A при превращении ее в единичную. Поэтому, преобразуя матрицу $(A \mid E)$ размера $n \times 2n$ так, чтобы матрица A превратилась в единичную, придем к матрице $(E \mid A^{-1})$.

Т е о р е м а 14. *Если A и B — квадратные матрицы, то* $|AB| = |A|\,|B|$.

Д о к а з а т е л ь с т в о. Допустим сначала, что $|A| = 0$. Ввиду теоремы 12 (ранг AB) $\leqslant$ (ранг A) $<$ (порядок A) = (порядок AB). Следовательно, $|AB| = 0 = |A|\,|B|$, что и требовалось. Теперь можно считать, что $|A| \neq 0$. Допустим, что A диагональна, т. е.

$$A = \begin{Vmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & d_n \end{Vmatrix}.$$

Учитывая теорему 9 и свойство III определителя, получаем

$$|AB| = \begin{vmatrix} d_1 b_{11} & \ldots & d_1 b_{1n} \\ \ldots & \ldots & \ldots \\ d_n b_{n1} & \ldots & d_n b_{nn} \end{vmatrix} = d_1 \ldots d_n |B| = |A|\,|B|.$$

Переходя к общему случаю, вспомним (см. с. 19), что элементарными преобразованиями строк матрицу A с ненулевым определителем можно привести к диагональному виду D. При этом $|A| = (-1)^k |D|$, где k — число осуществленных при этом приведении перемен местами строк. В силу теорем 8, 10 и 11 имеем $D = UA$, где U — произведение элементарных матриц. Если к матрице AB применить те же самые элементарные преобразования, то получим матрицу $U(AB)$, причем $|U(AB)| = (-1)^k |AB|$. Учитывая, что в случае диагональной матрицы A теорема верна, имеем

$$|AB| = (-1)^k |U(AB)| = (-1)^k |DB| = (-1)^k |D|\,|B| = |A|\,|B|,$$

что и требовалось.

С л е д с т в и е. *Если $|A| = 0$, то матрица A не имеет обратной.*

Действительно, если $|A| = 0$ и $AB = E$, то

$$0 = |A|\,|B| = |AB| = |E| = 1,$$

что невозможно.

Умножение матриц можно использовать для получения *правила Крамера*, позволяющего решать системы линейных уравнений. Нетрудно понять, что всякая система линейных уравнений может быть записана в форме, использующей произведение матриц:

$$A\begin{Vmatrix} x_1 \\ \cdots \\ x_n \end{Vmatrix} = \begin{Vmatrix} b_1 \\ \cdots \\ b_n \end{Vmatrix}, \qquad (*)$$

где A — матрица системы, а $\begin{Vmatrix} x_1 \\ \cdots \\ x_n \end{Vmatrix}$ и $\begin{Vmatrix} b_1 \\ \cdots \\ b_n \end{Vmatrix}$ — столбцы, состоящие из неизвестных и свободных членов соответственно. Допустим, что A — квадратная матрица, причем $|A| \neq 0$. Тогда рассмотрим столбец

$$C = A^{-1}\begin{Vmatrix} b_1 \\ \cdots \\ b_n \end{Vmatrix}.$$

Если этим столбцом заменить столбец неизвестных, то уравнения системы (*) обращаются в тождества. Следовательно, столбец C является решением системы (*). Если столбец D также является решением, то имеем $AC = \begin{Vmatrix} b_1 \\ \cdots \\ b_n \end{Vmatrix} = AD$. Умножая слева на A^{-1}, получаем $C = D$, чем доказана единственность решения. Наконец, обозначая через u_{ij} элементы матрицы A^{-1}, получим формулы для вычисления значений неизвестных:

$$x_i = c_i = \sum_{k=1}^{n} u_{ik}b_k = \sum_{k=1}^{n} \frac{A_{ki}}{|A|}\,b_k =$$

$$= \frac{\sum\limits_{k=1}^{n} b_k A_{ki}}{|A|} = \frac{\begin{vmatrix} a_{11} & \ldots & b_1 & \ldots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \ldots & b_n & \ldots & a_{nn} \end{vmatrix}}{|A|},$$

где $b_1, \ldots, b_n$ располагаются в i-м столбце. Это и есть правило Крамера.

Как и для строк, для двух матриц A и B одинакового размера можно определить их сумму $C = A + B$ как матрицу того же размера, где $c_{ij} = a_{ij} + b_{ij}$. Можно определить и произведение λA матрицы A на действительное число λ как матрицу того же размера, элементами которой служат числа λa_{ij}. Так же, как для строк, легко проверяются следующие свойства:

$$A + B = B + A, \qquad \lambda (A + B) = \lambda A + \lambda B,$$
$$(A + B) + C = A + (B + C), \qquad (\lambda + \mu) A = \lambda A + \mu A,$$
$$A + 0 = 0 + A = A, \qquad (\lambda\mu) A = \lambda (\mu A),$$
$$1A = A$$

уравнение $A + X = 0$ разрешимо,

(здесь A, B, C — матрицы, а λ и μ — числа). Замечания по поводу смысла используемых знаков, высказанные в примечании **) на с. 7, сохраняют свою силу и здесь. Умножение и сложение связаны дистрибутивными законами:

$$A (B + C) = AB + AC \text{ и } (A + B) C = AC + BC,$$

причем из существования одной из частей этих равенств следует существование другой. Допустим, например, что существует $A (B + C)$. Тогда матрицы A, B и C должны иметь размеры $m \times n$, $n \times p$ и $n \times p$ соответственно. Но тогда произведения AB и AC существуют и имеют размеры $m \times p$, а значит, существует и их сумма. Элементами, стоящими на месте (i, j) в левой и правой частях этого равенства, служат суммы

$$\sum_k a_{ik} (b_{kj} + c_{kj})$$

и

$$\sum_k a_{ik} b_{kj} + \sum_k a_{ik} c_{kj},$$

совпадающие ввиду свойств операций над действительными числами.

Без труда проверяются и равенства

$$\lambda (AB) = (\lambda A) B = A (\lambda B).$$

Упражнения

1. Доказать, что ранг матрицы не меняется при элементарных преобразованиях столбцов первого и второго типа. Изменяется ли ранг матрицы при элементарных преобразованиях третьего типа?

2. Доказать, что, применяя элементарные преобразования строк и столбцов всех трех типов, любую матрицу ранга r можно превратить в такую матрицу D, что $d_{11} = \ldots = d_{rr} = 1$, а на всех остальных местах стоят нули.

3. Если A и B — матрицы с одинаковым числом столбцов (строк), то

$$\text{ранг}\left\|\begin{matrix}A\\B\end{matrix}\right\| \leqslant \text{ранг } A + \text{ранг } B$$

$$(\text{ранг}\,\|\,A\;\;B\,\|) \leqslant \text{ранг } A + \text{ранг } B.$$

4. Если A и B — матрицы порядка n, то $AB - BA \neq E$. Указание: вычислить суммы диагональных элементов матриц AB и BA.

5. Если $|A|, |B| \neq 0$, то $(AB)^{-1} = B^{-1}A^{-1}$.

6. Если $|A| \neq 0$, то $(A^*)^{-1} = (A^{-1})^*$.

7. Если A и B — ненулевые матрицы порядка n и $AB = O$, то $|A| = |B| = 0$ (здесь утверждается больше, чем «$|A| = 0$ или $|B| = 0$»!).

8. Если $|A| = 0$, то определитель матрицы, составленной из алгебраических дополнений элементов матрицы A, также равен нулю.

9. Если $|A| \neq 0$, то ранг AB = ранг B и ранг CA = ранг C всякий раз, когда эти произведения существуют.

10. ранг $(A + B) \leqslant$ ранг $A +$ ранг B. Указание: использовать упражнение 3.

11. Если A — матрица размера $m \times n$ и ранг $A = m$, то существует такая матрица B, что

$$AB = \left\|\begin{matrix}1 & 0 & \ldots & 0 & 0 & \ldots & 0\\ 0 & 1 & \ldots & 0 & 0 & \ldots & 0\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\ 0 & 0 & \ldots & 1 & 0 & \ldots & 0\end{matrix}\right\|.$$

12. Если A — матрица размера $m \times n$ и ранг $A = m$, то существует такая матрица B, что $AB = E$.

13. Если A — матрица размера $m \times n$ и ранг $A = n$, то существует такая матрица B, что $BA = E$.

14. Любую матрицу A ранга r можно представить в виде суммы r матриц ранга 1 и нельзя представить в виде суммы меньшего числа таких матриц. Указание: представить матрицу A в виде $A = US$, где S — ступенчатая матрица, затем матрицу S представить как сумму r однострочных матриц и воспользоваться теоремой о ранге произведения.

15. Решить систему линейных уравнений:

$$\begin{cases} x_1 + x_2 = 0,\\ x_2 + x_3 = 0,\\ \ldots\ldots\ldots\\ x_{n-1} + x_n = 0,\\ x_n + x_1 = 0. \end{cases}$$

ГЛАВА II

ЭЛЕМЕНТЫ ОБЩЕЙ АЛГЕБРЫ

Под общей алгеброй понимается часть алгебры, занимающаяся изучением алгебраических систем, т. е. множеств, на которых заданы те или иные операции и отношения. В настоящей главе излагаются определения и простейшие свойства таких алгебраических систем, как полугруппы и группы, кольца и модули, структуры (решетки) и булевы алгебры.

§ 1. Отображения и операции

Скажем, что задано *отображение* φ из множества A в множество B, если каждому элементу из множества A поставлен в соответствие некоторый вполне определенный элемент из множества B. Подчеркнем, что данное высказывание не является определением. Понятие отображения является неопределяемым. Для обозначения отображения φ из A в B употребляются символы $\varphi\colon A \to B$ и $A \xrightarrow{\varphi} B$. Если $a \in A$, то поставленный ему в соответствие элемент из B будем обозначать через $\varphi(a)$ и называть его *образом элемента* a при отображении φ. Если $b \in B$, то всякий элемент a из A, для которого справедливо равенство $b = \varphi(a)$, называется *прообразом* элемента b. Множество A называется *началом* отображения φ, а множество B — его *концом*. Разумеется, каждый элемент из начала отображения φ имеет в точности один образ. Однако не у каждого элемента из конца этого отображения должен быть прообраз. С другой стороны, конец отображения может содержать элементы, имеющие несколько прообразов. Например, если A — множество действительных чисел и φ: $A \to A$, где $\varphi(x) = x^2$, то 1 и -1 служат прообразами элемента 1, а -1 прообразов не имеет. Подмножество конца отображения φ, состоящее из всех его элементов, имеющих прообраз (или, другими словами, таких элементов b, что $b = \varphi(a)$ для некоторого $a \in A$), называется *образом отображения* φ и обозначается $\operatorname{Im}\varphi$. Отображе-

ние φ считается *равным* отображению ψ, если начала и концы этих отображений совпадают и для каждого элемента x, принадлежащего их общему началу, справедливо равенство $\varphi(x) = \psi(x)$. Подчеркнем, что с точки зрения этого определения отображения $\varphi\colon A \to A$ и $\psi\colon A \to B$, где A — множество всех действительных чисел, B — множество положительных действительных чисел и $\varphi(x) = \psi(x) = 2^x$ для всех $x \in A$, различны.

Отображение $\varphi\colon A \to B$ называется *вложением*, если каждый элемент из B имеет не более одного прообраза, т. е. $\varphi(a') = \varphi(a'')$ влечет за собой $a' = a''$. Если каждый элемент из B имеет хотя бы один прообраз (или, другими словами, если $\operatorname{Im}\varphi = B$), то отображение φ называется *наложением*. Имея наложение $\varphi\colon A \to B$, часто говорят, что φ — отображение A *на* B. Отображение, являющееся одновременно вложением и наложением, называется *взаимно однозначным* *). Примером взаимно однозначного отображения служат подстановки, являющиеся отображениями множества $\{1, 2, \ldots, n\}$ на себя и рассматривавшиеся в конце § 2 гл. I. Важным примером взаимно однозначного отображения является *тождественное* отображение множества A на себя, определяемое условием: $\varphi(x) = x$ для всех $x \in A$. Это отображение будем обозначать через 1_A. Одним из таких отображений является *тождественная подстановка*

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

Если конец отображения φ совпадает с началом отображения ψ, то можно определить *произведение* $\varphi\psi$ **). Именно, если $\varphi\colon A \to B$, а $\psi\colon B \to C$, то $\varphi\psi$, по определению, отображает A в C, причем $\varphi\psi(x) = \psi(\varphi(x))$ для каждого $x \in A$. Предложенное определение выглядит более естественным, если образ элемента x при отображении φ записывать не как $\varphi(x)$, а как $x\varphi$. Тогда имеем $x(\varphi\psi) = (x\varphi)\psi$. Эта запись выглядит как ассоциативный закон, но это чисто внешнее сходство. В дальнейшем, если мы не имеем дела с умножением отображений, часто будем использовать и запись $\varphi(x)$. Если $\varphi\colon A \to B$, то

*) Вложение часто называют *инъективным отображением*, наложение — *сюръективным*, а взаимно однозначное отображение — *биективным*.

**) Заметим, что многие авторы говорят в этом случае о произведении $\psi\varphi$. Если стать на эту точку зрения, то формулировка некоторых результатов изменяется.

легко проверяется справедливость равенств $1_A\varphi = \varphi = \varphi 1_B$. Ассоциативность произведения отображений формулируется следующим образом.

Теорема 1. *Если* φ, ψ *и* χ — *отображения, то* $(\varphi\psi)\chi = \varphi(\psi\chi)$ (написанное равенство означает, в частности, что его левая и правая части существуют одновременно).

Доказательство. Пусть левая часть существует и φ: $A \to B$. Ввиду существования произведения $\varphi\psi$ имеем ψ: $B \to C$. Из определения произведения вытекает, что $\varphi\psi$: $A \to C$. Существование левой части дает χ: $C \to D$, после чего последовательно получаем $(\varphi\psi)\chi$: $A \to D$, $\psi\chi$: $B \to D$ и $\varphi(\psi\chi)$: $A \to D$. Таким образом, из существования левой части вытекает существование правой, причем начала и концы отображений, стоящих в этих частях, совпадают. К аналогичным выводам можно прийти, предполагая существование правой части. Если теперь $a \in A$, то, используя определение произведения, получаем цепочку равенств

$$a((\varphi\psi)\chi) = (a(\varphi\psi))\chi = ((a\varphi)\psi)\chi = (a\varphi)(\psi\chi) = a(\varphi(\psi\chi)).$$

Ввиду произвольности a это доказывает теорему.

Повторяя почти дословно доказательство теоремы I.3.8 *), можно установить следующий факт.

Теорема 2. *Если произведение отображений* $\varphi_1, \varphi_2, \ldots, \varphi_n$ *существует при некоторой расстановке скобок, то оно существует и при любой другой расстановке скобок, причем результат не зависит от выбора этой расстановки.*

Этот результат позволяет использовать запись $\varphi_1\varphi_2 \ldots \varphi_n$ не расставляя скобок.

Замечание. Если φ и ψ — отображения множества A в себя, то существуют как $\varphi\psi$, так и $\psi\varphi$. Однако, вообще говоря, эти произведения не совпадают. Например, если

$$\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{и} \quad \psi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

то

$$\varphi\psi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \text{но} \quad \psi\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Следующие две теоремы позволяют охарактеризовать вложение и наложение, используя свойства некоторых произведений.

*) Это означает, что имеется в виду теорема 8 из § 3 гл. I.

Теорема 3. *Отображение* φ *является вложением тогда и только тогда, когда из каждого равенства вида* $\psi\varphi = \chi\varphi$, *где* ψ *и* χ — *некоторые отображения, вытекает, что* $\psi = \chi$.

Доказательство. Пусть $\varphi\colon A \to B$ — вложение и $\psi\varphi = \chi\varphi$. Тогда как ψ, так и χ отображают некоторое множество C в A. Если $c \in C$, то имеем $(c\psi)\,\varphi = c\,(\psi\varphi) = c\,(\chi\varphi) = (c\chi)\,\varphi$. Поскольку φ — вложение, отсюда вытекает, что $c\psi = c\chi$. Ввиду произвольности c это означает, что $\psi = \chi$. Допустим теперь, что для отображения φ справедлива указанная в формулировке импликация, но φ не является вложением. Тогда найдутся a', $a'' \in A$ такие, что $a' \neq a''$, но $a'\varphi = a''\varphi$. Рассмотрим отображения ψ и χ множества A в себя, определяемые условиями $a\psi = a'$ и $a\chi = a''$ для всех $a \in A$. Тогда для всех $a \in A$ имеем

$$a\,(\psi\varphi) = (a\psi)\,\varphi = a'\varphi = a''\varphi = (a\chi)\,\varphi = a\,(\chi\varphi).$$

Следовательно, $\psi\varphi = \chi\varphi$, откуда, в силу условия, вытекает $\psi = \chi$, что невозможно.

Теорема 4. *Отображение* φ *является наложением тогда и только тогда, когда из каждого равенства вида* $\varphi\psi = \varphi\chi$, *где* ψ *и* χ — *некоторые отображения, вытекает, что* $\psi = \chi$.

Доказательство. Пусть $\varphi\colon A \to B$ — наложение и $\varphi\psi = \varphi\chi$. Тогда как ψ, как и χ отображают B в некоторое множество C. Если $b \in B$, то, поскольку φ — наложение, имеем $b = a\varphi$ для некоторого $a \in A$. Отсюда

$$b\psi = (a\varphi)\,\psi = a\,(\varphi\psi) = a\,(\varphi\chi) = (a\varphi)\,\chi = b\chi,$$

что ввиду произвольности элемента b влечет $\psi = \chi$. Допустим теперь, что для ψ справедлива указанная в формулировке импликация, но φ не является наложением. Тогда найдется элемент $b \in B$ такой, что $a\varphi \neq b$ для всех $a \in A$. Зафиксируем в B элемент $b_0 \neq b$ и рассмотрим отображение $\psi\colon B \to B$, определяемое условием:

$$x\psi = \begin{cases} x, & \text{если } x \neq b, \\ b_0, & \text{если } x = b. \end{cases}$$

Ясно, что $\psi \neq 1_B$, что в силу условия влечет $\varphi\psi \neq \varphi 1_B$. Однако для всех $a \in A$ имеем

$$a\,(\varphi\psi) \qquad (a\varphi)\,\psi = a\varphi = (a\varphi)\,1_B = a\,(\varphi 1_B).$$

Противоречие.

Непосредственным подсчетом или с использованием теорем 3 и 4 может быть доказана

Теорема 5. *Если* φ *и* ψ — *вложения, наложения или взаимно однозначные отображения, то то же самое справедливо и для произведения* $\varphi\psi$.

Если φ: $A \to B$ — взаимно однозначное отображение, то можно определить отображение φ^{-1}: $B \to A$, приняв за $y\varphi^{-1}$ для каждого $y \in B$ прообраз элемента y при отображении φ. Это определение имеет смысл, ибо каждый элемент из B имеет прообраз и притом только один. Обозначение объясняется следующей теоремой *).

Теорема 6. *Если* φ — *взаимно однозначное отображение множества* A *на множество* B, *то* $\varphi\varphi^{-1} = 1_A$ *и* $\varphi^{-1}\varphi = 1_B$.

Доказательство. Ясно, что $\varphi\varphi^{-1}$ отображает A в себя, а $\varphi^{-1}\varphi$ отображает B в себя. Если $x \in A$ и $x\varphi = y$, то

$$x(\varphi\varphi^{-1}) = (x\varphi)\varphi^{-1} = y\varphi^{-1} = x = x1_A$$

и

$$y(\varphi^{-1}\varphi) = (y\varphi^{-1})\varphi = x\varphi = y = y1_B.$$

Ввиду произвольности элемента x из A, первое равенство влечет $\varphi\varphi^{-1} = 1_A$. Соотношение $\varphi^{-1}\varphi = 1_B$ вытекает из второго равенства, если принять во внимание, что каждый элемент y из B может быть записан как $y = x\varphi$ для некоторого $x \in A$.

Система Σ непустых подмножеств множества A называется *разбиением*, если каждый элемент из A принадлежит одному и только одному подмножеству системы. Подмножества, входящие в разбиение, называются *смежными классами* разбиения. Смежный класс разбиения Σ, содержащий элемент a, условимся обозначать через $[a]_\Sigma$ или — если ясно, о каком разбиении идет речь,— через $[a]$. Множество смежных классов разбиения Σ множества A называется *фактормножеством* множества A по разбиению Σ и обозначается через A/Σ.

Примеры. **1.** A — множество зерен, насыпанных в мешки, Σ — система подмножеств, каждое из которых есть множество всех зерен, насыпанных в данный мешок, A/Σ — множество мешков.

2. A — множество всех целых чисел, A_0 и A_1 — множества всех четных и нечетных чисел соответственно, Σ состоит из A_0 и A_1, A/Σ — двухэлементное множество, элементами которого

*) По той же причине отображение φ^{-1} называют *обратным* отображению φ.

служат A_0 и A_1. При этом, например, $[0] = [2] = [300] = [-4] = A_0$, а $[1] = [-1] = [205] = A_1$.

3. Пусть A — множество всех действительных чисел. Положим $A_0 = \{0\}$, а для каждого положительного α образуем двухэлементное множество $A_\alpha = \{\alpha, -\alpha\}$. Ясно, что система Σ, состоящая из A_0 и всех A_α, является разбиением. Фактормножество A/Σ можно отождествить с множеством неотрицательных действительных чисел, отображая смежный класс A_α на число α.

Отображение π, при котором каждому элементу из A ставится в соответствие смежный класс, в котором этот элемент лежит, называется *естественным*. Ясно, что естественное отображение является наложением.

В рассмотренных выше примерах имеем: 1) $\pi(x)$ — мешок, в котором лежит зерно x; 2) $\pi(x) = A_0$, если x чётное, и $\pi(x) = A_1$, если x нечетное; 3) $\pi(x)$ — двухэлементное множество $\{x, -x\}$, если $x \neq 0$, и $\pi(0)$ — множество, состоящее из одного нуля.

Пусть теперь $\varphi\colon A \to B$ — наложение. Обозначим через A_b, где $b \in B$, множество всех прообразов элемента b. Нетрудно проверить, что система подмножеств $\{A_b \mid b \in B\}$ является разбиением множества A. Это разбиение называется *ядром отображения* φ и обозначается через $\operatorname{Ker}\varphi$.

Теорема 7 («теорема о гомоморфизме» для множеств). *Если* $\varphi\colon A \to B$ — *наложение и* $\pi\colon A \to A/\operatorname{Ker}\varphi$ — *естественное отображение, то существует взаимно однозначное отображение* $\chi\colon B \to A/\operatorname{Ker}\varphi$ *такое, что* $\varphi\chi = \pi$ (см. рис. 3).

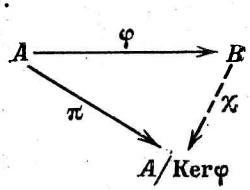


Рис. 3

Доказательство. Если $a \in A$, то $a\pi$ обозначает смежный класс разбиения $\operatorname{Ker}\varphi$, которому этот элемент a принадлежит. Если $b \in B$, то, поскольку φ — наложение, $b = a\varphi$ для некоторого $a \in A$. Положим $b\chi = a\pi$. Предложенное определение отображения χ корректно, т. е. не зависит от случайного выбора элемента a. В самом деле, если $b = a'\varphi$, то $a\pi = a'\pi$ в силу определения разбиения $\operatorname{Ker}\varphi$. Таким образом, χ оказывается

Таблица 1

	Множество	Операция	Справедливы ли законы: ассоциативный	Справедливы ли законы: коммутативный	Единица	Обратный элемент
1	Все действительные числа	Сложение	Да	Да	0	$-x$
2	Все действительные числа	Умножение	Да	Да	1	x^{-1}, если $x \neq 0$, 0 не имеет обратного
3	Действительные числа, отличные от нуля	Умножение	Да	Да	1	x^{-1}
4	Все целые числа	Сложение	Да	Да	0	$-x$
5	Все целые числа	Вычитание	Нет	Нет	Нет	Бессмысленно
6	Неотрицательные целые числа	Сложение	Да	Да	0	Имеется только у нуля
7	Квадратные матрицы порядка $n \geqslant 2$	Умножение	Да	Нет	E	Имеется только у невырожденных матриц*)
8	Невырожденные матрицы *) порядка $n \geqslant 2$	Умножение **)	Да	Нет	E	A^{-1}
9	Матрицы размера $m \times n$	Сложение	Да	Да	O	$-A$
10	Квадратные матрицы порядка n	$AB + BA$	Нет	Да	$\frac{1}{2}E$	$\frac{1}{4}A^{-1}$, если $\lvert A\rvert \neq 0$; обратного нет, если $\lvert A\rvert = 0$
11	Все отображения множества в себя	Умножение (см. § 1)	Да	Нет	Тождественное	Имеется только у взаимно однозначных отображений
12	Взаимно однозначные отображения множества на себя	Умножение	Да	Нет	Тождественное	Обратное отображение
13	Слова	Приписывание (ср. с. 67)	Да	Нет	Пустое слово	Имеется только у пустого слова
14	Векторы пространства, начинающиеся в фиксированной точке	Векторное умножение	Нет	Нет	Нет	Бессмысленно

*) Квадратная матрица называется *невырожденной*, если ее определитель отличен от нуля.
**) Заметим, что, ввиду теоремы I.3.14, произведение невырожденных матриц является невырожденной матрицей.

отображением из B в $A/\mathrm{Ker}\,\varphi$. Если $a \in A$, то

$$a(\varphi\chi) = (a\varphi)\chi = a\pi,$$

т. е. $\varphi\chi = \pi$. Если $b'\chi = b''\chi$, то, выбрав a', $a'' \in A$ так, что $b' = a'\varphi$ и $b'' = a''\varphi$, заметим, что $a'\pi = a''\pi$. В силу определения разбиения $\mathrm{Ker}\,\varphi$, отсюда вытекает, что

$$b' = a'\varphi = a''\varphi = b''.$$

Следовательно, χ — вложение. Наконец, произвольный элемент из $A/\mathrm{Ker}\,\varphi$ имеет вид $a\pi$, где $a \in A$. Поэтому уже доказанное равенство $a\pi = (a\varphi)\chi$ показывает, что χ — наложение. Таким образом, χ — взаимно однозначное отображение, что и требовалось.

Если A — некоторое множество, то обозначим через $A \times A$ множество всех пар вида (a, b), где $a, b \in A$. *Операцией* на множестве A называется всякое отображение множества $A \times A$ в множество A. Образ пары (a, b) называют *произведением* и обозначают через ab. Иногда вместо «произведения» говорят «сумма» и пишут $a + b$. Используются и другие обозначения (например, $a \circ b$, $a * b$ и т. п.). Многочисленные примеры множеств с разнообразными операциями собраны в таблицу 1.

Элемент $e \in A$ называется *единицей* (относительно данной операции), если $ae = ea = a$ для всех $a \in A$. Единица существует не всегда. Однако:

Теорема 8. *Множество с заданной операцией содержит не более одной единицы.*

Доказательство. Пусть e и f — единицы. Поскольку e — единица, то $ef = f$. Но $ef = e$, поскольку f — единица. Таким образом,

$$f = ef = e.$$

Если операцию называют сложением, то единицу обычно называют *нулем* и обозначают 0.

Если $(ab)c = a(bc)$ для любых $a, b, c \in A$, то операция называется *ассоциативной*, а если $ab = ba$ для всех $a, b \in A$, то *коммутативной*.

Если множество A с заданной операцией содержит единицу e, то элемент $b \in A$ называется *обратным элементу* $a \in A$, если $ab = ba = e$.

Теорема 9. *Если множество A с заданной ассоциативной операцией содержит единицу e, то каждый элемент из A имеет не более одного обратного.*

Доказательство. Пусть b и c — обратные элементу a. Тогда, учитывая определения единицы и об-

ратного элемента, имеем

$$b = be = b\,(ac) = (ba)\,c = ec = c.$$

Замечание. Требование ассоциативности существенно. Действительно, рассмотрим трехэлементное множество $\{e, a, b\}$ с умножением, задаваемым таблицей

$\cdot$	e	a	b
e	e	a	b
a	a	e	e
b	b	e	e

Здесь e — единица, а как a, так и b являются обратными к a.

Упражнения

1. Рассмотрим следующие отображения φ: $A \to B$:

	A	B	$\varphi(x)$
1	Целые числа	$\{0, 1\}$	0, если x четное, 1, если x нечетное
2	Действительные числа	Отрезок $[0, 1]$	Дробная часть числа x
3	Действительные числа	Целые числа	Целая часть числа x
4	Квадратные матрицы	Действительные числа	Определитель матрицы x
5	Целые числа	$\{0, 1\}$	0 для всех x
6	Целые числа	$\{0\}$	0 для всех x
7	Матрицы размера $m \times n$	Действительные числа	Сумма всех элементов матрицы x
8	Матрицы размера $m \times n$	n-мерные строки	Первая строка матрицы x

Какие из этих отображений являются наложениями (вложениями)? Найти ядра этих отображений. Рассмотреть факторможество по ядру и указать отображение χ, упоминаемое в формулировке теоремы 7.

2. Если $\varphi\psi$ — вложение, то φ — вложение.

3. Если $\varphi\psi$ — наложение, то ψ — наложение.

4. Пусть V — множество всех n-мерных строк, A — квадратная матрица порядка n и φ — отображение множества V в себя, задаваемое равенством

$$\varphi\,(x_1, \ldots, x_n) = (x_1, \ldots, x_n)\,A.$$

Доказать эквивалентность следующих утверждений: а) $|A| \neq 0$; б) φ — вложение; в) φ — наложение; г) φ — взаимно однозначное отображение.

5. Рассмотрим следующие операции на множестве A:

	Множество	Операция xy
1	Положительные целые числа	x^y
2	Матрицы порядка n	$xy - yx$
3	Неотрицательные целые числа	н. о. д. (x, y)
4	Неотрицательные целые числа	н. о. к. (x, y)
5	Неотрицательные целые числа	$\min(x, y)$
6	Произвольное множество	x

В примерах 3 и 4 считается, что 0 делится на 0. Какие из этих операций ассоциативны или коммутативны? В каких случаях существуют единица и обратные элементы?

§ 2. Полугруппы

Непустое множество A с заданной на нем ассоциативной операцией называется *полугруппой*. Все множества с операциями, приведенные в таблице 1, кроме 5, 10 и 14, оказываются полугруппами.

Рассуждения, применявшиеся для доказательства теоремы I.3.8 и теоремы 2 из § 1 позволяют доказать следующее:

Теорема 1. *Произведение нескольких элементов полугруппы не зависит от расстановки скобок.*

Этот результат позволяет использовать запись $a_1a_2 \ldots a_n$, не расставляя скобок. Заметим, что, в отличие от произведения матриц и отображений, это произведение существует всегда. Поэтому вышеупомянутые теоремы I.3.8 и 2 из §1 не являются следствиями теоремы 1.

Если операция полугруппы A не только ассоциативна, но и коммутативна, то полугруппа A называется *коммутативной* (или *абелевой*). Полугруппы 1, 2, 3, 4, 6, 9 из таблицы 1 коммутативны.

Теорема 2. *Если* $a_1, \ldots, a_n$ — *такие элементы полугруппы, что* $a_ia_j = a_ja_i$ *для любых* i *и* j, *то*

$$a_1a_2 \ldots a_n = a_{\sigma(1)}a_{\sigma(2)} \ldots a_{\sigma(n)},$$

где σ — *произвольная подстановка на множестве* $\{1, 2, \ldots, n\}$.

Доказательство. При $n = 2$ утверждение теоремы справедливо по условию. Допустим, что теорема верна для $n - 1$ сомножителей. Если $\sigma(n) = n$, то, учитывая теорему 1 и индуктивное предположение, имеем

$$a_{\sigma(1)} \ldots a_{\sigma(n-1)}a_n = (a_{\sigma(1)} \ldots a_{\sigma(n-1)})\, a_n = a_1 \ldots a_{n-1}a_n.$$

Если $n = \sigma(k)$, где $k < n$, то

$$a_{\sigma(1)} \ldots a_{\sigma(k-1)} a_n a_{\sigma(k+1)} \ldots a_{\sigma(n)} =$$
$$= (a_{\sigma(1)} \ldots a_{\sigma(k-1)})(a_n (a_{\sigma(k+1)} \ldots a_{\sigma(n)})) =$$
$$= (a_{\sigma(1)} \ldots a_{\sigma(k-1)})((a_{\sigma(k+1)} \ldots a_{\sigma(n)}) a_n) =$$
$$= a_{\sigma(1)} \ldots a_{\sigma(k-1)} a_{\sigma(k+1)} \ldots a_{\sigma(n)} a_n = a_1 \ldots a_n$$

в силу доказанного выше.

Следствие. *Для любых элементов* $a_1, a_2, \ldots, a_n$ *коммутативной полугруппы и любой подстановки* σ *на множестве* $\{1, 2, \ldots, n\}$ *справедливо равенство*

$$a_1 a_2 \ldots a_n = a_{\sigma(1)} a_{\sigma(2)} \ldots a_{\sigma(n)}.$$

Таким образом, в коммутативной полугруппе, вычисляя произведение нескольких сомножителей, можно не только ставить скобки произвольным образом, но и располагать сомножители в любом порядке.

Непустое подмножество H полугруппы называется *подполугруппой*, если произведение любых двух элементов из H снова лежит в H. Это, в частности, означает, что всякая подполугруппа является полугруппой относительно операции, определенной в исходной полугруппе. Например, четные числа образуют подполугруппы полугрупп 1, 2 и 4 из таблицы 1, а множество $\{-1, 0, 1\}$ — подполугруппу полугруппы 2 из той же таблицы. Но для полугруппы 1 это подмножество подполугруппой не является.

Теорема 3. *Непустое пересечение любого множества подполугрупп является подполугруппой.*

Доказательство. Пусть U — пересечение некоторого множества подполугрупп. Если $x, y \in U$, то x и y лежат в каждой из подполугрупп рассматриваемого множества. Но тогда в каждой из них лежит и произведение xy, а значит, $xy \in U$.

Замечание. Требование непустоты пересечения в теореме 3 существенно. Действительно, в примере 4 из таблицы 1 как положительные, так и отрицательные числа образуют подполугруппы, и пересечение этих подполугрупп пусто.

Отображение φ полугруппы A в полугруппу B называется *гомоморфизмом*, если $\varphi(xy) = \varphi(x)\varphi(y)$ для любых $x, y \in A$. Подчеркнем, что здесь xy обозначает операцию в полугруппе A, а $\varphi(x)\varphi(y)$ — операцию в полугруппе B. Гомоморфизм, являющийся вложением (наложением), называется *гомоморфным вложением* (*гомоморфным наложением*), а взаимно однозначный гомоморфизм—

Таблица 2

Гомоморфизмы φ: $A \to B$

	A	B	φ	Доказательство гомоморфности отображения	Тип отображения	Ker φ
1	Действительные числа относительно сложения	Действительные числа относительно умножения	$\varphi(x) = 2^x$	$\varphi(x+y) = 2^{x+y} = 2^x \cdot 2^y = \varphi(x)\varphi(y)$	Вложение	Класс $[x]$ одноэлементен для всех x
2	Действительные числа относительно сложения	Положительные действительные числа относительно умножения	То же	То же	Изоморфизм	То же
3	Квадратные матрицы порядка n относительно умножения	Действительные числа относительно умножения	$\varphi(X) = \lvert X\rvert$	$\varphi(XY) = \lvert XY\rvert = \lvert X\rvert\,\lvert Y\rvert = \varphi(X)\varphi(Y)$ (теорема 1.3.14)	Наложение	Класс $[X]$ состоит из всех таких матриц Y, что $\lvert Y\rvert = \lvert X\rvert$
4	Произвольная полугруппа	Произвольная полугруппа с единицей 1	$\varphi(x) = 1$	$\varphi(xy) = 1 = 1 \cdot 1 = \varphi(x)\varphi(y)$	—	$[x] = A$ для всех x
5	Произвольная полугруппа	A	$\varphi(x) = x$	$\varphi(xy) = xy = \varphi(x)\varphi(y)$	Изоморфизм	Как в примере 1
6	n-мерные строки относительно сложения	Действительные числа относительно сложения	$\varphi(x)$ — первая координата строки x	При сложении строк по определению складываются координаты	Наложение	Класс $[(x_1, x_2, \ldots, x_n)]$ состоит из всех строк вида $(x_1, y_2, \ldots, y_n)$

7	Целые числа относительно сложения	Множество $\{1, -1\}$ относительно умножения	$\varphi(x)=\begin{cases}1, \text{ если } x \text{ четное},\\ -1, \text{если } x \text{ нечетное}\end{cases}$	*)	Наложение	$[x]$ состоит из всех четных чисел, если x четное, и из всех нечетных в противном случае
8	Целые числа относительно умножения	Множество $\{1, 0, -1\}$ относительно умножения	$\varphi(x) = \operatorname{sgn} x$ **)	$\varphi(xy) = \operatorname{sgn}(xy) = \operatorname{sgn} x \cdot \operatorname{sgn} y = \varphi(x)\,\varphi(y)$	Наложение	$[x]$ состоит из всех положительных чисел, если $x>0$, из одного нуля, если $x=0$, и из всех отрицательных чисел, если $x<0$.
9	Действительные числа относительно умножения	Матрицы второго порядка относительно умножения	$\varphi(x) = \begin{Vmatrix} x & 0 \\ 0 & 0 \end{Vmatrix}$	$\varphi(xy) = \begin{Vmatrix} xy & 0 \\ 0 & 0 \end{Vmatrix} = \begin{Vmatrix} x & 0 \\ 0 & 0 \end{Vmatrix} \begin{Vmatrix} y & 0 \\ 0 & 0 \end{Vmatrix} = \varphi(x)\,\varphi(y)$	Вложение	Как в примере 1

*) Если x, $y \in A$, то возможны четыре случая: а) x и y четные; б) x и y нечетные; в) x четное, а y нечетное; г) x нечетное, а y четное. В случае а) имеем $\varphi(x+y)=1=1\cdot 1=\varphi(x)\varphi(y)$, а в случае б) $\varphi(x+y)=1=(-1)(-1)=\varphi(x)\varphi(y)$. В случае в) получаем $\varphi(x+y)=-1=1\cdot(-1)=\varphi(x)\varphi(y)$. Случай г) рассматривается аналогично.

**) $\operatorname{sgn} x = \begin{cases} 1, \text{ если } x>0, \\ 0, \text{ если } x=0, \\ -1, \text{ если } x<0. \end{cases}$

изоморфизмом. Если существует изоморфизм полугруппы A на полугруппу B, то эти полугруппы называются *изоморфными* *). Примеры гомоморфизмов приведены в таблице 2.

Теорема 4. *Если* $\varphi\colon A \to B$ — *гомоморфное наложение полугрупп и* e — *единица в* A, *то* $\varphi(e)$ — *единица в* B.

Доказательство. Если $b \in B$, то, поскольку φ — наложение, имеем $b = \varphi(a)$ для некоторого $a \in A$. Отсюда

$$b\varphi(e) = \varphi(a)\,\varphi(e) = \varphi(ae) = \varphi(a) = b,$$

поскольку φ — гомоморфизм. Аналогично проверяется, что

$$\varphi(e)\, b = b \text{ для всех } b \in B.$$

В силу теоремы 9 из § 1, каждый элемент a из данной полугруппы имеет не более одного обратного. Если такой обратный существует, то условимся обозначать его через a^{-1}.

Теорема 5. *Если* $\varphi\colon A \to B$ — *гомоморфное наложение полугрупп*, $a \in A$ *и* a^{-1} *существует*, *то* $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

Доказательство. Ввиду теоремы 4, $\varphi(e)$ — единица полугруппы B, если e — единица полугруппы A. Остается вспомнить определение обратного элемента и заметить, что

$$\varphi(a^{-1})\,\varphi(a) = \varphi(a^{-1}a) = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\,\varphi(a^{-1}).$$

---

*) Говоря «полугруппы A и B изоморфны», мы, на первый взгляд, вступаем в противоречие с определением изоморфизма, в котором полугруппы A и B не равноправны. Однако если $\varphi\colon A \to B$ — изоморфизм, то существует обратное взаимно однозначное отображение $\varphi^{-1}\colon B \to A$. При этом, каковы бы ни были $b', b'' \in B$, для некоторых $a', a'' \in A$ имеем $b' = a'\varphi$ и $b'' = a''\varphi$. Следовательно,

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

т. е. φ^{-1} оказывается гомоморфизмом, а значит, и изоморфизмом. Таким образом, на самом деле полугруппы A и B равноправны. Далее, если $\varphi\colon A \to B$ и $\psi\colon B \to C$ — гомоморфизмы полугрупп, то для любых $a', a'' \in A$ имеем

$$(a'a'')\,(\varphi\psi) = ((a'a'')\,\varphi)\,\psi = ((a'\varphi)\,(a''\varphi))\,\psi = (a'\varphi)\,\psi \cdot (a''\varphi)\,\psi = a'\,(\varphi\psi)\cdot a''\,(\varphi\psi).$$

Следовательно, $\varphi\psi$ — гомоморфизм полугруппы A в полугруппу C. В силу теоремы 5 из § 1, отсюда вытекает, что произведение изоморфизмов — изоморфизм. Это, в частности, означает, что если полугруппа A изоморфна полугруппе B, а полугруппа B — полугруппе C, то полугруппы A и C изоморфны.

Замечание. Для справедливости теорем 4 и 5 существенно, что φ — наложение. Действительно, для гомоморфизма 9 из таблицы 2 имеем

$$\varphi(1) = \begin{Vmatrix} 1 & 0 \\ 0 & 0 \end{Vmatrix} \neq E.$$

Более того, матрицы, обратной к $\varphi(1)$, не существует.

Теорема 6. *Если* φ: $A \to B$ — *гомоморфизм полугруппп, то* $\operatorname{Im}\varphi$ — *подполугруппа полугруппы* B.

Доказательство. Если $y, y' \in \operatorname{Im}\varphi$, то $y = \varphi(x)$ и $y' = \varphi(x')$ для некоторых $x, x' \in A$. Но тогда $\varphi(xx') = \varphi(x)\varphi(x') = yy'$, т. е. $yy' \in \operatorname{Im}\varphi$.

Разбиение Σ полугруппы A называется *допустимым*, если из того, что x и u принадлежат какому-то одному смежному классу разбиения Σ, а y и v также принадлежат одному смежному классу этого разбиения, вытекает, что xy и uv лежат в одном смежном классе.

Примеры. 1. Пусть A — полугруппа целых чисел относительно сложения и Σ — ее разбиение, состоящее из двух классов, один из которых содержит все четные числа, а второй — все нечетные. Для x, y, u и v, упоминаемых в определении, возможны следующие четыре случая:

	x и u	y и v	$x+y$	$u+v$
1	четные	четные	четное	четное
2	четные	нечетные	нечетное	нечетное
3	нечетные	четные	нечетное	нечетное
4	нечетные	нечетные	четное	четное

Как видно, во всех случаях $x + y$ и $u + v$ попадают в один и тот же смежный класс, т. е. разбиение Σ допустимое.

2. Пусть A — полугруппа целых чисел относительно умножения и Σ — ее разбиение, состоящее из трех классов: все положительные числа, нуль и все отрицательные числа. Допустимость разбиения видна из таблицы, приведенной на следующей странице.

3. Если A — полугруппа целых чисел относительно сложения, то разбиение, рассмотренное в предыдущем примере, допустимым не является. Действительно, 5 и 3 лежит в одном классе этого разбиения. То же самое верно для -4 и -3. Однако $5 + (-4) = 1$ и $3 + (-3) = 0$ принадлежат различным классам этого разбиения.

Если Σ — допустимое разбиение, то на фактормножестве A/Σ можно определить операцию, полагая

$$[x][y] = [xy],$$

	x и u	y и v	xy	uv
1	>0	>0	>0	>0
2	>0	$=0$	$=0$	$=0$
3	>0	<0	<0	<0
4	$=0$	>0	$=0$	$=0$
5	$=0$	$=0$	$=0$	$=0$
6	$=0$	<0	$=0$	$=0$
7	<0	>0	<0	<0
8	<0	$=0$	$=0$	$=0$
9	<0	<0	>0	>0

где через $[x]$ обозначен смежный класс разбиения Σ, содержащий элемент x. Это определение корректно. Действительно, из равенств $[x] = [u]$ и $[y] = [v]$ вытекает, что как x и u, так и y и v располагаются в одних и тех же классах разбиения Σ. Ввиду его допустимости, xy и uv также лежат в одном смежном классе, что дает $[xy] = [uv]$.

Из равенств

$$([x]\,[y])\,[z] = [xy]\,[z] = [(xy)\,z] = [x\,(yz)] = \\ = [x]\,[yz] = [x]\,([y]\,[z])$$

вытекает, что операция, определенная на фактормножестве, ассоциативна. Следовательно, фактормножество становится полугруппой, которая называется *факторполугруппой* полугруппы A по допустимому разбиению Σ. Если $\pi\colon A \to A/\Sigma$ — естественное отображение, то

$$\pi\,(xy) = [xy] = [x]\,[y] = \pi\,(x)\,\pi\,(y).$$

Следовательно, π оказывается гомоморфизмом (даже гомоморфным наложением) и потому называется *естественным гомоморфизмом*.

Для рассмотренных выше допустимых разбиений фактормножества состоят из двух и трех элементов соответственно. Обозначив элементы первого множества как *чет* и *нечет*, а второго как [1], [0] и [—1], получим следующие таблицы умножения:

•	*чет*	*нечет*
чет	*чет*	*нечет*
нечет	*нечет*	*чет*

•	[1]	[0]	[—1]
[1]	[1]	[0]	[—1]
[0]	[0]	[0]	[0]
[—1]	[—1]	[0]	[1]

Естественные гомоморфизмы определяются как

$$\pi(x) = \begin{cases} \textit{чет}, & \text{если } x \text{ четное}, \\ \textit{нечет}, & \text{если } x \text{ нечетное}, \end{cases}$$

в первом случае и как

$$\pi(x) = \begin{cases} [1], & \text{если } x > 0, \\ [0], & \text{если } x = 0, \\ [-1], & \text{если } x < 0, \end{cases}$$

во втором.

Теорема 7. *Если* φ: $A \to B$ — *гомоморфизм полугрупп, то разбиение* Ker φ (оно называется *ядром гомоморфизма* φ) *допустимо.*

Доказательство. Если x и u располагаются в одном смежном классе этого разбиения и то же самое справедливо для элементов y и v, то по определению разбиения Ker φ имеем $\varphi(x) = \varphi(u)$ и $\varphi(y) = \varphi(v)$. Отсюда, поскольку φ — гомоморфизм, вытекает, что

$$\varphi(xy) = \varphi(x)\,\varphi(y) = \varphi(u)\,\varphi(v) = \varphi(uv)$$

и, следовательно, xy и uv располагаются в одном классе разбиения Ker φ.

Таким образом, таблица 2 доставляет нам ряд примеров допустимых разбиений. Заметим еще, что всякое допустимое разбиение совпадает с Ker π, где π — естественный гомоморфизм.

Теорема 8 (теорема о гомоморфизме для полугрупп). *Если* φ: $A \to B$ — *гомоморфное наложение полугрупп и* π: $A \to A/\mathrm{Ker}\,\varphi$ — *естественный гомоморфизм, то существует изоморфизм* χ: $B \to A/\mathrm{Ker}\,\varphi$ *такой, что* $\varphi\chi = \pi$.

Доказательство. Рассмотрим взаимно однозначное отображение χ, существование которого доказано в теореме 7 из § 1. Для доказательства теоремы достаточно установить, что χ — гомоморфизм. Но если $b', b'' \in B$, то для некоторых $a', a'' \in A$ имеем $b' = \varphi(a')$ и $b'' = \varphi(a'')$. Вспоминая определение отображения χ и учитывая равенство $\varphi(a'a'') = \varphi(a')\,\varphi(a'') = b'b''$, получим

$$\chi(b')\chi(b'') = \pi(a')\,\pi(a'') = \pi(a'a'') = \chi(b'b''),$$

что и требовалось.

Если A — полугруппа и $a \in A$, то для всякого натурального n положим

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

Если A содержит единицу e, то полагаем $a^0 = e$.

Теорема 9. $a^m \cdot a^n = a^{m+n}$ *для всех* $m, n > 0$.

Доказательство. Ввиду теоремы 1

$$a^m \cdot a^n = (\underbrace{a \ldots a}_{m \text{ раз}})(\underbrace{a \ldots a}_{n \text{ раз}}) = \underbrace{a \ldots a}_{m+n \text{ раз}} = a^{m+n}.$$

Полугруппа A называется *моногенной*, если в ней содержится такой элемент a, что всякий элемент x из A может быть записан в форме $x = a^n$ для некоторого $n > 0$. Элемент a называется *образующим* (или *порождающим*) моногенной полугруппы. Важнейшим примером моногенной полугруппы является полугруппа $\boldsymbol{P}$ положительных целых чисел относительно сложения. Ее образующим служит 1. Зафиксируем положительные числа n и d и рассмотрим разбиение $\Sigma(n, d)$ множества $\boldsymbol{P}$, состоящее из одноэлементных классов $[1] = \{1\}$, $[2] = \{2\}$, ..., $[d-1] = \{d-1\}$ и бесконечных классов

$$[d] = \{d, d+n, d+2n, \ldots, d+kn, \ldots\},$$
$$[d+1] = \{d+1, d+1+n, d+1+2n, \ldots \ldots, d+1+kn, \ldots\},$$
$$[d+(n-1)] = \{d+(n-1), d+(n-1)+n, d+(n-1)+2n, \ldots, d+(n-1)+kn, \ldots\}.$$

Убедимся, что это разбиение допустимо. В самом деле, пусть $x, u \in [i]$ и $y, v \in [j]$, где $1 \leqslant i, j < d+n$. Возможны следующие четыре случая: 1) $i, j < d$; 2) $i < d$, $j \geqslant d$; 3) $i \geqslant d$, $j < d$; 4) $i, j \geqslant d$. В первом случае имеем $x = u = i$ и $y = v = j$, откуда $[x+y] = [u+v]$, поскольку $x + y = u + v$. Во втором случае $x = u = i$, $y = j + kn$ и $v = j + ln$ для подходящих k и l. Используя деление с остатком, запишем

$$i + j - d = sn + r,$$

где $0 \leqslant r < n$. Тогда

$$x + y = i + j + kn = d + (i + j - d) + kn = d + r + (s + k)\, n$$

и

$$u + v = i + j + ln = d + (i + j - d) + ln = d + r + (s + l)\, n,$$

откуда $[x+y] = [d+r] = [u+v]$. Третий случай рассматривается аналогично. В четвертом случае, используя

определение смежных классов, можно записать

$$x = i + kn = d + (i - d) + kn,$$
$$u = i + ln = d + (i - d) + ln,$$
$$y = j + pn = d + (j - d) + pn$$

и

$$v = j + qn = d + (j - d) + qn.$$

Тогда

$$x + y = d + (d + (i - d) + (j - d)) + (k + p)\, n$$

и

$$u + v = d + (d + (i - d) + (j - d)) + (l + q)\, n.$$

Разделив с остатком, получим

$$d + (i - d) + (j - d) = sn + r,$$

где $0 \leqslant r < n$. Отсюда

$$x + y = d + r + (k + p + s)\, n$$

и

$$u + v = d + r + (l + q + s)\, n,$$

т. е. $[x + y] = [d + r] = [u + v]$.

Факторполугруппу полугруппы $\boldsymbol{P}$ по рассмотренному разбиению называют *циклом с хвостом* (см. рис. 4). При

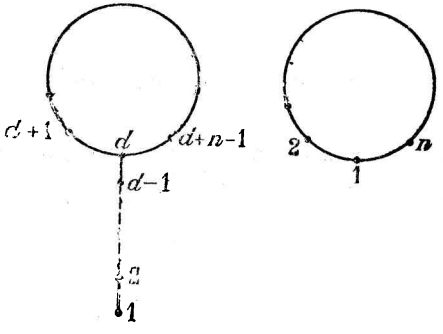


Рис. 4

$d = 1$ хвост оказывается пустым. Такую полугруппу называют *циклом*.

Теорема 10. *Всякая моногенная полугруппа изоморфна или аддитивной полугруппе* $\boldsymbol{P}$ *положительных чисел, или некоторому циклу с хвостом (возможно, пустым).*

Доказательство. Пусть A — моногенная полугруппа с образующим a. Рассмотрим отображение полугруппы $\boldsymbol{P}$ в полугруппу A, определяемое условием

$$\varphi(m) = a^m.$$

Ввиду моногенности полугруппы A, φ оказывается наложением. В силу теоремы 9

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

т. е. φ является гомоморфизмом. Из теоремы 8 вытекает, что A изоморфна факторполугруппе $\boldsymbol{P}/\Sigma$, где $\Sigma = \operatorname{Ker}\varphi$. Если все классы разбиения Σ одноэлементны, то $\boldsymbol{A}$ изоморфна $\boldsymbol{P}$. В противном случае обозначим через d наименьшее целое число, входящее в неодноэлементный класс, а число n выберем так, чтобы $d+n$ было наименьшим числом, отличным от d, но входящим в один класс с d. Тогда имеем классы $[1], [2], \ldots, [d-1], [d], [d+1], \ldots, [d+n-1]$, среди которых первые $d-1$ одноэлементные и $[d] \neq [d+i]$ при $i = 1, 2, \ldots$ $\ldots, n-1$. Докажем, что

$$[d+i] = [d+i+kn] \qquad (*)$$

при любых i и k. В силу определения разбиения Σ, для этого достаточно установить, что

$$\varphi(d+i) = \varphi(d+i+kn). \qquad (**)$$

При $k = 0$ это очевидно. Допустим, что $(**)$ доказано при всех i и $k = 0, 1, \ldots, t-1$. Тогда, вспоминая, что $\varphi(d) = \varphi(d+n)$, получаем

$$\begin{aligned}\varphi(d+i+tn) &= \varphi(d+i+(t-1)n+n) = \\ &= \varphi(d+i+(t-1)n)\,\varphi(n) = \varphi(d+i)\,\varphi(n) = \\ &= \varphi(d+i+n) = \varphi(d+n)\,\varphi(i) = \varphi(d)\,\varphi(i) = \\ &= \varphi(d+i).\end{aligned}$$

Тем самым равенство $(**)$, а значит и $(*)$, доказано. Остается убедиться, что разбиение Σ совпадает с разбиением $\Sigma(n, d)$. С этой целью заметим, что одноэлементные классы этих разбиений совпадают. Ввиду равенства $(*)$, для доказательства совпадения бесконечных классов достаточно установить, что смежные классы $[d+i]$ и $[d+j]$ разбиения Σ, где $0 \leqslant i < j < n$, различны. Но если $[d+i] = [d+j]$, то

$$\begin{aligned}[d] = [d+n] &= [d+j] + [n-j] = \\ &= [d+i] + [n-j] = [d+(n-(j-i))]\end{aligned}$$

и, поскольку $0 < n - (j - i) < n$, мы вступаем в противоречие с выбором числа n.

Пусть S — полугруппа, а X — ее непустое подмножество. Пересечение T всех подполугрупп полугруппы S, содержащих X, называется *подполугруппой, порожденной множеством* X. Существование полугруппы T вытекает из теоремы 3, поскольку подполугруппы, содержащие множество X, существуют (например, сама полугруппа S) и пересечение их непусто (все они содержат X). Ясно, что T — это наименьшая среди подполугрупп полугруппы S, содержащих множество X *). Если эта наименьшая подполугруппа совпадает с S, то говорят, что полугруппа S *порождается множеством* X. В частности, моногенная полугруппа порождается своим образующим.

Полугруппа $S = S(X)$ называется *свободной полугруппой со свободно порождающим множеством* X, если

(1) S порождается множеством X;

(2) для любого отображения $\varphi\colon X \to A$, где A — произвольная полугруппа, существует гомоморфизм $\overline{\varphi}\colon S(X) \to A$ такой, что $\overline{\varphi}(x) = \varphi(x)$ для любого $x \in X$.

Для доказательства существования свободных полугрупп возьмем произвольное непустое множество X, которое будем называть *алфавитом*. Всякую конечную последовательность $x_1 \ldots x_m$, где $x_i \in X$, назовем *словом* в алфавите X. Пусть $W = W(X)$ — множество всех непустых слов в алфавите X. Определим произведение двух слов u и v из $W(X)$ как слово, равное написанным подряд без пробела словам u и v. Эта операция ассоциативна и превращает W в полугруппу.

Теорема 11 (теорема существования свободной полугруппы). *$W = W(X)$ — свободная полугруппа со свободно порождающим множеством X.*

Доказательство. Назовем *длиной* $l(w)$ слова w количество входящих в него букв, причем каждая буква считается столько раз, сколько раз она входит в слово w. Оба свойства (1) и (2) из определения свободной полугруппы проверим индукцией по $l(w)$.

(1) Пусть T — подполугруппа полугруппы W, порожденная множеством X. Тогда любое слово $w \in W$ лежит в T. Действительно, если $l(w) = 1$, то $w \in X \subseteq T$. Если $l(w) > 1$, то $w = w'x$, где $l(w') < l(w)$ и $x \in X$. Следовательно, w', $x \in T$ по предполо-

*) Нетрудно доказать также, что подполугруппа T совпадает с множеством всех элементов полугруппы S, представимых в форме $x_1 \ldots x_m$, где $x_i \in X$.

жению индукции. Так как T — подполугруппа, а w — произведение двух ее элементов w' и x, то $w \in T$. Поэтому $W \subseteq T$. Обратное включение очевидно. Итак, $T = W$.

(2) Пусть φ — произвольное отображение множества X в некоторую полугруппу A с операцией $\circ$. Определим элемент $\overline{\varphi}(w)$ полугруппы A индукцией по $l(w)$. Если $l(w) = 1$, то $w \in X$, и мы положим

$$\overline{\varphi}(w) = \varphi(w). \qquad (*)$$

Если $l(w) > 1$, то $w = w'x$, где $l(w') < l(w)$, а $x \in X$. Тогда $\overline{\varphi}(w')$ и $\overline{\varphi}(x)$ уже определены. Положим

$$\overline{\varphi}(w) = \overline{\varphi}(w') \circ \overline{\varphi}(x). \qquad (**)$$

Покажем, что отображение $\overline{\varphi}\colon W \to A$ является гомоморфизмом, т. е. что $\overline{\varphi}(w_1w_2) = \overline{\varphi}(w_1) \circ \overline{\varphi}(w_2)$ для любых $w_1, w_2 \in W$. Проведем индукцию по длине второго сомножителя w_2. Если $l(w_2) = 1$, то доказываемое следует из равенства (**). Если же $l(w_2) > 1$, то $w_2 = w_2'x$, где $l(w_2') < l(w_2)$ и $x \in X$. Поэтому, учитывая (**) и индуктивное предположение, получаем

$$\overline{\varphi}(w_1w_2'x) = \overline{\varphi}(w_1w_2') \circ \overline{\varphi}(x) = (\overline{\varphi}(w_1) \circ \overline{\varphi}(w_2')) \circ \overline{\varphi}(x) =$$
$$= \overline{\varphi}(w_1) \circ (\overline{\varphi}(w_2') \circ \overline{\varphi}(x)) = \overline{\varphi}(w_1) \circ \overline{\varphi}(w_2).$$

Кроме того, если $x \in X$, то $\overline{\varphi}(x) = \varphi(x)$ в силу равенства (*). Итак, условия (1) и (2) выполнены.

Теорема 12 (свойство универсальности свободной полугруппы). *Для всякой полугруппы A найдутся свободная полугруппа S и гомоморфное наложение $\varphi\colon S \to A$.*

Доказательство. Пусть S — свободная полугруппа со свободно порождающим множеством A. В силу свойства (2) из определения свободной полугруппы, тождественное отображение множества A на себя продолжается до гомоморфизма $\varphi\colon S \to A$, который в данном случае оказывается наложением.

Теорема 13 (теорема единственности свободной полугруппы). *Если $S = S(X)$ — свободная полугруппа со свободно порождающим множеством X, то существует изоморфизм φ полугруппы S на полугруппу $W = W(X)$ слов в алфавите X, причем $\varphi(x) = x$ для всех $x \in X$.*

Доказательство. Согласно теореме 11 и свойству (2) из определения свободной полугруппы, тождественное отображение множества X на себя продолжается до гомоморфизмов $\varphi\colon S \to W$ и $\psi\colon W \to S$, причем $\varphi(x) = \psi(x) = x$ для всех $x \in X$. Таким образом,

$X \subseteq \operatorname{Im}\varphi$ и $X \subseteq \operatorname{Im}\psi$. Ввиду теоремы 6 и свойства (1) из определения свободной полугруппы, $\operatorname{Im}\varphi = W$ и $\operatorname{Im}\psi = S$, т. е. как φ, так и ψ оказываются наложениями. Более того, поскольку $x(\psi\varphi) = x$ для всех $x \in X$, нетрудно заметить, что $w(\psi\varphi) = w$ для всякого слова w в алфавите X, т. е. $\psi\varphi = 1_W$. Если $a\psi = b\psi$ для некоторых $a, b \in W$, то

$$a = a\psi\varphi = b\psi\varphi = b.$$

Следовательно, ψ — вложение, а значит, и изоморфизм.

Упражнения

1. Убедиться, что множество всех подмножеств некоторого множества с операцией пересечения (объединения) является коммутативной полугруппой. Есть ли у этих полугрупп единицы? Для каких элементов этих полугрупп существуют обратные? Доказать, что отображение φ, где $\varphi(M)$ — дополнение подмножества M, является изоморфизмом одной из этих полугрупп на другую.

2. Доказать, что как вырожденные, так и невырожденные матрицы образуют подполугруппы полугруппы матриц относительно умножения.

3. Доказать, что всякое непустое подмножество полугруппы 5 упражнения 5 из § 1 является подполугруппой.

4. На множестве действительных чисел определим операцию, положив $xy = 0$ для любых x и y. Доказать, что это полугруппа. Найти все ее подполугруппы.

5. На множестве четырехмерных строк определим операцию $(a, b, c, d)(s, t, u, v) = (a, b, u, v)$. Доказать, что это полугруппа и что все ее элементы являются идемпотентами (элемент e полугруппы называется *идемпотентом*, если $e^2 = e$).

6. Доказать, что множество всех идемпотентов коммутативной полугруппы с единицей является подполугруппой.

7. Пусть A и B — полугруппы. На множестве $A \times B$ всех пар (a, b), где $a \in A$, $b \in B$, определим операцию

$$(a, b)(a', b') = (aa', bb').$$

Доказать, что $A \times B$ — полугруппа, причем она содержит единицу тогда и только тогда, когда единицы существуют в полугруппах A и B. Указать какой-либо гомоморфизм полугруппы $A \times B$ на полугруппу A и найти его ядро. Доказать, что если полугруппа B содержит единицу, то существует гомоморфное вложение полугруппы A в полугруппу $A \times B$.

8. Будут ли гомоморфизмами полугрупп отображения $\varphi\colon A \to B$ из приводимой на следующей странице таблицы? В случае положительного ответа найти их ядра.

9. Пусть A и B — полугруппы m- и n-мерных строк соответственно относительно сложения, причем $m < n$. Доказать, что существуют гомоморфное вложение полугруппы A в полугруппу B и гомоморфное наложение полугруппы B на полугруппу A. Указать ядро найденного наложения. Доказать, что B изоморфна полугруппе $A \times C$ (см. упражнение 7), где C — полугруппа $(n - m)$-мерных строк.

	A	B	φ
1	n-мерные строки относительно сложения	Действительные числа относительно сложения	$\varphi(a_1, \ldots, a_n) = a_1 + \ldots + a_n$
2	Действительные числа относительно сложения	Целые числа относительно сложения	$\varphi(x) =$ (целой части числа x)
3	Действительные числа относительно умножения	Целые числа относительно умножения	То же
4	Полугруппа слов	Полугруппа слов	$\varphi(x) = x^2$
5	Произвольная полугруппа	Произвольная полугруппа с единицей	$\varphi(x) = 1$ для всех $x \in A$
6	Матрицы вида $\begin{Vmatrix} 1 & x \\ 0 & 1 \end{Vmatrix}$ относительно умножения	Действительные числа относительно сложения	$\varphi\left(\begin{Vmatrix} 1 & x \\ 0 & 1 \end{Vmatrix}\right) = x$

10. Доказать, что полугруппа слов в алфавите, состоящем из одной буквы, изоморфна полугруппе положительных целых чисел относительно сложения.

11. Убедиться, что двухэлементная полугруппа $\{-1, 1\}$ с операцией умножения не изоморфна полугруппе с таблицей умножения

$\cdot$	a	b
a	a	b
b	b	b

12. Доказать, что факторполугруппа, возникающая из допустимого разбиения примера 2 на с. 61, не изоморфна полугруппам с таблицами умножения

$\cdot$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

и

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	2

13. Доказать, что моногенные полугруппы $\boldsymbol{P}/\Sigma\ (m, c)$ и $\boldsymbol{P}/\Sigma\ (n, d)$ изоморфны тогда и только тогда, когда $m = n$ и $c = d$.

14. Доказать, что для каждого непустого множества X существует коммутативная полугруппа S, обладающая следующими свойствами: а) S порождается множеством X; б) для любого отображения φ: $X \to A$, где A — произвольная коммутативная полугруппа, существует гомоморфизм $\overline{\varphi}$: $S \to A$ такой, что $\overline{\varphi}(x) = \varphi(x)$ для всех $x \in X$.

15. Доказать, что для каждого непустого множества X существует полугруппа S с единицей, обладающая следующими свойствами: а) S порождается объединением $\{1\} \cup X$; б) для каждого

отображения $\varphi\colon X \to A$, где A — произвольная полугруппа с единицей, существует гомоморфизм $\overline{\varphi}\colon S \to A$ такой, что $\overline{\varphi}(x) = \varphi(x)$ для всех $x \in X$.

16. Доказать, что для каждого непустого множества X существует коммутативная полугруппа S, обладающая следующими свойствами: а) $s^2 = s$ для всех $s \in S$; б) S порождается множеством X; в) для каждого отображения $\varphi\colon X \to A$, где A — коммутативная полугруппа и $a^2 = a$ для всех $a \in A$, существует гомоморфизм $\overline{\varphi}\colon S \to A$ такой, что $\overline{\varphi}(x) = \varphi(x)$ для всех $x \in X$.

§ 3. Группы

Полугруппа называется *группой*, если она содержит единицу и для каждого ее элемента существует обратный. Среди полугрупп, приведенных в таблице 1, группами оказываются, например, полугруппы 1, 3, 4, 8 и 12.

Подмножество H группы G называется *подгруппой*, если H является подполугруппой (т. е. непусто и вместе с любыми двумя элементами содержит их произведение) и вместе с каждым элементом содержит обратный к нему. Всякая подгруппа H группы G содержит единицу группы G. Действительно, по условию существует элемент $h \in H$. Но тогда $h^{-1} \in H$, что в свою очередь влечет $1 = hh^{-1} \in H$. Нетрудно понять, что всякая подгруппа является группой относительно операций, определенных в исходной группе.

Подгруппами группы отличных от нуля действительных чисел (группа 3 из таблицы 1) будут, например, подмножество всех положительных действительных чисел, подмножество, состоящее из 1 и -1, совокупность всех степеней 2^m, где m — произвольное целое число. Однако, например, множество всех отличных от нуля целых чисел подгруппой не является. В группе целых чисел по сложению (группа 4 из таблицы 1) подгруппу образуют, например, четные числа (но не нечетные!). В группе невырожденных матриц (группа 8 из таблицы 1) можно указать подгруппу, состоящую из всех матриц с определителем, равным 1 (принять во внимание теорему I.3.14), и подгруппу, состоящую из всех невырожденных диагональных матриц.

Во всякой группе существуют две *тривиальные подгруппы*: вся группа и *единичная подгруппа*, состоящая из одной единицы.

Т е о р е м а 1. *Пересечение любого множества подгрупп является подгруппой.*

Д о к а з а т е л ь с т в о. Пусть U — пересечение некоторого множества подгрупп. Так как каждая из этих подгрупп содержит единицу 1, то $1 \in U$, т. е. U непусто. Ввиду теоремы 3 из § 2, U — подполугруппа. Если $g \in U$, то g принадлежит всем подгруппам рассматриваемо-

го множества. Но тогда каждая из них содержит g^{-1}, а значит, $g^{-1} \in U$.

Если H — подгруппа группы G и g — некоторый элемент из G, то множество всех произведений вида gh, где $h \in H$, называется *левым смежным классом* по подгруппе H, определенным элементом g, и обозначается через gH. Аналогично определяется *правый смежный класс* Hg. Если $g \in H$, то $gH = H$. Действительно, $gH \subseteq H$, поскольку H — подгруппа. Если теперь $h \in H$, то, поскольку H — подгруппа, имеем $g^{-1}h \in H$. Отсюда $h = g(g^{-1}h) \in gH$, т. е. $H \subseteq gH$. Из полученных включений вытекает равенство $gH = H$. Другие примеры смежных классов приводятся в таблице 3.

Таблица 3

	Группа G	Подгруппа H	Элемент g	Смежный класс gH
1	Действительные числа, отличные от 0 (группа 3 из таблицы 2)	Положительные действительные числа	-3	Все отрицательные действительные числа
2	То же	$\{1, -1\}$	-3	$\{-3, 3\}$
3	Целые числа (группа 4 из таблицы 2)	Четные числа	-3	Все нечетные числа
4	Невырожденные матрицы второго порядка (группа 8 из таблицы 2)	Матрицы с определителем, равным 1	$\begin{Vmatrix} 1 & 2 \\ 2 & 6 \end{Vmatrix}$	Все матрицы с определителем, равным 2
5	То же	Матрицы вида λE, где λ — любое отличное от 0 действительное число	$\begin{Vmatrix} 1 & 2 \\ 2 & 6 \end{Vmatrix}$	Все матрицы вида $\begin{Vmatrix} \lambda & 2\lambda \\ 2\lambda & 6\lambda \end{Vmatrix}$, где $\lambda \neq 0$
6	Взаимно однозначные отображения множества $\{1, 2, 3, 4\}$ на себя (группа 12 из таблицы 2)	Все такие отображения φ, что $\varphi(1) = 1$	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$	Все такие отображения φ, что $\varphi(4) = 1$

Теорема 2. *Множество левых смежных классов группы G по подгруппе H образует разбиение группы G.*

Доказательство. Если $g \in G$, то $g = g1$ и, поскольку $1 \in H$, имеем $g \in gH$. Поэтому для доказатель-

ства теоремы достаточно установить, что два различных смежных класса не пересекаются. Для этого достаточно доказать, что два смежных класса, имеющие общий элемент, совпадают. Но если $x \in aH \cap bH$, где $a, b \in G$, то $x = ah_1 = bh_2$, где $h_1, h_2 \in H$. Отсюда $a = (bh_2)\, h_1^{-1}$. Если, далее, $g \in aH$, то $g = ah$, где $h \in H$. Поэтому

$$g = ah = ((bh_2)\, h_1^{-1})\, h = b\, (h_2 h_1^{-1} h).$$

Из определения подгруппы вытекает, что $h_2 h_1^{-1} h \in H$. Следовательно, $g \in bH$. В силу произвольности g это означает, что $aH \subseteq bH$. Обратное включение доказывается аналогично.

Разбиение группы G на левые смежные классы по подгруппе H называется *левым разбиением по подгруппе* H. Аналогично, доказав правый аналог теоремы 2, можно говорить о *правом разбиении по подгруппе* H.

Теорема 3 (теорема Лагранжа). *Если H — подгруппа конечной группы G, то число элементов подгруппы H является делителем числа элементов группы G* *).

Докажем более сильное утверждение.

Теорема 3′. *Если n — число элементов группы G, m — число элементов ее подгруппы H и k — число правых смежных классов группы G по подгруппе H, то $n = km$.*

Доказательство. Пусть $h_1, \ldots, h_m$ — элементы подгруппы H. Смежный класс Hg содержит элементы $h_1 g, \ldots, h_m g$. Если $h_i g = h_j g$, то

$$h_i = (h_i g)\, g^{-1} = (h_j g)\, g^{-1} = h_j.$$

Таким образом, элементы $h_1 g, \ldots, h_m g$ различны, т. е. каждый смежный класс по подгруппе H содержит m элементов. Ввиду теоремы 2, $n = km$.

Для случая групп теоремы 4 и 5 из § 2 могут быть усилены.

Теорема 4. *Если φ: $G \to G'$ — гомоморфизм групп и 1 — единица группы G, то $\varphi(1)$ — единица группы G' и $\varphi(g^{-1}) = (\varphi(g))^{-1}$ для всех $g \in G$.*

Доказательство. Имеем $\varphi(1)\, \varphi(1) = \varphi(1 \cdot 1) = \varphi(1)$, откуда

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

*) Число элементов группы G часто называют *порядком группы* G. Тогда теорема 3 звучит так: *порядок подгруппы делит порядок группы.*

где $1'$ — единица группы G'. Далее,

$$\varphi(g^{-1})\,\varphi(g) = \varphi(g^{-1}g) = \varphi(1) = 1' = \varphi(1) = \varphi(gg^{-1}) = \varphi(g)\,\varphi(g^{-1}),$$

откуда $\varphi(g^{-1}) = (\varphi(g))^{-1}$ по определению обратного элемента.

Из теорем 4, 5 и 6 из § 2 получаем:

Теорема 5. *Если* $\varphi\colon G \to G'$ *— гомоморфизм полугрупп и* G *— группа, то* $\operatorname{Im}\varphi$ *— группа.*

Следствие. *Если* $\varphi\colon G \to G'$ *— гомоморфное наложение полугрупп и* G *— группа, то* G' *— группа.*

Применяя это следствие к естественному гомоморфизму, убеждаемся, что факторполугруппа группы является группой. Поэтому ее естественно назвать *факторгруппой.*

В случае групп оказывается возможным получить более прозрачное описание допустимых разбиений, чем для произвольных полугрупп. Введем важное определение: подгруппа H группы G называется *нормальной*, если $ghg^{-1} \in H$ для любых $h \in H$ и $g \in G$. Если группа коммутативна, то, ввиду следствия теоремы 2 из § 2, $ghg^{-1} = h(gg^{-1}) = h1 = h$, т. е. любая подгруппа коммутативной группы нормальна.

Примером нормальной подгруппы может служить подгруппа матриц с определителем, равным 1, в группе невырожденных матриц (см. пример 4 из таблицы 3). Действительно, если $|A| = 1$, то для любой невырожденной матрицы B, учитывая теорему I.3.14, имеем

$$|BAB^{-1}| = |B|\,|A|\,|B^{-1}| = |B|\,|B^{-1}| = |E| = 1.$$

Напротив, подгруппа D диагональных матриц в группе невырожденных матриц второго порядка нормальной не является. Действительно,

$$\begin{Vmatrix}1 & 1\\ 0 & 1\end{Vmatrix}\begin{Vmatrix}1 & 0\\ 0 & 2\end{Vmatrix}\begin{Vmatrix}1 & 1\\ 0 & 1\end{Vmatrix}^{-1} = \begin{Vmatrix}1 & 1\\ 0 & 1\end{Vmatrix}\begin{Vmatrix}1 & 0\\ 0 & 2\end{Vmatrix}\begin{Vmatrix}1 & -1\\ 0 & 1\end{Vmatrix} = \begin{Vmatrix}1 & 2\\ 0 & 2\end{Vmatrix}\begin{Vmatrix}1 & -1\\ 0 & 1\end{Vmatrix} = \begin{Vmatrix}1 & 1\\ 0 & 2\end{Vmatrix} \notin D.$$

Теорема 6. *Следующие свойства подгруппы* H *группы* G *равносильны:*

(1) H *— нормальная подгруппа;*

(2) $gH = Hg$ *для всех* $g \in G$ **);*

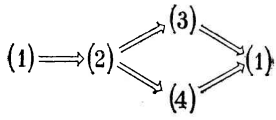
---

*) Это свойство, в частности, означает, что левое и правое разбиения по нормальной подгруппе H совпадают.

(3) *левое разбиение по подгруппе H допустимо*;

(4) *правое разбиение по подгруппе H допустимо.*

Доказательство. Достаточно доказать справедливость следующих импликаций:



(1) $\Rightarrow$ (2). Если $x \in gH$, то $x = gh$, где $h \in H$. Запишем

$$x = (ghg^{-1})\, g$$

и заметим, что $ghg^{-1} \in H$ по определению нормальной подгруппы. Следовательно, $x \in Hg$. Ввиду произвольности x имеем $gH \subseteq Hg$. Обратное включение доказывается аналогично.

(2) $\Rightarrow$ (3). Пусть $x, u \in aH$ и $y, v \in bH$, где $a, b \in G$. Тогда $x = ah_1$, $u = ah_2$, $y = bh_3$, $v = bh_4$, где $h_1, h_2, h_3, h_4 \in H$. Отсюда $xy = ah_1bh_3$ и $uv = ah_2bh_4$. Поскольку $Hb = bH$, то $h_1b = bh'$ и $h_2b = bh''$, где $h', h'' \in H$. Следовательно,

$$xy = abh'h_3 \in (ab)\, H$$

и

$$uv = abh''h_4 \in (ab)\, H,$$

что и доказывает допустимость левого разложения по H.

(2) $\Rightarrow$ (4). Аналогично.

(3) $\Rightarrow$ (1). Ясно, что при любом $h \in H$ элементы gh и g принадлежат одному смежному классу левого разбиения по подгруппе H. В силу допустимости этого разбиения, элементы ghg^{-1} и $gg^{-1} = 1$ также должны принадлежать одному смежному классу. Но $1 \in H$ и, следовательно, $ghg^{-1} \in H$.

(4) $\Rightarrow$ (1). Аналогично.

Теорема 7. *Всякое допустимое разбиение группы G является левым *) разбиением по некоторой нормальной подгруппе. Этой нормальной подгруппой является смежный класс разбиения, содержащий единицу.*

---

*) А в силу примечания на с. 74 также и правым.

Доказательство. Пусть Σ — допустимое разбиение группы G и H — смежный класс этого разбиения, содержащий 1. Если $h_1, h_2 \in H$, то, обозначив через $[x]$ смежный класс разбиения Σ, содержащий элемент x, будем иметь $[h_1] = [h_2] = [1]$. Из допустимости разбиения вытекает, что

$$[h_1h_2] = [1 \cdot 1] = [1] = H.$$

Таким образом, $h_1h_2 \in H$, т. е. H — подполугруппа. Если $h \in H$, то $[h] = [1]$. Из допустимости разбиения Σ вытекает, что

$$[h^{-1}] = [1 \cdot h^{-1}] = [hh^{-1}] = [1] = H,$$

т. е. $h^{-1} \in H$. Следовательно, H — подгруппа. Если K — некоторый класс разбиения Σ, то зафиксируем в K некоторый элемент k. Тогда $[k] = K$, и для всякого $h \in H$ имеем, что $[kh] = [k \cdot 1] = [k]$, т. е. $kh \in K$. Следовательно, $kH \subseteq K$. Если $x \in K$, то $[k^{-1}x] = [k^{-1}k] = [1]$. Следовательно, $k^{-1}x = h \in H$, откуда $x = kh \in kH$. Таким образом, $K \subseteq kH$, а значит, $K = kH$. Этим доказано, что разбиение Σ совпадает с разбиением по подгруппе H. Ее нормальность вытекает из теоремы 6.

Теорема 7 показывает, что вместо того, чтобы говорить о факторгруппе группы G по допустимому разбиению Σ, можно говорить о *факторгруппе группы G по нормальной подгруппе H*. В силу теоремы 7, эта нормальная подгруппа совпадает со смежным классом разбиения, содержащим единицу. С другой стороны, если $\varphi\colon G \to G'$ — гомоморфное наложение групп, то, в силу теоремы 7 из § 2, разбиение $\operatorname{Ker}\varphi$ допустимо и по той же причине определяется нормальной подгруппой, состоящей из всех прообразов единицы $1'$ группы G'. Поэтому в теории групп *ядром гомоморфизма* называют эту нормальную подгруппу и через $\operatorname{Ker}\varphi$ обозначают именно ее, т. е. $\operatorname{Ker}\varphi = \{g \mid g \in G,\ \varphi(g) = 1'\}$. В связи с этим теорему 8 из § 2 в случае групп можно переформулировать следующим образом.

Теорема 8 (теорема о гомоморфизме для групп). *Если $\varphi\colon G \to G'$ — гомоморфное наложение групп, $\operatorname{Ker}\varphi$ — нормальная подгруппа, являющаяся ядром этого гомоморфизма, и $\pi\colon G \to G/\operatorname{Ker}\varphi$ — естественный гомоморфизм, то существует изоморфизм $\chi\colon G' \to G/\operatorname{Ker}\varphi$ такой, что $\varphi\chi = \pi$.*

Если g — элемент группы G, а n — целое число, то полагаем *)

$$g^n = \begin{cases} \underbrace{g \dots g}_{n \text{ раз}}, & \text{если } n > 0, \\ 1, & \text{если } n = 0, \\ \underbrace{g^{-1} \dots g^{-1}}_{|n| \text{ раз}}, & \text{если } n < 0. \end{cases}$$

Теорема 9. $g^m \cdot g^n = g^{m+n}$.

Доказательство. Если $m = 0$, то

$$g^0 \cdot g^n = 1 \cdot g^n = g^n = g^{0+n}.$$

Случай, когда $n = 0$, рассматривается аналогично. Если же $m, n \neq 0$, то возможны следующие случаи:

	m	n
1	>0	>0
2	>0	<0
3	<0	>0
4	<0	<0

В случае 1, учитывая теорему 1 из § 2, имеем (ср. с теоремой 9 из § 2)

$$g^m \cdot g^n = \underbrace{(g \dots g)}_{m \text{ раз}} \underbrace{(g \dots g)}_{n \text{ раз}} = \underbrace{g \dots g}_{m+n \text{ раз}} = g^{m+n}.$$

Случай 2 распадается на подслучаи: а) $m > |n|$; б) $m = |n|$; в) $m < |n|$. При этом согласно правилам сложения чисел имеем $m + n = m - |n|$, $m + n = 0$ и $m + n = -(|n| - m)$ соответственно. Но тогда, поскольку $gg^{-1} = 1$, имеем

$$g^m \cdot g^n = \underbrace{(g \dots g)}_{m \text{ раз}} \underbrace{(g^{-1} \dots g^{-1})}_{|n| \text{ раз}} = \underbrace{g \dots g}_{m-|n| \text{ раз}} = g^{m-|n|} = g^{m+n},$$

$$g^m \cdot g^n = \underbrace{(g \dots g)}_{m \text{ раз}} \underbrace{(g^{-1} \dots g^{-1})}_{|n| \text{ раз}} = 1 = g^0 = g^{m+n}$$

*) Если операция в группе G записывается как сложение, то приводимое ниже определение выглядит так:

$$ng = \begin{cases} \underbrace{g + \dots + g}_{n \text{ раз}}, & \text{если } n > 0, \\ 0, & \text{если } n = 0, \\ \underbrace{(-g) + \dots + (-g)}_{|n| \text{ раз}}, & \text{если } n < 0. \end{cases}$$

Тогда доказываемые ниже теоремы 9 и 10 формулируются как $mg + ng = (m + n)g$ и $n(mg) = (mn)g$ соответственно.

или

$$g^m \cdot g^n = \underbrace{(g \dots g)}_{m \text{ раз}} \underbrace{(g^{-1} \dots g^{-1})}_{|n| \text{ раз}} = \underbrace{g^{-1} \dots g^{-1}}_{|n|-m \text{ раз}} = g^{-(|n|-m)} = g^{m+n}.$$

Случай 3 рассматривается аналогично.

В случае 4 имеем $m + n = -(|m| + |n|)$, откуда

$$g^m \cdot g^n = \underbrace{(g^{-1} \dots g^{-1})}_{|m| \text{ раз}} \underbrace{(g^{-1} \dots g^{-1})}_{|n| \text{ раз}} = \underbrace{g^{-1} \dots g^{-1}}_{|m|+|n| \text{ раз}} = g^{-(|m|+|n|)} = g^{m+n}.$$

Теорема 10. $(g^m)^n = g^{mn}$.

Доказательство. Если $m = 0$, то

$$(g^0)^n = 1^n = 1 = g^0 = g^{0 \cdot n}.$$

Если $n = 0$, то

$$(g^m)^0 = 1 = g^0 = g^{m \cdot 0}.$$

Если $m, n > 0$, то

$$(g^m)^n = \underbrace{\underbrace{(g \dots g)}_{m \text{ раз}} \dots \underbrace{(g \dots g)}_{m \text{ раз}}}_{n \text{ раз}} = \underbrace{g \dots g}_{mn \text{ раз}} = g^{mn}.$$

Далее, в силу теоремы 9 для любого целого числа k получаем

$$g^k g^{-k} = g^{-k} g^k = 1,$$

откуда

$$(g^k)^{-1} = g^{-k}.$$

Поэтому если $n < 0$, а значит, $n = -|n|$, то для любого целого числа m имеем

$$(g^m)^n = (g^m)^{-|n|} = ((g^m)^{|n|})^{-1} = (g^{m|n|})^{-1} = g^{-m|n|} = g^{mn}.$$

Если же $m < 0$, но $n > 0$, то

$$(g^m)^n = (g^{-|m|})^n = \underbrace{(g^{-1} \dots g^{-1})}_{|m| \text{ раз}}{}^n = ((g^{-1})^{|m|})^n = (g^{-1})^{|m|n} = g^{-|m|n} = g^{mn}.$$

Группа G называется *циклической*, если в ней существует такой элемент g, что для всякого x из G найдется такое целое число n, что $x = g^n$. Этот элемент g называется *образующим* (или *порождающим*) циклической группы G. Из теоремы 9 вытекает, что всякая циклическая группа коммутативна. В случае группы $\boldsymbol{Z}$ целых чисел по

сложению в качестве образующего можно взять 1 или -1, так что аддитивная группа целых чисел циклична. Если m — некоторое положительное целое число, то множество $\boldsymbol{Z}m$ всех целых чисел, делящихся на m, оказывается подгруппой. В силу коммутативности группы $\boldsymbol{Z}$, эта подгруппа является нормальной. Поэтому можно рассмотреть факторгруппу $\boldsymbol{Z}/\boldsymbol{Z}m$, которая называется *группой вычетов по модулю* m. Группа вычетов по модулю m содержит смежные классы $[0], [1], [2], \ldots, [m-1]$. Все эти классы различны, ибо $i - j \notin \boldsymbol{Z}m$, если $0 \leqslant j < i < m$. Убедимся, что других элементов в ней нет. Действительно, любое целое число u можно записать в виде $u = mq + r$, где $0 \leqslant r < m$. Учитывая равенство $[mq] = [0]$, вытекающее из включения $mq \in \boldsymbol{Z}m$, и определение операций в факторгруппе, получаем

$$[u] = [mq + r] = [mq] + [r] = [0] + [r] = [r].$$

Таким образом, группа вычетов по модулю m содержит в точности m элементов. Класс $[1]$ служит ее образующим. Естественно спросить: какие другие классы вычетов являются образующими этой группы? На этот вопрос отвечает

Теорема 11. *Класс* $[k]$, *где* $0 \leqslant k < m$, *является образующим группы вычетов по модулю* m *тогда и только тогда, когда числа* k *и* m *взаимно просты.*

Доказательству теоремы предпошлем следующую лемму:

Лемма. *Всякая ненулевая подгруппа группы* $\boldsymbol{Z}$ *совпадает с* $\boldsymbol{Z}m$ *для некоторого* m.

Доказательство. Пусть H — ненулевая подгруппа группы $\boldsymbol{Z}$. Тогда H содержит положительные целые числа. Пусть m — наименьшее среди них. Тогда $\boldsymbol{Z}m \subseteq H$. Если же x — произвольный элемент из H, то, разделив x на m с остатком, будем иметь $x = qm + r$, где $0 \leqslant r < m$. Ясно, что $r = x - qm \in H$. Если $r \neq 0$, то вступаем в противоречие с выбором числа m. Следовательно, $r = 0$. Отсюда $x = qm \in \boldsymbol{Z}m$, т. е. $H \subseteq \boldsymbol{Z}m$. Таким образом, $H = \boldsymbol{Z}m$, что и требовалось.

Доказательство теоремы 11. Допустим, что класс $[k]$ является образующим группы вычетов по модулю m. Если k и m не взаимно просты, то $k = k'd$ и $m = m'd$, где $d > 1$. Тогда

$$[m'k] = [m'k'd] = [mk'] = [0],$$

ибо $mk' \in \boldsymbol{Z}m$. Далее рассмотрим классы

$$[0],\ [k],\ [2k],\ \ldots,\ [(m'-1)\,k].$$

Так как $d > 1$, их меньше чем m. С другой стороны, для всякого целого s имеем $s = qm' + r$, где q — некоторое целое число и $0 \leqslant r < m'$. Отсюда

$$[sk] = [(qm' + r)k] = [qm'k] + [rk] = [qm'k'd] + [rk] = [qk'm] + [rk] = [0] + [rk] = [rk],$$

поскольку $qk'm \in \boldsymbol{Z}m$. Следовательно, выписанными выше классами исчерпываются все элементы группы вычетов по модулю m, что невозможно. Допустим теперь, что k и m взаимно просты. Тогда найдутся целые числа u и v такие, что $um + vk = 1$ *).

Отсюда

$$[1] = [um] + [vk] = [0] + [vk] = [vk].$$

Поэтому для любого $[s] \in \boldsymbol{Z}/\boldsymbol{Z}m$ (напомним, что $0 \leqslant s < m$)

$$[s] = s\,[1] = s\,[vk] = [svk] = (sv)\,[k]\ **),$$

т. е. $[k]$ оказывается образующим.

Строение циклических групп описывается следующей теоремой.

Т е о р е м а 12. *Всякая циклическая группа изоморфна или группе целых чисел по сложению, или группе вычетов по некоторому модулю m.*

Д о к а з а т е л ь с т в о. Пусть G — циклическая группа с образующим g. Рассмотрим отображение φ:

---

*) Это является следствием следующего утверждения:

Если m и n — целые числа и $d =$ н. о. д. *(m, n)* (т. е. наибольший общий делитель m и n), *то найдутся такие целые числа u и v, что $um + vn = d$.*

Для доказательства рассмотрим множества I всех целых чисел, представимых в форме $sm + tn$, где s и t — какие-то целые числа. Легко проверяется, что множество I является подгруппой группы $\boldsymbol{Z}$ и, в силу леммы, совпадает с $\boldsymbol{Z}d'$ для некоторого целого положительного d'. Поскольку $m = 1 \cdot m + 0 \cdot n \in I$ и $n = 0 \cdot m + 1 \cdot n \in I$, имеем $m = m'd'$ и $n = n'd'$ для подходящих m' и n'. Следовательно, d' оказывается общим делителем чисел m и n. Если же d'' — какой-либо общий делитель этих чисел, то $m = m''d''$ и $n = n''d''$ для подходящих m'' и n''. Поскольку $d' \in I$, то $d' = um + vn$ для некоторых целых чисел u и v. Поэтому

$$d' = um + vn = um''d'' + vn''d'' = (um'' + vn'')\,d'',$$

т. е. d' оказывается наибольшим общим делителем чисел m и n. Отсюда $d = \pm d'$, чем и заканчивается доказательство.

**) См. примечание на с. 77.

$Z \to G$, определяемое равенством $\varphi(n) = g^n$. Из цикличности группы G вытекает, что φ — наложение. В силу теоремы 9

$$\varphi(k + l) = g^{k+l} = g^k \cdot g^l = \varphi(k)\,\varphi(l),$$

т. е. φ оказывается гомоморфизмом. В силу теоремы 8, группа G изоморфна фактогруппе $\boldsymbol{Z}/\mathrm{Ker}\,\varphi$. Если $\mathrm{Ker}\,\varphi = \{0\}$, то все смежные классы по подгруппе $\mathrm{Ker}\,\varphi$ одноэлементные. Следовательно, $\boldsymbol{Z}/\mathrm{Ker}\,\varphi$ совпадает с $\boldsymbol{Z}$ и, значит, G изоморфна $\boldsymbol{Z}$. Если же $\mathrm{Ker}\,\varphi \neq 0$, то в силу леммы, предпосланной доказательству теоремы 11, $\mathrm{Ker}\,\varphi = \boldsymbol{Z}m$ для некоторого m и, следовательно, $\boldsymbol{Z}/\mathrm{Ker}\,\varphi$ является группой вычетов по модулю m, которой и изоморфна группа G.

Как уже отмечалось (полугруппа 12 из таблицы 1), множество всех взаимно однозначных отображений некоторого множества на себя является группой. Эта группа является в некотором смысле универсальной, как показывает следующая

Теорема 13 (теорема Кэли). *Для всякой группы G существует гомоморфное вложение ее в группу Q взаимно однозначных отображений множества G на себя* *).

Доказательство. Если $g \in G$, то обозначим через $\varphi(g)$ отображение множества G в себя, определяемое равенством $x(\varphi(g)) = xg$ для всех $x \in G$. Так как

$$x = (xg^{-1})g = (xg^{-1})(\varphi(g)),$$

то $\varphi(g)$ оказывается наложением. Если $x(\varphi(g)) = y(\varphi(g))$, то

$$x = (xg)\,g^{-1} = (x(\varphi(g)))\,g^{-1} = (y(\varphi(g)))g^{-1} = (yg)g^{-1} = y,$$

т. е. $\varphi(g)$ является вложением множества G в себя. Таким образом, $\varphi(g)$ — взаимно однозначное отображение множества G на себя, т. е. φ отображает G в Q. Если $\varphi(g_1) = \varphi(g_2)$, то

$$g_1 = 1(\varphi(g_1)) = 1(\varphi(g_2)) = g_2,$$

т. е. φ оказывается вложением. Из равенств

$$x(\varphi(g_1)\,\varphi(g_2)) = (x(\varphi(g_1)))(\varphi(g_2)) = (xg_1)\,g_2 = x(g_1g_2) = x(\varphi(g_1g_2)),$$

*) Ввиду теоремы 5, эта теорема допускает и такую формулировку: *всякая группа изоморфна подгруппе группы взаимно однозначных отображений некоторого множества на себя.*

где x — произвольный элемент из G, вытекает, что

$$\varphi(g_1)\,\varphi(g_2) = \varphi(g_1 g_2),$$

чем доказывается, что φ — гомоморфизм.

Пример. Пусть $G = \boldsymbol{Z}/3\boldsymbol{Z}$. Тогда группа Q, рассмотренная в теореме 13,— это группа подстановок множества $\{0, 1, 2\}$, и вложение φ, описанное в ходе доказательства теоремы 13, выглядит следующим образом:

$$\varphi([0]) = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}, \quad \varphi([1]) = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}, \quad \varphi([2]) = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}.$$

Из доказательства теоремы 13 видно, что всякая конечная группа вкладывается в группу взаимно однозначных отображений конечного множества на себя, т. е. в группу подстановок множества $\{1, 2, \ldots, n\}$ для некоторого n. Эту группу называют *симметрической группой степени n* и обозначают $\mathfrak{S}_n$. Симметрическая группа степени n содержит $n!$ элементов. Остановимся на некоторых из ее свойств.

Назовем *циклом* и обозначим $(i_1 \ldots i_k)$, где $i_1, \ldots, i_k$ — некоторые различные числа из множества $\{1, 2, \ldots, n\}$, такую подстановку σ, что

$$\sigma(i) = \begin{cases} i, & \text{если } i \neq i_1, \ldots, i_k, \\ i_{h+1}, & \text{если } i = i_h \text{ и } h \neq k, \\ i_1, & \text{если } i = i_k. \end{cases}$$

Например, в группе $\mathfrak{S}_6$ имеем

$$(135) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 1 & 6 \end{pmatrix}.$$

Двухэлементный цикл называется *транспозицией*. Транспозицией будет, например, подстановка

$$(35) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 3 & 6 \end{pmatrix}.$$

В дальнейшем термин *цикл* и символ $(i_1 \ldots i_k)$ обозначают как определенную выше подстановку, так и подмножество $\{i_1, \ldots, i_k\}$ множества $\{1, 2, \ldots, n\}$. Циклы, не содержащие общих элементов, называются *независимыми*. Например, в группе $\mathfrak{S}_6$ независимыми циклами будут (126) и (35).

Теорема 14. *Если ρ и σ — независимые циклы, то* $\rho\sigma = \sigma\rho$.

Доказательство. Заметим, что $i \in \rho$ влечет $i\rho \in \rho$, $i\rho \notin \sigma$ и $i \notin \sigma$. Аналогично, $i\sigma \in \sigma$, $i\sigma \notin \rho$ и $i \notin \rho$, если $i \in \sigma$. Поэтому

$$i(\rho\sigma) = (i\rho)\sigma = \begin{cases} i\sigma = i, & \text{если } i \notin \rho \cup \sigma, \\ i\rho, & \text{если } i \in \rho, \\ i\sigma, & \text{если } i \in \sigma, \end{cases}$$

и

$$i(\sigma\rho) = (i\sigma)\rho = \begin{cases} i\rho = i, & \text{если } i \notin \rho \cup \sigma, \\ i\rho, & \text{если } i \in \rho, \\ i\sigma, & \text{если } i \in \sigma. \end{cases}$$

Таким образом, $i(\rho\sigma) = i(\sigma\rho)$ для всех i, т. е. $\rho\sigma = \sigma\rho$.

Теорема 14 вместе с теоремой 2 из § 2 дает:

Теорема 15. *Если циклы* $\sigma_1, \ldots, \sigma_m$ *попарно независимы, то*

$$\sigma_1 \ldots \sigma_m = \sigma_{\pi(1)} \ldots \sigma_{\pi(m)}$$

для любой подстановки $\pi \in \mathfrak{S}_m$.

Теорема 16. *Каждая подстановка* τ *представляется в виде произведения попарно независимых циклов.*

Доказательство. Для каждого i рассмотрим множество $\{i = i\tau^0, i\tau, i\tau^2, i\tau^3, \ldots\}$. Так как $i\tau^k \in \{1, 2, \ldots, n\}$, то существует такое m, что $i\tau^m = i\tau^{m+h}$ для некоторого $h > 0$. Отсюда, учитывая теоремы 9 и 10, получаем

$$i = (i\tau^m)(\tau^m)^{-1} = i(\tau^{m+h-m}) = i\tau^h.$$

Можно считать h выбранным так, что числа $i, i\tau, \ldots, i\tau^{h-1}$ различны. Про цикл $\sigma = (i\ (i\tau) \ldots (i\tau^{h-1}))$ скажем, что он является *орбитой* подстановки τ, порожденной элементом i. Если u — произвольное целое число, то, записав $u = hq + r$, где $0 \leqslant r < h$, получим

$$i\tau^u = i(\tau^{hq}\tau^r) = (i((\tau^h)^q))\,\tau^r = i\tau^r \in \sigma.$$

Лемма 1. *Две орбиты подстановки* τ *или не пересекаются, или совпадают.*

Действительно, если орбиты $\sigma = (i\ (i\tau) \ldots (i\tau^{h-1}))$ и $\rho = (j\ (j\tau) \ldots (j\tau^{l-1}))$ содержат число d, то $d = i\tau^s = j\tau^t$, где, скажем, $t \geqslant s$. Но тогда

$$i = (j\tau^t)(\tau^s)^{-1} = j\tau^{t-s} \in \rho,$$

откуда $\sigma \subseteq \rho$. Аналогично получаем, что $\rho \subseteq \sigma$. Таким образом, $\sigma = \rho$.

Лемма 2. *Если* σ — *орбита подстановки* τ *и* $i \in \sigma$, *то* $i\tau = i\sigma$ (не забудьте о двусмысленности слова «цикл»!).

В самом деле, пусть $\sigma = (k\ (k\tau) \ldots (k\tau^{r-1}))$. Тогда $i = k\tau^h$, где $0 \leqslant h < r$, откуда

$$i\sigma = (k\tau^h)\,\sigma = \begin{cases} k = k\tau^r = (k\tau^{r-1})\,\tau = i\tau, & \text{если } h = r-1, \\ k\tau^{h+1} = (k\tau^h)\,\tau = i\tau, & \text{если } 0 \leqslant h < r-1. \end{cases}$$

Возвращаясь к доказательству теоремы, допустим, что $\sigma_1, \ldots, \sigma_m$ — все неодноэлементные орбиты подстановки τ. Если $i \notin \sigma_1 \cup \ldots \cup \sigma_m$, то $i\sigma_k = i$ для всех k, откуда

$$i\sigma_1 \ldots \sigma_m = i = i\tau.$$

В противном случае, ввиду леммы 1, $i \in \sigma_s$ в точности для одной орбиты σ_s. Поэтому $i \notin \sigma_1 \cup \ldots \cup \sigma_{s-1}$ и, значит, $i\sigma_1 = \ldots = i\sigma_{s-1} = i$. Кроме того, $i\tau \in \sigma_s$, откуда $i\tau \notin \sigma_{s+1} \cup \ldots \cup \sigma_m$ и, следовательно, $(i\tau)\sigma_{s+1} = \ldots = (i\tau)\sigma_m = i\tau$. Отсюда, учитывая лемму 2, получаем

$$i\sigma_1 \ldots \sigma_{s-1}\sigma_s\sigma_{s+1} \ldots \sigma_m = (i\sigma_s)\,\sigma_{s+1} \ldots \sigma_m = (i\tau)\,\sigma_{s+1} \ldots \sigma_m = i\tau.$$

Таким образом,

$$i\tau = i\,(\sigma_1 \ldots \sigma_m)$$

для всех i, т. е. $\tau = \sigma_1 \ldots \sigma_m$. Независимость циклов $\sigma_1, \ldots, \sigma_m$ вытекает из леммы.

Теорема 17. *Каждая подстановка представляется в виде произведения транспозиций.*

Доказательство. Ввиду теоремы 16 достаточно установить равенство

$$(i_1 \ldots i_k) = (i_1 i_2)(i_1 i_3) \ldots (i_1 i_k). \qquad (*)$$

Но $i\,((i_1 i_2) \ldots (i_1 i_k)) = i$, если $i \neq i_1, \ldots, i_k$. Если $i = i_k$, то

$$i\,((i_1 i_2) \ldots (i_1 i_k)) = i_k\,(i_1 i_k) = i_1.$$

Если же $i = i_s$, где $1 \leqslant s < k$, то

$$i\,((i_1 i_2) \ldots (i_1 i_k)) = i_s\,((i_1 i_s)\,(i_1 i_{s+1}) \ldots (i_1 i_k)) = i_1\,((i_1 i_{s+1}) \ldots (i_1 i_k)) = i_{s+1}\,((i_1 i_{s+2}) \ldots (i_1 i_k)) = i_{s+1}.$$

Таким образом,

$$i\,((i_1 i_2) \ldots (i_1 i_k)) = i\,(i_1 \ldots i_k)$$

для всех i, т. е. равенство $(*)$ справедливо.

Поскольку орбиты подстановки определены однозначно, из доказательства теоремы 16 можно усмотреть, что каждая подстановка представляется в виде произведения попарно независимых циклов однозначно с точностью до порядка сомножителей. Для представления подстановки в виде произведения транспозиций это не так, ибо из равенства (*) вытекает

$$(13)(15) = (135) = (351) = (35)(31).$$

Правда, $(13) = (31)$, но $(15) \neq (35)$. Некоторым утешением может служить следующая теорема.

Теорема 18. *Четность подстановки равна четности числа транспозиций, входящих в ее представление.*

Доказательство. Сначала будет установлена

Лемма. *Для любой подстановки* τ *и транспозиции* (ij) *подстановки* τ *и* $(ij)\,\tau$ *имеют различные четности.*

Действительно,

$$k((ij)\tau) = \begin{cases} k\tau, & \text{если } k \neq i,\ j, \\ j\tau, & \text{если } k = i, \\ i\tau, & \text{если } k = j. \end{cases}$$

Таким образом, если

$$\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix},$$

то

$$(ij)\tau = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ \tau(1) & \dots & \tau(j) & \dots & \tau(i) & \dots & \tau(n) \end{pmatrix}$$

и лемма вытекает из теоремы I.2.8.

Теперь, если $\tau = \tau_1 \dots \tau_m$, где τ_h — транспозиции, нужное утверждение следует из очевидного равенства $\tau = \tau_1 \dots \tau_m \varepsilon$, где ε — тождественная подстановка, являющаяся, конечно, четной. Надо только принять во внимание, что, ввиду леммы, при умножении на каждую из τ_h четность меняется.

Теорема 19. *Четные подстановки образуют нормальную подгруппу* $\mathfrak{A}_n$ *группы* $\mathfrak{S}_n$.

Доказательство. Пусть $\mathfrak{A}_n$ — совокупность всех четных подстановок из $\mathfrak{S}_n$. Ясно, что тождественная подстановка принадлежит $\mathfrak{A}_n$. Если $\sigma,\ \tau \in \mathfrak{A}_n$, то $\sigma\tau \in \mathfrak{A}_n$ ввиду теорем 17 и 18. Имеет место

Лемма. *Если* $\sigma_1, \dots, \sigma_m$ — *транспозиции, то*

$$(\sigma_1 \dots \sigma_m)^{-1} = \sigma_m \dots \sigma_1.$$

Для доказательства заметим, что $\sigma_i^2 = \varepsilon$, где ε — тождественная подстановка. Отсюда

$$\sigma_1 \ldots \sigma_m\sigma_m \ldots \sigma_1 = \varepsilon = \sigma_m \ldots \sigma_1\sigma_1 \ldots \sigma_m.$$

Если теперь $\sigma \in \mathfrak{A}_n$, то, ввиду леммы, из теорем 17 и 18 вытекает, что $\sigma^{-1} \in \mathfrak{A}_n$. Таким образом, $\mathfrak{A}_n$ — подгруппа в $\mathfrak{S}_n$. Если, наконец, $\sigma \in \mathfrak{A}_n$ и $\rho = \rho_1 \ldots \rho_m \in \in \mathfrak{S}_n$, где ρ_i — транспозиции, то, ввиду леммы,

$$\rho\sigma\rho^{-1} = \rho_1 \ldots \rho_m\sigma\rho_m \ldots \rho_1.$$

Но тогда из теоремы 18 вытекает, что

$$(\text{четность } \rho\sigma\rho^{-1}) = (\text{четность } \sigma) + 2m = (\text{четность } \sigma),$$

т. е. $\rho\sigma\rho^{-1} \in \mathfrak{A}_n$, если $\sigma \in \mathfrak{A}_n$.

Группу $\mathfrak{A}_n$ часто называют *знакопеременной группой*. Вернемся к рассмотрению произвольных групп.

Элемент z группы G называется *центральным*, если $zg = gz$ для всех $g \in G$. Множество всех центральных элементов группы G называется ее *центром*.

Т е о р е м а 20. *Центр Z группы G является ее подгруппой, и каждая подгруппа группы Z оказывается нормальной подгруппой группы G.*

Д о к а з а т е л ь с т в о. Ясно, что Z содержит единицу. Если $z', z'' \in Z$, то для любого $g \in G$ имеем

$$(z'z'')g = z'(z''g) = z'(gz'') = (z'g)z'' = (gz')z'' = g(z'z''),$$

т. е. $z'z'' \in Z$. Если $z \in Z$, то $gz = zg$ для всех $g \in G$. Отсюда

$$z^{-1}g = z^{-1}gzz^{-1} = z^{-1}zgz^{-1} = gz^{-1},$$

т. е. $z^{-1} \in Z$. Таким образом, Z — подгруппа. Наконец, если H — подгруппа группы Z, $g \in G$ и $h \in H$, то

$$ghg^{-1} = hgg^{-1} = h \in H.$$

Если a — элемент группы G, то про всякий элемент вида gag^{-1}, где $g \in G$, скажем, что он *сопряжен с элементом a*. Множество всех элементов, сопряженных с элементом a, называется его *классом сопряженности*. Ясно, что любой элемент содержится в своем классе сопряженности (достаточно взять $g = 1$) и что класс сопряженности центрального элемента никаких других элементов не содержит.

Т е о р е м а 21. *Два класса сопряженности группы G или не пересекаются, или совпадают, т. е. классы сопряженности группы G образуют разбиение.*

Доказательство. Пусть K и L — классы сопряженности элементов a и b соответственно, и пусть $u \in K \cap L$. Тогда $u = gag^{-1} = hbh^{-1}$, где $g, h \in G$. Если $v \in K$, то $v = cac^{-1}$ для некоторого $c \in G$. Отсюда

$$v = cg^{-1}ugc^{-1} = cg^{-1}hbh^{-1}gc^{-1} = (cg^{-1}h)b(cg^{-1}h)^{-1} \in L.$$

Таким образом, $K \subseteq L$. Обратное включение доказывается аналогично.

Пример. Непосредственным подсчетом можно убедиться, что группа $\mathfrak{S}_3$ распадается на следующие три класса сопряженности:

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

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

Теорема 22. *Пусть конечная группа G содержит n элементов и $g \in G$. Тогда $g^n = 1$, и если $g^m = 1$, но $g^k \neq 1$ при $1 \leqslant k < m$, то m делит n.*

Доказательство. Пусть $g \in G$, $g^m = 1$ и $g^k \neq 1$, если $1 \leqslant k < m$. Для любого целого положительного числа s имеем $s = qm + r$, где $0 \leqslant r < m$. В силу теорем 9 и 10,

$$g^s = (g^m)^q g^r = 1g^r = g^r.$$

Кроме того, если $0 < k < m$, то $g^k g^{m-k} = 1$ и $0 < m - k < m$. Следовательно, $\{1, g, \ldots, g^m\}$ — подгруппа группы G, содержащая m элементов. По теореме 3, m делит n. Этим доказано второе утверждение теоремы. Для доказательства первого рассмотрим множество $\{g, g^2, g^3, \ldots\}$. Ввиду конечности группы G, найдется такое число m, что $g^k = g^{k+m}$ для некоторого $m > 0$. Можно считать, что среди элементов $g^k, g^{k+1}, \ldots, g^{k+m-1}$ нет одинаковых. В силу теорем 9 и 10, отсюда вытекает, что

$$1 = g^k g^{-k} = g^{k+m} g^{-k} = g^m$$

и что среди элементов $1, g, g^2, \ldots, g^{m-1}$ нет одинаковых. Как доказано выше, отсюда вытекает, что $n = qm$ для некоторого целого числа q, и, следовательно, $g^n = (g^m)^q = 1^q = 1$ в силу теоремы 10.

В дальнейшем условимся обозначать через $|X|$ число элементов множества X (не путать с определителем матрицы!).

Теорема 23. *Пусть $K(g)$ — класс сопряженности элемента g группы G и $C(g)$ — множество всех таких*

элементов $x \in G$, что $xg = gx$. Тогда $C(g)$ — подгруппа группы G и $|K(g)||C(g)| = |G|$.

Доказательство. Положим $L = C(g)$. Ясно, что $1 \in L$. Если $x, y \in L$, то

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$$

и

$$x^{-1}g = x^{-1}g(xx^{-1}) = (x^{-1}(gx))x^{-1} = (x^{-1}(xg))x^{-1} = gx^{-1},$$

т. е. xy и x^{-1} принадлежат L. Следовательно, L — подгруппа. Обозначим через G/L множество правых смежных классов группы G по подгруппе L (подчеркнем, что, поскольку подгруппа L не предполагается нормальной, это не обязательно факторгруппа!) и определим отображение φ: $K(g) \to G/L$, полагая

$$\varphi(u^{-1}gu) = Lu.$$

Если $u^{-1}gu = v^{-1}gv$ для некоторых $u, v \in G$, то $(vu^{-1})g = g(vu^{-1})$. Отсюда $vu^{-1} \in L$. Поэтому $v \in Lu$, а значит, $Lu = Lv$. Этим доказана корректность определения отображения φ. Ясно, что это наложение. Если $\varphi(u^{-1}gu) = \varphi(v^{-1}gv)$, то $Lu = Lv$. Отсюда $u = lv$ для некоторого $l \in L$, а значит,

$$u^{-1}gu = v^{-1}l^{-1}glv = v^{-1}l^{-1}lgv = v^{-1}gv.$$

Таким образом, φ — вложение, а значит, и взаимно однозначное отображение. Учитывая теорему 3′, получаем

$$|K(g)||L| = |G/L||L| = |G|.$$

Теорема 24. *Центр группы G, где $|G| = p^k$, причем p — простое число и $k \geqslant 1$, содержит более одного элемента.*

Доказательство. Допустим, что 1 — единственный центральный элемент группы G, а $g_1, \ldots, g_t$ — представители всех остальных классов сопряженности. Положим $L_i = C(g_i)$. Ввиду теоремы 22, получаем

$$|K(g_i)||L_i| = p^k.$$

Отсюда $|L_i| = p^{k_i}$, где $0 \leqslant k_i \leqslant k$, а значит,

$$|K(g_i)| = p^{k-k_i}.$$

Если $k = k_i$ для некоторого i, то $|L_i| = |G|$. Отсюда $L_i = G$, т. е. g_i оказывается центральным элементом вопреки его выбору. Таким образом, $k - k_i \geqslant 1$ для всех i.

Представляя группу G в виде объединения классов сопряженности (см. теорему 21), получаем

$$p^k = |G| = 1 + |K(g_1)| + \ldots + |K(g_t)| = 1 + p^{k-k_1} + \ldots + p^{k-k_t},$$

т. е.

$$1 = p(p^{k-1} - p^{k-k_1-1} - \ldots - p^{k-k_t-1}),$$

что невозможно.

Упражнения

1. Доказать, что если A и B — группы, то $A \times B$ — группа (см. упражнение 7 из § 2), причем A и B изоморфны некоторым из ее нормальных подгрупп, а факторгруппа $(A \times B)/H$, где $H = \{(a, 1) \mid a \in A\}$, изоморфна группе B.

2. Показать, что $(ab)^{-1} = b^{-1}a^{-1}$ для любых элементов a и b из группы. Обобщить на произведение n элементов.

3. Доказать, что пересечение любого множества нормальных подгрупп является нормальной подгруппой.

4. Доказать, что множество матриц вида λE, где λ — отличное от нуля число, является нормальной подгруппой группы невырожденных матриц, а подгруппа примера 6 из таблицы 3 нормальной не является.

5. Доказать утверждение: если H и K — подгруппы G, содержащие m и n элементов соответственно, а числа m и n взаимно просты, то $H \cap K = \{1\}$.

6. Пусть $\varphi: G \to G'$ — гомоморфизм групп, H — подгруппа группы G, $\varphi(H)$ — множество всех элементов вида $\varphi(h)$, где $h \in H$. Доказать а) $\varphi(H)$ — подгруппа группы G'; б) если φ — наложение, а подгруппа H нормальна, то подгруппа $\varphi(H)$ также нормальна; в) если H' — подгруппа группы G' и φ — наложение, то существует такая подгруппа H группы G, что $\varphi(H) = H'$; г) если H и K — подгруппы группы G, содержащие $\operatorname{Ker}\varphi$, то $\varphi(H \cap K) = \varphi(H) \cap \varphi(K)$.

7. Доказать, что всякая факторгруппа и всякая подгруппа циклической группы является циклической группой.

8. Доказать, что группы $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$ и $\mathbf{Z}/4\mathbf{Z}$ не изоморфны.

9. Группа G не содержит подгрупп, отличных от G и от единичной, тогда и только тогда, когда она содержит p элементов, где p — простое число или 1, и, в частности, изоморфна группе вычетов по модулю p.

10. Пусть G — группа и $a \in G$. На множестве G определим новую операцию $\circ$, полагая $x \circ y = xay$. Доказать, что множество G с этой операцией является группой и что отображение $\varphi: G \to G$, где $\varphi(x) = xa^{-1}$, является изоморфизмом старой группы на новую.

11. Группа G называется *периодической*, если для всякого g из G найдется натуральное число n такое, что $g^n = 1$. Доказать, что для любой группы G и ее нормальной подгруппы H из периодичности групп H и G/H вытекает периодичность группы G.

12. Пусть G — группа положительных рациональных чисел по умножению и H — множество всех рациональных чисел, представимых в виде отношения двух положительных нечетных чисел. Доказать, что H — подгруппа и что факторгруппа G/H изоморфна группе Z.

13. Доказать, что не существует гомоморфного наложения группы всех рациональных чисел по сложению на группу всех целых чисел.

14. Осуществить вложение групп, указанных в упражнении 8, в группу $\mathfrak{S}_4$.

15. Пусть φ — отображение группы $\mathfrak{S}_n$ в группу невырожденных матриц порядка n, определяемое условием $\varphi(\sigma) = A$, где

$$a_{ij} = \begin{cases} 1, & \text{если } \sigma(i) = j, \\ 0 & \text{в противном случае.} \end{cases}$$

Доказать, что φ — гомоморфное вложение.

16. Доказать, что центр группы $\mathfrak{S}_n$ состоит из одной тождественной подстановки, а центр группы невырожденных матриц совпадает с множеством матриц вида λE, где λ — отличное от нуля число.

17. Если G — группа, Z — ее центр и $|G| = p^k$, где p — простое число, то $|Z| \geqslant p$.

18. Если факторгруппа группы G по ее центру циклическая, то G коммутативна.

§ 4. Кольца

Множество R с двумя операциями — сложением и умножением — называется *кольцом*, если

(1) R образует коммутативную группу относительно сложения (она называется *аддитивной группой* кольца);

(2) R образует полугруппу относительно умножения (она называется *мультипликативной полугруппой* кольца);

(3) сложение и умножение связаны дистрибутивными законами $(a + b)c = ac + bc$ и $a(b + c) = ab + ac$.

Ввиду (1), кольцо содержит нуль. Единица мультипликативной полугруппы (если она существует) называется *единицей кольца*. Вместо $a + (-b)$ обычно пишут $a - b$. Кольцо называется *коммутативным*, если коммутативна его мультипликативная полугруппа. Примерами колец служат целые, четные, рациональные и действительные числа с обычными операциями. Ввиду изложенного в конце гл. I, кольцо образуют квадратные матрицы порядка n. В отличие от перечисленных выше, это кольцо не коммутативно. За исключением кольца четных чисел, все вышеупомянутые кольца обладают единицей. Всякую коммутативную группу A можно превратить в кольцо, положив $ab = 0$ для любых $a, b \in A$. Это кольцо называется *кольцом с нулевым умножением*. Оно коммутативно, но без единицы. Коммутативное кольцо образуют действительные функции с обычными операциями. Его единицей служит функция, тождественно равная 1.

Из определения кольца можно вывести следующие свойства:

(а) $0 \cdot a = a \cdot 0 = 0$;
(б) $a(-b) = (-a)\, b = -ab$;
(в) $(a - b)\, c = ac - bc$, $a(b - c) = ab - ac$.

Действительно, учитывая свойства нуля и дистрибутивность, имеем

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

Прибавив к обеим частям $-0a$, получим $0 = 0a$. Аналогично доказывается, что $a0 = 0$. Далее, равенство $a(-b) = -ab$ вытекает из соотношения

$$ab + a(-b) = a(b + (-b)) = a0 = 0,$$

получаемого с учетом (а). Аналогично получаем, что $(-a)\, b = -ab$. Наконец, учитывая (б) и определение разности $a - b$, выводим

$$(a - b)\, c = (a + (-b))\, c = ac + (-b)c = \\ = ac + (-bc) = ac - bc$$

и, аналогично,

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

Подмножество H кольца R называется *подкольцом*, если оно является подгруппой его аддитивной группы и подполугруппой его мультипликативной полугруппы. Ясно, что подкольцо является кольцом относительно операций, определенных в исходном кольце. В качестве примеров можно указать кольцо четных чисел как подкольцо кольца целых чисел, а последнее как подкольцо колец рациональных и действительных чисел. Диагональные матрицы образуют подкольцо кольца матриц. Всякая подгруппа аддитивной группы кольца с нулевым умножением является подкольцом.

Согласно теоремам 3 из § 2 и 1 из § 3, справедлива

Т е о р е м а 1. *Пересечение любого множества подколец является подкольцом.*

Отображение φ кольца R в кольцо R' называется *гомоморфизмом*, если $\varphi(x + y) = \varphi(x) + \varphi(y)$ и $\varphi(xy) = \varphi(x)\, \varphi(y)$ для любых $x, y \in R$. Таким образом, кольцевой гомоморфизм является как гомоморфизмом аддитивных групп, так и гомоморфизмом мультипликативных полугрупп. Взаимно однозначный гомоморфизм называется *изоморфизмом*. Если существует изоморфизм кольца R на кольцо R', то эти кольца называются *изоморфными* *).

*) См. примечание на с. 60.

В качестве примеров укажем гомоморфизмы кольца диагональных матриц второго порядка и кольца действительных функций в кольцо действительных чисел, определяемые условиями

$$\varphi\left(\begin{Vmatrix} a & 0 \\ 0 & b \end{Vmatrix}\right) = a \text{ и } \varphi(f(x)) = f(0)$$

соответственно.

Согласно теоремам 6 из § 2 и 5 из § 3, справедлива

Т е о р е м а 2. *Если* $\varphi\colon R \to R'$ — *гомоморфизм колец, то* $\operatorname{Im}\varphi$ — *подкольцо кольца* R.

Разбиение кольца R называется *допустимым*, если оно является допустимым как для его аддитивной группы, так и для его мультипликативной полугруппы. Другими словами, разбиение Σ кольца R допустимо, если из того, что одному его смежному классу принадлежат как x и u, так и y и v, вытекает, что в одном и том же смежном классе лежат $x + y$ и $u + v$ и, кроме того, что в одном смежном классе лежат xy и uv.

Разбиение множества целых чисел, описанное в примере 1 из § 2, является допустимым разбиением кольца целых чисел, ибо приведенную там таблицу можно дополнить следующими столбцами:

	xy	uv
1	четное	четное
2	четное	четное
3	четное	четное
4	нечетное	нечетное

Если Σ — допустимое разбиение кольца R, то на фактормножестве R/Σ определим операции

$$[x] + [y] = [x + y]$$

и

$$[x][y] = [xy].$$

Допустимость разбиения позволяет доказать корректность этих определений (см. с. 62). После этого нетрудно проверить справедливость свойств (1)—(3) из определения кольца. Таким образом, фактормножество R/Σ оказывается кольцом. Это кольцо называется *факторкольцом* кольца R по разбиению Σ. Отображение, ставящее в соответствие каждому элементу из R содержащий его

смежный класс разбиения, оказывается кольцевым гомоморфизмом. Этот гомоморфизм называется *естественным*.

Для рассмотренного выше допустимого разбиения кольца целых чисел факторкольцо состоит из двух элементов. Обозначив их *чет* и *нечет*, получим следующие таблицы сложения и умножения:

$+$	*чет*	*нечет*
чет	*чет*	*нечет*
нечет	*нечет*	*чет*

$\cdot$	*чет*	*нечет*
чет	*чет*	*чет*
нечет	*чет*	*нечет*

Нулем этого кольца служит *чет*, а единицей — *нечет*.

Согласно теореме 7 из § 3, допустимое разбиение кольца, будучи допустимым разбиением его аддитивной группы, является разбиением на смежные классы по некоторой ее подгруппе. По какой же именно? Назовем подкольцо I кольца R *идеалом*, если произведения xr и rx лежат в I при любых $x \in I$ и $r \in R$. Идеалом кольца целых чисел будет, например, кольцо четных чисел. В кольце действительных функций идеалом является, например, множество всех таких функций f, что $f(0) = 0$. Ответ на поставленный вопрос дает

Т е о р е м а 3. *Разбиение Σ кольца R допустимо тогда и только тогда, когда оно является разбиением его аддитивной группы по некоторому идеалу. Этот идеал оказывается смежным классом разбиения Σ, содержащим 0.*

Д о к а з а т е л ь с т в о. Так как идеал вследствие коммутативности аддитивной группы кольца является ее нормальной подгруппой, то, согласно теореме 6 из § 3, разбиение кольца на смежные классы по идеалу является допустимым разбиением его аддитивной группы. Если как a и c, так и b и d располагаются в одном классе, то $a = c + x$ и $b = d + y$, где x и y — какие-то элементы из идеала. Отсюда

$$ab = (c + x)(d + y) = cd + (cy + xd + xy).$$

Так как элемент $cy + xd + xy$ лежит в идеале, то ab и cd располагаются в одном смежном классе по этому идеалу. Следовательно, разбиение по идеалу оказывается допустимым разбиением и для мультипликативной полугруппы. Пусть теперь Σ — произвольное допустимое разбиение кольца R. Ввиду теоремы 7 из § 3, это разбиение является разбиением по некоторой подгруппе I аддитивной группы кольца R. Если $x \in I$, то x и 0 лежат в одном смежном классе разбиения Σ. Если $r \in R$, то, поскольку r лежит в одном смежном классе с самим собой, а разбиение Σ допустимо, xr и $0r = 0$ попадают в один

смежный класс разбиения Σ. Следовательно, $xr \in I$. Аналогично проверяется, что $rx \in I$. Стало быть, I — идеал.

Теорема 3 показывает, что вместо того, чтобы говорить о факторкольце кольца R по допустимому разбиению, можно говорить о факторкольце кольца R по некоторому идеалу. В силу теоремы 3, этот идеал совпадает со смежным классом разбиения, содержащим 0. С другой стороны, если $\varphi\colon R \to R'$ — гомоморфное наложение колец, то разбиение $\operatorname{Ker}\varphi$ по той же причине определяется идеалом K, состоящим из всех прообразов нуля кольца R', т. е. $K = \{r \mid r \in R,\ \varphi(r) = 0'\}$. Поэтому в теории колец *ядром гомоморфизма* называют этот идеал и через $\operatorname{Ker}\varphi$ обозначают именно его (ср. с. 76). Еще раз подчеркнем, что если I — идеал, то смежный класс, определяемый элементом r, имеет вид $r + I$.

Теорема 4 (теорема о гомоморфизме для колец). *Если* $\varphi\colon R \to R'$ — *гомоморфное наложение колец*, $\operatorname{Ker}\varphi$ — *идеал, являющийся ядром этого гомоморфизма, и* $\pi\colon R \to R/\operatorname{Ker}\varphi$ — *естественный гомоморфизм, то существует изоморфизм* $\chi\colon R' \to R/\operatorname{Ker}\varphi$ *такой, что* $\varphi\chi = \pi$.

Доказательство. Пусть χ — групповой изоморфизм, существующий в силу теоремы 8 из § 3. Если теперь x', $y' \in R'$, то, поскольку φ — наложение, имеем $x' = x\varphi$ и $y' = y\varphi$, где $x, y \in R$. Напомним, что $x\pi$ — это смежный класс по $\operatorname{Ker}\varphi$. Поэтому, принимая во внимание определение отображения χ (см. доказательство теоремы 7 из § 1) и учитывая, что φ и π — гомоморфизмы колец, получаем

$$(x'y')\chi = ((xy)\varphi)\chi = (xy)\pi = x\pi \cdot y\pi = x'\chi \cdot y'\chi.$$

Следовательно, χ — кольцевой гомоморфизм, а значит, и кольцевой изоморфизм.

Легко проверяется, что подгруппы $\boldsymbol{Z}n$ являются идеалами кольца целых чисел. Поэтому факторгруппа $\boldsymbol{Z}/\boldsymbol{Z}n$ оказывается кольцом, которое называется *кольцом вычетов по модулю* n.

Легко проверить, что если $\varphi\colon R \to R'$ — гомоморфное наложение колец и кольцо R коммутативно, то кольцо R' также коммутативно. В частности, факторкольцо коммутативного кольца коммутативно. Поэтому коммутативными оказываются все кольца вычетов.

Ненулевой элемент a некоторого кольца называется *делителем нуля*, если $ab = 0$ или $ba = 0$ для некоторого

ненулевого элемента b. Если R — кольцо с 1, то элемент a называется *обратимым*, если $ab = 1 = ba$ для некоторого $b \in R$.

Теорема 5. *Обратимый элемент кольца не может быть делителем нуля.*

Доказательство. Допустим, что обратимый элемент a кольца R оказался делителем нуля. Тогда для некоторого $b \in R$ имеем $ab = 1 = ba$, а для некоторого ненулевого $c \in R$ — $ac = 0$ или $ca = 0$. Учитывая свойство (а), установленное в начале параграфа, получаем $c = (ba)\,c = b0 = 0$ или $c = c\,(ab) = 0b = 0$. Противоречие.

Коммутативное кольцо P называется *полем*, если оно содержит единицу, отличную от нуля, и каждый ненулевой элемент из P обратим. В силу теоремы 5, в поле нет делителей нуля. Отсюда и из определения поля, в частности, вытекает, что ненулевые элементы поля образуют коммутативную группу относительно умножения. Примерами полей служат кольца рациональных и действительных чисел. В дальнейшем будут приведены и другие примеры.

Заметим еще, что все полученные ранее результаты о матрицах и определителях над полем действительных чисел остаются справедливыми для матриц и определителей над произвольным полем, ибо в соответствующих доказательствах специфика поля действительных чисел никогда не использовалась. Более того, теоремы I.3.7 и I.3.8 остаются справедливыми для матриц с элементами из любого кольца. Как и выше, доказательства остаются прежними.

Теорема 6. *Кольцо вычетов по модулю n является полем тогда и только тогда, когда n — простое число.*

Доказательство. Пусть R — кольцо вычетов по модулю n. Допустим, что R — поле. Если n не является простым, то $n = kl$, где $0 < k$, $l < n$. Тогда классы $[k]$ и $[l]$ отличны от нуля. Но $[k]\,[l] = [n] = [0]$. Следовательно, $[k]$ — делитель нуля, что невозможно, поскольку R — поле. Предположим теперь, что n — простое число. Если $[k] \neq [0]$, то $0 < k < n$. Поскольку n делится лишь на 1 и на n, то н.о.д. $(k, n) = 1$. Следовательно, найдутся такие целые числа u и v, что $uk + vn = 1$ (см. примечание на с. 80). Отсюда

$$[u]\,[k] = [uk] + [0] = [uk] + [vn] = [uk + vn] = [1],$$

т. е. все ненулевые элементы из R обратимы.

Пусть P — поле. Положительное число p называется *характеристикой поля* P, если $\underbrace{1+\ldots+1}_{p \text{ раз}}=0$ и никакое положительное число, меньшее p, этим свойством не обладает. Если указанное свойство не имеет места ни для какого положительного числа, то говорят, что поле имеет *характеристику* 0. Полем характеристики нуль является, например, поле действительных чисел. Характеристику p, где p — простое число, имеет поле вычетов по модулю p. Имеет место

Теорема 7. *Характеристикой поля может быть только* 0 *или простое число.*

Доказательство. Если $n=kl$, где $1<k$, $l<n$, является характеристикой поля P, то $a=\underbrace{1+\ldots+1}_{k \text{ раз}}$ и $b=\underbrace{1+\ldots+1}_{l \text{ раз}}$ отличны от нуля. Однако $ab=$ $=\underbrace{1+\ldots+1}_{n=kl \text{ раз}}=0$, что противоречит отсутствию в поле делителей нуля.

Теорема 8. *Всякое коммутативное кольцо с единицей и без делителей нуля вкладывается в поле.*

Доказательство. Пусть R — коммутативное кольцо с единицей без делителей нуля. Обозначим через Q множество всех символов $\frac{a}{b}$, где $a, b \in R$, причем $b \neq 0$. Положим

$$\left[\frac{a}{b}\right]=\left\{\frac{x}{y} \,\middle|\, \frac{x}{y} \in Q, \quad ay=bx\right\}.$$

Убедимся, что подмножества $\left[\frac{a}{b}\right]$ образуют разбиение множества Q. Поскольку $\frac{a}{b} \in \left[\frac{a}{b}\right]$, для этого достаточно установить, что два таких множества, имеющие общий элемент, совпадают. Чтобы это доказать, допустим, что $\frac{u}{v} \in \left[\frac{a}{b}\right] \cap \left[\frac{c}{d}\right]$. Тогда $av=bu$ и $cv=du$. Если $\frac{x}{y} \in \left[\frac{a}{b}\right]$, то $ay=bx$. Докажем, что $cy=dx$. Действительно,

$$(bv)(cy-dx)=bduy-vdya=avdy-vdya=0.$$

Поскольку в R нет делителей нуля и $b, v \neq 0$, отсюда вытекает, что $cy-dx=0$. Следовательно, $cy=dx$, т. е.

$\frac{x}{y} \in \left[\frac{c}{d}\right]$. Таким образом, $\left[\frac{a}{b}\right] \subseteq \left[\frac{c}{d}\right]$. Обратное включение доказывается аналогично. Обозначим полученное разбиение через Σ и рассмотрим фактормножество Q/Σ. Определим на нем операции $+$ и $\cdot$, полагая

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad + bc}{bd}\right]$$

и

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right].$$

Ввиду отсутствия в R делителей нуля, правые части этих равенств имеют смысл. Убедимся, что определения корректны. Допустим, что $\left[\frac{a}{b}\right] = \left[\frac{u}{v}\right]$ и $\left[\frac{c}{d}\right] = \left[\frac{w}{z}\right]$. Надо убедиться, что

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{u}{v}\right] + \left[\frac{w}{z}\right] \text{ и } \left[\frac{a}{b}\right]\left[\frac{c}{d}\right] = \left[\frac{u}{v}\right]\left[\frac{w}{z}\right].$$

Но, по условию, $av = bu$ и $cz = dw$. Отсюда

$$(bd)(uz + wv) = bduz + bdwv =$$
$$= advz + bczv = (vz)(ad + bc)$$

и

$$(ac)(vz) = budw = (bd)(uw),$$

что и требовалось. После этого легко убедиться, что умножение ассоциативно и коммутативно, а сложение коммутативно. Ассоциативность сложения вытекает из равенств

$$\left(\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right]\right) + \left[\frac{u}{v}\right] = \left[\frac{ad + bc}{ba}\right] + \left[\frac{u}{v}\right] =$$
$$= \left[\frac{adv + bcv + bdu}{bdv}\right]$$

и

$$\left[\frac{a}{b}\right] + \left(\left[\frac{c}{d}\right] + \left[\frac{u}{v}\right]\right) = \left[\frac{a}{b}\right] + \left[\frac{cv + du}{dv}\right] =$$
$$= \left[\frac{adv + bcv + bdu}{bdv}\right].$$

Далее, из равенств

$$\left[\frac{a}{b}\right] + \left[\frac{0}{1}\right] = \left[\frac{a \cdot 1 + b \cdot 0}{b}\right] = \left[\frac{a}{b}\right]$$

и

$$\left[\frac{a}{b}\right] + \left[\frac{-a}{b}\right] = \left[\frac{ab - ab}{b^2}\right] = \left[\frac{0}{b^2}\right] = \left[\frac{0}{1}\right]$$

выводим, что Q/Σ — коммутативная группа относительно сложения. Кроме того, имеем

$$\left(\left[\frac{a}{b}\right]+\left[\frac{c}{d}\right]\right)\left[\frac{u}{v}\right]=\left[\frac{(ad+bc)\,u}{bdv}\right]=\left[\frac{(ad+bc)\,uv}{bdv^2}\right]=$$
$$=\left[\frac{au}{bv}\right]+\left[\frac{cu}{dv}\right]=\left[\frac{a}{b}\right]\left[\frac{u}{v}\right]+\left[\frac{c}{d}\right]\left[\frac{u}{v}\right].$$

Следовательно, Q/Σ — кольцо. Заметим, что второй закон дистрибутивности легко вывести из первого, поскольку умножение коммутативно. Кроме того,

$$\left[\frac{a}{b}\right]\left[\frac{1}{1}\right]=\left[\frac{a}{b}\right],$$

т. е. $\left[\frac{1}{1}\right]$ — единица кольца Q/Σ. Если $\left[\frac{a}{b}\right]\neq\left[\frac{0}{1}\right]$, то $a\neq 0$. Следовательно, $\left[\frac{b}{a}\right]\in Q/\Sigma$. Но $\left[\frac{a}{b}\right]\left[\frac{b}{a}\right]=$ $=\left[\frac{1}{1}\right]$. Значит, Q/Σ — поле. Определим отображение φ: $R\to Q/\Sigma$, положив $a\varphi=\left[\frac{a}{1}\right]$. Поскольку $\left[\frac{a}{1}\right]=\left[\frac{b}{1}\right]$ влечет $a=b$, это отображение является вложением, а из равенств

$$(a+b)\,\varphi=\left[\frac{a+b}{1}\right]=\left[\frac{a}{1}\right]+\left[\frac{b}{1}\right]=a\varphi+b\varphi$$

и

$$(ab)\,\varphi=\left[\frac{ab}{1}\right]=\left[\frac{a}{1}\right]\left[\frac{b}{1}\right]=a\varphi\cdot b\varphi$$

вытекает, что φ — гомоморфизм. Следовательно, φ осуществляет гомоморфное вложение кольца R в поле Q/Σ, что и требовалось.

Построим еще одно поле. Пусть $\boldsymbol{C}$ — множество матриц вида

$$\begin{Vmatrix} a & -b \\ b & a \end{Vmatrix}$$

над полем действительных чисел. Из равенств

$$\begin{Vmatrix} a & -b \\ b & a \end{Vmatrix}+\begin{Vmatrix} c & -d \\ d & c \end{Vmatrix}=\begin{Vmatrix} a+c & -(b+d) \\ b+d & a+c \end{Vmatrix}$$

и

$$\begin{Vmatrix} a & -b \\ b & a \end{Vmatrix}\begin{Vmatrix} c & -d \\ d & c \end{Vmatrix}=\begin{Vmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{Vmatrix}$$

видно, что C — подкольцо кольца матриц второго порядка, ибо

$$\begin{Vmatrix} 0 & 0 \\ 0 & 0 \end{Vmatrix} \in C \quad \text{и} \quad -\begin{Vmatrix} a & -b \\ b & a \end{Vmatrix} = \begin{Vmatrix} -a & b \\ -b & -a \end{Vmatrix} \in C.$$

Хотя само кольцо матриц не коммутативно, подкольцо C оказывается коммутативным, поскольку

$$\begin{Vmatrix} c & -d \\ d & c \end{Vmatrix} \begin{Vmatrix} a & -b \\ b & a \end{Vmatrix} = \begin{Vmatrix} ca - db & -(da + cb) \\ da + cb & ca - db \end{Vmatrix} =$$

$$= \begin{Vmatrix} a & -b \\ b & a \end{Vmatrix} \begin{Vmatrix} c & -d \\ d & c \end{Vmatrix}.$$

Более того, $E \in C$, и если

$$\begin{Vmatrix} a & -b \\ b & a \end{Vmatrix} \neq \begin{Vmatrix} 0 & 0 \\ 0 & 0 \end{Vmatrix},$$

то $a^2 + b^2 \neq 0$ и

$$\begin{Vmatrix} a & -b \\ b & a \end{Vmatrix} \begin{Vmatrix} \frac{a}{a^2+b^2} & \frac{b}{a^2+b^2} \\ -\frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{Vmatrix} = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} = E,$$

т. е. каждый ненулевой элемент из C обратим, причем обратный элемент также лежит в C. Таким образом, C оказывается полем, которое называется *полем комплексных чисел*. Матрицы, входящие в поле C, будем называть *комплексными числами*. Поле действительных чисел вкладывается в поле C с помощью гомоморфного вложения φ, где

$$\varphi(a) = \begin{Vmatrix} a & 0 \\ 0 & a \end{Vmatrix}.$$

Чтобы получить традиционную запись комплексных чисел, условимся отождествлять комплексное число $\begin{Vmatrix} a & 0 \\ 0 & a \end{Vmatrix}$ с действительным числом a и положим

$$i = \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix}.$$

Тогда

$$i^2 = \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix} = -1, \quad bi = \begin{Vmatrix} b & 0 \\ 0 & b \end{Vmatrix} \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & -b \\ b & 0 \end{Vmatrix}$$

и, следовательно,

$$\begin{Vmatrix} a & -b \\ b & a \end{Vmatrix} = a + bi.$$

Если $z = a + bi$ — комплексное число, то комплексное число $\bar{z} = a - bi$ называется *сопряженным с* z.

Непосредственным подсчетом проверяется

Т е о р е м а 9. *Отображение* φ: $\boldsymbol{C} \to \boldsymbol{C}$, *где* $\varphi(z) = \bar{z}$, — *изоморфизм, и* $\bar{z} = z$ *тогда и только тогда, когда* z — *действительное число.*

Если $z = a + bi$ — комплексное число, то $z\bar{z} = a^2 + b^2$ и, следовательно, является неотрицательным действительным числом. Число $|z| = \sqrt{z\bar{z}}$ назовем *нормой комплексного числа* z (не путать с обозначениями определителя матрицы и числа элементов множества) *).

Норма обладает следующими свойствами:

(1) $|u| = 0$ тогда и только тогда, когда $u = 0$;

(2) $|uv| = |u|\,|v|$;

(3) $|u + v| \leqslant |u| + |v|$.

Действительно, пусть $u = a + bi$ и $v = c + di$. Свойство (1) очевидно. Свойство (2) вытекает из соотношений

$$|uv|^2 = (ac - bd)^2 + (ad + bc)^2 =$$
$$= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 =$$
$$= (a^2 + b^2)(c^2 + d^2) = |u|^2\,|v|^2.$$

Для проверки неравенства (3) заметим, что

$$(|u| + |v|)^2 - |u + v|^2 = |u|^2 + |v|^2 + 2|u||v| -$$
$$- (u + v)\overline{(u + v)} = u\bar{u} + v\bar{v} + 2|u|\,|v| - u\bar{u} - v\bar{v} -$$
$$- (u\bar{v} + \bar{u}v) = 2|u|\,|v| - (u\bar{v} + \bar{u}v). \quad (*)$$

Далее,

$$u\bar{v} + \bar{u}v = (a + bi)(c - di) + (a - bi)(c + di) =$$
$$= ac + bd + (bc - ad)i + ac + bd - (bc - ad)i =$$
$$= 2(ac + bd)$$

и, следовательно,

$$(2|u|\,|v|)^2 - (u\bar{v} + \bar{u}v)^2 = 4u\bar{u}v\bar{v} - 4(ac + bd)^2 =$$
$$= 4((a^2 + b^2)(c^2 + d^2) - (ac + bd)^2) =$$
$$= 4(a^2c^2 + b^2c^2 + a^2d^2 + b^2d^2 - a^2c^2 - 2abcd - b^2d^2) =$$
$$= 4(a^2d^2 + b^2c^2 - 2abcd) = 4(ad - bc)^2 \geqslant 0.$$

Поскольку $2|u|\,|v| \geqslant 0$, отсюда вытекает, что

$$2|u|\,|v| \geqslant u\bar{v} + \bar{u}v.$$

---

*) Вместо «норма» часто говорят «модуль» или «абсолютная величина».

Используя (*), получаем

$$(|u|+|v|)^2-|u+v|^2\geqslant 0,$$

что доказывает неравенство (3).

Кольцо с единицей, отличной от нуля, называется *телом*, если каждый его ненулевой элемент обратим. Коммутативные тела — это в точности поля. Для построения примера некоммутативного тела рассмотрим множество $\boldsymbol{K}$ всех матриц вида

$$\begin{Vmatrix} u & v \\ -\bar{v} & \bar{u} \end{Vmatrix}$$

над полем комплексных чисел. Как и выше, легко проверяется, что $\boldsymbol{K}$ — подкольцо кольца матриц. Оно не коммутативно, поскольку, ввиду $\bar{i}=-i$, имеем

$$\begin{Vmatrix} i & 0 \\ 0 & -i \end{Vmatrix}\begin{Vmatrix} 0 & i \\ i & 0 \end{Vmatrix}=\begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix}\neq\begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix}=\begin{Vmatrix} 0 & i \\ i & 0 \end{Vmatrix}\begin{Vmatrix} i & 0 \\ 0 & -i \end{Vmatrix}.$$

Однако $E\in\boldsymbol{K}$, и если $u=a+bi$ и $v=c+di$, то $u\bar{u}+v\bar{v}=a^2+b^2+c^2+d^2$ — неотрицательное действительное число. Поэтому

$$\begin{Vmatrix} u & v \\ -\bar{v} & \bar{u} \end{Vmatrix}\neq\begin{Vmatrix} 0 & 0 \\ 0 & 0 \end{Vmatrix}$$

влечет за собой $u\bar{u}+v\bar{v}\neq 0$. Следовательно, имеем

$$\begin{Vmatrix} u & v \\ -\bar{v} & \bar{u} \end{Vmatrix}\begin{Vmatrix} \dfrac{\bar{u}}{u\bar{u}+v\bar{v}} & -\dfrac{v}{u\bar{u}+v\bar{v}} \\ \dfrac{\bar{v}}{u\bar{u}+v\bar{v}} & \dfrac{u}{u\bar{u}+v\bar{v}} \end{Vmatrix}=\begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}=$$

$$=\begin{Vmatrix} \dfrac{\bar{u}}{u\bar{u}+v\bar{v}} & -\dfrac{v}{u\bar{u}+v\bar{v}} \\ \dfrac{\bar{v}}{u\bar{u}+v\bar{v}} & \dfrac{u}{u\bar{u}+v\bar{v}} \end{Vmatrix}\begin{Vmatrix} u & v \\ -\bar{v} & \bar{u} \end{Vmatrix},$$

т. е. каждая ненулевая матрица из $\boldsymbol{K}$ обладает обратной, принадлежащей $\boldsymbol{K}$. Таким образом, $\boldsymbol{K}$ оказывается телом. Оно называется *телом кватернионов*, а его элементы — *кватернионами*.

Нетрудно проверить, что отображение

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

где a — действительное число, является гомоморфным вложением поля действительных чисел в тело кватернио-

нов. Отождествляя a с $\left\|\begin{matrix} a & 0 \\ 0 & a \end{matrix}\right\|$ и полагая

$$\boldsymbol{i} = \left\|\begin{matrix} i & 0 \\ 0 & -i \end{matrix}\right\|, \quad \boldsymbol{j} = \left\|\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}\right\|, \quad \boldsymbol{k} = \left\|\begin{matrix} 0 & i \\ i & 0 \end{matrix}\right\|,$$

получаем следующую таблицу умножения:

$\cdot$	1	$\boldsymbol{i}$	$\boldsymbol{j}$	$\boldsymbol{k}$
1	1	$\boldsymbol{i}$	$\boldsymbol{j}$	$\boldsymbol{k}$
$\boldsymbol{i}$	$\boldsymbol{i}$	-1	$\boldsymbol{k}$	$-\boldsymbol{j}$
$\boldsymbol{j}$	$\boldsymbol{j}$	$-\boldsymbol{k}$	-1	$\boldsymbol{i}$
$\boldsymbol{k}$	$\boldsymbol{k}$	$\boldsymbol{j}$	$-\boldsymbol{i}$	-1

Если a — действительное число, то $\bar{a} = a$. Поэтому

$$a \left\|\begin{matrix} u & v \\ -\bar{v} & \bar{u} \end{matrix}\right\| = \left\|\begin{matrix} au & av \\ -\overline{av} & \overline{au} \end{matrix}\right\|,$$

и, следовательно, если $u = a + bi$, а $v = c + di$, то

$$\left\|\begin{matrix} u & v \\ -\bar{v} & \bar{u} \end{matrix}\right\| = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}.$$

Кольцо R с единицей, отличной от нуля, называется *простым*, если оно не содержит идеалов, отличных от 0 и R. Легко проверить, что поле (и даже тело) является простым кольцом. Более того, справедлива

Т е о р е м а 10. *Кольцо матриц над телом простое.*

Д о к а з а т е л ь с т в о. Пусть R — кольцо матриц порядка n над телом D. Обозначим через aE_{ij} матрицу, у которой на месте (i, j) стоит элемент a, а на остальных местах — нули. Непосредственным подсчетом проверяется, что

$$aE_{ij} \cdot bE_{kl} = \begin{cases} (ab)E_{il}, & \text{если } j = k, \\ 0, & \text{если } j \neq k, \end{cases} \qquad (*)$$

и что для любой матрицы B имеем

$$B = \sum_{i,\,j} b_{ij}E_{ij}. \qquad (**)$$

Пусть I — ненулевой идеал кольца R. Тогда I содержит ненулевую матрицу A. Разумеется, $a_{pq} \neq 0$ для некоторых p и q. Учитывая (*) и (**), получаем

$$b_{ij}E_{ij} = ((b_{ij}a_{pq}^{-1})E)E_{ip}AE_{qj}.$$

Ввиду (**) отсюда вытекает, что I содержит произвольную матрицу B, а значит, $I = R$.

Элемент z кольца R называется *центральным*, если $za = az$ для всех $a \in R$. Совокупность Z всех центральных элементов кольца называется его *центром*.

Теорема 11. *Центр кольца является подкольцом.*

Доказательство. Ясно, что $0 \in Z$. Пусть $x, y \in Z$, т. е. для любого $a \in R$ имеем $xa = ax$ и $ya = ay$. Тогда

$$(x + y)a = xa + ya = ax + ay = a(x + y),$$
$$(-x)a = -xa = -ax = a(-x)$$

и

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy).$$

Следовательно, $x + y \in Z$, $-x \in Z$ и $xy \in Z$, значит, Z — подкольцо.

Теорема 12. *Центр Z кольца матриц над полем P совпадает с множеством матриц вида λE, где $\lambda \in P$.*

Доказательство. Для любой матрицы A в силу формул, приведенных в конце § 3 гл. I, имеем

$$(\lambda E)A = E(\lambda A) = (\lambda A) = (\lambda A)E = A(\lambda E),$$

т. е. $\lambda E \in Z$. Допустим теперь, что $A \in Z$. Используя обозначения и формулы, рассмотренные при доказательстве теоремы 10, имеем

$$\begin{Vmatrix} 0 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1} & \dots & a_{ii} & \dots & a_{in} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \dots & 0 \end{Vmatrix} = a_{i1}E_{i\hat{1}} + \dots + a_{in}E_{in} = E_{ii}A =$$

$$= AE_{ii} = a_{\hat{1}i}E_{1i} + \dots + a_{ni}E_{ni} = \begin{Vmatrix} 0 & \dots & a_{1i} & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & a_{ii} & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & a_{ni} & 0 \end{Vmatrix}.$$

Отсюда $a_{1i} = \dots = a_{i-1i} = a_{i+\hat{1}i} = \dots = a_{ni} = 0$ для всех i, т. е. матрица A диагональная. Поскольку при этом условии

$$a_{jj}E_{ij} = \sum_l a_{jl}E_{il} = E_{ij}(\sum_{k,l} a_{kl}E_{kl}) = E_{ij}A =$$

$$= AE_{ij} = (\sum_{k,l} a_{kl}E_{kl})E_{ij} = \sum_k a_{ki}E_{kj} = a_{ii}E_{ij}$$

для любых i и j, то $a_{11} = \dots = a_{nn} = \lambda$, т. е. $A = \lambda E$.

Упражнения

1. Пусть R и R' — кольца. На множестве $R \times R'$ (см. упражнение 7 из § 2) определим операции

$$(r, r') + (s, s') = (r + s, r' + s')$$

и

$$(r, r')(s, s') = (rs, r's').$$

Доказать, что $R \times R'$ становится кольцом, кольца R и R' изоморфны некоторым идеалам этого кольца, а факторкольцо $(R \times R')/I$, где $I = \{(r, 0) \mid r \in R\}$, изоморфно кольцу R'.

2. Доказать, что пересечение любого множества идеалов некоторого кольца также является идеалом этого кольца.

3. Доказать, что делителями нуля в кольце матриц над полем являются матрицы с нулевым определителем и только они. Вывести отсюда, что в кольце матриц всякий неделитель нуля обратим.

4. Доказать, что в кольце функций всякий неделитель нуля обратим.

5. Найти все делители нуля кольца $R \times R'$ из упражнения 1 для случая, когда R и R' — поля.

6. Если идеал I кольца R содержит обратимый элемент (в частности, если $1 \in I$), то $I = R$.

7. Пусть R, I и H — множества всех матриц вида

$$\begin{Vmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{Vmatrix}, \quad \begin{Vmatrix} 0 & g & h \\ 0 & 0 & 2k \\ 0 & 0 & 0 \end{Vmatrix} \quad \text{и} \quad \begin{Vmatrix} 0 & l & 2m \\ 0 & 0 & 2n \\ 0 & 0 & 0 \end{Vmatrix}$$

соответственно, где a, b, c, d, e, f, g, h, k, l, m, n — целые числа. Доказать, что R — кольцо, I — идеал кольца R, H — идеал кольца I, но H не является идеалом кольца R, являясь, однако, его левым идеалом (см. с. 107).

8. Доказать, что коммутативное кольцо с единицей, отличной от нуля, не имеющее идеалов, отличных от нуля и всего кольца, является полем. Показать, что нельзя отказаться от требования существования единицы.

9. Кольцо R называется *ниль-кольцом*, если для всякого элемента x из R найдется такое натуральное число n, что $x^n = 0$. Пусть R — некоторое кольцо, I — его идеал такой, что кольцо I и факторкольцо R/I являются ниль-кольцами. Доказать, что R — также ниль-кольцо.

10. Какие теоремы из гл. I остаются справедливыми для матриц с элементами из произвольного коммутативного кольца и, в частности, из кольца целых чисел?

11. Доказать, что, полагая $\varphi(z) = \begin{Vmatrix} z & 0 \\ 0 & \overline{z} \end{Vmatrix}$, мы получаем гомоморфное вложение поля комплексных чисел в тело кватернионов.

12. Доказать, что матрицы вида $\begin{Vmatrix} a & b \\ 2b & a \end{Vmatrix}$, где a и b — рациональные числа, образуют поле, изоморфное полю, образованному действительными числами вида $a + b\sqrt{2}$, где a и b — рациональные числа.

13. Тело кватернионов изоморфно кольцу, состоящему из всех матриц вида

$$\begin{Vmatrix} a & -b & c & d \\ b & a & -d & c \\ -c & d & a & b \\ -d & -c & -b & a \end{Vmatrix}$$

над полем действительных чисел.

14. Доказать, что центр кольца матриц над телом D совпадает с множеством всех матриц вида λE, где λ принадлежит центру тела D.

15. Если I — идеал кольца матриц над кольцом R, то найдется такой идеал U кольца R, что I совпадает с множеством всех матриц, элементы которых принадлежат U.

§ 5. Модули

Правым модулем над кольцом R с единицей или *правым R-модулем* называется коммутативная группа M, для которой определены произведения $ar \in M$ для любых $a \in M$ и $r \in R$, причем

(1) $(a + b)r = ar + br$,
(2) $a(r + s) = ar + as$,
(3) $a(rs) = (ar)s$,
(4) $a1 = a$

для любых a, $b \in M$ и r, $s \in R$. Подчеркнем, что символ $+$ в левой и правой частях равенства (2) имеет различный смысл: слева он означает сложение элементов кольца R, а справа — сложение элементов группы M. Различный смысл имеет также подразумеваемый в формуле (3) символ умножения: rs означает произведение элементов кольца R, а ar, $(ar)s$ и $a(rs)$ — произведение элемента из группы M на элемент кольца R. Примеры правых модулей приведены в таблице 4. Элементы модуля для краткости условимся называть *векторами* (ср. § 1 гл. III). Аналогично определяются *левые модули*, где произведение записывается как ra. Если кольцо R коммутативно, то разницы между правыми и левыми модулями нет. Действительно, пусть M — правый модуль над коммутативным кольцом R. Если $r \in R$ и $a \in M$, то положим $r \circ a = ar$. Тогда

$$r\circ(a + b) = (a + b)r = ar + br = r\circ a + r\circ b,$$
$$(r + s)\circ a = a(r + s) = ar + as = r\circ a + s\circ a,$$
$$(rs)\circ a = a(rs) = a(sr) = (as)r = r\circ(s\circ a)$$

Таблица 4

	Кольцо	Группа	Произведение ar
1	Произвольное кольцо R с единицей	Аддитивная группа кольца R	Произведение в кольце R
2	Произвольное кольцо R с единицей	Группа n-мерных строк $(a_1, \ldots, a_n)$, где $a_i \in R$	$(a_1, \ldots, a_n)\, r = (a_1 r, \ldots, a_n r)$
3	Целые числа	Произвольная коммутативная группа	$ar = \begin{cases} \underbrace{a + \ldots + a}_{r \text{ раз}}, & \text{если } r > 0, \\ 0, & \text{если } r = 0, \\ \underbrace{(-a) + \ldots + (-a)}_{\lvert r\rvert \text{ раз}}, & \text{если } r < 0. \end{cases}$ Свойства (1) и (4) очевидны, а (2) и (3) — это теоремы 9 и 10 из § 3 в аддитивной форме (см. примечание на с. 77)
4	Действительные числа	Аддитивная группа поля комплексных чисел	$\begin{Vmatrix} a & -b \\ b & a \end{Vmatrix} r = \begin{Vmatrix} ar & -br \\ br & ar \end{Vmatrix}$
5	Действительные числа	Аддитивная группа тела кватернионов	$\begin{Vmatrix} u & v \\ -\bar{v} & \bar{u} \end{Vmatrix} r = \begin{Vmatrix} ur & vr \\ -\overline{vr} & \overline{ur} \end{Vmatrix}$ (учесть, что $\bar{r} = r$)
6	Матрицы порядка n над произвольным кольцом	Матрицы порядка n, у которых все строки, начиная со второй, нулевые	Произведение в кольце матриц
7	Произвольное кольцо R с единицей	Аддитивная группа любого идеала кольца R	Произведение в кольце R
8	Подкольцо R произвольного кольца S, имеющее единицу (возможно, отличную от единицы кольца S)	Аддитивная группа кольца S	Произведение в кольце S

и

$$1 \circ a = a1 = a$$

для любых $a, b \in M$ и $r, s \in R$, т. е. M оказывается левым R-модулем. Подчеркнем, что коммутативность кольца R использована лишь при доказательстве третьего равенства (ср. замечание на с. 112—113).

Рассуждениями, аналогичными проводившимся на с. 91 для колец, устанавливается справедливость следующих свойств:

(а) $a0 = 0r = 0$,

(б) $(-a)r = a(-r) = -ar$,

(в) $(a - b)r = ar - br$, $a(r - s) = ar - as$,

где $a, b \in M$, $r, s \in R$.

Заметим, что символ 0 в формуле (а) обозначает как нуль кольца R, так и нуль группы M. Точно так же в различных смыслах в формулах (б) и (в) используется символ $-$.

Подмножество N правого модуля M над кольцом R называется *подмодулем*, если $a, b \in N$ влечет $a + b \in N$ и $ar \in N$ для всех $r \in R$.

Подгруппа H аддитивной группы кольца R называется *правым идеалом*, если $ar \in H$ для любых $a \in H$ и $r \in R$. Другими словами, правый идеал — это подмодуль правого R-модуля R. *Левый идеал* определяется аналогично. Правый идеал кольца матриц образуют, например, матрицы, у которых все строки, кроме первой, нулевые (см. пример 6 в таблице 4). Идеал — это правый идеал, одновременно являющийся и левым. Поэтому его часто называют *двусторонним идеалом*.

Аналогично теоремам 3 из § 2, 1 из § 3 и 1 из § 4 доказывается

Теорема 1. *Пересечение любого множества подмодулей является подмодулем.*

Если M — правый R-модуль, то выражение вида

$$a_1r_1 + \ldots + a_mr_m,$$

где $a_i \in M$ и $r_i \in R$, будем называть *линейной комбинацией* векторов $a_1, \ldots, a_m$. Если все $r_i = 0$, то линейная комбинация называется *тривиальной*. Если вектор равен линейной комбинации векторов $a_1, \ldots, a_m$, то говорят, что он *выражается через систему* $\mathfrak{A} = \{a_1, \ldots, a_m\}$. Например, в модуле 3-мерных строк (пример 2 из таблицы 4) каждый вектор выражается через систему $\{(1, 0, 0),$

$(0, 1, 0), (0, 0, 1)\}$, а в модуле примера 4 из той же таблицы 4 — через систему $\left\{\begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}, \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix}\right\}$. Если система $\mathfrak{A}$ бесконечна, то выражаемость элемента через систему $\mathfrak{A}$ определяется как его выражаемость через некоторую конечную подсистему системы $\mathfrak{A}$. Если каждый вектор системы $\mathfrak{A}$ выражается через систему $\mathfrak{A}'$, то скажем, что *система* $\mathfrak{A}$ *выражается через систему* $\mathfrak{A}'$.

Т е о р е м а 2 (о транзитивности линейной выражаемости). *Если система* $\mathfrak{A}$ *выражается через систему* $\mathfrak{A}'$, *а система* $\mathfrak{A}'$ *— через систему* $\mathfrak{A}''$, *то система* $\mathfrak{A}$ *выражается через систему* $\mathfrak{A}''$.

Д о к а з а т е л ь с т в о. Если $a \in \mathfrak{A}$, то $a = \sum_i a_i' r_i$, где $a_i' \in \mathfrak{A}'$, $r_i \in R$, ибо $\mathfrak{A}$ выражается через $\mathfrak{A}'$. Но $a_i' = \sum_j a_j'' r_{ij}$, где $a_j'' \in \mathfrak{A}''$, $r_{ij} \in R$, поскольку $\mathfrak{A}'$ выражается через $\mathfrak{A}''$. Отсюда

$$a = \sum_i \left(\sum_j a_j'' r_{ij}\right) r_i = \sum_j a_j'' \left(\sum_i r_{ij} r_i\right),$$

т. е. a выражается через $\mathfrak{A}''$.

Если $\mathfrak{A}$ — некоторая система векторов, то обозначим через $\mathfrak{L}(\mathfrak{A})$ и назовем *линейной оболочкой* системы $\mathfrak{A}$ множество всех векторов, выражающихся через систему $\mathfrak{A}$. Линейную оболочку системы, состоящей из одного вектора a, будем обозначать также через aR.

Т е о р е м а 3. *Линейная оболочка любой системы векторов* $\mathfrak{A}$ *является подмодулем.*

Д о к а з а т е л ь с т в о. Если $a, b \in \mathfrak{L}(\mathfrak{A})$, то $a = \sum_i a_i r_i$, $b = \sum_i a_i s_i$, где $a_i \in \mathfrak{A}$, $r_i, s_i \in R$. Отсюда

$$a + b = \sum a_i (r_i + s_i)$$

и

$$ar = \sum a_i (r_i r)$$

для любого $r \in R$, что и требовалось.

Т е о р е м а 4. *Линейная оболочка системы векторов* $\mathfrak{A}$ *совпадает с пересечением всех подмодулей, содержащих* $\mathfrak{A}$.

Д о к а з а т е л ь с т в о. Пусть U — пересечение, указанное в формулировке. Поскольку $\mathfrak{A} \subseteq U$, то $\mathfrak{L}(\mathfrak{A}) \subseteq U$ по определению подмодуля. С другой стороны, ввиду теоремы 3, $\mathfrak{L}(\mathfrak{A})$ — один из подмодулей, содержащих $\mathfrak{A}$, и, следовательно, $U \subseteq \mathfrak{L}(\mathfrak{A})$.

Отображение φ правого модуля M над кольцом R в правый модуль M' над тем же кольцом называется *гомоморфизмом*, если

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

и

$$\varphi(ar) = \varphi(a)r$$

для любых $a, b \in M$ и $r \in R$. Взаимно однозначный гомоморфизм называется *изоморфизмом*. Если существует изоморфизм модуля M на модуль M', то эти модули называются *изоморфными**).

В качестве примеров гомоморфизма модулей укажем отображения:

а) множества матриц порядка n над произвольным полем в множество n-мерных строк, где

$$\varphi(A) = (a_{11}, \ldots, a_{1n});$$

б) множества матриц порядка 2 в множество четырехмерных строк, где

$$\psi\left(\begin{Vmatrix} a & b \\ c & d \end{Vmatrix}\right) = (a, b, c, d);$$

в) множества n-мерных строк над полем P в себя, определяемое равенством

$$\chi(x_1, \ldots, x_n) = (x_1, \ldots, x_n)A,$$

где A — некоторая фиксированная матрица порядка n над полем P.

Изоморфизмом оказывается гомоморфизм ψ. Гомоморфизм χ является изоморфизмом тогда и только тогда, когда матрица A невырождена (см. упражнение 4 из § 1).

Аналогично теоремам 6 из § 2, 5 из § 3 и 2 из § 4 доказывается

Теорема 5. *Если* φ *— гомоморфизм правого* R*-модуля* M *в правый* R*-модуль* M', *то* $\operatorname{Im}\varphi$ *— подмодуль модуля* M'.

Разбиение Σ правого модуля M над кольцом R называется *допустимым*, если оно является допустимым разбиением группы M и из того, что векторы a и b из M принадлежат одному смежному классу разбиения Σ, вытекает, что для любого $r \in R$ векторы ar и br также лежат в одном смежном классе. Если Σ — допустимое разбиение модуля M, то на фактормножестве M/Σ определим операции

$$[a] + [b] = [a + b]$$

и $[a]r = [ar]$ $(a, b \in M, r \in R)$.

*) См. примечание на с. 60.

Допустимость разбиения позволяет доказать корректность этих определений (см. с. 62). После этого нетрудно проверить, что факторможество оказывается коммутативной группой относительно сложения и что справедливы свойства (1)—(4) из определения модуля. Таким образом, факторможество M/Σ становится правым R-модулем, который называется *фактормодулем* модуля M по разбиению Σ. Отображение, ставящее в соответствие каждому вектору из M содержащий его смежный класс разбиения Σ, оказывается модульным гомоморфизмом. Этот гомоморфизм называется *естественным*.

Теорема 6. *Разбиение Σ правого модуля M над кольцом R допустимо тогда и только тогда, когда оно является разбиением группы M по некоторому подмодулю. Этот подмодуль оказывается смежным классом разбиения Σ, содержащим 0.*

Доказательство. Допустим, что Σ — разбиение модуля M на смежные классы по некоторому подмодулю N. Согласно теореме 6 из § 3, Σ — допустимое разбиение группы M. Если a и b располагаются в одном классе разбиения Σ, то $a = b + x$ для некоторого $x \in N$. Поэтому для произвольного $r \in R$ имеем

$$ar = (b + x)r = br + xr.$$

Поскольку $xr \in N$, то ar и br располагаются в одном смежном классе разбиения Σ, что доказывает его допустимость. Пусть теперь Σ — произвольное допустимое разбиение модуля M. Ввиду теоремы 7 из § 3, это разбиение является разбиением по некоторой подгруппе N коммутативной группы M. Если $a \in N$, то из включений a, $0 \in N$ и допустимости разбиения Σ вытекает, что ar и $0r = 0$, где r — произвольный элемент из R, располагаются в одном смежном классе. Следовательно, $ar \in N$, т. е. N — подмодуль модуля M.

Теорема 6 показывает, что вместо того, чтобы говорить о фактормодуле модуля M по допустимому разбиению, можно говорить о фактормодуле модуля M по некоторому подмодулю. В силу теоремы 6, этот подмодуль совпадает со смежным классом разбиения, содержащим 0. С другой стороны, если $\varphi\colon M \to M'$ — гомоморфизм правых R-модулей, то разбиение Ker φ по той же причине определяется подмодулем K, состоящим из всех прообразов нуля модуля M', т. е. $K = \{a \mid a \in M,\ \varphi(a) = 0'\}$. Поэтому в теории модулей *ядром гомоморфизма* φ назы-

вают этот подмодуль и через $\operatorname{Ker}\varphi$ обозначают именно его (ср. с. 76, 94).

Теорема 7 (теорема о гомоморфизме для модулей). *Если* $\varphi\colon M \to M'$ — *гомоморфное наложение правых модулей над кольцом* R, $\operatorname{Ker}\varphi$ — *подмодуль модуля* M, *являющийся ядром этого гомоморфизма, и* $\pi\colon M \to M/\operatorname{Ker}\varphi$ — *естественный гомоморфизм, то существует изоморфизм* $\chi\colon M' \to M/\operatorname{Ker}\varphi$ *такой, что* $\varphi\chi = \pi$.

Доказательство. Пусть χ — групповой изоморфизм из M' на $M/\operatorname{Ker}\varphi$, существующий в силу теоремы 8 из § 3. Если теперь $x' \in M'$, то, поскольку φ — наложение, имеем $x' = x\varphi$ для некоторого $x \in M$. Напомним, что $x\pi$ — это смежный класс по $\operatorname{Ker}\varphi$. Поэтому, принимая во внимание определение отображения χ (см. доказательство теоремы 7 из § 1), для произвольного $x' \in M'$ получаем

$$(x'r)\chi = ((x\varphi)r)\chi = (xr)\varphi\chi = (xr)\pi = (x\pi)r = (x'\chi)r.$$

Следовательно, χ — модульный гомоморфизм, а значит, и модульный изоморфизм.

Теорема 8. *Множество* $\operatorname{Hom}(M, M')$ *всех гомоморфизмов правого* R*-модуля* M *в правый* R*-модуль* M' *становится коммутативной группой, если для* $\varphi, \psi \in \operatorname{Hom}(M, M')$ *положить*

$$x(\varphi + \psi) = x\varphi + x\psi$$

для всех $x \in M$.

Доказательство. Равенства

$$(x + y)(\varphi + \psi) = (x + y)\varphi + (x + y)\psi =$$
$$= x\varphi + y\varphi + x\psi + y\psi = x\varphi + x\psi + y\varphi + y\psi =$$
$$= x(\varphi + \psi) + y(\varphi + \psi)$$

и

$$(xr)(\varphi + \psi) = (xr)\varphi + (xr)\psi = (x\varphi)r + (x\psi)r =$$
$$= (x\varphi + x\psi)r = (x(\varphi + \psi))r,$$

где x, $y \in M$ и $r \in R$, показывают, что $\varphi + \psi \in \operatorname{Hom}(M, M')$. Отображение 0, переводящее все векторы из L в 0, очевидно, лежит в $\operatorname{Hom}(M, M')$, и

$$\varphi + 0 = 0 + \varphi = \varphi$$

для всех $\varphi \in \operatorname{Hom}(M, M')$. Положив $x(-\varphi) = -x\varphi$ для всех $x \in M$, как и выше, убеждаемся, что $(-\varphi) \in \operatorname{Hom}(M, M')$. При этом $\varphi + (-\varphi) = 0$, поскольку

$$x(\varphi + (-\varphi)) = x\varphi + (-x\varphi) = 0$$

для всех $x \in M$. Из равенств

$$x((\varphi + \psi) + \chi) = x(\varphi + \psi) + x\chi = x\varphi + x\psi + x\chi = \\ = x\varphi + x(\varphi + \chi) = x(\varphi + (\psi + \chi))$$

и

$$x(\varphi + \psi) = x\varphi + x\psi = x\psi + x\varphi = x(\psi + \varphi),$$

справедливых для всех $x \in M$ и любых φ, ψ, $\chi \in \in \mathrm{Hom}(M, M')$, вытекает, что $\mathrm{Hom}(M, M')$ является коммутативной группой.

Теорема 9. *Если M — правый R-модуль, то* $\mathrm{Hom}(M, M)$ — *кольцо с единицей, где сложение определено в теореме* 8, *а умножение — в начале* § 1 *).

Доказательство. Ввиду теоремы 8, $\mathrm{Hom}(M, M)$ — коммутативная группа. Если $\varphi, \psi \in \in \mathrm{Hom}(M, M)$, то для любых $a, b \in M$ и $r \in R$ имеем

$$(a + b)(\varphi\psi) = ((a + b)\varphi)\psi = (a\varphi + b\varphi)\psi = \\ = (a\varphi)\psi + (b\varphi)\psi = a(\varphi\psi) + b(\varphi\psi)$$

и

$$(ar)(\varphi\psi) = ((ar)\varphi)\psi = ((a\varphi)r)\psi = ((a\varphi)\psi)r = (a(\varphi\psi))r.$$

Следовательно, $\varphi\psi \in \mathrm{Hom}(M, M)$, т. е. $\mathrm{Hom}(M, M)$ является полугруппой по умножению (см. теорему 1 из § 1). Поскольку для любых $x \in M$ и φ, ψ, $\chi \in \in \mathrm{Hom}(M, M)$ имеет место

$$x((\varphi + \psi)\chi) = (x(\varphi + \psi))\chi = (x\varphi + x\psi)\chi = \\ = (x\varphi)\chi + (x\psi)\chi = x(\varphi\chi) + x(\psi\chi) = x(\varphi\chi + \psi\chi)$$

и

$$x(\varphi(\psi + \chi)) = (x\varphi)(\psi + \chi) = (x\varphi)\psi + (x\varphi)\chi = \\ = x(\varphi\psi) + x(\varphi\chi) = x(\varphi\psi + \varphi\chi),$$

$\mathrm{Hom}(M, M)$ оказывается кольцом. Единицей этого кольца является тождественное отображение 1_M.

Пусть M — правый R-модуль. Его аддитивную группу можно рассматривать как модуль над кольцом целых чисел (см. пример 3 из таблицы 4), и теорема 9 позволяет говорить о кольце эндоморфизмов этой группы, которое, в отличие от $\mathrm{Hom}(M, M)$, будем обозначать через $\mathrm{Hom}_{\mathbf{Z}}(M, M)$. Рассмотрим отображение $\Phi\colon R \to \mathrm{Hom}_{\mathbf{Z}}(M, M)$, где $x\Phi(r) = xr$ для любых $x \in M$ и $r \in R$. Равенство

$$(x + y)\Phi(r) = (x + y)r = xr + yr = x\Phi(r) + y\Phi(r)$$

*) Гомоморфизмы модуля M в себя обычно называются *эндоморфизмами*. Поэтому кольцо $\mathrm{Hom}(M, M)$ называется *кольцом эндоморфизмов* модуля M. Аналогичная терминология используется для групп, полугрупп, колец и др.

показывает, что $\Phi(r)$ действительно лежит в $\mathrm{Hom}_{\boldsymbol{Z}}(M, M)$. Из равенств

$$x\Phi(r+s) = x(r+s) = xr + xs = x\Phi(r) + x\Phi(s) = x(\Phi(r) + \Phi(s))$$

и

$$x\Phi(rs) = x(rs) = (xr)s = (x\Phi(r))\Phi(s) = x(\Phi(r)\Phi(s)),$$

где $x \in M$, $r, s \in R$, вытекает, что Φ — гомоморфизм колец. Заметим, что если G — произвольная коммутативная группа и Φ — гомоморфизм кольца R в кольцо $\mathrm{Hom}_{\boldsymbol{Z}}(G, G)$, то, полагая $xr = x\Phi(r)$ для любых $x \in G$ и $r \in R$, мы, как легко проверить, превращаем G в правый R-модуль. Тем самым установлена тесная связь между правыми R-модулями и гомоморфизмами кольца R в кольца эндоморфизмов коммутативных групп. Если M — левый R-модуль, то можно определить гомоморфизм Ψ аддитивной группы кольца R в аддитивную группу кольца $\mathrm{Hom}_{\boldsymbol{Z}}(M, M)$, положив $x\Psi(r) = rx$ для любых $x \in M$ и $r \in R$. Но тогда

$$x\Psi(rs) = (rs)x = r(sx) = (x\Psi(s))\Psi(r) = x(\Psi(s)\Psi(r)),$$

откуда

$$\Psi(rs) = \Psi(s)\Psi(r).$$

Следовательно, если кольцо R не коммутативно, то отображение Ψ не является гомоморфизмом колец. Однако можно проверить, что это отображение Ψ станет кольцевым гомоморфизмом, если использовать другое определение произведения отображений (см. примечание на с. 48). Действительно,

$$\Psi(rs)(x) = (rs)x = r(sx) = \Psi(r)(\Psi(s)(x)) = (\Psi(r)\Psi(s))(x)$$

для любых $x \in M$ и $r, s \in R$. Разумеется, если кольцо R коммутативно, то отображение Ψ оказывается гомоморфимом колец, и никаких затруднений не возникает. Тем самым еще раз показано, что для коммутативного кольца разницы между правыми и левыми модулями нет.

Т е о р е м а 10. *Правый R-модуль M является правым модулем над кольцом* $\mathrm{Hom}(M, M)$, *если произведение* $a\varphi$, *где* $a \in M$, $\varphi \in \mathrm{Hom}(M, M)$, *определить как образ элемента a при отображении* φ.

Д о к а з а т е л ь с т в о. Поскольку M — коммутативная группа по сложению, справедливость теоремы вытекает из равенств

$$(a+b)\varphi = a\varphi + b\varphi,$$
$$a(\varphi + \psi) = a\varphi + a\psi$$
$$a(\varphi\psi) = (a\varphi)\psi$$

и

$$a1_M = a,$$

где a и b — произвольные элементы из M, а φ и ψ — произвольные отображения из $\mathrm{Hom}(M, M)$. Сами же эти равенства непосредственно следуют из определений.

Суммой подмодулей назовем линейную оболочку их теоретико-множественного объединения. Сумму подмодулей $S_1, \ldots, S_m$ будем обозначать через $S_1 + \ldots + S_m$.

Теорема 11. *Подмодуль* $S_1 + \ldots + S_m$ *совпадает с множеством векторов, представимых в виде* $s_1 + \ldots + s_m$, *где* $s_i \in S_i$.

Доказательство. Пусть $S = S_1 + \ldots + S_m$ и S' — множество, упоминаемое в формулировке. Ясно, что S' — подмодуль и что

$$S' \subseteq \mathcal{L}(S_1 \cup \ldots \cup S_m) = S.$$

С другой стороны, поскольку $S_1 \cup \ldots \cup S_m \subseteq S'$, то согласно теореме 4 имеем $S \subseteq S'$.

Сумма $S_1 + \ldots + S_m$ называется *прямой суммой*, если каждое слагаемое имеет нулевое пересечение с суммой остальных, т. е.

$$(S_1 + \ldots + S_{i-1} + S_{i+1} + \ldots + S_m) \cap S_i = 0$$

для каждого i. Прямую сумму подмодулей $S_1, \ldots, S_m$ условимся обозначать через

$$S_1 \oplus \ldots \oplus S_m.$$

Ввиду теоремы 11 сумма и, в частности, прямая сумма не зависят от порядка слагаемых.

Теорема 12. *Пусть* $S = S_1 + \ldots + S_m$. *Тогда эквивалентны следующие свойства*:

(1) $S = S_1 \oplus \ldots \oplus S_m$;

(2) $(S_1 + \ldots + S_i) \cap S_{i+1} = 0$ *при* $i = 1, 2, \ldots, n-1$;

(3) *каждый вектор* s *из* S *единственным способом представляется в форме*

$$s = s_1 + \ldots + s_m,$$

где $s_i \in S_i$;

(4) *если* $s_i \in S_i$ *и*

$$s_1 + \ldots + s_m = 0,$$

то $s_i = 0$ *для всех* i.

Доказательство. (1) $\Rightarrow$ (2) тривиально.

(2) $\Rightarrow$ (3). Допустим, что

$$s_1 + \ldots + s_m = s'_1 + \ldots + s'_m,$$

где $s_i, s'_i \in S_i$. Если $s_i \neq s'_i$ для некоторого i, то среди таких номеров i выберем наибольший. Тогда $s_j = s'_j$

при $j > i$ и

$$s_i' - s_i = (s_1 - s_1') + \ldots + (s_{i-1} - s_{i-1}') \in$$
$$\in S_i \cap (S_1 + \ldots + S_{i-1}).$$

Ввиду (2), $s_i' - s_i = 0$, т. е. $s_i = s_i'$ вопреки допущению.

(3) $\Rightarrow$ (4). Достаточно заметить, что $0 = 0 + \ldots + 0$, где $0 \in S_i$.

(4) $\Rightarrow$ (1). Предположим, что

$$0 \neq x \in S_i \cap (S_1 + \ldots + S_{i-1} + S_{i+1} + \ldots + S_m),$$

т. е.

$$x = s_1 + \ldots + s_{i-1} + s_{i+1} + \ldots + s_m,$$

где $s_k \in S_k$. Отсюда

$$s_1 + \ldots + s_{i-1} + (-x) + s_{i+1} + \ldots + s_m = 0$$

и, следовательно, $x = 0$ ввиду (4). Противоречие.

Следствие. *Сумма $S + T$ двух подмодулей является прямой тогда и только тогда, когда $S \cap T = 0$.*

Теорема 13 (о транзитивности разложения в прямую сумму). *Пусть $S = S_1 \oplus \ldots \oplus S_m$ — прямая сумма. Тогда*

$$S = (S_1 \oplus \ldots \oplus S_{i-1}) \oplus (S_i \oplus \ldots \oplus S_m)$$

для каждого i, и если

$$S = S_1 \oplus \ldots \oplus S_m$$

и

$$S_i = S_{i1} \oplus \ldots \oplus S_{ik_i}$$

для каждого i, то

$$S = S_{11} \oplus \ldots \oplus S_{1k_1} \oplus S_{21} \oplus \ldots \oplus S_{2k_2} \oplus \ldots \oplus S_{m1} \oplus \ldots$$
$$\ldots \oplus S_{mk_m}.$$

Доказательство. Допустим, что

$$x \in (S_1 + \ldots + S_{i-1}) \cap (S_i + \ldots + S_m).$$

Тогда для подходящих $s_k \in S_k$ имеем

$$x = s_1 + \ldots + s_{i-1} = s_i + \ldots + s_m = s_1 + \ldots$$
$$\ldots + s_{i-1} + \underbrace{0 + \ldots + 0}_{m-i+1 \text{ раз}} = \underbrace{0 + \ldots + 0}_{i-1 \text{ раз}} + s_i + \ldots + s_m.$$

В силу свойства (3) теоремы 12 отсюда вытекает, что $s_k = 0$ для всех k. Следовательно, $x = 0$, и первое утверждение

доказываемой теоремы вытекает из следствия теоремы 12. Для доказательства второго утверждения заметим, что если $s \in S$, то $s = s_1 + \ldots + s_m$, где $s_i \in S_i$. Далее, $s_i = s_{i1} + \ldots + s_{ik_i}$, где $s_{ij} \in S_{ij}$. Отсюда

$$s = s_{11} + \ldots + s_{1k_1} + s_{21} + \ldots + s_{2k_2} + \ldots \\ \ldots + s_{m1} + \ldots + s_{mk_m},$$

т. е.

$$S = S_{11} + \ldots + S_{1k_1} + S_{21} + \ldots + S_{2k_2} + \ldots \\ \ldots + S_{m1} + \ldots + S_{mk_m}. \quad (*)$$

Если

$$s_{11} + \ldots + s_{1k_1} + s_{21} + \ldots + s_{2k_2} + \ldots \\ \ldots + s_{m1} + \ldots + s_{mk_m} = 0,$$

где $s_{ij} \in S_{ij}$, то, поскольку сумма $S_1 + \ldots + S_m$ прямая, по свойству (4) теоремы 12 имеем

$$s_{i1} + \ldots + s_{ik_i} = 0$$

для каждого i. Поскольку сумма $S_{i1} + \ldots + S_{ik_i}$ прямая, отсюда следует, что $s_{ij} = 0$ для каждого j. Таким образом, $s_{ij} = 0$ для любых i и j, и сумма $(*)$ оказывается прямой по свойству (4) теоремы 12.

Если N — подмодуль модуля M и φ: $M \to M'$ — гомоморфизм модулей, то положим

$$\varphi(N) = \{\varphi(x) \mid x \in N\}.$$

Легко проверить, что $\varphi(N)$ — подмодуль модуля M'. Если $N = M$, то, как легко видеть, $\varphi(N) = \operatorname{Im} \varphi$.

Теорема 14. *Если* φ: $M \to M'$ — *изоморфизм модулей и* $S_1 \oplus \ldots \oplus S_m$ — *прямая сумма подмодулей модуля* M, *то сумма* $\varphi(S_1) + \ldots + \varphi(S_m)$ *также прямая.*

Доказательство. Пусть $s'_1 + \ldots + s'_m = 0$, где $s'_i \in \varphi(S_i)$. Тогда $s'_i = \varphi(s_i)$, где $s_i \in S_i$, и

$$\varphi(s_1 + \ldots + s_m) = s'_1 + \ldots + s'_m = 0.$$

Отсюда $s_1 + \ldots + s_m = 0$ и, в силу свойства (4) теоремы 12, $s_i = 0$ для всех i. Но тогда $s'_i = 0$ для всех i, и по той же теореме 12 сумма $\varphi(S_1) + \ldots + \varphi(S_m)$ оказывается прямой.

Разлагая модуль в прямую сумму подмодулей, мы, грубо говоря, представляем данный большой модуль в виде суммы маленьких. Естественна обратная задача: как

из данных маленьких модулей построить новый большой модуль.

Пусть $M_1, \ldots, M_m$ — некоторые правые модули над кольцом R (не обязательно различные!). Рассмотрим множество всех строк вида $(a_1, \ldots, a_m)$, где $a_i \in M_i$. Это множество при покомпонентном определении операций превращается в правый модуль над кольцом R, который называется *внешней прямой суммой* модулей и обозначается $M_1 \oplus \ldots \oplus M_m$ или $\Sigma^{\oplus} M_i$. Приводимый ниже результат показывает, что эти обозначения согласуются с употреблявшимися раньше.

Теорема 15. *Пусть M — внешняя прямая сумма модулей $M_1, \ldots, M_m$ и S_i, $i = 1, 2, \ldots, m$, — множество всех строк вида $(0, \ldots, 0, a_i, 0, \ldots, 0)$, где $a_i \in M_i$. Тогда S_i — подмодули модуля M, модули M_i и S_i изоморфны для каждого i и M разлагается в прямую сумму подмодулей S_i.*

Доказательство. Ясно, что S_i — подмодули и что каждый из них имеет нулевое пересечение с суммой остальных. Изоморфизм φ: $M_i \to S_i$ можно установить, положив $\varphi(a) = (0, \ldots, a, \ldots, 0)$ для каждого $a \in M_i$. Наконец, равенство

$$(a_1, \ldots, a_m) = (a_1, 0, \ldots, 0) + \\ + (0, a_2, \ldots, 0) + \ldots + (0, 0, \ldots, a_m)$$

показывает, что $M = S_1 \oplus \ldots \oplus S_m$.

Теорема 16. *Если $M = M_1 \oplus \ldots \oplus M_m$, N_i — подмодуль в M_i и $N = N_1 + \ldots + N_m$, то фактормодуль M/N изоморфен внешней прямой сумме $(M_1/N_1) \oplus \ldots \ldots \oplus (M_m/N_m)$.*

Доказательство. Рассмотрим отображение

$$\varphi\colon\ M \to (M_1/N_1) \oplus \ldots \oplus (M_m/N_m),$$

определяемое условием

$$\varphi(a_1 + \ldots + a_m) = ([a_1], \ldots, [a_m]),$$

где $[a_i]$ — смежный класс из фактормодуля M_i/N_i, содержащий элемент a_i. Ввиду свойства (3) из теоремы 12, это определение корректно. Ясно, что φ — гомоморфное наложение. Если $a = a_1 + \ldots + a_m$ и $\varphi(a) = 0$, то $a_i \in N_i$ для всех i. Но тогда $a \in N$, т. е. $\operatorname{Ker} \varphi \subseteq N$. Ясно, что $N \subseteq \operatorname{Ker} \varphi$. Таким образом, $N = \operatorname{Ker} \varphi$, и искомый изоморфизм вытекает из теоремы 7.

Если $n = 2$, $N_1 = 0$ и $N_2 = M_2$, то получаем

Следствие. $(M_1 \oplus M_2)/M_2 \cong M_1$.

Будем говорить, что подмодуль S модуля M *выделяется прямым слагаемым*, если $M = S \oplus H$ для некоторого подмодуля H. Из приведенного выше следствия вытекает

Теорема 17. *Если подмодуль S модуля M выделяется прямым слагаемым, то M содержит подмодуль, изоморфный фактормодулю M/S.*

Подмодуль M модуля L называется *минимальным*, если $M \neq 0$ и соотношение $0 \subseteq N \subset M$*), где N — подмодуль модуля L, влечет за собой $N = 0$. В частности, правый идеал кольца R *минимален*, если он отличен от нуля и не содержит ненулевых правых идеалов кольца R, отличных от него самого. Модуль, являющийся своим минимальным подмодулем, называется *неприводимым*. Другими словами, *неприводимым* называется модуль, отличный от нуля и не содержащий никаких подмодулей, кроме себя самого и нулевого. Примером неприводимого модуля над кольцом целых чисел служат группы простого порядка (см. упражнение 9 из § 3). Поле (и даже тело) является неприводимым модулем над самим собой. Минимальными идеалами кольца $P \times P$, где P — поле (см. упражнения 1 и 6 из § 4), служат множества $\{(x, 0) \mid x \in P\}$, $\{(0, x) \mid x \in P\}$ и $\{(x, x) \mid x \in P\}$. Менее тривиальный пример доставляет следующая теорема.

Теорема 18. *Пусть R — кольцо матриц порядка n над телом D и M_i — множество всех матриц, у которых все элементы, расположенные вне i-й строки, равны 0. Тогда M_i — минимальный правый идеал кольца R.*

Доказательство. Легко проверить, что M_i — правый идеал кольца R. Рассмотрим ненулевой правый идеал H кольца R, лежащий в M_i. Правый идеал H содержит ненулевую матрицу, скажем, A. Тогда $a_{iq} \neq 0$ для некоторого q. Используя обозначения и формулы (*) и (**) из доказательства теоремы 10 из § 4, для любой матрицы $B \in M_i$ будем иметь

$$_{ij}E_{ij} = AE_{qj}(a_{iq}^{-1}b_{ij})\, E \in H.$$

Но тогда $B \in M_i$ влечет за собой

$$B = \sum_{j=1}^{n} b_{ij}E_{ij} \in H,$$

т. е. $H = M_i$.

*) Символ $X \subset Y$ означает, что X — подмножество множества Y и $X \neq Y$. Отметим, что некоторые авторы используют знак $\subset$ в том же смысле, что и $\subseteq$.

Теорема 19. *Правый R-модуль M неприводим тогда и только тогда, когда $M = aR$ для любого ненулевого элемента $a \in M$.*

Доказательство. Если модуль M неприводим и $0 \neq a \in M$, то aR — ненулевой подмодуль модуля M и, следовательно, $aR = M$. Если же модуль M не является неприводимым, то он содержит такой подмодуль H, что $\{0\} \neq H \subset M$. Если теперь $0 \neq a \in H$, то $aR \subseteq H$ и, следовательно, $M \neq aR$.

Подмодуль W модуля L называется *максимальным*, если $W \neq L$ и соотношение $W \subset N \subseteq L$, где N — подмодуль модуля L, влечет за собой $N = L$. В частности, правый идеал кольца R *максимален*, если он отличен от R и не содержится ни в каком правом идеале кольца R, отличном от него самого и от R. Примером максимального подмодуля служит нулевой подмодуль неприводимого модуля. Минимальные идеалы кольца $P \times P$, рассмотренного выше, максимальны.

Теорема 20. *Фактормодуль M/H правого R-модуля M неприводим тогда и только тогда, когда H — максимальный подмодуль.*

Доказательство. Если H — максимальный подмодуль и $[0] \neq [a] \in M/H$, где $[a]$, как и раньше, обозначает смежный класс, содержащий элемент $a \in M$, то $a \notin H$. Отсюда $H \subset H + aR \subseteq M$, что, ввиду максимальности подмодуля H, влечет $H + aR = M$. Если теперь $x \in M$, то $x = y + ar$, где $y \in H$ и $r \in R$. Отсюда $[x] = [ar] = [a]r$, т. е. $M/H = [a]R$, и неприводимость фактормодуля M/H вытекает из теоремы 19. Если, наоборот, M/H — неприводимый модуль, $H \subset K \subseteq M$ и $h \in K \setminus H$ *), то, по теореме 19, $M/H = [h]R$. Если теперь $x \in M$, то $[x] \in [h]R$, т. е. $x = hr + y$, где $r \in R$ и $y \in H \subset K$. Следовательно, $x \in K$. Таким образом, $M = K$, чем и завершается доказательство.

Теорема 21. *Правый модуль над кольцом R неприводим тогда и только тогда, когда он изоморфен фактормодулю R/M, где M — максимальный правый идеал кольца R.*

Доказательство. Если M — максимальный правый идеал, то неприводимость фактормодуля R/M вытекает из теоремы 20. Если же A — неприводимый правый R-модуль, то, по теореме 19, $A = aR$, где $0 \neq a \in A$,

*) Через $U \setminus V$ обозначается множество всех элементов множества U, не принадлежащих множеству V.

Определим отображение φ: $R \to A$, положив $\varphi(r) = ar$ для всех $r \in R$. Нетрудно проверить, что φ — гомоморфное наложение модулей. По теореме 7, $A \cong R/\mathrm{Ker}\,\varphi$, причем, в силу теоремы 20, $\mathrm{Ker}\,\varphi$ — максимальный правый идеал кольца R.

Замечание. Пусть R — кольцо матриц порядка n над телом D, W_i — множество всех матриц с нулевой i-й строкой и M_i — множество всех матриц, у которых все строки, кроме i-й, нулевые. Тогда W_i и M_i — правые идеалы кольца R. В силу следствия теоремы 12 $R = M_i \oplus W_i$. Отсюда, ввиду следствия теоремы 16, имеем $M_i \cong R/W_i$, и из теорем 18 и 20 вытекает, что W_i — максимальный идеал кольца R.

Модуль называется *вполне приводимым*, если он разлагается в прямую сумму конечного числа неприводимых подмодулей. Вполне приводимым правым модулем будет, например, внешняя прямая сумма минимальных правых идеалов. Конечные вполне приводимые модули над кольцом целых чисел описаны в упражнении 21. Другие примеры будут приведены в следующем параграфе.

Теорема 22. *Пусть M — вполне приводимый правый модуль и*

$$M = M_1 \oplus \ldots \oplus M_n$$

— одно из его разложений в прямую сумму неприводимых подмодулей. Тогда все ненулевые подмодули и фактормодули модуля M вполне приводимы, причем каждое из их неприводимых слагаемых изоморфно одному из модулей M_i. Каждый подмодуль модуля M выделяется прямым слагаемым. Каждый фактормодуль модуля M изоморфен его подмодулю.

Доказательство. Предварительно установим две леммы.

Лемма 1. *Если H — подмодуль модуля M и $H \neq M$, то при подходящей нумерации имеем*

$$M = H \oplus M_1 \oplus \ldots \oplus M_k,$$
$$H \cong M_{k+1} \oplus \ldots \oplus M_n$$

и

$$M/H \cong M_1 \oplus \ldots \oplus M_k.$$

Для доказательства, изменив, если нужно, нумерацию, имеем $M_1 \not\subseteq H$. Но тогда $M_1 \cap H \subset M_1$, откуда вследствие неприводимости модуля M_1 вытекает, что $M_1 \cap H = 0$. Если $H + M_1 \neq M$, то, как и выше, получим

$(H + M_1) \cap M_2 = 0$. Продолжая описанное построение, для некоторого натурального числа k будем иметь

$$(H + M_1 + M_2) \cap M_3 = 0,$$
$$(H + M_1 + M_2 + M_3) \cap M_4 = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(H + M_1 + \ldots + M_{k-1}) \cap M_k = 0$$

и

$$H + M_1 + \ldots + M_{k-1} + M_k = M.$$

В силу свойства (2) из теоремы 12 отсюда вытекает, что

$$M = H \oplus M_1 \oplus \ldots \oplus M_k.$$

Первая часть теоремы 13 позволяет записать

$$M = H \oplus (M_1 + \ldots + M_k),$$

т. е. H выделяется прямым слагаемым. Используя следствие теоремы 16 и первую часть теоремы 13, получаем

$$M/H \cong M_1 \oplus \ldots \oplus M_k$$

и

$$H \cong M/(M_1 + \ldots + M_k) = ((M_1 + \ldots + M_k) \oplus$$
$$\oplus (M_{k+1} + \ldots + M_n))/(M_1 + \ldots + M_k) \cong M_{k+1} \oplus \ldots \oplus M_n.$$

Лемма 2. *Если U — неприводимый подмодуль модуля M, то $U \cong M_i$ для некоторого i.*

Действительно, по лемме 1, $U \cong M_{k+1} \oplus \ldots \oplus M_n$. Но поскольку U неприводим, то эта прямая сумма содержит лишь одно слагаемое.

Возвращаясь к доказательству теоремы, заметим, что полная приводимость подмодулей и фактормодулей модуля M сразу следует из леммы 1. Применив к ним лемму 2, убедимся, что любой неприводимый подмодуль этих модулей изоморфен одному из M_i. Из леммы 1 вытекает также, что каждый подмодуль модуля M выделяется из него прямым слагаемым, а каждый фактормодуль модуля M изоморфен некоторому подмодулю модуля M.

Замечание. Если

$$M = M_1 \oplus \ldots \oplus M_m = M_1' \oplus \ldots \oplus M_n'$$

— два разложения вполне приводимого правого модуля M в прямую сумму неприводимых подмодулей, то каждый из модулей M_i изоморфен некоторому модулю M_j' и наоборот. Можно доказать, что $m = n$ и что число модулей, изоморфных данному модулю, одно и то же в обоих разло-

жениях. Это, однако, не означает совпадения слагаемых. Например, если A и B — группы вычетов по модулю 2, то $A \oplus B = A \oplus C$, где $C = \{(0, 0), (1, 1)\}$.

Правый R-модуль называется *конечно порожденным*, если он является линейной оболочкой некоторой конечной системы векторов.

Примером конечно порожденного модуля служит модуль n-мерных строк над произвольным кольцом R. Действительно, положив

$$e_i = (\underbrace{0, \ldots, 0}_{i-1}, 1, 0, \ldots, 0),$$

для любой строки $a = (r_1, \ldots, r_n)$, $r_i \in R$, будем иметь

$$a = e_1 r_1 + \ldots + e_n r_n.$$

Для получения примера модуля, не являющегося конечно порожденным, рассмотрим множество всех счетных последовательностей элементов некоторого кольца R и определим на нем операции, полагая

$$(a_1, a_2, \ldots) + (b_1, b_2, \ldots) = (a_1 + b_1, a_2 + b_2, \ldots)$$

и

$$(a_1, a_2, \ldots)\, r = (a_1 r, a_2 r_2, \ldots).$$

Нетрудно проверить, что таким образом возникает правый R-модуль W. Далее обозначим через V множество всех таких последовательностей из W, почти все (т. е. все, за исключением конечного числа) члены которых равны нулю. Легко видеть, что V — подмодуль модуля W. Допустим, что V — линейная оболочка последовательностей $v_1, \ldots, v_m \in V$. Но тогда найдется такой номер n, что все члены этих последовательностей, начиная с $(n + 1)$-го, равны нулю. Следовательно, равенство

$$(\underbrace{1, \ldots, 1}_{n+1}, 0, 0, \ldots) = v_1 r_1 + \ldots + v_m r_m$$

вопреки допущению не имеет места ни при каких $r_i \in R$. Таким образом, модуль V не конечно порожден. Несколько сложнее доказывается, что и сам модуль W не является конечно порожденным. Можно доказать также, что группа рациональных чисел не конечно порождена как модуль над кольцом целых чисел (см. упражнение 4).

Т е о р е м а 23. *Каждый конечно порожденный правый R-модуль M изоморфен фактормодулю правого модуля n-мерных строк над кольцом R для подходящего натурального числа n.*

Д о к а з а т е л ь с т в о. По определению, модуль M совпадает с линейной оболочкой некоторой конечной системы векторов, скажем, $a_1, \ldots, a_n$. Пусть V — модуль n-мерных строк. Определим отображение φ: $V \to M$,

полагая

$$\varphi(r_1, \ldots, r_n) = a_1 r_1 + \ldots + a_n r_n.$$

Легко проверяется, что φ — гомоморфизм модулей. Если $a \in M$, то

$$a = a_1 r_1 + \ldots + a_n r_n$$

для некоторых $r_i \in R$. Отсюда

$$\varphi(r_1, \ldots, r_n) = a,$$

т. е. φ оказывается наложением. По теореме 7, модуль M изоморфен $V/\mathrm{Ker}\,\varphi$.

Упражнения

1. Убедиться, что ситуация, описанная в примере 8 таблицы 4, возникает, если S — кольцо матриц порядка 2, а R — множество всех матриц вида $\begin{Vmatrix} a & 0 \\ 0 & 0 \end{Vmatrix}$. Указать единицу кольца R.

2. Доказать, что множество n-мерных строк, сумма координат каждой из которых равна нулю, образует подмодуль модуля строк.

3. Используя запись комплексных чисел в форме $a + bi$, где a и b — действительные числа, можно отождествить множество комплексных чисел с множеством всех точек действительной плоскости. Доказать, что всякая прямая, проходящая через начало координат, является подмодулем модуля комплексных чисел над полем действительных чисел (пример 4 из таблицы 4) и что это не так, если комплексные числа рассматривать как модуль над собой (пример 1 из таблицы 4).

4. Доказать, что линейная оболочка любого конечного множества рациональных чисел не совпадает со всей группой рациональных чисел по сложению, рассматриваемой как модуль над кольцом целых чисел (пример 3 из таблицы 4). Убедиться, что эта группа конечно порождена как модуль над полем рациональных чисел.

5. Доказать, что линейная оболочка двух целых чисел совпадает со всем кольцом целых чисел, рассматриваемым как модуль над собой (пример 1 из таблицы 4), тогда и только тогда, когда эти числа взаимно просты.

6. Пусть R — множество счетных последовательностей элементов из поля P с операциями

$$(a_1, a_2, \ldots) + (b_1, b_2, \ldots) = (a_1 + b_1,\ a_2 + b_2, \ldots)$$

и

$$(a_1, a_2, \ldots)(b_1, b_2, \ldots) = (a_1 b_1, a_2 b_2, \ldots).$$

Доказать, что R — коммутативное кольцо и что множество H, состоящее из всех последовательностей из R, у которых все члены, за исключением конечного числа, равны нулю, образует идеал кольца R. Доказать, что H не является конечно порожденным R-модулем, хотя R конечно порождено как R-модуль.

7. Фактормодуль конечно порожденного модуля конечно порожден.

8. Пусть N — подмодуль модуля M. Доказать, что из конечной порожденности модулей N и M/N вытекает конечная порожденность модуля M.

9. Сумма конечного множества конечно порожденных подмодулей конечно порождена.

10. Если A, B, C — подмодули модуля M, $A \subseteq B$, $A + C = B + C$ и $A \cap C = B \cap C$, то $A = B$.

11. Если A, B, C — подмодули модуля M и $A \subseteq C$, то $(A + B) \cap C = A + B \cap C$. Убедиться, что равенство $(A + B) \cap C = A \cap C + B \cap C$ не имеет места, если M — модуль двумерных строк над кольцом R (см. пример 2 из таблицы 4), а A, B и C — все строки вида $(0, r)$, $(r, 0)$ и (r, r) соответственно.

12. Если A и B — подмодули модуля M, то фактормодуль $(A + B)/A \cap B$ изоморфен внешней прямой сумме $(A/(A \cap B)) \oplus (B/(A \cap B))$.

13. Если M и M' — модули над коммутативным кольцом R, то определение $x(r\varphi) = r(x\varphi)$, где $x \in M$, $r \in R$, $\varphi \in \mathrm{Hom}(M, M')$, превращает $\mathrm{Hom}(M, M')$ в левый R-модуль. Убедиться, что коммутативность кольца R существенна.

14. Если $M = M' \oplus M''$ и $\mathrm{Hom}(M', M'') = \mathrm{Hom}(M'', M') = 0$, то кольцо $\mathrm{Hom}(M, M)$ изоморфно кольцу $\mathrm{Hom}(M', M') \times \mathrm{Hom}(M'', M'')$ (см. упражнение 1 из § 4).

15. Пусть M — модуль, $\varphi \in \mathrm{Hom}(M, M)$ и $\varphi^2 = \varphi$. Доказать, что $M = \mathrm{Ker}\,\varphi \oplus \mathrm{Im}\,\varphi$. Указание: каждый элемент $x \in M$ представить в форме $x = (x - x\varphi) + x\varphi$.

16. Доказать, что кольцо целых чисел не содержит минимальных идеалов.

17. Пусть R — кольцо действительных функций и W — множество функций, обращающихся в нуль в точке a. Доказать, что W — максимальный идеал кольца R.

18. Доказать, что идеал кольца целых чисел максимален тогда и только тогда, когда он порождается простым числом.

19. Модуль n-мерных строк над полем (и даже над телом) вполне приводим.

20. Правый R-модуль M изоморфен правому модулю n-мерных строк над кольцом R тогда и только тогда, когда M содержит элементы $a_1, \ldots, a_n$, обладающие следующими свойствами: а) M совпадает с линейной оболочкой системы $\{a_1, \ldots, a_n\}$; б) если H — произвольный правый R-модуль, то, каковы бы ни были элементы $b_1, \ldots, b_n \in H$, существует гомоморфизм φ: $M \to H$ такой, что $\varphi(a_i) = b_i$ для каждого i.

21. Конечная коммутативная группа G вполне приводима как модуль над кольцом целых чисел тогда и только тогда, когда для любого $a \in G$ число элементов подгруппы $\boldsymbol{Z}a$ свободно от квадратов (т. е. равно $p_1 \ldots p_m$, где p_i — различные простые числа).

§ 6. Правые идеалы в кольцах

Элемент e кольца R называется *идемпотентом*, если $e^2 = e$. Идемпотенты e и f называются *ортогональными*, если $ef = fe = 0$. В качестве примера можно указать ортогональные идемпотенты E_{ii} и E_{jj}, где $i \neq j$, в кольце матриц (см. доказательство теоремы 10 из § 4). Про правый идеал eR скажем, что он *порождается идемпотентом* e.

Правый идеал H кольца R назовем *правым идеалом с нулевым умножением*, если $xy = 0$ для любых $x, y \in H$.

Замечание. *Если e — идемпотент кольца R, то $x \in eR$ тогда и только тогда, когда $x = ex$.*

Действительно, ясно, что $ex \in eR$. Если же $x \in eR$, то $x = er$ для некоторого $r \in R$. Отсюда

$$x = er = e^2r = e(er) = ex.$$

В дальнейшем этот факт будет часто использоваться без специальных ссылок.

Теорема 1. *Если R — кольцо с единицей и $R = H_1 \oplus \ldots \oplus H_n$ — разложение в прямую сумму правых идеалов, то найдутся такие идемпотенты $e_1, \ldots, e_n$, что $H_i = e_iR$ для каждого i, $e_ie_j = 0$, если $i \neq j$, и $1 = e_1 + \ldots + e_n$.*

Доказательство. В силу теоремы 11 из § 5 $1 = e_1 + \ldots + e_n$, где $e_i \in H_i$. Умножая справа на e_i и используя определение прямой суммы, получаем

$$e_i - e_i^2 = e_1e_i + \ldots + e_{i-1}e_i + e_{i+1}e_i + \ldots + e_ne_i \in$$
$$\in H_i \cap (H_1 + \ldots + H_{i-1} + H_{i+1} + \ldots + H_n) = 0,$$

т. е. e_i — идемпотенты. По тем же соображениям имеем

$$e_j = e_1e_j + \ldots + e_{j-1}e_j + e_j + e_{j+1}e_j + \ldots + e_ne_j.$$

Отсюда

$$e_1e_j + \ldots + e_{j-1}e_j + e_{j+1}e_j + \ldots + e_ne_j = 0$$

и, используя свойство (4) теоремы 12 из § 5, получаем

$$e_1e_j = \ldots = e_{j-1}e_j = e_{j+1}e_j = \ldots = e_ne_j = 0,$$

т. е. $e_ie_j = 0$ при $i \neq j$. Если $x \in H_i$, то

$$x = e_1x + \ldots + e_nx,$$

откуда, как и выше,

$$x - e_ix = e_1x + \ldots + e_{i-1}x + e_{i+1}x + \ldots + e_nx \in$$
$$\in H_i \cap (H_1 + \ldots + H_{i-1} + H_{i+1} + \ldots + H_n) = 0.$$

Таким образом, $x = e_ix \in e_iR$, т. е. $H_i \subseteq e_iR$. Поскольку $e_i \in H_i$ влечет $e_iR \subseteq H_i$, то $H_i = e_iR$.

Теорема 2. *Сумма правых идеалов кольца R с единицей, порожденных попарно ортогональными идемпотентами, прямая.*

Доказательство. Пусть $e_1, \ldots, e_n$ — попарно ортогональные идемпотенты и $0 = x_1 + \ldots + x_n$,

где $x_i \in e_iR$. По замечанию, $x_i = e_ix_i$, а значит, $e_jx_i = e_je_ix_i = 0$, если $i \neq j$. Следовательно,

$$0 = e_i(x_1 + \ldots + x_n) = e_ix_i = x_i$$

и, согласно свойству (4) теоремы 12 из § 5, сумма $e_1R + \ldots + e_nR$ оказывается прямой.

Напомним, что правый идеал M кольца R называется *минимальным*, если из соотношений $0 \neq H \subseteq M$, где H — правый идеал кольца R, вытекает, что $H = M$. Другими словами, минимальный правый идеал — это неприводимый подмодуль правого R-модуля R.

Теорема 3. *Минимальный правый идеал кольца R с единицей или является правым идеалом с нулевым умножением, или порождается ненулевым идемпотентом.*

Доказательство. Пусть M — минимальный правый идеал кольца R. Если он не является правым идеалом с нулевым умножением, то $ab \neq 0$ для некоторых $a, b \in M$. Нетрудно проверить, что aM — правый идеал кольца R. При этом $0 \neq ab \in aM$ и, следовательно, $0 \neq aM \subseteq M$. В силу минимальности правого идеала M имеем $aM = M$. В частности, $a = ae$ для некоторого $e \in M$. Конечно, $e \neq 0$. Рассмотрим множество

$$H = \{x \mid x \in R,\ ax = 0\},$$

т. е. совокупность всех $x \in R$ таких, что $ax = 0$. Легко проверяется, что H — правый идеал кольца R. Ввиду теоремы 1 из § 5, $H \cap M$ — также правый идеал кольца R. При этом $H \cap M \subseteq M$. Но $H \cap M \neq M$, поскольку b лежит в M, но не лежит в H. Из минимальности правого идеала M вытекает, что $H \cap M = 0$. Но $e - e^2 \in M$ и

$$a(e - e^2) = ae - ae^2 = a - ae = 0,$$

т. е. $e - e^2 \in M \cap H = 0$. Следовательно, $e = e^2$. Наконец, из соотношения $0 \neq eR \subseteq M$, в силу минимальности правого идеала M, вытекает, что $eR = M$.

Теорема 4. *Если кольцо R с единицей не содержит ненулевых двусторонних идеалов с нулевым умножением, то оно не содержит и ненулевых правых идеалов с нулевым умножением.*

Доказательство. Предположим, что кольцо R содержит ненулевой правый идеал M с нулевым умножением. Рассмотрим множество I всевозможных сумм вида

$$r_1m_1 + \ldots + r_km_{k_2}$$

где $r_i \in R$, $m_i \in M$. Легко проверяется, что I — двусторонний идеал. Поскольку $M \subseteq I$, то $I \neq 0$. Однако, учитывая, что $m_i r_j' \in M$, если $r_j' \in R$, и что M — правый идеал с нулевым умножением, получаем

$$(r_1 m_1 + \ldots + r_k m_k)(r_1' m_1' + \ldots + r_l' m_l') = \\ = \sum_{i,\,j} r_i (m_i r_j') m_j' = 0.$$

Таким образом, I оказывается ненулевым двусторонним идеалом с нулевым умножением, что противоречит условию.

Кольцо R с единицей называется *вполне приводимым справа*, если R — вполне приводимый правый R-модуль. Другими словами, кольцо вполне приводимо справа, если оно разлагается в прямую сумму конечного числа своих минимальных правых идеалов. Вполне приводимым справа кольцом является каждое поле, а также конечная прямая сумма полей. Нетривиальный пример доставляет следующая теорема.

Т е о р е м а 5. *Кольцо матриц над телом вполне приводимо справа.*

Д о к а з а т е л ь с т в о. Пусть R — кольцо матриц порядка n над телом D. Используя теорему 12 из § 5 и обозначения, использованные в теореме 18 из § 5, имеем

$$R = M_1 \oplus \ldots \oplus M_n.$$

Остается заметить, что по той же теореме 18 M_i — минимальные правые идеалы кольца R.

Т е о р е м а 6. *Каждый правый идеал H вполне приводимого справа кольца R порождается идемпотентом. Этот идемпотент может быть выбран в центре кольца R* (такой идемпотент называется *центральным*) *тогда и только тогда, когда H — двусторонний идеал.*

Д о к а з а т е л ь с т в о. Ввиду теоремы 22 из § 5 $R = H \oplus H'$, где H' — правый идеал кольца R, и первое утверждение доказываемой теоремы вытекает из теоремы 1. При этом $1 = e + f$, где $e^2 = e$, $f^2 = f$, $ef = fe = 0$, $H = eR$ и $H' = fR$. Если H — двусторонний идеал, то для любого $r \in R$ имеем $re \in H = eR$ и, следовательно, $re = er'$ для некоторого $r' \in R$. Отсюда

$$fre = fer' = 0 \qquad (*)$$

для любого $r \in R$. Далее, правый идеал $erfR$ в силу уже доказанного порождается идемпотентом, т. е. $erfR = gR$, где $g^2 = g$. Отсюда $erf = gerf$ и $g = erfs$ для некоторого

$s \in R$. Ввиду (*)

$$g = g^2 = erfserfs = 0$$

и, следовательно,

$$erf = gerf = 0. \qquad (**)$$

Учитывая ортогональность e и f, (*) и (**), получаем

$$er - re = (e + f)(er - re)(e + f) = ere + fere + erf +$$
$$+ ferf - ere - fre - eref - fref = ere - ere = 0$$

для любого $r \in R$, т. е. e оказывается центральным идемпотентом. Наоборот, если e — центральный идемпотент, то равенство $r(ex) = e(rx)$, справедливое для любых x, $r \in R$, показывает, что eR — двусторонний идеал.

Теорема 7. *Пусть e — центральный идемпотент кольца R с единицей. Тогда*

(1) *eR — кольцо с единицей e, причем всякий правый (левый, двусторонний) идеал кольца eR оказывается правым (левым, двусторонним) идеалом кольца R;*

(2) *каждый минимальный правый идеал кольца R, лежащий в eR, является минимальным правым идеалом кольца eR;*

(3) *если кольцо R вполне приводимо справа, то кольцо eR также вполне приводимо справа.*

Доказательство. Поскольку

$$ex = (ee)x = e(ex) = e(xe) = (ex)e$$

для любого $x \in R$, то e оказывается единицей кольца eR. Если H — правый идеал кольца eR и $h \in H$, то $h = eh$. Отсюда

$$hr = (eh)r = (he)r = h(er) \in H$$

для любого $r \in R$, ибо $er \in eR$. Следовательно, H — правый идеал кольца R. Соответствующие утверждения для левых и двусторонних идеалов доказываются аналогично. Если, далее, M — минимальный правый идеал кольца R и $M \subseteq eR$, то рассмотрим соотношение $0 \neq H \subseteq M$, где H — правый идеал кольца R. В силу утверждения (1), H — правый идеал кольца R, что ввиду минимальности правого идеала M влечет $H = M$. Следовательно, M — минимальный правый идеал кольца eR. Наконец, если кольцо R вполне приводимо справа, то согласно теореме 22 из § 5 имеем

$$eR = M_1 \oplus \ldots \oplus M_m,$$

где M_i — минимальные правые идеалы кольца R. В силу утверждения (2), M_i — минимальные правые идеалы кольца eR, что доказывает утверждение (3).

Т е о р е м а 8. *Все ненулевые конечно порожденные правые модули над вполне приводимым справа кольцом R вполне приводимы. Каково бы ни было разложение кольца в прямую сумму минимальных правых идеалов, каждый неприводимый правый модуль над таким кольцом изоморфен одному из минимальных правых идеалов, встречающихся в этом разложении.*

Д о к а з а т е л ь с т в о. Пусть L — произвольный конечно порожденный правый R-модуль. По теореме 23 из § 5, модуль L изоморфен фактормодулю V/K, где V — модуль m-мерных строк для некоторого натурального m. Согласно теореме 15 из § 5, модуль V изоморфен внешней прямой сумме

$$\underbrace{R \oplus \ldots \oplus R}_{m \text{ раз}}.$$

Если теперь

$$R = M_1 \oplus \ldots \oplus M_n$$

— некоторое представление кольца R в виде прямой суммы минимальных правых идеалов, то, в силу теоремы 13 из § 5, модуль V изоморфен прямой сумме

$$M_1 \oplus \ldots \oplus M_n \oplus M_1 \oplus \ldots \oplus M_n \oplus \ldots \oplus M_1 \oplus \ldots \oplus M_n.$$

По теореме 22 из § 5, модуль V/K, а значит и модуль L, вполне приводим, причем в его представлении в виде прямой суммы неприводимых модулей встречаются лишь модули, изоморфные каким-либо правым идеалам M_i. В частности, поскольку неприводимый модуль неразложим в прямую сумму, он должен быть изоморфен одному из этих минимальных правых идеалов.

С л е д с т в и е. *Каждый конечно порожденный правый модуль над вполне приводимым справа кольцом изоморфен внешней прямой сумме некоторых минимальных правых идеалов этого кольца.*

Т е о р е м а 9. *Каждый неприводимый правый модуль над вполне приводимым справа кольцом изоморфен некоторому минимальному правому идеалу этого кольца.*

Д о к а з а т е л ь с т в о. Поскольку каждое кольцо с единицей является конечно порожденным правым модулем над собой (оно порождается единицей), то, ввиду

теоремы 19 из § 5, каждый неприводимый модуль конечно порожден. Теперь остается лишь применить только что сформулированное следствие.

Упражнения

1. Кольцо R называется *нильпотентным*, если существует такое натуральное n, что произведение любых n элементов из R равно нулю. Доказать, что кольцо не содержит ненулевых правых (левых, двусторонних) идеалов с нулевым умножением тогда и только тогда, когда оно не содержит ненулевых нильпотентных правых (левых, двусторонних) идеалов.

2. Элемент a кольца R называется *нильпотентным*, если $a^n = 0$ для некоторого натурального n. Доказать, что коммутативное кольцо не содержит ненулевых нильпотентных идеалов тогда и только тогда, когда оно не содержит ненулевых нильпотентных элементов. Рассматривая кольцо матриц второго порядка над полем, убедиться, что это неверно в некоммутативном случае.

3. Пусть R — кольцо, I — его идеал, а кольцо I и факторкольцо R/I нильпотентны. Доказать, что кольцо R также нильпотентно.

4. Доказать, что сумма нильпотентных правых идеалов нильпотентна.

5. Доказать, что всякое коммутативное вполне приводимое кольцо с единицей является прямой суммой полей.

6. Если все идемпотенты вполне приводимого справа кольца центральны, то все его правые идеалы являются двусторонними.

7. Доказать, что кольцо $D \times D$, где D — тело (см. упражнение 1 из § 4), вполне приводимо справа.

§ 7. Абелевы, разрешимые и простые группы

В этом параграфе рассматриваются группы, обладающие некоторыми дополнительными свойствами. Попутно устанавливаются некоторые важные свойства конечных групп (например, теорема Силова).

Начнем наше исследование с коммутативных или, что то же самое, абелевых групп. Как уже отмечалось, они являются модулями над кольцом целых чисел $\boldsymbol{Z}$ (см. пример 3 из таблицы 4). Поскольку кольцо $\boldsymbol{Z}$ коммутативно, то левые и правые модули можно не различать (см. с. 105, —107), и мы будем придерживаться левой записи.

Элемент a абелевой группы A называется *периодическим*, если $na = 0$ для некоторого ненулевого $n \in \boldsymbol{Z}$. Совокупность всех периодических элементов группы A называется ее *периодической частью* и обозначается через $T(A)$. Ясно, что $T(\boldsymbol{Z}) = \{0\}$. Если A — конечная группа, то $T(A) = A$ в силу теоремы 22 из § 3.

Теорема 1. *Если A — абелева группа, то $T(A)$ — ее подгруппа и $T(A/T(A)) = \{0\}$.*

Доказательство. Ясно, что $0 \in T(A)$. Если $x, y \in T(A)$, то $mx = ny = 0$, где $0 \neq m, n \in \boldsymbol{Z}$. Учитывая аддитивную форму теорем 9 и 10 из § 3 (см. примечание на с. 77), получаем

$$mn(x+y) = n(mx) + m(ny) = 0$$

и

$$m(-x) = -mx = 0.$$

Следовательно, $x+y$ и $-x$ принадлежат $T(A)$, т. е. $T(A)$ — подгруппа. Как и всякая подгруппа коммутативной группы, она нормальна, что дает возможность рассмотреть факторгруппу $A/T(A)$. Если $[x] \in T(A/T(A))$ (как всегда, $[x]$ обозначает смежный класс, содержащий элемент x), то для некоторого ненулевого $n \in \boldsymbol{Z}$ имеем $n[x] = [0]$. Отсюда $[nx] = [0]$, т. е. $nx \in T(A)$. Поскольку nx — периодический элемент, то $m(nx) = 0$ для некоторого ненулевого $m \in \boldsymbol{Z}$. Поскольку $mn \neq 0$, то $x \in T(A)$ и, следовательно, $[x] = [0]$.

Если A — абелева группа, то система $\{e_1, \ldots, e_n\}$ элементов из A называется *базой*, если для любого $a \in A$ найдутся такие $k_1, \ldots, k_n \in \boldsymbol{Z}$, что $a = k_1e_1 + \ldots + k_me_m$, а равенство $l_1e_1 + \ldots + l_ne_n = 0$, где $l_1, \ldots, l_n \in \boldsymbol{Z}$, влечет за собой $l_1 = \ldots = l_n = 0$. В качестве примера заметим, что строки $e_1, \ldots, e_n$, где $e_i = (\underbrace{0, \ldots, 0}_{i-1 \text{ раз}}, 1, 0, \ldots, 0)$, образуют базу группы строк с координатами из группы $\boldsymbol{Z}$.

Теорема 2. *Если* $\{e_1, \ldots, e_n\}$ — *база абелевой группы* F, $k_1, \ldots, k_n, k_1', \ldots, k_n' \in \boldsymbol{Z}$ *и*

$$k_1e_1 + \ldots + k_ne_n = k_1'e_1 + \ldots + k_n'e_n,$$

то $k_1 = k_1', \ldots, k_n = k_n'$.

Доказательство. Если

$$a = k_1e_1 + \ldots + k_ne_n = k_1'e_1 + \ldots + k_n'e_n,$$

то, принимая во внимание основные свойства модулей (см. с. 107), получаем

$$(k_1 - k_1')e_1 + \ldots + (k_n - k_n')e_n = 0,$$

откуда $k_1 - k_1' = \ldots = k_n - k_n' = 0$, т. е. $k_1 = k_1', \ldots, k_n = k_n'$.

Если e_1 — периодический элемент, то $me_1 = 0$ для некоторого ненулевого $m \in \boldsymbol{Z}$. Отсюда

$$me_1 + 0e_2 + \ldots + 0e_n = 0,$$

что противоречит определению базы. Таким образом, база не может содержать периодических элементов. Ввиду теоремы 22 из § 3, отсюда вытекает, что конечная группа не может иметь базы.

Абелеву группу, обладающую базой, назовем *свободной*.

Теорема 3 (лемма о базе). *Если F — свободная абелева группа с базой $\{f_1, \ldots, f_n\}$ и H — ее ненулевая подгруппа, то группа F обладает такой базой $\{e_1, \ldots, e_n\}$, что $se_1 \in H$ для некоторого ненулевого $s \in \mathbf{Z}$, а включение $k_1e_1 + k_2e_2 + \ldots + k_ne_n \in H$, где $k_1, \ldots, k_n \in \mathbf{Z}$, влечет за собой, что k_1 делит s.*

Доказательство. Если $\mathscr{C} = \{c_1, \ldots, c_n\}$ — некоторая база группы F, то обозначим через $\Gamma(\mathscr{C})$ наименьшее из таких целых положительных чисел k, что при подходящих целых числах $k_2, \ldots, k_n$ справедливо включение

$$kc_1 + k_2c_2 + \ldots + k_nc_n \in H.$$

Будем считать, что база $\mathscr{C}$ выбрана так, что $\Gamma(\mathscr{C}) \leqslant \Gamma(\mathscr{D})$ для любой базы $\mathscr{D}$ группы F, состоящей из n элементов. Пусть

$$h = \Gamma(\mathscr{C})c_1 + k_2c_2 + \ldots + k_nc_n \in H.$$

Осуществив деление с остатком, будем иметь

$$k_i = \Gamma(\mathscr{C})\, q_i + r_i \quad (i = 2, \ldots, n),$$

где $0 \leqslant r_i < \Gamma(\mathscr{C})$. Положим

$$c = c_1 + q_2c_2 + \ldots + q_nc_n$$

и

$$\mathscr{C}' = \{c, c_2, \ldots, c_n\}.$$

Если $g \in F$, то для подходящих $l_1, \ldots, l_n \in \mathbf{Z}$ имеем

$$g = l_1c_1 + l_2c_2 + \ldots + l_nc_n = l_1c + (l_2 - l_1q_2)\, c_2 + \ldots + (l_n - l_1q_n)\, c_n.$$

С другой стороны, если

$$l_1c + l_2c_2 + \ldots + l_nc_n = 0,$$

где $l_1, l_2, \ldots, l_n \in \mathbf{Z}$, то

$$l_1c_1 + (l_2 + l_1q_2)\, c_2 + \ldots + (l_n + l_1q_n)\, c_n = 0.$$

Поскольку $\mathscr{C}$ — база, то отсюда вытекает, что

$$l_1 = l_2 + l_1q_2 = \ldots = l_n + l_1q_n = 0,$$

откуда $l_1 = l_2 = \ldots = l_n = 0$. Таким образом, $\mathscr{C}'$ оказывается базой группы F. Предположим, что $r_i \neq 0$ для некоторого i. Ясно, что

$$\mathscr{C}'' = \{c_i, c, c_2, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n\}$$

является базой группы F. При этом

$$\begin{aligned} h = \Gamma(\mathscr{C})(c - q_2c_2 - \ldots - q_nc_n) + k_2c_2 + \ldots + k_nc_n = \\ = \Gamma(\mathscr{C})\, c + r_2c_2 + \ldots + r_nc_n = \\ = r_ic_i + \Gamma(\mathscr{C})\, c + r_2c_2 + \ldots + r_{i-1}c_{i-1} + \\ + r_{i+1}c_{i+1} + \ldots + r_nc_n. \end{aligned}$$

Следовательно, $\Gamma(\mathscr{C}'') \leqslant r_i < \Gamma(\mathscr{C})$, в то время как $\Gamma(\mathscr{C}) \leqslant \Gamma(\mathscr{C}'')$ по выбору базы $\mathscr{C}$. Таким образом, $r_2 = \ldots = r_n = 0$ и $h = \Gamma(\mathscr{C})\, c$, т. е. база $\mathscr{C}$ обладает первым из требуемых свойств.

Если, далее,

$$g = k_1c + k_2c_2 + \ldots + k_nc_n \in H$$

и

$$k_1 = \Gamma(\mathscr{C})\, q + r,$$

где $0 \leqslant r < \Gamma(\mathscr{C})$, то

$$\begin{aligned} rc - k_2c_2 - \ldots - k_nc_n = \\ = (q\Gamma(\mathscr{C}) - k_1)c - k_2c_2 - \ldots - k_nc_n = \\ = q\Gamma(\mathscr{C})c - g \in H, \end{aligned}$$

что противоречит выбору числа $\Gamma(\mathscr{C})$.

Т е о р е м а 4. *Следующие свойства конечно порожденной абелевой группы F эквивалентны*: (1) *F свободна*; (2) *F изоморфна группе n-мерных строк с координатами из группы $\boldsymbol{Z}$ для подходящего целого положительно числа n*; (3) *F изоморфна внешней прямой сумме n экземпляров группы $\boldsymbol{Z}$ для подходящего целого положительного числа n*; (4) $T(F) = \{0\}$.

Д о к а з а т е л ь с т в о. (1) $\Rightarrow$ (2). Если $\{e_1, \ldots, e_n\}$ — база группы F, а G — группа n-мерных строк с координатами из $\boldsymbol{Z}$, то определим отображение φ: $G \to F$, положив

$$\varphi(k_1, \ldots, k_n) = k_1e_1 + \ldots + k_ne_n.$$

Нетрудно проверить, что φ — гомоморфное наложение групп. Если $\varphi(k_1, \ldots, k_n) = \varphi(k_1', \ldots, k_n')$, то, ввиду теоремы 2, $k_1 = k_1'$, $k_2 = k_2'$, $\ldots$, $k_n = k_n'$, т. е. φ оказывается вложением и, следовательно, изоморфизмом.

(2) $\Rightarrow$ (4). Если $m, k_1, \ldots, k_n \in \boldsymbol{Z}$, $m \neq 0$ и $m(k_1, \ldots, k_n) = (0, \ldots, 0)$, то, очевидно, $k_1 = \ldots = k_n = 0$.

(4) $\Rightarrow$ (1). Поскольку F конечно порождена, то $F = \boldsymbol{Z}a_1 + \ldots + \boldsymbol{Z}a_n$, причем можно считать, что n выбрано наименьшим из возможных. Пусть G — абелева группа, обладающая базой $\{f_1, \ldots, f_n\}$ (например, группа n-мерных строк с координатами из группы $\boldsymbol{Z}$). Определим отображение φ: $G \to F$, положив

$$\varphi(k_1 f_1 + \ldots + k_n f_n) = k_1 a_1 + \ldots + k_n a_n.$$

В силу теоремы 2, это определение корректно. Ясно, что φ — гомоморфное наложение групп. По теореме 8 из § 3, $F \cong G/\mathrm{Ker}\,\varphi$. Если $\mathrm{Ker}\,\varphi = \{0\}$, то все доказано. В противном случае теорема 3 позволяет найти такую базу $\{e_1, \ldots, e_n\}$ группы G, что $se_1 \in \mathrm{Ker}\,\varphi$, где $0 \neq s \in \boldsymbol{Z}$. Если $[e_1]$ — смежный класс, содержащий элемент e_1, то $s[e_1] = [se_1] = [0]$, откуда $[e_1] = [0]$, поскольку $T(G/\mathrm{Ker}\,\varphi) = \{[0]\}$. Если теперь $g \in F$, то для подходящих $k_1, \ldots, k_n \in \boldsymbol{Z}$ имеем

$$g = \varphi(k_1 e_1 + \ldots + k_n e_n) = k_2\varphi(e_2) + \ldots + k_n\varphi(e_n).$$

Следовательно,

$$F = \boldsymbol{Z}\varphi(e_2) + \ldots + \boldsymbol{Z}\varphi(e_n),$$

что противоречит выбору числа n.

Остается заметить, что эквивалентность свойств (2) и (3) является следствием теоремы 15 из § 5.

Т е о р е м а 5. *Всякая конечно порожденная абелева группа A разлагается в прямую сумму свободной и конечной групп.*

Д о к а з а т е л ь с т в о. Из конечной порожденности группы A нетрудно вывести, что факторгруппа $A/T(A)$ также конечно порождена. Ввиду теорем 1 и 4, отсюда вытекает, что $A/T(A)$ — свободная группа. Пусть $\{[e_1], \ldots, [e_n]\}$ — база этой факторгруппы (как обычно, через $[a]$ обозначается смежный класс, содержащий элемент a). Пусть $F = \boldsymbol{Z}e_1 + \ldots + \boldsymbol{Z}e_n$. Если $k_1 e_1 + \ldots + k_n e_n = 0$, где $k_1, \ldots, k_n \in \boldsymbol{Z}$, то $k_1[e_1] + \ldots + k_n[e_n] = [0]$, откуда $k_1 = \ldots = k_n = 0$ по определению базы. Следовательно, F — свободная группа с базой $\{e_1, \ldots, e_n\}$. Далее, если $a \in A$, то

$$[a] = k_1[e_1] + \ldots + k_n[e_n],$$

где $k_1, \ldots, k_n \in \boldsymbol{Z}$, откуда

$$b = a - k_1 e_1 - \ldots - k_n e_n \in T(A),$$

Следовательно, $a = u + b$, где $u \in F$ и $b \in T(A)$, т. е. $A = F + T(A)$. Ввиду теоремы 4, $F \cap T(A) = \{0\}$ и $A = F \oplus T(A)$ по следствию теоремы 12 из § 5. По следствию теоремы 16 из § 5, $T(A) \cong A/F$, откуда, как уже отмечалось, вытекает конечная порожденность группы $T(A)$, т. е. $T(A) = \boldsymbol{Z}b_1 + \ldots + \boldsymbol{Z}b_m$ для некоторых $b_1, \ldots, b_m \in T(A)$. Ясно, что $\boldsymbol{Z}b_1, \ldots, \boldsymbol{Z}b_m$ — конечные группы. Но тогда оказывается конечной и группа $T(A)$, ибо

$$|T(A)| \leqslant |\boldsymbol{Z}b_1| \ldots |\boldsymbol{Z}b_m|.$$

Примарной циклической группой называется группа вычетов по модулю p^m, где p — простое число.

Теорема 6. *Всякая конечная абелева группа изоморфна внешней прямой сумме примарных циклических групп.*

Доказательство. Предварительно установим две леммы.

Лемма 1. *Всякая конечная абелева группа изоморфна прямой сумме циклических подгрупп.*

Проведем доказательство индукцией по числу элементов рассматриваемой группы A. При $|A| = 1$ доказываемое утверждение тривиально. Пусть $|A| \geqslant 2$. В силу теоремы 4 и теоремы 23 из § 5, $A \cong F/H$, где F — свободная абелева группа. Пусть n — число элементов, входящих в базу этой группы. Можно считать, что группа F выбрана так, что число n является наименьшим из возможных. Если бы подгруппа H была нулевой, то группа A оказалась бы бесконечной. Если же $H \neq \{0\}$, то применима теорема 3. Пусть $\{e_1, \ldots, e_n\}$ и s имеют тот же смысл, что и в этой теореме. Тогда для любого $h \in H$ имеем

$$h = k_1 s e_1 + k_2 e_2 + \ldots + k_n e_n,$$

где $k_1, \ldots, k_n \in \boldsymbol{Z}$. Поскольку $se_1 \in H$, то

$$k_2 e_2 + \ldots + k_n e_n \in H \cap F',$$

где $F' = \boldsymbol{Z}e_2 + \ldots + \boldsymbol{Z}e_n$. Другими словами,

$$H = \boldsymbol{Z}se_1 + H \cap F'.$$

С другой стороны, ясно, что

$$F = \boldsymbol{Z}e_1 \oplus F'.$$

По теореме 16 из § 5 отсюда вытекает, что

$$A \cong F/H \cong C_1 \oplus F'/H \cap F',$$

где $C_1 = \boldsymbol{Z}e_1 / \boldsymbol{Z}se_1$. Первое слагаемое, очевидно, является циклической группой. Если оно равно нулю, то мы вступаем в противоречие с выбором числа n, поскольку ясно, что F' — свободная абелева группа с базой $\{e_2, \ldots, e_n\}$. В противном случае $|F'/H \cap F'| < |A|$ и, в силу индуктивного предположения,

$$F'/H \cap F' \cong C_2 \oplus \ldots \oplus C_m,$$

где $C_2, \ldots, C_m$ — циклические группы. По теореме 13 из § 5,

$$A \cong C_1 \oplus C_2 \oplus \ldots \oplus C_m.$$

Лемма 2. *Всякая циклическая группа C изоморфна прямой сумме примарных циклических групп.*

Действительно, по теореме 12 из § 3, $C \cong \boldsymbol{Z}_n$, где $\boldsymbol{Z}_n$ — группа вычетов по модулю n. Пусть $n = p_1^{k_1} \ldots p_m^{k_m}$, где $p_1, \ldots, p_m$ — различные простые числа. Если $m = 1$, то C примарна. Пусть $m > 1$. Ясно, что н.о.д. $(r_1, p_m^{k_m}) = 1$, где $r = p_1^{k_1} \ldots p_{m-1}^{k_{m-1}}$. Отсюда $ur + vp_m^{k_m} = 1$ для некоторых $u, v \in \boldsymbol{Z}$ (см. примечание на с. 80). Поэтому для любого $g \in C$ имеем

$$g = u(rg) + v(p_m^{k_m})\, g \in C_1 + C_2,$$

т. е.

$$C = C_1 + C_2,$$

где $C_1 = rC$ и $C_2 = p_m^{k_m} C$. Кроме того, по теореме 22 из § 3,

$$p_m^{k_m} C_1 = |C|\, C = \{0\}$$

и

$$rC_2 = |C|\, C = \{0\}. \qquad (*)$$

Поэтому если $x \in C_1 \cap C_2$, то

$$x = u(rx) + v(p_m^{k_m} x) = 0.$$

В силу следствия теоремы 12 из § 5,

$$C = C_1 \oplus C_2.$$

Если $C_1 = \{0\}$, то $C = C_2$ и, ввиду $(*)$, $rC = \{0\}$, хотя $r[1] = [r] \neq [0]$, где $[k]$ — элемент группы вычетов $\boldsymbol{Z}_n$, содержащий число k, ибо $0 < r < n$. Следовательно, $C_1 \neq \{0\}$. Аналогично доказывается, что $C_2 \neq \{0\}$. По-

этому $|C_1|, |C_2| < |C|$, а из следствия теоремы 16 из § 5 нетрудно вывести, что C_1 и C_2 — циклические группы. Следовательно, к этим группам применимо индуктивное предположение, т. е.

$$C_1 \cong D_1' \oplus \ldots \oplus D_{l'}',$$

и

$$C_2 \cong D_1'' \oplus \ldots \oplus D_{l''}'',$$

где $D_1', \ldots, D_{l'}', D_1'', \ldots, D_{l''}''$ — примарные циклические группы. Отсюда

$$C \cong D_1' \oplus \ldots \oplus D_{l'}' \oplus D_1'' \oplus \ldots \oplus D_{l''}''$$

по теореме 13 из § 5.

Справедливость теоремы является следствием лемм 1 и 2 и теоремы 13 из § 5.

Следствие. *Если число элементов конечной абелевой группы A делится на простое число p, то A содержит подгруппу, состоящую из p элементов.*

Действительно, по теореме 6, $A \cong C_1 \oplus \ldots \oplus C_m$, где $C_1, \ldots, C_m$ — примарные циклические группы, откуда $|A| = |C_1| \ldots |C_m|$. Поэтому, например, $|C_1|$ делится на p. В силу теоремы 12 из § 3, $C_1 \cong \boldsymbol{Z}p^k$, а группа $\boldsymbol{Z}p^k$ содержит подгруппу $\{[0], [p^{k-1}], [2p^{k-1}], [(p-1)p^{k-1}]\}$, содержащую в точности p элементов.

Для установленного выше разложения конечной абелевой группы в прямую сумму примарных циклических групп имеет место теорема единственности (см. § 67 учебника А. Г. Куроша или § 5 гл. 7 учебника А. И. Кострикина). Из этой теоремы единственности следует, например, что группы 12-го порядка $A_1 = \boldsymbol{Z}_4 \oplus \boldsymbol{Z}_3$ и $A_2 = \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_3$, где $\boldsymbol{Z}_2$, $\boldsymbol{Z}_3$ и $\boldsymbol{Z}_4$ — группы вычетов по модулю 2, 3 и 4 соответственно, не изоморфны. Именно поэтому мы не ограничились установленной в лемме 1 разложимостью в прямую сумму циклических групп. Впрочем, во многих случаях неизоморфность прямых сумм можно установить и непосредственно. Например, в рассмотренной выше группе A_1 имеется элемент $a_1 = (1, 0)$ порядка 4 (т. е. $4a_1 = (0, 0)$, но $ka_1 \neq (0, 0)$, если $0 < k < 4$). Если $A_1 \cong A_2$, то найдется элемент $a_2 = (u', u'', u''')$ порядка 4. Однако $4a_2 = (0, 0, 0)$ влечет $u''' = 4u''' = 0$. Следовательно, $a_2 = (u', u'', 0)$, откуда $2a_2 = (0, 0, 0)$. В силу теоремы 22 из § 3 примарные циклические слагаемые группы порядка 12 могут иметь порядок 2, 3 или 4. Следовательно, существуют в точности две абелевых группы порядка 12.

Из теорем 4, 5 и 6, ввиду теоремы 13 из § 5, вытекает

Теорема 7. *Всякая конечно порожденная абелева группа изоморфна внешней прямой сумме примарных циклических групп и некоторого множества экземпляров группы $\boldsymbol{Z}$.*

Вернемся к рассмотрению произвольных групп. Отметим следующий интересный факт:

Теорема 8 (первая теорема Силова). *Если G — группа, p — простое число и $|G| = p^k m$, где $k \geqslant 1$, то G содержит такую подгруппу H, что $|H| = p^k$.*

Доказательство. Если $|G| = p$, то теорема тривиально справедлива. Поэтому можно предположить, что она верна для всех таких групп G', где $|G'| < |G|$, и что $|G| > 2$. Пусть $z_1, \ldots, z_s$ — все центральные элементы группы G, а $g_1, \ldots, g_t$ — представители всех остальных классов сопряженности. Применяя теорему 23 из § 3, получим

$$|K(g_i)|\,|C(g_i)| = |G|. \qquad (*)$$

Отсюда

$$|C(g_i)| = p^{k_i} m_i, \qquad (**)$$

где $0 \leqslant k_i \leqslant k$. Допустим сначала, что $k_i = k$ для некоторого i. Если $|C(g_i)| = |G|$, то $C(g_i) = G$ и g_i вопреки предположению оказывается центральным элементом. Следовательно, $|C(g_i)| < |G|$. Но тогда, в силу индуктивного предположения, группа $C(g_i)$, а значит, и группа G, содержит подгруппу, состоящую из p^k элементов. Таким образом, можно предполагать, что $k_i < k$ для всех i. Ввиду $(*)$ и $(**)$ отсюда следует, что $|K(g_i)|$ делится на p для каждого i. Далее, воспользовавшись теоремой 21 из § 3, представим G в виде объединения классов сопряженности. Поскольку $|K(z_j)| = 1$, то, обозначив через Z центр группы G, получим

$$p^k m = |G| = |Z| + |K(g_1)| + \ldots + |K(g_t)|,$$

откуда вытекает, что $|Z|$ делится на p. В силу следствия теоремы 6, Z содержит такую подгруппу U, что $|U| = p$. По теореме 20 из § 3, U — нормальная подгруппа группы G и, следовательно, существует факторгруппа G/U. По теореме 3′ из § 3

$$|G/U| = \frac{|G|}{|U|} = p^{k-1} m.$$

В силу индуктивного предположения, группа G/U содержит такую подгруппу $\overline{H}$, что $|\overline{H}| = p^{k-1}$. Обозначим через H множество всех таких элементов $h \in G$, что смежный класс $[h] = hU \in \overline{H}$. Легко проверить, что H — подгруппа группы G и что отображение $\varphi\colon H \to \overline{H}$, где $\varphi(h) = [h]$,— гомоморфное наложение групп. При этом

$\operatorname{Ker}\varphi = U$. В силу теорем 3′ и 8 из § 3.

$$|H| = |\overline{H}|\,|U| = p^{k-1}p = p^k,$$

что и требовалось.

Замечание. На первую теорему Силова можно смотреть как на частичное обращение теоремы Лагранжа (теорема 3 из § 3). Полное же обращение теоремы Лагранжа невозможно. Так, например, группа $\mathfrak{A}_4$, состоящая из 12 подстановок, не содержит подгрупп порядка 6. Другие теоремы Силова см. в § 4 гл. 7 учебника А. И. Кострикина.

Элемент группы G называется *коммутатором*, если он представим в форме $a^{-1}b^{-1}ab$, где $a, b \in G$. Множество G', состоящее из всевозможных произведений коммутаторов группы G, называется ее *коммутантом*. Ясно, что $1 \in G'$ и что произведение двух элементов из G' снова лежит в G'. Поскольку $(a^{-1}b^{-1}ab)^{-1} = b^{-1}a^{-1}ba$ и $(u_1 \ldots u_m)^{-1} = u_m^{-1} \ldots u_1^{-1}$, то $u \in G'$ влечет $u^{-1} \in G'$. Таким образом, G' — подгруппа группы G. Высшие коммутанты $G^{(i)}$ группы G определяются равенствами $G^{(2)} = (G')'$, $G^{(3)} = (G^{(2)})'$ и т. д. Так возникает ряд коммутантов:

$$G \supseteq G' \supseteq G^{(2)} \supseteq G^{(3)} \supseteq \ldots$$

Теорема 9. (1) *Все коммутанты $G^{(i)}$ являются нормальными подгруппами группы G.* (2) *Если H — подгруппа группы G, то $H^{(i)} \subseteq G^{(i)}$ для всех i.* (3) *Если H — нормальная подгруппа группы G, то $x \in G^{(i)}H$ тогда и только тогда, когда $[x] \in (G/H)^{(i)}$* (как и раньше, $[x] = xH$). (4) *Если H — нормальная подгруппа группы G, то факторгруппа G/H коммутативна в том и только том случае, когда $G' \subseteq H$.*

Доказательство. (1) Проведем индукцию по i. Положив $G^{(0)} = G$, заметим, что доказываемое утверждение справедливо при $i = 0$. Пусть $i \geqslant 1$. Как уже отмечалось, $G^{(i)}$ — подгруппа группы $G^{(i-1)}$. Если $a, b \in G^{(i-1)}$, то, в силу индуктивного предположения, $g^{-1}ag$, $g^{-1}bg \in G^{(i-1)}$ для любого $g \in G$. Отсюда

$$g^{-1}(a^{-1}b^{-1}ab)\,g = (g^{-1}a^{-1}g)(g^{-1}b^{-1}g)(g^{-1}ag)(g^{-1}bg) = (g^{-1}ag)^{-1}(g^{-1}bg)^{-1}(g^{-1}ag)(g^{-1}bg) \in (G^{(i-1)})' = G^{(i)}.$$

Если $u_1, u_2, \ldots, u_m$ — коммутаторы группы $G^{(i-1)}$, то $g^{-1}(u_1u_2 \ldots u_r)\,g = (g^{-1}u_1g)(g^{-1}u_2g) \ldots (g^{-1}u_mg) \in G^{(i)}$, поскольку, как только что показано, $g^{-1}u_kg \in G^{(i)}$ для $k = 1, \ldots, m$. Таким образом, $G^{(i)}$ — нормальная подгруппа группы G.

(2) Ясно, что $H^{(0)} = H \subseteq G = G^{(0)}$. Если доказаны включения $H^{(0)} \subseteq G^{(0)}$, $H^{(1)} \subseteq G^{(1)}$, ... $H^{(i-1)} \subseteq G^{(i-1)}$, то коммутаторы группы $H^{(i-1)}$ оказываются коммутаторами группы $G^{(i-1)}$, откуда $H^{(i)} = (H^{(i-1)})' \subseteq (G^{(i-1)})' = G^{(i)}$.

(3) Как и выше, положим $G^{(0)} = G$ и проведем индукцию по i. Справедливость доказываемого утверждения очевидна при $i = 0$. Пусть $i \geqslant 1$. Если $x = uh$, где $u \in G^{(i)}$ и $h \in H$, то $u = u_1 \ldots u_m$, где $u_k = a_k^{-1} b_k^{-1} a_k b_k$ $(k = 1, \ldots, m)$ для некоторых a_k, $b_k \in G^{(i-1)}$. Заметив, что $a_k = a_k \cdot 1$ и применив индуктивное предположение, получим $[a_k] \in (G/H)^{(i-1)}$. Аналогично $[b_k] \in (G/H)^{(i-1)}$. Отсюда

$$[u] = [u_1] \ldots [u_m] \in ((G/H)^{(i-1)})' = (G/H)^{(i)},$$

ибо $[u_k] = [a_k]^{-1} [b_k]^{-1} [a_k] [b_k]$ — коммутаторы группы $(G/H)^{(i-1)}$ и, следовательно,

$$[x] = [u] [h] = [u] \in (G/H)^{(i)}.$$

Наоборот, если $[x] \in (G/H)^{(i)}$, то $[x] = [u_1] \ldots [u_m]$, где $[u_k] = [a_k]^{-1} [b_k]^{-1} [a_k] [b_k]$ $(k = 1, \ldots, m)$ для некоторых $[a_k]$, $[b_k] \in (G/H)^{(i-1)}$. В силу индуктивного предположения, $a_k = c_k s_k$ и $b_k = d_k t_k$ для некоторых c_k, $d_k \in G^{(i-1)}$ и s_k, $t_k \in H$. Заметим, что $v_k = c_k^{-1} d_k^{-1} c_k d_k \in (G^{(i-1)})' = G^{(i)}$. С другой стороны, для некоторого $s \in H$ имеем

$$u_k = (c_k s_k)^{-1} (d_k t_k)^{-1} (c_k s_k)(d_k t_k)\, s = s_k^{-1} c_k^{-1} t_k^{-1} d_k^{-1} c_k s_k d_k t_k s.$$

Отсюда $[u_k] = [c_k]^{-1} [d_k]^{-1} [c_k] [d_k] = [v_k]$, ибо $[s_k] = [t_k] = [1]$, и, следовательно,

$$[x] = [u_1] \ldots [u_m] = [v_1] \ldots [v_m] = [v_1 \ldots v_m].$$

Таким образом, $x = v_1 \ldots v_m h$ для некоторого $h \in H$, причем $v_1 \ldots v_m \in G^{(i)}$.

(4) Если $G' \subseteq H$, то $a^{-1} b^{-1} ab \in H$ для любых a, $b \in G$, откуда $[b] [a] = [b] [a] [a^{-1} b^{-1} ab] = [a] [b]$. Наоборот, если G/H коммутативна, то $ab \in baH$. Отсюда $a^{-1} b^{-1} ab \in H$. Следовательно, H содержит все коммутаторы, а значит, $G' \subseteq H$.

Группа G называется *разрешимой*, если ряд ее коммутантов обрывается на конечном шаге, т. е. $G^{(m)} = \{1\}$ для некоторого m.

Название объясняется связью разрешимых групп с возможностью выразить корни многочлена через радикалы (см., например, Скорняков Л. А. Элементы общей алгебры.— М.: Наука, 1983, гл. VI, § 2, или Постников М. М. Теория Галуа.— М.:

Физматгиз, 1963, с. 89—90). Разрешимой является всякая коммутативная группа. Некоммутативной разрешимой группой оказывается, например, $\mathfrak{S}_3$. Действительно, поскольку группа $\mathfrak{S}_3$ не коммутативна, а факторгруппа $\mathfrak{S}_3/\mathfrak{A}_3$ коммутативна, то $|\mathfrak{S}_3'| \neq 1$ и, в силу теоремы 9 (4) $\mathfrak{S}_3' \subseteq \mathfrak{A}_3$. Но $|\mathfrak{A}_3| = 3$ и, значит, $\mathfrak{S}_3' = \mathfrak{A}_3$ по теореме Лагранжа (теорема 3 из § 3). Наконец, $\mathfrak{A}_3' = \{1\}$, т. е. $\mathfrak{S}_3^{(2)} = \{1\}$. Разрешимость группы $\mathfrak{S}_3$ вытекает также из доказываемой далее теоремы 12. Другие примеры доставляют теоремы 11 и 13.

Т е о р е м а 10. *Пусть G — конечная группа и H — ее подгруппа. Тогда*: (1) *если G разрешима, то H разрешима*; (2) *если G разрешима и H нормальна, то G/H разрешима*; (3) *если H нормальна и разрешима, а G/H разрешима, то G разрешима.*

Д о к а з а т е л ь с т в о. (1) Если $G^{(m)} = \{1\}$, то $H^{(m)} = \{1\}$ по теореме 9 (2).

(2) По условию, $G^{(m)} = \{1\}$ для некоторого m. Поэтому, если $[x] \in (G/H)^{(m)}$, то, по теореме 9 (3), $x \in G^{(m)}H = H$, т. е. $[x] = [0]$. Таким образом, $(G/H)^{(m)} = \{[1]\}$.

(3) Допустим, что $(G/H)^{(k)} = \{[1]\}$ и $H^{(l)} = \{1\}$. Если $y \in G^{(k)}$, т. е. $y = y \cdot 1$, где $1 \in H$, то по теореме 9(3), $[y] \in (G/H)^{(k)}$. Следовательно, $[y]=[1]$, т. е. $y \in H$. Таким образом, $G^{(k)} \subseteq H$, откуда

$$G^{(k+l)} = (G^{(k)})^{(l)} \subseteq H^{(l)} = \{1\}$$

по теореме 9 (2).

Т е о р е м а 11. *Если G — группа и $|G| = p^k$, где p — простое число и $k \geqslant 1$, то G разрешима.*

Д о к а з а т е л ь с т в о. Если $k = 1$, то G, будучи абелевой группой, разрешима. То же самое можно сказать, если G совпадает со своим центром Z. Поэтому, учитывая теоремы 3, 20 и 24 из § 3, при $k > 1$ можно предполагать, что $|Z| = p^l$, где $0 < l < k$. Теорема 20 из § 3 позволяет рассмотреть факторгруппу G/Z, причем $|G/Z| = p^{k-l} < p^k$ в силу теоремы 3′ из § 3. По индуктивному предположению, группа G/Z разрешима. Поскольку группа Z коммутативна, разрешимость группы G вытекает из теоремы 10(3).

Т е о р е м а 12. *Если G — группа и $|G| = pq$, где p и q — простые числа, то G разрешима.*

Д о к а з а т е л ь с т в о. Ввиду теоремы 11, можно считать, что $p \neq q$. По теореме 8, G содержит такие подгруппы A и B, что $|A| = p$ и $|B| = q$. Теоремы 1 и 3 из § 3 позволяют заключить, что

$$A \cap B = \{1\}. \qquad (*)$$

Рассмотрим множество

$$H = \{ab \mid a \in A,\ b \in B\}.$$

Если $a_1, a_2 \in A$, $b_1, b_2 \in B$ и $a_1 b_1 = a_2 b_2$, то

$$a_2^{-1} a_1 = b_2 b_1^{-1} \in A \cap B = \{1\},$$

откуда $a_1 = a_2$ и $b_1 = b_2$. Следовательно, $|H| = pq$ и, значит, $H = G$. Рассмотрим множество

$$C = \{x \mid x \in A,\ x^{-1} b x \in B \text{ для всех } b \in B\}.$$

Нетрудно проверить, что C — подгруппа группы A. По теореме 3 из § 3, $C = \{1\}$ или $C = A$. Допустим сначала, что $C = A$. Если $g \in G$, то, поскольку $G = H$, имеем $g = ab_1$, где $a \in A$ и $b_1 \in B$. Поэтому для любого $b \in B$ получаем

$$g^{-1} b g = b_1^{-1} (a^{-1} b a) b_1 \in B,$$

т. е. подгруппа B оказывается нормальной. Следовательно, рассмотрев факторгруппу G/B и заметив, что, ввиду теоремы 3′ из § 3, равенства $|G/B| = p$ и $|B| = q$ обеспечивают коммутативность групп G/B и B, получаем, что группа G разрешима по теореме 10 (3). Обратимся к случаю, когда $C = \{1\}$. Если $a \in A$, то, как легко проверить, множество $B_a = a^{-1} B a$ оказывается подгруппой группы G, причем $|B_a| = q$. Поэтому, допустив, что $a_1, a_2 \in A$ и $|B_{a_1} \cap B_{a_2}| > 1$, и принимая во внимание теоремы 1 и 3 из § 3, получим, что $|B_{a_1} \cap B_{a_2}| = q$, т. е. $B_{a_1} = B_{a_2}$. Если теперь $b \in B$, то $a_1^{-1} b a_1 = a_2^{-1} b' a_2$ для некоторого $b' \in B$, откуда

$$(a_1 a_2^{-1})^{-1} b (a_1 a_2^{-1}) = b' \in B.$$

Ввиду произвольности выбора элемента b, получаем, что

$$a_1 a_2^{-1} \in C = \{1\},$$

т. е. $a_1 = a_2$. Таким образом, если $A = \{a_1, a_2, \ldots, a_p\}$ и $B_i = a_i^{-1} B a_i$, то $B_i \cap B_j = \{1\}$ при $i \neq j$, а, ввиду теоремы 3 из § 3, $A \cap B_i = \{1\}$ для всех i. Следовательно, $|A \cup B_1 \cup \ldots \cup B_p| = (p-1) + p(q-1) + 1 = pq$, т. е.

$$A \cup B_1 \cup \ldots \cup B_p = G.$$

Если теперь $g \in G$, то $g^{-1} A g$ — подгруппа и $|g^{-1} A g| = p$. Поэтому $(g^{-1} A g) \cap B_i = \{1\}$ для всех i, откуда $g^{-1} A g \subseteq A$. Этим доказана нормальность подгруппы A.

Как и выше, применив к G/A и A теорему 10(3), убедимся в разрешимости группы G.

Замечание. Существенным обобщением теорем 11 и 12 является теорема 3 из § 2 гл. IV.

Пример бесконечной некоммутативной разрешимой группы доставляет следующий результат.

Теорема 13. *Совокупность G всех матриц вида*

$$\begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{Vmatrix}$$

над произвольным полем P, где $a_{11}, a_{22}, \dots, a_{nn} \neq 0$, является разрешимой группой.

Доказательство. Непосредственный подсчет показывает, что G — группа. Непосредственным же подсчетом проверяется

Лемма 1. *Если A и U — матрицы порядка k, D и Z — матрицы порядка l, C и V — матрицы размера $k \times l$ и D и W — матрицы размера $l \times k$, то*

$$\begin{Vmatrix} A & C \\ B & D \end{Vmatrix} \begin{Vmatrix} U & V \\ W & Z \end{Vmatrix} = \begin{Vmatrix} AU + CW & AV + CZ \\ BU + DW & BV + DZ \end{Vmatrix}.$$

Из леммы 1 вытекает

Лемма 2.

$$\begin{Vmatrix} E & C \\ O & E \end{Vmatrix} \begin{Vmatrix} E & V \\ O & E \end{Vmatrix} = \begin{Vmatrix} E & C+V \\ O & E \end{Vmatrix}.$$

Лемма 3. *Совокупность T_n всех таких матриц из G, что $a_{11} = a_{22} = \dots = a_{nn} = 1$, является разрешимой группой.*

Для доказательства сначала простым подсчетом убедимся, что H — подгруппа в G. Далее заметим, что $T_1 = \{1\}$. Это позволяет вести индукцию по n. Если $n \geqslant 2$, то рассмотрим отображение φ: $T_n \to T_{n-1}$, где

$$\varphi\left(\left\|\begin{array}{c|c} A & c \\ \hline 0 & 1 \end{array}\right\|\right) = A$$

(здесь 0 — $(n-1)$-мерная нулевая строка, а c — $(n-1)$-мерный столбец). Учитывая лемму 1, нетрудно проверить, что φ — гомоморфное наложение. Ясно также, что

Ker φ состоит из всех матриц вида

$$\left\|\begin{array}{c|c} E & c \\ \hline 0 & 1 \end{array}\right\|.$$

Поскольку T_{n-1} разрешима по индуктивному предположению, а из леммы 2 нетрудно вывести, что Ker φ — коммутативная группа, то разрешимость группы G вытекает из теоремы 10 (3).

Лемма 4. $G' \subseteq T_n$.

Действительно, при $n = 1$ это очевидно. Если же $n \geqslant 2$, то, используя лемму 1, получаем

$$\left\|\begin{array}{c|c} A^{-1} & c \\ \hline 0 & \alpha^{-1} \end{array}\right\| \left\|\begin{array}{c|c} B^{-1} & d \\ \hline 0 & \beta^{-1} \end{array}\right\| \left\|\begin{array}{c|c} A & c \\ \hline 0 & \alpha \end{array}\right\| \left\|\begin{array}{c|c} B & d \\ \hline 0 & \beta \end{array}\right\| = \left\|\begin{array}{c|c} A^{-1}B^{-1}AB & u \\ \hline 0 & 1 \end{array}\right\| \in T_n,$$

ибо $A^{-1}B^{-1}AB \in T_{n-1}$ по индуктивному предположению.

Возвращаясь к доказательству теоремы, заметим, что факторгруппа G/G' коммутативна по теореме 9(4), а разрешимость группы вытекает из леммы 3 и теоремы 10(1). Остается принять во внимание теорему 10(3).

Чтобы установить существование неразрешимых групп, заметим, что неразрешима всякая некоммутативная *простая группа*, т. е. неединичная группа, не содержащая нормальных подгрупп, отличных от $\{1\}$ и всей группы. Действительно, если G — простая группа, то $G' = \{1\}$ или G. В первом случае G коммутативна по теореме 9 (4), а во втором $\{1\} \neq G = G' = G'' = \ldots$ Таким образом, поставленную задачу решает

Теорема 14. *Знакопеременная группа $\mathfrak{A}_5$ проста и некоммутативна.*

Доказательство. Сначала установим три леммы.

Лемма 1. *Если подгруппа H группы $\mathfrak{A}_5$ содержит все циклы длины* 3, *то $H = \mathfrak{A}_5$.*

В самом деле, для произведения двух транспозиций имеем

$$(ij)\,(il) = (ijl)$$

и

$$(ij)\,(kl) = (ijk)\,(ilk),$$

где i, j, k и l — различные числа. Следовательно, всякий элемент из $\mathfrak{A}_5$, будучи, согласно теореме 18 из § 3, представимым в виде произведения четного числа транспозиций, представим и в виде произведения циклов длины 3, а следовательно, принадлежит H.

Лемма 2. *Если нормальная подгруппа H группы $\mathfrak{A}_5$ содержит хотя бы один цикл длины* 3, *то* $H = \mathfrak{A}_5$.

Для доказательства, согласно лемме 1, достаточно установить, что H содержит все циклы длины 3. Допустим, что $(ijk) \in H$, а (pqr) — произвольный цикл длины 3. В силу теоремы I.2.8 *), одна из подстановок

$$\begin{pmatrix} i & j & k & s & t \\ p & q & r & u & v \end{pmatrix} \text{ и } \begin{pmatrix} i & j & k & s & t \\ p & q & r & v & u \end{pmatrix},$$

где

$$\{i, j, k, s, t\} = \{p, q, r, u, v\} = \{1, 2, 3, 4, 5\},$$

четная. Обозначим ее через σ. Если σ — первая из выписанных подстановок, то для $\tau = \sigma^{-1}(ijk)\,\sigma$ из равенств $\tau(p) = q$, $\tau(q) = r$, $\tau(r) = p$, $\tau(u) = u$ и $\tau(v) = v$ вытекает, что $\tau = (pqr)$. Но $\tau = \sigma^{-1}(ijk)\,\sigma \in H$. Аналогично рассматривается второй случай.

Лемма 3. *Если нормальная подгруппа H группы $\mathfrak{A}_5$ содержит хотя бы один цикл длины* 5, *то* $H = \mathfrak{A}_5$.

В самом деле, допустим, что $(ijklm) \in H$. Поскольку $(ikj) = (ik)\,(ij) \in \mathfrak{A}_5$, то

$$(ijl) = (imlkj)\,(ikj)\,(ijklm)\,(ijk) = \\ = (ijklm)^{-1}\,(ijk)^{-1}\,(ijklm)\,(ijk) \in H$$

и $H = \mathfrak{A}_5$ по лемме 2.

Возвращаясь к доказательству теоремы, допустим, что нормальная подгруппа H группы $\mathfrak{A}_5$ отлична от $\mathfrak{A}_5$ и содержит нетождественную подстановку σ. Согласно теореме 16 из § 3, σ представляется как произведение циклов, причем, в силу лемм 2 и 3, σ не может быть циклом длины 3 или 5. Следовательно, $\sigma = (ij)\,(kl)$, или $\sigma = (ij)$ или $\sigma = (ijk)\,(lm) = (ij)\,(ik)\,(lm)$, или $\sigma = (ijkl) = (ij)\,(ik)\,(il)$. Но во всех случаях, кроме первого, $\sigma \notin \mathfrak{A}_5$ в силу теоремы I.3.18. В первом же случае, имея $\{i, j, k, l, m\} = \{1, 2, 3, 4, 5\}$, и учитывая, что

$$(ijm)^{-1}\sigma\,(ijm) = (imj)\,(ij)\,(kl)\,(ijm) = (jm)\,(kl) \in H,$$

получим

$$(imj) = (ij)\,(kl)\,(jm)\,(kl) \in H,$$

вопреки лемме 2. Некоммутативность группы $\mathfrak{A}_5$ видна из соотношений

$$((1\,2)(3\,4))((1\,3)(2\,5)) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix} = \\ = ((1\,3)(2\,5))((1\,2)(3\,4)).$$

*) См. примечание на с. 49.

В качестве примера бесконечной простой группы укажем группу $SO(3)$, состоящую из всех ортогональных матриц порядка 3 с определителем, равным 1. Правда, соответствующее доказательство нуждается в сведениях о линейных пространствах, выходящих за рамки изложенного в следующей главе. Для доказательства напомним, что если $A \in SO(3)$, то существует такая ортогональная матрица U, что

$$U^{-1}AU = T(\varphi), \qquad (*)$$

где

$$T(\varphi) = \begin{Vmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{Vmatrix}$$

(см. например: Кострикин А. И., Манин Ю. И. Линейная алгебра и геометрия.— М.: Наука, 1986, с. 136, теорема 4б); с. 32, п. 8в)). Поскольку $|-U| = -|U|$, то можно считать, что в равенстве $(*)$ имеем $U \in SO(3)$. Допустим, что H — неодноэлементная нормальная подгруппа группы $SO(3)$. Тогда найдется неединичная матрица $A \in H$. В силу сделанного замечания, из формулы $(*)$ вытекает, что для некоторого $\varphi_0 \neq 2\pi k$ имеем $T(\varphi_0) \in H$. Положим $s = \sin\varphi_0$, $c = \cos\varphi_0$ и

$$B(a) = \begin{Vmatrix} a & -b & 0 \\ b & a & 0 \\ 0 & 0 & 1 \end{Vmatrix},$$

где a — любое число из отрезка $[0, 1]$, а $b = \sqrt{1-a^2}$. Ясно, что $B(a) \in SO(3)$, откуда $D(a) = (B(a)^{-1}T(\varphi_0)^{-1}B(a))T(\varphi_0) \in H$. Заметив, что $T(\varphi_0)^{-1} = T(-\varphi_0)$, а

$$B(a)^{-1} = \begin{Vmatrix} a & b & 0 \\ -b & a & 0 \\ 0 & 0 & 1 \end{Vmatrix},$$

будем иметь

$$D(a) = \begin{Vmatrix} a & b & 0 \\ -b & a & 0 \\ 0 & 0 & 1 \end{Vmatrix} \begin{Vmatrix} 1 & 0 & 0 \\ 0 & c & s \\ 0 & -s & c \end{Vmatrix} \begin{Vmatrix} a & -b & 0 \\ b & a & 0 \\ 0 & 0 & 1 \end{Vmatrix} \begin{Vmatrix} 1 & 0 & 0 \\ 0 & c & -s \\ 0 & s & c \end{Vmatrix} =$$

$$= \begin{Vmatrix} a & bc & bs \\ -b & ac & as \\ 0 & -s & c \end{Vmatrix} \begin{Vmatrix} a & -bc & bs \\ b & ac & -as \\ 0 & s & c \end{Vmatrix}.$$

Вычислим след $\mathrm{Tr}(D(a))$ матрицы $D(a)$ (см. цитированную выше книгу А. И. Кострикина и Ю. И. Манина, с. 33, п. 9):

$$\mathrm{Tr}(D(a)) = a^2 + b^2c + b^2c + a^2c^2 + as^2 + as^2 + c^2 =$$
$$= a^2 + 2(1-a^2)c + a^2c^2 + 2a(1-c^2) + c^2 =$$
$$= a^2(1-c)^2 + 2a(1-c^2) + 2c + c^2.$$

Как уже отмечалось, для подходящей матрицы $V \in SO(3)$ имеем

$$V^{-1}D(a)V = T(\varphi(a)).$$

Учитывая инвариантность следа при изменении базы (см. цитированную выше книгу А. И. Кострикина и Ю. И.Манина, с. 33, п. 9),

получаем

$$\cos \varphi (a) = \frac{\operatorname{Tr}(T(\varphi(a))) - 1}{2} = \frac{\operatorname{Tr}(D(a)) - 1}{2} =$$

$$= \frac{a^2(1-c)^2 + 2a(1-c^2) + (2c + c^2 - 1)}{2}.$$

Поскольку

$$\cos \varphi (1) = 1$$

и

$$\left.\frac{d \cos(\varphi(a))}{da}\right|_{a=1} = \left.\frac{2a(1-c)^2 + 2(1-c^2)}{2}\right|_{a=1} = 2(1-c) > 0,$$

то найдется такое число $\delta > 0$, что $\cos \varphi (a) \neq 0$ для всех $a \in [1 - \delta, 1]$. В силу непрерывности функции $\cos \varphi (a)$ ее значения заполняют весь отрезок $[\cos \varphi (1 - \delta), 1]$. Но тогда углы $\varphi (a)$ заполняют отрезок $[0, \varepsilon]$ для некоторого $\varepsilon > 0$. Следовательно, найдется такое целое положительное число n, что $0 < \psi < 2\pi/n$ влечет $T(\psi) \in H$. Поэтому если B — произвольная матрица из $SO(3)$ и $W^{-1}BW = T(\varphi)$, где $W \in SO(3)$, то $T(\varphi/n) \in H$, откуда

$$B = WT(\varphi)\ W^{-1} = W(T(\varphi/n))^n W^{-1} \in H.$$

Упражнения

1. Сколько существует неизоморфных абелевых групп порядков 10, 18, 24 и 105?
2. Для каких чисел n все абелевы группы порядка n циклические? (Разумеется, все эти группы изоморфны между собой.)
3. Прямая сумма двух конечных циклических групп является циклической группой тогда и только тогда, когда порядки слагаемых взаимно просты.
4. Свободная абелева группа является циклической тогда и только тогда, когда она изоморфна Z.
5. Все базы свободной абелевой группы содержат одно и то же число элементов.
6. Если G и H — разрешимые группы, то и группа $G \times H$ разрешима.
7. Доказать, что группа $\mathfrak{S}_5$ неразрешима.
8. Пусть R — кольцо с единицей, I — идеал кольца R и произведение любых n элементов из I равно нулю (другими словами, идеал I нильпотентен). Доказать, что множество всех элементов вида $1 + x$, где $x \in I$, является разрешимой группой по умножению. Используя этот результат, получить новое доказательство теоремы 13.
9. Если центр группы порядка pqr, где p, q и r — простые числа, неодноэлементный, то эта группа разрешима.
10. Знакопеременная группа $\mathfrak{A}_n$ проста тогда и только тогда, когда $n \geqslant 5$.

§ 8. Структуры и булевы алгебры

Пусть P — произвольное непустое множество. *Отношением* на множестве P называется подмножество ρ прямого произведения $P \times P$. Вместо $(a, b) \in \rho$ часто пишет-

Таблица 5

	Множество P	Отношение ρ
1	Произвольное	$(a, b) \in \rho$, если $a = b$
2	Произвольное	$(a, b) \in \rho$, если a и b лежат в одном смежном классе данного разбиения Σ множества P
3	Целые числа	$(m, n) \in \rho$, если $m \leqslant n$
4	Целые числа	$(m, n) \in \rho$, если m делит n (считается, что 0 делит 0)
5	Неотрицательные целые числа	$(m, n) \in \rho$, если m делит n
6	Все подмножества данного множества	$(A, B) \in \rho$, если $A \subseteq B$
7	Все подмножества данного множества	$(A, B) \in \rho$, если $A \cap B$ непусто
8	Множество действительных функций	$(f, g) \in \rho$, если $f(x) \leqslant g(x)$ для всех x
9	Множество действительных функций	$(f, g) \in \rho$, если $f(x) \leqslant g(x)$ для некоторого x
10	Множество точек плоскости	$(M, N) \in \rho$, если $M = N$ или прямая MN параллельна оси x
11	Множество точек плоскости	$(M, N) \in \rho$, если $M = N$ или прямая MN перпендикулярна оси x и точка M расположена ниже точки N

ся $a\rho b$. Примеры отношений приведены в таблице 5. Отношение $\leqslant$ на множестве P называется *порядком*, если

(1) $a \leqslant a$ для всех $a \in P$ (рефлексивность);

(2) если $a \leqslant b$ и $b \leqslant c$, то $a \leqslant c$ (транзитивность);

(3) если $a \leqslant b$ и $b \leqslant a$, то $a = b$ (антисимметричность).

Порядком являются отношения в примерах 1, 3, 5, 6, 8 и 11 (см. таблицу 5). Отношение ρ примера 4 порядком не является, поскольку, например $3 \neq -3$, хотя $(3, -3)$ и $(-3, 3)$ принадлежат ρ, т. е. для этого отношения не выполнено свойство (3). Свойство (3) не имеет места и для отношений из примеров 2 и 10. Отношения примеров 7 (если множество содержит не менее двух элементов) и 9 также не являются порядком, ибо для них не выполнено свойство транзитивности. Порядок, указанный в примере 1, называется *тривиальным*.

Множество P называется *частично упорядоченным*, если оно непусто и на нем зафиксирован некоторый порядок. Разумеется, на одном и том же множестве можно за-

фиксировать различные порядки. Возникающие при этом частично упорядоченные множества считаются различными (например, множество неотрицательных целых чисел с порядками, описанными в примерах 3 и 5 из таблицы 5). Множество с тривиальным порядком называется *тривиальным частично упорядоченным множеством*. Всякое подмножество частично упорядоченного множества является частично упорядоченным множеством относительно того же порядка.

Частично упорядоченные множества P и P' называются *изоморфными*, если существует взаимно однозначное отображение φ множества P на множество P' такое, что $a \leqslant b$ имеет место тогда и только тогда, когда $\varphi(a) \leqslant \varphi(b)$ *). Отображение φ частично упорядоченного множества P в частично упорядоченное множество P' называется *изотонным*, если $a \leqslant b$ влечет $\varphi(a) \leqslant \varphi(b)$.

Элементы a и b частично упорядоченного множества называются *сравнимыми*, если имеет место $a \leqslant b$ или $b \leqslant a$. Два элемента тривиального частично упорядоченного множества, очевидно, сравнимы тогда и только тогда, когда они совпадают.

Если любые два элемента частично упорядоченного множества сравнимы, то оно называется *цепью* (или *линейно упорядоченным множеством*). Цепью является, например, частично упорядоченное множество примера 3 из таблицы 5. Элемент v частично упорядоченного множества P называется *наибольшим*, если $x \leqslant v$ для всех $x \in P$. Если же $u \leqslant x$ для всех $x \in P$, то элемент u называется *наименьшим*. Наибольший элемент часто называют *единицей*, а наименьший — *нулем*. Конечно, частично упорядоченное множество может не содержать ни нуля, ни единицы. Таким, в частности, будет неодноэлементное тривиальное частично упорядоченное множество. Однако более одного наибольшего элемента частично упорядоченное множество содержать не может. В самом деле, если v и v' — наибольшие элементы частично упорядоченного множества P, то $v \leqslant v'$ и $v' \leqslant v$, а, следовательно, $v = v'$ по свойству антисимметричности. Аналогично устанавливается единственность наименьшего элемента. Элемент w частично упорядоченного множества P называется *максимальным*, если из $w \leqslant x$ для некоторого $x \in P$ вытекает $x = w$. Если из $x \leqslant m$ для некоторого $x \in P$ следует, что $x = m$, то m называется *минимальным* эле-

*) См. примечание на с. 60.

ментом. Легко проверяется, что всякий наибольший элемент является максимальным, а всякий наименьший элемент — минимальным. Обратное, вообще говоря, места не имеет. Так, например, в тривиальном частично упорядоченном множестве всякий элемент является как максимальным, так и минимальным. Другой пример минимальных, но не наименьших элементов дают простые числа в множестве целых положительных чисел, отличных от 1, упорядоченном по делимости (см. пример 5 из таблицы 5). Наибольшим и наименьшим элементами в частично упорядоченном множестве подмножеств (пример 6 из таблицы 5) являются все данное множество и пустое подмножество соответственно. Частично упорядоченные множества примеров 3 и 11 из таблицы 5 ни наибольшего, ни наименьшего элементов не содержат.

Заметим, что определение наименьшего элемента получается из определения наибольшего элемента простой заменой символа $\leqslant$ на символ $\geqslant$. Точно таким же образом связаны понятия минимального и максимального элементов. Вообще, имея какое-либо высказывание о частично упорядоченном множестве и заменяя $\leqslant$ на $\geqslant$, получаем новое высказывание. Высказывания, связанные таким образом, называются *двойственными*.

Если A — непустое подмножество частично упорядоченного множества P, то *верхним* (*нижним*) *конусом* множества A назовем множество всех таких элементов $x \in P$, что $a \leqslant x$ ($x \leqslant a$) для всех $a \in A$. Верхний и нижний конусы множества A будем обозначать символами $A^{\triangle}$ и $A^{\triangledown}$ соответственно. Наименьший (наибольший) элемент верхнего (нижнего) конуса множества A (если он существует) называется *точной верхней* (*нижней*) *гранью* множества A. Точную верхнюю (нижнюю) грань множества A в частично упорядоченном множестве P будем обозначать $\sup_P A$ ($\inf_P A$). Впрочем, индекс P часто будет опускаться. Подчеркнем, что $\sup_P A$ и $\inf_P A$ — однозначно определенные элементы множества P, ибо, как было отмечено на с. 149, $A^{\triangle}$ ($A^{\triangledown}$) содержит не более одного наименьшего (наибольшего) элемента.

Примеры. 1. Если P — частично упорядоченное множество неотрицательных целых чисел, упорядоченных по делимости (пример 5 из таблицы 5), то

$\{18, 12\}^{\triangle}$=\{множество всех чисел из P, делящихся на 18 и 12 одновременно\}=$\{36n,\ n = 0, 1, 2, \ldots\}$,

$\{18, 12\}^{\triangledown}$=\{множество всех чисел из P, делящих 18 и 12 одновременно\}=$\{1, 2, 3, 6\}$,

$\sup\{18, 12\}=36$ и $\inf\{18, 12\} = 6$.

2. Если P — частично упорядоченное множество функций (пример 8 из таблицы 5), то верхний конус $\{\sin x, \cos x\}^{\triangle}$ — это все функции, графики которых лежат в горизонтально заштрихованной области на рис. 5. Графики функций, входящих в нижний конус

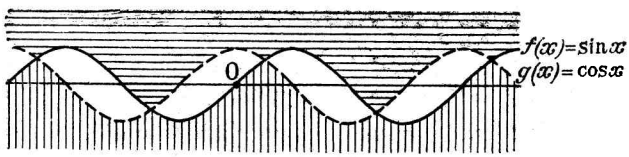


Рис. 5

$\{\sin x, \cos x\}^{\triangledown}$, лежат в области с вертикальной штриховкой на том же рисунке. Точные грани $\sup\{\sin x, \cos x\}$ и $\inf\{\sin x, \cos x\}$ изображены на рис. 6 и 7 соответственно.

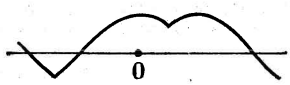


Рис. 6

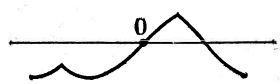


Рис. 7

3. В частично упорядоченном множестве подмножеств (пример 6 из таблицы 5) точная верхняя (нижняя) грань совпадает с объединением (пересечением) подмножеств.

Частично упорядоченное множество P называется *нижней (верхней) полуструктурой*, если каждое двухэлементное его подмножество имеет точную нижнюю (верхнюю) грань. Если частично упорядоченное множество является нижней и верхней полуструктурой одновременно, то оно называется *структурой* *). Частично упорядоченные множества примеров 3, 5, 6 и 8 из таблицы 5 оказываются структурами. Структурой оказывается и всякая цепь, ибо если, например, $a \leqslant b$, то $\sup\{a, b\} = b$ и и $\inf\{a, b\} = a$. Напротив, в примере 11 мы имеем частично упорядоченное множество, не являющееся ни нижней, ни верхней полуструктурой. Действительно, верхний (нижний) конус любой пары точек, не расположенных одна под другой, пуст.

Полуструктуры тесно связаны с коммутативными полугруппами, все элементы которых идемпотентны.

Т е о р е м а 1. *Пусть P — коммутативная полугруппа, причем $a^2 = a$ для любого $a \in P$. Определим от-*

*) Широко распространен также термин «*решетка*».

ношения

$$a \leqslant b, \text{ если } a = ab,$$

и

$$a \trianglelefteqslant b, \text{ если } b = ab.$$

Тогда каждое из этих отношений оказывается порядком и множество P с порядком $\leqslant$ (с порядком $\trianglelefteqslant$) оказывается нижней (верхней) полуструктурой, причем

$$\inf\{a, b\} = ab \qquad (\sup\{a, b\} = ab).$$

Доказательство. Рефлексивность обоих отношений вытекает из равенства $a^2 = a$. Если $a \leqslant b$ и $b \leqslant c$ ($a \trianglelefteqslant b$ и $b \trianglelefteqslant c$), то $a = ab$ и $b = bc$ ($b = ab$ и $c = bc$). Учитывая ассоциативность умножения, получаем

$$a = ab = a(bc) = (ab)c = ac$$
$$(c = bc = (ab)c = a(bc) = ac),$$

т. е. $a \leqslant c$ ($a \trianglelefteqslant c$). Таким образом, оба отношения транзитивны. Если $a \leqslant b$ и $b \leqslant a$ ($a \trianglelefteqslant b$ и $b \trianglelefteqslant a$), то $a = ab$ и $b = ba$ ($b = ab$ и $a = ba$), откуда $a = b$ в силу коммутативности умножения. Таким образом, $\leqslant$ и $\trianglelefteqslant$ — порядки. Из равенств $(ab)\,a = a\,(ab) = a^2b = ab$ и $(ab)\,b = ab^2 = ab$ вытекает, что $ab \in \{a, b\}^{\triangledown}$ относительно порядка $\leqslant$. Если $x \in \{a, b\}^{\triangledown}$, то $x \leqslant a$ и $x \leqslant b$, т. е. $x = xa$ и $x = xb$. Отсюда

$$x(ab) = (xa)\,b = xb = x,$$

т. е. $x \leqslant ab$. Следовательно, ab — наибольший элемент нижнего конуса $\{a, b\}^{\triangledown}$, т. е. $ab = \inf\{a, b\}$. Чтобы доказать, что $ab \in \{a, b\}^{\triangle}$ относительно порядка $\trianglelefteqslant$, обратим внимание на равенства $a\,(ab) = a^2b = ab$ и $b\,(ab) = (ba)\,b = (ab)\,b = ab^2 = ab$, откуда $a \trianglelefteqslant ab$ и $b \trianglelefteqslant ab$. Кроме того, если $x \in \{a, b\}^{\triangle}$, то $a \trianglelefteqslant x$ и $b \trianglelefteqslant x$, т. е. $x = ax$ и $x = bx$. Отсюда

$$(ab)\,x = a\,(bx) = ax = x,$$

т. е. $ab \trianglelefteqslant x$. Следовательно, ab — наименьший элемент верхнего конуса $\{a, b\}^{\triangle}$ относительно порядка $\trianglelefteqslant$, т. е. $ab = \sup\{a, b\}$.

Теорема 2. *Если L — структура, то полагая*

$$a + b = \sup\{a, b\},$$
$$ab = \inf\{a, b\},$$

имеем:

(1)	$(a + b) + c = a + (b + c)$;	(1′)	$(ab)\,c = a\,(bc)$;
(2)	$a + b = b + a$;	(2′)	$ab = ba$;
(3)	$a + a = a$;	(3′)	$aa = a$;
(4)	$(a + b)\,a = a$;	(4′)	$ab + a = a$.

Доказательство. Как было отмечено на с. 150, $a + b$ и ab — однозначно определенные элементы множества L. Другими словами, $+$ и $\cdot$ — операции на множестве L. Свойства (2) и (2′) очевидны. Для доказательства свойств (3) и (3′) достаточно заметить, что $\{a, a\}^{\triangle} = a^{\triangle}$ и $\{a, a\}^{\triangledown} = a^{\triangledown}$. Для доказательства свойства (1) положим $a + b = s$, $b + c = t$, $s + c = u$ и $a + t = v$. Тогда $s \leqslant u$ и $c \leqslant u$, ибо $u \in \{s, c\}^{\triangle}$. Кроме того, $a \leqslant s$ и $b \leqslant s$, поскольку $s \in \{a, b\}^{\triangle}$. Учитывая транзитивность порядка, имеем $a \leqslant u$, $b \leqslant u$ и $c \leqslant u$, т. е. $u \in \{a, b, c\}^{\triangle}$. Если $x \in \{a, b, c\}^{\triangle}$, то $a \leqslant x$, $b \leqslant x$ и $c \leqslant x$ и, в частности, $x \in \{a, b\}^{\triangle}$. Поскольку s — наименьший элемент верхнего конуса $\{a, b\}^{\triangle}$, то $s \leqslant x$. Вместе с $c \leqslant x$ это дает, что $x \in \{s, c\}^{\triangle}$. Но u — наименьший элемент верхнего конуса $\{s, c\}^{\triangle}$ и, следовательно, $u \leqslant x$. Этим доказано, что u — наименьший элемент верхнего конуса $\{a, b, c\}^{\triangle}$. С другой стороны, из неравенств $a \leqslant v$, $b \leqslant t \leqslant v$ и $c \leqslant t \leqslant v$ вытекает, что $v \in \{a, b, c\}^{\triangle}$. Если же $x \in \{a, b, c\}^{\triangle}$, то $a \leqslant x$, $b \leqslant x$ и $c \leqslant x$. Отсюда $x \in \{b, c\}^{\triangle}$, а значит, $t \leqslant x$. Вместе с $a \leqslant x$ это дает, что $x \in \{a, t\}^{\triangle}$, а значит, $v \leqslant x$. Следовательно, v — наименьший элемент верхнего конуса $\{a, b, c\}^{\triangle}$. Поскольку u — также наименьший элемент этого верхнего конуса, то, как отмечалось на с. 149, $u = v$. Тем самым доказана справедливость свойства (1). Свойство (1′) доказывается двойственным рассуждением (т. е. вместо верхних конусов следует рассматривать нижние). Переходя к доказательству свойства (4), заметим, что $a \leqslant a + b$ и, следовательно, $a \in \{a, a + b\}^{\triangledown}$. Но если $x \in \{a, a + b\}^{\triangledown}$, то $x \leqslant a$, т. е. a — наибольший элемент нижнего конуса $\{a, a + b\}^{\triangledown}$ и по определению $a = (a + b)\,a$. Двойственным рассуждением устанавливается свойство (4′).

Замечание. Проанализировав доказательство теоремы 2, нетрудно понять, что свойства (1)—(3) ((1′)—(3′)) остаются справедливыми для любой верхней (нижней) полуструктуры.

Из свойств (1), (2), (1′) и (2′) видно, что структура является коммутативной полугруппой как относительно операции $+$, так и относительно операции $\cdot$.

Теорема 2 допускает следующее обращение.

Теорема 3. *Всякое множество P с двумя операциями $+$ и $\cdot$, обладающими свойствами* (1)—(4) *и* (1′)—(4′), *можно превратить в структуру, положив*

$$a \leqslant b, \text{ если } a = ab.$$

При этом

$$ab = \inf \{a, b\},$$
$$a + b = \sup \{a, b\}$$

и неравенство $a \leqslant b$ имеет место тогда и только тогда, когда $a + b = b$.

Доказательство. В силу теоремы 1, P — частично упорядоченное множество, причем $ab = \inf \{a, b\}$. Ввиду $a(a + b) = a$ и

$$b(a + b) = b(b + a) = b$$

имеем $a + b \in \{a, b\}^{\triangle}$. Если $x \in \{a, b\}^{\triangle}$, то $ax = a$ и $bx = b$, откуда по (4′), (2) и (2′) получаем

$$x = x + xa = x + ax = x + a,$$
$$x = x + xb = x + bx = x + b.$$

Но тогда, учитывая (3), (1), (2), (2′) и (4), имеем

$$(a + b)x = (a + b)(x + x) = (a + b)(x + a + x + b) =$$
$$= (a + b)(x + (a + b)) = a + b,$$

т. е.

$$a + b \leqslant x.$$

Таким образом, $a + b$ — наименьший элемент верхнего конуса $\{a, b\}^{\triangle}$, т. е.

$$a + b = \sup \{a, b\}.$$

Поэтому, если $a \leqslant b$, то b оказывается наименьшим элементом верхнего конуса $\{a, b\}^{\triangle}$ и, значит, $a + b = b$. Если же $a + b = b$, то $b \in \{a, b\}^{\triangle}$, откуда $a \leqslant b$.

Из определения операций $+$ и $\cdot$, учитывая, что $\sup \{a, b\}$ ($\inf \{a, b\}$) — это наименьший (наибольший) элемент верхнего (нижнего) конуса $\{a, b\}^{\triangle}$ ($\{a, b\}^{\triangledown}$), получаем:

Следствие 1. *Если $a, b \leqslant c$, то $a + b \leqslant c$.*

Следствие 2. *Если $c \leqslant a, b$, то $c \leqslant ab$.*

Замечая, что $a \leqslant b$ и $c \leqslant d$ влечет $b + d \in \{a, c\}^{\triangle}$ и $ac \in \{b, d\}^{\triangledown}$, выводим:

Следствие 3. *Если $a \leqslant b$ и $c \leqslant d$, то $a + c \leqslant b + d$ и $ac \leqslant bd$.*

Если в соответствии с теоремой 2 от структуры перейти к множеству с двумя операциями, а от него к структуре в соответствии с теоремой 3, то, как нетрудно проверить, возникает исходная структура. То же самое имеет место и при переходе от множества с операциями к структуре, а затем снова к множеству с операциями.

Отображение φ структуры L в структуру L' называется *гомоморфизмом*, если $\varphi(a+b)=\varphi(a)+\varphi(b)$ и $\varphi(ab)=\varphi(a)\,\varphi(b)$ для всех $a, b \in L$. Взаимно однозначный гомоморфизм называется *изоморфизмом*. Если L — структура функций (пример 8 из таблицы 5), а L' — структура действительных чисел с обычным порядком и $\varphi(f)=f(0)$, то φ оказывается гомоморфизмом. Действительно, если, например, $f(0) \leqslant g(0)$, то

$$\varphi(\sup_L(f, g)) = g(0) = \sup_{L'}\{f(0), g(0)\} = \sup_{L'}\{\varphi(f), \varphi(g)\},$$

$$\varphi(\inf_L(f, g)) = f(0) = \inf_{L'}\{f(0), g(0)\} = \inf_{L'}\{\varphi(f), \varphi(g)\}.$$

Гомоморфизм структур является изотонным отображением. Действительно, если φ — гомоморфизм структур и $a \leqslant b$, то согласно теореме 3 $a = ab$. Отсюда $\varphi(a) = \varphi(a)\cdot\varphi(b)$, т. е. $\varphi(a) \leqslant \varphi(b)$. Однако изотонное отображение не обязано быть структурным гомоморфизмом Например, пусть L — структура подмножеств множества $M = \{1, 2, \ldots, n\}$, где $n \geqslant 3$ (пример 6 из таблицы 5), L' — структура целых чисел с обычным порядком и

$$\varphi(A) = \{\text{число точек подмножества } A\}.$$

Изотонность этого отображения очевидна. Однако

$$\varphi(\sup_L(\{1, 2\}, \{3\})) = \varphi(\{1, 2, 3\}) = 3 \neq 2 = \sup_{L'}\{2, 1\} = \sup_{L'}\{\varphi(\{1, 2\}), \varphi(\{3\})\}.$$

Непустое подмножество H структуры L называется *подструктурой*, если $a, b \in H$ влечет за собой $a+b \in H$ и $ab \in H$. Любое подмножество цепи оказывается подструктурой. Совокупность конечных подмножеств структуры всех подмножеств бесконечного множества (пример 6 из таблицы 5) также оказывается подструктурой.

Аналогично теоремам 6 из § 2, 5 из § 3, 2 из § 4 и 5 из § 5 доказывается.

Теорема 4. *Если* φ — *гомоморфизм структуры* L *в структуру* L', *то* $\operatorname{Im}\varphi$ — *подструктура структуры* L'.

Структура L называется *дистрибутивной*, если для любых $a, b, c \in L$ имеет место $(a+b)c = ac + bc$.

Т е о р е м а 5. *Структура всех подмножеств некоторого множества* (пример 6 из таблицы 5) *дистрибутивна*.

Д о к а з а т е л ь с т в о. Если A, B и C — подмножества множества M и $x \in (A \cup B) \cap C$, то $x \in C$ и, кроме того, $x \in A$ или $x \in B$. Таким образом, $x \in A \cap C$ или $x \in B \cap C$, т. е. $x \in (A \cap C) \cup (B \cap C)$. Наоборот, если $x \in (A \cap C) \cup (B \cap C)$, то $x \in A \cap C$ или $x \in B \cap C$. В обоих случаях $x \in C$ и, кроме того, $x \in A$ или $x \in B$. Значит, $x \in (A \cup B) \cap C$.

В качестве другого примера дистрибутивной структуры укажем произвольную цепь. Действительно, если a, b, c — элементы цепи, то имеет место $a \leqslant b \leqslant c$, $a \leqslant c \leqslant b$, $b \leqslant a \leqslant c$, $b \leqslant c \leqslant a$, $c \leqslant a \leqslant b$ или $c \leqslant b \leqslant a$. В этих случаях имеем

	$a+b$	$(a+b)c$	ac	bc	$ac+bc$
1	b	b	a	b	b
2	b	c	a	c	c
3	a	a	a	b	a
4	a	c	c	b	c
5	b	c	c	c	c
6	a	c	c	c	c

Таким образом, $(a + b)c = ac + bc$ во всех случаях.

Примером недистрибутивной структуры служит пятиэлементное множество $\{0, 1, a, b, c\}$ с порядком, задаваемым условиями $0 \leqslant a \leqslant 1$, $0 \leqslant b \leqslant 1$ и $0 \leqslant c \leqslant 1$ (см. рис. 8). Здесь $(a + b)\, c = 1c = c$, но $ac + bc = 0 + 0 = 0$.

Т е о р е м а 6. *Следующие свойства структуры L эквивалентны*:

(1) L *дистрибутивна*;

(2) $ab + c = (a + c)(b + c)$ *для любых* $a, b, c \in L$;

(3) $ab + ac + bc = (a + b)(a + c)(b + c)$ *для любых* $a, b, c \in L$.

Д о к а з а т е л ь с т в о. (1) $\Rightarrow$ (2). Имеем

$$(a + c)(b + c) = (a + c)\, b + c = ab + bc + c = ab + c.$$

(2) $\Rightarrow$ (3). Действительно,

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

(3) $\Rightarrow$ (1). Если $a \leqslant c$, то $ac = a = a + ab = a\, b + ac$.

Поэтому

$$ac + bc = ab + ac + bc =$$
$$= (a + b)(a + c)(b + c) = (a + b)\, c\, (b + c) = (a + b)\, c,$$

поскольку $c \leqslant b + c$. Таким образом, доказываемое соотношение дистрибутивности установлено в предположении, что $a \leqslant c$. Чтобы установить его справедливость в общем случае, положим

$$u = ab + ac + bc$$

и

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

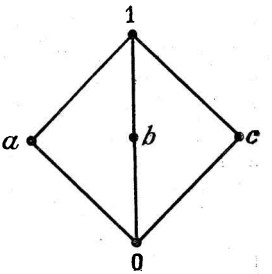


Рис. 8

Из теоремы 3 и ее следствия 1 вытекает, что $ac + bc \leqslant c$. Используя уже доказанный частный случай дистрибутивного закона, получим

$$cu = c\,(ab + (ac + bc)) =$$
$$= cab + c\,(ac + bc) = abc + ac + bc = ac + bc,$$
$$cv = c\,(a + b)(a + c)(b + c) = (a + b)\, c.$$

Но $u = v$ по условию. Поэтому

$$(a + b)\, c = cv = cu = ac + bc.$$

Пусть D — дистрибутивная структура. Непустое подмножество I структуры D называется *идеалом*, если x, $y \in I$ влечет $x + y \in I$ и $xd \in I$ для всякого d из D.

Теорема 7. *Если нижний конус некоторого подмножества дистрибутивной структуры не пуст, то он является идеалом* *).

Доказательство. Если x, $y \in A^{\nabla}$, то $x \leqslant a$ и $y \leqslant a$ для каждого $a \in A$. Ввиду следствия 1 теоремы 3 $x + y \leqslant a$ для каждого $a \in A$, и, кроме того, если $d \in D$, то $xd \leqslant x \leqslant a$ для каждого $a \in A$. Таким образом, $x + y$ и xd лежат в A^{∇}, т. е. A^{∇} — идеал.

Теорема 8. *Если I и J — идеалы дистрибутивной структуры D, то идеалом в D является и множество всех сумм вида $x + y$, где $x \in I$, $y \in J$.*

Доказательство. Если x, $x' \in I$, y, $y' \in J$ и $d \in D$, то

$$(x + y) + (x' + y') = (x + x') + (y + y')$$

*) Эта теорема справедлива для произвольной структуры при том же самом определении идеала.

и

$$(x + y)\, d = xd + yd,$$

причем $x + x'$, $xd \in I$ и $y + y'$, $yd \in J$.

Идеал, рассмотренный в теореме 8, называется *суммой идеалов* I и J и обозначается через $I + J$.

Теорема 9. *Всякая конечная дистрибутивная структура изоморфна подструктуре структуры всех подмножеств некоторого конечного множества.*

Доказательство. Пусть a и b — два различных элемента конечной дистрибутивной структры D. Если $a \leqslant b$ и $b \leqslant a$, то $a = b$. Следовательно, имеем $a \not\leqslant b$ или $b \not\leqslant a$. Допустим, что $b \not\leqslant a$. (Случай, когда $a \not\leqslant b$, рассматривается аналогично.) Существуют идеалы структуры D, которые содержат a, но не содержат b. Ввиду теоремы 7 таким будет, например, нижний конус a^{∇}. Поскольку структура конечна, то среди таких идеалов есть максимальные, т. е. не вкладывающиеся в строго больший идеал, обладающий указанным свойством. Пусть $I_{a,b}$ — один из таких максимальных идеалов.

Лемма 1. *Если* $c \notin I_{a,b}$, *то* $b = u + s$, *где* $u \leqslant c$ *и* $s \in I_{a,b}$.

Для доказательства положим $I = I_{a,b}$ и рассмотрим идеал $c^{\nabla} + I$. Поскольку структура D конечна, она содержит наименьший элемент 0. Поскольку $0d = 0$ для всех $d \in D$, элемент 0 принадлежит любому идеалу структуры D. Отсюда $x = 0 + x \in c^{\nabla} + I$ для всех $x \in I$, т. е. $I \subseteq c^{\nabla} + I$, и $c = c + 0 \in c^{\nabla} + I$. Следовательно, $I \subset c^{\nabla} + I$. Отсюда $b \in c^{\nabla} + I$, ибо I максимален среди идеалов, содержащих a, но не содержащих b. Приняв во внимание определение суммы идеалов, получаем, что $b = u + s$, где $u \in c^{\nabla}$, т. е. $u \leqslant c$, и $s \in I$.

Лемма 2. *Если* x, $y \notin I_{a,b}$, *то* $xy \notin I_{a,b}$.

Действительно, ввиду леммы 1 имеем $b = u + s = v + t$, где $u \leqslant x$, $v \leqslant y$ и s, $t \in I_{a,b}$. Ввиду теоремы 2 и следствия 3 теоремы 3 отсюда следует

$$b = b^2 = (u + s)(v + t) \leqslant (x + s)(y + t) = xy + (xt + sy + st).$$

Поскольку $xt + sy + st \in I_{a,b}$, то предположение, что $xy \in I_{a,b}$, влечет $b \in I_{a,b}$, вопреки выбору идеала $I_{a,b}$.

Пусть $2 = \{0, 1\}$ — двухэлементная цепь, где $0 \leqslant 1$, и

$$\varphi_{a,b}(x) = \begin{cases} 1, & \text{если } x \in D \setminus I_{a,b}, \\ 0, & \text{если } x \in I_{a,b}. \end{cases}$$

Лемма 3. $\varphi_{a,b}$ — *гомоморфное наложение структуры* D *на структуру* **2**.

Для доказательства достаточно заметить, что $I_{a,b} \neq D$, и установить, что, условившись писать φ и I вместо $\varphi_{a,b}$ и $I_{a,b}$ соответственно, имеем

$$\varphi(x+y) = \varphi(x) + \varphi(y)$$

и

$$\varphi(xy) = \varphi(x)\,\varphi(y)$$

для любых $x, y \in D$. Возможны следующие четыре случая:

1) $x, y \in I$; 2) $x \in I, y \notin I$; 3) $x \notin I, y \in I$, 4) $x, y \notin I$.

Заметим, что $x + y \in I$ влечет $x = x(x+y) \in I$ и $y = y(x+y) \in I$. Поэтому в первых трех случаях имеем

$$\varphi(x+y) = 0 = 0+0 = \varphi(x) + \varphi(y),$$
$$\varphi(xy) = 0 = 0\cdot 0 = \varphi(x)\,\varphi(y),$$
$$\varphi(x+y) = 1 = 0+1 = \varphi(x) + \varphi(y),$$
$$\varphi(xy) = 0 = 0\cdot 1 = \varphi(x)\varphi(y)$$

и

$$\varphi(x+y) = 1 = 1+0 = \varphi(x) + \varphi(y),$$
$$\varphi(xy) = 0 = 1\cdot 0 = \varphi(x)\,\varphi(y)$$

соответственно. В четвертом случае, учитывая лемму 2, получаем

$$\varphi(x+y) = 1 = 1+1 = \varphi(x) + \varphi(y)$$

и

$$\varphi(xy) = 1 = 1\cdot 1 = \varphi(x)\,\varphi(y).$$

Теперь обозначим через M множество всех пар (a, b), где $a, b \in D$ и $a \neq b$, а через P — структуру всех подмножеств множества M. Для доказательства теоремы укажем гомоморфное вложение структуры D в структуру P. С этой целью для всякого x из D положим:

$$\Phi(x) = \{(a, b) \in M \mid x \notin I_{a,b}\} = \{(a, b) \in M \mid \varphi_{a,b}(x) = 1\}.$$

Ясно, что Φ — отображение множества D в множество P. Если $x \neq y$, то имеем, например, $y \not\leqslant x$. Но тогда $x \in I_{x,y}$ и $y \notin I_{x,y}$, т. е. $(x, y) \notin \Phi(x)$, но $(x, y) \in \Phi(y)$. Следовательно, $\Phi(x) \neq \Phi(y)$, т. е. Φ — вложение.

Остается доказать, что

$$\Phi(x+y) = \Phi(x) \cup \Phi(y)$$

и

$$\Phi(xy) = \Phi(x) \cap \Phi(y).$$

Но если $(a, b) \in \Phi(x + y)$, то, учитывая лемму 3, имеем

$$1 = \varphi_{a,b}(x + y) = \varphi_{a,b}(x) + \varphi_{a,b}(y).$$

Отсюда $\varphi_{a,b}(x) = 1$ или $\varphi_{a,b}(y) = 1$, т. е. или $(a, b) \in \Phi(x)$, или $(a, b) \in \Phi(y)$. Последнее означает, что $(a, b) \in \Phi(x) \cup \Phi(y)$. Таким образом, $\Phi(x + y) \subseteq \Phi(x) \cup \Phi(y)$. Если же $(a, b) \in \Phi(x) \cup \Phi(y)$, то имеем, например, $(a, b) \in \Phi(x)$. Отсюда

$$\varphi_{a,b}(x + y) = \varphi_{a,b}(x) + \varphi_{a,b}(y) = 1 + \varphi_{a,b}(y) = 1,$$

т. е. $(a, b) \in \Phi(x + y)$. Таким образом, $\Phi(x) \cup \Phi(y) \subseteq \Phi(x + y)$, и первое из нужных соотношений доказано. Если теперь $(a, b) \in \Phi(xy)$, то, принимая во внимание лемму 3, имеем

$$1 = \varphi_{a,b}(xy) = \varphi_{a,b}(x)\varphi_{a,b}(y),$$

что возможно лишь при $\varphi_{a,b}(x) = \varphi_{a,b}(y) = 1$. Но тогда $(a, b) \in \Phi(x) \cap \Phi(y)$, т. е. $\Phi(xy) \subseteq \Phi(x) \cap \Phi(y)$. Если, наконец, $(a, b) \in \Phi(x) \cap \Phi(y)$, то

$$\varphi_{a,b}(xy) = \varphi_{a,b}(x)\varphi_{a,b}(y) = 1 \cdot 1 = 1,$$

т. е. $(a, b) \in \Phi(xy)$. Таким образом, $\Phi(x) \cap \Phi(y) \subseteq \Phi(xy)$, чем и заканчивается доказательство, так как $\operatorname{Im} \Phi$ — подструктура структуры P согласно теореме 4.

Дистрибутивная структура B с нулем и единицей называется *булевой алгеброй*, если для каждого элемента a из B найдется такой элемент $a' \in B$, что $a + a' = 1$ и $aa' = 0$. Этот элемент называется *дополнением* элемента a. Структура всех подмножеств любого множества является булевой алгеброй. Цепь же, содержащая более двух элементов, булевой алгеброй не является.

Т е о р е м а 10. *Каждый элемент булевой алгебры имеет только одно дополнение.*

Д о к а з а т е л ь с т в о. Если a' и b — дополнения элемента a, то

$$a' = a' \cdot 1 = a'(a + b) = a'a + a'b = 0 + a'b = ab + a'b = (a + a')b = 1 \cdot b = b,$$

Теорема 11. *В булевой алгебре справедливы следующие соотношения*:

$$(a + b)' = a'b',$$
$$(ab)' = a' + b',$$
$$a'' = a,$$
$$0' = 1,\ 1' = 0.$$

Доказательство. Равенство $a = a''$ сразу следует из теоремы 10. Учитывая теорему 6, получаем

$$(a + b) + a'b' = (a + b + a')(a + b + b') = 1 \cdot 1 = 1,$$
$$(a + b)(a'b') = aa'b' + ba'b' = 0 + 0 = 0.$$

Отсюда в силу теоремы 10 имеем $(a + b)' = a'b'$. Далее, учитывая уже доказанные соотношения, получаем

$$(ab)' = (a''b'')' = ((a' + b')')' = a' + b'.$$

Наконец, из равенств $1 + 0 = 1$ и $1 \cdot 0 = 0$ и теоремы 10 вытекают последние два соотношения.

Теорема 12. *Всякая конечная булева алгебра изоморфна структуре всех подмножеств некоторого конечного множества.*

Доказательство. Пусть B — конечная булева алгебра. Элемент p из B называется *атомом*, если $p \neq 0$ и $0 \neq x \leqslant p$ влечет $x = p$*). Обозначим через M множество всех атомов булевой алгебры B, а через P — булеву алгебру всех подмножеств множества M.

Лемма 1. *Если* $0 \neq x \in B$, *то найдется такой атом* p, *что* $p \leqslant x$.

Для доказательства положим $x_0 = x$. Допустим, что найдены различные ненулевые элементы $x_0, x_1, \ldots, x_m \in B$, такие, что

$$x_m \leqslant \ldots \leqslant x_1 \leqslant x_0.$$

Если x_m — атом, то можно положить $p = x_m$. В противном случае найдется элемент $x_{m+1} \in B$ такой, что $x_{m+1} \leqslant x_m$, $x_{m+1} \neq x_m$ и $x_{m+1} \neq 0$. Если $x_{m+1} = x_i$, где $0 \leqslant i < m$, то $x_i = x_{m+1} \leqslant x_m \leqslant x_i$, откуда $x_i = x_m$ в силу антисимметричности. Следовательно, $x_0, x_1, \ldots, x_m, x_{m+1}$ — различные элементы из B. Остается заметить, что, ввиду конечности множества B, описанный процесс построения элементов x_i не может продолжаться бесконечно.

*) Другими словами, p — минимальный элемент частично упорядоченного множества ненулевых элементов булевой алгебры B.

Лемма 2. *Каждый ненулевой элемент x из B равен сумме всех атомов, лежащих в нижнем конусе x^{∇}.*

В самом деле, если $x \in B$, то пусть $p_1, \ldots, p_n$ — все атомы, принадлежащие нижнему конусу x^{∇}, и $y = p_1 + \ldots + p_n$. В силу следствия 1 теоремы 3, $y \leqslant x$. Поэтому

$$x = x(y + y') = xy + xy' = y + xy'. \qquad (*)$$

Допустим, что $xy' \neq 0$. Тогда по лемме 1 найдется атом $p \leqslant xy'$. Но $xy' \leqslant x$. Следовательно, $p \leqslant x$, а значит, $p = p_i$ для некоторого i. Кроме того, $p_i \leqslant y$. По следствию 3 теоремы 3

$$p_i = pp_i \leqslant (xy')y \leqslant y'y = 0,$$

т. е. $p_i = 0$, что невозможно. Таким образом, $xy' = 0$, что вместе с (*) дает $x = y$.

Теперь определим отображение Ф множества B в множество P, полагая

$$\Phi(x) = M \cap x^{\nabla}.$$

Если $\Phi(x) = \Phi(y)$, то из леммы 2 сразу следует, что $x = y$, т. е. Ф оказывается вложением. Пусть теперь U — некоторое подмножество из M. Если U пусто, то $U = \Phi(0)$. В противном случае обозначим через x сумму всех атомов, лежащих в U. Ясно, что $U \subseteq \Phi(x)$. Если $q \in \Phi(x)$, то из равенства

$$q = xq = \sum_{p \in U} pq$$

вытекает, что $pq \neq 0$ для некоторого $p \in U$. Но тогда

$$0 \neq pq \leqslant p$$

и

$$0 \neq pq \leqslant q,$$

откуда в силу определения атома следует

$$q = pq = p \in U.$$

Таким образом, $\Phi(x) = U$, т. е. Ф является наложением.

Для дальнейшего понадобится

Лемма 3. *Если $x \leqslant y$, то $\Phi(x) \subseteq \Phi(y)$.*

Действительно, если $x \leqslant y$, то $x^{\nabla} \subseteq y^{\nabla}$, откуда

$$\Phi(x) = M \cap x^{\nabla} \subseteq M \cap y^{\nabla} = \Phi(y),$$

Остается убедиться в справедливости равенств

$$\Phi(x+y) = \Phi(x) \cup \Phi(y)$$

и

$$\Phi(xy) = \Phi(x) \cap \Phi(y)$$

для всех $x, y \in B$. Из леммы 3 вытекают включения

$$\Phi(x) \cup \Phi(y) \subseteq \Phi(x+y)$$

и

$$\Phi(xy) \subseteq \Phi(x) \cap \Phi(y).$$

Если $p \in \Phi(x+y)$, то $p \leqslant x+y$. Отсюда

$$p = p(x+y) = px + py.$$

Следовательно, $px \neq 0$ или $py \neq 0$. В первом случае имеем

$$0 < px \leqslant p,$$

откуда $px = p$, а значит, $p \leqslant x$, что означает $p \in \Phi(x)$. Во втором случае получаем, что $p \in \Phi(y)$. Таким образом, $\Phi(x+y) \subseteq \Phi(x) \cup \Phi(y)$ и, следовательно, $\Phi(x+y) = \Phi(x) \cup \Phi(y)$. Наконец, включение $p \in \Phi(x) \cap \Phi(y)$ влечет $p \leqslant x$ и $p \leqslant y$. Отсюда $p \leqslant xy$, т. е. $p \in \Phi(xy)$. Следовательно, $\Phi(x) \cap \Phi(y) \subseteq \Phi(xy)$, а значит, и $\Phi(xy) = \Phi(x) \cap \Phi(y)$.

Остановимся на связи булевых алгебр с кольцами.

Кольцо R называется *булевым*, если $a^2 = a$ для всех a из R.

Теорема 13. *Булево кольцо коммутативно, и $a + a = 0$ (т. е. $a = -a$) для всех элементов a.*

Доказательство. Во-первых,

$$a + a = (a+a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a,$$

откуда $a + a = 0$. Во-вторых,

$$a + b = (a+b)^2 = a^2 + ab + ba + b^2 = a + b + ab + ba.$$

Отсюда $ab + ba = 0$. Учитывая доказанное выше, получаем

$$ab = ab + (ba + ba) = (ab + ba) + ba = ba.$$

Теорема 14. *Пусть B — булева алгебра. Для любых $a, b \in B$ положим*

$$a \# b = ab' + a'b$$

и

$$a \circ b = ab.$$

Тогда B становится булевым кольцом с единицей.

Доказательство. Равенство $a^2 = a$, ассоциативность умножения, наличие единицы и коммутативность обеих операций очевидны. Далее, учитывая теорему 11_3 имеем

$$\begin{aligned}(a \# b) \# c &= (ab' + a'b)\, c' + (ab' + a'b)'\, c = \\ &= ab'c' + a'bc' + (a' + b)\,(a + b')\, c = \\ &= ab'c' + a'bc' + a'b'c + bac = \\ &= a\,(b'c' + bc) + a'\,(bc' + b'c) = \\ &= a\,(b' + c)\,(b + c') + a'\,(bc' + b'c) = \\ &= a\,(bc' + b'c)' + a'\,(bc' + b'c) = a \# (b \# c)_3\end{aligned}$$

$$a \# 0 = a0' + a'0 = a \cdot 1 = a$$

и

$$a \# a = aa' + a'a = 0,$$

т. е. B оказывается абелевой группой по сложению. Наконец,

$$\begin{aligned}(a \# b) \circ c &= (ab' + a'b)\, c = ab'c + ab'c = \\ &= ac\,(b' + c') + (a' + c')\, bc = (ac)\,(bc)' + (ac)'(bc) = \\ &= a \circ c \# b \circ c.\end{aligned}$$

Теорема 15. *Пусть R — булево кольцо с единицей относительно операций $\#$ и $\circ$. Положим*

$$a + b = a \# b \# a \circ b$$

и

$$ab = a \circ b.$$

Тогда R становится булевой алгеброй B. Кольцо, получаемое из алгебры B с помощью теоремы 14, совпадает с R. Применение только что описанной конструкции к кольцу, указанному в теореме 14, приводит к исходной булевой алгебре.

Доказательство. Ассоциативность операций $+$ и $\cdot$, а также равенство $aa = a$ проверяются непосредственным подсчетом. Коммутативность булева кольца, установленная в теореме 13, обеспечивает коммутативность этих операций. Кроме того, $a \# a = 0$ по

теореме 13. Поэтому

$$a + a = a \# a \# a \circ a = a,$$

$$(a + b)\, a = (a \# b \# a \circ b) \circ a = a \circ a \# a \circ b \# a \circ b \circ a = a \circ a \# a \circ b \# a \circ b = a$$

и

$$a + ab = a \# a \circ b \# a \circ (a \circ b) = a \# a \circ b \# a \circ b = a.$$

В силу теоремы 3, B оказывается структурой. Ясно, что $a1 = a$ и $a0 = 0$ для всех $a \in B$, т. е. структура B обладает нулем и единицей. Из равенств

$$a\,(1 \# a) = a \circ 1 \# a \circ a = a \# a = 0$$

и

$$a + (1 \# a) = a \# 1 \# a \# a \circ (1 \# a) = a \# 1 \# a \# a \# a = 1$$

вытекает, что B — структура с дополнениями. Ее дистрибутивность проверяется следующим образом:

$$(a + b)\, c = (a \# b \# ab) \circ c = ac \# bc \# ac \circ bc = ac + bc.$$

Заключительные утверждения теоремы вытекают из равенств

$$ab' + a'b =$$

$$= a \circ (1 \# b) \# (1 \# a) \circ b \# a \circ (1 \# b) \circ b \circ (1 \# a) =$$

$$= a \# ab \# b \# ab \# ab \# aba \# abb \# abab = a \# b,$$

$$(a \# b) \# a \circ b = (ab' + a'b)\,(ab)' + (ab' + a'b)'\,ab =$$

$$= (ab' + a'b)\,(a' + b') + (a' + b)\,(a + b')ab =$$

$$= ab' + a'b + ab = ab' + ab + a'b + ab =$$

$$= a\,(b' + b) + (a' + a)\, b = a + b.$$

Упражнения

1. Какие из отношений, приводимых в таблице на следующей странице, являются порядками?

2. Пусть P — множество неотрицательных целых чисел с обычным порядком, а P' — то же самое множество, упорядоченное по делимости (пример 5 из таблицы 5), φ: $P \to P'$ и ψ: $P' \to P$ — тождественные отображения. Является ли какое-нибудь из них изотонным?

3. Если φ: $P \to P'$ — изоморфизм частично упорядоченных множеств, то элемент a является наименьшим, наибольшим, минимальным или максимальным элементом частично упорядоченного множества P тогда и только тогда, когда соответствующим свойством обладает элемент $\varphi(a)$ частично упорядоченного множества P'. Построить примеры, показывающие, что это не всегда так, если φ — изотонное отображение.

	Множество	Отношение ρ
1	Подмодули модуля A	Включение (ср. пример 6 из таблицы 5)
2	Треугольники на плоскости	$a\rho b$, если площадь треугольника a не превосходит площади треугольника b
3	Слова (включая пустое)	$a\rho b$, если $b = au$ для некоторого слова u
4	То же	$a\rho b$, если $b = uav$ для некоторых слов u и v
5	Слова от двух или более букв	$a\rho b$, если существуют такие слова u и v, что $au = bv$
6	Слова от одной буквы	То же

4. Доказать, что существуют в точности два неизоморфных двухэлементных частично упорядоченных множества.

5. В конечном частично упорядоченном множестве всегда существуют как минимальные, так и максимальные элементы. Однако наибольший (наименьший) элемент может не существовать.

6. Элемент a максимален (минимален) тогда и только тогда, когда $a^{\triangle} = \{a\}$ (когда $a^{\triangledown} = \{a\}$).

7. Доказать следующие свойства конусов: а) если $A \subseteq B$, то $A^{\triangle} \supseteq B^{\triangle}$ и $A^{\triangledown} \supseteq B^{\triangledown}$; б) $A \subseteq A^{\triangle\triangledown} \cap A^{\triangledown\triangle}$; в) $A^{\triangle} = A^{\triangle\triangledown\triangle}$; г) $A^{\triangledown} = A^{\triangledown\triangle\triangledown}$; д) $(A \cup B)^{\triangle} = A^{\triangle} \cap B^{\triangle}$; е) $(A \cup B)^{\triangledown} = A^{\triangledown} \cap B^{\triangledown}$.

8. Элемент, являющийся максимальным и минимальным одновременно, не сравним ни с каким отличным от него элементом.

9. Если a и b — максимальные элементы, то точная верхняя грань множества $\{a, b\}$ существует тогда и только тогда, когда $a = b$.

10. Найти точные верхние и точные нижние грани (или доказать их отсутствие) двухэлементных подмножеств в частично упорядоченных множествах примеров 3, 5 и 8 из таблицы 5 и 1, 3 и 4 из упражнения 1. В тех случаях, когда частично упорядоченное множество оказывается структурой, выяснить, является ли она дистрибутивной.

11. Всякий минимальный (максимальный) элемент структуры является наименьшим (наибольшим).

12. Если a, b, c — элементы структуры и $a + b + c = abc$, то $a = b = c$.

13. Доказать равносильность следующих свойств структуры L: а) L — цепь; б) все непустые подмножества из L являются подструктурами; в) $a = bc$ влечет $a = b$ или $a = c$.

14. Изотонное отображение цепи в любую структуру является гомоморфизмом структур.

15. Доказать, что дистрибутивность структуры L равносильна каждому из следующих свойств: а) неравенство $a \leqslant b$ имеет место тогда и только тогда, когда $ac \leqslant bc$ и $a + c \leqslant b + c$ для некоторого $c \in L$; б) $(a + b)(c + ab) = ab + ac + bc$ для любых $a, b, c \in L$; в) $(a + b)c \leqslant a + bc$ для любых $a, b, c \in L$.

16. Идеал I дистрибутивной структуры D называется *простым*, если $ab \in I$ влечет за собой $a \in I$ или $b \in I$. Доказать, что всякий

максимальный идеал M дистрибутивной структуры D (т. е. идеал, отличный от D и не содержащийся ни в каком ее идеале, отличном от M и D) прост и что нижний конус a^{∇} является простым идеалом тогда и только тогда, когда $a = bc$ влечет за собой $a = b$ или $a = c$.

17. Следующие утверждения об элементах a и b из булевой алгебры равносильны: а) $a \leqslant b$; б) $ab' = 0$; в) $a' + b = 1$.

18. Всякое допустимое разбиение булевой алгебры является допустимым разбиением соответствующего булева кольца и наоборот.

19. Булево кольцо является полем тогда и только тогда, когда оно двухэлементно.

20. Идемпотенты любого коммутативного кольца образуют булево кольцо относительно операций

$$e + f = e + f - ef,$$
$$e \circ f = ef.$$

21. Убедиться, что подгруппы группы $(\boldsymbol{Z}/2\boldsymbol{Z}) \oplus (\boldsymbol{Z}/2\boldsymbol{Z})$ образуют структуру, изоморфную структуре, изображенной на рис. 8 (см. с. 157).

ГЛАВА III

ЛИНЕЙНЫЕ ПРОСТРАНСТВА И ЛИНЕЙНЫЕ АЛГЕБРЫ

Общая теория линейных пространств излагается здесь в минимальном объеме. Поэтому некоторые факты, обычно выводимые из общей теории, сопровождаются специальными доказательствами. Как правило, приводятся лишь результаты, необходимые для дальнейшего. Исключение сделано для теорем, освещающих связь теории линейных пространств с системами линейных уравнений. Результаты, справедливые для произвольных модулей, изложены в § 5 предыдущей главы и, разумеется, широко используются здесь. Что касается линейных алгебр, то в качестве основного объекта изучения выступают конечномерные вполне приводимые алгебры.

Отбор результатов диктуется потребностями теории представлений конечных групп, излагаемой в гл. IV. В связи с этим конечность размерности линейной алгебры включена в определение. Значительное место уделено алгебре линейных преобразований линейного пространства.

§ 1. Линейные пространства

Модуль над полем P называется *линейным пространством*. Поскольку коммутативность поля позволяет не различать правые и левые модули, будем записывать линейные пространства как левые модули. Подмодуль и фактормодуль линейного пространства будем называть *подпространством и факторпространством* соответственно.

Отметим простой, но важный факт.

Теорема 1. *Если L — линейное пространство над полем P, $a \in L$, $0 \neq \lambda \in P$ и $\lambda a = 0$, то $a = 0$.*

Доказательство. Поскольку $\lambda \neq 0$, а P — поле, то существует элемент λ^{-1}. Вспоминая определение и простейшие свойства модуля, получаем

$$a = 1a = (\lambda^{-1}\lambda)\, a = \lambda^{-1}(\lambda a) = \lambda^{-1} 0 = 0.$$

Линейное пространство называется *конечномерным*, если оно является линейной оболочкой некоторого конечного множества векторов, т. е. конечно порожденным модулем. Конечномерным оказывается, например, пространство n-мерных строк над полем (см. с. 122). Линейное пространство, не являющееся конечномерным, называется *бесконечномерным*. Бесконечномерным пространством является, например, множество всех таких счетномерных строк над полем, у которых почти все координаты равны нулю (см. с. 122).

Теорема 2. *Линейное пространство L над полем P является неприводимым P-модулем тогда и только тогда, когда $L = Pa$ для некоторого ненулевого вектора $a \in L$.*

Доказательство. Если L — неприводимый P-модуль и $0 \neq a \in L$, то Pa, будучи ненулевым подмодулем модуля L, совпадает с L (ср. теорема II.5.19). Если же $L = Pa$, где $a \neq 0$, и L' — ненулевой подмодуль модуля L, то найдется ненулевой вектор $b \in L'$. Поскольку $b = \lambda a$, где $0 \neq \lambda \in P$, то

$$a = 1a = (\lambda^{-1}\lambda)\, a = \lambda^{-1}(\lambda a) = \lambda^{-1} b \in L',$$

откуда $L \subseteq L'$, т. е. $L = L'$.

Конечная система векторов линейного пространства называется *линейно зависимой*, если существует их нетривиальная линейная комбинация, равная нулю. Другими словами, система векторов $\{a_1, \ldots, a_m\}$ называется *линейно зависимой*, если существуют элементы $\lambda_1, \ldots, \lambda_m \in P$, из которых хотя бы один отличен от нуля, такие, что $\lambda_1 a_1 + \ldots + \lambda_m a_m = 0$. Система, не являющаяся линейно зависимой, называется *линейно независимой*. Линейно независимую систему образуют, например, векторы $e_1, \ldots, e_n$ из пространства n-мерных строк (см. с. 122). Действительно, если $\lambda_1 e_1 + \ldots + \lambda_n e_n = 0$ для некоторых $\lambda_i \in P$, то $(\lambda_1, \ldots, \lambda_n) = 0$, т. е. все λ_i равны нулю. Система, содержащая нулевой вектор, всегда линейно зависима. Действительно, если $\{0, a_1, \ldots, a_m\}$ — такая система, то в качестве равной нулю нетривиальной линейной комбинации можно взять $1 \cdot 0 + 0a_1 + \ldots + 0a_m$.

Теорема 3. *Система, состоящая из одного вектора, линейно зависима тогда и только тогда, когда этот вектор нулевой.*

Доказательство. Если система $\{a\}$ линейно зависима, то $\lambda a = 0$, где $0 \neq \lambda \in P$, и $a = 0$ согласно теореме 1. Если $a = 0$, то система $\{a\}$ линейно зависима, поскольку $1 \cdot a = a = 0$.

Теорема 4. *Система, содержащая два или более векторов линейного пространства, линейно зависима в том и только в том случае, когда хотя бы один из векторов системы линейно выражается через остальные.*

Доказательство. Допустим, что система векторов $\{a_1, \ldots, a_n\}$, где $n \geqslant 2$, линейно зависима, т. е.

$$\lambda_1 a_1 + \ldots + \lambda_n a_n = 0,$$

причем $\lambda_i \neq 0$ для некоторого i. Тогда

$$a_i = \left(-\frac{\lambda_1}{\lambda_i}\right) a_1 + \ldots + \left(-\frac{\lambda_{i-1}}{\lambda_i}\right) a_{i-1} + \\ + \left(-\frac{\lambda_{i+1}}{\lambda_i}\right) a_{i+1} + \ldots + \left(-\frac{\lambda_n}{\lambda_i}\right) a_n.$$

Следовательно, вектор a_i линейно выражается через остальные. С другой стороны, если

$$a_i = \lambda_1 a_1 + \ldots + \lambda_{i-1} a_{i-1} + \lambda_{i+1} a_{i+1} + \ldots + \lambda_n a_n,$$

то

$$\lambda_1 a_1 + \ldots + \lambda_{i-1} a_{i-1} + (-1)\, a_i + \lambda_{i+1} a_{i+1} + \ldots + \lambda_n a_n = 0,$$

где $\lambda_i = -1 \neq 0$, т. е. система $\{a_1, \ldots, a_n\}$ линейно зависима.

Теорема 5. *Сумма $Pa_1 + \ldots + Pa_m$, где a_i — ненулевые векторы, является прямой тогда и только тогда, когда система векторов $\mathfrak{A} = \{a_1, \ldots, a_m\}$ линейно независима.*

Доказательство. Допустим, что сумма прямая, но система $\mathfrak{A}$ линейно зависима. Тогда для подходящих $\lambda_i \in P$ имеем

$$\lambda_1 a_1 + \ldots + \lambda_m a_m = 0,$$

причем хотя бы одно из λ_i, скажем λ_p, отлично от нуля. Но $\lambda_i a_i \in Pa_i$ и, согласно свойству (4) теоремы II.5.12, $\lambda_i a_i = 0$ для всех i. В частности, $\lambda_p a_p = 0$. Ввиду теоремы 1 $a_p = 0$, вопреки условию. Наоборот, если система $\mathfrak{A}$ линейно независима и $0 = x_1 + \ldots + x_m$, где $x_i \in Pa_i$, то $x_i = \lambda_i a_i$ для некоторого $\lambda_i \in P$. Таким образом, $\lambda_1 a_1 + \ldots + \lambda_m a_m = 0$. Из линейной независимости системы $\mathfrak{A}$ вытекает $\lambda_1 = \ldots = \lambda_m = 0$, т. е. $x_1 = \ldots = \ldots = x_m = 0$. Остается еще раз применить теорему II.5.12.

Линейно независимая система векторов, линейная оболочка которой совпадает со всем пространством (под-

пространством), называется *базой* этого пространства (подпространства). Например, упоминавшиеся выше векторы $\{e_1, \ldots, e_n\}$ образуют базу пространства V n-мерных строк, ибо, как уже отмечалось, они линейно независимы, а V совпадает с их линейной оболочкой (см. с. 122).

Т е о р е м а 6. *Всякое ненулевое конечномерное линейное пространство L над полем P обладает базой, причем все его базы содержат одно и то же число векторов. Если $\{e_1, \ldots, e_n\}$ — база пространства L, $a \in L$ и $a = \lambda_1 e_1 + \ldots + \lambda_n e_n$, то числа $\lambda_i \in P$ определяются однозначно.*

Д о к а з а т е л ь с т в о. По определению конечномерного пространства, $L = \mathscr{L}(a_1, \ldots, a_m) = Pa_1 + \ldots + Pa_m$, причем $a_i \neq 0$ для некоторого i. Если $m = 1$, то система $\{a_1\}$ является базой пространства L в силу теоремы 3. Если $m > 1$, то можно предполагать, что для линейной оболочки меньшего числа векторов существование базы уже доказано. Если векторы $a_1, \ldots, a_m$ линейно независимы, то они и образуют базу пространства L. В противном случае из теоремы 4 вытекает, что, например, $a_m \in \mathscr{L}(a_1, \ldots, a_{m-1})$. Следовательно, $L = \mathscr{L}(a_1, \ldots, a_{m-1})$, и база пространства L существует по индуктивному предположению*). Допустим теперь, что как $\{e_1, \ldots, e_n\}$, так и $\{f_1, \ldots, f_m\}$ — базы линейного пространства L, причем $m < n$. Запишем

$$e_j = \sum_{i=1}^{m} a_{ij} f_i,$$

где $a_{ij} \in P$ $(j = 1, \ldots, n)$ и составим систему линейных уравнений:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = 0. \end{cases}$$

---

*) Приведем другое доказательство, в некотором смысле более поучительное. Именно, заметим, что поскольку $P = P \cdot 1$, то, в силу теоремы 2, поле P является неприводимым, а значит, вполне приводимым P-модулем. Поэтому, согласно теореме II.6.8, L оказывается вполне приводимым P-модулем. Учитывая теорему 2, получаем, что

$$L = Pe_1 \oplus \ldots \oplus Pe_n,$$

где e_i — ненулевые векторы из L. Из определения суммы подмодулей вытекает, что $L = \mathscr{L}(e_1, \ldots, e_n)$, а теорема 5 обеспечивает линейную независимость системы $\{e_1, \ldots, e_n\}$. Таким образом, $\{e_1, \ldots, e_n\}$ — база пространства L.

Поскольку число неизвестных больше числа уравнений, эта система согласно теореме I.1.4 имеет ненулевое решение, скажем, $(\alpha_1, \ldots, \alpha_n)$. Отсюда

$$\sum_{j=1}^{n} \alpha_j e_j = \sum_{j=1}^{n} \alpha_j \sum_{i=1}^{m} a_{ij} f_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij} \alpha_j \right) f_i = \sum_{i=1}^{n} 0 f_i = 0.$$

Поскольку $\alpha_j \neq 0$ для некоторого j, это противоречит линейной независимости системы $\{e_1, \ldots, e_n\}$. Для доказательства последнего утверждения теоремы допустим, что $a = \mu_1 e_1 + \ldots + \mu_n e_n$, где $\mu_i \in P$. Тогда после вычитания получаем

$$(\lambda_1 - \mu_1) e_1 + \ldots + (\lambda_n - \mu_n) e_n = 0.$$

Ввиду линейной независимости системы $\{e_1, \ldots, e_n\}$ отсюда вытекает, что $\lambda_i - \mu_i = 0$, т. е. $\lambda_i = \mu_i$ для всех i.

Однозначно определяемые числа λ_i, упоминающиеся в формулировке теоремы 6, называются *координатами вектора a в базе* $\{e_1, \ldots, e_n\}$.

Линейное пространство называется *n-мерным* (или *имеющим размерность n*), если оно обладает базой, состоящей из n векторов. По теореме 6, n векторов содержит любая база n-мерного линейного пространства. Размерность линейного пространства L условимся обозначать через $\dim L$. Как и следовало ожидать, размерность линейного пространства n-мерных строк равна n, ибо, как уже отмечалось, система $\{e_1, \ldots, e_n\}$ служит его базой.

Согласно теоремам 2 и 5, каждое ненулевое конечномерное линейное пространство вполне приводимо. Поэтому из теоремы II.5.22 вытекает

Теорема 7. *Всякое подпространство конечномерного линейного пространства выделяется прямым слагаемым.*

Теорема 8. *Следующие свойства суммы подпространств $S = S_1 + \ldots + S_m$ некоторого линейного пространства эквивалентны:*

(1) *сумма является прямой;*

(2) *объединение любых баз линейных пространств S_i служит базой линейного пространства S;*

(3) *объединение некоторых баз линейных пространств S_i служит базой линейного пространства S.*

Доказательство. (1) $\Rightarrow$ (2). Допустим, что $S = S_1 \oplus \ldots \oplus S_m$. Если $\{e_{i1}, \ldots, e_{in_i}\}$ — произвольная база подпространства S_i, то согласно теореме 5 $S_i =$

$= Pe_{i1} \oplus \ldots \oplus Pe_{in_i}$. Теперь остается использовать теорему II.5.13 и еще раз теорему 5.

Импликация (2) $\Rightarrow$ (3) тривиальна.

(3) $\Rightarrow$ (1). Предположим теперь, что $\{e_{i1}, \ldots, e_{in_i}\}$ — некоторые базы подпространств S_i,

$$\mathscr{E} = \{e_{11}, \ldots, e_{1n_1}, e_{21}, \ldots, e_{2n_2}, \ldots, e_{m1}, \ldots, e_{mn_m}\}$$

— база подпространства S и

$$s_1 + \ldots + s_m = 0,$$

где $s_i \in S_i$. Тогда

$$s_i = \lambda_{i1}e_{i1} + \ldots + \lambda_{in_i}e_{in_i}$$

для подходящих $\lambda_{ij} \in P$, откуда

$$\lambda_{11}e_{11} + \ldots + \lambda_{1n_1}e_{1n_1} + \lambda_{21}e_{21} + \ldots$$
$$\ldots + \lambda_{2n_2}e_{2n_2} + \ldots + \lambda_{m1}e_{m1} + \ldots + \lambda_{mn_m}e_{mn_m} = 0.$$

Поскольку система $\mathscr{E}$ линейно независима, отсюда следует, что $\lambda_{ij} = 0$ для всех i и j. Но тогда $s_i = 0$ для всех i и $S = S_1 \oplus \ldots \oplus S_m$ в силу свойства (4) теоремы II.5.12.

Т е о р е м а 9. *Следующие свойства линейного пространства L над полем P эквивалентны*:

(1) $\dim L = n$;

(2) *L изоморфно линейному пространству n-мерных строк*;

(3) *L представляется в виде прямой суммы n одномерных подпространств.*

Д о к а з а т е л ь с т в о. (1) $\Rightarrow$ (2). Пусть $\{f_1, \ldots, f_n\}$ — база пространства L и V — пространство n-мерных строк. Определим отображение φ: $V \to L$, полагая

$$\varphi(\lambda_1, \ldots, \lambda_n) = \lambda_1 f_1 + \ldots + \lambda_n f_n.$$

Легко проверяется, что это — гомоморфизм. Поскольку $L = \mathscr{L}(f_1, \ldots, f_n)$, он оказывается наложением. Из последнего утверждения теоремы 6 вытекает, что φ — вложение. Таким образом, φ — изоморфизм, что и требовалось.

(2) $\Rightarrow$ (1). Пусть V — пространство n-мерных строк,

$$e_i = (\underbrace{0, \ldots, 0}_{i-1}, 1, 0, \ldots, 0)$$

и φ: $V \to L$ — изоморфизм. Если $a \in L$, то для некоторого $v \in V$ имеем

$$a = \varphi(v) = \varphi\left(\sum_{i=1}^{n} \lambda_i e_i\right) = \sum_{i=1}^{n} \lambda_i \varphi(e_i),$$

т. е. $L = \mathcal{L}(\varphi(e_1), \ldots, \varphi(e_n))$. Если $\lambda_1\varphi(e_1) + \ldots + \lambda_n\varphi(e_n) = 0$ для некоторых $\lambda_i \in P$, то

$$\varphi(\lambda_1, \ldots, \lambda_n) = \varphi(\lambda_1 e_1 + \ldots + \lambda_n e_n) = \lambda_1\varphi(e_1) + \ldots + \lambda_n\varphi(e_n) = 0.$$

Отсюда $(\lambda_1, \ldots, \lambda_n) = 0$, т. е. $\lambda_i = 0$ для всех i. Следовательно, $\{\varphi(e_1), \ldots, \varphi(e_n)\}$ — база пространства L.

Поскольку линейное пространство одномерно тогда и только тогда, когда оно обладает базой, состоящей из одного вектора, то импликация (3) $\Rightarrow$ (1) сразу следует из теоремы 8, а импликация (1) $\Rightarrow$ (3) — из теоремы 5.

Ввиду свойства (2) теоремы 9 имеем

Следствие 1. *Изоморфные конечномерные линейные пространства имеют одинаковую размерность.*

Из свойства (3) теоремы 9 и теоремы о транзитивности разложения в прямую сумму (теорема II.5.13) вытекает

Следствие 2.

$$\dim(L_1 \oplus \ldots \oplus L_m) = \dim L_1 + \ldots + \dim L_m.$$

Следствие 3. *Если* $\dim L = n$ *и* $a_1, \ldots, a_{n+1} \in L$, *то система* $\{a_1, \ldots, a_{n+1}\}$ *линейно зависима.*

Действительно, если система $\{a_1, \ldots, a_{n+1}\}$ линейно независима и $L' = \mathcal{L}(a_1, \ldots, a_{n+1})$, то $\dim L' = n + 1$. В силу теоремы 7, $L = L' \oplus H$ для некоторого H, и, согласно следствию 2, $n = n + 1 + \dim H$, что невозможно.

Теорема 10. *Если* L' — *подпространство линейного пространства* L *и* $\dim L' = \dim L$, *то* $L = L'$.

Доказательство. Если $L \neq L'$, то, согласно теореме 7, $L = L' \oplus H$, где $H \neq 0$. Ввиду теоремы 8, база пространства L содержит больше векторов, чем база пространства L'. Следовательно, $\dim L > \dim L'$.

Гомоморфизмы линейных пространств будем называть *линейными отображениями*, а линейные отображения линейного пространства в себя — *линейными преобразованиями.*

Теорема 11. *Множество* $\mathrm{Hom}(L, L')$ *всех линейных отображений линейного пространства* L *над полем* P *в линейное пространство* L' *над полем* P *становится линейным пространством, если для* $\varphi, \psi \in \mathrm{Hom}(L, L')$ *и*

$\lambda \in P$ *положить*

$$x(\varphi + \psi) = x\varphi + x\psi$$

и

$$x(\lambda\varphi) = \lambda(x\varphi)$$

для всех $x \in L$.

Доказательство. Ввиду теоремы II.5.8, $\mathrm{Hom}(L, L')$ является абелевой группой. Из равенств

$$(x + y)(\lambda\varphi) = \lambda((x + y)\varphi) = \lambda(x\varphi + y\varphi) = \\ = \lambda(x\varphi) + \lambda(y\varphi) = x(\lambda\varphi) + y(\lambda\varphi)$$

и

$$(\xi x)(\lambda\varphi) = \lambda((\xi x)\varphi) = \lambda(\xi(x\varphi)) = \\ = (\lambda\xi)(x\varphi) = (\xi\lambda)(x\varphi) = \xi(\lambda(x\varphi)) = \xi(x(\lambda\varphi)),$$

где $x, y \in L$ и $\xi \in P$, вытекает, что $\lambda\varphi \in \mathrm{Hom}(L, L')$. Равенства же

$$x(\lambda(\varphi + \psi)) = \lambda(x(\varphi + \psi)) = \lambda(x\varphi + x\psi) = \\ = \lambda(x\varphi) + \lambda(x\psi) = x(\lambda\varphi) + x(\lambda\psi) = x(\lambda\varphi + \lambda\psi),$$

$$x((\lambda + \mu)\varphi) = (\lambda + \mu)(x\varphi) = \lambda(x\varphi) + \mu(x\varphi) = \\ = x(\lambda\varphi) + x(\mu\varphi) = x(\lambda\varphi + \mu\varphi),$$

$$x((\lambda\mu)\varphi) = (\lambda\mu)(x\varphi) = \lambda(\mu(x\varphi)) = \lambda(x(\mu\varphi)) = x(\lambda(\mu\varphi))$$

и

$$x(1\varphi) = 1(x\varphi) = x\varphi,$$

справедливые для всех $x \in L$, любых $\varphi, \psi \in \mathrm{Hom}(L, L')$ и $\lambda, \mu \in P$, показывают, что $\mathrm{Hom}(L, L')$ оказывается линейным пространством.

Столбец

$$e = \begin{Vmatrix} e_1 \\ \cdots \\ e_n \end{Vmatrix}$$

где e_i — векторы, назовем *вектор-столбцом*. Вектор-столбец называется *независимым* (*базисным*), если входящие в него векторы линейно независимы (образуют базу пространства). Если A — матрица размера $m \times n$, а e — вектор-столбец длины n, то естественным образом определяется произведение Ae, являющееся вектор-столбцом длины m. Простой подсчет показывает, что $(AB)e = A(Be)$, причем из существования одной из частей этого равенства следует существование другой.

Т е о р е м а 12. *Если вектор-столбец e независим, то из равенства $Ae = Be$ вытекает, что $A = B$.*

Д о к а з а т е л ь с т в о. Данное равенство означает, что

$$a_{i1}e_1 + \ldots + a_{in}e_n = b_{i1}e_1 + \ldots + b_{in}e_n$$

для каждого i и, следовательно, $a_{ij} = b_{ij}$ для всех j по теореме 6.

Пусть теперь φ — линейное отображение линейного пространства L в линейное пространство L'. В пространствах L и L' зафиксируем базисные вектор-столбцы e и e' соответственно. Будем предполагать, что $\dim L = m$ и $\dim L' = n$. Положим

$$\varphi(e) = \begin{Vmatrix} \varphi(e_1) \\ \cdot\ \cdot\ \cdot \\ \varphi(e_m) \end{Vmatrix}.$$

Матрица A размера $m \times n$, строками которой служат координаты векторов, входящих в $\varphi(e)$, в базе e', называется *матрицей линейного отображения φ в базах $\{e, e'\}$*. Таким образом, если A — матрица линейного отображения φ в базах $\{e, e'\}$, то

$$\varphi(e) = Ae'.$$

Если теперь $(\xi_1, \ldots, \xi_m)$ — координаты вектора x в базе e, а $(\xi'_1, \ldots, \xi'_n)$ — координаты вектора $\varphi(x)$ в базе e', то

$$(\xi'_1, \ldots, \xi'_n)e' = \varphi\left(\sum_{i=1}^{m} \xi_i e_i\right) =$$

$$= \sum_{i=1}^{m} \xi_i \varphi(e_i) = (\xi_1, \ldots, \xi_m)\varphi(e) = (\xi_1, \ldots, \xi_m)Ae',$$

откуда

$$(\xi'_1, \ldots, \xi'_n) = (\xi_1, \ldots, \xi_m)A$$

в силу теоремы 12. Это равенство носит название *формулы для вычисления образа вектора при линейном отображении с матрицей A*.

П р и м е р. Пусть L — линейное пространство матриц размера 2×3 над некоторым полем P, L' — пространство 3-мерных строк над тем же полем, E_{ij} — матрица, у которой на месте (i, j) стоит 1,

а на остальных местах — нуль,

$$e = \begin{Vmatrix} E_{11} \\ E_{12} \\ E_{13} \\ E_{21} \\ E_{22} \\ E_{23} \end{Vmatrix}, \quad e' = \begin{Vmatrix} (1, & 0, & 0) \\ (1, & 1, & 0) \\ (1, & 1, & 1) \end{Vmatrix}.$$

$\varphi(X) = (2, 1) X$ для всех $X \in L$.

Нетрудно проверить, что φ — линейное отображение и что

$$\varphi(e) = \begin{Vmatrix} (2, & 0, & 0) \\ (0, & 2, & 0) \\ (0, & 0, & 2) \\ (1, & 0, & 0) \\ (0, & 1, & 0) \\ (0, & 0, & 1) \end{Vmatrix}.$$

Легко проверяемые равенства

$$(2, 0, 0) = 2(1, 0, 0) + 0(1, 1, 0) + 0(1, 1, 1),$$
$$(0, 2, 0) = -2(1, 0, 0) + 2(1, 1, 0) + 0(1, 1, 1),$$
$$(0, 0, 2) = 0(1, 0, 0) + (-2)(1, 1, 0) + 2(1, 1, 1),$$
$$(1, 0, 0) = 1(1, 0, 0) + 0(1, 1, 0) + 0(1, 1, 1),$$
$$(0, 1, 0) = -1(1, 0, 0) + 1(1, 1, 0) + 0(1, 1, 1),$$
$$(0, 0, 1) = 0(1, 0, 0) + (-1)(1, 1, 0) + 1(1, 1, 1)$$

показывает, что матрица

$$A = \begin{Vmatrix} 2 & 0 & 0 \\ -2 & 2 & 0 \\ 0 & -2 & 2 \\ 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{Vmatrix}$$

служит матрицей линейного отображения φ в базах $\{e, e'\}$. Используя формулу для вычисления образа вектора, можно, например, получить

$$\varphi\left(\begin{Vmatrix} 2 & 3 & 0 \\ 1 & 0 & 1 \end{Vmatrix}\right) = \varphi((2, 3, 0, 1, 0, 1)\, e) = (2, 3, 0, 1, 0, 1)\, Ae' =$$
$$= (-1, 5, 1)\, e' = (-1)(1, 0, 0) + 5(1, 1, 0) + (1, 1, 1) = (5, 6, 1).$$

Убедимся теперь, что при фиксированных базах e и e' *всякая матрица размера* $m \times n$ *служит матрицей одного и только одного линейного отображения* $\varphi \in \operatorname{Hom}(L, L')$. В самом деле, если дана матрица A, то положим

$$\varphi\left(\sum_{i=1}^{m} \xi_i e_i\right) = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ij} \xi_i\right) e'_j.$$

Простой подсчет показывает, что $\varphi \in \mathrm{Hom}\,(L, L')$ и что матрица линейного отображения φ в базах $\{e, e'\}$ совпадает с A. Если ψ — другое линейное отображение с той же самой матрицей A, то по формуле вычисления образа вектора имеем

$$\varphi(x) = (\xi_1, \ldots, \xi_m)\, Ae' = \psi(x)$$

для всех $x \in L$, откуда $\varphi = \psi$.

Теорема 13. *Если зафиксированы базы e и e' в пространствах L и L' над полем P соответственно, $\dim L = m$ и $\dim L' = n$, то отображение Φ, ставящее в соответствие каждому линейному отображению $\varphi \in \mathrm{Hom}\,(L, L')$ его матрицу в базах $\{e, e'\}$, является изоморфизмом линейного пространства $\mathrm{Hom}\,(L, L')$ на линейное пространство $P_{m\times n}$ всех матриц размера $m \times n$ над полем P.*

Доказательство. Проведенными выше рассмотрениями уже установлено, что Φ осуществляет взаимно однозначное отображение множества $\mathrm{Hom}\,(L, L')$ на множество $P_{m\times n}$ всех матриц размера $m \times n$. Если теперь $\varphi, \psi \in \mathrm{Hom}\,(L, L')$, $\chi = \varphi + \psi$, $\lambda \in P$, $\lambda\varphi = \omega$, $\Phi(\varphi) = A$, $\Phi(\psi) = B$, $\Phi(\chi) = C$ и $\Phi(\omega) = D$, то, учитывая определение операций в пространстве $\mathrm{Hom}\,(L, L')$, имеем

$$Ce' = \chi(e) = \varphi(e) + \psi(e) = Ae' + Be' = (A + B)\, e'$$

и

$$De' = \omega(e) = (\lambda\varphi)(e) = \lambda(\varphi(e)) = \lambda(Ae') = (\lambda A)\, e',$$

откуда $C = A + B$ и $D = \lambda A$ по теореме 12. Таким образом, Φ оказывается гомоморфизмом, а следовательно, и изоморфизмом линейных пространств.

Теорема 14. *Пусть L, L' и L'' — линейные пространства над полем P, $\varphi \in \mathrm{Hom}\,(L, L')$, $\psi \in \mathrm{Hom}\,(L', L'')$, A — матрица линейного отображения φ в базах $\{e, e'\}$, B — матрица линейного отображения ψ в базах $\{e', e''\}$ и C — матрица линейного отображения $\varphi\psi$ в базах $\{e, e''\}$. Тогда $C = AB$.*

Доказательство. Достаточно заметить, что

$$Ce'' = e(\varphi\psi) = (e\varphi)\,\psi = (Ae')\psi = \\ = A(e'\psi) = A(Be'') = (AB)\, e'',$$

и принять во внимание теорему 12.

Если теперь L — линейное пространство над полем P, то линейное преобразование $\varphi \in \mathrm{Hom}\,(L, L)$ является линей-

ным отображением L в L. Матрица этого линейного отображения в базах $\{e, e\}$, где e — некоторая база пространства L, называется *матрицей линейного преобразования* φ *в базе* e.

Пример. Пусть L — линейное пространство матриц второго порядка над некоторым полем P, $\{E_{11}, E_{12}, E_{21}, E_{22}\}$ — база пространства L и $\varphi(X) = X^*$ для всякой матрицы X из L. Тогда

$$\varphi\left(\left\|\begin{matrix} E_{11} \\ E_{12} \\ E_{21} \\ E_{22} \end{matrix}\right\|\right) = \left\|\begin{matrix} E_{11} \\ E_{21} \\ E_{12} \\ E_{22} \end{matrix}\right\|$$

и, следовательно,

$$A = \left\|\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}\right\|$$

— матрица линейного преобразования φ в данной базе. По формуле вычисления образа вектора имеем

$$\varphi\left(\left\|\begin{matrix} 2 & 2 \\ 1 & 0 \end{matrix}\right\|\right) = (2, 2, 1, 0)\, Ae = (2, 1, 2, 0)\, e = \left\|\begin{matrix} 2 & 1 \\ 2 & 0 \end{matrix}\right\|,$$

как и следовало ожидать.

Теорема 15. *Если в* n*-мерном линейном пространстве* L *над полем* P *зафиксирована база* e, *то отображение* Φ, *ставящее в соответствие каждому линейному преобразованию* $\varphi \in \mathrm{Hom}(L, L)$ *его матрицу в базе* e, *является изоморфизмом кольца* $\mathrm{Hom}(L, L)$ *на кольцо* P_n *квадратных матриц порядка* n *над полем* P.

Доказательство. Согласно теореме II.5.9, $\mathrm{Hom}(L, L)$ является кольцом. В силу теоремы 13, Φ осуществляет изоморфизм абелевых групп (и даже линейных пространств), а из теоремы 14 вытекает, что $\Phi(\varphi\psi) = \Phi(\varphi)\Phi(\psi)$.

Если в линейном пространстве L зафиксирован базисный вектор-столбец e, то, ввиду теоремы 6, каждому вектору x из L однозначно соответствует строка $(\xi_1, \ldots, \xi_n)$, составленная из его координат в базе e. При этом

$$x = (\xi_1, \ldots, \xi_n)\, e.$$

Пусть теперь e и f — два базисных вектор-столбца и T — матрица, строками которой служат координаты векторов, входящих в f, в базе e. Матрица T называется *матрицей перехода* от базы e к базе f. При этом имеет место равенство $f = Te$. Если U — матрица перехода от базы f

к базе e, то $e = Uf$. Отсюда

$$Ee = e = Uf = U(Te) = (UT)e$$

и, согласно теореме 12, $UT = E$. Ввиду теоремы I.3.14, матрица перехода всегда невырожденная. Наоборот, если дана невырожденная матрица T и базисный вектор-столбец e, то рассмотрим вектор-столбец

$$f = Te.$$

Если векторы, входящие в f, линейно зависимы, то найдется ненулевая строка $(\lambda_1, \ldots, \lambda_n)$ такая, что

$$(\lambda_1, \ldots, \lambda_n) f = 0.$$

Отсюда $(0, \ldots, 0) e = (\lambda_1, \ldots, \lambda_n) Te$, т. е., согласно теореме 12, $(0, \ldots, 0) = (\lambda_1, \ldots, \lambda_n) T$, а значит, $(\lambda_1, \ldots, \lambda_n) = (0, \ldots, 0) T^{-1} = (0, \ldots, 0)$, что противоречит выбору строки $(\lambda_1, \ldots, \lambda_n)$. Таким образом, вектор-столбец f независим. Следовательно, $\dim(\mathcal{L}(f_1, \ldots, f_n)) = n$ и, ввиду теоремы 10, $\mathcal{L}(f_1, \ldots, f_n) = L$. Таким образом, f оказывается базисным вектор-столбцом, причем T служит матрицей перехода от базы e к базе f. Этим доказано, что *всякая невырожденная матрица служит матрицей перехода.*

Если T — матрица перехода от базы e к базе e', $(\xi_1, \ldots, \xi_n)$ — координаты вектора x в базе e, а $(\xi_1', \ldots, \xi_n')$ — его координаты в базе e', то

$$e' = Te \quad \text{и} \quad x = (\xi_1, \ldots, \xi_n) e = (\xi_1', \ldots, \xi_n') e'.$$

Отсюда

$$(\xi_1, \ldots, \xi_n) e = (\xi_1', \ldots, \xi_n') Te$$

и, следовательно,

$$(\xi_1, \ldots, \xi_n) = (\xi_1', \ldots, \xi_n') T.$$

Эта формула называется *формулой изменения координат при изменении базы.*

Пусть L — линейное пространство над полем P, $\varphi \in \mathrm{Hom}(L, L)$, а A и B — матрицы линейного преобразования φ в базах e и f соответственно. Если T — матрица перехода от базы e к базе f, то

$$Bf = \varphi(f) = \varphi(Te) = T\varphi(e) = TAe = TAT^{-1}f,$$

откуда, согласно теореме 12, $B = TAT^{-1}$. Эта формула носит название *формулы изменения матрицы линейного преобразования при изменении базы.*

Пусть φ — линейное преобразование n-мерного линейного пространства L над полем P и A — матрица этого линейного преобразования в базе $\boldsymbol{e}$. Определитель $|A - tE|$ оказывается многочленом степени n над полем P относительно t. Если B — матрица того же самого линейного преобразования φ в базе $\boldsymbol{f}$, то, как только что показано, $B = TAT^{-1}$, где T — матрица перехода от $\boldsymbol{e}$ к $\boldsymbol{f}$. В силу теоремы I.3.14 и соотношений, установленных в конце § 3 гл. I,

$$|A - tE| = |T||A - tE||T^{-1}| = |T(A - tE)T^{-1}| = \\ = |TAT^{-1} - T(tE)T^{-1}| = |B - tE|,$$

Таким образом, многочлен $|A - tE|$ не меняется при изменении базы, что позволяет назвать его *характеристическим многочленом линейного преобразования* φ. Корни характеристического многочлена линейного преобразования φ называются *характеристическими корнями* этого линейного преобразования.

Допустим теперь, что рассматривается n-мерное линейное пространство над полем комплексных чисел $\boldsymbol{C}$. Тогда каждое линейное преобразование φ имеет в точности n характеристических корней (если каждый корень считать столько раз, какова его кратность) *). Сумма всех этих корней называется *следом* линейного преобразования φ и обозначается через $\mathrm{Tr}\,\varphi$ **). По формуле Виета ***) сумма всех характеристических корней равняется коэффициенту характеристического многочлена, стоящему при t^{n-1}, умноженному на $\frac{-1}{(-1)^n} = (-1)^{n-1}$. С другой стороны, если A — матрица линейного преобразования φ в некоторой базе, то, вычисляя определитель $|A - tE|$ с помощью теоремы I.2.9, нетрудно заметить, что t^{n-1} возникает лишь при вычислении произведения элементов, стоящих на главной диагонали. Поскольку это произведение равно $(a_{11} - t) \ldots (a_{nn} - t)$, то коэффициент при t^{n-1} равен $(-1)^{n-1}(a_{11} + \ldots + a_{nn}) = (-1)^{n-1}\,\mathrm{Tr}\,\varphi$.

---

*) См. с. 157 учебника А. Г. Куроша или с. 273 учебника А. И. Кострикина.

**) Чтобы эти определения были пригодны для любого поля, надо рассматривать корни в поле разложения характеристического многочлена (см. с. 304 учебника А. Г. Куроша или с. 276 учебника А. И. Кострикина).

***) См. с. 159 и 305 учебника А. Г. Куроша или с. 253 учебника А. И. Кострикина.

Поскольку, как было отмечено, характеристический многочлен от базы не зависит, нами доказана

Теорема 16. *След линейного преобразования линейного пространства над полем* C *равен сумме диагональных элементов матрицы этого линейного преобразования в любой базе.*

Теорема 17. *Пусть* φ *— линейное преобразование линейного пространства* L *над полем* C. *Число* $\lambda \in C$ *является характеристическим корнем линейного преобразования* φ *тогда и только тогда, когда существует ненулевой вектор* $v \in L$ *такой, что* $\varphi(v) = \lambda v$ *).

Доказательство. Пусть A — матрица линейного преобразования в некоторой базе e и $\lambda \in C$. Рассмотрим систему линейных уравнений:

$$(A - \lambda E)^* \begin{Vmatrix} x_1 \\ \dots \\ x_n \end{Vmatrix} = \begin{Vmatrix} 0 \\ \dots \\ 0 \end{Vmatrix}. \qquad (*)$$

Из теоремы I.3.7 легко вывести, что строка $(\alpha_1, \dots, \alpha_n)$— решение этой системы тогда и только тогда, когда

$$(\alpha_1, \dots, \alpha_n)(A - \lambda E) = (0, \dots, 0).$$

Ввиду теоремы 15, $(A - \lambda E)$ — матрица линейного преобразования $\varphi - \lambda 1_L$ в базе e. Поэтому формула для вычисления образа вектора показывает, что вектор

$$v = \alpha_1 e_1 + \dots + \alpha_n e_n$$

удовлетворяет соотношению $(\varphi - \lambda 1_L)(v) = 0$ или, что то же самое, $\varphi(v) = \lambda v$ тогда и только тогда, когда $(\alpha_1, \dots, \alpha_n)$ — решение системы $(*)$. Значит, согласно следствию теоремы I.3.5, вектор v может быть выбран ненулевым в том и только в том случае, когда $|A - \lambda E| = 0$, или, что то же самое, когда λ — характеристический корень линейного преобразования φ.

Теорема 18. *Если* $\lambda_1, \dots, \lambda_n$ *— все характеристические корни взаимно однозначного линейного преобразования* φ *линейного пространства над полем* C, *причем каждый корень выписывается столько раз, какова его кратность, то* $\lambda_1^{-1}, \dots, \lambda_n^{-1}$ *— все характеристические корни линейного преобразования* φ^{-1}, *причем каждый корень выписывается столько раз, какова его кратность.*

---

*) Вектор v называется *собственным вектором* линейного преобразования φ, отвечающим характеристическому корню λ. В связи с этим число λ часто называют *собственным значением* линейного преобразования φ.

Доказательство. Поскольку $\operatorname{Ker}\varphi = 0$, то, ввиду теоремы 17, $\lambda_i \neq 0$ для всех i. Пусть A — матрица линейного преобразования φ в некоторой базе. Тогда *)

$$|A - tE| = (-1)^n(t - \lambda_1)\ldots(t - \lambda_n).$$

Согласно теореме 15, A^{-1} служит матрицей линейного преобразования φ^{-1} в той же базе. Ведя вычисления в поле рациональных дробей **) и принимая во внимание свойство III определителя и теорему 1.3.14, получаем

$$\begin{aligned}|A^{-1} - tE| &= |A^{-1}||E - tA| = \\ &= t^n|A^{-1}|(-1)^n\left|A - \frac{1}{t}E\right| = \\ &= t^n|A^{-1}|\left(\frac{1}{t} - \lambda_1\right)\ldots\left(\frac{1}{t} - \lambda_n\right) = \\ &= (-1)^n|A^{-1}|\lambda_1\ldots\lambda_n(t - \lambda_1^{-1})\ldots(t - \lambda_n^{-1}),\end{aligned}$$

чем и завершается доказательство.

Теорема 19. *Если* $\lambda_1, \ldots, \lambda_n$ — *все характеристические корни линейного преобразования* φ *линейного пространства* L *над полем* C, *причем каждый корень выписывается столько раз, какова его кратность,* $|\lambda_k| = 1$ ***) *для всех* k *и* $|\operatorname{Tr}\varphi| = n$, *то* $\lambda_1 = \ldots = \lambda_n$.

Доказательство. Сначала установим следующее утверждение.

Лемма. *Если* $|\lambda| = |\mu| = 1$ *и* $|\lambda + \mu| = 2$, *то* $\lambda = \mu$.

Действительно,

$$\begin{aligned}4 + |\lambda - \mu|^2 &= |\lambda + \mu|^2 + |\lambda - \mu|^2 = \\ &= (\lambda + \mu)(\bar{\lambda} + \bar{\mu}) + (\lambda - \mu)(\bar{\lambda} - \bar{\mu}) = \\ &= \lambda\bar{\lambda} + \lambda\bar{\mu} + \bar{\lambda}\mu + \mu\bar{\mu} + \lambda\bar{\lambda} - \bar{\lambda}\mu - \lambda\bar{\mu} + \mu\bar{\mu} = \\ &= 2(|\lambda|^2 + |\mu|^2) = 4.\end{aligned}$$

Отсюда $|\lambda - \mu| = 0$, а значит, $\lambda = \mu$ по свойству (1) нормы (см. с. 100).

Обратимся к доказательству теоремы. Если $|\lambda_k + \lambda_{k+1}| < 2$ для некоторого k, то, ввиду свойства (3)

---

*) Как известно, если $\lambda_1, \ldots, \lambda_n$ — все корни многочлена $F(t)$ со старшим коэффициентом a, причем каждый корень выписывается столько раз, какова его кратность, то $F(t) = a(t - \lambda_1)\ldots(t - \lambda_n)$ (см. с. 156 учебника А. Г. Куроша или с. 282 учебника А. И. Кострикина).

**) См. § 50 гл. X учебника А. Г. Куроша или п. 2 § 4 гл. 5 учебника А. И. Кострикина.

***) Здесь $|z|$ — норма комплексного числа z.

нормы,

$$n = |\operatorname{Tr}\varphi| = |\lambda_1 + \ldots + \lambda_n| \leqslant$$
$$\leqslant |\lambda_1 + \ldots + \lambda_{k-1}| + |\lambda_k + \lambda_{k+1}| + |\lambda_{k+2} + \ldots + \lambda_n| <$$
$$< (k-1) + 2 + (n - (k+1)) = n,$$

что невозможно. Следовательно, $|\lambda_k + \lambda_{k+1}| = 2$ для всех k и, согласно лемме, $\lambda_k = \lambda_{k+1}$. Таким образом, $\lambda_1 = \ldots = \lambda_n$, что и требовалось.

Теорема 20. *Если φ — линейное преобразование n-мерного линейного пространства L над полем C, $\varphi^m = 1_L$ для некоторого m и все характеристические корни линейного преобразования φ равны λ, то $\varphi = \lambda 1_L$, а λ оказывается корнем степени m из единицы.*

Доказательство. Пусть A — матрица линейного преобразования φ в некоторой базе. Если $\xi_1, \ldots, \xi_m$ — все корни степени m из единицы, то имеем равенство многочленов *)

$$(t - \xi_1) \ldots (t - \xi_m) = t^m - 1.$$

Поскольку $A^m = E$ по теореме 15, то попарная перестановочность матриц $A, \xi_1 E, \ldots, \xi_m E$, вытекающая из теоремы II.4.12, позволяет записать

$$(A - \xi_1 E) \ldots (A - \xi_m E) = A^m - E = 0. \qquad (*)$$

В силу теоремы I.3.14 отсюда следует, что, скажем, $|A - \xi_1 E| = 0$. Но тогда $\xi_1 = \lambda$, $|A - \xi_i E| \neq 0$ при $i \geqslant 2$, и по теореме I.3.13 существуют матрицы $(A - \xi_i E)^{-1}$. Умножая равенство $(*)$ справа на

$$(A - \xi_m E)^{-1} \ldots (A - \xi_2 E)^{-1},$$

получим

$$A - \xi_1 E = 0,$$

откуда в силу теоремы 15 имеем $\varphi = \xi_1 1_L$, что и требовалось.

Теорема 21 (теорема о ранге). *Ранг матрицы равен размерности линейной оболочки ее строк.*

Доказательство. Если A — матрица, то обозначим через $\mathcal{L}(A)$ линейную оболочку ее строк.

Лемма 1. *Если от матрицы A к матрице B перешли конечным числом элементарных преобразований строк, то $\mathcal{L}(B) \subseteq \mathcal{L}(A)$.*

---

*) См. примечание *) на с. 183.

В самом деле, очевидно, достаточно доказать лемму для случая, когда применено только одно элементарное преобразование. Если это перемена местами двух строк, то утверждение леммы тривиально, ибо матрицы A и B состоят из одних и тех же строк. Если же к i-й строке a_i матрицы A прибавлена ее j-я строка a_j, умноженная на λ, то для i-й строки b_i матрицы B имеем $b_i = a_i + \lambda a_j \in \mathcal{L}(A)$ и $\mathcal{L}(B) \subseteq \mathcal{L}(A)$ в силу теоремы II.5.2.

Из леммы 1 и теоремы I.1.2 вытекает

Лемма 2. *Если от матрицы A к матрице B перешли конечным числом элементарных преобразований строк, то $\mathcal{L}(B) = \mathcal{L}(A)$.*

Лемма 3. *Если ступенчатая матрица S содержит r ненулевых строк, то* $\dim \mathcal{L}(S) = r$.

Для доказательства, очевидно, достаточно установить линейную независимость ненулевых строк $s_1, \ldots, s_r$ матрицы S. Но если

$$s_i = (s_{i1}, \ldots, s_{in}),$$

s_{ik_i} — первый ненулевой элемент строки s_i и

$$\lambda_1 s_1 + \ldots + \lambda_r s_r = 0,$$

то

$$\begin{aligned}
&\lambda_1 s_{1k_1} = 0,\\
&\lambda_1 s_{1k_2} + \lambda_2 s_{2k_2} = 0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\lambda_1 s_{1k_{r-1}} + \lambda_2 s_{2k_{r-1}} + \ldots + \lambda_{r-1} s_{r-1\,k_{r-1}} = 0,\\
&\lambda_1 s_{1k_r} + \lambda_2 s_{2k_r} + \ldots + \lambda_{r-1} s_{r-1\,k_r} + \lambda_r s_{rk_r} = 0,
\end{aligned}$$

откуда последовательно получаем, что $\lambda_1 = 0$, $\lambda_2 = 0, \ldots$ $\ldots, \lambda_{r-1} = 0$, $\lambda_r = 0$.

Теперь для доказательства теоремы замечаем, что, согласно лемме 2, для данной матрицы A имеем $\mathcal{L}(A) = \mathcal{L}(S)$, где S — ступенчатая матрица, к которой согласно теореме I.1.1 можно перейти от A элементарными преобразованиями строк. Из теорем I.3.1 и I.3.3 и леммы 3 получаем

$$\text{ранг } A = \text{ранг } S = \dim \mathcal{L}(S) = \dim \mathcal{L}(A).$$

Если V — подпространство линейного пространства L и a — вектор из L, то смежный класс $a + V$ называется *линейным многообразием*.

Теорема 22. *Совокупность всех решений однородной (произвольной) системы m линейных уравнений*

от n неизвестных с коэффициентами из поля P образует подпространство (пусто или образует линейное многообразие) пространства n-мерных строк над полем P. Размерность пространства решений равна $n - r$, где r — ранг матрицы данной системы.

Доказательство. Если A — матрица данной однородной системы линейных уравнений с n неизвестными над полем P, $\lambda \in P$, а $a = (\alpha_1, \ldots, \alpha_n)$ и $b = (\beta_1, \ldots, \beta_n)$ — решения этой системы, то, подставляя строки $a + b$ и λa в i-е уравнение данной системы, получаем

$$a_{i1}(\alpha_1 + \beta_1) + \ldots + a_{in}(\alpha_n + \beta_n) =$$
$$= (a_{i1}\alpha_1 + \ldots + a_{in}\alpha_n) + (a_{i1}\beta_1 + \ldots + a_{in}\beta_n) =$$
$$= 0 + 0 = 0$$

и

$$a_{i1}(\lambda\alpha_1) + \ldots + a_{in}(\lambda\alpha_n) = \lambda(a_{i1}\alpha_1 + \ldots + a_{in}\alpha_n) =$$
$$= \lambda 0 = 0.$$

Таким образом, $a + b$ и λa оказываются решениями, что и доказывает справедливость первого утверждения теоремы об однородных системах. Если дана неоднородная система и она несовместна, то множество ее решений пусто. Если же она совместна, то выберем одно из ее решений, скажем строку c, и обозначим через W пространство решений однородной системы, полученной из данной системы заменой свободных членов нулями. Легко проверить, что каждый вектор из линейного многообразия $c + W$ служит решением данной системы. Наоборот, если u — произвольное решение этой системы, то разность $u - c$ оказывается решением соответствующей однородной системы, т. е. $u - c \in W$, откуда $u \in c + W$. Для доказательства второго утверждения теоремы заметим, что, согласно теореме I.3.6, $n - r$ неизвестных нашей системы являются свободными. Поскольку нумерация неизвестных не имеет значения, можно считать, что главными являются неизвестные $x_1, \ldots, x_r$. Пусть V — пространство $(n - r)$-мерных строк. Если $u = (u_1, \ldots, u_{n-r})$, то обозначим через $\varphi(u)$ то единственное решение данной системы, которое получается после придания свободным неизвестным значений $u_1, \ldots, u_{n-r}$. Поскольку

$$\varphi(u) = (\ldots, u_1, \ldots, u_{n-r}),$$

φ оказывается взаимно однозначным отображением пространства V на пространство решений. Пусть теперь u, $v \in V$. Поскольку решения $\varphi(u) + \varphi(v)$ и $\varphi(u + v)$ имеют одни и те же значения свободных неизвестных, они должны совпадать, т. е.

$$\varphi(u + v) = \varphi(u) + \varphi(v).$$

Аналогично доказывается, что $\varphi(\lambda u) = \lambda\varphi(u)$ для любого $\lambda \in P$. Таким образом, отображение φ линейно, т. е. оказывается изоморфизмом. Остается принять во внимание следствие 1 теоремы 9.

Базу пространства решений однородной системы линейных уравнений часто называют фундаментальной системой решений.

Т е о р е м а 23. *Всякое подпространство S пространства n-мерных строк V над полем P служит пространством решений некоторой однородной системы линейных уравнений от n неизвестных с коэффициентами из поля P.*

Д о к а з а т е л ь с т в о. По теореме 7 $V = S \oplus T$, где T — некоторое подпространство пространства V. Если $\boldsymbol{f}$ и $\boldsymbol{g}$ — базы пространств S и T соответственно, то по теореме 8 их объединение служит базой пространства V. Как отмечено на с. 177, существует линейное преобразование φ пространства V такое, что $\varphi(f) = 0$ для всех $f \in \boldsymbol{f}$ и $\varphi(g) = g$ для всех $g \in \boldsymbol{g}$. Ясно, что $\varphi(x) = 0$ для всех $x \in S$ и $\varphi(y) = y$ для всех $y \in T$. Если же $\varphi(v) = 0$ для некоторого $v \in V$, то, записав $v = s + t$, где $s \in S$ и $t \in T$, получим

$$0 = \varphi(v) = \varphi(s) + \varphi(t) = 0 + t = t,$$

откуда $v \in S$. Таким образом, $v \in S$ тогда и только тогда, когда $\varphi(v) = 0$. Теперь обозначим через A матрицу линейного преобразования φ в базе $\boldsymbol{e} = \{e_1, \ldots, e_n\}$, где

$$e_i = (\underbrace{0, \ldots, 0}_{i-1}, 1, 0, \ldots, 0).$$

Используя формулу для вычисления образа вектора (см. с. 176), заметим, что равенство

$$\varphi((\alpha_1, \ldots, \alpha_n)) = (\beta_1, \ldots, \beta_n)$$

равносильно равенству

$$(\alpha_1, \ldots, \alpha_n)\, A = (\beta_1, \ldots, \beta_n),$$

которое в силу второго утверждения теоремы I.3.7 равносильно равенству

$$A^* \begin{Vmatrix} \alpha_1 \\ \dots \\ \alpha_n \end{Vmatrix} = \begin{Vmatrix} \beta_1 \\ \dots \\ \beta_n \end{Vmatrix}.$$

Следовательно, $(\alpha_1, \dots, \alpha_n) \in S$ тогда и только тогда, когда

$$A^* \begin{Vmatrix} \alpha_1 \\ \dots \\ \alpha_n \end{Vmatrix} = \begin{Vmatrix} 0 \\ \dots \\ 0 \end{Vmatrix},$$

т. е. тогда и только тогда, когда $(\alpha_1, \dots, \alpha_n)$ служит решением однородной системы линейных уравнений:

$$\begin{cases} a_{11}^* x_1 + \dots + a_{1n}^* x_n = 0, \\ \dots\dots\dots\dots\dots\dots \\ a_{n1}^* x_1 + \dots + a_{nn}^* x_n = 0. \end{cases}$$

Теорема 24. *Всякое линейное многообразие пространства n-мерных строк над полем P служит многообразием решений некоторой системы линейных уравнений от n неизвестных с коэффициентами из поля P.*

Доказательство. Рассмотрим многообразие $M = b + S$, где b — вектор, а S — подпространство. В силу теоремы 23, подпространство S служит пространством решений системы

$$A \begin{Vmatrix} x_1 \\ \dots \\ x_n \end{Vmatrix} = \begin{Vmatrix} 0 \\ \dots \\ 0 \end{Vmatrix}. \qquad (*)$$

Пусть $b = (\beta_1, \dots, \beta_n)$. Простой подсчет показывает, что M совпадает с многообразием решений системы

$$A \begin{Vmatrix} x_1 \\ \dots \\ x_n \end{Vmatrix} = A \begin{Vmatrix} \beta_1 \\ \dots \\ \beta_n \end{Vmatrix}.$$

Действительно, если $a = (\alpha_1, \dots, \alpha_n)$ — решение этой системы, то вектор $s = (\alpha_1 - \beta_1, \dots, \alpha_n - \beta_n)$, будучи решением системы $(*)$, лежит в S. Следовательно, $a = b + s \in M$. Если же $a = (\alpha_1, \dots, \alpha_n) \in M$, то $a = b +$

$+ s$, где $s = (\xi_1, \ldots, \xi_n) \in S$. Отсюда

$$A \begin{Vmatrix} \alpha_1 \\ \cdots \\ \alpha_n \end{Vmatrix} = A \begin{Vmatrix} \beta_1 \\ \cdots \\ \beta_n \end{Vmatrix} + A \begin{Vmatrix} \xi_1 \\ \cdots \\ \xi_n \end{Vmatrix} = A \begin{Vmatrix} \beta_1 \\ \cdots \\ \beta_n \end{Vmatrix},$$

ибо $(\xi_1, \ldots, \xi_n)$ — решение системы (*).

Упражнения

1. Если линейное пространство бесконечномерно, то оно содержит подпространства любой конечной размерности.

2. Если система векторов $\{a_1, \ldots, a_m\}$ линейно независима, а система $\{a_1, \ldots, a_m, b_1, \ldots, b_n\}$ линейно зависима, то хотя бы один из добавленных векторов линейно выражается через все отличные от него (но не обязательно через $a_1, \ldots, a_m$).

3. Если V — подпространство линейного пространства L, то $\dim L = \dim V + \dim (L/V)$.

4. Если U и V — подпространства линейного пространства L, то

$$\dim (U + V) + \dim (U \cap V) = \dim U + \dim V.$$

5. Пусть V — линейное пространство n-мерных строк над полем P и φ — изоморфизм поля P на себя. Определим новое умножение элементов из P на элементы из V, полагая $\lambda \circ v = \varphi(\lambda) v$. Убедиться, что это определение превращает абелеву группу V в линейное пространство V' над полем P, и привести конкретный изоморфизм линейного пространства V на пространство V'.

6. Если L и L' — линейные пространства и $L = U \oplus V$, то линейное пространство $\mathrm{Hom}(L, L')$ изоморфно внешней прямой сумме $\mathrm{Hom}(U, L') \oplus \mathrm{Hom}(V, L')$, а линейное пространство $\mathrm{Hom}(L', L)$ — внешней прямой сумме $\mathrm{Hom}(L', U) \oplus \mathrm{Hom}(L', V)$. Кроме того, кольцо $\mathrm{Hom}(L, L)$ изоморфно кольцу матриц вида

$$\begin{Vmatrix} \varphi & \psi \\ \chi & \rho \end{Vmatrix},$$

где $\varphi \in \mathrm{Hom}(U, U)$, $\psi \in \mathrm{Hom}(U, V)$, $\chi \in \mathrm{Hom}(V, U)$, $\rho \in \mathrm{Hom}(V, V)$, а операции определены так же, как для обычных матриц.

7. Линейное преобразование φ линейного пространства L над полем P имеет одну и ту же матрицу во всех базах тогда и только тогда, когда $\varphi = \lambda 1_L$ для некоторого $\lambda \in P$.

8. Пусть φ — линейное преобразование линейного пространства L над полем комплексных чисел C. Если $\lambda \in C$, то положим $V(\lambda) = \{x \mid x \in L, \ \varphi(x) = \lambda x\}$. Доказать, что $V(\lambda)$ — подпространство и что $V(\lambda) \cap V(\mu) = 0$, если $\lambda \neq \mu$.

9. Если линейное преобразование φ линейного пространства над полем комплексных чисел нильпотентно (т. е. $\varphi^m = 0$ для некоторого m), то все его характеристические корни равны нулю. Установить справедливость обратного утверждения.

10. Доказать, что $\mathrm{Tr}(\varphi\psi) = \mathrm{Tr}(\psi\varphi)$ для любых линейных преобразований φ и ψ.

11. Пусть $a + U$ и $b + V$ — линейные многообразия. Доказать, что $a + U = b + V$ тогда и только тогда, когда $U = V$ и $a - b \in U$.

12. Доказать, что непустое подмножество M линейного пространства L над полем P является линейным многообразием тогда и только тогда, когда из соотношений

$$a_1, \ldots, a_m \in M, \qquad \lambda_1, \ldots, \lambda_m \in P$$

и

$$\lambda_1 + \ldots + \lambda_m = 1$$

вытекает, что

$$\lambda_1 a_1 + \ldots + \lambda_m a_m \in M.$$

13. Пересечение двух (и даже любого множества) линейных многообразий или пусто, или является линейным многообразием.

14. Если M' и M'' — линейные многообразия, то среди линейных многообразий, содержащих объединение $M' \cup M''$, существует наименьшее.

15. Указать систему линейных уравнений, описывающую пересечение линейных подпространств $S \cap T$, если указаны системы линейных уравнений, описывающие подпространства S и T.

§ 2. Линейные алгебры и модули над ними

Если кольцо R является конечномерным линейным пространством над полем P и для любых $\lambda \in P$ и $x, y \in R$ имеет место $(\lambda x)\, y = \lambda\,(xy) = x\,(\lambda y)$, то R называется *линейной алгеброй* над полем P *). Нетрудно убедиться, что поле комплексных чисел является алгеброй над полем действительных чисел. Другой пример доставляют квадратные матрицы над полем.

Теорема 1. *Линейная алгебра R над полем P, обладающая единицей* 1, *отличной от* 0, *содержит подполе $P \cdot 1$, изоморфное полю P.*

Доказательство. Построим отображение φ поля P в алгебру R, полагая $\varphi(\lambda) = \lambda 1$. Тогда

$$\varphi(\lambda + \mu) = (\lambda + \mu)1 = \lambda 1 + \mu 1 = \varphi(\lambda) + \varphi(\mu)$$

и

$$\varphi(\lambda\mu) = (\lambda\mu)1 = \lambda(\mu 1) = \lambda(1 \cdot (\mu 1)) = (\lambda 1) \cdot (\mu 1) = \varphi(\lambda) \cdot \varphi(\mu),$$

т. е. φ — гомоморфизм колец. Если $\varphi(\lambda) = \varphi(\mu)$, т. е. $\lambda 1 = \mu 1$, то $\lambda = \mu$ ввиду теоремы 1 из § 1. Следовательно, φ — гомоморфное вложение. Но тогда ясно, что поле P и кольцо $\operatorname{Im}\varphi = P1$ изоморфны.

Подмножество U линейной алгебры R над полем P называется *подалгеброй*, если оно является подкольцом кольца R и подпространством линейного пространства R.

*) В современной литературе требование конечности размерности в определение линейной алгебры не включается.

Ясно, что подалгебра является линейной алгеброй относительно операций, определенных в исходной алгебре. Из теорем II.4.1 и II.5.1 вытекает

Теорема 2. *Пересечение любого множества подалгебр является подалгеброй.*

Левым, *правым* и *двусторонним идеалом* линейной алгебры R над полем P назовем соответственно левый, правый и двусторонний идеал кольца R, являющийся подпространством линейного пространства R. Вообще говоря, идеал кольца не обязан быть идеалом алгебры. В самом деле, пусть $\boldsymbol{R}$ — множество действительных чисел, рассматриваемое как линейное пространство над полем действительных чисел. Положив $ab = 0$ для всех $a, b \in \boldsymbol{R}$, превратим $\boldsymbol{R}$ в алгебру над полем действительных чисел. Тогда множество всех целых чисел оказывается идеалом кольца $\boldsymbol{R}$, хотя идеалом алгебры $\boldsymbol{R}$ не является. Однако положение меняется, если R — алгебра с единицей. Действительно, согласно теореме 1, линейная алгебра R с единицей над полем P содержит поле P. Следовательно, для каждого правого или левого модуля над кольцом R и, в частности, для любого левого или правого идеала кольца R определено умножение на элементы поля P. Имея в виду это умножение, получаем следующее утверждение.

Теорема 3. *Пусть R — линейная алгебра с единицей над полем P. Тогда всякий левый, правый и двусторонний идеал кольца R является соответственно левым, правым и двусторонним идеалом алгебры R. Всякий правый (левый) модуль над кольцом R является линейным пространством над полем P, причем*

$$\lambda (ar) = (\lambda a) r = a (\lambda r) \qquad (\lambda (ra) = r (\lambda a) = (\lambda r) a)$$

для любых $a \in A$, $r \in R$, $\lambda \in P$.

Отображение φ линейной алгебры R над полем P в линейную алгебру R' над тем же полем называется *гомоморфизмом линейных алгебр*, если φ является гомоморфизмом колец и гомоморфизмом линейных пространств одновременно. Взаимно однозначный гомоморфизм называется *изоморфизмом*. Если существует изоморфизм линейной алгебры R на линейную алгебру R', то эти алгебры называются *изоморфными* *).

Из теорем II.4.2 и II.5.5 вытекает

---

*) См. примечание на с. 60.

Теорема 4. *Если* φ: $R \to R'$ — *гомоморфизм линейных алгебр, то* $\operatorname{Im}\varphi$ — *подалгебра линейной алгебры* R'.

Ввиду теорем 3, II.4.3 и II.5.6 имеем следующее утверждение.

Теорема 5. *Допустимыми разбиениями линейной алгебры* R *с единицей являются разбиения по некоторому идеалу кольца* R. *Факторкольцо линейной алгебры над полем* P *по любому идеалу оказывается линейной алгеброй над тем же самым полем.* (Это факторкольцо естественно называть *факторалгеброй.*)

Из теорем II.4.4 и II.5.7 вытекает

Теорема 6 (теорема о гомоморфизме для линейных алгебр). *Если* φ: $R \to R'$ — *гомоморфное наложение линейных алгебр,* $\operatorname{Ker}\varphi$ — *идеал, являющийся ядром этого гомоморфизма, и* π: $R \to R/\operatorname{Ker}\varphi$ — *естественный гомоморфизм, то существует изоморфизм* χ: $R' \to R/\operatorname{Ker}\varphi$ *такой, что* $\varphi\chi = \pi$.

Теорема 7. *Пусть* L — *линейное пространство над полем* P. *Тогда* $\operatorname{Hom}(L, L)$ — *линейная алгебра над полем* P. *Если* $\dim L = n$ *и* e — *база линейного пространства* L, *то отображение* Φ, *ставящее в соответствие каждому линейному преобразованию* $\varphi \in \operatorname{Hom}(L, L)$ *его матрицу в базе* e, *является изоморфизмом линейной алгебры* $\operatorname{Hom}(L, L)$ *на линейную алгебру* P_n *квадратных матриц порядка* n *над полем* P.

Доказательство. В силу теорем II.5.9 и 11 из § 1, множество $\operatorname{Hom}(L, L)$ является как кольцом, так и линейным пространством над полем P. При этом $\dim \operatorname{Hom}(L, L) = n^2$ в силу теоремы 13 из § 1. Кроме того, для любых $x \in L$, $\varphi, \psi \in \operatorname{Hom}(L, L)$ и $\lambda \in P$

$$x((\lambda\varphi)\psi) = (x(\lambda\varphi))\psi = (\lambda(x\varphi))\psi = ((\lambda x)\varphi)\psi = (\lambda x)(\varphi\psi) = x(\lambda(\varphi\psi))$$

и

$$x(\varphi(\lambda\psi)) = (x\varphi)(\lambda\psi) = \lambda((x\varphi)\psi) = \lambda(x(\varphi\psi)) = x(\lambda(\varphi\psi)).$$

Следовательно, $\operatorname{Hom}(L, L)$ — линейная алгебра над полем P. В силу теоремы 13 из § 1, Φ осуществляет изоморфизм линейных пространств, а из теоремы 15 из § 1 вытекает, что Φ — изоморфизм колец. Таким образом, Φ оказывается изоморфизмом линейных алгебр.

Пусть G — конечная группа и P — некоторое поле. Рассмотрим линейное пространство PG над полем P, приняв элементы группы G за базу. Таким образом,

элементами пространства PG служат линейные комбинации $\sum_{g\in G} \lambda_g g$, где $\lambda_g \in P$. Поскольку базисные элементы можно перемножать как элементы группы, это умножение можно распространить на произвольные элементы линейного пространства PG, полагая

$$\Big(\sum_{g\in G} \lambda_g g\Big)\Big(\sum_{h\in G} \mu_h h\Big) = \sum_{g,\, h\in G} (\lambda_g \mu_h)(gh) = \sum_{k\in G} \nu_k k,$$

где $\nu_k = \sum_{\substack{g,\, h\in G \\ gh=k}} \lambda_g \mu_h$. Легко проверяется, что это определение превращает линейное пространство PG в линейную алгебру над полем P, которая называется *групповой алгеброй группы* G над полем P.

Т е о р е м а 8. *Элемент* $a = \sum_{g\in G} \lambda_g g$ групповой алгебры PG конечной группы G над полем P лежит в *центре* Z *алгебры* PG тогда и только тогда, когда $\lambda_u = \lambda_v$ для *любой пары сопряженных элементов* u *и* v *из* G. *Размерность центра* Z *) групповой алгебры равна числу классов сопряженности группы* G.

Д о к а з а т е л ь с т в о. Пусть $a \in Z$, $u,\ v \in G$ и $v = wuw^{-1}$ для некоторого $w \in G$. Тогда $aw = wa$, откуда

$$\sum_{g\in G} \lambda_g g = a = waw^{-1} = \sum_{g\in G} \lambda_g (wgw^{-1}).$$

Сравнивая коэффициенты при v, убеждаемся, что $\lambda_v = \lambda_u$. Наоборот, если a удовлетворяет указанному условию, то для любых $w,\ g \in G$ имеем $\lambda_g = \lambda_{wgw^{-1}}$. Отсюда

$$waw^{-1} = \sum_{g\in G} \lambda_g (wgw^{-1}) = \sum_{g\in G} \lambda_{wgw^{-1}} (wgw^{-1}) = \sum_{h\in G} \lambda_h h = a,$$

поскольку, когда g пробегает группу G, элементы wgw^{-1} также пробегают всю эту группу. Таким образом, $wa = aw$ для всех $w \in G$. Если теперь $x = \sum_{w\in G} \xi_w w$ — произвольный элемент из PG, то

$$xa = \sum_{w\in G} \xi_w (wa) = \sum_{w\in G} \xi_w (aw) = a \sum_{w\in G} \xi_w w = ax,$$

*) Под *центром* линейной алгебры R понимается центр кольца R. Если алгебра R содержит единицу, то, как легко проверить, ее центр оказывается подпространством линейного пространства R и, следовательно, является подалгеброй алгебры R.

т. е. $a \in Z$. Пусть, далее, $K_1, \ldots, K_m$ — различные классы сопряженных элементов группы G. В силу теоремы II.3.21, эти классы попарно не пересекаются. Пусть w_i — сумма всех элементов из класса K_i (разумеется, вычисляемая в алгебре PG). Если

$$\lambda_1 w_1 + \ldots + \lambda_m w_m = 0,$$

где $\lambda_i \in P$, то, очевидно, $\lambda_1 = \ldots = \lambda_m = 0$, ибо элементы группы G по определению образуют базу пространства PG. Следовательно, система $\{w_1, \ldots, w_m\}$ линейно независима. Поскольку, согласно первой части теоремы, коэффициенты элемента a из Z при элементах группы, принадлежащих одному классу сопряженности, совпадают,

$$a = \lambda_1 \Big(\sum_{g \in K_1} g \Big) + \ldots + \lambda_m \Big(\sum_{g \in K_m} g \Big) = \lambda_1 w_1 + \ldots + \lambda_m w_m.$$

Таким образом, элементы $w_1, \ldots, w_m$ образуют базу пространства Z и, следовательно, $\dim Z = m$.

Т е о р е м а 9. *Если линейная алгебра D над полем комплексных чисел $\boldsymbol{C}$ является телом, то $D = \boldsymbol{C}$.*

Д о к а з а т е л ь с т в о. Ввиду теоремы 1 можно считать, что $\boldsymbol{C} \subseteq D$. Если $z \in D$, то, согласно следствию 3 теоремы 10 из § 1, для подходящего номера n элементы $1, z, \ldots, z^n$ оказываются линейно зависимыми над $\boldsymbol{C}$. Следовательно, найдутся комплексные числа $\lambda_0, \lambda_1, \ldots$ $\ldots, \lambda_n$, не все равные нулю и такие, что

$$\lambda_0 + \lambda_1 z + \ldots + \lambda_n z^n = 0.$$

Другими словами, z оказывается корнем многочлена

$$F(t) = \lambda_0 + \lambda_1 t + \ldots + \lambda_n t^n$$

с комплексными коэффициентами. Не ограничивая общности, можно считать, что $\lambda_n = 1$. Согласно следствию основной теоремы алгебры многочленов *),

$$F(t) = (t - \alpha_1) \ldots (t - \alpha_n),$$

где $\alpha_i \in \boldsymbol{C}$. Отсюда

$$(z - \alpha_1) \ldots (z - \alpha_n) = 0$$

и, поскольку, согласно теореме II.4.5, в теле D нет делителей нуля, для некоторого i получаем $z = \alpha_i \in \boldsymbol{C}$.

В соответствии с определением, данным на с. 127, линейная алгебра R называется *вполне приводимой*

*) См. примечание *) на с. 183.

справа, если она разлагается в прямую сумму минимальных правых идеалов. В силу теорем 3 и II.6.5, вполне приводимой справа линейной алгеброй оказывается кольцо матриц над полем.

Т е о р е м а 10. *Если R — вполне приводимая справа алгебра с единицей над полем P, то существуют такие попарно ортогональные центральные идемпотенты $e_1, \ldots, e_n$, что*

$$1 = e_1 + \ldots + e_n \quad и \quad R = e_1R \oplus \ldots \oplus e_nR,$$

где e_iR — двусторонние идеалы, каждый из которых является простой алгеброй с единицей.

Д о к а з а т е л ь с т в о. Напомним, что теорема 3 позволяет не различать идеалы алгебры R и кольца R. Далее, для сокращения речи условимся называть идемпотент e алгебры R *простым*, если e — ненулевой центральный идемпотент и eR — простая алгебра.

Л е м м а. *Каждый ненулевой двусторонний идеал I алгебры R содержит простой идемпотент.*

Действительно, пусть M — ненулевой двусторонний идеал алгебры R, лежащий в I и как линейное пространство над полем P имеющий наименьшую размерность среди ненулевых двусторонних идеалов алгебры R, лежащих в I. В силу теоремы 10 из § 1, M не содержит ненулевых двусторонних идеалов алгебры R. Согласно теореме II.6.6, идеал M порождается центральным идемпотентом, скажем e. Если алгебра M не является простой, то она содержит двусторонний идеал, отличный от 0 и от M. Но, согласно теореме II.6.7, этот идеал должен быть идеалом алгебры R, что невозможно. Таким образом, e оказывается простым идемпотентом.

Ввиду леммы, алгебра R содержит простой идемпотент. В силу теорем II.6.2 и 8 из § 1, а также следствия 3 теоремы 9 из § 1, она не может содержать бесконечного множества попарно ортогональных идемпотентов. Поэтому в ней существует множество $\{e_1, \ldots, e_n\}$ попарно ортогональных простых идемпотентов, которое не может быть вложено в большее множество попарно ортогональных простых идемпотентов. Положим

$$e = e_1 + \ldots + e_n.$$

Учитывая ортогональность идемпотентов e_i, нетрудно подсчитать, что $e^2 = e$ и $e_ie = e_i$ для каждого i. Если $e \neq 1$, то $(1 - e)^2 = 1 - e - e + e = 1 - e$ и, в силу теоремы II.6.6, $(1 - e)R$ — ненулевой двусторонний

идеал алгебры R. Согласно лемме найдется простой идемпотент $f \in (1-e)R$. Поскольку f централен и $f = (1-e)r$ для некоторого $r \in R$, то $fe_i = e_i f = e_i e(1-e)r = 0$. Следовательно, множество $\{e_1, \ldots, e_n\}$, вопреки допущению, вкладывается в большее множество $\{e_1, \ldots, e_n, f\}$ попарно ортогональных простых идемпотентов. Таким образом, $e = 1$ и, ввиду теоремы II.6.2,

$$R = 1 \cdot R = e_1 R \oplus \ldots \oplus e_n R.$$

По определению простого идемпотента, алгебры $e_i R$ простые. В силу теоремы II.6.6, они являются двусторонними идеалами алгебры R.

Т е о р е м а 11. *Линейная алгебра R с единицей над полем P, не содержащая ненулевых двусторонних идеалов с нулевым умножением, вполне приводима справа.*

Д о к а з а т е л ь с т в о. Напомним, что теорема 3 позволяет не различать правые идеалы алгебры R и кольца R. Для сокращения речи условимся называть идемпотент e алгебры R *минимальным*, если eR — минимальный правый идеал.

Л е м м а. *Каждый ненулевой правый идеал H алгебры R содержит минимальный идемпотент.*

Действительно, пусть M — ненулевой правый идеал алгебры R, лежащий в H и как линейное пространство над полем P имеющий наименьшую размерность среди ненулевых правых идеалов алгебры R, лежащих в H. В силу теоремы 10 из § 1, M оказывается минимальным правым идеалом алгебры R. Ввиду теоремы II.6.4, M не является правым идеалом с нулевым умножением и, согласно теореме II.6.3, порождается идемпотентом e. Конечно, идемпотент e минимален и $e \in H$.

Возвращаясь к доказательству теоремы, заметим, что, согласно лемме, алгебра R содержит минимальный идемпотент. Но, в силу теорем II.6.2 и 8 из § 1, а также следствия 3 теоремы 9 из § 1, она не может содержать бесконечного множества попарно ортогональных идемпотентов. Поэтому в ней существует множество $\{e_1, \ldots, e_n\}$ попарно ортогональных минимальных идемпотентов, которое не может быть вложено в большее множество попарно ортогональных минимальных идемпотентов. Положим

$$e = e_1 + \ldots + e_n.$$

Учитывая ортогональность идемпотентов e_i, нетрудно подсчитать, что $e^2 = e$ и $e_i e = e_i = e e_i$ для каждого i.

Допустим, что $e \neq 1$. Тогда правый идеал $(1 - e)R$ отличен от нуля и, согласно лемме, содержит минимальный идемпотент f. Поскольку $f \in (1 - e)R$, то $f = (1 - e)\, r$ для некоторого $r \in R$. Отсюда

$$e_i f = e_i ef = e_i e\,(1 - e)\, r = e_i 0 r = 0.$$

Если $fe = 0$, то

$$fe_i = fee_i = 0e_i = 0$$

для каждого i и, вопреки допущению, множество $\{e_1, \ldots, e_n\}$ вкладывается в большее множество $\{e_1, \ldots, e_n, f\}$ попарно ортогональных минимальных идемпотентов. Таким образом, $fe \neq 0$, но $ef = 0$. Рассмотрим элемент $g = f\,(1 - e)$. Равенство

$$g^2 = f\,(1 - e) f\,(1 - e) = f(f - ef)(1 - e) = \\ = f^2\,(1 - e) = f\,(1 - e) = g$$

показывает, что g — идемпонент. Если $g = 0$, то $f = fe$, откуда

$$0 \neq f = f^2 = fef = f0 = 0,$$

что невозможно. Если же $g \neq 0$, то из соотношения $0 \neq gR \subseteq fR$ и минимальности правого идеала fR вытекает, что $gR = fR$. Следовательно, g — минимальный идемпотент. Но

$$e_i g = e_i f(1 - e) = 0\,(1 - e) = 0$$

и

$$ge_i = f\,(1 - e)\, e_i = f\,(1 - e)\, ee_i = f0e_i = 0,$$

и мы опять сумели вложить множество $\{e_1, \ldots, e_n\}$ в большее множество $\{e_1, \ldots, e_n, g\}$ попарно ортогональных минимальных идемпотентов. Полученное противоречие показывает, что $e = 1$. Ввиду теоремы II.6.2

$$R = 1 \cdot R = e_1 R \oplus \ldots \oplus e_n R,$$

что и требовалось.

Следствие. *Простая линейная алгебра* (т. е. линейная алгебра, являющаяся простым кольцом) *с единицей вполне приводима справа.*

Теорема 12. *Все минимальные правые идеалы простой линейной алгебры R с единицей изоморфны друг другу как правые R-модули.*

Доказательство. Пусть M и N — минимальные правые идеалы алгебры R. Из теорем 3, II.6.3 и

II.6.4 вытекает, что $M = eR$ и $N = fR$, где $e^2 = e$ и $f^2 = f$. Нетрудно проверить, что множество I всевозможных сумм вида

$$\sum r_i e s_i \quad (r_i, s_i \in R)$$

оказывается двусторонним идеалом алгебры R. При этом $I \neq 0$, поскольку $0 \neq e \in I$. Следовательно, $I = R$, а значит,

$$1 = \sum r_i e s_i$$

для подходящих r_i, $s_i \in R$. Из равенства

$$0 \neq f = \sum f r_i e s_i$$

следует, что $fr_ie \neq 0$ при некотором i. Определим отображение φ: $M \to N$, полагая

$$\varphi(er) = fr_ier.$$

Легко видеть, что φ — гомоморфизм правых R-модулей. Поскольку $\varphi(e) = fr_ie \neq 0$, имеем $\operatorname{Ker}\varphi \subset M$, откуда $\operatorname{Ker}\varphi = 0$ в силу минимальности правого идеала M. Из минимальности правого идеала N и соотношения

$$0 \neq fr_ie \in \operatorname{Im}\varphi \subseteq N$$

вытекает, что $\operatorname{Im}\varphi = N$. Таким образом, φ, будучи вложением и наложением одновременно, оказывается изоморфизмом.

Т е о р е м а 13. *Пусть R — простая линейная алгебра с единицей над полем комплексных чисел $\boldsymbol{C}$ и $R = M_1 \oplus \ldots \oplus M_n$ — ее представление в виде прямой суммы минимальных правых идеалов. Тогда* $\dim M_i = n$ *для каждого i и* $\dim R = n^2$.

Д о к а з а т е л ь с т в о. Согласно теореме II.6.1

$$1 = e_1 + \ldots + e_n,$$

где $e_i^2 = e_i$, $e_ie_j = 0$ при $i \neq j$ и $M_i = e_iR$.

Л е м м а 1. *e_iRe_i — линейное пространство над полем $\boldsymbol{C}$, изоморфное одномерному пространству $\boldsymbol{C}$.*

Действительно, ясно, что e_iRe_i — подкольцо кольца R. Равенство $\lambda(e_ire_i) = e_i(\lambda r)e_i$, где $\lambda \in \boldsymbol{C}$, $r \in R$, показывает, что это подпространство пространства R, а следовательно, и подалгебра алгебры R. Единицей этой подалгебры служит e_i. Если $e_ire_i \neq 0$, то из соотношения

$$0 \neq e_ire_iR \subseteq e_iR$$

и минимальности правого идеала e_iR вытекает, что $e_ire_iR = e_iR$. Следовательно,

$$e_i = e_ire_is$$

для некоторого $s \in R$. Отсюда

$$e_i = e_i^2 = (e_ire_i)(e_ise_i).$$

Но по тем же соображениям

$$(e_ise_i)(e_ite_i) = e_i$$

для некоторого $t \in R$, откуда

$$e_ire_i = (e_ire_i)e_i = (e_ire_i)(e_ise_i)(e_ite_i) = e_ite_i.$$

Таким образом, e_ire_i обратим в алгебре e_iRe_i, т. е. e_iRe_i оказывается телом, и справедливость леммы вытекает из теоремы 9.

Лемма 2. *e_iRe_j — одномерное подпространство линейного пространства R.*

В самом деле, без труда проверяется, что e_iRe_j — подпространство. Согласно теореме 12 существует изоморфизм правых R-модулей φ: $e_jR \to e_iR$. Тогда

$$0 \neq \varphi(e_j) = \varphi(e_je_j) = \varphi(e_j)e_j \in e_iRe_j.$$

Следовательно, $e_iRe_j \neq 0$. Если $y \in e_iRe_j$, то $y = \varphi(x)$, где $x \in e_jR$. Отсюда, учитывая включение $xe_j \in e_jRe_j$ и принимая во внимание лемму 1, получаем

$$y = ye_j = \varphi(x)e_j = \varphi(xe_j) = \varphi(\lambda e_j) = \lambda\varphi(e_j)$$

для некоторого $\lambda \in \boldsymbol{C}$. Кроме того, $\varphi(e_j) \in e_iRe_j$. Следовательно, $\{\varphi(e_j)\}$ — база пространства e_iRe_j.

Лемма 3. $e_iR = (e_iRe_1) \oplus \ldots \oplus (e_iRe_n)$.

Действительно, для всякого $r \in R$ имеем

$$e_ir = e_ir1 = e_ire_1 + \ldots + e_ire_n \in \sum_{j=1}^{n} e_iRe_j.$$

Если же

$$e_ir_1e_1 + \ldots + e_ir_ne_n = 0,$$

то, умножая справа на e_j, получаем $e_ir_je_j = 0$ для каждого j. Остается принять во внимание свойство (4) теоремы II.5.12.

Возвращаясь к доказательству теоремы, заметим, что, в силу свойства (3) теоремы 9 из § 1, леммы 2 и 3 обеспечивают справедливость равенства $\dim e_iR = n$. После

этого равенство $\dim R = n^2$ вытекает из следствия 2 теоремы 9 из § 1.

Т е о р е м а 14. *Простая алгебра R с единицей над полем комплексных чисел C изоморфна алгебре матриц над полем C.*

Д о к а з а т е л ь с т в о. В силу следствия из теоремы 11, алгебра R вполне приводима справа, т. е. представима в форме

$$R = M_1 \oplus \ldots \oplus M_n,$$

где M_i — минимальные правые идеалы. Согласно теореме 13, $\dim M_i = n$. Пусть R' — алгебра линейных преобразований линейного пространства M_1. Определим отображение Φ алгебры R в алгебру R', положив

$$x\Phi(r) = xr$$

для всякого $x \in M_1$ и $r \in R$. Из равенств

$$(x + y)\,\Phi(r) = (x + y)\,r = xr + yr = x\Phi(r) + y\Phi(r)$$

и

$$(\lambda x)\,\Phi(r) = (\lambda x)\,r = \lambda(xr) = \lambda(x\Phi(r)),$$

справедливых для любых x, $y \in M_1$ и $\lambda \in C$, вытекает, что $\Phi(r) \in R'$. Равенства

$$x\Phi(r + s) = x(r + s) = xr + xs = \\ = x\Phi(r) + x\Phi(s) = x(\Phi(r) + \Phi(s)),$$

$$x\Phi(rs) = x(rs) = (xr)s = (x\Phi(r))\Phi(s) = x(\Phi(r)\Phi(s))$$

и

$$x\Phi(\lambda r) = x(\lambda r) = \lambda(xr) = \lambda(x\Phi(r)) = x(\lambda\Phi(r)),$$

справедливые для любых $x \in M_1$, r, $s \in R$ и $\lambda \in C$, показывают, что

$$\Phi(r + s) = \Phi(r) + \Phi(s),$$
$$\Phi(rs) = \Phi(r)\,\Phi(s),$$
$$\Phi(\lambda r) = \lambda\Phi(r).$$

Следовательно, Φ — гомоморфизм линейных алгебр. Поскольку $\Phi(1)$ — тождественное отображение, ядро $\operatorname{Ker}\Phi \neq R$ и, будучи двусторонним идеалом алгебры R, равно нулю. Следовательно, Φ — гомоморфное вложение алгебр. Поскольку, ввиду теорем 7 и 13,

$$\dim(\operatorname{Im}\Phi) = \dim R = n^2 = \dim R',$$

из теоремы 10 из § 1 вытекает, что $\operatorname{Im}\Phi = R'$. Следовательно, Φ — наложение, а значит, изоморфизм. Остается еще раз принять во внимание теорему 7.

Т е о р е м а 15. *Пусть R — вполне приводимая справа алгебра с единицей над полем комплексных чисел $\boldsymbol{C}$. Тогда R допускает представление*

$$R = R_1 \oplus \ldots \oplus R_m$$

в виде прямой суммы двусторонних идеалов, причем справедливы следующие утверждения:

(1) $R_i R_j = 0$, *если* $i \neq j$;

(2) *каждый из двусторонних идеалов R_i изоморфен алгебре матриц над полем $\boldsymbol{C}$;*

(3) *каждый минимальный правый идеал алгебры R лежит в одном из идеалов R_i, и два минимальных правых идеала алгебры R изоморфны как правые R-модули тогда и только тогда, когда они лежат в одном и том же идеале R_i;*

(4) *каждый неприводимый правый R-модуль изоморфен некоторому минимальному правому идеалу алгебры R;*

(5) *если $M_1, \ldots, M_m$ — все неизоморфные неприводимые правые R-модули и $\dim M_i = n_i$, то R как правый R-модуль изоморфен внешней прямой сумме*

$$\underbrace{(M_1 \oplus \ldots \oplus M_1)}_{n_1 \text{ раз}} \oplus \underbrace{(M_2 \oplus \ldots \oplus M_2)}_{n_2 \text{ раз}} \oplus \ldots$$

$$\ldots \oplus \underbrace{(M_m \oplus \ldots \oplus M_m)}_{n_m \text{ раз}};$$

(6) *элемент z алгебры R принадлежат ее центру Z *) тогда и только тогда, когда $z = z_1 + \ldots + z_i$, где z_i принадлежит центру Z_i алгебры R_i;*

(7) *центр Z алгебры R имеет размерность m.*

Д о к а з а т е л ь с т в о. Будем иметь в виду, что, согласно теореме 3, каждый правый R-модуль является линейным пространством над полем $\boldsymbol{C}$ и что та же теорема позволяет не делать различия между правыми идеалами алгебры R и кольца R. То же самое верно и для двусторонних идеалов. По теореме 10

$$R = R_1 \oplus \ldots \oplus R_m,$$

где R_i — двусторонние идеалы алгебры R, каждый из которых является простой алгеброй с единицей. После

*) См. примечание на с. 193.

этого утверждение (2) сразу следует из теоремы 14. Для доказательства утверждения (1) достаточно заметить, что $R_iR_j \subseteq R_i \cap R_j = 0$, поскольку сумма прямая. Если, далее, M — минимальный правый идеал алгебры R и $0 \neq x \in M$, то в обозначениях теоремы 10 имеем

$$x = 1x = (e_1 + \ldots + e_m)\, x = e_1x + \ldots + e_mx,$$

причем $e_ix \neq 0$ для некоторого i. Поскольку

$$e_ix = xe_i \in R_i \cap M,$$

то

$$0 \neq R_i \cap M \subseteq M.$$

Ввиду теоремы II.5.1, $R_i \cap M$ — правый идеал алгебры R, и из минимальности правого идеала M вытекает, что $R_i \cap M = M$. Последнее означает, что $M \subseteq R_i$, т. е. справедливость первой части утверждения (3). Если же M и M' — минимальные правые идеалы алгебры R, лежащие в идеале R_i, то, будучи согласно теореме II.6.7 минимальными правыми идеалами кольца R_i, они в силу теоремы 12 изоморфны как правые R_i-модули. Если φ: $M \to M'$ — этот изоморфизм, то для любых $r \in R$ и $x \in M$, записав $r = r_1 + \ldots + r_n$, где $r_j \in R_j$, и принимая во внимание (1), получаем

$$\varphi(xr) = \varphi(xr_i) = \varphi(x)\, r_i = \varphi(x)\, r.$$

Следовательно, φ оказывается изоморфизмом правых R-модулей. Допустим теперь, что M и M' — минимальные правые идеалы алгебры R, $M \subseteq R_i$, $M' \subseteq R_j$, $i \neq j$ и φ: $M \to M'$ — изоморфизм правых R-модулей. Затем выберем в M элемент $x \neq 0$ и, вспоминая, что $e_i \in Z$, запишем его как $x = e_iy = ye_i$, где $y \in R$. Поскольку $\varphi(x) \in R_j$, то, учитывая (1), получаем

$$\varphi(x) = \varphi(ye_i) = \varphi(ye_i^2) = \varphi(ye_i)\, e_i = \varphi(x)\, e_i = 0,$$

чего не может быть при изоморфизме. Тем самым установлена справедливость утверждения (3). Утверждение (4) содержится в теореме II.6.9. Из этой же теоремы и утверждения (3) вытекает, что при подходящей нумерации каждый из модулей M_i, упоминаемых в утверждении (5), изоморфен некоторому минимальному правому идеалу алгебры R, являющемуся, как это следует из теорем 10 и II.6.7, минимальным правым идеалом алгебры R_i. Из утверждения (3) и теоремы 13 вытекает, что R_i как

правый R-модуль изоморфен внешней прямой сумме

$$\underbrace{M_i \oplus \ldots \oplus M_i}_{n_i \text{ раз}},$$

откуда непосредственно следует (5). Допустим теперь, что $z = z_1 + \ldots + z_m$, где $z_i \in Z_i$. Записав произвольный элемент $r \in R$ в форме $r = r_1 + \ldots + r_m$, где $r_i \in R_i$, и используя (1), получаем

$$rz = r_1 z_1 + \ldots + r_m z_m = z_1 r_1 + \ldots + z_m r_n = zr,$$

т. е. $z \in Z$. Наоборот, если $z \in Z$ и $z = z_1 + \ldots + z_m$, где $z_i \in R_i$, то для любого $r_i \in R_i$ имеем

$$r_i z_i = r_i z = z r_i = z_i r_i,$$

т. е. $z_i \in Z_i$. Таким образом, доказано утверждение (6). Отсюда и из теоремы II.5.12 вытекает, что

$$Z = Z_1 \oplus \ldots \oplus Z_m.$$

В силу теоремы II.4.12 $\dim Z_i = 1$, и утверждение (7) вытекает из следствия 2 теоремы 9 из § 1.

З а м е ч а н и е. Теорема 15 позволяет решить задачу: сколько существует не изоморфных друг другу вполне приводимых справа алгебр над полем комплексных чисел, имеющих данную размерность n? Например, если $n = 12$, то, ввиду свойства (2), каждой такой алгебре соответствует представление числа 12 в виде суммы квадратов. Таких представлений имеется пять:

$$12 = 1 + 1 + \ldots + 1,$$
$$12 = 4 + 1 + 1 + \ldots + 1,$$
$$12 = 4 + 4 + 1 + 1 + 1 + 1,$$
$$12 = 4 + 4 + 4,$$
$$12 = 9 + 1 + 1 + 1.$$

Первому из этих представлений соответствует коммутативная алгебра, являющаяся прямой суммой 12 экземпляров поля комплексных чисел, второму — прямая сумма алгебры двумерных матриц и 8 экземпляров поля комплексных чисел, трем оставшимся — прямые суммы алгебр матриц порядков 2, 2, 1, 1, 1 и 1, затем 2, 2 и 2 и, наконец, 3, 1, 1 и 1 соответственно. Алгебры эти не изоморфны, поскольку согласно утверждению (7) размерности их центров равны 12, 9, 6, 3 и 4 соответственно. Правда, иногда доказательство неизоморфности требует

более тонких рассуждений (например, для $27 = 9 + 9 + 9$ и $27 = 25 + 1 + 1$).

Т е о р е м а 16 (теорема Машке). *Групповая алгебра CG конечной группы G над полем комплексных чисел C вполне приводится справа.*

Д о к а з а т е л ь с т в о. Если

$$x = \sum_{g \in G} \lambda_g g \in CG,$$

то положим

$$x^* = \sum_{g \in G} \bar{\lambda}_g g^{-1}.$$

Ясно, что $x^{**} = x$. Если теперь

$$y = \sum_{h \in G} \mu_h h \in CG,$$

то

$$xy = \sum_{k \in G} \nu_k k,$$

где $\nu_k = \sum\limits_{\substack{g,\, h \in G \\ gh = k}} \lambda_g \mu_h$. В силу теоремы II.4.9, $\bar{\nu}_k = \sum\limits_{\substack{g,\, h \in G \\ gh = k}} \bar{\lambda}_g \bar{\mu}_h$. Поэтому

$$(xy)^* = \sum_{k \in G} \bar{\nu}_k k^{-1} = \sum_{k \in G} \Big(\sum_{\substack{g,\, h \in G \\ gh = k}} \bar{\lambda}_g \bar{\mu}_h \Big) h^{-1} g^{-1} = y^* x^*.$$

Далее,

$$xx^* = \sum_{g,\, h \in G} \lambda_g \bar{\lambda}_h g h^{-1} = \Big(\sum_{g \in G} \lambda_g \bar{\lambda}_g \Big) 1 + \ldots,$$

т. е. коэффициент при единице группы G равен $\nu = \sum\limits_{g \in G} \lambda_g \bar{\lambda}_g$. Если $\lambda_g = a_g + b_g i$, где a_g, b_g — действительные числа, то $\nu = \sum\limits_{g \in G} (a_g^2 + b_g^2)$ и, следовательно, $\nu \neq 0$, если $x \neq 0$. Таким образом, $xx^* \neq 0$, если $x \neq 0$. Предположим теперь, что I — ненулевой идеал алгебры CG с нулевым умножением. Если $0 \neq x \in I$, то $xx^* \in I$ и, следовательно,

$$(xx^*)(xx^*)^* = (xx^*)(x^{**}x^*) = (xx^*)(xx^*) = 0,$$

хотя $xx^* \neq 0$. Таким образом, алгебра CG не содержит ненулевых идеалов с нулевым умножением и ее полная приводимость вытекает из теоремы 11.

Теорема 17. *Число неизоморфных неприводимых правых модулей над групповой алгеброй CG конечной группы G над полем комплексных чисел C равно числу классов сопряженности группы G.*

Доказательство. В силу теоремы 16, алгебра CG вполне приводима справа. Поэтому из теоремы II.6.8 вытекает, что каждый неприводимый правый CG-модуль изоморфен некоторому минимальному правому идеалу алгебры CG. Сопоставляя утверждения (3) и (7) теоремы 15, видим, что число неизоморфных минимальных правых CG-модулей равно размерности центра алгебры CG. Согласно же теореме 8, последняя равна числу классов сопряженности группы G.

Из теорем 15 (5) и 16, учитывая следствие 2 теоремы 9 из § 1, выводим следующее утверждение.

Теорема 18. *Если $M_1, \ldots, M_m$ — все неизоморфные неприводимые правые модули над групповой алгеброй CG конечной группы G над полем комплексных чисел C, то*

$$|G| = (\dim M_1)^2 + \ldots + (\dim M_m)^2.$$

Упражнения

1. Поле действительных чисел не является конечномерной алгеброй над полем рациональных чисел.

2. Указать в линейной алгебре матриц над полем P подполе, изоморфное полю P, но отличное от PE, где E — единичная матрица.

3. Убедиться, что групповая алгебра группы $\mathfrak{S}_3$ над полем вычетов по модулю 3 не является вполне приводимой справа.

4. Убедиться, что алгебра верхних треугольных матриц (т. е. таких, у которых члены, расположенные под главной диагональю, нулевые) не является вполне приводимой справа.

5. Коммутативная алгебра над полем C вполне приводима справа тогда и только тогда, когда она изоморфна прямой сумме нескольких экземпляров поля C.

6. Вполне приводимая справа алгебра над полем C не содержит делителей нуля тогда и только тогда, когда она изоморфна C.

7. Если все идемпотенты вполне приводимой справа алгебры над полем C центральны или если она не содержит ненулевых *нильпотентных* элементов (т. е. таких элементов a, что $a^m = 0$ для некоторого m), то она коммутативна.

8. Пусть S — кольцо матриц второго порядка над кольцом R с единицей. Доказать изоморфизм колец R и $\begin{Vmatrix} 1 & 0 \\ 0 & 0 \end{Vmatrix} S \begin{Vmatrix} 1 & 0 \\ 0 & 0 \end{Vmatrix}$.

9. Сколько существует попарно не изоморфных вполне приводимых справа алгебр над полем комплексных чисел размерностей 3, 4, 5, 6, 10, 20?

10. Доказать, что групповые алгебры групп $\boldsymbol{Z}/4\boldsymbol{Z}$ и $\boldsymbol{Z}/2\boldsymbol{Z} \oplus \boldsymbol{Z}/2\boldsymbol{Z}$ над полем комплексных чисел изоморфны, хотя сами эти группы не изоморфны.

11. Пусть R — вполне приводимая справа алгебра и $e^2 = e \in R$. Доказать, что правый R-модуль eR неприводим тогда и только тогда, когда неприводим левый R-модуль Re.

12. Доказать, что всякая вполне приводимая справа алгебра вполне приводима слева.

13. Указать для групповой алгебры группы G над полем $\boldsymbol{C}$ разложение, существующее согласно теоремам 15 и 16, для следующих групп G: а) группы вычетов по модулю 2 или 3; б) $(\boldsymbol{Z}/2\boldsymbol{Z}) \times (\boldsymbol{Z}/2\boldsymbol{Z})$; в) $\mathfrak{S}_3$; г) $\mathfrak{A}_4$ (см. конец § 3 гл. II).

14. Доказать, что групповая алгебра группы G над полем $\boldsymbol{C}$ проста тогда и только тогда, когда G — одноэлементная группа.

ГЛАВА IV

ПРЕДСТАВЛЕНИЯ КОНЕЧНЫХ ГРУПП

В первом параграфе настоящей главы излагаются основные определения теории представлений конечных групп и устанавливаются результаты, касающиеся связи числа неприводимых представлений и их размерности с порядком группы G. Во втором параграфе эти результаты используются для доказательства разрешимости некоторых конечных групп. На протяжении этой главы под группой всегда понимается конечная группа.

§ 1. Основы теории представлений

Представлением конечной группы G называется гомоморфизм этой группы в группу взаимно однозначных линейных преобразований линейного пространства V над полем комплексных чисел $\boldsymbol{C}$*), которая называется линейной группой пространства V и обозначается через $GL(V)$. Таким образом, представление группы G — это гомоморфизм $\Phi\colon G \to GL(V)$. Пространство V называется *пространством представления* Φ. *Размерностью представления* Φ (в обозначениях $\dim \Phi$) называется размерность пространства представления. Учитывая связь между линейными преобразованиями и матрицами (см. теоремы I.3.13, I.3.14 и III.1.15), нетрудно вывести, что если $\dim V = n$, то группа $GL(V)$ изоморфна группе невырожденных матриц порядка n. При $n = 1$ группа $GL(1)$ изоморфна группе отличных от нуля комплексных чисел по умножению. Эту группу будем называть *мультипликативной группой поля* $\boldsymbol{C}$. Групповую алгебру группы G над полем $\boldsymbol{C}$, как и раньше, обозначим через $\boldsymbol{C}G$.

Если V — пространство представления Φ группы G, то определим произведение vg для $v \in V$ и $g \in G$,

*) Таким образом, мы говорим о *комплексном представлении группы*. Разумеется, можно рассматривать представления, использующие линейные пространства над другими полями.

положив

$$vg = v\Phi(g).$$

Тогда для любых $g, h \in G$ и $\lambda \in \boldsymbol{C}$ имеем

$$v(gh) = v\Phi(gh) = v(\Phi(g)\Phi(h)) = (v\Phi(g))\Phi(h) = (vg)h$$

и

$$(\lambda v)g = (\lambda v)\Phi(g) = \lambda(v\Phi(g)) = \lambda(vg).$$

Теперь можно превратить V в правый модуль над алгеброй $\boldsymbol{C}G$, положив

$$v\Big(\sum_{g\in G}\lambda_g g\Big) = \sum_{g\in G}\lambda_g(vg),$$

где $\lambda_g \in \boldsymbol{C}$, $v \in V$, $g \in G$. Действительно, учитывая определение операций в алгебре Hom (V, V) и в алгебре $\boldsymbol{C}G$, для любых $\lambda, \lambda_g, \mu_h \in \boldsymbol{C}$, $g, h \in G$ и $u, v \in V$ имеем

$$(u+v)\Big(\sum_{g\in G}\lambda_g g\Big) = \sum_{g\in G}\lambda_g((u+v)g) =$$

$$= \sum_{g\in G}\lambda_g((u+v)\Phi(g)) = \sum_{g\in G}\lambda_g(u\Phi(g) + v\Phi(g)) =$$

$$= \sum_{g\in G}\lambda_g(ug) + \sum_{g\in G}\lambda_g(vg) = u\Big(\sum_{g\in G}\lambda_g g\Big) + v\Big(\sum_{g\in G}\lambda_g g\Big),$$

$$v\Big(\sum_{g\in G}\lambda_g g + \sum_{g\in G}\mu_g g\Big) =$$

$$= v\Big(\sum_{g\in G}(\lambda_g + \mu_g)g\Big) = \sum_{g\in G}(\lambda_g + \mu_g)(vg) =$$

$$= \sum_{g\in G}\lambda_g(vg) + \sum_{g\in G}\mu_g(vg) = v\Big(\sum_{g\in G}\lambda_g g\Big) + v\Big(\sum_{g\in G}\mu_g g\Big),$$

$$v\Big(\sum_{g\in G}\lambda_g g \cdot \sum_{h\in G}\mu_h h\Big) = v\Big(\sum_{g,\,h\in G}(\lambda_g\mu_h)(gh)\Big) =$$

$$= \sum_{g,\,h\in G}(\lambda_g\mu_h)(v(gh)) = \sum_{g,\,h\in G}(\lambda_g\mu_h)((vg)h) =$$

$$= \Big(\sum_{g\in G}\lambda_g(vg)\Big)\Big(\sum_{h\in G}\mu_h h\Big) = \Big(v\Big(\sum_{g\in G}\lambda_g g\Big)\Big)\Big(\sum_{h\in G}\mu_h h\Big),$$

$$v1 = v\Phi(1) = v.$$

Полученный таким образом модуль называется *модулем представления* Φ.

С другой стороны, если M — правый модуль над групповой алгеброй $\boldsymbol{C}G$, то, поскольку $\boldsymbol{C}G$ содержит $\boldsymbol{C}$, M является линейным пространством над полем $\boldsymbol{C}$, и можно определить гомоморфизм Φ: $G \to GL(M)$, положив $x\Phi(g) = xg$ для всех $x \in M$ и $g \in G$. Таким образом, с модулем над групповой алгеброй $\boldsymbol{C}G$ связано вполне определенное представление группы G.

Представления Φ и Ψ группы G с пространствами представлений V и W соответственно называются *эквивалентными*, если существует изоморфизм линейных пространств $\varphi\colon V \to W$ такой, что

$$\Phi(g) = \varphi\Psi(g)\varphi^{-1}$$

для всех $g \in G$.

Теорема 1. *Два представления группы G эквивалентны тогда и только тогда, когда изоморфны их модули представления.*

Доказательство. Пусть Φ и Ψ — представления группы G, V и W — модули этих представлений. Допустим, что Φ и Ψ эквивалентны, и рассмотрим соответствующий изоморфизм φ линейных пространств. Если $r = \sum_{g\in G} \lambda_g g$ — элемент групповой алгебры CG, то для любого $v \in V$ имеем

$$(vr)\varphi = \Big(\sum_{g\in G} \lambda_g (vg)\Big)\varphi =$$

$$= \Big(\sum_{g\in G} \lambda_g (v\Phi(g))\Big)\varphi = \sum_{g\in G} \lambda_g [v(\varphi\Psi(g)\varphi^{-1}\varphi)] =$$

$$= \sum_{g\in G} \lambda_g [(v\varphi)\Psi(g)] = (v\varphi)\Big(\sum_{g\in G} \lambda_g g\Big) = (v\varphi)r,$$

т. е. φ оказывается изоморфизмом левых CG-модулей. Наоборот, если имеется изоморфизм φ модуля V на модуль W, то φ, очевидно, является изоморфизмом линейных пространств, и для любых $g \in G$ и $v \in V$ имеем

$$v(\varphi\Psi(g)) = (v\varphi)\Psi(g) = (v\varphi)g =$$

$$= (vg)\varphi = (v\Phi(g))\varphi = v(\Phi(g)\varphi).$$

Отсюда

$$\varphi\Psi(g) = \Phi(g)\varphi$$

и, следовательно,

$$\Phi(g) = \varphi\Psi(g)\varphi^{-1}$$

для всех $g \in G$, т. е. Φ и Ψ — эквивалентные представления.

Если $\Phi_1, \ldots, \Phi_m$ — представления группы G и $V_1, \ldots, V_m$ — пространства этих представлений, то образуем внешнюю прямую сумму

$$V = V_1 \oplus \ldots \oplus V_m$$

и для каждого $g \in G$ положим

$$(v_1, \ldots, v_m)\,\Phi(g) = (v_1\Phi_1(g), \ldots, v_m\Phi_m(g)).$$

Легко проверяется, что $\Phi(g) \in GL(V)$ и что Φ — гомоморфизм группы G в группу $GL(V)$. Следовательно, Φ — представление группы G. Оно называется *прямой суммой* представлений Φ_i и обозначается через $\Phi_1 \oplus \ldots \ldots \oplus \Phi_m$.

Подпространство U пространства V представления Φ называется *инвариантным*, если $u\Phi(g) \in U$ для любых $u \in U$ и $g \in G$. Представление Φ называется *неприводимым*, если единственные его инвариантные подпространства — нуль и все пространство V.

Теорема 2. *Представление неприводимо тогда и только тогда, когда неприводим его модуль.*

Доказательство. Пусть Φ — представление группы G и V — пространство этого представления. Если представление Φ неприводимо, H — подмодуль CG-модуля V, $0 \neq H \subset V$ и $x \in H$, то $xg \in H$ для всех $g \in G \subseteq CG$. Отсюда $x\Phi(g) = xg \in H$ для всех $g \in G$. Следовательно, H — инвариантное подпространство пространства V, отличное от 0 и V, что противоречит неприводимости представления Φ. Наоборот, если V — неприводимый CG-модуль и U — отличное от 0 и V инвариантное подпространство пространства V, то для любого $u \in U$ и $r = \sum_{g \in G} \lambda_g g \in CG$ имеем

$$ur = \sum_{g \in G} \lambda_g (ug) = \sum_{g \in G} \lambda_g (u\Phi(g)) \in U.$$

Следовательно, U — отличный от 0 и V подмодуль модуля V, что противоречит неприводимости последнего.

Теорема 3. *Число неэквивалентных неприводимых представлений конечной группы G равно числу классов сопряженности этой группы.*

Доказательство. Из теорем 1 и 2 вытекает, что число неэквивалентных неприводимых представлений группы G равно числу неизоморфных неприводимых модулей над алгеброй CG. Но, в силу следствия теоремы III.2.17, число неприводимых модулей над алгеброй CG равно числу классов сопряженности группы G.

Теорема 3 в ряде случаев позволяет подсчитать количество неприводимых представлений данной конечной группы. С другой стороны, ввиду теорем 2 и II. 6.8, все остальные представления этой группы могут быть сконструированы из неприводимых. В ряде случаев построенная теория дает также возможность определить не только число неприводимых представлений, но и их размерность. Правда, никакого алгоритма для решения этой задачи она не дает.

Примеры. 1. G — коммутативная группа. В этом случае алгебра CG коммутативна. Значит, все алгебры матриц, входящие в

ее разложение, описываемое теоремой III. 2.15, коммутативны и, следовательно, это матрицы первого порядка. В силу теорем III.2.13 и II.6.8, каждый неприводимый CG-модуль одномерен. В силу теоремы 2, все неприводимые представления группы G одномерны. В силу теоремы 3, число их равно порядку группы G. В частности, если G — группа вычетов по модулю 3, а 1, ζ, ζ^2 — все корни степени 3 из 1, то ее неприводимыми представлениями будут (вместо линейных преобразований пишутся матрицы порядка 1):

Φ_0: $\Phi_0(g) = 1$ для всех $g \in G$,

Φ_1: $\Phi_1(0) = 1$, $\Phi_1(1) = \zeta$, $\Phi_1(2) = \zeta^2$,

Φ_2: $\Phi_2(0) = 1$, $\Phi_2(1) = \zeta^2$, $\Phi_2(2) = \zeta^4 = \zeta$.

Всякое другое представление — это прямая сумма перечисленных. Например,

$$\Phi = \Phi_0 \oplus \Phi_1 \oplus \Phi_1 \oplus \Phi_2$$

— четырехмерное представление, где

$$\Phi(0) = E, \quad \Phi(1) = \begin{Vmatrix} 1 & 0 & 0 & 0 \\ 0 & \zeta & 0 & 0 \\ 0 & 0 & \zeta & 0 \\ 0 & 0 & 0 & \zeta^2 \end{Vmatrix}$$

и

$$\Phi(2) = \begin{Vmatrix} 1 & 0 & 0 & 0 \\ 0 & \zeta^2 & 0 & 0 \\ 0 & 0 & \zeta^2 & 0 \\ 0 & 0 & 0 & \zeta \end{Vmatrix}.$$

2. Группа $\mathfrak{S}_3$. Групповая алгебра шестимерна. Группа $\mathfrak{S}_3$ имеет три класса сопряженности. В силу теоремы 3 существуют три неизоморфных неприводимых представления, среди которых — одномерное единичное представление φ_0, где $\varphi_0(g) = 1$ для всех $g \in \mathfrak{S}_3$. Если n_1 и n_2 — размерности двух других представлений, то, учитывая строение алгебры $C\mathfrak{S}_3$ (см. теоремы III.2.15(2) и III.2.16), имеем

$$6 = 1 + n_1^2 + n_2^2.$$

Отсюда $n_1 = 1$ и $n_2 = 2$. Таким образом, группа $\mathfrak{S}_3$ имеет еще одно одномерное неприводимое представление Φ_1 и одно двумерное неприводимое представление Φ_2. Теорема II.3.19 позволяет положить

$$\Phi_1(g) = \begin{cases} 1, & \text{если } g \text{ — четная подстановка,} \\ -1, & \text{если } g \text{ — нечетная подстановка.} \end{cases}$$

Представление Φ_2 можно определить так:

$$\Phi_2\left(\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}\right) = E,$$

$$\Phi_2\left(\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\right) = \begin{Vmatrix} 1 & 0 \\ -1 & -1 \end{Vmatrix},$$

$$\Phi_2\left(\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\right) = \begin{Vmatrix} -1 & -1 \\ 0 & 1 \end{Vmatrix},$$

$$\Phi_2\left(\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right)=\begin{Vmatrix}0&1\\1&0\end{Vmatrix},$$
$$\Phi_2\left(\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right)=\begin{Vmatrix}0&1\\-1&-1\end{Vmatrix},$$
$$\Phi_2\left(\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right)=\begin{Vmatrix}-1&-1\\1&0\end{Vmatrix}.$$

Т е о р е м а 4. *Если* Φ *— представление конечной группы* G *и* $g \in G$, *то* $\Phi(g)^m$ *для некоторого натурального* m *оказывается тождественным преобразованием и каждый характеристический корень линейного преобразования* $\Phi(g)$ *является корнем из единицы.*

Д о к а з а т е л ь с т в о. В силу теоремы II.3.22, имеем $g^m = 1$ для некоторого m, откуда $\Phi(g)^m$ — тождественное преобразование. Если λ — характеристический корень линейного преобразования $\Phi(g)$, то, согласно теореме III.1.17, $v\Phi(g) = \lambda v$ для некоторого ненулевого вектора v. Отсюда

$$v = v\underbrace{\Phi(g)\ldots\Phi(g)}_{m\text{ раз}} = \lambda^m v.$$

Поскольку $v \neq 0$, то $\lambda^m = 1$ в силу теоремы III.1.1.

Если Φ — представление группы G, то отображение χ_Φ группы G в поле $\boldsymbol{C}$, определяемое равенством

$$\chi_\Phi(g) = \operatorname{Tr}\Phi(g)$$

для всех $g \in G$, называется *характером представления* Φ.

Таблицы характеров рассмотренных выше представлений выглядят следующим образом:

1. Группа вычетов по модулю 3.

	0	1	2
χ_{Φ_0}	1	1	1
χ_{Φ_1}	1	ζ	ζ^2
χ_{Φ_2}	1	ζ^2	ζ
χ_Φ	4	ζ	ζ^2

2. Группа $\mathfrak{S}_3$.

	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$
χ_{Φ_0}	1	1	1	1	1	1
χ_{Φ_1}	1	−1	−1	−1	1	1
χ_{Φ_2}	2	0	0	0	−1	−1

Т е о р е м а 5. *Если* Φ *— представление группы* G *и* g, $h \in G$, *то* $\chi_\Phi(ghg^{-1}) = \chi_\Phi(h)$.

Д о к а з а т е л ь с т в о. Как уже отмечалось, теоремы I.3.13, I.3.14 и III.1.15 позволяют смотреть на $\Phi(g)$ как на невырожденную матрицу. Но тогда равенство

$$\Phi(ghg^{-1}) = \Phi(g)\Phi(h)\Phi(g)^{-1}$$

и формула изменения матрицы линейного преобразования при изменении базы (см. с. 180) показывают, что $\Phi(ghg^{-1})$ и $\Phi(h)$ — это матрицы одного и того же линейного преобразования в разных базах. Согласно теореме III.1.16, следы этих матриц равны, что и требовалось.

Т е о р е м а 6. *Если* Φ *и* Ψ *— эквивалентные представления группы* G, *то* $\chi_\Phi = \chi_\Psi$.

Д о к а з а т е л ь с т в о. Пусть V и W — пространства представлений Φ и Ψ соответственно. Если представления Φ и Ψ эквивалентны и $g \in G$, то $\Phi(g) = \varphi\Psi(g)\varphi^{-1}$, где $\varphi\colon V \to W$ — изоморфизм линейных пространств. Пусть

$$e = \begin{Vmatrix} e_1 \\ \cdot\ \cdot\ \cdot \\ e_n \end{Vmatrix} \text{ — базисный вектор-столбец из } V.$$

Если $\lambda_1(e_1\varphi) + \ldots + \lambda_n(e_n\varphi) = 0$ для некоторых $\lambda_i \in \boldsymbol{C}$, то $(\lambda_1 e_1 + \ldots + \lambda_n e_n)\varphi = 0$, откуда $\lambda_1 e_1 + \ldots + \lambda_n e_n = 0$, а значит, $\lambda_1 = \ldots = \lambda_n = 0$. Таким образом, вектор-столбец $e\varphi$ *) линейно независим. Из теоремы III.1.10 вытекает, что он базисный. Обозначим через A матрицу линейного преобразования $\Phi(g)$ в базе e, а через B — матрицу линейного преобразования $\Psi(g)$ в базе $e\varphi$. Тогда

$$B(e\varphi) = (e\varphi)\Psi(g) = (e\Phi(g))\varphi = (Ae)\varphi = A(e\varphi)\ **),$$

откуда $A = B$ по теореме III.1.12. Следовательно,

$$\chi_\Phi(g) = \operatorname{Tr} A = \operatorname{Tr} B = \chi_\Psi(g).$$

Ввиду произвольности элемента $g \in G$ имеем $\chi_\Phi = \chi_\Psi$, что и требовалось.

---

*) Если φ — линейное отображение, то, как уже отмечалось, $e\varphi$ означает вектор-столбец $\begin{Vmatrix} e_1\varphi \\ \cdot\ \cdot\ \cdot \\ e_n\varphi \end{Vmatrix}$.

**) Равенство $(Ae)\varphi = A(e\varphi)$ проверяется непосредственным подсчетом, использующим линейность отображения φ.

Наша ближайшая цель — доказать, что и, наоборот, из равенства характеров вытекает эквивалентность представлений.

Теорема 7. *Если* Φ — *представление группы* G, *то* $\chi_\Phi(g^{-1}) = \overline{\chi_\Phi(g)}$ *для каждого* $g \in G$.

Доказательство. Если $\lambda_1, \ldots, \lambda_n$ — собственные значения линейного преобразования $\Phi(g)$, то

$$\chi_\Phi(g) = \operatorname{Tr}\Phi(g) = \lambda_1 + \ldots + \lambda_n.$$

Согласно теореме 4, λ_i — корень из единицы. Но тогда $\lambda_i\overline{\lambda}_i$ — положительный действительный корень из единицы (см. с. 100), откуда $\lambda_i\overline{\lambda}_i = 1$, т. е. $\overline{\lambda}_i = \lambda_i^{-1}$. Ввиду теоремы III.1.18

$$\chi_\Phi(g^{-1}) = \operatorname{Tr}\Phi(g^{-1}) = \operatorname{Tr}(\Phi(g))^{-1} =$$
$$= \lambda_1^{-1} + \ldots + \lambda_n^{-1} = \overline{\lambda}_1 + \ldots + \overline{\lambda}_n = \overline{\operatorname{Tr}\Phi(g)} = \overline{\chi_\Phi(g)}.$$

Теорема 8. *Если*

$$\Phi = \Phi_1 \oplus \ldots \oplus \Phi_m,$$

где Φ, Φ_i — *представления группы* G, *то*

$$\chi_\Phi = \chi_{\Phi_1} + \ldots + \chi_{\Phi_m}.$$

Доказательство. Если V_i — пространство представления Φ_i и $\{e_{i1}, \ldots, e_{in_i}\}$ — его база, то

$$V = V_1 \oplus \ldots \oplus V_m$$

— пространство представления Φ и, согласно теореме III.1.8,

$$\{e_{11}, \ldots, e_{1n_1}, e_{21}, \ldots, e_{2n_2}, \ldots, e_{m1}, \ldots, e_{mn_m}\}$$

— его база. Если $g \in G$, то поскольку $e_{ij}\Phi(g) = e_{ij}\Phi_i(g)$ для каждого i, матрицей линейного преобразования $\Phi(g)$ в этой базе будет матрица

$$A = \begin{Vmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_m \end{Vmatrix},$$

где A_i — матрица линейного преобразования $\Phi_i(g)$ в базе $\{e_{i1}, \ldots, e_{in_i}\}$. Ввиду теоремы III.1.16

$$\chi_\Phi(g) = \operatorname{Tr}\Phi(g) = \operatorname{Tr}\Phi_1(g) + \ldots + \operatorname{Tr}\Phi_m(g) =$$
$$= \chi_{\Phi_1}(g) + \ldots + \chi_{\Phi_m}(g).$$

Теорема 9. *Пусть* $\Phi_1, \ldots, \Phi_m$ — *все эквивалентные неприводимые представления группы* G, $\dim \Phi_i = n_i$ *и* $1 \neq g \in G$. *Тогда*

$$n_1\chi_{\Phi_1}(g) + \ldots + n_m\chi_{\Phi_m}(g) = 0.$$

Доказательство. Групповая алгебра $\boldsymbol{C}G$, будучи модулем над собой, может рассматриваться как пространство некоторого представления Φ. Приняв элементы группы G за базу этого пространства, заметим, что линейное преобразование $\Phi(g)$ переводит каждый элемент h этой базы в отличный от h элемент hg той же базы. Следовательно, на главной диагонали матрицы линейного преобразования $\Phi(g)$ в этой базе стоят нули, и

$$\chi_\Phi(g) = 0$$

по теореме III.1.16. С другой стороны, из теорем 2, III.2.16 и III.2.15 (5) вытекает, что

$$\Phi = \underbrace{(\Phi_1 \oplus \ldots \oplus \Phi_1)}_{n_1 \text{ раз}} \oplus \underbrace{(\Phi_2 \oplus \ldots \oplus \Phi_2)}_{n_2 \text{ раз}} \oplus \ldots \oplus \underbrace{(\Phi_m \oplus \ldots \oplus \Phi_m)}_{n_m \text{ раз}}.$$

В силу теоремы 8

$$0 = \chi_\Phi(g) = n_1\chi_{\Phi_1}(g) + n_2\chi_{\Phi_2}(g) + \ldots + n_m\chi_{\Phi_m}(g).$$

Если $g \in G$, то обозначим через $K(g)$ множество всех элементов группы G, сопряженных с g, через $|K(g)|$ — число элементов множества $K(g)$ и через z_g — элемент групповой алгебры $\boldsymbol{C}G$, равный сумме всех элементов из $K(g)$. В силу теоремы III.2.8, z_g — центральный элемент алгебры $\boldsymbol{C}G$. Теоремы III.2.15 (2) и III.2.16 позволяют указать изоморфизм φ алгебры $\boldsymbol{C}G$ на внешнюю прямую сумму

$$R_1 \oplus \ldots \oplus R_m$$

алгебр матриц над полем $\boldsymbol{C}$. Ввиду теорем II.4.12 и III.2.15 (6)

$$\varphi(z_g) = (\lambda_1(g)E, \ldots, \lambda_m(g)E), \qquad (*)$$

где $\lambda_i(g)$ — комплексные числа. Если, далее, Φ — неприводимое представление группы G и M — модуль представления Φ, то, по теореме 2, M — неприводимый правый $\boldsymbol{C}G$-модуль. Теоремы II.6.8 и III.2.15 (3) позволяют считать, что M — минимальный правый идеал алгебры $\boldsymbol{C}G$, причем $\varphi(M)$ принадлежит в точности одному

прямому слагаемому R_i. Комплексное число $\lambda_i(g)$ из формулы (*) назовем *центральной* Φ-*компонентой элемента* g и будем обозначать через $\lambda_\Phi(g)$. Наконец, если $r \in CG$, то обозначим через $T(r)$ линейное преобразование линейного пространства M, определяемое равенством

$$xT(r) = xr$$

для всех $x \in M$. Поскольку пространство M является правым CG-модулем, то $T(r)$ действительно оказывается линейным преобразованием пространства M.

Теорема 10. *Для любого неприводимого представления* Φ *группы* G *имеем*

$$\operatorname{Tr} T(z_g) = |K(g)| \chi_\Phi(g) = \lambda_\Phi(g) \dim \Phi.$$

Доказательство. В силу теорем 2, III.2.13 и III.2.15 (3), $\dim \Phi$ равна порядку матрицы $\lambda_\Phi(g)E$ в формуле (*). Пусть для определенности $\lambda_\Phi(g) = \lambda_1(g) = \lambda_1$. Если $x \in M$, то, вспоминая, что $\varphi(M) \subseteq R_1$, можно записать

$$\varphi(x) = (A, 0, \ldots, 0),$$

где A — некоторая матрица. Поэтому

$\varphi(xz_g) = \varphi(x)\varphi(z_g) = (A, 0, \ldots, 0)(\lambda_1(g)E, \lambda_2(g)E, \ldots$
$\ldots, \lambda_m(g)E) = \lambda_1(A, 0, \ldots, 0) = \lambda_1\varphi(x) = \varphi(\lambda_1 x)$, откуда, поскольку φ — изоморфизм, получаем

$$xT(z_g) = xz_g = \lambda_1 x.$$

Следовательно, $\lambda_1 E$, где E — единичная матрица порядка $\dim \Phi$, служит матрицей линейного преобразования $T(z_g)$ в любой базе, и по теореме III.1.16

$$\operatorname{Tr} T(z_g) = \lambda_1 \cdot \dim \Phi.$$

С другой стороны, из теорем III.1.15 и III.1.16 вытекает, что след суммы линейных преобразований равен сумме следов слагаемых. Поэтому

$$\operatorname{Tr} T(z_g) = \sum_{x \in K(g)} \operatorname{Tr} T(x) = \sum_{x \in K(g)} \chi_\Phi(x) = |K(g)| \chi_\Phi(g),$$

ибо $\chi_\Phi(x) = \chi_\Phi(g)$ по теореме 5.

Теорема 11. *Если* Φ *— неприводимое представление группы* G, $\dim \Phi = n$ *и* $a, b \in G$, *то*

$$z_a z_b = \sum_{c \in S} \lambda_{ab}^{(c)} z_c,$$

где S *— множество представителей классов сопряженности группы* G, *а* $\lambda_{ab}^{(c)}$ *— целые числа,*

$$\lambda_\Phi(a)\lambda_\Phi(b) = \sum_{c\in S} \lambda_{ab}^{(c)}\lambda_\Phi(c),$$

$$\lambda_\Phi(1) = 1$$

и

$$|K(a)|\,|K(b)|\,\chi_\Phi(a)\chi_\Phi(b) = n\sum_{c\in S}\lambda_{ab}^{(c)}\,|K(c)|\,\chi_\Phi(c).$$

Доказательство. В силу теоремы III.2.8, элементы z_c, где c пробегает S, образуют базу центра Z алгебры CG. Поскольку $z_a z_b \in Z$, то

$$z_a z_b = \sum_{c\in S}\lambda_{ab}^{(c)} z_c$$

для некоторых $\lambda_{ab}^{(c)} \in C$. Ясно, что в левой части этого равенства коэффициентами при элементах группы G служат целые числа. В силу единственности выражения элемента линейного пространства через базу, то же самое верно и для правой части равенства, т. е. $\lambda_{ab}^{(c)}$ должны быть целыми числами. Далее, ввиду равенства (*) на с. 215, имеем

$$\begin{aligned}(\lambda_1(a)\lambda_1(b)E, \ldots, \lambda_m(a)\lambda_m(b)E) &= \\ = (\lambda_1(a)E\cdot\lambda_1(b)E, \ldots, \lambda_m(a)E\cdot\lambda_m(b)E) &= \\ = \varphi(z_a)\varphi(z_b) = \varphi(z_a z_b) = \varphi\Big(\sum_{c\in S}\lambda_{ab}^{(c)}z_c\Big) &= \\ = \sum_{c\in S}\lambda_{ab}^{(c)}\varphi(z_c) = \sum_{c\in S}\lambda_{ab}^{(c)}(\lambda_1(c)E, \ldots, \lambda_m(c)E).&\end{aligned}$$

Отсюда, поскольку в силу определения $\lambda_\Phi(g) = \lambda_i(g)$ для всех $g \in G$ при некотором i, вытекает, что

$$\lambda_\Phi(a)\lambda_\Phi(b) = \sum_{c\in S}\lambda_{ab}^{(c)}\lambda_\Phi(c).$$

Используя теорему 10, получаем

$$\begin{aligned}|K(a)|\,|K(b)|\,\chi_\Phi(a)\chi_\Phi(b) &= \lambda_\Phi(a)\lambda_\Phi(b)n^2 = \\ &= \sum_{c\in S}\lambda_{ab}^{(c)}\lambda_\Phi(c)n^2 = n\sum_{c\in S}\lambda_{ab}^{(c)}\,|K(c)|\,\chi_\Phi(c).\end{aligned}$$

Наконец, поскольку $z_1 = 1$ и $\varphi(1) = (\lambda_1(1)E, \ldots, \lambda_m(1)E) = (E, \ldots, E)$, имеем $\lambda_\Phi(1) = 1$, ибо, как уже отмечалось, $\lambda_\Phi(1) = \lambda_i(1)$ для некоторого номера i.

Теорема 12. *Пусть* $\Phi_1, \ldots, \Phi_m$ *— все неэквивалентные неприводимые представления группы* G, a, $b \in$

$\in G$ *и* $|G|$ *— число элементов группы* G. *Тогда*

$$\chi_{\Phi_1}(a)\chi_{\Phi_1}(b)+\ldots+\chi_{\Phi_m}(a)\chi_{\Phi_m}(b)=$$
$$=\begin{cases}0, & \text{если } b^{-1}\notin K(a),\\ \dfrac{|G|}{|K(b)|}, & \text{если } b^{-1}\in K(a).\end{cases}$$

Доказательство. Согласно теореме 11

$$|K(a)||K(b)|\chi_{\Phi_i}(a)\chi_{\Phi_i}(b)=$$
$$=n_i\sum_{c\in S}\lambda_{ab}^{(c)}|K(c)|\chi_{\Phi_i}(c) \qquad (*)$$

для каждого i, где $n_i=\dim\Phi_i$.

(а) *Если* $b^{-1}\notin K(a)$, *то* $\lambda_{ab}^{(1)}=0$.
Действительно,

$$\sum_{c\in S}\lambda_{ab}^{(c)}z_c=z_az_b=\sum_{g\in K(a)}\sum_{h\in K(b)}gh.$$

Если $\lambda_{ab}^{(1)}\neq 0$, то $gh=1$ для некоторых $g\in K(a)$ и $h\in K(b)$. Если $g=uau^{-1}$ и $h=vbv^{-1}$, где $u, v\in G$, то $uau^{-1}vbv^{-1}=1$, откуда

$$b^{-1}=v^{-1}uau^{-1}v=(v^{-1}u)\,a\,(v^{-1}u)^{-1}\in K(a),$$

вопреки условию.

(б) *Если* $b^{-1}\in K(a)$, *то* $h^{-1}\in K(a)$ *для всех* $h\in K(b)$ *и* $\lambda_{ab}^{(1)}=|K(a)|=|K(b)|$.

В самом деле, если $b^{-1}=uau^{-1}$ и $h=vbv^{-1}$, где $u, v\in G$, то

$$h^{-1}=vuau^{-1}v^{-1}=(vu)a(vu)^{-1}\in K(a).$$

Таким образом, положив $K(b)^{-1}=\{x^{-1}\mid x\in K(b)\}$, имеем $K(b)^{-1}\subseteq K(a)$. Аналогично получаем, что $K(a)^{-1}\subseteq K(b)$ и, следовательно, $K(a)\subseteq K(b)^{-1}$. Отсюда $K(a)=K(b)^{-1}$, а значит,

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

Далее, учитывая теорему 11, получаем

$$z_az_b=\sum_{h\in K(b)}h^{-1}h+\sum_{1\neq c\in S}\lambda_{ab}^{(c)}z_c$$

и, следовательно, $\lambda_{ab}^{(1)}=|K(a)|=|K(b)|$.

Суммируя равенства (*) по i и используя теорему 9, будем иметь

$$|K(a)||K(b)|\sum_{i=1}^{m}\chi_{\Phi_i}(a)\chi_{\Phi_i}(b)=\sum_{c\in S}\lambda_{ab}^{(c)}|K(c)|\sum_{i=1}^{m}n_i\chi_{\Phi_i}(c)=$$

$$=\lambda_{ab}^{(1)}|K(1)|\sum_{i=1}^{m}n_i\chi_{\Phi_i}(1)=\lambda_{ab}^{(1)}\sum_{i=1}^{m}n_i^2.$$

Ввиду (а) и (б) отсюда вытекает, что

$$|K(a)||K(b)|\sum_{c=1}^{m}\chi_{\Phi_i}(a)\chi_{\Phi_i}(b)=$$

$$=\begin{cases}0, & \text{если } b^{-1}\notin K(a),\\ \lambda_{ab}^{(1)}\sum\limits_{i=1}^{m}n_i^2=|K(a)||G|, & \text{если } b^{-1}\in K(a),\end{cases}$$

поскольку $|G|=\sum\limits_{i=1}^{m}n_i^2$ в силу теорем 2 и III.2.18. Остается разделить полученное равенство на $|K(a)||K(b)|$.

Теорема 13. *Если* $\Phi_1,\ldots,\Phi_m$ — *все неприводимые представления группы* G, *то*

$$\sum_{g\in G}\chi_{\Phi_i}(g)\overline{\chi_{\Phi_j}(g)}=\begin{cases}|G|, & \text{если } i=j,\\ 0, & \text{если } i\neq j.\end{cases}$$

Доказательство. В силу теоремы 3, группа G распадается на m классов сопряженности. Пусть $g_1,\ldots,g_m$ — представители всех этих классов. Положим

$$\chi_i=\chi_{\Phi_i},\qquad a_{ij}=\chi_i(g_j)\text{ и}$$

$$b_{ij}=\frac{|K(g_i)|}{|G|}\overline{\chi_j(g_i)}.$$

Рассмотрим матрицы $A=\|a_{ij}\|$, $B=\|b_{ij}\|$ и $C=BA$. Ввиду теорем 7 и 12

$$c_{ij}=\sum_{k=1}^{m}b_{ik}a_{kj}=\frac{1}{|G|}\sum_{k=1}^{m}|K(g_i)|\overline{\chi_k(g_i)}\chi_k(g_j)=$$

$$=\frac{1}{|G|}|K(g_i)|\sum_{k=1}^{m}\chi_k(g_i^{-1})\chi_k(g_j)=\begin{cases}1, & \text{если } i=j,\\ 0, & \text{если } i\neq j.\end{cases}$$

Таким образом, $BA=E$. Но тогда $AB=E$, т. е.

$$\frac{1}{|G|}\sum_{k=1}^{m}K(g_k)\chi_i(g_k)\overline{\chi_j(g_k)}=\sum_{k=1}^{m}a_{ik}b_{kj}=\begin{cases}1, & \text{если } i=j,\\ 0, & \text{если } i\neq j.\end{cases}$$

Ввиду теоремы 5 отсюда вытекает

$$\sum_{g\in G}\chi_i(g)\overline{\chi_j(g)}=\sum_{k=1}^{m}|K(g_k)|\,\chi_i(g_k)\overline{\chi_j(g_k)}=\begin{cases}|G|, & \text{если } i=j,\\ 0, & \text{если } i\neq j.\end{cases}$$

Теорема 14. *Если* Φ *и* Ψ *— представления группы* G *и* $\chi_\Phi=\chi_\Psi$, *то представления* Φ *и* Ψ *эквивалентны.*

Доказательство. Пусть M и N — модули представлений Φ и Ψ соответственно. Ввиду следствия теоремы II.6.8, из теоремы III.2.16 вытекает, что модули M и N изоморфны внешним прямым суммам минимальных правых идеалов алгебры CG, скажем,

$$\underbrace{(M_1\oplus\ldots\oplus M_1)}_{k_1\text{ раз}}\oplus\underbrace{(M_2\oplus\ldots\oplus M_2)}_{k_2\text{ раз}}\oplus\ldots$$

$$\ldots\oplus\underbrace{(M_m\oplus\ldots\oplus M_m)}_{k_m\text{ раз}}$$

и

$$\underbrace{(M_1\oplus\ldots\oplus M_1)}_{l_1\text{ раз}}\oplus\underbrace{(M_2\oplus\ldots\oplus M_2)}_{l_2\text{ раз}}\oplus\ldots$$

$$\ldots\oplus\underbrace{(M_m\oplus\ldots\oplus M_m)}_{l_m\text{ раз}}$$

соответственно. Если Φ_i — неприводимое представление с модулем представления M_i (учесть теорему 2), то в силу теоремы 8

$$\chi_\Phi(g)=k_1\chi_{\Phi_1}(g)+\ldots+k_m\chi_{\Phi_m}(g)$$

для всех $g\in G$. В силу теоремы 13

$$\sum_{g\in G}\chi_\Phi(g)\overline{\chi_{\Phi_i}(g)}=k_i|G|.$$

По тем же соображениям

$$\sum_{g\in G}\chi_\Psi(g)\overline{\chi_{\Phi_i}(g)}=l_i|G|.$$

Отсюда

$$k_i=\frac{\sum\limits_{g\in G}\chi_\Phi(g)\overline{\chi_{\Phi_i}(g)}}{|G|}=\frac{\sum\limits_{g\in G}\chi_\Psi(g)\overline{\chi_{\Phi_i}(g)}}{|G|}=l_i.$$

Следовательно, модули представлений Φ и Ψ изоморфны, а значит, сами представления эквивалентны по теореме 1.

Наконец, докажем, что размерность неприводимого представления делит порядок группы. С этой целью на-

зовем комплексное число ξ *целым алгебраическим*, если

$$\xi^n + a_1\xi^{n-1} + \ldots + a_{n-1}\xi + a_n = 0,$$

где $a_1, \ldots, a_n$ — целые числа.

Теорема 15. *Если рациональное число является целым алгебраическим, то оно целое.*

Доказательство. Пусть $\frac{p}{q}$ — несократимое представление рационального целого алгебраического числа. Тогда

$$\left(\frac{p}{q}\right)^n + a_1\left(\frac{p}{q}\right)^{n-1} + \ldots + a_{n-1}\left(\frac{p}{q}\right) + a_n = 0,$$

где $a_1, \ldots, a_n$ — целые числа. Отсюда

$$p^n = -(a_1p^{n-1}q + \ldots + a_{n-1}pq^{n-1} + a_nq^n),$$

т. е. p^n делится на q, что противоречит взаимной простоте чисел p и q.

Теорема 16. *Целые алгебраические числа образуют подкольцо поля комплексных чисел.*

Доказательство. Сначала установим:

Лемма. *Если* $\omega_1, \ldots, \omega_m \in \boldsymbol{C}$ *и группа*

$$M = \boldsymbol{Z}\omega_1 + \ldots + \boldsymbol{Z}\omega_m$$

является подкольцом поля $\boldsymbol{C}$, *то* M *состоит из целых алгебраических чисел.*

Действительно, если $\omega_1 = \ldots = \omega_m = 0$, то $M = 0$, и лемма справедлива. Допустим, что не все ω_i равны 0. Если $\alpha \in M$, то

$$\alpha\omega_i = \sum_{j=1}^{m} a_{ij}\omega_j$$

для некоторых целых чисел a_{ij}. Тогда система линейных уравнений:

$$\begin{cases} (a_{11} - \alpha)x_1 + a_{12}x_2 + \ldots + a_{1m}x_m = 0, \\ a_{21}x_1 + (a_{22} - \alpha)x_2 + \ldots + a_{2m}x_m = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + (a_{mm} - \alpha)x_m = 0 \end{cases}$$

имеет ненулевое решение $(\omega_1, \ldots, \omega_m)$. В силу следствия теоремы I.3.5, определитель $|A - \alpha E| = 0$, т. е. α оказывается корнем многочлена $|A - tE|$ с целыми коэффициентами, причем коэффициент при старшем члене равен ± 1. А это и означает, что α — целое алгебраическое число.

Для доказательства теоремы допустим, что α и β — целые алгебраические числа. Тогда

$$\alpha^m + a_1\alpha^{m-1} + \ldots + a_m = 0 \qquad (*)$$

и

$$\beta^n + b_1\beta^{n-1} + \ldots + b_n = 0, \qquad (**)$$

где $a_1, \ldots, a_m, b_1, \ldots, b_n$ — целые числа. Рассмотрим множество M всех комплексных чисел, представимых в форме

$$\sum_{i,\,j} c_{ij}\alpha^i\beta^j,$$

где $0 \leqslant i < m$, $0 \leqslant j < n$, а c_{ij} — целые числа. Равенства $(*)$ и $(**)$ позволяют показать, что $\alpha^k\beta^l \in M$ при любых неотрицательных целых k и l (для этого достаточно заметить, что соотношения $(*)$ и $(**)$ позволяют выразить α^k и β^l, где $k \geqslant m$ и $l \geqslant n$, через меньшие степени α и β соответственно). Следовательно, M — подкольцо поля $\boldsymbol{C}$. В силу леммы, все его элементы и, в частности, $\alpha + \beta$, $0 - \alpha$ и $\alpha\beta$ — целые алгебраические числа, что и доказывает теорему.

Теорема 17. *Если* Φ *— неприводимое представление группы* G *и* $g \in G$, *то центральная* Φ*-компонента* $\lambda_\Phi(g)$ *элемента* g *является целым алгебраическим числом.*

Доказательство. Пусть $g_1, \ldots, g_m$ — представители всех классов сопряженности группы G. В силу теоремы 11

$$\lambda_\Phi(g)\lambda_\Phi(g_i) = \sum_{k=1}^{m} \lambda_{ik}\lambda_\Phi(g_k),$$

где $\lambda_{ik} = \lambda_{gg_i}^{(g_k)}$ — целые числа. Тогда строка

$$(\lambda_\Phi(g_1), \ldots, \lambda_\Phi(g_m))$$

служит решением системы линейных уравнений:

$$\begin{cases} (\lambda_{11} - \lambda_\Phi(g))x_1 + \lambda_{12}x_2 + \ldots + \lambda_{1m}x_m = 0, \\ \lambda_{21}x_1 + (\lambda_{22} - \lambda_\Phi(g))x_2 + \ldots + \lambda_{2m}x_m = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \lambda_{m1}x_1 + \lambda_{m2}x_2 + \ldots + (\lambda_{mm} - \lambda_\Phi(g))x_m = 0. \end{cases}$$

В силу теоремы 11 $\lambda_\Phi(1) = 1$, т. е. рассматриваемая система имеет ненулевое решение. Пусть $A = \| \lambda_{ij} \|$. В силу следствия теоремы I.3.5, определитель $|A - \lambda_\Phi(g)E| = 0$. Следовательно, $\lambda_\Phi(g)$, являясь корнем многочлена $|A - tE| = 0$ с целыми коэффициентами и коэффициен-

том ± 1 при старшем члене, оказывается целым алгебраическим числом.

Теорема 18. *Если* Φ *— представление группы* G *и* $g \in G$, *то* $\chi_\Phi(g)$ *— целое алгебраическое число, причем* $|\chi_\Phi(g)| \leqslant \dim \Phi$.

Доказательство. Допустим, что $\dim \Phi = n$. Если $\lambda_1, \ldots, \lambda_n$ — все характеристические корни линейного преобразования $\Phi(g)$ (здесь каждый корень выписан столько раз, какова его кратность), то

$$\chi_\Phi(g) = \lambda_1 + \ldots + \lambda_n.$$

Согласно теореме 4, λ_i — корни из единицы, т. е. целые алгебраические числа. В силу теоремы 16, $\chi_\Phi(g)$ также целое алгебраические число. Далее, ввиду свойства (2) нормы комплексного числа (см. с. 100), $|\lambda_i| = 1$. Поэтому, в силу свойства (3) нормы комплексного числа (там же), имеем

$$|\chi_\Phi(g)| \leqslant |\lambda_1| + \ldots + |\lambda_n| = n = \dim \Phi.$$

Теорема 19. *Если* Φ *— неприводимое представление группы* G, *то число* $\dim \Phi$ *делит* $|G|$.

Доказательство. В силу теорем 10 и 17

$$\frac{|K(g)|\chi_\Phi(g)}{\dim \Phi} = \lambda_\Phi(g)$$

— целое алгебраическое число для всякого $g \in G$. По теореме 18 целым алгебраическим является и число $\chi_\Phi(g)$. Число $\overline{\chi_\Phi(g)}$, будучи корнем того же самого целочисленного многочлена*), является целым алгебраическим. Применяя теорему 16, убеждаемся, что

$$\frac{|K(g)|\chi_\Phi(g)}{\dim \Phi} \cdot \overline{\chi_\Phi(g)}$$

— целое алгебраическое число для всякого $g \in G$. Отсюда, обозначив через $g_1, \ldots, g_m$ представители всех классов сопряженности группы G и снова применяя теорему 16, видим, что

$$\sum_{i=1}^{m} \frac{|K(g_i)|\chi_\Phi(g_i)\overline{\chi_\Phi(g_i)}}{\dim \Phi}$$

*) Здесь используется тот факт, что число, сопряженное корню многочлена с действительными коэффициентами, является корнем того же самого многочлена (см. с. 160 учебника А. Г. Куроша или с. 282 учебника А. И. Кострикина).

— целое алгебраическое число. Ввиду теорем 5 и 13, целым алгебраическим оказывается и число

$$\frac{|G|}{\dim \Phi} = \frac{\sum\limits_{g \in G} \chi_\Phi(g)\,\overline{\chi_\Phi(g)}}{\dim \Phi} = \frac{\sum\limits_{i=1}^{m} |K(g_i)|\,\chi_\Phi(g_i)\,\overline{\chi_\Phi(g_i)}}{\dim \Phi}.$$

Но число $\frac{|G|}{\dim \Phi}$, будучи рациональным, должно быть целым в силу теоремы 15. А это и означает, что число $|G|$ делится на $\dim \Phi$.

Упражнения

1. Доказать, что конечная группа коммутативна тогда и только тогда, когда все ее непроводимые представления одномерны.

2. Составить таблицы характеров для следующих групп: $\boldsymbol{Z}/4\boldsymbol{Z}$, $(\boldsymbol{Z}/2\boldsymbol{Z})\times(\boldsymbol{Z}/2\boldsymbol{Z})$, $\boldsymbol{Z}/6\boldsymbol{Z}$, знакопеременные группы $\mathfrak{A}_3$ и $\mathfrak{A}_4$ (см. конец § 3 гл. II), группа кватернионов, т. е. подгруппа $\{\pm 1, \pm i, \pm j, \pm k\}$ мультипликативной группы тела кватернионов (см. конец § 4, гл. II). При составлении таблицы полезно пользоваться «соотношениями ортогональности», установленными в теоремах 12 и 13. Найти неприводимые представления этих групп.

3. Доказать, что наименьшая некоммутативная группа содержит 6 элементов.

4. Пусть Φ — представление группы G. Рассматривая $\Phi(g)$ как матрицу, положим $\Psi(g) = (\Phi(g^{-1}))^*$ для всех $g \in G$. Доказать, что Ψ — представление группы G и что представления Φ и Ψ эквивалентны тогда и только тогда, когда $\chi_\Phi(g)$ — действительное число для всех $g \in G$. Установить, что представление Ψ неприводимо тогда и только тогда, когда неприводимо представление Φ.

5. Доказать, что группа, порожденная двумя элементами a и b, для которых справедливы равенства $a^5 = 1$, $b^2 = 1$ и $abab = 1$, содержит 10 элементов. Найти неприводимые представления этой группы.

6. Доказать, что группа, порожденная двумя элементами a и b, для которых справедливы равенства $a^4 = 1$, $b^2 = 1$ и $abab = 1$, содержит 8 элементов. Найти неприводимые представления этой группы. Доказать, что она не изоморфна группе кватернионов (см. упражднение 2).

§ 2. Приложение теории представлений

В качестве одного из приложений установим достаточное условие разрешимости, обобщающее теоремы II.7.11 и II.7.12. Однако для этого нам понадобятся некоторые дополнительные свойства целых алгебраических чисел.

Пусть $\boldsymbol{Q}$ — поле рациональных чисел, ξ — комплексное число и $\boldsymbol{Q}[\xi]$ — линейная оболочка системы $\{1, \xi, \xi^2, \ldots\}$ в поле комплексных чисел, рассматриваемом как

линейное пространство над полем Q. Легко проверяется, что $Q[\xi]$ — подкольцо поля комплексных чисел.

Теорема 1. *Пусть ω_0 — целое алгебраическое число. Тогда существует неприводимый над полем Q многочлен f с целыми коэффициентами *) такой, что коэффициент при его старшем члене равен 1 и $f(\omega_0) = 0$. Если ω — какой-либо корень многочлена f, то существует изоморфизм φ кольца $Q[\omega_0]$ на кольцо $Q[\omega]$ такой, что $\varphi(\omega_0) = \omega$ и $\varphi(r) = r$ для всех $r \in Q$.*

Доказательство. Напомним, что многочлен g с целыми коэффициентами называется *примитивным*, если не существует простого числа p, на которое делятся все его коэффициенты. Поскольку ω_0 — целое алгебраическое число, то, по определению, существует многочлен g с целыми коэффициентами такой, что коэффициент при его старшем члене равен 1 и $g(\omega_0) = 0$. Многочлен g можно представить как $g = g_1 \ldots g_m$, где g_i — многочлены, неприводимые над полем Q **). Отсюда

$$g_1(\omega_0) \ldots g_m(\omega_0) = g(\omega_0) = 0,$$

значит, например, $g_1(\omega_0) = 0$. Можно считать, что многочлен g_1 примитивен. Положим $g_2 \ldots g_m = \frac{rh}{s}$, где r и s — взаимно простые целые числа, причем $r > 0$, а h — примитивный многочлен. По лемме Гаусса ***) многочлен $g_1 h$ примитивен. Поэтому из равенства

$$sg = sg_1 \ldots g_m = rg_1 h$$

вытекает, что $s = 1$. Поскольку коэффициент при старшем члене многочлена g равен 1, то то же самое верно и для многочлена g_1. Положив $f = g_1$, убедимся в справедливости первого утверждения теоремы. Далее, для любых $r_0, r_1, \ldots, r_m \in Q$ положим

$$\varphi\left(\sum_{i=0}^{m} r_i \omega_0^i\right) = \sum_{i=0}^{m} r_i \omega^i.$$

Если $\sum_{i=0}^{m} r_i \omega_0^i = 0$, то рассмотрим многочлен $g = \sum_{i=0}^{m} r_i x^i$. Если $d =$ н.о.д. (f, g), то $d = uf + vg$ для некоторых мно-

*) Напомним, что многочлен над полем P называется *неприводимым*, если он не может быть представлен в виде произведения многочленов с коэффициентами из P, имеющих меньшую степень.

**) См. с. 290 учебника А. Г. Куроша или с. 229 учебника А. И. Кострикина.

***) См. с. 351 учебника А. Г. Куроша или с. 230 учебника А. И. Кострикина.

гочленов u и v*). Отсюда

$$d(\omega_0) = u(\omega_0) f(\omega_0) + v(\omega_0) g(\omega_0) = 0.$$

Следовательно, степень многочлена $d \geqslant 1$. Но $f = dh$ для некоторого многочлена h, и поскольку f неприводим над полем $\boldsymbol{Q}$, то $0 \neq h \in \boldsymbol{Q}$. С другой стороны, $g = dk$ для некоторого многочлена k, откуда $g = fkh^{-1} = fq$, где $q = kh^{-1}$. Но тогда

$$\varphi\left(\sum_{i=0}^{m} r_i \omega_0^i\right) = \sum_{i=0}^{m} r_i \omega^i = g(\omega) = f(\omega) q(\omega) = 0,$$

что доказывает корректность определения отображения φ кольца $\boldsymbol{Q}[\omega_0]$ в кольцо $\boldsymbol{Q}[\omega]$. Простые выкладки показывают, что это гомоморфное наложение кольца $\boldsymbol{Q}[\omega_0]$ на кольцо $\boldsymbol{Q}[\omega]$. Если

$$\varphi\left(\sum_{i=0}^{m} r_i \omega_0^i\right) = 0,$$

то, как и выше, убеждаемся, что $g = fq$ для некоторого многочлена q, откуда $g(\omega_0) = f(\omega_0) q(\omega_0) = 0$. Тем самым доказано, что φ — изоморфизм колец.

Теорема 2 (критерий непростоты). *Если класс сопряженности элемента g группы G содержит p^d элементов, где p простое и $d \geqslant 1$, то группа G содержит нормальную подгруппу, отличную от G и от единичной подгруппы* (т. е. группа G не является простой).

Доказательство. Допустим, что группа G не содержит нетривиальных нормальных подгрупп. Обозначим через K класс сопряженности элемента g. Поскольку $|K| \neq 1$, то группа G не коммутативна.

Лемма. *Если Φ — не единичное неприводимое представление группы G и $n = \dim \Phi$, то*

$$n \cdot \chi_\Phi(g) = p\alpha,$$

где α — целое алгебраическое число.

Действительно, справедливость леммы тривиальна, если $\chi_\Phi(g) = 0$, и вытекает из теорем 16 и 18 из § 1, если n делится на p. Если это не так, то

$$\text{н.о.д.}(|K|, n) = \text{н.о.д.}(p^d, n) = 1.$$

Следовательно,

$$u \cdot n + v|K| = 1$$

*) См. с. 140 учебника А. Г. Куроша или с. 227 учебника А. И. Кострикина.

для некоторых целых u и v*). В силу теорем 10 и 17 из § 1,

$$\frac{|K|\chi_\Phi(g)}{n} = \lambda_\Phi(g)$$

— целое алгебраическое число. Ввиду теорем 16 и 18 из § 1, целым алгебраическим оказывается и число

$$\omega = \frac{\chi_\Phi(g)}{n} = u\chi_\Phi(g) + v\frac{|K|\chi_\Phi(g)}{n}.$$

Допустим, что $|\chi_\Phi(g)| = \dim \Phi$, т. е. $|\operatorname{Tr}\Phi(g)| = \dim \Phi$. Но, ввиду теоремы 4 из § 1, норма характеристических корней линейного преобразования $\Phi(g)$ равна 1. Поэтому из той же теоремы 4 вместе с теоремами III.1.19 и III.1.20 вытекает, что $\Phi(g) = \lambda_0 1_V$, где V — пространство представления Φ и $\lambda_0 \in \boldsymbol{C}$. Обозначив через H множество всех таких элементов x из G, что $\Phi(x) = \lambda 1_V$ для некоторого $\lambda \in \boldsymbol{C}$, нетрудно заметить, что H — нормальная подгруппа группы G. Поскольку $g \in H$, то $H \neq \{1\}$ и в силу допущения $H = G$. Таким образом, Φ — гомоморфизм группы G в группу всех линейных преобразований вида $\lambda 1_V$. Без труда проверяется, что эта группа коммутативна. Если $\operatorname{Ker}\Phi = \{1\}$, то коммутативной должна быть и группа G, что несовместимо с $|K| \neq 1$. Следовательно, $\operatorname{Ker}\Phi = G$, т. е., вопреки условию леммы, представление Φ оказывается единичным. Тем самым установлено, что $|\chi_\Phi(g)| \neq \dim \Phi$, а значит, $|\chi_\Phi(g)| < \dim \Phi = n$ по теореме 18 из § 1. Допустим, что все характеристические корни линейного преобразования $\Phi(g)$ совпадают. Тогда из теоремы III.1.20 и теоремы 4 из § 1 вытекает, что $\Phi(g) = \lambda 1_V$, где $\lambda \in \boldsymbol{C}$. Отсюда, учитывая ту же теорему 4 и свойство (2) нормы (см. с. 100), получаем

$$n > |\chi_\Phi(g)| = |\operatorname{Tr}\Phi(g)| = |n\lambda| = n|\lambda| = n,$$

что невозможно. Следовательно,

$$n\omega = \chi_\Phi(g) = \lambda_1 + \ldots + \lambda_n,$$

где $\lambda_1, \ldots, \lambda_n$ — корни степени n из единицы, среди которых есть различные. Ввиду теоремы 1 существует неприводимый над полем рациональных чисел многочлен f с целыми коэффициентами такой, что его коэффициент при старшем члене равен 1 и $f(\omega) = 0$. Если ω' — ка-

*) См. примечание на с. 80.

кой-либо другой корень многочлена f, то в силу той же теоремы 1 существует описанный там изоморфизм φ, для которого $\varphi(\omega) = \omega'$. Отсюда

$$n\omega' = \varphi(n\omega) = \varphi(\lambda_1) + \ldots + \varphi(\lambda_n).$$

Поскольку

$$(\varphi(\lambda_i))^n = \varphi(\lambda_i^n) = \varphi(1) = 1,$$

то $n\omega'$ равен сумме корней степени n из единицы, среди которых есть различные. Используя лемму, установленную при доказательстве теоремы III.1.19, нетрудно получить, что $|n\omega'| < n$, а значит, $|\omega'| < 1$. Таким образом, нормы всех корней многочлена f меньше 1. В силу формул Виета*) и свойства (2) нормы комплексного числа (см. с. 100), то же самое верно и для свободного члена этого многочлена. Поскольку этот свободный член — целое число, он равен нулю, вопреки неприводимости многочлена f. Полученное противоречие доказывает лемму.

Возвращаясь к доказательству теоремы, обозначим через Φ_0 единичное, а через $\Phi_1, \ldots, \Phi_m$ все остальные неприводимые представления группы G, положим $n_i = \dim \Phi_i$ и, воспользовавшись теоремой 9 из § 1, запишем

$$1 + n_1\chi_{\Phi_1}(g) + \ldots + n_m\chi_{\Phi_m}(g) = 0.$$

Ввиду леммы $n_i\chi_{\Phi_i}(g) = p\alpha_i$, где α_i — целое алгебраическое число, для $i = 1, \ldots, m$. Ввиду теоремы 16 из § 1

$$-\frac{1}{p} = \alpha_1 + \ldots + \alpha_m$$

— целое алгебраическое число, вопреки теореме 15 из § 1. Полученное противоречие завершает доказательство теоремы.

Т е о р е м а 3 (теорема Бернсайда). *Если G — группа и $|G| = p^m q^n$, где p и q простые, то группа G разрешима.*

Д о к а з а т е л ь с т в о. Будем вести индукцию по $m + n$. Если $m + n = 1$, то $|G|$ — простое число. В силу теоремы II.3.3, G не содержит нетривиальных подгрупп. Следовательно, она циклическая, а значит, коммутативная.

Л е м м а. *Если $m + n > 1$, то G или коммутативная, или содержит нетривиальную нормальную подгруппу.*

---

*) Именно: что произведение корней многочлена со старшим коэффициентом 1 с точностью до знака совпадает с произведением корней (см. примечание ***) на с. 181).

Действительно, допустим для определенности, что $n \geqslant 1$. Тогда по теореме II.7.8, G содержит такую подгруппу H, что $|H| = q^n$. В силу теоремы II.3.24, центр группы H содержит элемент $z \neq 1$. По теореме II.3.23.

$$|K(z)|\,|C(z)| = |G|,$$

где $K(z)$ — класс сопряженности элемента z в группе G. Кроме того, $H \subseteq C(z)$. Ввиду теоремы I.3.3′ $|C(z)| = p^d q^n$, где $0 \leqslant d \leqslant m$, а значит, $|K(z)| = p^{m-d}$. Если $m - d > 0$, то применима теорема 2. Если же $m - d = 0$, то $|K(z)| = 1$, т. е. z принадлежит центру Z группы G. Если $G = Z$, то G коммутативна. В противном случае Z оказывается нетривиальной нормальной подгруппой группы G в силу теоремы II.3.20.

Для доказательства теоремы заметим, что если G не коммутативна, то она согласно лемме содержит нетривиальную нормальную подгруппу H. В силу теоремы II.3.3′, как число элементов группы H, так и число элементов факторгруппы G/H являются произведением степеней не более чем двух простых чисел. В силу индуктивного предположения, обе они разрешимы, и разрешимость группы G вытекает из теоремы II.7.9.

Замечание. Отметим, что только в самое последнее время удалось найти доказательство теоремы Бернсайда, не использующее теории представлений (см. Гагеи Т. М. Некоторые вопросы теории конечных групп, § 8—9.//К теории конечных групп: Пер. с англ./Под ред. А. И. Кострикина.— М.: Мир, 1979).

В заключение опишем группы, содержащие не более 10 элементов.

Подгруппа $\{\pm 1, \pm \boldsymbol{i}, \pm \boldsymbol{j}, \pm \boldsymbol{k}\}$ мультипликативной группы тела кватернионов (см. с. 102) называется *группой кватернионов*.

Условимся говорить, что группа G *порождается своим подмножеством* X, если никакая отличная от G подгруппа группы G не содержит множества X. Нетрудно доказать, что в этом случае каждый элемент g группы G может быть представлен в форме

$$g = x_1^{\varepsilon_1} \ldots x_m^{\varepsilon_m},$$

где $x_i \in X$ и $\varepsilon_i = \pm 1$, вообще говоря, различными способами.

Теорема 4. *Группа G изоморфна группе кватернионов тогда и только тогда, когда $|G| = 8$ и G порождается элементами a и b, удовлетворяющими условиям $a^4 = 1$, $a^2 = b^2$ и $aba = b$.*

Доказательство. Если G — группа кватернионов, то из таблицы умножения, приведенной на с. 102, видно, что $-1=i^2$, $1=i^4$, $-i=i^3$, $-j=i^2j$, $k=ij$ и $-k=i^3j$, т. е. G порождается множеством $\{i, j\}$. С помощью той же таблицы умножения получаем $i^2=-1=j^2$ и $iji=j$. Пусть теперь G — группа, удовлетворяющая условиям теоремы. Тогда $ba=a^3b$, $bab=a^3b^2=a^5=a$ и $abab=a^2$, т. е. возникает следующая таблица умножения:

·	1	a	b	ab
1	1	a	b	ab
a	a	a^2	ab	a^2b
b	b	$a^2(ab)$	a^2	a
ab	ab	b	a^2a	a^2

Сравнивая ее с таблицей умножения, приведенной на с. 102, и замечая, что a^2 лежит в центре группы G, нетрудно убедиться, что отображение φ группы кватернионов Q в группу G, задаваемое таблицей

x	1	i	j	k	-1	$-i$	$-j$	$-k$
$\varphi(x)$	1	a	b	ab	a^2	a^2a	a^2b	$a^2(ab)$

оказывается гомоморфизмом. Поскольку a, $b\in\operatorname{Im}\varphi$, то ввиду теоремы II.3.5 $\operatorname{Im}\varphi=G$, т. е. φ является наложением. Поскольку $|Q|=8=|G|$, то отображение φ взаимно однозначно, т. е. изоморфизм.

Пусть $\theta=\frac{2\pi}{n}$. Простой подсчет показывает, что матрицы

$$\begin{Vmatrix}\cos k\theta & -\sin k\theta\\ \sin k\theta & \cos k\theta\end{Vmatrix},\quad \begin{Vmatrix}\cos k\theta & -\sin k\theta\\ -\sin k\theta & -\cos k\theta\end{Vmatrix}\quad (k=0, 1, \ldots, n-1)$$

образуют подгруппу группы невырожденных матриц второго порядка над полем действительных чисел. Эта подгруппа называется *группой диэдра* и обозначается через D_n. Можно показать, что группа D_n изоморфна группе симметрий правильного n-угольника (см. Кострикин А. И. Введение в алгебру.— М.: Наука, 1977, с. 327—328).

Теорема 5. *Группа G изоморфна группе диэдра D_n тогда и только тогда, когда $|G|=2n$ и G порождается элементами g и a, удовлетворяющими условиям $g^n=a^2=agag=1$.*

Доказательство. Если $G = D_n$, то, как легко видеть, указанные соотношения справедливы для элементов

$$g = \begin{Vmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{Vmatrix} \quad \text{и} \quad a = \begin{Vmatrix} 1 & 0 \\ 0 & -1 \end{Vmatrix}.$$

Пусть теперь G — группа, удовлетворяющая условиям теоремы. Тогда $ga = ag^{n-1}$, откуда легко вывести

$$g^s a = ag^{s(n-1)},$$
$$g^s \cdot ag^t = ag^{s(n-1)+t},$$
$$ag^s \cdot ag^t = g^{s(n-1)+t}$$

и

$$ag^s \cdot ag^t = g^{s(n-1)+s} = g^{ns} = 1,$$

где $s,\ t = 1, 2, \ldots, n-1$. Эти равенства показывают, что

$$H = \{1, g, \ldots, g^{n-1}, a, ag, \ldots, ag^{n-1}\}$$

— подгруппа группы G. Поскольку $a,\ g \in H$, то $G = H$. Положим

$$G_k = \begin{Vmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{Vmatrix} \quad \text{и} \quad A = \begin{Vmatrix} 1 & 0 \\ 0 & -1 \end{Vmatrix}.$$

Тогда

$$AG_k = \begin{Vmatrix} \cos k\theta & -\sin k\theta \\ -\sin k\theta & -\cos k\theta \end{Vmatrix}.$$

Далее определим наложение φ: $D_n \to G$, положив

$$\varphi(G_k) = g^k \quad \text{и} \quad \varphi(AG_k) = ag^k.$$

Поскольку $|D_n| = 2n = |G|$, то φ — взаимно однозначное отображение. Равенства

$$\varphi(G_kG_l) = \varphi(G_{k+l}) = g^{k+l} = \varphi(G_k)\varphi(G_l),$$
$$\varphi(G_k \cdot AG_l) = \varphi(AG_{l-k}) = ag^{l-k} = g^k \cdot ag^l = \varphi(G_k)\varphi(AG_l),$$
$$\varphi(AG_kG_l) = \varphi(AG_{k+l}) = ag^{k+l} = ag^k \cdot g^l = \varphi(AG_k)\varphi(G_l)$$

и

$$\varphi(AG_kAG_l) = \varphi(G_{l-k}) = g^{l-k} = ag^k \cdot ag^l = \varphi(AG_k)\varphi(AG_l)$$

показывают, что φ — изоморфизм.

Сведем вместе некоторые факты, касающиеся размерности неприводимых представлений.

Теорема 6. *Пусть G — конечная группа и k_n — число ее n-мерных неприводимых представлений. Тогда:*

(1) $|G| = k_1 + 2^2k_2 + 3^2k_3 + \ldots$, *причем* $k_1 \geqslant 1$ *и* $k_n = 0$, *если* n *не делит* $|G|$;

(2) *группа* G *коммутативна тогда и только тогда, когда* $k_i = 0$ *для всех* $i \geqslant 2$;

(3) *если* $|G| \leqslant 5$, *то группа* G *коммутативна*;

(4) $k_1 = |G/G'|$;

(5) *если* $|G| = p^2$, *где* p — *нечетное простое число, то группа* G *коммутативна.*

Доказательство. (1). Каждая группа допускает одномерное представление Ф, где $\Phi(g) = 1$ для всех $g \in G$. Следовательно, $k_1 \geqslant 1$. Если n не делит $|G|$, то $k_n = 0$ по теореме 19 из § 1. В силу теоремы 2 из § 1 размерность неприводимых представлений группы G совпадает с размерностью неприводимых правых модулей над групповой алгеброй $\boldsymbol{C}G$. По теореме III.2.16 эта алгебра вполне приводима справа. В силу теорем III.2.15 (2), (3), (4) каждому n-мерному неприводимому модулю над такой алгеброй соответствует прямое слагаемое, имеющее размерность n^2 согласно теореме III.2.13. Учитывая строение алгебры $\boldsymbol{C}G$ (теорема III.2.15) и следствие 2 теоремы III.1.9, можно записать

$$|G| = \dim \boldsymbol{C}G = k_1 + 2^2k_2 + 3^2k_3 + \ldots$$

(2) Ввиду (1) из теоремы 3 в § 1 вытекает, что коммутативность группы G равносильна равенству

$$k_1 + \ldots + k_n = |G| = k_1 + 4k_2 + \ldots + m^2k_m,$$

возможному лишь при $k_2 = \ldots = k_m = 0$.

(3) Если G некоммутативна, то, согласно (2), $k_i \neq 0$ для некоторого $i \geqslant 2$ и, следовательно, $|G| \geqslant 1 + i^2k_i \geqslant 5$ в силу (1).

(4) Ввиду (2) из теоремы II.7.9 (4) вытекает, что все неприводимые представления группы G/G' одномерны. Следовательно, если Ф — неприводимое представление группы G/G' и $\pi\colon G \to G/G'$ — естественный гомоморфизм, то $\pi\Phi$ — одномерное неприводимое представление группы G. Если же $\overline{\Phi}$ — одномерное неприводимое представление группы G, то для каждого $g \in G$ положим

$$\Phi(g\pi) = \overline{\Phi}(g).$$

Если $g\pi = g_1\pi$, то в силу теоремы II.7.9 (4)

$$gg_1^{-1} \in \operatorname{Ker} \pi = G' \subseteq \operatorname{Ker} \overline{\Phi},$$

откуда $\overline{\Phi}(g) = \overline{\Phi}(g_1)$. Таким образом, Ф определено корректно и оказывается представлением группы G/G'. Ра-

зумеется, $\pi\Phi = \overline{\Phi}$. Поскольку $\pi\Phi = \pi\Phi_1$ влечет за собой $\Phi = \Phi_1$ в силу теоремы II.1.4, нами установлено взаимно однозначное соответствие между всеми неприводимыми представлениями группы G/G' и всеми одномерными неприводимыми представлениями группы G. Остается заметить, что число неприводимых представлений группы G/G' равно $|G/G'|$ в силу теоремы 3 из § 1.

(5) Если $|G| = p^2$, где p — нечетное простое число, то ввиду теоремы 19 из § 1 равенство (1) превращается в $p^2 = k_1 + k_p p^2$, где $k_1 \geqslant 1$. Отсюда $k_p = 0$, и остается лишь применить свойство (2).

Теорема 7. *Если G — группа и $|G| = 2p$, где p — нечетное простое число, то G или коммутативна или изоморфна группе диэдра D_{2p}.*

Доказательство. Ввиду теоремы 6 (1)

$$2p = k_1 + 4k_2 + p^2 k_p,$$

откуда $k_p = 0$. В силу теорем 6 (4) и II.3.3′, $k_1 = 1$, 2 или p. Но равенства $2p = 1 + 4k_2$ и $2p = p + 4k_2$, очевидно, невозможны. Следовательно, $|G/G'| = 2$ и $|G'| = p$ по теореме II.3.3. Из теоремы II.3.3 нетрудно вывести, что G' — циклическая группа. Обозначим через g ее образующий. Кроме того, согласно теореме II.7.8, G содержит двуэлементную циклическую подгруппу K, скажем, с образующим a. Таким образом, $g^p = a^2 = 1$. Рассмотрим множество

$$H = \{1, g, \ldots, g^{p-1}, a, ag, \ldots, ag^{p-1}\}.$$

Если $g^i = ag^j$, то

$$1 \neq a = g^{i+p-j} \in G' \cap K = 1,$$

ибо $|G' \cap K| = 1$ в силу теоремы II.3.3. Следовательно, $|H| = 2p$. Отсюда $G = H$ и, в частности, G порождается элементами a и g. Ввиду теоремы II.7.9 (4)

$$aga = a^{-1}ga \in G',$$

т. е. $aga = g^s$, где $0 \leqslant s < p$. Отсюда

$$g = ag^s a = (aga)^s = g^{s^2}.$$

Следовательно, $g^{s^2-1} = 1$ и, как легко вывести из теоремы II.3.3, p делит $s^2 - 1 = (s-1)(s+1)$. Но это возможно лишь при $s = 1$ или $p - 1$. В первом случае имеем $aga = g$, откуда $ag = ga$, т. е. группа G оказывается коммутативной. Во втором случае получаем $aga =$

$= g^{p-1}$, откуда $agag = 1$, и остается лишь применить теорему 5.

Теорема 8. *Если G — некоммутативная группа и $|G| = 8$, то G изоморфна или группе кватернионов или группе диэдра D_4.*

Доказательство. Разумеется, группа G не циклическая. Если $x^2 = 1$ для всех $x \in G$, то для любых x, $y \in G$ получим $xyxy = 1$. Отсюда $xy = yx$, вопреки некоммутативности группы G. Поэтому, учитывая теорему II.3.3, получаем, что G содержит четырехэлементную циклическую группу H, скажем, с образующим g. Если $a \notin H$, то ввиду теоремы II.3.2

$$G = \{1, g, g^2, g^3, a, ag, ag^2, ag^3\}, \qquad (*)$$

откуда $a^2 = ag^s$ или g^s, где $0 \leqslant s \leqslant 3$. Однако первое предположение влечет $a = g^s$, что несовместимо с (*). Если $a^2 = g$ или g^3, то

$$G = \{1, a, a^2, a^3, a^4, a^5, a^6, a^7\},$$

что противоречит некоммутативности группы G. Следовательно, $a^2 = 1$ или g^2. В первом случае имеем $g^4 = a^2 = 1$ и $gag = g^s$ или ag^s, где $0 \leqslant s \leqslant 3$. Если $gag = g^s$, то $a = g^{s+6} = g^{s+2}$, вопреки (*). Следовательно,

$$gag = ag^s, \qquad (**)$$

откуда $aga = g^{s-1}$. Но тогда

$$g = ag^{s-1}a = (aga)^{s-1} = g^{(s-1)(s-1)} = g^{s^2-2s+1} = g^{s(s-2)+1},$$

т. е. $g^{s(s-2)} = 1$. Поэтому 4 делит $s(s-2)$ и, следовательно, $s = 0$ или 2. Если $s = 2$, то (**) превращается в $gag = ag^2$, откуда $ga = ag$, вопреки некоммутативности группы G. Если же $s = 0$, то (**) принимает вид $gag = a$. Отсюда $agag = 1$, и G изоморфна D_4 по теореме 5. Обратимся к случаю, когда $g^4 = 1$ и $a^2 = g^2$. Кроме того, имеем $ga = g^s$ или ag^s, где $0 \leqslant s \leqslant 3$. При первом предположении получим $a = g^{s+3}$, что противоречит (*). Следовательно, $ga = ag^s$. Если $s = 0$, то $1 \neq g = 1$. Если $s = 1$, то возникает противоречие с некоммутативностью группы G. Если $s = 2$, то $ga = ag^2 = a^3$, откуда $g^2 \neq g = a^2 = g^2$. Таким образом, $s = 3$, т. е. $ga = ag^3$. Отсюда $gag = a$, и G изоморфна группе кватернионов по теореме 4.

В приведенной ниже таблице через $\boldsymbol{Z}_m$ обозначена группа вычетов по модулю m, а через Q — группа ква-

тернионов. При ее составлении использованы теоремы 6—8 и II.7.6. Кроме того, используется тот факт, что группа, содержащая p элементов, где p — простое число, циклическая. Это может быть выведено из теоремы II.3.3.

Группы, содержащие не более 10 элементов

Число элементов	Коммутативные группы	Некоммутативные группы
2	Z_2	—
3	Z_3	—
4	Z_4, $Z_2 \oplus Z_2$	—
5	Z_5	—
6	Z_6	$D_3 \cong \mathfrak{S}_3$
7	Z_7	—
8	Z_8, $Z_4 \oplus Z_2$, $Z_2 \oplus Z_2 \oplus Z_2$	D_4, Q
9	Z_9, $Z_3 \oplus Z_3$	—
10	Z_{10}	D_5

Число групп, содержащих не более 20 элементов

Число элементов	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Число групп	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5	1	5
В том числе некоммутативных	0	0	0	0	1	0	2	0	1	0	3	0	1	0	9	0	3	0	3

Проверка правильности заполнения последней таблицы не составляет труда, если число элементов отлично от 12, 16, 18 и 20. На основании материала, имеющегося в настоящем пособии, можно исследовать случаи 12, 18 и 20 элементов. Случай же 16 элементов требует более мощных средств.

Упражнения

1. Найти центр и коммутант групп, рассмотренных в упражнениях 2 — 4 из § 1. Какие из них разрешимы?

2. Доказать, что для любого одномерного представления Φ группы G найдется такое одномерное представление Ψ группы G/G', что $\Phi(g) = \Psi(gG')$ для всех $g \in G$.

3. Доказать, что существует лишь одна (с точностью до изоморфизма) некоммутативная группа, состоящая из 10 элементов. Найти ее центр, коммутант, неприводимые представления и их характеры (ср. упражнение 5 из § 1).

4. Доказать, что некоммутативная простая группа содержит не менее 30 элементов.

5. Доказать, что некоммутативная простая группа имеет лишь одно одномерное представление. Указание: принять во внимание теорему II.7.9 (4) и упражнение 2.

УКАЗАТЕЛЬ РАСПОЛОЖЕНИЯ ТЕОРЕМ

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

УКАЗАТЕЛЬ ОБОЗНАЧЕНИЙ

Цена 45 коп.