Л. Я. Куликов

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Л. Я. Куликов

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Допущено Министерством просвещения СССР в качестве учебного пособия для студентов педагогических институтов по специальностям «Математика», «Математика и физика» и «Физика и математика»

Москва «Высшая школа» 1979

ББК 22.143
К90
УДК 512(075)

Рецензенты:
кафедра алгебры, теории чисел и методики математики Куйбышевского государственного педагогического института им. В. В. Куйбышева (зав. кафедрой — проф. Б. М. Бредихин) и докт. физ.-мат. наук, проф. М. М. Глухов

Куликов Л. Я.

К90 Алгебра и теория чисел: Учеб. пособие для педагогических институтов. — М.: Высш. школа, 1979. — 559 с., ил.

В пер.: 1 р. 10 к.

В книге систематически изложены элементы логики, множества и отношения, алгебры и алгебраические системы, основные числовые системы, основы линейной алгебры, включающие системы линейных неравенств, группы, теоретико-числовые темы, кольца и кольца полиномов, полиномы над основными числовыми полями и элементы теории полей.

Предназначается для студентов физико-математических факультетов педагогических институтов.

$\text{К}\frac{60602-348}{001(01)-79}$ 34—79 4306020400 517.1
ББК 22.143

ПРЕДИСЛОВИЕ

В последние годы в педагогических институтах введена новая программа единого курса алгебры и теории чисел. Главная цель этого курса — изучение основных алгебраических систем и воспитание алгебраической культуры, необходимой будущему учителю для глубокого понимания целей и задач как основного школьного курса математики, так и школьных факультативных курсов. Предлагаемое учебное пособие написано в соответствии с новыми программами.

Условно можно считать, что книга состоит из трех частей, тесно связанных между собой. К первой части относятся элементы логики, множества и отношения, начальные сведения об алгебрах и алгебраических системах и основные числовые системы. Элементы логики и теории множеств даются на содержательном уровне и в дальнейшем существенным образом используются как в курсе алгебры, так и в других математических дисциплинах. Начальные сведения об алгебрах и алгебраических системах, о группах и кольцах даны в третьей главе. На этой основе изучаются основные числовые системы: система натуральных чисел, кольцо целых чисел, поле рациональных чисел, система действительных чисел и поле комплексных чисел. Система действительных чисел вводится как полное архимедовски упорядоченное поле. Во второй части (главы 5—9) излагается линейная алгебра. Сначала рассматриваются арифметические векторные пространства и системы линейных уравнений вне связи с определителями. Лишь в шестой главе дано приложение определителей к решению систем линейных уравнений. Такой подход имеет преимущества перед традиционным, так как вычислительная сторона основных задач темы становится менее трудной, теория систем линейных уравнений органически включается в теорию арифметических векторных пространств. В девятой главе изложены

системы линейных неравенств и элементы линейного программирования (стандартные и канонические задачи, теорема двойственности и симплекс-метод).

Третья часть книги (главы 10 — 17) посвящена группам, теоретико-числовым темам, кольцам и кольцам полиномов. В последних двух главах изучаются кольца полиномов над основными числовыми полями и элементы теории полей.

Многие главы тесно связаны с новой школьной программой и могут служить основой для школьных факультативных курсов.

Все главы делятся на параграфы. В ссылках на параграф той же главы указывается номер параграфа, в ссылках же на параграф другой главы номер главы предшествует номеру параграфа. Теоремы, предложения и следствия нумеруются последовательно в пределах параграфа. При ссылке на теорему или предложение той же главы указывается номер параграфа и теоремы, а при ссылке на теорему или предложение другой главы указываются последовательно номера главы, параграфа и теоремы. Например, ссылка «теорема 4.2» обозначает теорему 2 четвертого параграфа той же главы, «теорема 4.2.6» — теорему 6 параграфа 2 главы 4.

Автор благодарит рецензентов, проф. Б. М. Бредихина и проф. М. М. Глухова, за ряд критических замечаний, способствующих улучшению рукописи книги.

Автор

Глава первая
ЭЛЕМЕНТЫ ЛОГИКИ

§ 1. ЛОГИКА ВЫСКАЗЫВАНИЙ

Высказывания. Понятие «высказывание» первично. Под высказыванием в логике понимают повествовательное предложение, о котором можно говорить, что оно истинно или ложно. Любое высказывание либо истинно, либо ложно, и никакое высказывание не является одновременно истинным и ложным.

Примеры высказываний: «$0 < 1$», «$2 \cdot 3 = 6$», «5 есть четное число», «1 есть простое число». Истинностное значение первых двух высказываний — «истина», истинностное значение последних двух — «ложь».

Вопросительные и восклицательные предложения не являются высказываниями. Определения не являются высказываниями. Например, определение «целое число называется четным, если оно делится на 2» не является высказыванием. Однако повествовательное предложение «если целое число делится на 2, то оно четное» есть высказывание, и притом истинное. В логике высказываний отвлекаются от смыслового содержания высказывания, ограничиваясь рассмотрением его с той позиции, что оно либо истинно, либо ложно.

В дальнейшем будем понимать под значением высказывания его истинностное значение («истина» или «ложь»). Высказывания будем обозначать прописными латинскими буквами, а их значения, т. е. «истина» или «ложь» — соответственно буквами И и Л.

Логика высказываний изучает связи, которые полностью определяются тем, каким образом одни высказывания строятся из других, называемых *элементарными*. Элементарные высказывания при этом рассматриваются как целые, не разложимые на части, внутренняя структура которых нас не будет интересовать.

Логические операции над высказываниями. Из элементарных высказываний с помощью логических опера-

ций можно получать новые, более сложные высказывания. Истинностное значение сложного высказывания зависит от истинностных значений высказываний, составляющих сложное высказывание. Эта зависимость устанавливается в данных ниже определениях и отражается в истинностных таблицах. В левых столбцах этих таблиц размещаются всевозможные распределения истинностных значений для высказываний, непосредственно составляющих рассматриваемое сложное высказывание. В правом столбце пишут истинностные значения сложного высказывания соответственно распределениям в каждой строке.

Пусть A и B — произвольные высказывания, относительно которых мы не предполагаем, что известны их истинностные значения. *Отрицанием высказывания* A называется новое высказывание, истинное тогда и только тогда, когда A ложно. Отрицание A обозначается через $\neg A$ и читается «не A» или «неверно, что A». Операция отрицания полностью определяется истинностной таблицей

A	$\neg A$
И	Л
Л	И

Пример. Высказывание «неверно, что 5 — четное число», имеющее значение И, есть отрицание ложного высказывания «5 — четное число».

С помощью операции *конъюнкции* из двух высказываний получается одно сложное высказывание, обозначаемое $A \wedge B$. По определению, высказывание $A \wedge B$ истинно тогда и только тогда, когда оба высказывания истинны. Высказывания A и B называются соответственно *первым* и *вторым членами конъюнкции* $A \wedge B$. Запись «$A \wedge B$» читается как «A и B». Истинностная таблица для конъюнкции имеет вид

A	B	$A \wedge B$
И	И	И
И	Л	Л
Л	И	Л
Л	Л	Л

Пример. Высказывание «7 — простое число и 6 — нечетное число» ложно, как конъюнкция двух высказываний, одно из которых ложно.

Дизъюнкцией двух высказываний A и B называется высказывание, обозначаемое $A \vee B$, истинное в том и только в том случае, когда хотя бы одно из высказываний

A и B истинно. Соответственно этому высказывание $A \vee B$ ложно в том и только том случае, когда и A и B оба ложны. Высказывания A и B называются соответственно *первым и вторым членами дизъюнкции* $A \vee B$. Читается запись $A \vee B$ как «A или B». Союз «или» в данном случае носит неразделительный смысл, поскольку высказывание $A \vee B$ истинно и при истинности обоих членов. Дизъюнкция имеет следующую истинностную таблицу:

A	B	$A \vee B$
И	И	И
И	Л	И
Л	И	И
Л	Л	Л

Пример. Высказывание «$3 < 8$ или $5 < 2$», являющееся дизъюнкцией двух высказываний, одно из которых истинно, имеет значение И.

Высказывание, обозначаемое $A \to B$, ложное в том и только в том случае, когда A истинно, а B ложно, называется *импликацией* с посылкой A и заключением B. Высказывание $A \to B$ читается как «если A, то B», или «A влечет B», или «из A следует B». Истинностная таблица для импликации такова:

A	B	$A \to B$
И	И	И
И	Л	Л
Л	И	И
Л	Л	И

Отметим, что между посылкой и заключением могут отсутствовать причинно-следственные связи, но это не может повлиять на истинность или ложность импликации. Например, высказывание «если 5 — простое число, то биссектриса равностороннего треугольника является медианой» будет истинным, хотя в обычном понимании второе не следует из первого. Истинным также будет высказывание «если $2+2=5$, то $6+3=9$», поскольку истинно его заключение. При данном определении, если заключение истинно, импликация будет истинной независимо от истинностного значения посылки. В том случае, когда ложна посылка, импликация будет истинна независимо от истинностного значения заключения. Эти обстоятельства кратко формулируют так: «истина следует из чего угодно», «из ложного следует все, что угодно».

Высказывание, обозначаемое через $A \leftrightarrow B$, истинное в том и только в том случае, когда A и B имеют одно и то же истинностное значение, называется *эквиваленцией*. Высказывание $A \leftrightarrow B$ читается как «A тогда и только тогда, когда B», или «A эквивалентно B», или «A необходимо и достаточно для B». Истинностная таблица для эквиваленции имеет вид

A	B	$A \leftrightarrow B$
И	И	И
И	Л	Л
Л	И	Л
Л	Л	И

Пример. Высказывание «$2 > 5$ тогда и только тогда, когда $3 + 0 = 4$» истинно, как эквиваленция двух ложных высказываний.

Формулы логики высказываний. Основной задачей логики высказываний является изучение логических форм сложных высказываний с помощью логических операций. Понятие логической формы сложного высказывания уточняется с помощью вводимого ниже понятия формулы логики высказываний.

Для обозначения высказываний будем использовать малые буквы конца латинского алфавита (возможно, с индексами). При этом, какое высказывание (истинное или ложное) будет обозначать та или иная буква, предполагаем неизвестным. Фактически буквы

(1) $p,\ q,\ r,\ \ldots,\ p_1,\ q_1,\ r_1,\ \ldots$

будут играть роль переменных, принимающих в качестве значений истинностные значения «истина» и «ложь». Обычно эти переменные называются *пропозициональными переменными*; будем также называть их *элементарными формулами* или *атомами*.

Для построения формул логики высказываний кроме символов (1) используются знаки логических операций

$$\neg,\ \wedge,\ \vee,\ \rightarrow,\ \leftrightarrow,$$

а также символы, обеспечивающие возможность однозначного прочтения формул, — левая и правая скобки: (,).

Понятие *формулы логики высказываний* определим следующим образом:

1) элементарные формулы (атомы) суть формулы логики высказываний;

2) если A и B — формулы, то $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$ тоже являются формулами логики высказываний;

3) только те выражения являются формулами логики высказываний, для которых это следует из 1) и 2).

Определение формулы содержит перечисление правил образования формул. Согласно определению, всякая формула логики высказываний либо есть атом, либо образуется из атомов в результате последовательного применения правила 2). Например, выражения

$$p, (\neg q), ((r \vee s) \to t), ((p \vee (\neg p)) \leftrightarrow (p \to q))$$

являются формулами логики высказываний.

Обозначать произвольные формулы логики высказываний будем большими буквами латинского алфавита (возможно, с индексами):

$$A, B, C, \ldots, A_1 B_1, C_1, \ldots$$

При этом не исключено, что одна и та же формула может быть обозначена различными буквами.

Заметим, что никакой атом не имеет вида $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$. Такой вид имеют сложные формулы.

В первой главе вместо «формула логики высказываний» часто будем говорить просто «формула» там, где это не может вызвать недоразумений.

Число скобок в формулах можно уменьшить, введя соглашения: 1) в сложной формуле будем опускать внешнюю пару скобок. 2) упорядочим знаки логических операций по «старшинству»: $\leftrightarrow$, $\to$, $\vee$, $\wedge$, $\neg$. В этом списке знак $\leftrightarrow$ имеет самую большую область действия, а знак $\neg$ — самую маленькую. Под областью действия знака операции понимаются те части формулы, к которым «применяется» (на которые «действует») рассматриваемое вхождение этого знака. Договоримся опускать во всякой формуле те пары скобок, которые можно восстановить, учитывая «порядок старшинства». При восстановлении скобок сначала расставляются все скобки, относящиеся ко всем вхождениям знака $\neg$ (при этом мы продвигаемся слева направо), затем ко всем вхождениям знака $\wedge$ и т. д.

Пример. В формуле $B \leftrightarrow \neg C \vee D \wedge A$ скобки восстанавливаются следующими шагами:

$$B \leftrightarrow (\neg C) \vee D \wedge A, \qquad B \leftrightarrow ((\neg C) \vee (D \wedge A)),$$
$$B \leftrightarrow (\neg C) \vee (D \wedge A), \qquad (B \leftrightarrow ((\neg C) \vee (D \wedge A))).$$

Не всякая формула может быть записана без скобок. Например, в формулах $A \to (B \to C)$, $\neg(A \to B)$ дальнейшее исключение скобок невозможно.

Законы логики. Существуют формулы, которые принимают значение И независимо от того, какие значения принимают входящие в них атомы. Например,

$$A \vee \neg A,\ A \to A,\ (A \to B) \vee (B \to A),\ A \to (B \to A).$$

Такие формулы играют особую роль в логике.

ОПРЕДЕЛЕНИЕ. Формула логики высказываний, которая принимает значение «истина» при любом распределении значений входящих в эту формулу атомов, называется *тождественно истинной формулой*, *тавтологией* или *законом логики*.

Существуют формулы, которые принимают значение «ложь» независимо от того, какие значения принимают входящие в них атомы. Например,

$$A \wedge \neg A,\ (A \vee \neg A) \to (A \wedge \neg A).$$

ОПРЕДЕЛЕНИЕ. Формула логики высказываний, принимающая значение «ложь» при любом распределении значений входящих в эту формулу атомов, называется *тождественно ложной формулой* или *противоречием*.

Легко убедиться, что если A — противоречие, то $\neg A$ будет тавтологией, и наоборот. Например, формула $p \wedge \neg p$ тождественно ложна, а $\neg(p \wedge \neg p)$ — тавтология.

Существуют формулы, которые принимают как значение И, так и значение Л в зависимости от того, какие значения принимают входящие в них атомы. Например,

$$A \vee A,\ A \to B,\ A \wedge B \to B \wedge C.$$

Запись $\models A$ означает, что формула A есть тавтология; например, $\models A \vee \neg A$. Этот закон носит название *закона исключенного третьего*.

ТЕОРЕМА 1.1. *Если A и $(A \to B)$ — тавтологии, то B — тавтология.*

Доказательство. Пусть A и $(A \to B)$ — тавтологии. Допустим, что для какого-либо распределения истинностных значений атомов, входящих в A и B, формула B принимает значение «ложь». Так как A — тавтология, то при том же распределении истинностных значений атомов формула A принимает значение И. Следовательно, формула $(A \to B)$ получит значение Л, что противоречит предположению о том, что $(A \to B)$ есть тавтология. Значит, фор-

мула B принимает значение И при любом распределении истинностных значений ее атомов. □ *)

ТЕОРЕМА 1.2. *Пусть A — формула, содержащая атомы $p_1, \ldots, p_n$, а B — формула, получающаяся из A одновременной подстановкой формул $A_1, \ldots, A_n$ вместо $p_1, \ldots, p_n$ соответственно. Если A — тавтология, то и B — тавтология.*

Доказательство. Пусть задано произвольное распределение истинностных значений атомов, входящих в B. Для этого распределения значений атомов формулы $A_1, \ldots, A_n$ примут соответственно истинностные значения $a_1, \ldots, a_n$. Если атомам $p_1, \ldots, p_n$ придать соответственно значения $a_1, \ldots, a_n$, то в результате истинностное значение формулы A совпадет со значением формулы B при заданном распределении значений атомов, входящих в B. Так как, по условию, A — тавтология, то B при заданном распределении значений атомов принимает значение «истина», т. е. B тоже тавтология. □

Эта теорема показывает, что любая подстановка в тавтологию приводит к тавтологии.

Ниже (в теореме 1.3) приведены часто встречающиеся законы логики.

ТЕОРЕМА 1.3. *Следующие формулы являются тавтологиями:*

Тавтологические импликации:

$p \wedge (p \to q) \to q$	— *закон заключения;*
$p \wedge q \to p$ $p \wedge q \to q$	— *законы удаления конъюнкции;*
$p \to p \vee q$ $q \to p \vee q$	— *законы введения дизъюнкции;*
$(p \vee q) \wedge \neg q \to p$	— *закон удаления дизъюнкции;*
$p \to \neg\neg p$	— *закон введения двойного отрицания*
$\neg\neg p \to p$	— *закон удаления двойного отрицания;*
$(p \to q) \wedge (q \to p) \to (p \leftrightarrow q)$	— *закон введения эквиваленции;*

*) □ — знак, означающий, что доказательство теоремы или предложения закончено.

$(p \leftrightarrow q) \rightarrow (p \rightarrow q)$
$(p \leftrightarrow q) \rightarrow (q \rightarrow p)$ — *законы удаления эквиваленции;*

$(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$ — *закон контрапозиции;*

$(\neg p \rightarrow q) \wedge (\neg p \rightarrow \neg q) \rightarrow p$ — *закон доказательства от противного;*

$(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$ — *закон силлогизма;*

$(p \rightarrow r) \wedge (q \rightarrow r) \rightarrow (p \vee q \rightarrow r)$ — *закон сложения посылок;*

$(p \rightarrow q) \wedge (p \rightarrow r) \rightarrow (p \rightarrow q \wedge r)$ — *закон умножения заключений;*

$(p \leftrightarrow q) \wedge (q \leftrightarrow r) \rightarrow (p \leftrightarrow r)$ — *закон транзитивности эквиваленции.*

Тавтологические эквиваленции:

$p \leftrightarrow p$ — *закон тождества;*

$p \wedge p \leftrightarrow p$ — *закон идемпотентности конъюнкции;*

$p \vee p \leftrightarrow p$ — *закон идемпотентности дизъюнкции;*

$p \wedge q \leftrightarrow q \wedge p$ — *закон коммутативности конъюнкции;*

$p \vee q \leftrightarrow q \vee p$ — *закон коммутативности дизъюнкции;*

$p \wedge (q \wedge r) \leftrightarrow (p \wedge q) \wedge r$ — *закон ассоциативности конъюнкции;*

$p \vee (q \vee r) \leftrightarrow (p \vee q) \vee r$ — *закон ассоциативности дизъюнкции;*

$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$ — *закон дистрибутивности конъюнкции относительно дизъюнкции;*

$p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$ — *закон дистрибутивности дизъюнкции относительно конъюнкции;*

$\neg \neg p \leftrightarrow p$ — *закон двойного отрицания;*

$(p \leftrightarrow q) \leftrightarrow (q \leftrightarrow p)$ — *закон коммутативности эквиваленции;*

$(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$ — *закон контрапозиции;*

$\neg (p \vee q) \leftrightarrow (\neg p \wedge \neg q)$ — *закон отрицания дизъюнкции;*

$\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$ — *закон отрицания конъюнкции;*

$(p \leftrightarrow q) \leftrightarrow (\neg p \leftrightarrow \neg q)$ — *закон противоположности;*

$p \rightarrow (q \rightarrow r) \leftrightarrow q \rightarrow (p \rightarrow r)$ — *закон перестановки посылок.*

Тавтологии, выражающие одни операции через другие:

$p \rightarrow q \leftrightarrow \neg p \vee q;$
$p \rightarrow q \leftrightarrow \neg(p \wedge \neg q);$
$p \vee q \leftrightarrow \neg p \rightarrow q;$
$p \vee q \leftrightarrow \neg(\neg p \wedge \neg q);$
$p \wedge q \leftrightarrow \neg(p \rightarrow \neg q);$
$p \wedge q \leftrightarrow \neg(\neg p \vee \neg q);$
$(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p).$

Чтобы доказать, что каждая из приведенных формул является тавтологией, надо применить метод истинностных таблиц, т. е. составить для каждой формулы истинностную таблицу и убедиться, что в каждой строке крайнего правого столбца стоит буква И.

Рассмотрим, к примеру, закон силлогизма:

p	q	r	$p \rightarrow q$	$q \rightarrow r$	$p \rightarrow r$	$(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$
И	И	И	И	И	И	И
И	И	Л	И	Л	Л	И
И	Л	И	Л	И	И	И
И	Л	Л	Л	И	Л	И
Л	И	И	И	И	И	И
Л	И	Л	И	Л	И	И
Л	Л	И	И	И	И	И
Л	Л	Л	И	И	И	И

Заметим, что на основании законов ассоциативности можно опускать скобки, посредством которых осуществляется группировка членов многочленных конъюнкций и дизъюнкций. Из закона двойного отрицания следует, что при желании всегда можно избежать двух подряд стоящих знаков «$\neg$» и более.

Упражнения

1. Составьте таблицу истинности для каждой из формул

(a) $p \to q \leftrightarrow \neg p \vee q$; (c) $r \to (r \to q)$;

(b) $p \to \neg (q \wedge r)$; (d) $(p \wedge q) \to (s \wedge \neg s \to p \vee s)$.

2. Что можно сказать об истинностном значении высказывания $\neg A \wedge B \leftrightarrow A \vee B$, если значение высказывания $A \to B$ есть Л?

3. Докажите, что формулы теоремы 1.3 являются тавтологиями.

4. Пусть C — формула, в которой выделено некоторое вхождение формулы A, а C' — формула, полученная из C заменой этого вхождения формулы A на формулу B. Докажите, что если $A \leftrightarrow B$ — тавтология, то $C \leftrightarrow C'$ — тоже тавтология.

5. Сколько строк имеет истинностная таблица для формулы логики высказываний, имеющей n различных атомов?

6. Пусть формула A построена из атомов $p_1, \ldots, p_n$ только с помощью знаков $\neg$, $\wedge$, $\vee$, а формула A^* получена из A заменой каждого вхождения символа $\wedge$ символом $\vee$ и наоборот и заменой каждого вхождения p_i вхождением $\neg p_i$ и наоборот. Докажите, что формула $\neg A \leftrightarrow A^*$ — тавтология.

7. Докажите, что следующие формулы являются тавтологиями:

(a) $(A \wedge B) \to C \leftrightarrow A \to (B \to C)$;

(b) $(A \wedge B) \to C \leftrightarrow (A \wedge \neg C) \to \neg B$;

(c) $\neg (A \to B) \leftrightarrow A \wedge \neg B$;

(d) $(A \to B) \wedge \neg B \to \neg A$;

(e) $A \to (\neg A \to B)$;

(f) $A \to (B \to A)$;

(g) $(\neg A \to A) \to A$;

(h) $(A \to B) \to (A \wedge C \to B \wedge C)$;

(i) $(A \to B) \wedge (C \to \mathrm{D}) \to (A \wedge C \to B \wedge \mathrm{D})$;

(k) $(A \to B) \wedge (C \to \mathrm{D}) \to (A \vee C \to B \vee \mathrm{D})$;

(l) $\neg (A \leftrightarrow B) \leftrightarrow (\neg (A \to B) \vee \neg (B \to A))$.

8. Докажите, что никакая формула логики высказываний, при построении которой используются только знаки логических операций $\wedge$, $\vee$, не является ни тавтологией, ни противоречием.

§ 2. ЛОГИЧЕСКОЕ СЛЕДСТВИЕ

Основные определения. Пусть $A_1, \ldots, A_m, B$ — формулы логики высказываний.

ОПРЕДЕЛЕНИЕ. Формула B называется *логическим следствием формул* $A_1, \ldots, A_m$, если при любом выборе истинностных значений атомов, входящих в формулы $A_1, \ldots, A_m, B$, формула B получает значение «истина» всякий раз, когда каждая из формул $A_1, \ldots, A_m$ получает значение «истина».

Запись

$$A_1, \ldots, A_m \models B$$

означает, что формула B — логическое следствие формул $A_1, \ldots, A_m$ (формулы $A_1, \ldots, A_m$ логически влекут формулу B).

Используя таблицы истинности, можно сказать, что формула B есть логическое следствие формул $A_1, \ldots, A_m$, если в таблицах, построенных по перечню атомов $p_1, \ldots, p_n$, входящих в $A_1, \ldots, A_m, B$, формула B имеет значение И во всех тех строках, в которых $A_1, \ldots, A_m$ одновременно имеют значение И. Другими словами, совокупность тех наборов значений атомов, для которых истинны все формулы $A_1, \ldots, A_m$, содержится в совокупности тех наборов значений атомов, для которых истинна формула B. Очевидно, порядок атомов $p_1, \ldots, p_n$, входящих в формулы $A_1, \ldots, A_m, B$, безразличен.

Пример. $A \to B,\ A \to \neg B \models \neg A$, что видно из таблицы:

A	B	$A \to B$	$A \to \neg B$	$\neg A$
И	И	И	Л	Л
И	Л	Л	И	Л
Л	И	И	И	И
Л	Л	И	И	И

Из определения логического следствия вытекает, что тавтология логически следует из любой формулы логики высказываний, а противоречие логически влечет любую формулу.

ОПРЕДЕЛЕНИЕ. Формулы A и B называются *равносильными* (*логически эквивалентными*), если при любом выборе истинностных значений атомов, входящих в A и B, формулы A и B принимают одинаковые истинностные значения.

Запись $A \equiv B$ означает, что формулы A и B равносильны.

Из определения логической эквивалентности формул следует, что любые две тавтологии логически эквивалентны, так же как и любые два противоречия.

Формула A *равносильна* B *тогда и только тогда, когда* $A \models B$ и $B \models A$.

ТЕОРЕМА 2.1. *Формулы* A *и* B *равносильны тогда и только тогда, когда формула* $A \leftrightarrow B$ *является тавтологией.*

Доказательство теоремы предлагается читателю в качестве упражнения.

ТЕОРЕМА 2.2. (а) $A \models B$ *тогда и только тогда, когда* $\models A \to B$; (b) $A_1, \ldots, A_m \models B$ *тогда и только тогда, когда* $\models A_1 \wedge \ldots \wedge A_m \to B$.

Доказательство. (а) Пусть $A \models B$. Импликация $A \to B$ имеет истинностное значение Л, когда A получает значение И и одновременно B получает значение Л. Однако в силу условия $A \models B$ такого распределения истинностных значений атомов, входящих в A и B, не существует. Следовательно, формула $A \to B$ всегда получает значение И, т. е. $\models A \to B$.

Предположим теперь, что $\models A \to B$. Рассмотрим произвольное распределение истинностных значений атомов, входящих в A и B, при котором A имеет значение И. Так как $A \to B$ по предположению получает значение И при этом распределении, то и B получает значение И при этом распределении. Таким образом, $A \models B$.

(b) Из определения конъюнкции следует, что $A_1, \ldots, A_m \models B$ тогда и только тогда, когда $A_1 \wedge \ldots \wedge A_m \models B$. Кроме того, в силу (а)

$$A_1 \wedge \ldots \wedge A_m \models B \text{ тогда и только тогда, когда } \models A_1 \wedge \ldots \wedge A_m \to B.$$

Следовательно, $A_1, \ldots, A_m \models B$ тогда и только тогда, когда $\models A_1 \wedge \ldots \wedge A_m \to B$. □

Пример. $(A \to B), (B \to C) \models (A \to C)$, так как формула $(A \to B) \wedge (B \to C) \to (A \to C)$ является тавтологией.

ТЕОРЕМА 2.3. $A_1, \ldots, A_m, B \models C$ *тогда и только тогда, когда* $A_1, \ldots, A_m \models B \to C$.

Доказательство. Предположим, что $A_1, \ldots, A_m, B \models C$, и докажем, что тогда $A_1, \ldots, A_m \models B \to C$. Допустим, что существует такое распределение истинностных значений атомов, входящих в формулы $A_1, \ldots, A_m, B, C$, при котором формулы $A_1, \ldots, A_m$ принимают значение И, а формула $B \to C$ принимает значение Л. Для этого же распределения значений атомов формулы $A_1, \ldots, A_m, B$ приняли бы одновременно значение И, а формула C — значение Л. Следовательно, такого распределения истинностных значений атомов не существует. Таким образом, если $A_1, \ldots, A_m, B \models C$, то $A_1, \ldots, A_m \models B \to C$.

Предположим теперь, что $A_1, \ldots, A_m \models B \to C$, и докажем, что $A_1, \ldots, A_m, B \models C$. Допустим, что существует такое распределение истинностных значений атомов, входящих в формулы $A_1, \ldots, A_m, B, C$, при котором фор-

мулы $A_1, \ldots, A_m, B$ принимают значение И, а формулы C — значение Л. При этом же распределении истинностных значений атомов формулы $A_1, \ldots, A_m$ приняли бы значение И, а формула $B \to C$ — значение Л, что противоречило бы предположению. Следовательно, такого распределения истинностных значений атомов не существует. Таким образом, если $A_1, \ldots, A_m \models B \to C$, то $A_1, \ldots, A_m, B \models C$. □

СЛЕДСТВИЕ 2.4. *$A, B \models C$ тогда и только тогда, когда $\models A \to (B \to C)$. В более общем виде: $A_1, A_2, \ldots, A_m \models B$ тогда и только тогда, когда $\models A_1 \to (A_2 \to \to (\ldots (A_m \to B) \ldots))$.*

Для доказательства достаточно несколько раз применить теорему 2.3.

Из теоремы 2.3 следует, что тавтологическим эквиваленциям, приведенным в теореме 1.3, отвечают следующие равносильности (логические эквивалентности):

$A \equiv A;$
$A \wedge A \equiv A;$
$A \vee A \equiv A;$
$A \wedge B \equiv B \wedge A;$
$A \vee B \equiv B \vee A;$
$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C;$
$A \vee (B \vee C) \equiv (A \vee B) \vee C;$
$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C);$
$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C);$
$\neg\neg A \equiv A;$
$(A \leftrightarrow B) \equiv (B \leftrightarrow A);$
$(A \to B) \equiv (\neg B \to \neg A);$
$\neg (A \vee B) \equiv \neg A \wedge \neg B;$
$\neg (A \wedge B) \equiv \neg A \vee \neg B;$
$(A \leftrightarrow B) \equiv (\neg A \leftrightarrow \neg B);$
$A \to (B \to C) \equiv B \to (A \to C);$
$A \to B \equiv \neg A \vee B;$
$A \to B \equiv \neg (A \wedge \neg B);$
$A \vee B \equiv \neg A \to B;$
$A \vee B \equiv \neg (\neg A \wedge \neg B);$
$A \wedge B \equiv \neg (A \to \neg B);$
$A \wedge B \equiv \neg (\neg A \vee \neg B);$
$(A \leftrightarrow B) \equiv (A \to B) \wedge (B \to A).$

Схемы доказательств. Доказательства тех или иных утверждений в математике строятся на основании определенных правил, сущность которых выражают тавтологические импликации логики высказываний. Они схематично отражают шаги построения доказательств, поэтому их называют *схемами* или *правилами доказательств* (см., например, ниже правило заключения, правило контрапозиции и т. д.). Приведем правила, которые соответствуют первым 15 тавтологическим импликациям теоремы 1.3:

$A,\ A \to B \models B$ — правило заключения;

$A,\ B \models A \wedge B$ — правило введения конъюнкции;

$A \wedge B \models A$, $A \wedge B \models B$ — правила удаления конъюнкции;

$A \models A \vee B$, $B \models A \vee B$ — правила введения дизъюнкции;

$A \vee B,\ \neg B \models A$ — правило удаления дизъюнкции;

$A \models \neg\neg A$ — правило введения двойного отрицания;

$\neg\neg A \models A$ — правило удаления двойного отрицания;

$A \to B,\ B \to A \models A \leftrightarrow B$ — правило введения эквиваленции;

$A \leftrightarrow B \models A \to B$, $A \leftrightarrow B \models B \to A$ — правила удаления эквиваленций;

$A \to B \models \neg B \to \neg A$ — правило контрапозиции;

$\neg A \to B,\ \neg A \to \neg B \models A$ — правило доказательства от противного;

$A \to B,\ B \to C \models A \to C$ — правило силлогизма;

$A \to C,\ B \to C \models A \vee B \to C$ — доказательство разбором случаев.

Часто при записи этих правил помещают посылки над горизонтальной линией, а заключение — под ней. При такой

записи приведенные выше схемы доказательств принимают вид:

$$\frac{A \to B \quad A}{B}$$ — правило отделения;

$$\frac{A \quad B}{A \wedge B}$$ — правило введения конъюнкции;

$$\frac{A \wedge B}{A}; \quad \frac{A \wedge B}{B}$$ — правила удаления конъюнкции;

$$\frac{A}{A \vee B}; \quad \frac{B}{A \vee B}$$ — правила введения дизъюнкции;

$$\frac{A \vee B \quad \neg B}{A}$$ — правило удаления дизъюнкции;

$$\frac{A}{\neg\neg A}$$ — правило введения двойного отрицания;

$$\frac{\neg\neg A}{A}$$ — правило удаления двойного отрицания;

$$\frac{A \to B \quad B \to A}{A \leftrightarrow B}$$ — правило введения эквиваленции;

$$\frac{A \leftrightarrow B}{A \to B}; \quad \frac{A \leftrightarrow B}{B \to A}$$ — правила удаления эквиваленции;

$$\frac{A \to B}{\neg B \to \neg A}$$ — правило контрапозиции;

$$\frac{\neg A \to B \quad \neg A \to \neg B}{A}$$ — правило доказательства от противного;

$$\frac{A \to B \quad B \to C}{A \to C}$$ — правило силлогизма;

$$\frac{A \to C \quad B \to C}{A \vee B \to C}$$ — доказательство разбором случаев.

Косвенное доказательство (доказательство от противного). Совокупность формул $A_1, \ldots, A_m$ логики высказываний называется *противоречивой*, если при любом распределении истинностных значений входящих в них атомов хотя бы одна из формул $A_1, \ldots, A_m$ получает значение Л. Легко видеть, что совокупность формул $A_1, \ldots, A_m$ про-

тиворечива тогда и только тогда, когда формула $A_1 \wedge \ldots \wedge A_m$ есть противоречие, т. е. является тождественно ложной формулой.

ТЕОРЕМА 2.5. *Если из совокупности формул* $A_1, \ldots, A_m$ *логически следует противоречие, то эта совокупность формул противоречива.*

Доказательство. Предположим, что $A_1, \ldots, A_m \models F$, где F — тождественно ложная формула. Тогда по теореме 2.3

$$\models A_1 \wedge \ldots \wedge A_m \to F.$$

В силу таблицы истинности для импликации отсюда следует, что формула $A_1 \wedge \ldots \wedge A_m$ тождественно ложна. Следовательно, совокупность формул $A_1, \ldots, A_m$ противоречива. □

Тождественно ложные формулы (противоречия) играют существенную роль в методе косвенного доказательства, называемого также *методом доказательства от противного*. Основой такого рода доказательств является следующая теорема.

ТЕОРЕМА 2.6. *Если из формул* $A_1, \ldots, A_m, \neg B$ *логически следует противоречие, то* $A_1, \ldots, A_m \models B$.

Доказательство. Предположим, что $A_1, \ldots, A_m, \neg B \models F$, где F — противоречие. Тогда по теореме 2.5 совокупность формул $A_1, \ldots, A_m, \neg B$ противоречива. Поэтому если для какого-либо распределения истинностных значений атомов, входящих в формулы $A_1, \ldots, A_m, \neg B$, все формулы $A_1, \ldots, A_m$ получают значение И, то формула $\neg B$ получает значение Л, а значит, B получает значение И. Следовательно, $A_1, \ldots, A_m \models B$. □

Таким образом, если нужно доказать, что некоторое высказывание B логически следует из данных посылок, мы присоединяем к этим посылкам $\neg B$ и показываем, что из посылок следует противоречие (обычно оно имеет вид $C \wedge \neg C$). После этого можно заключить, что высказывание B есть логическое следствие исходных посылок. Частным является случай, когда $m = 0$, т. е. не задаются никакие посылки. Если, допустив истинность $\neg B$, выведем противоречие $(C \wedge \neg C)$, то можем утверждать истинность B. Это рассуждение основывается на правиле доказательства от противного: $\neg B \to C, \neg B \to \neg C \models B$.

Очень распространенным является способ доказательства разбором случаев, который заключается в следующем. Пусть требуется доказать истинность высказывания C.

Строим высказывания A и B такие, что $A \vee B$, $A \to C$, $B \to C$ — истинные высказывания (часто в качестве B берут отрицание A). Тогда на основании соответствующей схемы доказательства можно утверждать истинность C.

На основании правила силлогизма можно утверждать истинность высказывания $A \to B$, если можно построить такую цепочку импликаций

$$A \to A_1,\ A_1 \to A_2, \ldots,\ A_{n-1} \to A_n,\ A_n \to B,$$

каждая из которых истинна.

Упражнения

1. Обоснуйте следующие схемы доказательств:

(a) $\dfrac{A \to \neg B}{B \to \neg A}$;

(b) $\dfrac{A,\ A \leftrightarrow B}{B}$;

(c) $\dfrac{A \to B}{(B \to C) \to (A \to C)}$;

(d) $\dfrac{A \leftrightarrow B,\ B \leftrightarrow C}{A \leftrightarrow C}$;

(e) $\dfrac{A \leftrightarrow B,\ C \leftrightarrow D}{A \vee C \leftrightarrow B \vee C}$;

(f) $\dfrac{A \leftrightarrow B,\ C \leftrightarrow D}{A \wedge C \leftrightarrow B \wedge D}$;

(g) $\dfrac{A \to B,\ C \to D}{A \vee C,\ B \vee D}$;

(h) $\dfrac{A \to B,\ C \to D}{A \wedge C \to B \wedge D}$;

(i) $\dfrac{A \to B,\ A \to C}{A \to B \wedge C}$;

(j) $\dfrac{A \to (B \to C)}{(A \to B) \to (A \to C)}$;

(k) $\dfrac{A \to C}{A \wedge B \to C}$;

(l) $\dfrac{A \to (B \to C)}{A \wedge B \to C}$;

(m) $\dfrac{\neg A}{A \to B}$;

(n) $\dfrac{A \to B,\ \neg B}{\neg A}$;

(o) $\dfrac{(A \wedge \neg B) \to (C \wedge \neg C)}{A \to B}$;

(p) $\dfrac{A \to (B \to C)}{B \to (A \to C)}$;

(q) $\dfrac{A \to (B \to C)}{A \to (\neg C \to \neg B)}$.

2. Докажите, что для любой формулы логики высказываний существует логически эквивалентная формула, построенная только с помощью одной из следующих пар связок:

(a) $\neg$, $\to$; (b) $\neg$, $\vee$; (c) $\neg$, $\wedge$.

3. Докажите, что

(a) $\neg A \vee B,\ C \to \neg B \models A \to \neg C$;

(b) $A \vee B,\ A \to C,\ B \to D \models C \vee D$;

(c) $A \to (B \to C),\ \neg D \vee A,\ B \models D \to C$;

(d) $A \vee B \to C \vee D,\ D \vee E \to F \models A \to F$.

§ 3. ПРЕДИКАТЫ

Средства, предоставляемые логикой высказываний, оказываются недостаточными для анализа многих математических рассуждений. Например, средствами логики высказываний нельзя установить правильность такого рассуждения: «Всякое целое число является рациональным числом; 25 — целое число, следовательно, 25 — рациональное число». Это объясняется тем, что в логике высказываний простые высказывания, из которых с помощью логических операций строятся сложные, рассматриваются как нерасчленяемые. Они не подвергаются анализу структуры в смысле связей объектов и их свойств. Поэтому возникает необходимость в построении такой логической системы, средствами которой можно исследовать строение тех высказываний, которые в логике высказываний рассматриваются как элементарные. Такой логической системой является логика предикатов, содержащая как часть логику высказываний.

Свободные переменные. В математике широко используются буквенные обозначения. Некоторые буквы, выделяемые в тексте, обозначают произвольные объекты определенного вида. Обычно каждая такая буква сохраняет свою индивидуальность, т. е. обозначает один и тот же объект на всем протяжении некоторого текста. Различные буквы могут обозначать как один и тот же объект, так и различные объекты. Используемые таким образом буквы называются *свободными переменными*.

Допустимыми значениями свободной переменной называются те объекты определенного вида, для обозначения которых употребляется эта переменная. Так, допустимыми значениями свободной переменной могут быть высказывания. Такая свободная переменная называется *пропозициональной*.

Допустимыми значениями свободной переменной могут быть натуральные, или целые, числа. Такая свободная переменная называется соответственно *натуральной* или *целочисленной*.

Если допустимыми значениями свободной переменной являются действительные или комплексные числа, то такая переменная называется соответственно *действительной* или *комплексной*.

Предикаты. Рассмотрим предложение

(1) $x+y=3$,

содержащее натуральные переменные x и y. Это предло-

жение не является высказыванием, так как о нем нельзя сказать, истинно оно или ложно. Оно называется *предикатом* или *условием* (на x и y). Приведем другие примеры предложений с переменными:

(2) x есть простое число;

(3) x есть четное число;

(4) x меньше y;

(5) x есть общий делитель y, z.

Будем считать, что допустимыми значениями переменных x, y и z являются натуральные числа. Если в предложениях (1)—(5) заменить переменные их допустимыми значениями, то получатся высказывания, которые могут быть как истинными, так и ложными. Например,

$0+1=3$;

2 есть простое число;

3 есть четное число;

5 меньше 7;

3 есть общий делитель 6 и 12.

ОПРЕДЕЛЕНИЕ. Предложения с переменными, дающие высказывания в результате замены свободных переменных их допустимыми значениями, называются *предикатами*.

Предложения (1)—(5) могут служить примерами предикатов.

По числу входящих свободных переменных различают предикаты *одноместные*, *двухместные*, *трехместные* и т. д. Предикаты (2) и (3) — одноместные, предикаты (1) и (4) — двухместные, предикат (5) — трехместный. Высказывания будем считать нульместными предикатами.

Заменяя в одноместном предикате (2) переменную натуральными числами, будем получать высказывания:

0 есть простое число;

1 есть простое число;

2 есть простое число;

3 есть простое число и т. д.

Некоторые из них являются истинными. Таким образом, данный одноместный предикат выделяет среди натуральных чисел те, при подстановке которых вместо переменной получается истинное высказывание, и его можно рассматривать как условие на значения свободной переменной, входящей в предикат. В данном случае числа, удовлетворяющие этому условию, — простые.

Одноместный предикат можно рассматривать как условие на объекты данного вида; двухместный — как условие на пары объектов данного вида и т. д.

Предикаты можно задавать различными способами. В алгебре часто рассматривают предикаты, заданные с помощью уравнений, неравенств, а также систем уравнений или неравенств. Например, неравенство $x+x^{-1}>0$ задает одноместный предикат, уравнение $x^2+y=0$ — двухместный, а система уравнений $x+y=0$, $x-y+z=0$ — трехместный (x, y, z — рациональные переменные).

Обозначать предикаты будем большими буквами латинского алфавита (возможно, с нижними индексами) с указанием в скобках всех свободных переменных, входящих в этот предикат. Например, $A(x, y)$ — обозначение двухместного предиката, $R(x, y, z)$ — трехместного и $Q(x_1, \ldots, x_n)$ — обозначение n-местного предиката.

В дальнейшем мы будем говорить об истинностном значении произвольного предиката на том или ином наборе входящих в него свободных переменных, понимая под этим истинностное значение высказывания, которое получается в результате замены свободных переменных соответствующими им значениями из рассматриваемого набора.

Высказывание, которое получается при подстановке в предикат $R(x_1, \ldots, x_n)$ набора допустимых значений $(a_1, \ldots, a_n)$ вместо его переменных, будем обозначать $R(a_1, \ldots, a_n)$. Если это высказывание истинное (ложное), говорят, что набор значений $(a_1, \ldots, a_n)$ удовлетворяет (не удовлетворяет) предикату $R(x_1, \ldots, x_n)$.

Отметим, что следует различать предикаты, выражающие одно и то же условие, но имеющие переменные с различными допустимыми значениями. Например, предикат, заданный уравнением $2x-3=0$, где x — целочисленная переменная, следует отличать от предиката, заданного тем же уравнением, если при этом x рассматривается как рациональная переменная. Первый предикат не принимает значений И ни при каких допустимых значениях x, а второй принимает значение И при допустимом значении переменной $x=3/2$. Таким образом, при задании предиката нужно указывать область допустимых значений переменных этого предиката.

Операции над предикатами. Предикаты, как и высказывания, принимают значения И и Л, поэтому над ними можно производить логические операции, аналогичные операциям логики высказываний.

Начнем с простого частного случая — одноместных предикатов, у которых области допустимых значений переменных совпадают. Образуем из двух предикатов $P(x)$ и $Q(y)$ новый предикат $P(x) \wedge Q(y)$. Это предикат от двух свободных переменных x и y, и истинностное значение его на любом наборе (a, b) допустимых значений переменных определяется как истинностное значение высказывания $P(a) \wedge P(b)$. Аналогично определяются предикаты

$$P(x) \vee Q(y), \quad \neg P(x), \quad P(x) \to Q(y), \quad P(x) \leftrightarrow Q(y).$$

Следует различать предикаты: двухместный $P(x) \wedge Q(y)$ и одноместный $P(x) \wedge Q(x)$; в первый допустимые значения подставляют вместо свободных переменных x и y независимо друг от друга, а во второй — вместо единственной свободной переменной x.

Над многоместными предикатами аналогично определяются операции: конъюнкция, дизъюнкция, отрицание, импликация и эквиваленция. Рассмотрим, например, случай двухместных предикатов. Пусть $P(x, y)$, $Q(y, z)$ — два предиката, у которых совпадают области допустимых значений переменных. Тогда $P(x, y) \wedge Q(y, z)$ есть трехместный предикат от x, y, z, истинностное значение которого на любом наборе (a, b, c) допустимых значений свободных переменных определяется как значение высказывания $P(a, b) \wedge Q(b, c)$. Заметим, что при рассмотрении операций над предикатами нужно следить, какие переменные обозначены различными буквами, а какие — одинаковыми.

Рассмотрим еще несколько примеров:

1) $A(x) \vee B(x, y)$ — предикат от свободных переменных x и y;
2) $\neg A(y) \wedge D(z, x)$ — предикат от свободных переменных x, y, z;
3) $E(x, y, z) \to F(z)$ — предикат от свободных переменных x, y, z.

Предикат $A(x) \vee B(x, y)$ принимает значение И на наборе значений (a, b), если хотя бы одно из высказываний $A(a)$ и $B(a, b)$ будет истинно, и принимает значение Л, если оба эти высказывания ложны. Аналогично можно установить истинностные значения остальных предикатов на том или ином наборе значений свободных переменных.

Логическое следствие. Равносильные предикаты.

ОПРЕДЕЛЕНИЕ. Предикат $A(x_1, \ldots, x_n)$ называется *тождественно истинным*, если для любого набора допу-

стимых значений входящих в него свободных переменных его истинностным значением является И.

Примером тождественно истинного предиката может служить трехместный предикат, заданный неравенством $(x+y)^2+z^2 \geqslant 0$, где x, y, z — рациональные переменные.

Пусть $A(x_1, \ldots, x_m)$ и $B(y_1, \ldots, y_n)$ — предикаты, имеющие одинаковые области допустимых значений свободных переменных.

ОПРЕДЕЛЕНИЕ. Предикат $B(y_1, \ldots, y_n)$ называется *логическим следствием предиката* $A(x_1, \ldots, x_m)$, если предикат $A(x_1, \ldots, x_m) \to B(y_1, \ldots, y_n)$ является тождественно истинным.

Запись $A(x_1, \ldots, x_m) \models B(y_1, \ldots, y_n)$ означает, что предикат $B(y_1, \ldots, y_n)$ есть логическое следствие предиката $A(x_1, \ldots, x_m)$.

Например, если x — целочисленная переменная, $R(x)$ — обозначение предиката «x — четное число», $P(x)$ — обозначение предиката «x кратно 4», то $R(x)$ логически следует из $P(x)$, т. е. $P(x) \models R(x)$. Здесь предикат $P(x)$ не следует логически из предиката $R(x)$.

Рассмотрим два n-местных предиката $A(x_1, \ldots, x_n)$ и $B(x_1, \ldots, x_n)$ от одних и тех же свободных переменных. Предикат $B(x_1, \ldots, x_n)$ будет логическим следствием предиката $A(x_1, \ldots, x_n)$ тогда и только тогда, когда любой набор значений переменных $x_1, \ldots, x_n$, удовлетворяющий предикату $A(x_1, \ldots, x_n)$, удовлетворяет также предикату $B(x_1, \ldots, x_n)$.

Доказательство этого утверждения предоставляется читателю.

ОПРЕДЕЛЕНИЕ. Предикат $B(z_1, \ldots, z_n)$ называется *логическим следствием* предикатов $A_1(x_1, \ldots, x_m), \ldots, A_k(y_1, \ldots, y_l)$, если предикат

$$A(x_1, \ldots, x_m) \wedge \ldots \wedge A_k(y_1, \ldots, y_l) \to B(z_1, \ldots, z_n)$$

является тождественно истинным. (При этом предполагается, что все свободные переменные рассматриваемых предикатов имеют одни и те же допустимые значения.)

Пример. Пусть $P(x)$ — предикат «x — четное число», $Q(x)$ — предикат «x кратно трем», $R(x)$ — предикат «x кратно шести». Тогда $P(x), Q(x) \models R(x)$.

ОПРЕДЕЛЕНИЕ. Предикаты $A(x_1, \ldots, x_m)$ и $B(y_1, \ldots, y_n)$ называются *равносильными* (*логически эквивалентными*), если предикат $A(x_1, \ldots, x_m) \leftrightarrow B(y_1, \ldots, y_n)$ является тождественно истинным. Запись $A(x_1, \ldots, x_m) \equiv$

$\equiv B(y_1, \ldots, y_n)$ означает, что предикаты $A(x_1, \ldots, x_m)$ и $B(y_1, \ldots, y_n)$ равносильны.

Легко видеть, что предикаты $A(x_1, \ldots, x_m)$ и $B(y_1, \ldots, y_n)$ равносильны тогда и только тогда, когда

$$A(x_1, \ldots, x_m) \models B(y_1, \ldots, y_n) \text{ и } B(y_1, \ldots, y_n) \models A(x_1, \ldots, x_m).$$

Нетрудно доказать, что предикаты $A(x_1, \ldots, x_m)$ и $B(x_1, \ldots, x_n)$ равносильны тогда и только тогда, когда их истинностные значения совпадают на любом наборе допустимых значений переменных $x_1, \ldots, x_n$. Примером равносильных предикатов могут служить предикаты, заданные уравнениями $x^3 - y^3 = 0$ и $2(x-y)(x^2+xy+y^2) = 0$, где x, y — рациональные переменные.

ОПРЕДЕЛЕНИЕ. Предикат $A(x_1, \ldots, x_n)$ называется *тождественно ложным*, если его истинностным значением является Л для любого набора допустимых значений входящих в него свободных переменных.

Например, тождественно ложным является предикат $x+1=x$, где x — целочисленная переменная.

ОПРЕДЕЛЕНИЕ. Предикат $A(x_1, \ldots, x_n)$ называется *выполнимым*, если существует хотя бы один набор допустимых значений входящих в него свободных переменных, на котором его истинностным значением является И.

Например, выполнимыми являются предикаты «x — простое число», «x делится на y», «$x^2 - 5x + 6 = 0$», где x — целочисленная переменная.

Из данных определений вытекает, что тождественно истинный предикат логически следует из любого предиката, а из тождественно ложного предиката логически следует любой предикат.

Любой предикат либо тождественно истинен, либо выполним, либо тождественно ложен.

Упражнения

1. Приведите пример таких предикатов $P(x, y, z)$ и $R(x, y, z)$ где x, y, z — натуральные переменные, чтобы один из них был логическим следствием другого.

2. Приведите примеры одно-, двух- и трехместных тождественно ложных, тождественно истинных и выполнимых (но не тождественно истинных) предикатов.

3. Постройте предикаты $A(x)$ и $B(x)$, где x — целочисленная переменная, такие, что:

(а) предикаты $A(x)$ и $B(x)$ — нетождественно истинны, а $A(x) \vee B(x)$ — тождественно истинный предикат;

(б) $A(x)$ и $B(x)$ — выполнимые предикаты, а $A(x) \wedge B(x)$ — невыполнимый предикат.

Рассмотрим новые операции, которые применяются к предикатам или высказываниям и дают в результате их применения предикаты или высказывания. Эти операции выражают утверждения общности или существования.

Квантор общности. Пусть $A(x)$ — предикат от одной свободной переменной x. Под выражением $\forall x A(x)$ будем подразумевать высказывание, истинное, если $A(x)$ принимает значение И для всех допустимых значений переменной x, т. е. если предикат $A(x)$ тождественно истинен, и ложное в противном случае. Высказывание $\forall x A(x)$ уже не зависит от x. Символ $\forall x$, приписываемый слева к предикату $A(x)$, называется *квантором общности* по переменной x. Если же A есть высказывание, то $\forall x A$ есть высказывание, истинное тогда и только тогда, когда A истинно.

Рассмотрим теперь предикат от нескольких свободных переменных, например предикат $A(x, y, z)$ от трех переменных. Этот предикат при произвольной замене всех свободных переменных, кроме x, их значениями b и c представляет собой предикат, зависящий только от свободной переменной x, а выражение

$$\forall x A(x, b, c)$$

есть высказывание. Предикат $\forall x A(x, y, z)$ становится высказыванием в результате задания значений всех входящих в него свободных переменных, кроме x, значит, от x не зависит. Таким образом, $\forall x A(x, y, z)$ зависит от всех свободных переменных, входящих в $A(x, y, z)$, кроме x, т. е. это двухместный предикат от y и z. Этот предикат на данном наборе значений свободных переменных b, c принимает значение И тогда и только тогда, когда предикат $A(x, b, c)$, зависящий только от одной свободной переменной x, является тождественно истинным. Символ $\forall x$ можно читать так: «для всякого x» или «для всех x», а запись $\forall x A(x, y, z)$ читается так: «для всякого x имеет место $A(x, y, z)$» или, короче, «для каждого x $A(x, y, z)$».

Переменная x, от которой предикат $\forall x A(x, y, z)$ не зависит, называется *связанной переменной* (в отличие от переменных y, z, которые являются свободными).

Квантор существования. Для квантора существования употребляется символ $\exists x$, приписываемый слева к предикату или высказыванию. Пусть $A(x)$ — предикат от одной свободной переменной x. Под выражением $\exists x A(x)$ будем

подразумевать высказывание, истинное, если $A(x)$ принимает значение И хотя бы для одного из допустимых значений переменной x, т. е. предикат $A(x)$ является выполнимым, и ложное в противном случае. Если же A — высказывание, то $\exists xA$ есть высказывание, истинное тогда и только тогда, когда A истинно.

Пусть теперь $A(x, y, z)$ есть трехместный предикат. Если в этом предикате заменить все свободные переменные, кроме x, их значениями, например значениями b, c, то получится предикат $A(x, b, c)$, зависящий только от одной свободной переменной x, а выражение

$$\exists xA(x, b, c)$$

будет высказыванием. Значит, выражение $\exists xA(x, y, z)$ есть предикат, становящийся высказыванием в результате задания значений всех свободных переменных, кроме x, и, значит, от x не зависит. Таким образом, выражение $\exists xA(x, y, z)$ есть предикат, зависящий только от y и z, значит, применение квантора к трехместному предикату привело к двухместному предикату. Переменная x, от которой предикат $\exists xA(x, y, z)$ не зависит, называется *связанной переменной*.

Предикат $\exists xA(x, y, z)$ принимает значение И на данном наборе b, c допустимых значений тогда и только тогда, когда одноместный предикат $A(x, b, c)$ выполним.

Символ $\exists x$ называется *квантором существования* по переменной x и читается так: «существует x такое, что». Выражение $\exists xA(x, y, z)$ читается так: «хотя бы при одном x имеет место $A(x, y, z)$ или «существует такое x, что $A(x, y, z)$».

Совершенно аналогично применяются кванторы к любому предикату с бо́льшим числом переменных. В результате применения квантора к n-местному предикату (при $n > 0$) получается $(n-1)$-местный предикат.

К одному и тому же предикату можно применять кванторы несколько раз. Например, применив к предикату $A(x, y)$ квантор существования по x, мы получим одноместный предикат $\exists xA(x, y)$, к которому опять можем применить квантор существования или квантор общности по переменной y. В результате получим высказывание

$$\exists y(\exists xA(x, y)) \quad \text{или} \quad \forall y(\exists xA(x, y)).$$

Скобки обычно опускают, получая при этом выражения

$$\exists y\exists xA(x, y) \quad \text{или} \quad \forall y\exists xA(x, y).$$

Отметим, что одинаковые кванторы можно переставлять, получая при этом эквивалентные высказывания, т. е. истинные эквиваленции:

$$\forall x \forall y\,(x,\ y) \leftrightarrow \forall y \forall x A\,(x,\ y);$$
$$\exists x \exists y A\,(x,\ y) \leftrightarrow \exists y \exists x A\,(x,\ y).$$

В самом деле, высказывания $\forall x \forall y\ A\,(x,\ y)$ и $\forall y \forall x A\,(x,\ y)$ оба истинны тогда и только тогда, когда предикат $A\,(x,\ y)$ тождественно истинен. Высказывания $\exists x \exists y\,(x,\ y)$ и $\exists y \exists x A\,(x,\ y)$ оба истинны тогда и только тогда, когда $A\,(x,\ y)$ — выполнимый предикат. Однако если к предикату применять последовательно разные кванторы, то порядок их следования существен. Например, высказывания $\forall y \exists x A\,(x,\ y)$ и $\exists x \forall y A\,(x,\ y)$, вообще говоря, не эквивалентны, т. е. могут иметь разные истинностные значения.

Применение к предикату одного или нескольких кванторов (общности, существования) называется *квантификацией*.

Рассмотрим применение кванторов на примере. Пусть $x+y>0$ — двухместный предикат, где x и y — целочисленные переменные. Этот предикат выражает положительность суммы двух целых чисел и представляет собой некоторое высказывание всякий раз, когда переменным x и y придаются конкретные значения. Если к этому предикату применить квантор существования по переменной y, то получится одноместный предикат

$$\exists y\,(x+y>0).$$

Когда переменной x этого предиката придается какое-либо значение, то получается высказывание. Предикат $\exists y\,(x+y>0)$ истинен для тех значений переменной x, для которых существует целое число y, дающее в сумме с x положительное число. Легко убедиться, что этот предикат тождественно истинен, поэтому если применить к нему квантор общности по переменной x, то получится истинное высказывание

$$\forall x \exists y\,(x+y>0),$$

утверждающее, что для всякого целого числа x существует некоторое целое число y такое, что их сумма положительна. Это высказывание надо отличать от высказывания

$$\exists y \forall x\,(x+y>0),$$

утверждающего, что существует целое число, сумма которого со всяким целым числом положительна. Это последнее высказывание ложно.

Запись высказываний на языке логики предикатов. Рассмотрим четыре основных типа высказываний, часто встречающихся в математике. В символической записи этих высказываний (записи на языке логики предикатов) используются кванторы.

Пусть $A(x)$ — обозначение предиката «x — нечетное число», а $B(x)$ — обозначение предиката «x — простое число», где x — целочисленная переменная.

1. Высказывание «Всякое нечетное число является простым числом» можно переформулировать следующим образом: «Для всякого x, если x — нечетное, то x — простое число». Теперь ясно, что это высказывание на языке предикатов запишется так:

$$\forall x(A(x) \to B(x)).$$

2. Высказывание «Никакое нечетное число не является простым числом», или «Для всякого x, если x — нечетное, то x не является простым», в символической форме запишется так:

$$\forall x(A(x) \to \neg B(x)).$$

Заметим, что истинностное значение высказывания в наших рассуждениях не играет роли.

3. Следующий тип высказывания: «Некоторые нечетные числа — простые». Суть его в том, что существует такое x, которое одновременно является и нечетным числом, и простым. Поэтому высказывание третьего типа на языке логики предикатов запишется в виде

$$\exists x(A(x) \wedge B(x)).$$

Эта последняя запись не эквивалентна записи

$$\exists x(A(x) \to B(x)),$$

которая выражает совсем не тот смысл, что исходное высказывание.

4. К четвертому типу относится высказывание «Некоторые нечетные числа не являются простыми». Это высказывание записывается так:

$$\exists x(A(x) \wedge \neg B(x)).$$

Рассмотренные примеры показывают, как любое высказывание, относящееся к одному из четырех основных типов, можно записать в символической форме.

В дальнейшем иногда для высказывания «Существует положительное x такое, что $A(x)$» вместо символической записи

$$\exists x\,(x > 0 \wedge A(x))$$

будет употребляться более короткая запись $(\exists x > 0)\,A(x)$. Аналогично, для высказывания «Для всякого положительного x имеет место $A(x)$» вместо записи

$$\forall x\,(x > 0 \to A(x))$$

будет употребляться запись $(\forall x > 0)\,A(x)$.

Упражнения

1. Запишите на языке логики предикатов следующие высказывания:

(a) Некоторые действительные числа являются рациональными.

(b) Ни одно простое число не является точным квадратом.

(c) Некоторые четные числа не делятся на 8.

(d) Всякое число, кратное 6, делится на 3.

2. Пусть $P(x)$ обозначает «x — простое число», $Q(x)$ — «x — четное число», $R(x)$ — «x — целое число», $D(x, y)$ — «x делит y». Сформулируйте словами следующие высказывания, записанные на языке логики предикатов. Отметьте, какие из них истинные и какие ложные:

(a) $\forall x P(x) \to \neg Q(x)$;

(b) $\forall x\,(\neg P(x) \to \forall y\,(P(y) \to \neg D(x, y)))$;

(c) $\forall x\,(Q(x) \to \forall y\,(D(x, y) \to Q(y)))$;

(d) $\forall x \exists y\,(R(x) \wedge R(y) \to D(x, y))$;

(e) $\forall y \forall x\,(R(x) \wedge R(y) \to D(x, y))$;

(f) $\exists x \forall y\,(R(x) \wedge R(y) \to D(x, y))$.

3. Используя логические символы, запишите следующие высказывания:

(a) Числа 5 и 12 не имеют общих делителей, отличных от $+1$ и -1.

(b) Натуральное число, делящееся на 6, делится на 2 и на 3.

(c) Для любого целого числа x существует такое целое число y, что $x = 2y$ или $x = 2y + 1$.

(d) Для любого натурального числа существует натуральное число, которое больше его.

(e) Существует наименьшее натуральное число.

(f) Система уравнений $x + y = 0$, $x + y = 1$ не имеет решений (несовместна).

(g) Не существует такого рационального числа x, что $x^2 - 2 = 0$.

(h) Для всяких целых x и z существует целое число y такое, что $x + y = z$.

(i) Для любых двух рациональных чисел x и y существует рациональное число z такое, что $x < z$ и $z < y$.

4. Выясните, имеют ли место следующие равносильности для любых предикатов $P(x, y)$, $Q(x)$, $R(x)$. Если нет, то приведите примеры предикатов, подтверждающие это:

(a) $\forall x \exists y P(x, y) \equiv \exists y \forall x P(x, y)$;
(b) $\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y)$;
(c) $\forall x (R(x) \vee Q(x)) \equiv \forall x R(x) \vee \forall x Q(x)$;
(d) $\exists x (R(x) \wedge Q(x)) \equiv \exists x R(x) \wedge \exists x Q(x)$;
(e) $\forall x \forall y (R(x) \vee Q(y)) \equiv \forall x R(x) \vee \forall x Q(x)$;
(f) $\forall x Q(x) \to \exists x R(x) \equiv \exists x (Q(x) \to R(x))$;
(g) $\exists x R(x) \vee \forall x Q(x) \equiv \exists x (R(x) \to Q(x))$;
(h) $\forall x (R(x) \to Q(x)) \equiv \forall x R(x) \to \forall x Q(x)$.

§ 5. ПРЕДИКАТНЫЕ ФОРМУЛЫ. ЗАКОНЫ ЛОГИКИ

Элементарные формулы. Пусть в нашем распоряжении имеется список переменных

$$x, y, z, u, w, \ldots, x_1, y_1, z_1, u_1, w_1, \ldots,$$

которые часто называют *предметными переменными*, так как вместо них подставляются имена определенных предметов

$$a, b, c, a_1, b_1, c_1, \ldots$$

Кроме того, будем считать, что для каждого натурального n имеется некоторая совокупность выражений

$$P(x_1, x_2, \ldots, x_n), Q(x, y, \ldots, t), R(y_1, \ldots, y_n), \ldots,$$

называемых n-местными *предикатными символами*. Например, $P(x)$, $Q(y)$ — одноместные предикатные символы, $P(x, y)$, $Q(x_1, x_2)$ — двухместные, $P(x, y, z)$, $R(x_1, x_2, x_3)$ — трехместные, A, B, ..., P, Q — нульместные. Исходя из этой совокупности предикатных символов, образуем выражения, которые будем называть элементарными формулами или атомами логики предикатов.

ОПРЕДЕЛЕНИЕ. *Элементарной формулой* называется выражение, которое получается из предикатного символа подстановкой вместо входящих в него переменных $(x, y, \ldots)$ каких-либо не обязательно различных предметных переменных.

Например, исходя из одноместного предикатного символа $P(x)$, получаем элементарные формулы (атомы), $P(x)$, $P(y)$, $P(u)$ и т. д.; исходя из двухместного предикатного символа $Q(x, y)$, — элементарные формулы $Q(x, y)$, $Q(y, z)$, $Q(u, v)$, $Q(x, x)$ и т. д. Исходя из предикатного символа

$R(x, y, z)$ — элементарные формулы $R(x, y, z)$, $R(y, z, x)$, $R(u, v, w)$, $R(x, x, x)$, $R(x, y, x)$ и т. д. Исходные нульместные предикатные символы также попадают в совокупность элементарных формул. Элементарные формулы образуют более обширную совокупность, чем исходная совокупность предикатных символов, так как предметные переменные, входящие в элементарные формулы, не обязаны быть различными.

Предикатные формулы. *Предикатные формулы* (формулы логики предикатов) вводятся следующим образом:

(a) всякая элементарная формула есть предикатная формула:

(b) если $\boldsymbol{A}$ и $\boldsymbol{B}$ — предикатные формулы, то $(\neg \boldsymbol{A})$, $(\boldsymbol{A} \wedge \boldsymbol{B})$, $(\boldsymbol{A} \vee \boldsymbol{B})$, $(\boldsymbol{A} \rightarrow \boldsymbol{B})$ и $(\boldsymbol{A} \leftrightarrow \boldsymbol{B})$ суть предикатные формулы. Если $\boldsymbol{A}$ — предикатная формула и x — предметная переменная, то $(\forall x \boldsymbol{A})$ и $(\exists x \boldsymbol{A})$ суть предикатные формулы;

(c) выражение есть предикатная формула в том случае, если оно есть элементарная формула или построено из элементарных формул последовательным применением правил a) и b).

Предикатные формулы, не являющиеся элементарными формулами, называются *составными предикатными формулами*.

Для обозначения формул логики предикатов будем употреблять большие буквы латинского алфавита, напечатанные жирным шрифтом: $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, ..., $\boldsymbol{R}$, $\boldsymbol{P}$, $\boldsymbol{Q}$ и т. д.

В формулах $(\forall x \boldsymbol{A})$ и $(\exists x \boldsymbol{A})$ формула A называется *областью действия кванторов* $\forall x$ и $\exists x$ соответственно.

Обычно принимают соглашения об опускании скобок. Кроме того, считают, что кванторы связывают сильнее остальных операций. Поэтому формулу $(\forall x P(x)) \rightarrow R(x, y)$ можно записать так: $\forall x P(x) \rightarrow R(x, y)$.

ОПРЕДЕЛЕНИЕ. Предикатная формула называется *общезначимой*, если после замены входящих в нее элементарных формул любыми предикатами получается тождественно истинный предикат.

ОПРЕДЕЛЕНИЕ. Предикатные формулы называются *равносильными*, если после замены входящих в них элементарных формул любыми предикатами получаются равносильные предикаты. Записывать равносильность формул $\boldsymbol{A}$ и $\boldsymbol{B}$ будем так: $\boldsymbol{A} \equiv \boldsymbol{B}$.

Легко доказать, что предикатная формула $\boldsymbol{A} \leftrightarrow \boldsymbol{B}$ общезначима тогда и только тогда, когда $\boldsymbol{A}$ и $\boldsymbol{B}$ — равносильные предикатные формулы.

Целый ряд равносильностей логики предикатов можно получить из равносильностей логики высказываний. Например, равносильностям логики высказываний

$$A \wedge B \equiv B \wedge A;$$
$$\neg\neg A \equiv A;$$
$$\neg(A \vee B) \equiv \neg A \wedge \neg B;$$
$$\neg(A \wedge B) \equiv \neg A \vee \neg B$$

соответствуют равносильности логики предикатов

$$\boldsymbol{A \wedge B \equiv B \wedge A};$$
$$\boldsymbol{\neg\neg A \equiv A};$$
$$\boldsymbol{\neg(A \vee B) \equiv \neg A \wedge \neg B};$$
$$\boldsymbol{\neg(A \wedge B) \equiv \neg A \vee \neg B}.$$

Аналогично, тождественно истинные формулы логики высказываний служат источником для получения общезначимых формул логики предикатов. Например, тавтологии $A \vee \neg A$ соответствует общезначимая формула логики предикатов $\boldsymbol{A \vee \neg A}$. Действительно, подставив в любую конкретную формулу $\boldsymbol{A}$ вместо входящих в нее предикатных символов произвольные предикаты, получим некоторый предикат $P(x_1, \ldots, x_n)$. При этом формула $\boldsymbol{A \vee \neg A}$ превратится в предикат $P(x_1, \ldots, x_n) \vee \neg P(x_1, \ldots, x_n)$, который принимает значение И при любых допустимых значениях переменных (в силу закона исключенного третьего в логике высказываний).

Рассуждая так же, можно обосновать остальные общезначимые формулы и равносильности логики предикатов, перенесенные из логики высказываний.

Кроме общезначимых формул и равносильностей логики предикатов, получаемых таким образом, существуют специфические общезначимые формулы и равносильности, связанные с применением кванторов. Некоторые из них мы рассмотрим.

Законы логики предикатов. Рассмотрим ряд равносильностей, играющих большую роль в логике предикатов. Строгое их доказательство проводить не будем. Равносильность

$$(1) \quad \neg(\forall x A(x)) \equiv \exists x(\neg A(x))$$

соответствует обычному пониманию смысла кванторов. Высказывания «Неверно, что всякий объект x удовлетворяет

условию $A(x)$» и «Существует объект x, не удовлетворяющий условию $A(x)$» имеют одинаковый смысл, что и отражает равносильность (1).

Равносильность

(2) $\neg(\exists x A(x)) \equiv \forall x(\neg A(x))$

соответствует тому, что высказывание «Неверно, что существует объект x удовлетворяющий условию $A(x)$» обычно понимают в том же смысле, что и высказывание «Ни один объект x не удовлетворяет условию $A(x)$».

Применяя отрицание к обеим частям (1) и (2) и учитывая закон двойного отрицания, получаем еще две равносильности:

(3) $\forall x A(x) \equiv \neg(\exists x \neg A(x))$;

(4) $\exists x A(x) \equiv \neg(\forall x \neg A(x))$;

они показывают, что квантор существования можно выразить через квантор общности и наоборот.

Следующие две равносильности выражают свойства дистрибутивности квантора общности относительно конъюнкции и квантора существования относительно дизъюнкции:

(5) $\exists x A(x) \vee \exists x B(x) \equiv \exists x(A(x) \vee B(x))$;

(6) $\forall x A(x) \wedge \forall x B(x) \equiv \forall x(A(x) \wedge B(x))$.

С истинностью этих равносильностей находятся в соответствии следующие содержательные рассуждения. Левая часть (5) принимает значение И в том и только в том случае, когда или $A(x)$, или $B(x)$ принимает значение И хотя бы для одного допустимого значения x, т. е. когда по крайней мере один из предикатов $A(x)$ и $B(x)$ выполним. Но как раз в этом и только в этом случае будет выполним предикат $A(x) \vee B(x)$, т. е. будет истинным высказывание $\exists x(A(x) \vee B(x))$. Аналогичные рассуждения можно провести относительно равносильности (6).

Квантор существования не дистрибутивен относительно конъюнкции, т. е. формулы $\exists x(A(x) \wedge B(x))$ и $\exists x A(x) \wedge \wedge \exists x B(x)$ не равносильны. Нетрудно подобрать пример двух выполнимых предикатов, конъюнкция которых невыполнима. Для таких предикатов первая формула принимает значение Л, а вторая — И. Также не равносильны формулы $\forall x(A(x) \vee B(x))$ и $\forall x A(x) \vee \forall x B(x)$, т. е. квантор общности не дистрибутивен относительно дизъюнкции.

Каждой равносильности логики предикатов соответствует общезначимая формула. Например, общезначимыми будут следующие формулы (их часто называют *законами логики*):

(1) $\neg(\forall x A(x)) \leftrightarrow \exists x(\neg A(x))$;

(2) $\neg(\exists x A(x)) \leftrightarrow \forall x(\neg A(x))$;

(3) $\forall x A(x) \leftrightarrow \neg(\exists x \neg A(x))$;

(4) $\exists x A(x) \leftrightarrow \neg(\forall x \neg A(x))$;

(5) $\exists x A(x) \vee \exists x B(x) \leftrightarrow \exists x(A(x) \vee B(x))$;

(6) $\forall x A(x) \wedge \forall x B(x) \leftrightarrow \forall x(A(x) \wedge B(x))$.

В логике высказываний существует общий метод, позволяющий за конечное число шагов выяснить для любой пропозициональной формулы, является ли она тождественно истинной (метод истинностных таблиц). В логике предикатов не существует такого общего метода, по которому за конечное число шагов для любой предикатной формулы можно решить, общезначима она или нет. Для некоторых видов формул такие методы существуют.

Упражнения

1. Выясните, являются ли общезначимыми следующие формулы (если нет, то подтвердите это примерами):

(a) $\exists x P(x) \rightarrow \forall x P(x)$;

(b) $\forall x P(x) \rightarrow P(y)$;

(c) $P(y) \rightarrow \forall x P(x)$;

(d) $\exists x Q(x) \rightarrow Q(y)$;

(e) $\forall x \exists y Q(x, y) \rightarrow \exists y \forall x Q(x, y)$;

(f) $\forall x \forall y \forall z (P(x, y) \wedge P(y, z) \rightarrow P(x, z))$;

(g) $\forall x P(x) \vee \forall x Q(x) \leftrightarrow \exists x (P(x) \wedge Q(x))$;

(h) $\forall x (P(x) \leftrightarrow Q(x)) \rightarrow (\exists x P(x) \leftrightarrow \exists x Q(x))$;

(i) $\exists x P(x) \wedge \exists x Q(x) \rightarrow \exists x (P(x) \wedge Q(x))$;

(j) $\forall x (P(x) \vee Q(x)) \rightarrow \forall x P(x) \vee \forall x Q(x)$.

2. Обоснуйте общезначимость следующих формул:

(a) $\forall x P(x) \vee \forall x Q(x) \rightarrow \forall x (P(x) \vee Q(x))$;

(b) $\exists x (P(x) \wedge Q(x)) \rightarrow \exists x P(x) \wedge \exists x Q(x)$;

(c) $\forall x (P(x) \rightarrow Q(x)) \rightarrow (\forall x P(x) \rightarrow \forall x Q(x))$;]

(d) $\forall x (P(x) \leftrightarrow Q(x)) \rightarrow (\forall x P(x) \leftrightarrow \forall x Q(x))$;

(e) $\forall x (P(x) \rightarrow Q(x)) \rightarrow (\exists x P(x) \rightarrow \exists x Q(x))$;

(f) $\forall x \boldsymbol{Q}(x) \to \exists x \boldsymbol{Q}(x)$;
(g) $\forall x P(x) \to P(y)$;
(h) $\boldsymbol{Q}(y) \to \exists x \boldsymbol{Q}(x)$;
(i) $\neg \neg \forall x P(x, y) \to \forall x P(x, y)$;
(j) $\forall x \forall y P(x, y) \leftrightarrow \forall y \forall x P(x, y)$;
(k) $\exists x \exists y \boldsymbol{R}(x, y) \leftrightarrow \exists y \exists x \boldsymbol{R}(x, y)$;
(l) $\exists x P(x) \wedge \exists x \boldsymbol{Q}(x) \leftrightarrow \exists x \exists y (P(x) \wedge \boldsymbol{Q}(y))$;
(m) $\forall x \boldsymbol{R}(x) \vee \forall x \boldsymbol{Q}(x) \leftrightarrow \forall x \forall y (P(x) \vee \boldsymbol{Q}(y))$;
(n) $\forall x \boldsymbol{Q}(x, z) \leftrightarrow \forall y \boldsymbol{Q}(y, z)$;
(o) $\exists x P(x, z) \leftrightarrow \exists y P(y, z)$;
(p) $\forall x \neg P(x) \vee \forall x \boldsymbol{Q}(x) \leftrightarrow \exists x P(x) \to \forall x \boldsymbol{Q}(x)$;
(r) $\exists x (P(x) \to \boldsymbol{Q}(x)) \leftrightarrow \forall x P(x) \to \exists x \boldsymbol{Q}(x)$.

Глава вторая
МНОЖЕСТВА И ОТНОШЕНИЯ

§ 1. МНОЖЕСТВА

Понятие множества. Понятие множества — одно из основных понятий математики. Под *множеством* понимают совокупность объектов (предметов или понятий), которая рассматривается как одно целое. Например, можно говорить о множестве всех натуральных чисел, о множестве букв на данной странице, о множестве корней данного уравнения и т. п. Объекты, входящие в состав множества, называются его *элементами*. Понятие множества принимается как исходное, первичное, т. е. не сводимое к другим понятиям.

Утверждения «Объект a есть элемент множества A», «Объект a принадлежит множеству A», которые имеют один и тот же смысл, сокращенно записывают в виде $a \in A$.

Если элемент a не принадлежит множеству A, то пишут $a \notin A$.

Символ $\in$ называется *знаком принадлежности*.

ОПРЕДЕЛЕНИЕ. Два множества A и B называют *равными* и пишут $A = B$, если A и B содержат одни и те же элементы.

Таким образом, *множества* A и B *равны,* если для любого x $x \in A$ тогда и только тогда, когда $x \in B$. В связи с этим доказательство равенства двух данных множеств A и B обычно состоит из доказательства двух утверждений: 1) для любого x, если $x \in A$, то $x \in B$; 2) для любого x, если $x \in B$, то $x \in A$.

Часто множество обозначается его элементами, заключенными в фигурные скобки. Так, например, множество, состоящее из элементов a, b, c, обозначается $\{a, b, c\}$. Множество, состоящее из элементов $a_1, a_2, \ldots, a_n$, обозначается $\{a_1, a_2, \ldots, a_n\}$.

Множества $\{1, 2, 3,\}$ и $\{3, 1, 2, 1\}$ равны, так как каждый элемент первого множества принадлежит второму множе-

ству и наоборот. Они оба состоят из трех элементов. Обычно используют запись $\{1, 2, 3\}$.

Множество может состоять из одного элемента. Необходимо различать элемент a и множество $\{a\}$, содержащее только один элемент a, хотя бы потому, что допускаются множества, элементы которых сами суть множества. Например, множество $a = \{2, 1\}$ состоит из двух элементов 2 и 1; множество $\{a\}$ состоит из одного элемента a, который сам является двухэлементным множеством.

Подмножества.

ОПРЕДЕЛЕНИЕ. Множество A называется *подмножеством* множества B, если каждый элемент множества A принадлежит множеству B.

Если A есть подмножество множества B, то говорят также, что A содержится в B, и пишут $A \subset B$. Символ $\subset$ называется *знаком включения*. Согласно определению,

$$A \subset B \leftrightarrow (\text{для каждого } x,\ x \in A \rightarrow x \in B).$$

Множество A называется *собственным подмножеством* множества B, если $A \subset B$ и $A \neq B$. Запись $A \overset{\subset}{\neq} B$ означает, что A является собственным подмножеством множества B.

Отметим свойства отношения включения, легко следующие из определения:

(a) отношение включения *рефлексивно*, т. е. $A \subset A$ для каждого множества A;

(b) отношение включения *транзитивно*, т. е. для любых множеств A, B, C из $A \subset B$ и $B \subset C$ следует $A \subset C$;

(c) отношение включения *антисимметрично*, т. е. для любых множеств A, B, C из $A \subset B$ и $B \subset A$ следует $A = B$.

Из свойства (c) следует, что для доказательства равенства множеств A и B достаточно доказать, что $A \subset B$ и $B \subset A$, т. е.

$$(A = B) \leftrightarrow (A \subset B \wedge B \subset A).$$

В теории множеств принимается следующий принцип выделения подмножеств данного множества с помощью одноместных предикатов: *для любого множества A и одноместного предиката $P(x)$, имеющего смысл для всех элементов множества A* (т. е. такого, что для любого x из A $P(x)$ либо истинно, либо ложно), *существует множество, состоящее в точности из тех элементов множества A, для которых $P(x)$ истинно.*

Это множество обозначают так:

$\{x \in A \mid P(x)$ истинно$\}$, или, короче, $\{x \in A \mid P(x)\}$. Последняя запись читается так: «множество таких x из A, что $P(x)$ истинно» или «множество таких x из A, что верно $P(x)$». Иногда для обозначения этого же множества используется и такая запись:

$$\{x \mid x \in A \wedge P(x)\}.$$

Если два одноместных предиката $P(x)$ и $Q(x)$ равносильны, то согласно определению равенства множеств они определяют одно и то же подмножество множества A, т. е. из равносильности $P(x) \equiv Q(x)$ следует равенство

$$\{x \in A \mid P(x)\} = \{x \in A \mid Q(x)\}.$$

Пустое множество. Введем новое важное понятие.

ОПРЕДЕЛЕНИЕ. Множество, не содержащее ни одного элемента, называется *пустым множеством*.

Таким образом, множество A называют пустым, если для любого x $x \notin A$. Такое множество единственно. В самом деле, если C и D — пустые множества, то для каждого x верна эквивалентность $x \in C \leftrightarrow x \in D$, так как оба ее члена ложны. Согласно определению равенства множеств отсюда следует, что $C = D$.

Единственное пустое множество обозначается символом $\emptyset$. Таким образом, для каждого x $x \notin \emptyset$.

ПРЕДЛОЖЕНИЕ. 1.1. *Пустое множество является подмножеством любого множества.*

Доказательство. В самом деле, пусть A — любое множество. Для каждого x верна импликация $x \in \emptyset \rightarrow x \in A$, так как импликация с ложной посылкой истинна. Следовательно, $\emptyset \subset A$. □

Операции над множествами. Рассмотрим операции над множествами, с помощью которых можно получать из любых двух множеств новые множества.

ОПРЕДЕЛЕНИЕ. *Объединением множеств* A и B называется множество, состоящее из тех и только тех элементов, которые принадлежат хотя бы одному из множеств A и B.

Такое множество всегда существует.

Из определения равенства двух множеств следует, что для любых множеств A и B существует единственное множество, являющееся их объединением. В самом деле, если бы существовали два таких множества C и D, то они со-

держали бы одни и те же элементы и поэтому совпадали. Это единственное множество, объединение множеств A и B, обозначается $A \cup B$. Таким образом, по определению,

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

Следовательно, для произвольного x верна эквивалентность

$$x \in A \cup B \leftrightarrow x \in A \vee x \in B.$$

Из определения объединения множеств следует также, что $A \subset A \cup B$ и $B \subset A \cup B$.

Пример. Если $A = \{1, 9, 18\}$ и $B = \{1, 5, 9\}$, то $A \cup B = \{1, 5, 9, 18\}$.

ОПРЕДЕЛЕНИЕ. *Пересечением множеств* A и B называется множество, состоящее из тех и только тех элементов, которые принадлежат как множеству A, так и множеству B.

Такое множество всегда существует.

Для любых двух множеств A и B существует единственное множество, являющееся их пересечением. В самом деле, если бы существовали два таких множества C и D, то они содержали бы одни и те же элементы и поэтому совпадали. Пересечение множеств A и B обозначается $A \cap B$. Таким образом, по определению,

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

Следовательно, для произвольного x верна эквивалентность

$$x \in A \cap B \leftrightarrow x \in A \wedge x \in B.$$

Из определения пересечения множеств следует, что $A \cap B \subset A$ и $A \cap B \subset B$.

Пример. Если $A = \{1/2, 2/3, 5/6\}$, $B = \{1, 3/2, 1/2\}$, то $A \cap B = \{1/2\}$.

ОПРЕДЕЛЕНИЕ. *Разностью множеств* A и B называется множество, элементами которого являются элементы множества A, не принадлежащие множеству B, и только они.

Для любых множеств A и B всегда существует такое множество, и притом единственное. Разность множеств A и B обозначается $A \setminus B$. Таким образом, по определению,

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}.$$

Следовательно, для любого x верна эквивалентность

$$x \in A \setminus B \leftrightarrow x \in A \wedge x \notin B.$$

Пример. Если $A=\{6, 9, 12, 13\}$, $B=\{6, 9, 10\}$, то $A \setminus B=\{12, 13\}$.

ТЕОРЕМА 1.2. *Для любых множеств A и B эквивалентны следующие три соотношения:*

(a) $A \subset B$; (b) $A \cup B=B$; (c) $A \cap B=A$.

Доказательство. (a)$\rightarrow$(b). Каждый элемент множества $A \cup B$ принадлежит A или B и в силу (a) является элементом множества B, т. е. $A \cup B \subset B$. Кроме того, $B \subset A \cup B$; следовательно, $A \cup B=B$;

(a)$\rightarrow$(c). В силу (a) каждый элемент множества A есть общий элемент A и B, т. е. $A \subset A \cap B$. Кроме того, $A \cap B \subset A$; следовательно, $A \cap B=A$;

(b)$\rightarrow$(c). Имеем $A \subset A \cup B$ и в силу (b) $A \cup B \subset B$, поэтому $A \subset B$. Поскольку (a)$\rightarrow$(c), то следует равенство (c);

(c)$\rightarrow$(a). В силу (c) $A \subset A \cap B$. Кроме того, $A \cap B \subset B$; следовательно, $A \subset B$. □

Основные свойства операций над множествами. Операции объединения и пересечения над множествами обладают рядом свойств. Мы рассмотрим основные, наиболее важные свойства этих операций.

ТЕОРЕМА 1.3. *Для любых множеств A, B и C имеем*:

(1) $A \cup A=A$ — *идемпотентность объединения;*

(2) $A \cap A=A$ — *идемпотентность пересечения*;

(3) $A \cup B=B \cup A$ — *коммутативность объединения;*

(4) $A \cap B=B \cap A$ — *коммутативность пересечения*;

(5) $A \cup (B \cup C)=(A \cup B) \cup C$ — *ассоциативность объединения*;

(6) $A \cap (B \cap C)=(A \cap B) \cap C$ — *ассоциативность пересечения*;

(7) $A \cup (B \cap C)=(A \cup B) \cap (A \cup C)$ — *дистрибутивность объединения относительно пересечения*;

(8) $A \cap (B \cup C)=(A \cap B) \cup (A \cap C)$ — *дистрибутивность пересечения относительно объединения.*

Доказательство. Первые четыре свойства, свойства идемпотентности и коммутативности, легко следуют из определения операций объединения и пересечения. Для того чтобы доказать свойство ассоциативности (5), достаточно заметить, что $A \cup (B \cup C)$ есть множество элементов, принадлежащих множеству A, или множеству B, или множеству C, и множество $(A \cup B) \cup C$ состоит из тех же элементов. Аналогично доказывается свойство (6).

Докажем свойство (7). Пусть

$$D = A \cup (B \cap C), \quad E = (A \cup B) \cap (A \cup C).$$

Надо доказать, что множества D и E равны, т. е. (a) если $x \in D$, то $x \in E$; (b) если $x \in E$, то $x \in D$.

Пусть $x \in A \cup (B \cap C)$. Тогда возможны два случая:

(a_1) $x \in A$ и (a_2) $x \in B \cap C$.

В случае (a_1) $x \in A \cup B$ и $x \in A \cup C$; следовательно, $x \in E$. В случае (a_2) $x \in B$ и $x \in C$, так что $x \in A \cup B$ и $x \in A \cup C$; следовательно, $x \in E$.

Предположим теперь, что $x \in E$, т. е. $x \in (A \cup B) \cap \cap (A \cup C)$, тогда

$$x \in A \cup B \text{ и } x \in A \cup C.$$

При этом если $x \notin A$, то $x \in B$ и $x \in C$, так что $x \in B \cap C$; следовательно, $x \in A \cup (B \cap C)$. Если же $x \in A$, то $x \in A \cup \cup (B \cap C)$, т. е. $x \in D$. Из (a) и (b) следует равенство (5).

Свойство дистрибутивности (8) доказывается аналогично. □

Универсальное множество. Дополнение множества. Во многих приложениях теории множеств рассматриваются только такие множества, которые содержатся в некотором фиксированном множестве. Например, в геометрии мы имеем дело с множествами точек данного пространства, в элементарной арифметике — с подмножествами множества всех целых чисел.

Всюду ниже буквы A, B, ... обозначают множества, содержащиеся в некотором фиксированном множестве, которое назовем *универсальным* и будем обозначать через U. Таким образом, мы считаем, что для каждого рассматриваемого множества A имеем $A \subset U$. Следовательно, для каждого множества A

(1) $A \cup U = U$, $A \cap U = A$.

ОПРЕДЕЛЕНИЕ. Множество $U \setminus A$ называется *дополнением множества* A и обозначается через A' (или через $\bar{A}$). Дополнение $U \setminus A'$ множества A' обозначается через A'' (или $\bar{\bar{A}}$).

Нетрудно видеть, что

(2) $A \cup A' = U$, $A \cap A' = \phi$.

ПРЕДЛОЖЕНИЕ 1.4. *Для любого множества* A

(3) $A'' = A$ (закон инволюции).

Доказательство предоставляется провести читателю.

ПРЕДЛОЖЕНИЕ 1.5. *Если* $A \subset B$, *то* $B' \subset A'$.

Доказательство. Пусть $A \subset B$. Надо доказать, что для всякого x из U, если $x \in B'$, то $x \in A'$. Действительно, если $x \in B'$, то $x \notin B$. Учитывая условие $A \subset B$, мы заключаем, что $x \notin A$ и $x \in A'$. □

ТЕОРЕМА 1.6. *Имеют место следующие тождества:*

(4) $(A \cup B)' = A' \cap B'$
(5) $(A \cap B)' = A' \cup B'$ } *(законы де Моргана для множеств).*

Доказательство. Покажем, что для всякого x

(6) $x \in (A \cup B)' \leftrightarrow x \in A' \cap B'$.

В самом деле, $x \in (A \cup B)'$ тогда и только тогда, когда $x \notin A \cup B$. Но $x \notin A \cup B$ в том и только в том случае, когда $x \notin A$ и $x \notin B$, т. е. когда $x \in A'$ и $x \in B'$ и, значит, $x \in A' \cap B'$.

Тождество (5) можно доказать следующим образом. Используя тождество (4) и закон инволюции, получим

$$(A' \cup B')' = A'' \cap B'' = A \cap B.$$

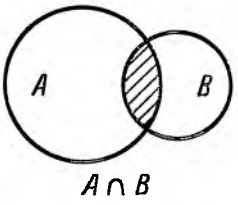
Следовательно,

$$(A \cap B)' = (A' \cup B')'' = A' \cup B',$$

т. е. справедливо тождество (5). □

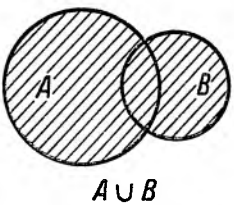
Диаграммы Эйлера — Венна. Для графического изображения множеств и их свойств используются так называемые диаграммы Эйлера, которые называются также диаграммами Венна. Множество изображается кругом (или другой связной фигурой) на плоскости и мыслится как множество точек круга. Если изобразить кругами множества A и B, то множества $A \cap B$ и $A \cup B$ изобра-

зятся заштрихованными областями (рис. 1 и 2). Множества $A \setminus B$ и $B \setminus A$ изобразятся соответственно на диаграммах (рис. 3 и 4). Отношение $A \subset B$ изображено на рис. 5.



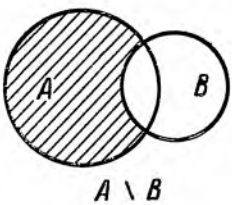
$A \cap B$

Рис. 1



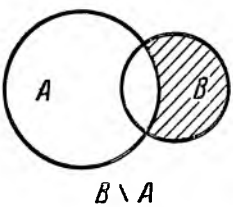
$A \cup B$

Рис. 2



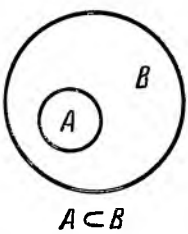
$A \setminus B$

Рис. 3



$B \setminus A$

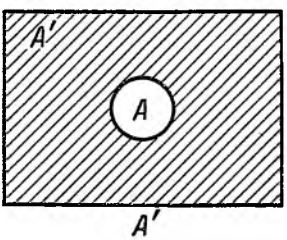
Рис. 4



$A \subset B$

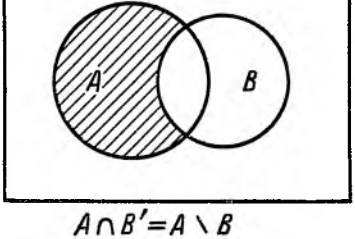
Рис. 5

Универсальное множество U изображается множеством точек некоторого прямоугольника. Дополнение A' множества A до U изображается на рис. 6 той (заштрихованной)



A'

Рис. 6



$A \cap B' = A \setminus B$

Рис. 7

частью прямоугольника, которая находится за пределами круга, изображающего множество A. Равенство $A \setminus B = A \cap B'$ иллюстрируется на рис. 7.

Упражнения

1. Докажите следующие тождества:

(a) $A \setminus B = A \cap B'$;
(b) $A \setminus (A \setminus B) = A \cap B$;
(c) $B \cup (A \setminus B) = A \cup B$;
(d) $B \cap (A \setminus B) = \emptyset$;
(e) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
(f) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

Изобразите их с помощью диаграмм Эйлера — Венна.

2. Покажите на примерах, что не всегда верны следующие формулы:

(a) $(A \cup B) \setminus B = A$; (b) $(A \setminus B) \cup B = A$.

3. Докажите следующие утверждения:

(a) $B \subset A \to (A \setminus B) \cup B = A$;
(b) $A \subset B \equiv A \cap B = A$;
(c) $A \subset B \equiv A \cup B = A$;
(d) $A \cap B = \emptyset \to (A \cup B) \setminus B = A$;
(e) $A \subset B \to A \setminus C \subset B \setminus C$;
(f) $A \subset B \to A \cap C \subset B \cap C$;
(g) $A \subset B \to A \cup C \subset B \cup C$;
(h) $B \subset A \wedge C = A \setminus B \to A = B \cup C$;
(i) $A \not\subset B \wedge B \cap C = \emptyset \to A \cup C \not\subset B \cup C$;
(k) $C = A \setminus B \to B \cap C = \emptyset$;
(l) $A \not\subset B \to A \setminus B \neq \emptyset$;
(m) $B \cap C = \emptyset \wedge A \cap C \neq \emptyset \to A \setminus B \neq \emptyset$;
(n) $A \subset C \to A \cup (B \cap C) = (A \cup B) \cap C$.

Проиллюстрируйте их с помощью диаграмм Эйлера — Венна.

4. Докажите следующие равносильности:

(a) $A \cup B = \emptyset \equiv A = \emptyset \wedge B = \emptyset$;
(b) $A \setminus B = A \equiv B \setminus A = B$;
(c) $A \cup B = A \setminus B \equiv B = \emptyset$;
(d) $A \setminus B = A \cap B \equiv A = \emptyset$;
(e) $A \cup B \subset C \equiv A \subset C \wedge B \subset C$;
(f) $C \subset A \cap B \equiv C \subset A \wedge C \subset B$;
(g) $A \subset B \cup C \equiv A \setminus B \subset C$;
(h) $A \cap B = A \cup B \equiv A = B$;
(i) $A \subset B \subset C \equiv A \cup B = B \cap C$.

5. Пусть A и B — конечные множества. Докажите, что $n(A \cap B) = n(A) + n(B) - n(A \cap B)$, где $n(M)$ — число элементов множества M.

6. Докажите, что множество, состоящее из n элементов, имеет 2^n различных подмножеств.

7. Покажите, что при $m < n$ множество, состоящее из n элементов, имеет $\frac{n!}{(n-m)!\,(m!)}$ различных m-элементных подмножеств (где $m! = 1 \cdot 2 \ldots m$).

8. Пусть $A(x)$ и $B(x)$ — одноместные предикаты и U — область допустимых значений переменной x. Докажите, что тогда

$\{x \mid A(x) \vee B(x)\} = \{x \mid A(x)\} \cup \{x \mid B(x)\}$;
$\{x \mid A(x) \wedge B(x)\} = \{x \mid A(x)\} \cap \{x \mid B(x)\}$;
$\{x \mid \neg A(x)\} = U \setminus \{x \mid A(x)\} = \{x \mid A(x)\}'$;
$\{x \mid A(x) \to B(x)\} = \{x \mid A(x)\}' \cup \{x \mid B(x)\}$;
$\{x \mid A(x) \leftrightarrow B(x)\} = (\{x \mid A(x)\}' \cap \{x \mid B(x)\}') \cup (\{x \mid A(x)\} \cap \{x \mid B(x)\})$.

§ 2. БИНАРНЫЕ ОТНОШЕНИЯ

Прямое произведение множеств. Пусть даны какие-нибудь объекты a и b. Если $a \neq b$, то множество $\{a, b\}$ называется *неупорядоченной парой объектов* a и b. Отметим, что всегда $\{a, b\} = \{b, a\}$.

Введем новое исходное понятие — понятие упорядоченной пары. Любым двум объектам a и b поставим в соответствие новый объект — их упорядоченную пару $\langle a, b\rangle$.

ОПРЕДЕЛЕНИЕ. Упорядоченные пары $\langle a, b\rangle$ и $\langle c, d\rangle$ называют *равными* и пишут $\langle a, b\rangle = \langle c, d\rangle$ в том и только в том случае, когда $a = c$ и $b = d$.

В частности, $\langle a, b\rangle = \langle b, a\rangle$ в том и только в том случае, когда $a = b$.

В дальнейшем часто будем говорить «пара $\langle a, b\rangle$» вместо «упорядоченная пара $\langle a, b\rangle$». Элемент a называется *первым элементом пары* $\langle a, b\rangle$, а b — *вторым элементом пары*.

ОПРЕДЕЛЕНИЕ. *Прямым произведением множеств* A и B называется множество всех упорядоченных пар $\langle x, y\rangle$ таких, что $x \in A$ и $y \in B$. Это множество обозначается $A \times B$.

Таким образом,

$$A \times B = \{\langle x, y\rangle \mid x \in A \wedge y \in B\}.$$

Пример. Пусть $A = \{0, 1, 2\}$ и $B = \{3, 5\}$. Тогда имеем:

$A \times B = \{\langle 0, 3\rangle, \langle 0, 5\rangle, \langle 1, 3\rangle, \langle 1, 5\rangle, \langle 2, 3\rangle, \langle 2, 5\rangle\}$;
$B \times A = \{\langle 3, 0\rangle, \langle 5, 0\rangle, \langle 3, 1\rangle, \langle 5, 1\rangle, \langle 3, 2\rangle, \langle 5, 3\rangle\}$.
$A \times A = \{\langle 0, 0\rangle, \langle 0, 1\rangle, \langle 0, 2\rangle, \langle 1, 1\rangle, \langle 1, 0\rangle, \langle 1, 2\rangle, \langle 2, 0\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle\}$;
$B \times B = \{\langle 3, 3\rangle, \langle 3, 5\rangle, \langle 5, 5\rangle, \langle 5, 3\rangle\}$.

Обобщением понятия упорядоченной пары является понятие к о р т е ж а (упорядоченного набора) n объектов. Кортеж n объектов $a_1, \ldots, a_n$ обозначается через $\langle a_1, \ldots, a_n \rangle$.

ОПРЕДЕЛЕНИЕ. Два кортежа $\langle a_1, \ldots, a_n \rangle$ и $\langle b_1, \ldots, b_n \rangle$ называют *равными* и пишут $\langle a_1, \ldots, a_n \rangle = \langle b_1, \ldots, b_n \rangle$ в том и только в том случае, когда $a_1 = b_1, \ldots, a_n = b_n$.

Кортежи трех объектов называют также *упорядоченными тройками. Прямым произведением трех множеств* A, B и C называется множество всех таких упорядоченных троек $\langle x, y, z \rangle$, что $x \in A$, $y \in B$ и $z \in C$. Это множество обозначается через $A \times B \times C$; таким образом,

$$A \times B \times C = \{\langle x, y, z \rangle \mid x \in A, y \in B, z \in C\}.$$

Пусть A — непустое множество и n — целое положительное число. Через A^n обозначается множество всех кортежей $\langle x_1, \ldots, x_n \rangle$ элементов из A, т. е.

$$A^n = \{\langle x_1, \ldots, x_n \rangle \mid x_1 \in A, \ldots, x_n \in A\}.$$

При этом будем считать, что $A^1 = A$. Множество A^n называется n-кратным прямым произведением множества A или n-й степенью множества A. В частности, $A^2 = A \times A$ и $A^3 = A \times A \times A$.

ОПРЕДЕЛЕНИЕ. *Прямым произведением* n множеств $A_1, \ldots, A_n$ называется множество всех кортежей длины n $\langle x_1, \ldots, x_n \rangle$ таких, что $x_1 \in A_1, \ldots, x_n \in A_n$.

Прямое произведение множеств $A_1, \ldots, A_n$ обозначается символом $A_1 \times A_2 \times \ldots \times A_n$; таким образом,

$$A_1 \times \ldots \times A_n = \{\langle x_1, \ldots, x_n \rangle \mid x_1 \in A_1, \ldots, x_n \in A_n\}.$$

Бинарные отношения. Одним из основных является понятие бинарного отношения.

ОПРЕДЕЛЕНИЕ. *Бинарным отношением* называется любое множество упорядоченных пар.

Из определения следует, что бинарным отношением является любое подмножество прямого произведения двух множеств.

Если R — бинарное отношение и $\langle x, y \rangle \in R$, то говорят, что x и y *связаны отношением* R, или что *элемент* x *находится в отношении* R к y, или что для x и y *выполняется отношение* R. Вместо записи $\langle x, y \rangle \in R$ часто используют более простую

$$xRy,$$

которая также является записью утверждения «элементы x и y связаны отношением R».

ОПРЕДЕЛЕНИЕ. Множество всех первых элементов пар из R называется *областью определения отношения* R и обозначается $\mathrm{Dom}\,R$:

$$\mathrm{Dom}\,R = \{x \mid \exists y\,(\langle x,\ y\rangle \in R)\}.$$

Множество всех вторых элементов пар из R называется *областью значений отношения* R и обозначается $\mathrm{Im}\,R$:

$$\mathrm{Im}\,R = \{y \mid \exists x\,(\langle x,\ y\rangle \in R)\}.$$

ОПРЕДЕЛЕНИЕ. Множество $\mathrm{Dom}\,R \cup \mathrm{Im}\,R$ называется *областью отношения* R.

Легко видеть, что

$$R \subset \mathrm{Dom}\,R \times \mathrm{Im}\,R.$$

Если $R \subset A \times B$, то говорят, что R есть *отношение между элементами множеств* A и B или что R *определено на паре множеств* A и B. Если $A \subset C$ и $B \subset D$, то $R \subset C \times D$, т. е. R есть также отношение между элементами множеств C и D. Если $R \subset A \times B$, то $\mathrm{Dom}\,R \subset A$ и $\mathrm{Im}\,R \subset B$. Таким образом, каждое отношение R является отношением между элементами множеств $\mathrm{Dom}\,R$ и $\mathrm{Im}\,R$.

ОПРЕДЕЛЕНИЕ. Если $R \subset A \times A$, то говорят, что R есть *бинарное отношение* на множестве A.

Ясно, что каждое бинарное отношение R является отношением на области отношения R.

ОПРЕДЕЛЕНИЕ. Бинарные отношения R и S называются *равными*, если для любых x, y $\langle x,\ y\rangle \in R$ тогда и только тогда, когда $\langle x,\ y\rangle \in S$, т. е. если R и S равны как множества.

ОПРЕДЕЛЕНИЕ. Пусть R и S — бинарные отношения. Множество всех пар $\langle x,\ y\rangle$ таких, что для некоторого z $\langle x,\ z\rangle \in S$ и $\langle z,\ y\rangle \in R$, называется *композицией* (или *суперпозицией*) *отношений* S и R и обозначается через $R \cdot S$.

По определению, имеем

$$R \cdot S = \{\langle x,\ y\rangle \mid \exists z\,(xSz \wedge zRy)\}.$$

Пример. Если $S = \{\langle 1, 2\rangle, \langle 2, 4\rangle, \langle 3, 6\rangle\}$, $R = \{\langle 1, 3\rangle, \langle 2, 6\rangle, \langle 3, 9\rangle, \langle 4, 12\rangle\}$, то $R \cdot S = \{\langle 1, 6\rangle, \langle 2,12\rangle\}$.

ОПРЕДЕЛЕНИЕ. *Инверсией* бинарного отношения R называется множество всех упорядоченных пар $\langle x, y\rangle$ таких, что $\langle y,\ x\rangle \in R$.

Инверсия отношения R обозначается через $R^{\smile}$. Таким образом, по определению,

$$R^{\smile} = \{\langle x, y\rangle \mid \langle y, x\rangle \in R\}.$$

Пример. Если $R = \{\langle 2, 5\rangle, \langle 8, 15\rangle, \langle 4, 1\rangle\}$, то $R^{\smile} = \{\langle 5, 2\rangle, \langle 15, 8\rangle, \langle 1, 4\rangle\}$.

ПРЕДЛОЖЕНИЕ 2.1. *Если R — любое бинарное отношение*, то

(a) $\mathrm{Dom}\,(R^{\smile}) = \mathrm{Im}\,R$, (b) $\mathrm{Im}\,(R^{\smile}) = \mathrm{Dom}\,R$, (c) $(R^{\smile})^{\smile} = R$,

т. е. если $R^{\smile}$ — инверсия R, то R — инверсия $R^{\smile}$.

Это предложение непосредственно следует из определения инверсии $R^{\smile}$ отношения R.

ОПРЕДЕЛЕНИЕ. Отношение R называется *ограничением* отношения S, а S — *расширением* R, если $R \subset S$.

ОПРЕДЕЛЕНИЕ. Бинарное отношение R называется *ограничением отношения* S множеством A, если $R = (A \times A) \cap S$.

Если бинарное отношение R является ограничением отношения S множеством A, то R — ограничение S и $\mathrm{Dom}\,R \subset A$.

ТЕОРЕМА 2.2. *Композиция отношений обладает свойством ассоциативности, т. е. для любых бинарных отношений R, S, T*

(1) $(R \cdot S) \cdot T = R \cdot (S \cdot T)$.

Доказательство. Для любых x и y имеем

$$\begin{aligned} x(R \cdot S) \cdot Ty &\leftrightarrow \exists z\,(xTz \wedge zR \cdot Sy) \\ &\leftrightarrow \exists z\,\exists t\,(xTz \wedge zSt \wedge tRy) \\ &\leftrightarrow \exists t\,\exists z\,(xTz \wedge zSt \wedge tRy) \\ &\leftrightarrow \exists t\,[\exists z\,(xTz \wedge zSt) \wedge tRy] \\ &\leftrightarrow \exists t\,[xS \cdot Tt \wedge tRy] \\ &\leftrightarrow xR \cdot (S \cdot T)\,y. \end{aligned}$$

Следовательно, равенство (1) верно для любых бинарных отношений R, S и T. □

ТЕОРЕМА 2.3. *Для любых бинарных отношений R и S*

$(R \cdot S)^{\smile} = S^{\smile} \cdot R^{\smile}$.

Доказательство. Для любых x и y имеем

$$\begin{aligned} x(R \cdot S)^{\smile} y &\leftrightarrow yR \cdot Sx \\ &\leftrightarrow \exists z\,(ySz \wedge zRx) \\ &\leftrightarrow \exists z\,(xR^{\smile}z \wedge zS^{\smile}y) \\ &\leftrightarrow xS^{\smile} \cdot R^{\smile}y. \end{aligned}$$

Следовательно, $(R \circ S)^{\smile} = S^{\smile} \cdot R^{\smile}$ для любых бинарных отношений R и S. □

***n*-местные отношения.** Обобщением понятия бинарного отношения является понятие n-местного отношения.

ОПРЕДЕЛЕНИЕ. *n-местным отношением* ($n \geqslant 1$) называется любое множество кортежей длины n (т. е. любое множество упорядоченных наборов n объектов).

Таким образом, n-местным отношением является всякое подмножество прямого произведения n множеств.

Двухместное отношение называют также *бинарным отношением*, а трехместное — *тернарным отношением*. Тернарное отношение — это любое множество упорядоченных троек, т. е. всякое подмножество прямого произведения трех множеств.

ОПРЕДЕЛЕНИЕ. Пусть A^n есть n-я степень непустого множества A, $n \geqslant 1$. Любое подмножество множества A^n называется *n-местным отношением на множестве A*, а число n — *рангом отношения*.

В частности, одноместным отношением на A является любое подмножество множества A; трехместным (тернарным) отношением на A будет всякое подмножество множества A^3, т. е. любое множество упорядоченных троек элементов множества A.

Пусть $A(x_1, \ldots, x_n)$ — произвольный n-местный предикат со свободными переменными $x_1, \ldots, x_n$. С ним можно связать n-местное отношение

$$R = \{\langle x_1, \ldots, x_n\rangle \mid A(x_1, \ldots x_n)\}.$$

Отношение R называется *графиком предиката* $A(x_1, \ldots, x_n)$.

Представление бинарных отношений графами. *Графом* называется фигура на плоскости, состоящая из конечного числа точек — вершин графа — и линий, соединяющих некоторые из вершин. Линия, соединяющая какие-либо две вершины графа, называется *ребром* графа. Линии могут быть прямыми или кривыми. Точки пересечения некоторых ребер графа могут не являться вершинами графа. Граф, на котором указаны стрелками направления всех его ребер, называется *ориентированным*.

Существует простой способ представления бинарных отношений на конечных множествах ориентированными графами. Пусть A — непустое конечное множество и R — бинарное отношение на A, т. е. $R \subset A \times A$. Представим элементы множества A точками на плоскости. Каждой паре

$\langle a, b\rangle$ из R при $a \neq b$ поставим в соответствие ориентированное ребро (рис. 8), идущее от точки a к точке b. Паре $\langle a, a\rangle$ из R поставим в соответствие петлю (рис. 9) с фиксированным направлением обхода (например, всегда против часовой стрелки).

Рис. 8

Рис. 9

Таким образом, бинарному отношению R ставится в соответствие следующая геометрическая фигура: точки плоскости, представляющие элементы множества $\mathrm{Dom}\,R \cup \cup \mathrm{Im}\,R$, и ориентированные ребра — каждой паре $\langle a, b\rangle$ из R ставится в соответствие ориентированное ребро, идущее от точки a к точке b, или петля, если $a = b$. Такая геометрическая фигура называется *ориентированным графом отношения* R или просто *графом отношения* R.

Если в отношение R входит как пара $\langle a, b\rangle$, так и пара $\langle b, a\rangle$, то в графе отношения R есть два ребра, с вершинами a и b, ориентированные в противоположные стороны. В этом случае два ребра заменяются одним ребром с двумя стрелками (рис. 10).

Ребро с двумя стрелками называется *неориентированным*.

Рис. 10

Рис. 11

Каждое бинарное отношение на конечном множестве можно представить ориентированным графом. С другой стороны, *каждый ориентированный граф представляет бинарное отношение на множестве его вершин.*

Пример. На рис. 11 изображен граф отношения

$$R = \{\langle a, b\rangle, \langle b, c\rangle, \langle d, d\rangle, \langle e, a\rangle, \langle e, e\rangle\}.$$

Упражнения

1. Покажите, что для любых элементов a, b, c, d (не обязательно различных) $\{a, b\} = \{c, d\}$ тогда и только тогда, когда $a = c$ и $b = d$ или $a = d$ и $b = c$.

2. Покажите, что для любых элементов a, b, c, d $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ тогда и только тогда, когда $a=c$ и $b=d$.

Замечание. В силу этого упорядоченную пару $\langle a, b\rangle$ часто определяют в теоретико-множественных терминах как множество $\{\{a\}, \{a, b\}\}$.

3. Покажите, что $\langle\langle a, b\rangle, c\rangle = \langle\langle d, e\rangle, f\rangle$ тогда и только тогда, когда $a=d$, $b=e$, $c=f$.

4. Докажите, что для любых множеств A, B, C, D:

(a) $\mathrm{Dom}\,(A\times B)=A$;

(b) $\mathrm{Im}\,(A\times B)=B$;

(c) $(A\cap B)\times(C\cap D)=(A\times C)\cap(B\times D)$;

(d) $(A\cap B)\times C=(A\times C)\cap(B\times C)$;

(e) $A\times(B\cap C)=(A\times B)\cap(A\times C)$;

(f) $(B\cup C)\times A=(B\times A)\cup(C\times A)$;

(g) $(A\times B=\emptyset)\equiv(A=\emptyset\vee B=\emptyset)$;

(h) $(A\setminus B)\times C=(A\times C)\setminus(B\times C)$.

5. Покажите на примерах, что приведенные ниже равенства верны не для любых множеств A, B и C:

(a) $A\times B=B\times A$;

(b) $A\times(B\times C)=(A\times B)\times C$.

6. Докажите, что для любых бинарных отношений R, S, T:

(a) $(\mathrm{Dom}\,(R)=\emptyset)\equiv(R=\emptyset)\equiv(\mathrm{Im}\,(R)=\emptyset)$;

(b) $\mathrm{Dom}\,(R^{\smile})=\mathrm{Im}\,(R)$;

(c) $\mathrm{Im}\,(R^{\smile})=\mathrm{Dom}\,(R^{\smile})$;

(d) $(R^{\smile})^{\smile}=R$;

(e) $(R\circ S)^{\smile}=S^{\smile}\circ R^{\smile}$;

(f) $\mathrm{Dom}\,(R\circ S)\subset\mathrm{Dom}\,S$;

(g) $\mathrm{Im}\,(R\circ S)\subset\mathrm{Im}\,R$.

7. Покажите на примере, что композиция бинарных отношений не коммутативна.

8. Найдите $\mathrm{Dom}\,(R)$, $\mathrm{Im}\,(R)$, $R^{\smile}$, $R\circ R$, $R\circ R^{\smile}$, $R^{\smile}\circ R$ для следующих отношений:

(a) $R=\{\langle x, y\rangle \mid x, y\in\mathbf{N}$ и x делит $y\}$;

(b) $R=\{\langle x, y\rangle \mid x, y\in\mathbf{N}$ и y делит $x\}$;

(c) $R=\{\langle x, y\rangle \mid x, y\in\mathbf{Q}$ и $x+y\leqslant 0\}$, где $\mathbf{Q}$ — множество всех рациональных чисел;

(d) $R=\{\langle x, y\rangle \mid x, y\in\mathbf{Q}$ и $2x\leqslant 3y\}$.

§ 3. ФУНКЦИИ

Понятие функции (отображения). Одним из основных понятий математики является понятие функции.

ОПРЕДЕЛЕНИЕ. Бинарное отношение f называется *функцией* (*отображением*), если для любых x, y, z из того, что $\langle x, y\rangle\in f$ и $\langle x, z\rangle\in f$, следует, что $y=z$.

Другими словами, отношение f называется функцией, если для любого x из области определения отношения f существует единственное y такое, что $\langle x, y\rangle \in f$. Этот единственный элемент y обозначается через $f(x)$ и называется *значением функции* f для аргумента x. Если $\langle x, y\rangle \in f$, то используется общепринятая запись $y = f(x)$, а также запись

$$f : x \longmapsto y.$$

Областью определения функции f называется множество

$$\mathrm{Dom}\, f = \{x \mid \exists y\, (\langle x, y\rangle \in f)\}.$$

Областью значений функции f называется множество

$$\mathrm{Im}\, f = \{y \mid \exists x (\langle x, y\rangle \in f\}.$$

Две функции f и g называют *равными* (пишут $f = g$), если f и g равны как множества, т. е. для любых x, y $\langle x, y\rangle \in f$ тогда и только тогда, когда $\langle x, y\rangle \in g$. Следовательно, функции f и g равны тогда и только тогда, когда $\mathrm{Dom}\, f = \mathrm{Dom}\, g$ и $f(x) = g(x)$ для каждого x из $\mathrm{Dom}\, f$.

Функции называются также *отображениями*. Если функция f задана на паре множеств A и B, т. е. $f \subset A \times B$, то говорят, что f есть отображение из A в B. Если при этом $A = \mathrm{Dom}\, f$ и $\mathrm{Im}\, f \subset B$, то говорят, что f есть *отображение множества* A в B, и записывают в виде

$$f : A \to B \text{ или } A \xrightarrow[f]{} B.$$

Если $A = \mathrm{Dom}\, f$ и $B = \mathrm{Im}\, f$, то говорят, что f есть *отображение множества* A *на* B.

Множество всех отображений A в B обозначается символом B^A.

Образом множества C при отображении f называется множество

$$f(C) = \{f(x) \mid x \in C\}.$$

Легко показать, что для любого множества C и всякого отображения f

$$f(C) = f(C \cap \mathrm{Dom}\, f).$$

Прообразом множества M при отображении f называется множество

$$f^{\smile}(M) = \{x \in \mathrm{Dom}\, f \mid f(x) \in M\},$$

т. е. множество всех тех элементов x из области определения функции f, для которых $f(x) \in M$. Нетрудно проверить, что для любого множества M и любого отображения f имеем

$$f^{\smile}(M) = f^{\smile}(M \cap \operatorname{Im} f).$$

Мы видели, что бинарное отношение может быть задано как график некоторого двухместного условия (предиката). Функция также может быть задана при помощи двухместного условия. Пусть $A(x, y)$ — двухместное условие на x и y такое, что нет удовлетворяющих этому условию двух упорядоченных пар, которые имели бы одинаковые первые элементы и различные вторые элементы. Тогда график условия $A(x, y)$, т. е. множество $\{\langle x, y\rangle \mid A(x, y)\}$, является функцией.

Так, например, функция, определяемая условием $x^2 - y = 1$ на множестве $\mathbf{Z}$ целых чисел, может быть задана как множество

$$f = \{\langle x, y\rangle \mid x, y \in \mathbf{Z} \text{ и } x^2 - y = 1\},$$

или в виде

$$f = \{\langle x, y\rangle \mid x, y \in \mathbf{Z} \text{ и } y = x^2 - 1\},$$

или следующим образом:

$$f = \{\langle x, x^2 - 1\rangle \mid x, y \in \mathbf{Z}\}.$$

Функция, область определения которой состоит из упорядоченных пар, называется *функцией двух переменных*. Функция, область определения которой состоит из упорядоченных троек, называется *функцией трех переменных*. Если f — функция двух переменных, то обычно вместо $f(\langle x, y\rangle)$ пишут $f(x, y)$. Если f — функция трех переменных, то вместо $f(\langle x, y, z\rangle)$ пишут $f(x, y, z)$.

В общем случае функция, область определения которой состоит из кортежей длины n, называется *функцией n переменных*. Если f — функция n переменных, то вместо $f(\langle x_1, \ldots, x_n\rangle)$ пишут $f(x_1, \ldots, x_n)$.

Композиция функций. Рассмотрим свойства композиции функций. При этом композиция функций понимается как композиция отношений.

ТЕОРЕМА 3.1. *Пусть f и g — функции. Тогда их композиция $f \cdot g$ также есть функция такая, что*

(1) $\mathrm{Dom}\, f \cdot g = \{x \mid g(x) \in \mathrm{Dom}\, f\}$;

(2) $(f \cdot g)(x) = f(g(x))$ *для каждого* $x \in \mathrm{Dom}\,(f \cdot g)$;

(3) $f \cdot g = \{\langle x, f(g(x))\rangle \mid g(x) \in \mathrm{Dom}\ f\}$.

Доказательство. По определению композиции бинарных отношений $f \cdot g$ есть множество всех пар $\langle x, y\rangle$ таких, что для некоторого z выполняется одновременно $\langle x, z\rangle \in g$ и $\langle z, y\rangle \in f$, т. е.

$$f \cdot g = \{\langle x, y\rangle \mid \exists\ z(\langle x, z\rangle \in g \wedge \langle z, y\rangle \in f)\}.$$

Так как g — функция, то $\langle x, z\rangle \in g$ означает, что $x \in \mathrm{Dom}\, g$ и $z = g(x)$. Поскольку f — функция, вхождение $\langle z, y\rangle \in f$ означает, что

$$z = g(x) \in \mathrm{Dom}\ f \text{ и } y = f(z) = f(g(x)).$$

Следовательно,

$$f \cdot g = \{\langle x, y\rangle \mid \langle g(x), y\rangle \in f\};$$
$$\langle x, y\rangle \in f \cdot g \leftrightarrow y = f(g) \wedge (g(x) \in \mathrm{Dom}\, f);$$
$$f \cdot g = \{\langle x, f(g(x))\rangle \mid g(x) \in \mathrm{Dom}\ f\}.$$

Следовательно, $f \cdot g$ есть функция, для которой выполняются равенства (1), (2), (3). □

Следствие 3.2. *Пусть f, g — произвольные функции; тогда*

(a) $\mathrm{Dom}\,(f \cdot g) \subset \mathrm{Dom}\ g$, $\mathrm{Im}\,(f \cdot g) \subset \mathrm{Im}\, f$;

(b) *если* $\mathrm{Im}\, g \subset \mathrm{Dom}\, f$, то $\mathrm{Dom}\,(f \cdot g) = \mathrm{Dom}\, g$;

(c) *если* $\mathrm{Im}\, g = \mathrm{Dom}\, f$, то $\mathrm{Dom}\,(f \cdot g) = \mathrm{Dom}\, g$ и $\mathrm{Im}\,(f \cdot g) = \mathrm{Im}\, f$.

Теорема 3.3. *Если g — отображение множества A в B и f — отображение множества B в C, то $f \cdot g$ является отображением множества A в C.*

Доказательство. По условию, $\mathrm{Im}\, g \subset \mathrm{Dom}\, f = B$. По следствию 3.2, отсюда вытекает, что

$$\mathrm{Dom}\ f \cdot g = \mathrm{Dom}\ g = A,\ \mathrm{Im}\ f \cdot g \subset \mathrm{Im}\ f \subset C.$$

Следовательно, $f \cdot g$ является отображением множества A в C. □

ТЕОРЕМА 3.4. *Если g — отображение множества A на B и f — отображение множества B на C, то $f \cdot g$ является отображением множества A на C.*

Эта теорема непосредственно вытекает из теоремы 3.3 и следствия 3.2.

ТЕОРЕМА 3.5. *Композиция функций обладает свойством ассоциативности, т. е.* $f \cdot (g \cdot h) = (f \cdot g) \cdot h$ *для любых функций* f, g *и* h.

Теорема 3.5 непосредственно следует из теоремы 2.2.

ОПРЕДЕЛЕНИЕ. Отображение i_A множества A на себя такое, что $i_A(x) = x$ для каждого x *из* A, называется *тождественным* или *единичным отображением множества* A *на себя*.

ТЕОРЕМА 3.6. *Пусть* f *— отображение множества* A *на* B. *Тогда* $f \cdot f^{\smile} = i_B$.

Доказательство. Инверсия $f^{\smile}$ функции f есть бинарное отношение такое, что

$$f^{\smile} = \{\langle y, x\rangle | \langle x, y\rangle \in f\}.$$

По определению композиции отношений

$$(1)\quad f \cdot f^{\smile} = \{\langle y, z\rangle | \exists x (\langle y, x\rangle \in f^{\smile} \wedge \langle x, z\rangle \in f\}.$$

Из $\langle y, x\rangle \in f^{\smile}$ и $\langle x, z\rangle \in f$ следует

$$(2)\quad \langle x, y\rangle \in f \text{ и } \langle x, z\rangle \in f.$$

Так как f — функция, то из (2) следует равенство $y = z$. Поэтому (1) можно записать в виде

$$f \cdot f^{\smile} = \{\langle y, y\rangle | \exists x (\langle x, y\rangle \in f)\}.$$

Отсюда, поскольку f есть отображение A на B, получаем

$$f \cdot f^{\smile} = \{\langle y, y\rangle | y \in B\}.$$

Следовательно, $f \cdot f^{\smile} = i_B$. □

ТЕОРЕМА 3.7. *Пусть* f, g, h *— функции, удовлетворяющие условию*

$$(1)\quad \text{Dom } g = \text{Dom } h \subset \text{Im } f.$$

Тогда если $g \cdot f = h \cdot f$, *то* $g = h$.

Доказательство. Предположим, что

$$(2)\quad g \cdot f = h \cdot f.$$

В силу (1) для любого y из Dom g найдется элемент x такой, что $y = f(x)$. Отсюда в силу (2) следует, что

$$g(y) = g(f(x)) = h(f(x)) = h(y),$$

т. е. $g(y) = h(y)$ для любого y из Dom g. Кроме того, в силу (1) Dom g = Dom h. Следовательно, $g = h$. □

Инъективные функции. Среди функций, рассматриваемых в математике, большую роль играют инъективные функции.

ОПРЕДЕЛЕНИЕ. Функция f называется *инъективной,* если для любых x, y (из $\mathrm{Dom}\, f$) из условия $f(x) = f(y)$ следует, что $x = y$.

Другими словами, функция f инъективна, если для любых x, y, z из того, что $\langle x, z\rangle \in f$ и $\langle y, z\rangle \in f$, следует, что $x = y$.

В силу закона контрапозиции из определения следует, что *функция f инъективна тогда и только тогда, когда для любых x, y, если $x \neq y$, то $f(x) \neq f(y)$,* т. е. для различных аргументов функция f принимает различные значения.

ОПРЕДЕЛЕНИЕ. Инъективное отображение непустого множества A на себя называется *подстановкой множества A* или *преобразованием множества A.*

В частности, подстановкой является тождественное или единичное отображение i_A множества A на себя, т. е. такое отображение, что $i_A(x) = x$ для каждого x из A.

ПРЕДЛОЖЕНИЕ 3.8. *Если f — отображение из множества A в множество B, то $f \cdot i_A = f$, $i_B \cdot f = f$.* □

ТЕОРЕМА 3.9. *Композиция любых двух инъективных функций является инъективной функцией.*

Доказательство. Пусть f и g — инъективные функции. В силу инъективности f для любых x, y, если $f(g(x)) = f(g(y))$, то $g(x) = g(y)$. Далее, в силу инъективности g для любых x, y, если $g(x) = g(y)$, то $x = y$. Поэтому для любых x, y, если $f(g(x)) = f(g(y))$, то $x = y$. Следовательно, для любых x, y, если $(f \cdot g)(x) = (f \cdot g)(y)$, то $x = y$. Таким образом, функция $f \cdot g$ инъективна. □

СЛЕДСТВИЕ 3.10. *Композиция любых двух подстановок множества A есть подстановка множества A.*

Это следствие непосредственно вытекает из теорем 3.4 и 3.9.

Пусть f — функция. Инверсия $f^{\smile} = \{\langle x, y\rangle \mid \langle y, x\rangle \in f\}$ функции f может не быть функцией. Так, например, если дана функция $f = \{\langle x, x^2\rangle \mid x \in \mathbf{Z}\}$, где $\mathbf{Z}$ — множество всех целых чисел, то отношение $f^{\smile} = \{\langle x^2, x\rangle \mid x \in \mathbf{Z}\}$ не является функцией, так как содержит пары $\langle 1,1\rangle$ и $\langle 1, -1\rangle$ с одинаковыми первыми элементами и различными вторыми элементами.

Однако для функции $g = \{\langle x, 2x\rangle \mid x \in \mathbf{N}\}$, где $\mathbf{N}$ — множество всех целых неотрицательных чисел, инверсия $g^{\smile} = \{\langle 2x, x\rangle \mid x \in \mathbf{N}\}$ является функцией.

ПРЕДЛОЖЕНИЕ 3.11. *Если f и g — функции, то*

(a) $\mathrm{Dom}\, f^{\smile} = \mathrm{Im}\, f$; (c) $(f^{\smile})^{\smile} = f$;

(b) $\mathrm{Im}\, f^{\smile} = \mathrm{Dom}\, f$; (d) $(f \cdot g)^{\smile} = g^{\smile} \cdot f^{\smile}$.

Это предложение непосредственно следует из предложения 2.1 и теоремы 2.3.

СЛЕДСТВИЕ 3.12. *Если f — отображение множества A на B и $f^{\smile}$ — функция, то $f^{\smile}$ является отображением множества B на A.*

ТЕОРЕМА 3.13. *Инверсия $f^{\smile}$ функции f тогда и только тогда является функцией, когда функция f инъективна.*

Доказательство. Отношение $f^{\smile}$ является функцией тогда и только тогда, когда для любых x, y, z, если $\langle z, x\rangle \in f^{\smile}$ и $\langle z, y\rangle \in f^{\smile}$, то $x = y$. Это условие равносильно условию инъективности функции f:

для любых x, y, z, если $\langle x, z\rangle \in f$ и $\langle y, z\rangle \in f$, то $x = y$. Следовательно, отношение $f^{\smile}$ является функцией тогда и только тогда, когда функция f инъективна. □

СЛЕДСТВИЕ 3.14. *Если f — инъективная функция, то $f^{\smile}$ — тоже инъективная функция. При этом если f — инъективное отображение A на B, то $f^{\smile}$ есть инъективное отображение B на A.*

ТЕОРЕМА 3.15. *Пусть f, g, h — функции, удовлетворяющие условиям*:

(1) $f \cdot g = f \cdot h$;

(2) $\mathrm{Dom}\, g = \mathrm{Dom}\, h$, $\mathrm{Im}\, g \subset \mathrm{Dom}\, f$, $\mathrm{Im}\, h \subset \mathrm{Dom}\, f$.

Тогда если функция f инъективна, то $g = h$.

Доказательство. Предположим, что функция f инъективна. В силу условий (1) и (2)

$f(g(x)) = f(h(x))$ для любого x из $\mathrm{Dom}\, g$.

В силу инъективности f отсюда следует, что $g(x) = h(x)$ для любого x из $\mathrm{Dom}\, g$. Кроме того, ввиду (2) $\mathrm{Dom}\, g = \mathrm{Dom}\, h$. Следовательно, $g = h$. □

Обратимые функции. Пусть f — отображение множества A на B.

ОПРЕДЕЛЕНИЕ. Функция φ называется *левой обратной* к функции f, если φ — отображение B на A и $\varphi \cdot f = i_A$. Функция, обладающая левой обратной, называется *обратимой слева*.

ОПРЕДЕЛЕНИЕ. Функция h называется *правой обратной* к функции f, если h — отображение B на A и $f \cdot h = i_B$.

Функция, обладающая правой обратной, называется *обратимой справа*.

ОПРЕДЕЛЕНИЕ. Функция g называется *обратной* к функции f, если g — отображение B на A, $g \cdot f = i_A$ и $f \cdot g = i_B$. Функция, обладающая обратной, называется *обратимой*. Функция, обратная к функции f, обозначается символом f^{-1}.

Из определений следует: а) если φ — левая обратная к f функция, то функция f является правой обратной к φ; b) если h — правая обратная к f функция, то функция f является левой обратной к h; с) если функция g — обратная к f, то функция f является обратной к g; в этом случае функции f и g называются *взаимно обратными*.

ТЕОРЕМА 3.16. *Если f — инъективное отображение множества A на B, то $f^{\smile} \cdot f = i_A$, $f \cdot f^{\smile} = i_B$.*

Доказательство. Пусть f — инъективное отображение множества A на B. Тогда, по теореме 3.13, отношение $f^{\smile}$ является функцией и для любых x, y условие

(1) $f^{\smile}(y) = x$

равносильно условию

(2) $f(x) = y$.

В силу (2) и (1) для любого x из A имеем

$$f^{\smile}(f(x)) = x \text{ и } (f^{\smile} \cdot f)(x) = x,$$

т. е. $f^{\smile} \cdot f = i_A$. Далее, в силу (1) и (2) для любого y из B

$$f(f^{\smile}(y)) = y \text{ и } (f \cdot f^{\smile})(y) = y, \text{ т. е. } f \cdot f^{\smile} = i_B. \square$$

СЛЕДСТВИЕ 3.17. *Если f — инъективное отображение множества A на B, то f — обратимая функция, причем функция $f^{\smile}$ является обратной к f.*

СЛЕДСТВИЕ 3.18. *Если f — подстановка множества A, то $f^{\smile} \cdot f = i_A$ и $f \cdot f^{\smile} = i_A$.*

ТЕОРЕМА 3.19. *Пусть f — отображение множества A на B, обратимое слева. Любая левая обратная к f функция совпадает с $f^{\smile}$ и является также правой обратной к f и f обратима.*

Доказательство. Пусть $\varphi : B \to A$ есть левая обратная к f функция, т. е.

(1) $\varphi \cdot f = i_A$.

По теореме 3.6 и предложению 3.8,

(2) $f \cdot f^{\smile} = i_B$, $i_A \cdot f^{\smile} = f^{\smile}$, $\varphi \cdot i_B = \varphi$.

В силу (2) и (1)

$$\varphi = \varphi \cdot i_B = \varphi \cdot (f \cdot f^{\smile}) = (\varphi \cdot f) \cdot f^{\smile} = i_A \cdot f^{\smile} = f^{\smile},$$

следовательно, $\varphi = f^{\smile}$. Кроме того, $f \cdot \varphi = f \cdot f^{\smile} = i_B$, т. е. функция φ является также правой обратной к f и, следовательно, f обратима. □

ТЕОРЕМА 3.20. *Пусть f — отображение множества A на B, обратимое справа. Любая правая обратная к f функция совпадает с $f^{\smile}$ и является также левой обратной к f и f обратима.*

Доказательство. Пусть $h: B \to A$ есть правая обратная к f функция, т. е.

(1) $f \cdot h = i_B$.

По теореме 3.6 и предложению 3.8,

(2) $h \cdot h^{\smile} = i_A, \quad i_B \cdot h^{\smile} = h^{\smile}$.

В силу (2) и (1)

$$f = f \cdot i_A = f \cdot (h \cdot h^{\smile}) = (f \cdot h) \cdot h^{\smile} = i_B \cdot h^{\smile} = h^{\smile}.$$

По теореме 2.1, из $f = h^{\smile}$ следует $h = f^{\smile}$. Кроме того, $h \cdot f = f^{\smile} \cdot f = i_A$, т. е. функция h является также левой обратной к f и, следовательно, f обратима. □

ТЕОРЕМА 3.21. *Следующие свойства функции f равносильны*:

(a) *инверсия $f^{\smile}$ функции f является функцией*;
(b) *функция f инъективна*;
(c) *функция f обратима справа*;
(d) *функция f обратима слева*;
(e) *функции f обратима*;
(g) *все функции, обратные к f (левые, правые, двусторонние), существуют и совпадают с $f^{\smile}$.*

Доказательство. По теореме 3.13 свойства (a) и (b) равносильны.

Если f — инъективное отображение A на B, то по теореме 3.14 $f^{\smile}$ является отображением B на A и $f \cdot f^{\smile} = i_B$ — функция f обратима справа. Следовательно, из (b) следует (c).

Если функция f обратима справа, то, по теореме 3.20, она также обратима слева. Таким образом, из (c) следует (d). Если функция f обратима слева, то, по теореме 3.19, функция f обратима. Следовательно, из (d) следует (e).

Предположим, что функция f обратима. Тогда она обратима слева и справа. На основании теорем 3.19 и 3.20 все функции, обратные к f, совпадают с $f^{\smile}$.

Если выполняется условие (g), то инверсия $f^{\smile}$ функции f является функцией. Таким образом, из (g) следует (a).

Следовательно, свойства (a), (b), (c), (d), (e), (g) равносильны. □

ТЕОРЕМА 3.22. *Если функции f и g обратимы, то обратима также функция $f \cdot g$ и $(f \cdot g)^{-1} = g^{-1} \cdot f^{-1}$.*

Доказательство. Пусть f и g — обратимые функции. Тогда их инверсии $f^{\smile}$ и $g^{\smile}$ суть функции и

(1) $f^{\smile} = f^{-1}$, $g^{\smile} = g^{-1}$.

По теореме 2.3,

(2) $(f \cdot g)^{\smile} = g^{\smile} \cdot f^{\smile}$.

Так как $g^{\smile}$ и $f^{\smile}$ — функции, то их композиция $g^{\smile} \cdot f^{\smile}$ есть функция; следовательно, в силу (2) $(f \cdot g)^{\smile}$ является функцией. Поэтому функция $f \cdot g$ обратима и

(3) $(f \cdot g)^{\smile} = (f \cdot g)^{-1}$.

На основании равенств (1), (2), (3) заключаем, что функция $f \cdot g$ обратима и $(f \cdot g)^{-1} = g^{-1} \cdot f^{-1}$. □

Ограничение функции. Частным случаем ограничения бинарного отношения является ограничение функции.

ОПРЕДЕЛЕНИЕ. Функция g называется *ограничением* (или *сужением*) *функции* f, если $g \subset f$. Если $g \subset f$, то говорят также, что f есть *расширение* (или *продолжение*) *функции* g.

ОПРЕДЕЛЕНИЕ. Функция g называется *ограничением функции f множеством A* (или *сужением функции f на множество A*), если $g \subset f$ и $\mathrm{Dom}\, g = A$.

Ограничение функции f множеством A обозначается f_A или $f \mid A$.

ПРЕДЛОЖЕНИЕ 3.23. *Если $A \subset \mathrm{Dom}\, f$, то функция $f \cdot i_A$ является ограничением функции f множеством A*, т. е. $f_A = f \cdot i_A$.

Это предложение непосредственно следует из определения функции f_A.

ТЕОРЕМА 3.24. *Функция g является ограничением функции f тогда и только тогда, когда* $\mathrm{Dom}\, g \subset \mathrm{Dom}\, f$ *и $g(x) = f(x)$ для любого x* из $\mathrm{Dom}\, g$.

Доказательство. Предположим, что $g \subset f$. Тогда $\mathrm{Dom}\, g \subset \mathrm{Dom}\, f$ и для любого $x \in \mathrm{Dom}\, g$ из $\langle x, y \rangle \in g$ следует $\langle x, y \rangle \in f$, следовательно, $g(x) = f(x)$.

Теперь предположим, что $\mathrm{Dom}\, g \subset \mathrm{Dom}\, f$ и $g(x) = f(x)$ для любого $x \in \mathrm{Dom}\, g$. Тогда для любых x, y из $\langle x, y\rangle \in g$, т. е. из $y = g(x)$, следует, что $y = f(x)$ и $\langle x, y\rangle \in f$, следовательно, $g \subset f$. □

Упражнения

1. Какие из следующих отношений являются функциями? Укажите их области определения и области значений:

(a) $\{\langle x, y\rangle \mid x, y \in \mathbf{N} \text{ и } y = x^2\}$;

(b) $\{\langle x, y\rangle \mid x, y \in \mathbf{N} \text{ и } x < y \leqslant x+1\}$;

(c) $\{\langle x, y\rangle \mid x, y \in \mathbf{Z} \text{ и } y = x^2\}$;

(d) $\{\langle x, y\rangle \mid x, y \in \mathbf{N} \text{ и } x \text{ делит } y\}$;

(e) $\{\langle x, y\rangle \mid x, y \in \mathbf{Z} \text{ и } y = |x|\}$;

(f) $\{\langle x, y\rangle \mid x, y \in \mathbf{Z} \text{ и } x = y^2\}$.

Здесь и далее $\mathbf{Z}$ — множество всех целых чисел, $\mathbf{N}$ — множество всех целых неотрицательных чисел.

2. Пусть $A = \{0, 1\}$ — двухэлементное множество. Найдите все отображения множества A в себя и укажите, какие из них инъективны.

3. Найдите все отображения множества $A = \{0, 1, 2\}$ на множество $B = \{0, 1\}$.

4. Докажите, что для каждой функции f и любого множества A $f(A) = \emptyset$ тогда и только тогда, когда $A \cap \mathrm{Dom}\, f = \emptyset$.

5. Докажите, что если f есть такое отображение множества A на A, что $f \circ f = f$, то $f = i_A$.

6. Докажите, что если f — функция и A, B — множества, то $f(A \cap B) \subset f(A) \cap f(B)$. Покажите на примерах, что случай равенства $f(A \cap B) = f(A) \cap f(B)$ может не иметь места.

7. Пусть $R \subset A \times B$. Докажите, что R является отображением множества A в B тогда и только тогда, когда $R \circ R^{\smile} \subset i_B$ и $i_A \subset R^{\smile} \circ R$.

8. Докажите, что каждая из следующих функций имеет обратную. Найдите область определения обратной функции:

(a) $f = \{\langle x, y\rangle \mid x, y \in \mathbf{N} \text{ и } y = 2x+1\}$;

(b) $f = \{\langle n, n^2\rangle \mid n \in \mathbf{N}\}$;

(c) $f = \{\langle x, y\rangle \mid x, y \in \mathbf{N} \text{ и } y = x^3\}$.

9. Для любых множеств A, B и C докажите, что:
(a) существует инъективное отображение множества $A \times B$ на $B \times A$;
(b) существует инъективное отображение множества $(A \times B) \times C$ на $A \times (B \times C)$.

10. Пусть f — отображение множества A в A. Докажите, что если $f \circ f \circ f = i_A$, то f является инъективным отображением множества A на A.

11. Пусть f — отображение из множества A в B. Покажите, что если C, $D \subset B$ и $C \cap D = \emptyset$, то $f^{\smile}(A) \cap f^{\smile}(B) = \emptyset$.

12. Докажите, что для любой функции f выполняются соотношения:

(a) $f^{\smile}(A \cup B) = f^{\smile}(A) \cup f^{\smile}(B)$;

(b) $f^{\smile}(A \cap B) = f^{\smile}(A) \cap f^{\smile}(B)$;

(c) $f^{\smile}(A \setminus B) = f^{\smile}(A) \setminus f^{\smile}(B)$;

(d) $A \subset B \to f^{\smile}(A) \subset f^{\smile}(B)$.

13. Докажите, что если $A \subset \mathrm{Dom}\, f$ и $B \subset \mathrm{Im}\, f$, то

(a) $A \subset f^{\smile}(f(A))$; (b) $f(f^{\smile}(B)) = B$.

14. Докажите, что $f(A) \setminus f(B) \subset f(A \setminus B)$ для каждой функции f и любых множеств A и B. Если f — инъективная функция, то $f(A) \setminus f(B) = f(A \setminus B)$ для любых множеств A и B.

15. Пусть f — отображение множества A в B и g — отображение множества B в C. Докажите, что:

(a) если отображение $g \circ f$ инъективно, то и f инъективно; (b) если $g \circ f$ есть отображение A на C, то g есть отображение B на C.

16. Докажите, что отображение $f: A \to B$ является инъективным отображением множества A на B тогда и только тогда, когда существует отображение $g: B \to A$ такое, что $g \circ f = i_A$ и $f \circ g = i_B$.

17. Докажите, что бинарное отношение $R \subset A \times B$ является инъективным отображением множества A на B тогда и только тогда, когда $R \circ R^{\smile} = i_B$ и $R^{\smile} \circ R = i_A$.

18. Докажите, что функция f удовлетворяет условию $f(A \cap B) = f(A) \cap f(B)$ для любых множеств A и B тогда и только тогда, когда функция f инъективна.

19. Пусть A и B — конечные множества, состоящие из m и n элементов соответственно, и $m \leqslant n$. Докажите, что существует $n(n-1)\ldots(n-m+1)$ инъективных отображений множества A в B.

20. Пусть A и B — конечные множества, состоящие из m и n элементов соответственно.

(a) При каких m и n существует инъективное отображение множества A в B?

(b) Сколько существует отображений множества A в B?

(c) Сколько существует бинарных отношений между элементами множеств A и B?

§ 4. ОТНОШЕНИЕ ЭКВИВАЛЕНТНОСТИ

Некоторые виды бинарных отношений. По некоторым важным свойствам бинарные отношения делятся на виды.

ОПРЕДЕЛЕНИЕ. Бинарное отношение R на множестве A называется *рефлексивным* на A, если для каждого x из A xRx.

Отношение R рефлексивно на A тогда и только тогда, когда $i_A \subset R$, где $i_A = \{\langle x, x\rangle \mid x \in A\}$. Если отношение R рефлексивно, то каждая вершина его графа имеет петлю. Обратно: граф, каждая вершина которого имеет петлю, представляет некоторое рефлексивное отношение.

В качестве примеров рефлексивных отношений можно указать отношение параллельности на множестве прямых

плоскости, отношение равенства на каком-либо множестве чисел и отношение делимости на какой-либо совокупности целых чисел.

ОПРЕДЕЛЕНИЕ. Бинарное отношение R на множестве A называется *антирефлексивным* на A, если для каждого x из A $\langle x, x\rangle \notin R$, т. е. для каждого x из A не выполняется условие xRx.

Отношение R антирефлексивно на A тогда и только тогда, когда $i_A \cap R = \emptyset$. Если отношение R антирефлексивно, то ни одна вершина его графа не имеет петли. Обратно: если ни одна вершина графа не имеет петли, то граф представляет антирефлексивное отношение.

Например, отношение неравенства ($\neq$) на каком-нибудь множестве чисел и отношение перпендикулярности на множестве прямых плоскости являются антирефлексивными.

ОПРЕДЕЛЕНИЕ. Бинарное отношение R (на A) называется *транзитивным* (на A), если для любых x, y, z из области отношения R (из A) из xRy и yRz следует xRz.

Отношение R транзитивно тогда и только тогда, когда $R \cdot R \subset R$. Если отношение R транзитивно, то его граф обладает свойством: для каждой пары рёбер $\langle x, y\rangle$ и $\langle y, z\rangle$ имеется замыкающее ребро $\langle x, z\rangle$, и наоборот.

Например, отношение делимости на множестве целых чисел является транзитивным. Отношение неравенства ($\neq$) не является транзитивным.

ОПРЕДЕЛЕНИЕ. Бинарное отношение R (на A) называется *симметричным* (на A), если для любых x, y из области отношения R (из A) из xRy следует yRx.

Отношение R симметрично тогда и только тогда, когда $R^{\smile} = R$. Если отношение R симметрично, то каждое ребро его графа не ориентировано. Обратно: граф с неориентированными ребрами представляет некоторое симметричное бинарное отношение.

Например, симметричными являются отношение параллельности прямых, отношение перпендикулярности прямых и отношение равенства.

ОПРЕДЕЛЕНИЕ. Бинарное отношение R (на A) называется *антисимметричным* (на A), если для любых x, y из области отношения R (из A) из xRy и yRx следует $x = y$.

Отношение R антисимметрично на A тогда и только тогда, когда $R \cap R^{\smile} \subset i_A$. Граф антисимметричного отношения не имеет неориентированных ребер, но может иметь петли.

Например, отношение включения $\subset$ на какой-либо совокупности множеств является антисимметричным.

ОПРЕДЕЛЕНИЕ. Бинарное отношение R на множестве A называется *связанным на* A, если для любых элементов x, y множества A из $x \neq y$ следует $xRy \vee yRx$.

Отношение R связанно на A в том и только в том случае, когда $A \times A \setminus i_A \subset R \cup R^{\smile}$.

Бинарное отношение R на A связанно на A тогда и только тогда, когда для любых x, y из A *либо* $x = y$, *либо* xRy, *либо* yRx, т. е. $A \times A = i_A \cup R \cup R^{\smile}$.

Граф связанного отношения обладает следующим свойством: любые две (различные) вершины графа соединены ребром. Обратное также верно.

Так, например, обычное отношение «меньше» ($<$) на какой-либо совокупности чисел является связанным.

Отношение эквивалентности. Важным видом бинарного отношения является отношение эквивалентности.

ОПРЕДЕЛЕНИЕ. Бинарное отношение на множестве A называется *отношением эквивалентности* на A, если оно рефлексивно, симметрично и транзитивно (на A).

Отношение эквивалентности часто обозначают символами $\sim$, $\approx$ или $\equiv$.

Примеры. 1. Пусть A — непустое множество и $i_A = \{\langle x, x\rangle \mid x \in A\}$ — отношение тождества на множестве A. Отношение i_A есть отношение эквивалентности на A.

2. Пусть A — множество прямых на плоскости и

$$R = \{\langle x, y\rangle \mid x, y \in A \text{ и } x \text{ параллельно } y\}$$

— отношение параллельности. Отношение параллельности на A есть отношение эквивалентности.

3. Пусть $\mathbf{Z}$ — множество всех целых чисел и m — целое число, отличное от нуля. Отношение

$$R = \{\langle x, y\rangle \mid x, y \in \mathbf{Z} \text{ и } x - y \text{ делится на } m\}$$

называется *отношением сравнения по модулю* m. Это отношение является отношением эквивалентности на $\mathbf{Z}$.

4. Пусть A — множество направленных отрезков данной плоскости. Отношение эквиполентности направленных отрезков является отношением эквивалентности на A.

5. Отношение подобия на множестве треугольников данной плоскости есть отношение эквивалентности.

6. Два множества называются *равномощными*, если существует инъективное отображение одного множества на дру-

гое. Отношение равномощности на любой данной совокупности множеств является отношением эквивалентности.

ОПРЕДЕЛЕНИЕ. Пусть R — отношение эквивалентности на множестве A и $a \in A$. *Классом эквивалентности, порожденным элементом* a, называется множество $\{x \in A \mid xRa\}$, т. е. множество всех таких x из A, что $\langle x, a\rangle \in R$.

Класс эквивалентности, порожденный элементом a, обозначается через a/R или $[a]_R$. Совокупность всех классов эквивалентности отношения R на множестве A обозначается через A/R или $[A]_R$.

ОПРЕДЕЛЕНИЕ. Любой элемент класса эквивалентности называется представителем этого класса. *Полной системой представителей классов эквивалентности* называется множество представителей всех классов, по одному из каждого класса.

В примере 1 классами эквивалентности являются одноэлементные подмножества A. В примере 2 классы эквивалентности называются *пучками параллельных прямых.* В примере 3 классы эквивалентности называются *классами вычетов по модулю* m и каждый класс состоит из всех тех чисел, которые при делении на m дают один и тот же остаток. В примере 4 классы эквивалентности называются *векторами* плоскости. В примере 5 классы эквивалентности суть множества попарно подобных треугольников. В примере 6 классами эквивалентности являются классы равномощных множеств.

Фактор-множество. Пусть A — непустое множество.

ОПРЕДЕЛЕНИЕ. *Фактор-множеством множества* A *по отношению эквивалентности* R называется множество A/R всех классов эквивалентности.

ОПРЕДЕЛЕНИЕ. *Разбиением множества* A называется такое семейство его непустых подмножеств, что каждый элемент множества A входит в точности в один член семейства.

Другими словами, разбиение множества A есть семейство его непустых подмножеств, объединение которых совпадает с множеством A, а пересечение любых двух из них пусто.

ТЕОРЕМА 4.1. *Пусть* R *— отношение эквивалентности на (непустом) множестве* A. *Тогда фактор-множество* A/R *является разбиением множества* A.

Доказательство. Каждый элемент a множества A принадлежит классу эквивалентности a/R. Надо доказать, что каждый элемент множества A принадлежит в точности

одному члену семейства A/R. Для этого достаточно показать, что классы эквивалентности, имеющие хотя бы один общий элемент, совпадают. Пусть a/R и b/R — классы эквивалентности, имеющие общий элемент c, пусть x — любой элемент из a/R, тогда xRa, aRc, cRb и в силу транзитивности отношения R xRb. Таким образом, $a/R \subset b/R$. Аналогично доказывается, что $b/R \subset a/R$. Следовательно, $a/R = b/R$. Итак, установлено, что фактор-множество A/R является разбиением множества A. □

СЛЕДСТВИЕ 4.2. *Пусть R — отношение эквивалентности на множестве A, тогда*

(1) $a \in a/R$ *для любого* a *из* A;

(2) *для любых* a, b *из* A $a/R = b/R$ *тогда и только тогда, когда* aRb;

(3) $a/R \neq b/R$ *тогда и только тогда, когда* $a/R \cap b/R = \emptyset$;

(4) $A = \bigcup_{x \in A} x/R$.

Это следствие непосредственно вытекает из теоремы 4.1.

Пусть S — разбиение непустого множества A и R_S — бинарное отношение, определяемое следующим образом: $\langle x,y\rangle \in R_S$ тогда и только тогда, когда x и y принадлежат одному и тому же члену семейства S.

ТЕОРЕМА 4.3. *Отношение R_S, соответствующее разбиению S непустого множества A, является отношением эквивалентности на A, причем фактор-множество A/R_S совпадает с разбиением S.*

Доказательство теоремы не представляет трудности и предлагается читателю в качестве упражнения.

Отношение равнообразности отображения. Пусть f — отображение множества A в B. Рассмотрим бинарное отношение R на A такое, что xRy тогда и только тогда, когда $f(x) = f(y)$.

ОПРЕДЕЛЕНИЕ. *Пусть f — отображение множества A в B. Бинарное отношение R,*

$$R = \{\langle x,\ y\rangle \mid f(x) = f(y),\ x,\ y \in A\},$$

называется *отношением равнообразности отображения f.*

ТЕОРЕМА 4.4. *Пусть f — любое отображение и $A = \mathrm{Dom}\, f$. Отношение равнообразности отображения f является отношением эквивалентности на множестве A.*

Доказательство. Пусть R — отношение равнообразности отображения f. Отношение R рефлексивно на A, так как $f(x) = f(x)$ для любого x из A. Отношение R транзитивно, так как для любых x, y, z из $f(x) = f(y)$ и

$f(y)=f(z)$ следует $f(x)=f(z)$. Отношение R симметрично, так как для любых x, y из $f(x)=f(y)$ следует $f(y)=f(x)$. Следовательно, R является отношением эквивалентности на множестве A. □

Если $a \in A = \mathrm{Dom}\, f$, $f(a)=b$ и R — отношение равнообразности отображения f, то класс эквивалентности, порожденный элементом a, есть $f^{\smile}(b)$. Множество $\{f^{\smile}(x) \mid x \in \mathrm{Im}\, f\}$ является фактор-множеством множества A по отношению эквивалентности R, т. е. $A/R = \{f^{\smile}(x) \mid x \in \mathrm{Im}\, f\}$.

Любое отношение эквивалентности R_1 на множестве A можно рассматривать как отношение равнообразности некоторого отображения множества A. В самом деле, можно определить *естественное отображение множества A на фактор-множество A/R_1*, ставя в соответствие каждому x из A единственный класс эквивалентности x/R_1, содержащий x. Легко проверить, что отношение эквивалентности R_1 совпадает с отношением равнообразности естественного отображения множества A на A/R_1.

Упражнения

1. С точки зрения наличия свойств рефлексивности, антирефлексивности, симметричности, антисимметричности, транзитивности рассмотрите следующие отношения:

(a) $\{\langle x, y\rangle \mid x, y \in \mathbf{Z} \text{ и } x \leqslant y+1\}$, где $\mathbf{Z}$ — множество всех целых чисел;

(b) $\{\langle x, y\rangle \mid x, y \in \mathbf{Z} \text{ и } x^2=y^2\}$;

(c) $\{\langle x, y\rangle \mid x, y \in \mathbf{Z} \text{ и } |x|=|y|\}$;

(d) $\{X, Y \mid X, Y \subset \mathbf{Z} \text{ и } X \cap Y = \emptyset\}$;

(e) $\{\langle x, y\rangle \mid x, y \in \mathbf{N} \text{ и } x \text{ делит } y\}$ ($\mathbf{N}$ — множество всех целых неотрицательных чисел);

(f) $\{\langle x, y\rangle \mid x, y \in \mathbf{N} \text{ и } x < y\}$;

(g) $\{\langle x, y\rangle \mid x, y \in \mathbf{N} \text{ и } x+y=1\}$;

(h) $\{\langle x, y\rangle \mid x, y \in \mathbf{N} \text{ и } x \leqslant y\}$;

(i) $\{\langle x, y\rangle \mid x, y \in \mathbf{N} \text{ и } x \neq y\}$;

(k) $\{\langle x, y\rangle \mid x, y \in \mathbf{Z} \text{ и } x^2+x=y^2+y\}$;

(l) $\{\langle x, y\rangle \mid x, y \in \mathbf{Z} \text{ и } x^2+y^2=1\}$.

2. Приведите примеры бинарных отношений:

(a) рефлексивных и транзитивных, но не антисимметричных;

(b) транзитивных и симметричных, но не рефлексивных;

(c) рефлексивных и транзитивных, но не симметричных;

(d) рефлексивных и симметричных, но не транзитивных.

3. Пусть $R \subset A \times A$. Докажите, что:

(a) R рефлексивно на множестве A тогда и только тогда, когда $i_A \subset R$;

(b) R симметрично тогда и только тогда, когда $R^{\smile} \subset R$;

(c) R транзитивно тогда и только тогда, когда $R \cdot R \subset R$.

4. Докажите, что симметричное и антисимметричное бинарное отношение R является транзитивным.

5. Найдите все фактор-множества множества $\{1, 2, 3\}$.

6. Покажите, что множество $\{1\ 2, 3, 4\}$ имеет 15 различных фактор-множеств.

7. Докажите, что если R есть транзитивное и симметричное бинарное отношение на множестве A, где A — область отношения R, то R является эквивалентностью на A.

8. Докажите, что бинарное отношение R с областью определения $\mathrm{Dom}\ R = A$ тогда и только тогда является отношением эквивалентности на A, когда $R \circ R \subset R$ и $R^{\smile} = R$.

9. Докажите, что если R есть отношение эквивалентности на множестве A, то $R^{\smile}$ также есть отношение эквивалентности на A.

10. Докажите, что пересечение любой совокупности отношений эквивалентности на множестве A есть отношение эквивалентности на множестве A.

11. Докажите, что для любого непустого множества M существует инъективное отображение множества всех разбиений множества M на множество всех отношений эквивалентности на M.

12. Докажите, что фактор-множество $\mathbf{Z}/\mathrm{mod}\ m$ множества целых чисел $\mathbf{Z}$ по отношению сравнения по модулю m имеет ровно m элементов.

§ 5. ОТНОШЕНИЯ ПОРЯДКА

Отношения порядка. Пусть R — бинарное отношение на множестве A.

ОПРЕДЕЛЕНИЕ. Бинарное отношение R на множестве A называется *отношением порядка на A* или *порядком на A*, если оно транзитивно и антисимметрично.

ОПРЕДЕЛЕНИЕ. Отношение порядка R на множестве A называется *нестрогим*, если оно рефлексивно на A, т. е. $\langle x, x\rangle \in R$ для всякого x из A.

Отношение порядка R называют *строгим* (на A), если оно антирефлексивно на A, т. е. $\langle x, x\rangle \notin R$ для любого x из A. Однако из антирефлексивности транзитивного отношения R следует его антисимметричность. Поэтому можно дать следующее эквивалентное определение.

ОПРЕДЕЛЕНИЕ. Бинарное отношение R на множестве A называется *строгим порядком на A*, если оно транзитивно и антирефлексивно на A.

Примеры. 1. Пусть $P(M)$ — множество всех подмножеств множества M. Отношение включения $\subset$ на множестве $P(M)$ есть отношение нестрогого порядка.

2. Отношения $<$ и $\leqslant$ на множестве действительных чисел являются соответственно отношением строгого и нестрогого порядка.

3. Отношение делимости во множестве натуральных чисел есть отношение нестрогого порядка.

ОПРЕДЕЛЕНИЕ. Бинарное отношение R на множестве A называется *отношением предпорядка* или *предпорядком* на A, если оно рефлексивно на A и транзитивно.

Примеры. 1. Отношение делимости во множестве целых чисел не является порядком. Однако оно рефлексивно и транзитивно, значит является предпорядком.

2. Отношение $\models$ логического следования является предпорядком на множестве формул логики высказываний.

Линейный порядок. Важным частным случаем порядка является линейный порядок.

ОПРЕДЕЛЕНИЕ. Отношение порядка на множестве A называется *отношением линейного порядка* или *линейным порядком* на A, если оно связанно на A, т. е. для любых x, y из A

либо xRy, *либо* $x=y$, *либо* yRx.

Отношение порядка, не являющееся линейным, обычно называют *отношением частичного порядка* или *частичным порядком*.

Примеры. 1. Отношение «меньше» на множестве действительных чисел есть отношение линейного порядка.

2. Отношение порядка, принятое в словарях русского языка, называется *лексикографическим*. Лексикографический порядок на множестве слов русского языка есть линейный порядок.

3. Отношение включения $\subset$ на совокупности подмножеств данного множества M является частичным порядком, если M содержит не менее двух различных элементов.

Одно и то же множество можно линейно упорядочить различными отношениями порядка. Так, например, на непустом конечном множестве M, состоящем из n элементов, можно ввести $n!$ различных линейных порядков.

Упорядоченное множество. Пусть R — произвольное отношение порядка на непустом множестве A.

ОПРЕДЕЛЕНИЕ. *Упорядоченным множеством* называется пара $\langle A, R\rangle$, где A — непустое множество и R — отношение порядка на A. Если порядок R на A линейный, то пара $\langle A, R\rangle$ называется *линейно упорядоченным множеством*. Если порядок R на A частичный, то пара $\langle A, R\rangle$ называется *частично упорядоченным множеством*.

ОПРЕДЕЛЕНИЕ. Пусть $\langle A, \prec\rangle$ — упорядоченное множество. Элемент a из A называется *наименьшим* (*наибольшим*) *в* A, если $a \prec x$ ($x \prec a$) для любого элемента x из A, отличного от a.

Любое упорядоченное множество имеет не более одного наименьшего и не более одного наибольшего элемента.

ОПРЕДЕЛЕНИЕ. Пусть $\langle A, \prec\!\!\!\cdot \rangle$ — упорядоченное множество. Элемент a из A называется *минимальным* (*максимальным*) в A, если выполняется условие: для любого x из A, если $x \prec\!\!\!\cdot a$, то $x = a$ (если $a \prec\!\!\!\cdot x$, то $a = x$).

Упорядоченное множество может иметь несколько минимальных и максимальных элементов.

Пример. Пусть R — отношение делимости в множестве $\mathbf{N} \setminus \{0,1\}$ ($\mathbf{N}$ — множество натуральных чисел). В упорядоченном множестве $\langle \mathbf{N} \setminus \{0,1\}, R \rangle$ любое простое число является минимальным элементом.

В линейно упорядоченном множестве понятия наименьшего (наибольшего) и минимального (максимального) элементов совпадают.

ОПРЕДЕЛЕНИЕ. Линейно упорядоченное множество $\langle A, R \rangle$ называется *вполне упорядоченным множеством*, если каждое непустое подмножество множества A имеет наименьший элемент.

Примеры. 1. Если $<$ есть обычное отношение «меньше» на множестве $\mathbf{N}$ натуральных чисел, то $\langle \mathbf{N}, < \rangle$ является вполне упорядоченным множеством.

2. Пусть $<$ есть обычное отношение «меньше» на множестве $\mathbf{R}$ всех действительных чисел. Тогда линейно упорядоченное множество $\langle \mathbf{R}, < \rangle$ не является вполне упорядоченным множеством.

Упражнения

1. Докажите, что тождественное отображение i_A множества A есть отношение порядка на множестве A.

2. Покажите, что отношение

$$R = \{\langle x, y \rangle \mid x, y \in \mathbf{N} \text{ и } (x \text{ делит } y \text{ или } x < y)\}$$

есть линейный порядок на множестве $\mathbf{N}$ натуральных чисел.

3. Пусть $A = \{1, 2, 3, 4, 5, 6, 7\}$ и

$$R = \{\langle x, y \rangle \mid x, y \in A \text{ и } (x - y) \vdots 2\}.$$

Покажите, что R есть отношение порядка на A, найдите максимальные и минимальные элементы.

4. Пусть отношения $<$ и $\leqslant$ определяются на множестве $\mathbf{N}$ натуральных чисел обычным образом. Докажите, что $< \circ < \neq <$; $\leqslant \circ < = < = <$; $\leqslant \circ \geqslant = \mathbf{N} \times \mathbf{N}$.

5. Постройте линейный порядок на множестве $\mathbf{N} \times \mathbf{N}$.

6. Покажите, что конечное множество, состоящее из n элементов, можно линейно упорядочить $n!$ способами.

7. Покажите, что отношение включения $\subset$ не является линейным порядком на совокупности $P(A)$ всех подмножеств множества A, если A содержит не менее двух элементов.

8. Докажите, что любое вполне упорядоченное множество является линейно упорядоченным.

9. Докажите, что бинарное отношение R на множестве A является отношением нестрогого порядка тогда и только тогда, когда $R \circ R = R$ и $R \circ R^{\smile} = i_A$.

10. Докажите, что если R есть отношение порядка (линейного порядка), то обратное отношение $R^{\smile}$ также есть отношение порядка (линейного порядка).

11. Пусть $\leqslant$ есть отношение нестрогого порядка на множестве A. Докажите, что отношение $<$ антирефлексивно и транзитивно на A.

12. Пусть $<$ — бинарное отношение, антирефлексивное и транзитивное на множестве A. Докажите, что отношение $\leqslant$ такое, что $x \leqslant y \equiv (x < y) \vee (x = y)$, есть отношение нестрогого порядка на A.

13. Докажите, что для линейно упорядоченного множества понятия наибольшего (наименьшего) и максимального (минимального) элементов совпадают.

14. Докажите, что если R есть частичный (линейный, полный) порядок на множестве A и $B \subset A$, то $R \cap (B \times B)$ является частным (линейным, полным) порядком на множестве B.

15. Пусть R — отношение предпорядка на множестве A. Положим $a \sim b \equiv (\langle a, b\rangle \in R \wedge \langle b, a\rangle \in R)$. Докажите, что:

(a) если $a \sim c$, $b \sim d$, $\langle a, b\rangle \in R$, то $\langle c, d\rangle \in R$;

(b) $\sim$ есть отношение эквивалентности на A;

(c) R_1 есть отношение порядка на $A/\sim$, где

$R_1 = \{\langle a/\sim, b/\sim\rangle \mid \langle a, b\rangle \in R\}$.

Глава третья

АЛГЕБРЫ И АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ

§ 1. БИНАРНЫЕ ОПЕРАЦИИ

Бинарные и n-местные операции. Пусть A — непустое множество.

ОПРЕДЕЛЕНИЕ. *Бинарной операцией на множестве A называется отображение множества $A \times A$ в A.*

Обычное сложение и умножение целых чисел суть примеры бинарных операций на множестве целых чисел. Пусть $P(M)$ — множество всех подмножеств множества M; объединение $\bigcup$ и пересечение $\bigcap$ — примеры бинарных операций на множестве $P(M)$.

Пусть f — произвольная бинарная операция на множестве A. Если при отображении f элемент c соответствует паре $\langle a, b\rangle$, т. е. $\langle\langle a, b\rangle, c\rangle \in f$, то вместо записи

$$f(\langle a, b\rangle) = c \text{ или } f(a, b) = c$$

пишут также

$$afb = c \text{ или } \langle a, b\rangle \longmapsto c$$

и элемент c называют *композицией элементов a и b*.

ОПРЕДЕЛЕНИЕ. Пусть A^n есть n-я степень непустого множества A и $n \geqslant 1$. Отображение множества A^n в A называется *n-местной операцией на множестве A*, а число n — рангом операции. *Нульместной операцией на множестве A* называется выделение (фиксация) какого-нибудь элемента множества A, число 0 называется *рангом нульместной операции*.

ОПРЕДЕЛЕНИЕ. Отображение из множества A^n в A называется *частичной n-местной операцией на A*, если область определения отображения не совпадает с A^n.

Операции ранга 0, 1 и 2 называют также *нульарной (нульместной)*, *унарной* и *бинарной* соответственно. Унарную операцию называют также *оператором*.

Примеры. 1. Отображение, ставящее в соответствие каждому множеству A из $P(M)$ его дополнение $M \setminus A$, есть *унарная операция на множестве* $P(M)$.

2. В области натуральных чисел вычитание не всегда возможно. Поэтому вычитание на множестве натуральных чисел есть частичная бинарная операция.

3. Операция деления рациональных чисел есть частичная бинарная операция на множестве рациональных чисел.

4. Операция, ставящая в соответствие каждому кортежу n натуральных чисел наибольший общий делитель этих чисел, является n-местной операцией на множестве натуральных чисел.

Для обозначения n-местной операции обычно используют ту же форму записи, что и для произвольных отображений (функций). Если f есть n-местная операция на множестве A и

$$\langle\langle a_1, \ldots, a_n\rangle, a_{n+1}\rangle \in f,$$

то пишут $a_{n+1} = f(a_1, \ldots, a_n)$ и говорят, что a_{n+1}, — значение операции f для набора аргументов $a_1, \ldots, a_n$.

Виды бинарных операций. Пусть $\top$ и $\perp$ — произвольные бинарные операции на множестве A.

ОПРЕДЕЛЕНИЕ. Бинарная операция $\top$ называется *коммутативной*, если для любых a, b из A выполняется равенство $a \top b = b \top a$.

ОПРЕДЕЛЕНИЕ. Бинарная операция $\top$ называется *ассоциативной*, если для любых элементов a, b, c из A выполняется равенство $a \top (b \top c) = (a \top b) \top c$.

ОПРЕДЕЛЕНИЕ. Бинарная операция $\top$ называется *дистрибутивной относительно бинарной операции* $\perp$, если для любых a, b, c из A выполняются равенства

$$(a \perp b) \top c = (a \top c) \perp (b \top c) \quad \text{и} \quad c \top (a \perp b) = (c \top a) \perp (c \top b).$$

Если операция $\top$ ассоциативна, то можно опускать скобки и писать $a \top b \top c$ вместо $a \top (b \top c)$ или $(a \top b) \top c$.

Примеры. 1. Сложение и умножение рациональных чисел являются коммутативными и ассоциативными бинарными операциями.

2. Операция вычитания на множестве рациональных чисел не коммутативна и не ассоциативна.

3. Операции объединения и пересечения подмножеств множества M коммутативны и ассоциативны на множестве $P(M)$.

4. Композиция функций есть ассоциативная операция. Композиция функций не коммутативна: в общем случае равенство $f \circ g = g \circ f$ не выполняется.

5. На множестве $P(M)$ подмножеств некоторого множества операции объединения и пересечения взаимно дистрибутивны друг относительно друга.

6. Умножение целых чисел дистрибутивно относительно сложения. Однако сложение целых чисел не дистрибутивно относительно умножения, так как в общем случае равенство $a + bc = (a + b)(a + c)$ не выполняется.

Нейтральные элементы. Пусть $\top$ — бинарная операция на множестве A.

ОПРЕДЕЛЕНИЕ. Элемент e из A называется *левым нейтральным относительно операции* $\top$, если для любого a из A выполняется равенство $e \top a = a$. Элемент e из A называется *правым нейтральным относительно операции* $\top$, если для любого a из A имеем $a \top e = a$.

ОПРЕДЕЛЕНИЕ. Элемент e из A называется *нейтральным относительно операции* $\top$, если для любого элемента a из A верны равенства $e \top a = a = a \top e$.

ТЕОРЕМА 1.1. *Если нейтральный элемент относительно бинарной операции* $\top$ *существует, то он единствен.*

Доказательство. Пусть e и e' — нейтральные элементы относительно $\top$. Тогда $e' = e' \top e = e$, т. е. $e' = e$. □

СЛЕДСТВИЕ 1.2. *Если нейтральный элемент относительно операции* $\top$ *существует, то все левые и правые нейтральные элементы относительно* $\top$ *с ним совпадают.*

Примеры. 1. Число 0 есть нейтральный элемент относительно сложения целых чисел. Число 1 есть нейтральный элемент относительно умножения целых чисел.

2. Пустое множество есть нейтральный элемент относительно операции объединения множеств. Универсальное множество является нейтральным элементом относительно операции пересечения множеств.

3. Рассмотрим множество Φ отображений непустого множества A на его непустое собственное подмножество B и операцию — композицию отображений. Множество Φ не имеет ни одного правого нейтрального элемента. Всякий элемент $\varphi \in \Phi$ такой, что $\varphi(x) = x$ для любого x из B, является левым нейтральным элементом относительно рассматриваемой операции.

Регулярные элементы. Пусть $\top$ — бинарная операция на множестве A.

ОПРЕДЕЛЕНИЕ. Элемент $a \in A$ называется *регулярным справа относительно операции* $\top$, если для любых элементов b, c множества A из $a \top b = a \top c$ следует $b = c$. Элемент $a \in A$ называется *регулярным слева относительно* $\top$, если для любых элементов b, c множества A из $b \top a = c \top a$ следует $b = c$.

ОПРЕДЕЛЕНИЕ. Элемент $a \in A$ называется *регулярным относительно операции* $\top$, если он регулярен слева и справа относительно $\top$.

Таким образом, в случае регулярности элемента a в равенствах типа $a \top b = a \top c$ и $b \top a = c \top a$ возможно «сокращение» на a.

Примеры. 1. Всякое целое число регулярно относительно сложения.

2. Всякое целое число, отличное от нуля, регулярно относительно умножения; число нуль не регулярно относительно умножения.

ТЕОРЕМА 1.3. *Если элементы a и b регулярны относительно ассоциативной операции $\top$, то их композиция $a \top b$ также является регулярным элементом относительно* $\top$.

Доказательство. Пусть a и b — элементы, регулярные относительно $\top$. Пусть c, d — элементы из A, удовлетворяющие условию

(1) $(a \top b) \top c = (a \top b) \top d$.

Поскольку операция $\top$ ассоциативна, $a \top (b \top c) = a \top (b \top d)$. В силу регулярности элемента a имеем $b \top c = b \top d$. Отсюда в силу регулярности элемента b следует равенство

(2) $c = d$.

Итак, для любых элементов c, d множества A из (1) следует (2), следовательно, элемент $a \top b$ регулярен справа. Аналогично убеждаемся, что этот элемент регулярен слева. □

Симметричные элементы. Пусть $\top$ — бинарная операция на множестве A, обладающая нейтральным элементом e.

ОПРЕДЕЛЕНИЕ. Элемент u из A называется *левым симметричным к элементу* $a \in A$ относительно операции $\top$, если $u \top a = e$. Элемент v из A называется *правым симметричным к* a относительно операции $\top$, если $a \top v = e$.

ОПРЕДЕЛЕНИЕ. Элемент $a' \in A$ называется *симметричным к элементу* $a \in A$ относительно операции $\top$, если

$a \top a' = e = a' \top a$. В этом случае элемент a называется *симметризуемым*, а элементы a и a' — *взаимно симметричными*.

Примеры. 1. Относительно сложения целых чисел симметричным к данному целому числу является то же число, взятое со знаком минус.

2. Относительно умножения рациональных чисел симметричным к ненулевому числу a является $1/a$; число нуль не имеет симметричного относительно умножения.

ТЕОРЕМА 1.4. *Если операция* $\top$ *ассоциативна и элемент* a *симметризуем, то существует единственный элемент, симметричный к* a.

Доказательство. Пусть u, v — элементы, симметричные к элементу a относительно $\top$, т. е.

$$a \top u = e = u \top a, \quad a \top v = e = v \top a.$$

Тогда в силу ассоциативности $\top$

$$u = u \top e = u \top (a \top v) = (u \top a) \top v = e \top v = v,$$

т. е. $u = v$. □

СЛЕДСТВИЕ 1.5. *Если элемент* a *имеет симметричный элемент* a' *относительно ассоциативной операции* $\top$, *то все левые и все правые симметричные к* a *элементы совпадают с элементом* a'.

ТЕОРЕМА 1.6. *Если элементы* a, b *симметризуемы относительно ассоциативной операции* $\top$, *то элемент* $a \top b$ *также симметризуем и элемент* $b' \top a'$ *является симметричным к* $a \top b$.

Доказательство. Пусть a' и b' — элементы, симметричные к a и b соответственно. В силу ассоциативности $\top$

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

Также убеждаемся, что $(b' \top a') \top (a \top b) = e$. Следовательно, элемент $a \top b$ симметризуем и элемент $b' \top a'$ является симметричным к $a \top b$. □

ТЕОРЕМА 1.7. *Элемент, симметризуемый относительно ассоциативной операции* $\top$, *является регулярным относительно* $\top$.

Доказательство. Пусть a — симметризуемый элемент и для элементов b, c множества A верно равенство $a \top b = a \top c$. Тогда если a' — элемент, симметричный к a, то $a' \top (a \top b) = a' \top (a \top c)$. В силу ассоциативности операции $\top$ $(a' \top a) \top b = (a' \top a) \top c$. Следовательно, $e \top b = e \top c$

и $b=c$. Аналогично убеждаемся, что для любых элементов b, c множества A из равенства $b\top a=c\top a$ следует $b=c$. Таким образом, элемент a является регулярным относительно $\top$. □

Подмножества, замкнутые относительно операций. Пусть $\top$ — бинарная операция на множестве A и $B\subset A$.

ОПРЕДЕЛЕНИЕ. Подмножество B множества A называется *замкнутым относительно операции* $\top$, если для любых a, b из B элемент $a\top b$ принадлежит B.

Отметим, что пустое подмножество замкнуто относительно любой операции $\top$.

Примеры. 1. Множество всех четных чисел замкнуто относительно сложения и умножения целых чисел.

2. Множество всех нечетных чисел замкнуто относительно умножения, но не замкнуто относительно сложения целых чисел.

3. Множество всех элементов (из A), регулярных относительно ассоциативной операции $\top$, замкнуто относительно $\top$.

ПРЕДЛОЖЕНИЕ 1.8. *Множество всех элементов, симметризуемых относительно ассоциативной бинарной операции* $\top$, *замкнуто относительно* $\top$.

Доказательство этого предложения непосредственно вытекает из теоремы 1.6.

Пусть B — непустое множество, $B\subset A$, замкнутое относительно операции $\top$. Тогда на B можно определить бинарную операцию $\top'$ следующим образом:

$a\top' b=a\top b$ для любых a, b из B.

Операция $\top'$ называется *ограничением операции* $\top$ *множеством* B, а операция $\top$ — продолжением операции $\top'$ на множество A.

Аддитивная и мультипликативная формы записи. Наиболее часто используются аддитивная и мультипликативная формы записи бинарной операции. При аддитивной форме записи бинарную операцию $\top$ называют *сложением* и пишут $a+b$ вместо $a\top b$, называя элемент $a+b$ суммой a и b. Элемент, симметричный элементу a, обозначают $(-a)$ и называют *противоположным элементу* a. Нейтральный элемент относительно сложения обозначают символом 0 и называют *нулевым элементом* относительно сложения. При аддитивной записи свойства ассоциативности и коммутативности записываются в виде

$$a+(b+c)=(a+b)+c,\quad a+b=b+a.$$

При мультипликативной форме записи бинарную операцию называют *умножением* и пишут $a \cdot b$ (вместо $a \top b$), называя элемент $a \cdot b$ произведением a и b. Элемент, симметричный a, обозначают a^{-1} и называют *обратным элементу* a. Нейтральный элемент относительно умножения обозначают через e или 1 и называют *единичным элементом* или *единицей относительно умножения*. При мультипликативной записи свойства ассоциативности и коммутативности записываются в виде

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

Свойство дистрибутивности умножения относительно сложения записывается в виде

$$(a + b) \cdot c = a \cdot c + b \cdot c, \quad c(a + b) = c \cdot a + c \cdot b.$$

Конгруэнция. Пусть R — отношение эквивалентности на множестве A и $\top$ — бинарная операция на A.

ОПРЕДЕЛЕНИЕ. Отношение эквивалентности R называется *конгруэнцией относительно операции* $\top$, если для любых элементов a, b, c, d множества A из aRc и bRd следует $(a \top b) R (c \top d)$.

ТЕОРЕМА 1.9. *Пусть* $\top$ *— бинарная операция на множестве* A *и* R *— конгруэнция относительно* $\top$. *Тогда равенство*

(1) $(a/R) \top^* (b/R) = (a \top b)/R$,

где $a, b \in A$, *определяет бинарную операцию* $\top^*$ *на фактор-множестве* A/R.

Доказательство. Бинарное отношение $\top^*$ состоит из пар вида

(2) $\langle\langle a/R, b/R\rangle, (a \top b)/R\rangle$, где $a, b \in A$.

Надо доказать, что $\top^*$ — функция. Пусть

$$\langle\langle c/R, d/R\rangle, (c \top d)/R\rangle \in \top^*.$$

Надо показать, что из равенства

(3) $\langle a/R, b/R\rangle = \langle c/R, d/R\rangle$

следует $(a \top b)/R = (c \top d)/R$. Из (3) следуют равенства $a/R = c/R$, $b/R = d/R$ и соотношения

(4) aRc, bRd.

Так как R — конгруэнция относительно $\top$, то из (4) следует:

$$(a \top b) R (c \top d) \quad \text{и} \quad (a \top b)/R = (c \top d)/R.$$

Следовательно, отношение $\top^*$ является бинарной операцией на фактор-множестве A/R. □

ОПРЕДЕЛЕНИЕ. Бинарная операция $\top^*$, определенная на фактор-множестве A/R равенством (1), называется *операцией, ассоциированной с операцией* $\top$ *посредством конгруэнции* R.

Упражнения.

1. Пусть $\mathbf{N}^*$ — множество всех целых положительных чисел и $\top$ — операция на $\mathbf{N}^*$ возведения в степень, т. е. $a \top b = a^b$ для любых a, $b \in \mathbf{N}^*$. Покажите, что операция $\top$ не коммутативна и не ассоциативна.

2. Пусть a, b — фиксированные рациональные числа. Покажите, что отображение $\langle x, y\rangle \longmapsto ax + by$, где x, y — любые рациональные числа, является бинарной ассоциативной операцией на множестве рациональных чисел.

3. Пусть $\mathbf{N}$ — множество всех натуральных чисел и (x, y) — наибольший общий делитель натуральных чисел x и y. Докажите, что отображение $\langle x, y\rangle \longmapsto (x, y)$ является коммутативной и ассоциативной бинарной операцией на множестве $\mathbf{N}$.

4. Пусть $[x, y]$ — наименьшее общее кратное натуральных чисел x и y. Покажите, что отображение $\langle x, y\rangle \longmapsto [x, y]$ является коммутативной и ассоциативной операцией на множестве $\mathbf{N}$.

5. Пусть $P(U)$ — множество всех подмножеств непустого множества U. Множество $X \Delta Y$, определяемое формулой

$$X \Delta Y = (X \setminus Y) \cup (Y \setminus X),$$

называется *симметрической разностью множеств* X и Y. Докажите, что Δ есть коммутативная и ассоциативная бинарная операция на множестве $P(U)$. Покажите, что операция $\cap$ дистрибутивна относительно операции Δ.

6. Приведите пример множества A, отношения эквивалентности R на A и бинарной операции $\top$ на A таких, что

(a) R — конгруэнция относительно $\top$,

(b) R не является конгруэнцией относительно $\top$.

§ 2. АЛГЕБРЫ

Понятие алгебры. Дадим определение основного понятия курса алгебры.

ОПРЕДЕЛЕНИЕ. *Алгеброй* называется упорядоченная пара $\mathscr{A} = \langle A, \Omega\rangle$, где A — непустое множество и Ω — множество операций на A.

Таким образом, алгебра $\mathscr{A}$ определяется двумя множествами:

(a) непустым множеством A, обозначаемым также через $|\mathscr{A}|$; это множество называется *основным множеством алгебры* $\mathscr{A}$, а его элементы — *элементами алгебры* $\mathscr{A}$;

(b) множеством операций Ω, определенных на A и называемых *главными операциями алгебры* $\mathscr{A}$.

Если $\langle A, \Omega\rangle$ — алгебра, то говорят также, что множество A есть алгебра относительно операций Ω.

ОПРЕДЕЛЕНИЕ. Алгебры $\mathscr{A} = \langle A, \Omega\rangle$ и $\mathscr{B} = \langle B, \Omega'\rangle$ называются *однотипными*, если существует инъективное отображение множества Ω на Ω', при котором любая операция $f_{\mathscr{A}}$ из Ω и соответствующая ей при отображении операция $f_{\mathscr{B}}$ из Ω' имеют один и тот же ранг.

Наиболее частым является случай, когда множество Ω конечно, т. е. $\Omega = \{f_1, \ldots, f_s\}$. В этом случае вместо записи

$$\mathscr{A} = \langle A, \{f_1, \ldots, f_s\}\rangle$$

обычно употребляется запись

$$\mathscr{A} = \langle A, f_1, \ldots, f_s\rangle.$$

Если среди главных операций $f_1, \ldots, f_s$ алгебры есть нульместные, например $f_{r+1}, \ldots, f_s$, и $a_{r+1}, \ldots, a_s$ — элементы, которые они выделяют в $|\mathscr{A}|$, то употребляется также запись

$$\mathscr{A} = \langle A, f_1, \ldots, f_r, a_{r+1}, \ldots, a_s\rangle.$$

При этом выделенные элементы $a_{r+1}, \ldots, a_s$ — значения главных нульместных операций — называются *выделенными* или *главными элементами алгебры* $\mathscr{A}$.

Типом алгебры $\mathscr{A} = \langle A, f_1, \ldots, f_s\rangle$ называется последовательность $(r(f_1), \ldots, r(f_s))$, где $r(f_i)$ — *ранг операции* f_i. Алгебры $\mathscr{A}$ и $\mathscr{B} = \langle B, f'_1, \ldots, f'_s\rangle$ являются однотипными, если их типы совпадают, т. е. ранг операции f_i совпадает с рангом соответствующей операции f'_i для $i = 1, \ldots, s$.

Примеры. 1. Пусть $+$ и $\cdot$ (сложение и умножение) — арифметические операции на множестве $\mathbf{Z}$ целых чисел. Алгебра $\langle \mathbf{Z}, +, \cdot\rangle$ является алгеброй типа (2, 2).

2. Пусть $+$ и $\cdot$ суть арифметические операции на множестве $\mathbf{N}$ натуральных чисел. Алгебра $\langle \mathbf{N}, +, \cdot\rangle$ есть алгебра типа (2, 2).

3. Пусть $P(U)$ — множество всех подмножеств непустого множества U и $\cap$, $\cup$, $'$ суть операции пересечения, объединения и дополнения над подмножествами множества U. Алгебра $\langle P(U), \cap, \cup, '\rangle$ является алгеброй типа (2, 2, 1).

ОПРЕДЕЛЕНИЕ. Алгебра $\mathscr{A} = \langle A, *, e\rangle$ типа (2, 0), где A — произвольное непустое множество, $*$ — ассоциативная бинарная операция на A, e — нейтральный элемент относительно $*$, называется *моноидом*.

Пример. Пусть M — любое конечное непустое множество, A — множество всех отображений M в M, $*$ — опе-

рация композиции отображений M в M, i_M — тождественное отображение M в M. Тогда $\langle A, *, i_A\rangle$ — моноид.

Гомоморфизмы алгебр. Пусть $\mathscr{A}$ и $\mathscr{B}$ — однотипные алгебры, $f_{\mathscr{A}}$ — произвольная главная операция алгебры $\mathscr{A}$ и $f_{\mathscr{B}}$ — соответствующая ей главная операция алгебры $\mathscr{B}$. Говорят, что отображение h множества $|\mathscr{A}|$ в множество $|\mathscr{B}|$ сохраняет операцию $f_{\mathscr{A}}$ алгебры $\mathscr{A}$, если

(1) $h(f_{\mathscr{A}}(a_1, \ldots, a_m)) = f_{\mathscr{B}}(h(a_1), \ldots, h(a_m))$ для любых $a_1, \ldots, a_m$ из $|\mathscr{A}|$,

где m — ранг операции $f_{\mathscr{A}}$.

Отметим случай, когда $f_{\mathscr{A}}$ — нульместная операция, т. е. она выделяет какой-то элемент a алгебры $\mathscr{A}$. Тогда соответствующая ей операция $f_{\mathscr{B}}$ тоже будет нульместной и, значит, выделит какой-то элемент b алгебры $\mathscr{B}$. В этом случае условие (1) примет вид

$$h(a) = b,$$

т. е. выделенный элемент a алгебры $\mathscr{A}$ переходит при отображении h в соответствующий ему выделенный элемент b алгебры $\mathscr{B}$.

ОПРЕДЕЛЕНИЕ. *Гомоморфизмом алгебры* $\mathscr{A}$ в (на) однотипную алгебру $\mathscr{B}$ называется такое отображение h множества $|\mathscr{A}|$ в (на) $|\mathscr{B}|$, которое сохраняет все главные операции алгебры $\mathscr{A}$, т. е. удовлетворяет условию (1) для любой главной операции $f_{\mathscr{A}}$ алгебры $\mathscr{A}$. Гомоморфизм алгебры $\mathscr{A}$ на $\mathscr{B}$ называется *эпиморфизмом*.

ОПРЕДЕЛЕНИЕ. Гомоморфизм h алгебры $\mathscr{A}$ на алгебру $\mathscr{B}$ называется *изоморфизмом*, если h есть инъективное отображение множества $|\mathscr{A}|$ на $|\mathscr{B}|$. Алгебры $\mathscr{A}$ и $\mathscr{B}$ называются *изоморфными*, если существует изоморфизм алгебры $\mathscr{A}$ на $\mathscr{B}$.

Запись $\mathscr{A} \cong \mathscr{B}$ означает, что алгебры $\mathscr{A}$ и $\mathscr{B}$ изоморфны.

ОПРЕДЕЛЕНИЕ. Гомоморфизм h алгебры $\mathscr{A}$ в алгебру $\mathscr{B}$ называется *мономорфизмом* или *вложением*, если h является инъективным отображением множества $|\mathscr{A}|$ в $|\mathscr{B}|$.

ОПРЕДЕЛЕНИЕ. Гомоморфизм алгебры $\mathscr{A}$ в себя называется *эндоморфизмом алгебры* $\mathscr{A}$. Изоморфизм алгебры $\mathscr{A}$ на себя называется *автоморфизмом алгебры* $\mathscr{A}$.

Так, например, автоморфизмом алгебры $\mathscr{A}$ является тождественное отображение множества $|\mathscr{A}|$ на себя.

Пример. Пусть $+$ есть операция сложения на множестве $\mathbf{R}$ действительных чисел и $\cdot$ есть операция умно-

жения на множестве $\mathbf{R}^*$ положительных действительных чисел. Каждая из алгебр $\langle \mathbf{R}^*, \cdot, 1\rangle$ и $\langle \mathbf{R}, +, 0\rangle$ имеет тип $(2, 0)$. Покажем, что они изоморфны. Рассмотрим отображение h:

$$h(x) = \log x \quad \text{для любого } x \text{ из } \mathbf{R}^*.$$

Нетрудно видеть, что h есть отображение $\mathbf{R}^*$ на $\mathbf{R}$. Отображение h инъективно, так как для любых x, y из $\mathbf{R}^*$ выполняется условие: если $\log x = \log y$, то $x = y$. Кроме того, $h(1) = 0$ и для любых x, y из $\mathbf{R}^*$ имеем $\log(xy) = \log x + \log y$, т. е. $h(x, y) = h(x) + h(y)$. Таким образом, отображение h сохраняет главные операции алгебры $\langle \mathbf{R}^*, \cdot, 1\rangle$. Следовательно, h является изоморфизмом первой алгебры на вторую.

ТЕОРЕМА 2.1. *Пусть h — гомоморфизм алгебры $\mathscr{A}$ в алгебру $\mathscr{B}$ и g — гомоморфизм алгебры $\mathscr{B}$ в алгебру $\mathscr{C}$. Тогда их композиция $g \cdot h$ является гомоморфизмом алгебры $\mathscr{A}$ в алгебру $\mathscr{C}$.*

Доказательство. Пусть $f_{\mathscr{A}}$ — произвольная главная операция алгебры $\mathscr{A}$ (ранга $m > 0$), $f_{\mathscr{B}}$ — соответствующая ей главная операция алгебры $\mathscr{B}$ и $f_{\mathscr{C}}$ — главная операция алгебры $\mathscr{C}$, соответствующая операции $f_{\mathscr{B}}$. Надо доказать, что для любых элементов $a_1, \ldots, a_m$ из $|\mathscr{A}|$

$$(1)\quad g \cdot h(f_{\mathscr{A}}(a_1, \ldots, a_m)) = f_{\mathscr{C}}(g \cdot h(a_1), \ldots, g \cdot h(a_m)).$$

По определению композиции отображений

$$g \cdot h(f_{\mathscr{A}}(a_1, \ldots, a_m)) = g(h(f_{\mathscr{A}}(a_1, \ldots, a_m))).$$

Так как, по условию, h и g — гомоморфизмы, то

$$\begin{aligned} g(h(f_{\mathscr{A}}(a_1, \ldots, a_m))) &= g(f_{\mathscr{B}}(h(a_1), \ldots, h(a_m))) = \\ &= f_{\mathscr{C}}(g(h(a_1)), \ldots, g(h(a_m))) = \\ &= f_{\mathscr{C}}((g \cdot h)(a_1), \ldots, (g \cdot h)(a_m)). \end{aligned}$$

Следовательно, равенство (1) справедливо. Для нульместных главных операций рассуждения проводятся аналогично. □

ТЕОРЕМА 2.2. *Пусть h — гомоморфизм алгебры $\mathscr{A}$ на алгебру $\mathscr{B}$ и g — гомоморфизм алгебры $\mathscr{B}$ на алгебру $\mathscr{C}$. Тогда их композиция $g \cdot h$ является гомоморфизмом алгебры $\mathscr{A}$ на алгебру $\mathscr{C}$.*

Эта теорема непосредственно следует из теоремы 2.1 и теоремы 2.3.4.

ТЕОРЕМА 2.3. *Пусть h — изоморфизм алгебры $\mathscr{A}$ на алгебру $\mathscr{B}$ и g — изоморфизм алгебры $\mathscr{B}$ на алгебру $\mathscr{C}$. Тогда их композиция $g \cdot h$ является изоморфизмом алгебры $\mathscr{A}$ на алгебру $\mathscr{C}$.*

Доказательство. По теореме 2.1 из условия следует, что $g \cdot h$ есть гомоморфизм алгебры $\mathscr{A}$ в алгебру $\mathscr{C}$. Далее, по условию, h — инъективное отображение множества $|\mathscr{A}|$ на $|\mathscr{B}|$ и g — инъективное отображение множества $|\mathscr{B}|$ на $|\mathscr{C}|$. Согласно теоремам 2.3.9 и 2.3.4, отсюда следует, что $g \cdot h$ есть инъективное отображение множества $|\mathscr{A}|$ на $|\mathscr{C}|$. Следовательно, $g \cdot h$ является изоморфизмом алгебры $\mathscr{A}$ на алгебру $\mathscr{C}$. □

ТЕОРЕМА 2.4. *Пусть h — изоморфизм алгебры $\mathscr{A}$ на алгебру $\mathscr{B}$. Тогда отображение h^{-1} является изоморфизмом алгебры $\mathscr{B}$ на алгебру $\mathscr{A}$.*

Доказательство. По условию, h — инъективное отображение множества $|\mathscr{A}|$ на $|\mathscr{B}|$. Поэтому, по следствию 2.3.14, h^{-1} является инъективным отображением $|\mathscr{B}|$ на $|\mathscr{A}|$. Пусть $f_{\mathscr{A}}$ — произвольная главная операция алгебры $\mathscr{A}$ (ранга m) и $f_{\mathscr{B}}$ — соответствующая ей главная операция алгебры $\mathscr{B}$. Нам достаточно доказать, что для любых элементов $b_1, \ldots, b_m$ из $|\mathscr{B}|$

$$(1)\quad h^{-1}(f_{\mathscr{B}}(b_1, \ldots, b_m)) = f_{\mathscr{A}}(h^{-1}(b_1), \ldots, h^{-1}(b_m)).$$

Это условие равносильно следующему:

$$(2)\quad h(f_{\mathscr{A}}(h^{-1}(b_1), \ldots, h^{-1}(b_m)) = f_{\mathscr{B}}(b_1, \ldots, b_m).$$

Так как, по условию, h — гомоморфизм алгебры $\mathscr{A}$ на $\mathscr{B}$, то

$$h(f_{\mathscr{A}}(h^{-1}(b_1), \ldots, h^{-1}(b_m))) = \\ = f_{\mathscr{B}}(h(h^{-1}(b_1)), \ldots, h(h^{-1}(b_m))) = f_{\mathscr{B}}(b_1, \ldots, b_m),$$

т. е. выполняется (2) и, значит, (1). Следовательно, h^{-1} является изоморфизмом алгебры $\mathscr{B}$ на алгебру $\mathscr{A}$. □

ТЕОРЕМА 2.5. *Отношение изоморфизма на каком-либо множестве алгебр является отношением эквивалентности.*

Доказательство. Тождественное отображение алгебры $\mathscr{A}$ на $\mathscr{A}$, т. е. такое отображение h, что $h(a) = a$ для любого a из $|\mathscr{A}|$, очевидно, является изоморфизмом алгебры $\mathscr{A}$ на $\mathscr{A}$. По теореме 2.3, отношение изоморфизма обладает свойством транзитивности. По теореме 2.4, отношение изоморфизма обладает свойством симметричности. Следовательно, отношение изоморфизма является отношением эквивалентности. □

Подалгебры. Пусть f — n-местная операция на множестве A и B — непустое подмножество множества A. В соответствии с понятием ограничения функции множеством говорят, что n-местная операция g на B является ограничением операции f множеством B, если

$$g(b_1, \ldots, b_n) = f(b_1, \ldots, b_n) \text{ для любых } b_1, \ldots, b_n \text{ из } B.$$

В частности, нульместная операция g на B является ограничением нульместной операции f на A множеством B, если $g = f$, т. е. если g и f выделяют в B и A соответственно один и тот же элемент. Ограничение операции f множеством B будем обозначать символом $f|B$.

Пусть $\mathscr{A} = \langle A, \Omega \rangle$ и $\mathscr{B} = \langle B, \Omega' \rangle$ — однотипные алгебры.

ОПРЕДЕЛЕНИЕ. Алгебра $\mathscr{B}$ называется *подалгеброй* однотипной ей алгебры $\mathscr{A}$, если $B \subset A$ и тождественное отображение множества B в A является мономорфизмом алгебры $\mathscr{B}$ в алгебру $\mathscr{A}$, т. е. для каждой главной операции $f_{\mathscr{B}}$ алгебры $\mathscr{B}$

$$f_{\mathscr{B}}(b_1, \ldots, b_m) = f_{\mathscr{A}}(b_1, \ldots, b_m) \text{ для любых } b_1, \ldots, b_m \text{ из } B,$$

где m — ранг операции $f_{\mathscr{A}}$, а $f_{\mathscr{B}}$ — главная операция алгебры $\mathscr{B}$, соответствующая $f_{\mathscr{A}}$.

Напомним, что под тождественным отображением множества B в A понимается такое отображение h, что $h(b) = b$ для любого элемента b из B.

Легко показать, что данное выше определение подалгебры эквивалентно следующему. Алгебра $\mathscr{B}$ называется *подалгеброй* однотипной ей алгебры $\mathscr{A}$, если $B \subset A$ и каждая главная операция $f_{\mathscr{B}}$ алгебры $\mathscr{B}$ является ограничением соответствующей операции $f_{\mathscr{A}}$ алгебры $\mathscr{A}$ множеством B.

Запись $\mathscr{B} \rightarrowtail \mathscr{A}$ означает, что алгебра $\mathscr{B}$ есть подалгебра алгебры $\mathscr{A}$.

Пусть $\mathscr{A} = \langle A, \Omega \rangle$ — алгебра и $B \subset A$.

ОПРЕДЕЛЕНИЕ. Подмножество B множества $|\mathscr{A}|$ называется *замкнутым в алгебре* $\mathscr{A}$, если B замкнуто относительно каждой главной операции $f_{\mathscr{A}}$ алгебры $\mathscr{A}$, т. е.

(1) $f_{\mathscr{A}}(b_1, \ldots, b_m) \in B$ *для любых* $b_1, \ldots, b_m$ *из* B,

где m — ранг операции $f_{\mathscr{A}}$. Если $f_{\mathscr{A}}$ — нульместная операция, то условие (1) принимает вид $f_{\mathscr{A}} \in B$.

Очевидно, если $\mathscr{B} \rightarrowtail \mathscr{A}$, то множество $|\mathscr{B}|$ замкнуто в алгебре $\mathscr{A}$.

Из данных выше определений непосредственно вытекает следующая теорема.

ТЕОРЕМА 2.6. *Пусть* $\mathscr{A} = \langle A, f_1, \ldots, f_s \rangle$ *— алгебра и* B *— непустое подмножество множества* A*, замкнутое в алгебре* $\mathscr{A}$*. Тогда алгебра*

(2) $\mathscr{B} = \langle B, f_1 | B, \ldots, f_s | B \rangle$

является подалгеброй алгебры $\mathscr{A}$*.*

Поскольку замкнутое в алгебре $\mathscr{A}$ непустое подмножество B множества $|\mathscr{A}|$ однозначно (указанным выше образом) определяет подалгебру $\mathscr{B}$, то вместо записи (2) для этой подалгебры употребляют запись

$$\mathscr{B} = \langle B, f_1, \ldots, f_s \rangle.$$

Примеры. 1. Пусть $+$ и $\cdot$ (сложение и умножение) — обычные арифметические операции на множестве $\mathbf{Z}$ целых чисел и $\mathbf{N}$ — множество натуральных чисел. Тогда алгебра $\langle \mathbf{N}, +, \cdot \rangle$ является подалгеброй алгебры $\langle \mathbf{Z}, +, \cdot \rangle$.

2. Пусть $P(U)$ — множество всех подмножеств непустого множества U, а $\cap$, $\cup$ и $'$ суть соответственно операции пересечения, объединения и дополнения. Алгебра $\langle \{\emptyset, U\}, \cap, \cup, ' \rangle$ является подалгеброй алгебры $\langle P(U), \cap, \cup, ' \rangle$.

ТЕОРЕМА 2.7. *Если* $\mathscr{A}$ *— подалгебра алгебры* $\mathscr{B}$ *и* $\mathscr{B}$ *— подалгебра алгебры* $\mathscr{C}$*, то* $\mathscr{A}$ *является подалгеброй алгебры* $\mathscr{C}$*.*

Доказательство. Пусть $\mathscr{A} \rightarrowtail \mathscr{B}$. Тогда $|\mathscr{A}| \subset |\mathscr{B}|$ и

(1) $f_{\mathscr{A}}(a_1, \ldots, a_m) = f_{\mathscr{B}}(a_1, \ldots, a_m)$ для любых $a_1, \ldots, a_m$ из $|\mathscr{A}|$,

где $f_{\mathscr{A}}$ — произвольная главная операция алгебры $\mathscr{A}$ и m — ее ранг, а $f_{\mathscr{B}}$ — соответствующая ей операция алгебры $\mathscr{B}$. Далее, если $\mathscr{B} \rightarrowtail \mathscr{C}$, то $|\mathscr{B}| \subset |\mathscr{C}|$ и

(2) $f_{\mathscr{B}}(a_1, \ldots, a_m) = f_{\mathscr{C}}(a_1, \ldots, a_m)$ для любых $a_1, \ldots, a_m$ из $|\mathscr{B}|$,

где $f_{\mathscr{C}}$ — главная операция алгебры $\mathscr{C}$, соответствующая операции $f_{\mathscr{B}}$. Поэтому $|\mathscr{A}| \subset |\mathscr{C}|$ и в силу (1), (2)

$f_{\mathscr{A}}(a_1, \ldots, a_m) = f_{\mathscr{C}}(a_1, \ldots, a_m)$ для любых $a_1, \ldots, a_m$ из $|\mathscr{A}|$.

Следовательно, $\mathscr{A}$ является подалгеброй алгебры $\mathscr{C}$. □

ТЕОРЕМА 2.8. *Бинарное отношение* $\rightarrowtail$ (*«быть подалгеброй»*) *на множестве подалгебр алгебры* $\mathscr{A}$ *является отношением нестрогого порядка.*

Доказательство. Тождественное отображение множества $|\mathscr{A}|$ на $|\mathscr{A}|$ есть мономорфизм алгебры $\mathscr{A}$ на $\mathscr{A}$. Следовательно, $\mathscr{A} \rightarrowtail \mathscr{A}$, т. е. отношение $\rightarrowtail$ рефлексивно. В силу теоремы 2.7 отношение $\rightarrowtail$ транзитивно.

Покажем, что отношение $\rightarrowtail$ антисимметрично. Предположим, что подалгебры $\mathscr{B}$ и $\mathscr{C}$ алгебры $\mathscr{A}$ удовлетворяют условиям

(1) $\mathscr{B} \rightarrowtail \mathscr{C}$ и $\mathscr{C} \rightarrowtail \mathscr{B}$.

Тогда $|\mathscr{B}| \subset |\mathscr{C}|$, $|\mathscr{C}| \subset |\mathscr{B}|$ и, значит,

(2) $|\mathscr{B}| = |\mathscr{C}|$.

Далее, в силу (1) для произвольной главной операции $f_{\mathscr{B}}$ алгебры $\mathscr{B}$

(3) $f_{\mathscr{B}}(b_1, \ldots, b_m) = f_{\mathscr{C}}(b_1, \ldots, b_m)$ для любых $b_1, \ldots, b_m$ из $|\mathscr{B}|$, где m — ранг операции $f_{\mathscr{B}}$. В силу (2) и (3)

(4) $f_{\mathscr{B}} = f_{\mathscr{C}}$ для любой главной операции $f_{\mathscr{B}}$ алгебры $\mathscr{B}$.

На основании (2) и (4) заключаем, что $\mathscr{B} = \mathscr{C}$. Следовательно, отношение $\rightarrowtail$ антисимметрично.

Итак, установлено, что отношение $\rightarrowtail$ рефлексивно, транзитивно и антисимметрично, значит оно является отношением нестрогого порядка. □

ТЕОРЕМА 2.9. *Пересечение произвольной совокупности подмножеств множества* $|\mathscr{A}|$, *замкнутых в алгебре* $\mathscr{A}$, *является множеством, замкнутым в алгебре* $\mathscr{A}$.

Доказательство. Пусть $\{C_i \mid i \in I\}$ — произвольная совокупность подмножества C_i множества $|\mathscr{A}|$, замкнутых в алгебре $\mathscr{A}$, и $C = \bigcap\limits_{i \in I} C_i$. Если $C = \emptyset$, то теорема верна, так как пустое множество замкнуто в $\mathscr{A}$. Рассмотрим случай, когда $C \neq \emptyset$. Пусть $f_{\mathscr{A}}$ — произвольная главная операция алгебры $\mathscr{A}$, m — ее ранг и $c_1, \ldots, c_m$ — любые элементы множества C. Тогда

(1) $f_{\mathscr{A}}(c_1, \ldots, c_m) \in C_i$ для каждого i из I,

так как множество C_i замкнуто относительно операции $f_{\mathscr{A}}$. В силу (1)

$$f_{\mathscr{A}}(c_1, \ldots, c_m) \in \bigcap_{i \in I} C_i = C,$$

т. е. множество C замкнуто относительно всех главных операций алгебры $\mathscr{A}$. □

Пусть $\mathscr{A}$ — алгебра,

(I) $\{\mathscr{A}_i \mid i \in I\}$

— произвольная совокупность подалгебр $\mathscr{A}_i$ алгебры $\mathscr{A}$ такая, что $\bigcap\limits_{i \in I} |\mathscr{A}_i|$ — непустое множество.

ОПРЕДЕЛЕНИЕ. *Пересечением совокупности* (I) подалгебр алгебры $\mathscr{A}$ называется подалгебра $\mathscr{B}$ алгебры $\mathscr{A}$ такая, что $|\mathscr{B}| = \bigcap\limits_{i \in I} |\mathscr{A}_i|$.

Корректность данного определения следует из того, что (по теореме 2.9) множество $|\mathscr{B}| = \bigcap\limits_{i \in I} |\mathscr{A}_i|$ замкнуто в алгебре $\mathscr{A}$, а также из того, что непустое замкнутое в алгебре $\mathscr{A}$ подмножество $|\mathscr{B}|$ множества $|\mathscr{A}|$ (по теореме 2.6) однозначно определяет подалгебру алгебры $\mathscr{A}$ с основным множеством $|\mathscr{B}|$.

Запись $\mathscr{B} = \bigcap\limits_{i \in I} \mathscr{A}_i$ означает, что алгебра $\mathscr{B}$ есть пересечение совокупности (I) подалгебр $\mathscr{A}_i$ алгебры $\mathscr{A}$.

Итак, если (I) — произвольная совокупность подалгебр алгебры $\mathscr{A} = \langle A, f_1, \ldots, f_s \rangle$ такая, что $\bigcap\limits_{i \in I} |\mathscr{A}_i| \neq \emptyset$, то алгебра $\mathscr{B}$,

$$\mathscr{B} = \langle B, f_1 \mid B, \ldots, f_s \mid B \rangle,$$

где $B = \bigcap\limits_{i \in I} |\mathscr{A}_i|$, является пересечением алгебр совокупности (I).

ТЕОРЕМА 2.10. *Если в алгебре $\mathscr{A}$ среди главных операций есть хотя бы одна нульместная, то пересечение любой (непустой) совокупности подалгебр алгебры $\mathscr{A}$ является подалгеброй алгебры $\mathscr{A}$.*

Доказательство. Действительно, если $\{\mathscr{A}_i \mid i \in I\}$ — произвольная совокупность подалгебр алгебры $\mathscr{A}$, имеющей хотя бы одну нульместную главную операцию $f_{\mathscr{A}}$, то множество $B = \bigcap\limits_{i \in I} |\mathscr{A}_i|$ не пусто, так как оно содержит элемент, выделяемый операцией $f_{\mathscr{A}}$. Тогда множество B, замкнутое в $\mathscr{A}$ по теореме 2.9, однозначно определяет (по теореме 2.6) подалгебру алгебры $\mathscr{A}$ с основным множеством B. □

Из определения подалгебры следует, что для любого непустого множества M элементов данной алгебры $\mathscr{A}$, $M \subset |\mathscr{A}|$, существует наименьшая подалгебра $\mathscr{B}$, содержащая M.

Нетрудно видеть, что такой подалгеброй является пересечение всех подалгебр алгебры $\mathscr{A}$, содержащих множество M. Эта наименьшая подалгебра B называется *подалгеброй, порожденной множеством* M, а M — системой образующих для алгебры $\mathscr{B}$.

Фактор-алгебра. Пусть $\mathscr{A}$ — алгебра и R — отношение эквивалентности на множестве $|\mathscr{A}|$.

ОПРЕДЕЛЕНИЕ. Отношение R называется *конгруэнцией* или *отношением конгруэнтности в алгебре* $\mathscr{A}$, если R является конгруэнцией относительно каждой главной операции $f_{\mathscr{A}}$ алгебры $\mathscr{A}$, т. е. для любых элементов $a_1, b_1, \ldots, a_m, b_m$ множества $|\mathscr{A}|$ из

(1) $a_1 R b_1, \ldots, a_m R b_m$

следует

(2) $f_{\mathscr{A}}(a_1, \ldots, a_m) R f_{\mathscr{A}}(b_1, \ldots, b_m)$,

где m — ранг операции $f_{\mathscr{A}}$.

Пусть $\mathscr{A} = \langle A, \Omega\rangle$ — алгебра, R — конгруэнция в $\mathscr{A}$ и A/R — фактор-множество множества A по R. На множестве A/R определим m-местную операцию $f_{\mathscr{A}/R}$, соответствующую операции $f_{\mathscr{A}}$ из Ω, следующим образом:

(3) $f_{\mathscr{A}/R}(a_1/R, \ldots, a_m/R) = f_{\mathscr{A}}(a_1, \ldots, a_m)/R$
для любых $a_1, \ldots, a_m$ из A.

Это определение корректно, так как в силу (2) значение правой части (3) не зависит от выбора элементов $a_1, \ldots, a_m$ соответственно в классах эквивалентности $a_1/R, \ldots, a_m/R$ (см. доказательство теоремы 1.9). Операция $f_{\mathscr{A}/R}$ называется *операцией, ассоциированной с операцией* $f_{\mathscr{A}}$ посредством конгруэнции R. Обозначим через Ω^* множество всех операций, ассоциированных с главными операциями алгебры $\mathscr{A}$ посредством конгруэнции R, $\Omega^* = \{f_{\mathscr{A}/R} \mid f_{\mathscr{A}} \in \Omega\}$.

ОПРЕДЕЛЕНИЕ. Пусть $\mathscr{A} = \langle A, \Omega\rangle$ — алгебра и R — конгруэнция в $\mathscr{A}$. Алгебра $\langle A/R, \Omega^*\rangle$ называется *факторалгеброй* алгебры $\mathscr{A}$ по конгруэнции R и обозначается через $\mathscr{A}/R$.

ТЕОРЕМА 2.11. *Пусть R — конгруэнция в алгебре $\mathscr{A}$. Тогда отображение h множества $|\mathscr{A}|$ в $|\mathscr{A}|/R$ такое, что*

(1) $h(a) = a/R$ *для любого a из $|\mathscr{A}|$,*
является гомоморфизмом алгебры $\mathscr{A}$ на фактор-алгебру $\mathscr{A}/R$.

Доказательство. Из (1) следует, что h есть отображение $|\mathscr{A}|$ на $|\mathscr{A}|/R$. Надо показать, что h сохраняет все главные операции алгебры $\mathscr{A}$. Пусть $f_{\mathscr{A}}$ — произвольная главная операция алгебры $\mathscr{A}$ и $f_{\mathscr{A}/R}$ — ассоциированная с ней главная операция фактор-алгебры $\mathscr{A}/R$. Тогда в силу (1) для любых $a_1, \ldots, a_m$ из $|\mathscr{A}|$

$$\begin{aligned} h(f_{\mathscr{A}}(a_1, \ldots, a_m)) &= f_{\mathscr{A}}(a_1, \ldots, a_m)/R = \\ &= f_{\mathscr{A}/R}(a_1/R, \ldots, a_m/R) = \\ &= f_{\mathscr{A}/R}(h(a_1), \ldots, h(a_m)), \end{aligned}$$

где m — ранг операции $f_{\mathscr{A}}$. Следовательно, h является гомоморфизмом алгебры $\mathscr{A}$ на фактор-алгебру $\mathscr{A}/R$. □

Отметим, что гомоморфизм h, определяемый с помощью (1), называется *естественным гомоморфизмом* алгебры $\mathscr{A}$ на фактор-алгебру $\mathscr{A}/R$.

ТЕОРЕМА 2.12. *Пусть h — гомоморфизм алгебры $\mathscr{A}$ в алгебру $\mathscr{B}$ и R — такое бинарное отношение на $|\mathscr{A}|$, что для любых a, b из $|\mathscr{A}|$*

(1) *aRb тогда и только тогда, когда $h(a) = h(b)$.*

Тогда R является конгруэнцией в алгебре A.

Доказательство. Отношение R есть отношение равнообразности отображения h, и в силу теоремы 2.4.4 оно является отношением эквивалентности на $|\mathscr{A}|$.

Пусть $f_{\mathscr{A}}$ — произвольная главная операция (ранга m) алгебры $\mathscr{A}$ и $f_{\mathscr{B}}$ — соответствующая ей главная операция алгебры $\mathscr{B}$. В силу (1) для любых $a_1, b_1, \ldots, a_m, b_m$ множества $|\mathscr{A}|$ из

(2) $a_1Rb_1, \ldots, a_mRb_m$

следуют равенства

(3) $h(a_1) = h(b_1), \ldots, h(a_m) = h(b_m)$.

Предположим, что элементы $a_1, b_1, \ldots, a_m, b_m$ удовлетворяют условиям (2) и, следовательно, условиям (3). Тогда, поскольку h — гомоморфизм $\mathscr{A}$ в $\mathscr{B}$, имеем

$$\begin{aligned} h(f_{\mathscr{A}}(a_1, \ldots, a_m)) &= f_{\mathscr{B}}(h(a_1), \ldots, h(a_m)) = \\ &= f_{\mathscr{B}}(h(b_1), \ldots, h(b_m)) = \\ &= h(f_{\mathscr{A}}(b_1, \ldots, b_m)). \end{aligned}$$

Таким образом, из (2) следует равенство

$$h(f_{\mathscr{A}}(a_1, \ldots, a_m)) = h(f_{\mathscr{A}}(b_1, \ldots, b_m)).$$

Отсюда, по определению R, получаем

(4) $f_{\mathscr{A}}(a_1, \ldots, a_m) R f_{\mathscr{A}}(b_1, \ldots, b_m)$.

Итак, для любых элементов a_1, b_1, ..., a_m, b_m множества $|\mathscr{A}|$ из (2) следует (4). Следовательно, R является конгруэнцией в $\mathscr{A}$. □

Упражнения

1. Пусть $+$, $\cdot$ суть обычные операции сложения и умножения на множестве **N** натуральных чисел и h—отображение множества **N** в **N** такое, что $h(x)=2^x$ для всякого x из **N**. Докажите, что h является гомоморфизмом алгебры $\langle \mathbf{N}, + \rangle$ в алгебру $\langle \mathbf{N}, \cdot \rangle$.

2. Пусть $+$ и $\cdot$ суть обычные операции сложения и умножения на множестве **R** действительных чисел и a—фиксированное положительное действительное число. Пусть h—отображение **R** в **R** такое, что $h(x)=a^x$ для всякого x из **R**. Докажите, что h является гомоморфизмом алгебры $\langle \mathbf{R}, + \rangle$ в алгебру $\langle \mathbf{R}, \cdot \rangle$.

3. Пусть h—гомоморфизм алгебры $\langle A, f \rangle$ на алгебру $\langle B, g \rangle$, где f и g—бинарные операции. Докажите, что:

(a) если операция f коммутативна, то и операция g коммутативна;

(b) если операция f ассоциативна, то и операция g ассоциативна;

(c) если e—нейтральный элемент относительно операции f, то $f(e)$ является нейтральным элементом относительно операции g;

(d) если элемент x симметризуем относительно операции f, то элемент $f(x)$ симметризуем относительно операции g; если элементы x и x' взаимно симметричны относительно операции f, то элементы $f(x)$ и $f(x')$ взаимно симметричны относительно операции g.

4. Пусть **N**—множество натуральных чисел, $B=\{2^x \mid x \in \mathbf{N}\}$. Пусть h—отображение алгебры $\langle \mathbf{N}, + \rangle$ на алгебру $\langle B, \cdot \rangle$ такое, что для любого x из **N** верно равенство $h(x)=2^x$. Покажите, что h является изоморфизмом.

5. Пусть **R**—множество действительных чисел, $\mathbf{R}^{\ddagger}$—множество положительных действительных чисел, a—положительное действительное число, отличное от единицы. Пусть h—отображение алгебры $\langle \mathbf{R}, + \rangle$ в алгебру $\langle \mathbf{R}^{\ddagger}, \cdot \rangle$ такое, что $h(x)=a^x$ для каждого x из **R**. Докажите, что h является изоморфизмом.

6. Пусть f—мономорфизм алгебры $\mathscr{A}$ в $\mathscr{B}$ и g—мономорфизм алгебры $\mathscr{B}$ в алгебру $\mathscr{C}$. Докажите, что композиция $g \circ f$ является мономорфизмом алгебры $\mathscr{A}$ в алгебру $\mathscr{C}$.

7. Приведите пример алгебры $\mathscr{A}$ и отношения эквивалентности R на $|\mathscr{A}|$, которое не является конгруэнцией в алгебре $\mathscr{A}$.

8. Пусть h есть гомоморфизм алгебры $\mathscr{A}$ в алгебру $\mathscr{B}$. Докажите, что множество $\mathrm{Im}\,|\mathscr{A}|$ (гомоморфный образ основного множества алгебры $\mathscr{A}$) замкнуто в алгебре $\mathscr{B}$.

9. Пусть h—гомоморфизм алгебры $\mathscr{A}$ в алгебру $\mathscr{B}$. Докажите, что алгебра

$$\langle \mathscr{C}, f_1 \mid \mathscr{C}, \ldots, f_s \mid \mathscr{C} \rangle,$$

где $\mathscr{C}=\mathrm{Im}\,|\mathscr{A}|$, является подалгеброй алгебры $\mathscr{B}=\langle \mathscr{B}, f_1, \ldots, f_s \rangle$. Эту алгебру называют *гомоморфным образом* алгебры $\mathscr{A}$ при гомоморфизме h.

10. Пусть h—гомоморфизм алгебры $\mathscr{A}$ в алгебру $\mathscr{B}$. Докажите, что гомоморфный образ алгебры $\mathscr{A}$ при этом гомоморфизме изомор-

фен фактор-алгебре $\mathscr{A}/R$, где R — конгруэнция, порожденная гомоморфизмом h.

11. Докажите, что всякий гомоморфизм h алгебры $\mathscr{A}$ на алгебру $\mathscr{B}$ есть композиция естественного гомоморфизма алгебры $\mathscr{A}$ на свою фактор-алгебру и изоморфизма этой фактор-алгебры на алгебру $\mathscr{B}$.

§ 3. ГРУППЫ

Понятие группы. Одним из частных случаев алгебр являются группы, которые играют большую роль в математике и ее приложениях.

ОПРЕДЕЛЕНИЕ. Алгебра $\mathscr{G} = \langle G, *, ' \rangle$ типа (2, 1) называется *группой*, если ее главные операции удовлетворяют условиям (аксиомам):

(1) бинарная операция $*$ ассоциативна, т. е. для любых элементов a, b, c из G $a*(b*c) = (a*b)*c$;

(2) в G имеется правый нейтральный элемент относительно операции $*$, т. е. такой элемент e, что $a*e = a$ для всякого элемента a из G;

(3) для любого элемента a из G $a*a' = e$.

Таким образом, группа — это непустое множество с двумя операциями на нем — бинарной операцией $*$ и унарной операцией $'$, причем бинарная операция ассоциативна и обладает правым нейтральным элементом, а унарная операция есть операция перехода к правому симметричному элементу относительно бинарной операции и, значит, каждый элемент группы имеет правый симметричный ему элемент относительно бинарной операции группы $*$.

ОПРЕДЕЛЕНИЕ. Группа $\mathscr{G} = \langle G, *, ' \rangle$ называется *абелевой* или *коммутативной*, если бинарная операция группы $*$ коммутативна, т. е. для любых a, b из G $a*b = b*a$.

ОПРЕДЕЛЕНИЕ. *Порядком группы* $\mathscr{G} = \langle G, *, ' \rangle$ называется число элементов основного множества G группы, если G конечно. Если G — бесконечное множество, то группу $\mathscr{G}$ называют *группой бесконечного порядка*.

При изучении групп обычно используется мультипликативная или аддитивная форма записи главных операций группы. При *мультипликативной записи* бинарную операцию группы называют *умножением* и пишут $a \cdot b$ (или ab) вместо $a*b$, называя элемент $a \cdot b$ *произведением элементов* a и b. Элемент, симметричный a, обозначают a^{-1} и называют *обратным элементу* a. Нейтральный элемент относительно умножения обозначают через e, 1 или $1_{\mathscr{G}}$ и назы-

вают *единичным элементом* или *единицей группы*. При мультипликативной записи приведенное выше определение группы формулируется следующим образом.

Алгебра $\mathfrak{G} = \langle G, \cdot, {}^{-1} \rangle$ типа (2, 1) называется *группой*, если ее главные операции удовлетворяют условиям:

(1) бинарная операция $\cdot$ ассоциативна, т. е. для любых элементов a, b, c из G верно равенство $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

(2) в G имеется правая единица, т. е. такой элемент e, что $a \cdot e = a$ для всякого элемента a из G;

(3) для любого элемента a из G выполняется равенство $a \cdot a^{-1} = e$.

Понятие натуральной степени a^n элемента a мультипликативной группы $\langle G, \cdot, {}^{-1} \rangle$ определяется следующим образом:

$$a^0 = e, \quad a^n = a \cdot a \ldots a \quad \text{для} \quad n \in \mathbf{N} \setminus \{0\}.$$

При *аддитивной записи* бинарную операцию группы называют *сложением* и пишут $a + b$ вместо $a * b$, называя элемент $a + b$ *суммой элементов* a и b. Элемент, симметричный элементу a, обозначают $(-a)$ и называют *противоположным элементу* a. Нейтральный элемент относительно сложения обозначают символом 0 или $0_{\mathfrak{G}}$ и называют *нулевым элементом* или *нулем группы*. При аддитивной записи определение группы формулируется следующим образом.

Алгебра $\mathfrak{G} = \langle G, +, - \rangle$ типа (2, 1) называется *группой*, если ее главные операции удовлетворяют условиям:

(1) бинарная операция $+$ ассоциативна, т. е. для любых элементов a, b, c из G имеем $a + (b + c) = (a + b) + c$;

(2) в G имеется правый нуль, т. е. такой элемент 0, что $a + 0 = a$ для всякого элемента a из G;

(3) для любого элемента a из G $a + (-a) = 0$.

Примеры групп. 1. Пусть $\mathbf{Q}$ — множество всех рациональных чисел с обычным сложением и унарной операцией —, операцией перехода от числа a к противоположному числу $(-a)$. Алгебра $\mathfrak{Q} = \langle \mathbf{Q}, +, - \rangle$ типа (2, 1) является группой. Она называется *аддитивной группой рациональных чисел*.

2. Пусть $\mathbf{Q}^*$ — множество всех отличных от нуля рациональных чисел с обычным умножением и унарной операцией $^{-1}$ — операцией перехода от числа a к обратному числу a^{-1}. Алгебра $\mathfrak{Q}^* = \langle \mathbf{Q}^*, \cdot, {}^{-1} \rangle$ является группой. Эта группа называется *мультипликативной группой рациональных чисел*.

3. Пусть $\mathbf{R}$ — множество всех действительных чисел с обычным сложением и унарной операцией —, ставящей в соответствие каждому действительному числу r противоположное число $-r$. Алгебра $\mathscr{R}_+ = \langle \mathbf{R}, +, - \rangle$ является группой. Она называется *аддитивной группой действительных чисел.*

4. Пусть $\mathbf{R}^*$ — множество всех отличных от нуля действительных чисел с обычным умножением и унарной операцией $^{-1}$, ставящей в соответствие каждому отличному от нуля числу r обратное число r^{-1}. Алгебра $\mathscr{R}^* = \langle \mathbf{R}^*, \cdot, ^{-1} \rangle$ является группой. Эта группа называется *мультипликативной группой действительных чисел.*

5. Пусть S_n — совокупность всех подстановок множества $M = \{1, \ldots, n\}$, т. е. совокупность инъективных отображений этого множества на себя. Пусть $\mathscr{S}_n = \langle S_n, \cdot, ^{-1} \rangle$ — алгебра с бинарной операцией $\cdot$ — композицией отображений, и унарной операцией $^{-1}$, ставящей в соответствие функции f из S_n обратную ей функцию f^{-1}. Эта алгебра является группой. В самом деле, по теореме 2.3.10, композиция любых двух подстановок множества M есть подстановка этого множества. По теореме 2.3.5, композиция подстановок ассоциативна. Тождественная подстановка i_M есть нейтральный элемент относительно композиции подстановок. Для любой подстановки f множества M $f \cdot f^{-1} = i_M$. Эта группа называется *симметрической группой подстановок степени* n; она имеет порядок $n!$ и не коммутативна при $n > 2$.

6. Пусть G — множество всех векторов данной плоскости с обычной операцией $+$ сложения векторов и унарной операцией —, ставящей в соответствие каждому вектору v противоположный вектор $(-v)$. Алгебра $\langle G, +, - \rangle$ является группой. Эта группа называется *аддитивной группой векторов плоскости.*

7. Пусть G — множество всех вращений плоскости вокруг данной точки O. Вращение плоскости рассматривается как преобразование плоскости, т. е. инъективное отображение плоскости на себя. Два вращения на углы α и β рассматриваются как совпадающие, если $\alpha - \beta = 2n\pi$, где n — целое число. Композиция $\varphi \cdot \psi$ двух вращений ψ и φ соответственно на углы α и β есть вращение на угол $\alpha + \beta$. Если ψ — вращение на угол α, то ψ^{-1} — вращение на угол $(-\alpha)$. Алгебра $\langle G, \cdot, ^{-1} \rangle$ является группой. Она называется *группой вращений плоскости* вокруг данной точки.

8. Пусть H_n — множество, состоящее из n вращений данной плоскости на углы $2k\pi/n$, $k=0, 1, \ldots, n-1$, вокруг данной точки O, отображающих правильный n-угольник с центром в точке O на себя. Алгебра $\langle H_n, \cdot, {}^{-1}\rangle$ является группой. Она называется *группой вращений правильного n-угольника.*

9. Пусть G — множество всех вращений пространства вокруг точки O, отображающих данное правильное тело (тетраэдр, куб, икосаэдр, додекаэдр) с центром в точке O на себя. Алгебра $\langle G, \cdot, {}^{-1}\rangle$ является группой. Она называется *группой вращений* (*самосовмещений*) данного правильного тела.

Простейшие свойства группы. Ниже используется мультипликативная форма записи операций группы.

СВОЙСТВО 3.1. *Для любого элемента a группы $a^{-1}a=e$, т. е. правый обратный к a элемент является также левым обратным.*

Доказательство. Из второй и третьей аксиом группы следует, что

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

В силу аксиом группы отсюда вытекают равенства

$$a^{-1}a=(a^{-1}a)\,e=(a^{-1}a)\,(a^{-1}\,(a^{-1})^{-1})=((a^{-1}a)\,a^{-1})\,(a^{-1})^{-1}=$$
$$=a^{-1}(a^{-1})^{-1}=e, \text{ т. е. } a^{-1}a=e. \square$$

СВОЙСТВО 3.2. *Для каждого элемента a группы элемент a^{-1} является единственным обратным элементом. Каждый элемент a группы имеет единственный правый и единственный левый обратный элемент, причем оба они совпадают с a^{-1}.*

Это свойство непосредственно вытекает из определения обратного элемента, свойства 3.1, теоремы 1.4 и следствия 1.5 из нее.

СВОЙСТВО 3.3. *Для любого элемента a группы $ea=a$, т. е. правая единица является также и левой единицей.*

Доказательство. Из аксиом группы и свойства 3.1 следует, что

$$ea=(aa^{-1})\,a=a\,(a^{-1}a)=ae=a, \text{ т. е. } ea=a. \square$$

СВОЙСТВО 3.4. *Элемент e группы является единственным единичным элементом группы. Он же является*

единственным левым и единственным правым единичным элементом группы.

Это свойство непосредственно следует из определения единичных элементов, свойства 3.3, теоремы 1.1 и следствия 1.2 из нее.

СВОЙСТВО 3.5. *Для любых элементов a, b группы каждое из уравнений $ax=b$ и $ya=b$ относительно переменных x и y имеет в группе единственное решение.*

Доказательство. Элемент $a^{-1}b$ есть решение уравнения $ax=b$, так как $a(a^{-1}b)=(aa^{-1})b=eb=b$. С другой стороны, если c — произвольное решение уравнения $ax=b$, то $c=ec=(a^{-1}a)c=a^{-1}(ac)=a^{-1}b$. Следовательно, элемент $a^{-1}b$ является единственным решением первого уравнения. Аналогично доказывается, что элемент ba^{-1} является единственным решением второго уравнения. □

СВОЙСТВО 3.6 (*закон сокращения*). *Для любых элементов a, b, c группы из $ac=bc$ следует $a=b$ и из $ca=cb$ следует $a=b$.*

Доказательство. Если $ac=bc$, то a и b являются решениями уравнения $yc=bc$. По свойству 3.3 отсюда следует, что $a=b$. Аналогично доказывается, что из $ca=cb$ следует $a=b$. □

СВОЙСТВО 3.7. *Для любых элементов a, b, c группы из $ab=a$ следует $b=e$ и из $ca=a$ следует $c=e$.*

Доказательство. Если $ab=a$, то $ab=ae$. По закону сокращения, из $ab=ae$ следует $b=e$. Аналогично, из $ca=a$ следует $ca=ea$ и $c=e$. □

СВОЙСТВО 3.8. *В группе элемент a есть обратный к a^{-1}, т. е. $(a^{-1})^{-1}=a$.*

Доказательство. По третьей аксиоме группы, $(a^{-1})(a^{-1})^{-1}=e$. По свойству 3.1, $a^{-1}a=e$. Таким образом, $a^{-1}(a^{-1})^{-1}=a^{-1}a$. По закону сокращения, отсюда следует равенство $(a^{-1})^{-1}=a$. □

СВОЙСТВО 3.9. *Для любых элементов a, b группы из $ab=e$ следует, что $b=a^{-1}$ и $a=b^{-1}$.*

Это свойство непосредственно вытекает из определения обратного элемента и свойства 3.2.

Гомоморфизмы групп. В соответствии с определением гомоморфизма алгебр и с тем, что группы — частный случай алгебр, дадим следующие определения.

Пусть $\mathscr{G}=\langle G, \cdot, {}^{-1}\rangle$ и $\mathscr{H}=\langle H, \circ, {}^{-1}\rangle$ — мультипликативные группы.

Говорят, что отображение h множества G в H сохраняет главные операции группы $\mathscr{G}$, если выполняются

условия:

(1) $h(ab)=h(a)\circ h(b)$ для любых a, b из G;

(2) $h(a^{-1})=(h(a))^{-1}$ для любого a из G.

ОПРЕДЕЛЕНИЕ. *Гомоморфизмом группы* $\mathscr{G}$ в (на) группу $\mathscr{H}$ называется отображение множества G в (на) H, сохраняющее главные операции группы $\mathscr{G}$. Гомоморфизм группы $\mathscr{G}$ на $\mathscr{H}$ называется *эпиморфизмом*.

ОПРЕДЕЛЕНИЕ. Гомоморфизм h группы $\mathscr{G}$ на группу $\mathscr{H}$ называется *изоморфизмом*, если h является инъективным отображением множества G на H. Группы $\mathscr{G}$ и $\mathscr{H}$ называются *изоморфными*, если существует изоморфизм группы $\mathscr{G}$ на $\mathscr{H}$.

Запись $\mathscr{G}\cong\mathscr{H}$ означает, что группы $\mathscr{G}$ и $\mathscr{H}$ изоморфны.

ОПРЕДЕЛЕНИЕ. Гомоморфизм h группы $\mathscr{G}$ в группу $\mathscr{H}$ называется *мономорфизмом* или *вложением*, если h является инъективным отображением множества G в H.

ОПРЕДЕЛЕНИЕ. Гомоморфизм группы $\mathscr{G}$ в себя называется *эндоморфизмом группы* $\mathscr{G}$. Изоморфизм группы $\mathscr{G}$ на себя называется *автоморфизмом группы* $\mathscr{G}$.

Так, например, автоморфизмом является тождественное отображение группы на себя.

ТЕОРЕМА 3.1. *Если отображение h группы $\mathscr{G}=\langle G, \cdot, {}^{-1}\rangle$ в группу $\mathscr{H}=\langle H, \circ, {}^{-1}\rangle$ сохраняет бинарную операцию группы $\mathscr{G}$*, т. е.

(1) $h(ab)=h(a)\circ h(b)$ *для любых* a, b *из* G,

то h переводит единицу группы $\mathscr{G}$ в единицу группы $\mathscr{H}$ и является гомоморфизмом.

Доказательство. Пусть e — единица группы $\mathscr{G}$ и $e'=h(e)$. В силу (1) $h(e\cdot e)=h(e)\circ h(e)=h(e)$, т. е. $e'\circ e'=e'$. Отсюда, по свойству 3.7, следует, что e' является единицей группы $\mathscr{H}$.

Пусть a — любой элемент группы $\mathscr{G}$. В силу (1) из $a\cdot a^{-1}=e$ следует $h(a)\circ h(a^{-1})=e'$. По свойству 3.9, отсюда вытекает, что

(2) $h(a^{-1})=(h(a))^{-1}$ для любого a из G.

На основании (1) и (2) заключаем, что h является гомоморфизмом группы $\mathscr{G}$ в $\mathscr{H}$. □

ТЕОРЕМА 3.2. *Отношение изоморфизма на какомнибудь множестве групп рефлексивно, транзитивно и симметрично, т. е. является отношением эквивалентности.*

Эта теорема непосредственно следует из теоремы 2.5.

Примеры. 1. Пусть $\mathbf{Q}^*$ — множество всех рациональных чисел, отличных от нуля, и $\mathcal{Q}^* = \langle \mathbf{Q}^*, \cdot, {}^{-1} \rangle$ — мультипликативная группа рациональных чисел. Пусть $\mathbf{Q}_+$ — множество всех положительных рациональных чисел и $\mathcal{Q}_+ = \langle \mathbf{Q}_+, \cdot, {}^{-1} \rangle$ — мультипликативная группа положительных рациональных чисел. Отображение h множества $\mathbf{Q}^*$ на $\mathbf{Q}_+$, определяемое формулой $h(a) = |a|$ для каждого a из $\mathbf{Q}^*$, где $|a|$ — абсолютное значение числа a, сохраняет главные операции группы $\mathcal{Q}^*$. В самом деле, для любых a, b из $\mathbf{Q}^*$ верны равенства $|ab| = |a||b|$ и $|a^{-1}| = |a|^{-1}$. Следовательно, отображение h является гомоморфизмом группы $\mathcal{Q}^*$ на $\mathcal{Q}_+$.

2. Пусть $\mathbf{R}_+$ — множество всех положительных действительных чисел и $\mathscr{R}_+ = \langle \mathbf{R}_+, \cdot, {}^{-1} \rangle$ — мультипликативная группа положительных действительных чисел. Пусть $\mathbf{R}$ — множество всех действительных чисел и $\mathscr{R} = \langle \mathbf{R}, +, - \rangle$ — аддитивная группа действительных чисел. Рассмотрим отображение f: $\mathbf{R}_+ \to \mathbf{R}$, определяемое формулой $f(x) = \log x$. Функция f есть инъективное отображение множества $\mathbf{R}_+$ на $\mathbf{R}$, сохраняющее главные операции группы $\mathscr{R}_+$. В самом деле, для любых x, y из $\mathbf{R}_+$

$$\log(xy) = \log x + \log y, \quad \log(x^{-1}) = -\log x.$$

Следовательно, f является изоморфизмом группы $\mathscr{R}_+$ на группу $\mathscr{R}$.

3. Пусть g — отображение множества $\mathbf{R}$ на $\mathbf{R}_+$, определяемое формулой $g(x) = 2^x$. Отображение g есть инъективное отображение $\mathbf{R}$ на $\mathbf{R}_+$ и сохраняет главные операции аддитивной группы $\mathscr{R} = \langle \mathbf{R}, +, - \rangle$, так как $2^{x+y} = 2^x 2^y$ и $2^{-x} = (2^x)^{-1}$. Следовательно, g является изоморфизмом аддитивной группы $\mathscr{R}$ на мультипликативную группу $\mathscr{R}_+ = \langle \mathbf{R}, \cdot, {}^{-1} \rangle$.

Подгруппы. Пусть $\mathscr{G} = \langle G, \cdot, {}^{-1} \rangle$ — группа.

ОПРЕДЕЛЕНИЕ. *Подгруппой группы* $\mathscr{G}$ называется любая подалгебра этой группы.

Более подробно в соответствии с определением подалгебры определение подгруппы можно сформулировать следующим образом.

Алгебра $\mathscr{H} = \langle H, \odot, {}^{-1} \rangle$ типа (2, 1) называется *подгруппой группы* $\mathscr{G} = \langle G, \cdot, {}^{-1} \rangle$, если $H \subset G$ и тождественное отображение множества H в G является моно-

морфизмом алгебры $\mathscr{K}$ в $\mathscr{G}$, т. е. выполняются условия:

(1) $a \odot b = a \cdot b$ для любых a, b из H;
(2) $a^{-1} = a^{-1}$ для любого a из H.

Запись $\mathscr{K} \rightarrowtail \mathscr{G}$ означает, что алгебра $\mathscr{K}$ является подгруппой группы $\mathscr{G}$.

Если $\mathscr{K} \rightarrowtail \mathscr{G}$, то из определения подгруппы следует, что множество H замкнуто в группе $\mathscr{G}$, значит применение любой главной операции группы $\mathscr{G}$ к элементам из H приводит снова к элементу из H. Кроме того, в силу условий (1) и (2) каждая главная операция алгебры $\mathscr{K}$ является ограничением соответствующей главной операции группы $\mathscr{G}$ множеством H.

ТЕОРЕМА 3.3. *Любая подгруппа группы является группой. Нейтральный элемент группы является нейтральным элементом любой ее подгруппы.*

Доказательство. Пусть $\mathscr{K} = \langle H, \odot, {}^{-1} \rangle$ — подгруппа мультипликативной группы $\mathscr{G} = \langle G, \cdot, {}^{-1} \rangle$ и e — нейтральный элемент группы $\mathscr{G}$.

Бинарная операция $\odot$ алгебры $\mathscr{K}$ ассоциативна, так как в силу (1) для любых a, b, c из H имеем

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

Элемент e принадлежит H, так как в силу (1) и (2) для любого a из H имеем $e = a \cdot a^{-1} = a \odot a^{-1} \in H$. В силу (1) для любого a из H верны равенства $a \odot e = a \cdot e = a$, т. е. e является правым нейтральным элементом относительно операции $\odot$.

В силу (2) для любого a из H получаем $a \odot a^{-1} = a \cdot a^{-1} = e$, т. е. $a \odot a^{-1} = e$. Следовательно, алгебра $\mathscr{K}$ является группой и e — ее нейтральный элемент. □

Пусть $\mathscr{G} = \langle G, \cdot, {}^{-1} \rangle$ — мультипликативная группа и A — непустое подмножество множества G, замкнутое относительно главных операций группы $\mathscr{G}$. Пусть $\odot$ и ${}^{-1}$ — ограничения главных операций группы $\mathscr{G}$ множеством A, т. е.

$a \odot b = a \cdot b$ для любых a, b из A;
$a^{-1} = a^{-1}$ для любого a из A.

Тогда, по теоремам 2.6 и 3.3, алгебра

(3) $\mathscr{A} = \langle A, \odot, {}^{-1} \rangle$

является подгруппой группы $\mathscr{G}$. Таким образом, подгруппа $\mathscr{A}$ группы $\mathscr{G}$ однозначно определяется непустым подмножеством A, замкнутым в $\mathscr{G}$. Поэтому вместо записи (3) пишут: «подгруппа $\mathscr{A} = \langle A, \cdot, {}^{-1}\rangle$» или говорят: «множество A является подгруппой группы $\mathscr{G}$ относительно операций $\cdot$ и $^{-1}$».

ТЕОРЕМА 3.4. *Бинарное отношение* $\rightarrow$ (*«быть подгруппой»*) *на множестве подгрупп данной группы рефлексивно, транзитивно и антисимметрично и, следовательно, является отношением нестрогого порядка.*

Эта теорема есть частный случай теоремы 2.8.

ТЕОРЕМА 3.5. *Пересечение произвольной* (*непустой*) *совокупности подгрупп группы* $\mathscr{G}$ *является подгруппой группы* $\mathscr{G}$.

Эта теорема непосредственно следует из теоремы 3.3.

Из теоремы 3.6 следует, что для любого множества M элементов группы $\mathscr{G}$ существует наименьшая подгруппа $\mathscr{H}$, содержащая M. Нетрудно видеть, что $\mathscr{H}$ является пересечением всех подгрупп группы $\mathscr{G}$, содержащих M. Эта наименьшая подгруппа $\mathscr{H}$ называется *подгруппой, порожденной множеством* M, а M — *множеством образующих* или *системой образующих группы* $\mathscr{H}$.

ОПРЕДЕЛЕНИЕ. Группа называется *циклической*, если она порождается одним элементом (одноэлементным множеством).

Примеры. 1. Пусть $\mathscr{R}_+ = \langle \mathbf{R}, +, -\rangle$ — аддитивная группа действительных чисел. Множество $\mathbf{Q}$ рациональных чисел есть подмножество множества $\mathbf{R}$, замкнутое относительно главных операций группы $\mathscr{R}_+$. Следовательно, алгебра $\mathscr{Q} = \langle \mathbf{Q}, +, -\rangle$, аддитивная группа рациональных чисел, является подгруппой группы $\mathscr{R}_+$.

2. Пусть $\mathscr{R}^* = \langle \mathbf{R}^*, \cdot, {}^{-1}\rangle$ — мультипликативная группа действительных чисел. Множество $\mathbf{Q}^*$ отличных от нуля рациональных чисел есть подмножество множества $\mathbf{R}^*$, замкнутое относительно главных операций группы $\mathscr{R}^*$. Следовательно, алгебра $\mathscr{Q}^* = \langle \mathbf{Q}^*, \cdot, {}^{-1}\rangle$, мультипликативная группа рациональных чисел, является подгруппой группы $\mathscr{R}^*$.

3. Пусть $\mathscr{G} = \langle G, \circ, {}^{-1}\rangle$ — группа вращений плоскости вокруг данной точки O и H_n — множество, состоящее из n вращений плоскости вокруг точки O, отображающих правильный n-угольник с центром в точке O на себя. Множество H_n замкнуто относительно главных операций группы $\mathscr{G}$. Следовательно, алгебра $\mathscr{H}_n = \langle H_n, \circ, {}^{-1}\rangle$, группа

вращений правильного n-угольника, является подгруппой группы $\mathscr{G}$.

Упражнения

1. Выяснить, являются ли следующие множества рациональных чисел замкнутыми относительно главных операций аддитивной группы рациональных чисел:

(a) множество всех целых чисел;

(b) множество всех натуральных чисел;

(c) множество всех четных целых чисел;

(d) множество всех целых чисел, кратных данному целому n;

(e) множество всех нечетных целых чисел;

(f) множество всех рациональных чисел с нечетными знаменателями;

(g) множество всех рациональных чисел с четными знаменателями.

2. Выяснить, являются ли следующие множества рациональных чисел замкнутыми относительно главных операций мультипликативной группы рациональных чисел:

(a) множество $\{1, -1\}$;

(b) множество всех отличных от нуля чисел с четными знаменателями;

(c) множество всех отличных от нуля рациональных чисел с нечетными знаменателями;

(d) множество всех целочисленных степеней числа 2;

(e) множество $\{p^n \mid n$ — целое число$\}$, где p — простое число.

3. Составьте таблицу умножения для элементов следующих групп;

(a) группа вращений правильного треугольника;

(b) группа вращений квадрата;

(c) группа вращений правильного пятиугольника;

(d) аддитивная группа классов вычетов по модулю 5;

(e) мультипликативная группа классов вычетов по модулю 5, взаимно простых с числом 5;

(f) группа всех симметрий ромба;

(g) группа всех симметрий правильного треугольника;

(h) симметрическая группа подстановок третьей степени;

(i) группа симметрий прямоугольника, не являющегося квадратом;

(j) группа всех симметрий квадрата.

4. Докажите с помощью индукции, что порядок симметрической группы подстановок степени n равен $n!$

5. Докажите, что если $a^2 = e$ (e — единичный элемент группы) для любого элемента a мультипликативной группы, то группа абелева.

6. Пусть g и h — элементы мультипликативной группы $\mathscr{G}$. Определим степень с отрицательным показателем: $a^{-n} = (a^{-1})^n$. Докажите, что для любых чисел m и n:

(a) $(g^{-1})^n = (g^n)^{-1}$;

(b) $g^m g^n = g^{m+n}$;

(c) $(g^m)^n = g^{mn}$;

(d) $(g \cdot h)^m = g^m \cdot h^m$, если $\mathscr{G}$ — абелева группа.

7. Докажите, что всякая группа с четырьмя или меньшим числом элементов абелева.

8. Покажите, что всякая группа с тремя элементами является циклической. Докажите, что любые две группы, имеющие по три элемента каждая, изоморфны.

9. Пусть $\mathcal{G}$ — аддитивная абелева группа и n — целое число. Покажите, что отображение $x \longmapsto nx$ является эндоморфизмом группы $\mathcal{G}$.

10. Покажите, что отображение $x \longmapsto 3^x$ является изоморфизмом аддитивной группы действительных чисел на мультипликативную группу положительных действительных чисел.

11. Докажите, что симметрическая группа подстановок третьей степени изоморфна группе симметрий правильного треугольника.

12. Докажите, что группа вращений квадрата не изоморфна группе симметрий ромба.

13. Пусть $\mathcal{G}$ — мультипликативная абелева группа. Покажите, что отображение $x \longmapsto x^{-1}$ является автоморфизмом группы $\mathcal{G}$.

14. Докажите, что группа симметрий правильного тетраэдра изоморфна симметрической группе подстановок четвертой степени.

15. Докажите, что алгебра, изоморфная группе, является группой.

§ 4. КОЛЬЦА

Понятие кольца. Кольца, как и группы, являются очень важным частным случаем алгебр.

ОПРЕДЕЛЕНИЕ. *Кольцом* называется алгебра $\mathcal{K} = \langle K, +, -, \cdot, 1\rangle$ типа (2, 1, 2, 0), главные операции которой удовлетворяют следующим условиям:

(1) алгебра $\langle K, +, -\rangle$ есть абелева группа;

(2) алгебра $\langle K, \cdot, 1\rangle$ есть моноид;

(3) умножение дистрибутивно относительно сложения, т. е. для любых элементов a, b, c из K

$$(a+b)\cdot c = a\cdot c + b\cdot c,\quad c\cdot(a+b) = c\cdot a + c\cdot b.$$

Основное множество K кольца $\mathcal{K}$ обозначается также через $|\mathcal{K}|$. Элементы множества K называются *элементами кольца* $\mathcal{K}$.

ОПРЕДЕЛЕНИЕ. Группа $\langle K, +, -\rangle$ называется *аддитивной группой кольца* $\mathcal{K}$. Нуль этой группы, т. е. нейтральный элемент относительно сложения, называется *нулем кольца* и обозначается через 0 или $0_{\mathcal{K}}$.

ОПРЕДЕЛЕНИЕ. Моноид $\langle K, \cdot, 1\rangle$ называется *мультипликативным моноидом кольца* $\mathcal{K}$. Элемент 1, обозначаемый также через $1_{\mathcal{K}}$, являющийся нейтральным относительно умножения, называется *единицей кольца* $\mathcal{K}$.

Кольцо $\mathcal{K}$ называется *коммутативным*, если $a\cdot b = b\cdot a$ для любых элементов a, b кольца. Кольцо $\mathcal{K}$ называется *нулевым*, если $|\mathcal{K}| = \{0_{\mathcal{K}}\}$.

ОПРЕДЕЛЕНИЕ. Кольцо $\mathcal{K}$ называется *областью целостности*, если оно коммутативно, $0_{\mathcal{K}} \neq 1_{\mathcal{K}}$ и для любых $a, b \in K$ из $a\cdot b = 0$ следует $a = 0$ или $b = 0$.

ОПРЕДЕЛЕНИЕ. Элементы a и b кольца $\mathcal{K}$ назы-

ваются *делителями нуля*, если $a \neq 0$, $b \neq 0$ и $ab = 0$ или $ba = 0$.

Отметим, что любая область целостности не имеет делителей нуля.

Примеры. 1. Пусть $\mathbf{Q}$ — множество всех рациональных чисел и

$$\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}.$$

Алгебра

$$\mathfrak{A}[\sqrt{2}] = \langle \mathbf{Q}[\sqrt{2}], +, -, \cdot, 1 \rangle$$

типа (2, 1, 2, 0), где $+$, $\cdot$ суть обычные операции сложения и умножения действительных чисел и $-$ есть унарная операция перехода от данного числа к противоположному, является коммутативным кольцом.

2. Пусть K — множество всех действительных функций, определенных на множестве $\mathbf{R}$ действительных чисел. Сумма $f+g$, произведение $f \cdot g$, функция $(-f)$ и единичная функция $\mathbf{1}$ определяются как обычно, а именно:

$$(f+g)(x) = f(x) + g(x);$$
$$(f \cdot g)(x) = f(x) \cdot g(x);$$
$$(-f)(x) = -f(x);$$
$$\mathbf{1}(x) = 1.$$

Непосредственная проверка показывает, что алгебра $\langle K, +, -, \cdot, 1 \rangle$ является коммутативным кольцом.

3. Пусть $\mathscr{K} = \langle K, +, -, \cdot, 1 \rangle$ — произвольное кольцо. Таблица вида

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

где a, b, c, d — элементы из K, называется *квадратной матрицей* второго порядка над $\mathscr{K}$ или 2×2-матрицей над $\mathscr{K}$. Множество всех 2×2-матриц над $\mathscr{K}$ обозначим через $K^{2\times 2}$. На этом множестве введем отношение равенства. Матрицы

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ и } \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

называют *равными* и пишут

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} e & f \\ g & h \end{bmatrix},$$

если $a = e$, $b = f$, $c = g$, $d = h$.

Матрицы

$$I=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \text{ и } \begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$$

называются *единичной* и *нулевой* соответственно. На множестве 2×2-матриц над $\mathscr{K}$ операции сложения, умножения и унарная операция — определяются следующим образом:

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}+\begin{bmatrix}a_1 & b_1\\ c_1 & d_1\end{bmatrix}=\begin{bmatrix}a+a_1 & b+b_1\\ c+c_1 & d+d_1\end{bmatrix};$$

$$-\begin{bmatrix}a & b\\ c & d\end{bmatrix}=\begin{bmatrix}-a & -b\\ -c & -d\end{bmatrix};$$

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}\cdot\begin{bmatrix}a_1 & b_1\\ c_1 & d_1\end{bmatrix}=\begin{bmatrix}aa_1+bc_1 & ab_1+bd_1\\ ca_1+dc_1 & cb_1+dd_1\end{bmatrix}.$$

Непосредственно проверяется, что алгебра $\langle K^{2\times 2}, +, -\rangle$ есть абелева группа, алгебра $\langle K^{2\times 2}, \cdot, I\rangle$ — моноид и умножение матриц дистрибутивно относительно сложения. Следовательно, алгебра $\langle K^{2\times 2}, +, -, \cdot, I\rangle$ является кольцом, причем некоммутативным. Это кольцо называется *кольцом 2×2-матриц над $\mathscr{K}$* и обозначается символом $\mathscr{K}^{2\times 2}$.

Простейшие свойства кольца. Пусть $\mathscr{K}$ — кольцо. Так как алгебра $\langle K, +, -\rangle$ есть абелева группа, то в силу свойства 3.5 для любых элементов a, b из K уравнение $b+x=a$ имеет единственное решение $a+(-b)$, которое обозначается также через $a-b$.

ТЕОРЕМА 4.1. *Пусть $\mathscr{K}=\langle K, +, -, \cdot, 1\rangle$ — кольцо. Тогда для любых элементов a, b, c кольца:*

(1) *если* $a+b=a$, *то* $b=0$;
(2) *если* $a+b=0$, *то* $b=-a$;
(3) $-(-a)=a$;
(4) $0\cdot a=a\cdot 0=0$;
(5) $(-a)b=a(-b)=-(ab)$;
(6) $(-a)(-b)=a\cdot b$;
(7) $(a-b)c=ac-bc$ и $c(a-b)=ca-cb$.

Доказательство. (1) Если $a+b=a$, то

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

(2) Если $a+b=0$, то

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

(3) В аддитивной группе кольца $(-a)+(-(-a))=-a+a$. Отсюда, по закону сокращения, следует равенство $-(-a)=a$.

(4) В силу дистрибутивности умножения относительно сложения $0 \cdot a + 0 \cdot a = (0+0) \cdot a = 0 \cdot a$, т. е. $0 \cdot a + 0 \cdot a = 0 \cdot a$. В силу (1) из последнего равенства следует $0 \cdot a = 0$.

(5) В силу (4) и дистрибутивности умножения относительно сложения $ab + (-a)\,b = (a + (-a))b = 0 \cdot b = 0$, т. е. $ab + (-a)\,b = 0$. Отсюда в силу (2) следует $(-a)\,b = -(ab)$. Аналогично доказывается, что $a(-b) = -(ab)$.

(6) В силу (5) и (3) $(-a) \cdot (-b) = -((-a) \cdot b) = -(-(ab)) = a \cdot b$.

(7) В силу (5) и дистрибутивности умножения относительно сложения $(a-b) \cdot c = (a + (-b)) \cdot c = a \cdot c + (-b) \cdot c = a \cdot c + (-b \cdot c) = a \cdot c - b \cdot c$. Аналогично доказывается, что $c \cdot (a-b) = c \cdot a - c \cdot b$. □

Гомоморфизмы колец. В соответствии с определением гомоморфизма алгебр и с тем, что кольца — частный случай алгебр, дадим следующие определения.

Пусть $\mathscr{K} = \langle K, +, -, \circ, 1\rangle$ и $\mathscr{K}' = \langle K', +, -, \cdot, 1'\rangle$ — кольца. Говорят, что отображение h множества K в K' сохраняет главные операции кольца $\mathscr{K}$, если выполнены условия:

(1) $h(a+b) = h(a) + h(b)$ для любых a, b из K;

(2) $h(-a) = -h(a)$ для любого a из K;

(3) $h(a \cdot b) = h(a) \circ h(b)$ для любых a, b из K;

(4) $h(1) = 1'$.

ОПРЕДЕЛЕНИЕ. *Гомоморфизмом кольца $\mathscr{K}$ в (на) кольцо $\mathscr{K}'$* называется отображение множества K в (на) K', сохраняющее все главные операции кольца $\mathscr{K}$. Гомоморфизм кольца $\mathscr{K}$ на $\mathscr{K}'$ называется *эпиморфизмом*.

ОПРЕДЕЛЕНИЕ. Гомоморфизм h кольца $\mathscr{K}$ на кольцо $\mathscr{K}'$ называется *изоморфизмом*, если h является инъективным отображением множества K на K'. Кольца $\mathscr{K}$ и $\mathscr{K}'$ называются *изоморфными*, если существуют изоморфизм кольца $\mathscr{K}$ на $\mathscr{K}'$.

Запись $\mathscr{K} \cong \mathscr{K}'$ означает, что кольца $\mathscr{K}$ и $\mathscr{K}'$ изоморфны.

ОПРЕДЕЛЕНИЕ. Гомоморфизм h кольца $\mathscr{K}$ в кольцо $\mathscr{K}'$ называется *мономорфизмом* или *вложением*, если h является инъективным отображением множества K в K'.

ОПРЕДЕЛЕНИЕ. Гомоморфизм кольца $\mathscr{K}$ в себя называется *эндоморфизмом кольца $\mathscr{K}$*. Изоморфизм кольца $\mathscr{K}$ на себя называется *автоморфизмом кольца $\mathscr{K}$*.

Так, например, автоморфизмом кольца является тождественное отображение кольца на себя.

ТЕОРЕМА 4.2. *Если отображение h кольца $\mathscr{K}$ в кольцо $\mathscr{K}'$ переводит единицу кольца $\mathscr{K}$ в единицу кольца $\mathscr{K}'$ и сохраняет операции сложения и умножения, т. е.*

$$h(x+y)=h(x)+h(y) \text{ для любых } x, y \text{ из } K,$$
$$h(xy)=h(x)\cdot h(y) \text{ для любых } x, y \text{ из } K,$$

то h переводит нуль кольца $\mathscr{K}$ в нуль кольца $\mathscr{K}'$ и является гомоморфизмом.

Доказательство. Рассмотрим аддитивные группы

$$\langle K, +, -\rangle \text{ и } \langle K', +, -\rangle$$

колец $\mathscr{K}$ и $\mathscr{K}'$. По условию, h сохраняет операцию сложения. Отсюда, согласно теореме 3.1, следует, что h переводит нуль кольца $\mathscr{K}$ в нуль кольца $\mathscr{K}'$ и является гомоморфизмом группы $\langle K, +, -\rangle$ в группу $\langle K', +, -\rangle$. В частности, $h(-x)=-h(x)$ для любого x из K. Следовательно, отображение h сохраняет все главные операции кольца $\mathscr{K}$ и является гомоморфизмом. □

ТЕОРЕМА 4.3. *Отношение изоморфизма на каком-нибудь множестве колец рефлексивно, транзитивно и симметрично* и, значит, *является отношением эквивалентности.*

Эта теорема непосредственно следует из теоремы 2.5.

Примеры. 1. Пусть $\mathbf{Q}$ — множество рациональных чисел, $\mathbf{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,\ b\in Q\}$. Алгебра $\mathscr{Q}[\sqrt{2}]=\langle \mathbf{Q}[\sqrt{2}], +, -, \cdot, 1\rangle$ является кольцом. Отображение $f: \mathbf{Q}[\sqrt{2}]\to \mathbf{Q}[\sqrt{2}]$, определяемое формулой $f(a+b\sqrt{2})=a-b\sqrt{2}$, есть инъективное отображение множества $\mathbf{Q}[\sqrt{2}]$ на себя. Отображение f сохраняет главные операции кольца $\mathbf{Q}[\sqrt{2}]$. Действительно, для любых $x=a+b\sqrt{2}$ и $y=c+d\sqrt{2}$

$$f(xy)=f(ac+2bd+(ad+bc)\sqrt{2})=(ac+2bd)-(ad+bc)\sqrt{2}=(a-b\sqrt{2})(c-d\sqrt{2})=f(x)f(y);$$
$$f(x+y)=f(a+b\sqrt{2}+c+d\sqrt{2})=a-b\sqrt{2}+b-d\sqrt{2}=f(x)+f(y);$$
$$f(1_{\mathscr{Q}})=1=1_{\mathscr{Q}[\sqrt{2}]}.$$

Следовательно, отображение f является автоморфизмом кольца $\mathscr{Q}[\sqrt{2}]$.

2. Пусть K — множество всех матриц вида $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$ с рациональными a и b и $\mathscr{K}=\langle K, +, -, \cdot, 1\rangle$ — кольцо таких

матриц. Отображение $h: \mathbf{Q}[\sqrt{2}] \to K$, определяемое формулой

$$h(a+b\sqrt{2}) = \begin{bmatrix} a & b \\ 2b & a \end{bmatrix},$$

есть инъективное отображение множества $\mathbf{Q}[\sqrt{2}]$ на K. Нетрудно проверить, что отображение h сохраняет главные операции кольца $\mathcal{Q}[\sqrt{2}]$. Следовательно, h является изоморфизмом кольца $\mathcal{Q}[\sqrt{2}]$ на кольцо $\mathcal{K}$.

3. Пусть L — множество всех матриц вида $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, называемых *диагональными*, с рациональными a и b. Алгебра $\mathcal{L} = \langle L, +, -, \cdot, I \rangle$, где $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, является кольцом. Отображение $f: L \to \mathbf{Q}$, определяемое формулой

$$f\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\right) = a \text{ для любых } a, b \text{ из } \mathbf{Q},$$

есть отображение, сохраняющее главные операции кольца $\mathcal{L}$. Следовательно, f является гомоморфизмом кольца $\mathcal{L}$ на кольцо $\mathcal{Q}$ рациональных чисел.

Подкольца. Пусть $\mathcal{K} = \langle K, +, -, \cdot, 1 \rangle$ — кольцо.

ОПРЕДЕЛЕНИЕ. *Подкольцом кольца* $\mathcal{K}$ называется любая подалгебра этого кольца.

Более подробно в соответствии с определением подалгебры определение подкольца можно сформулировать следующим образом.

Алгебра $\mathcal{L} = \langle L, \oplus, \ominus, \odot, 1_{\mathcal{L}} \rangle$ типа (2, 1, 2, 0) называется *подкольцом кольца* $\mathcal{K}$, если $L \subset K$ и тождественное отображение множества L в K является мономорфизмом алгебры $\mathcal{L}$ в $\mathcal{K}$, т. е. выполняются условия:

(1) $a \oplus b = a + b$ для любых a, b из L;

(2) $\ominus a = -a$ для любого a из L;

(3) $a \odot b = a \cdot b$ для любых a, b из L;

(4) $1_{\mathcal{L}} = 1_{\mathcal{K}}$.

Запись $\mathcal{L} \rightarrowtail \mathcal{K}$ означает, что алгебра $\mathcal{L}$ является подкольцом кольца $\mathcal{K}$.

Если $\mathcal{L} \rightarrowtail \mathcal{K}$, то из определения подкольца следует, что множество L замкнуто относительно каждой главной операции кольца $\mathcal{K}$, т. е. применение любой главной операции кольца $\mathcal{K}$ к элементам из L приводит снова к элементам множества L. Кроме того, в силу условий (1)—(4)

каждая главная операция алгебры $\mathscr{L}$ является ограничением соответствующей главной операции кольца $\mathscr{K}$ множеством L.

ТЕОРЕМА 4.4. *Любое подкольцо кольца является кольцом. Нуль и единица кольца являются нулем и единицей любого его подкольца.*

Доказательство. Пусть $\mathscr{L} = \langle L, \oplus, \ominus, \odot, 1_{\mathscr{L}} \rangle$ — подкольцо кольца $\mathscr{K} = \langle K, +, -, \cdot, 1 \rangle$ и 0 — нуль кольца $\mathscr{K}$. В силу условий (1) и (2) алгебра $\langle L, \oplus, \ominus \rangle$ есть подгруппа аддитивной группы $\langle K, +, - \rangle$ кольца $\mathscr{K}$. Поэтому алгебра $\langle L, \oplus, \ominus \rangle$ является абелевой группой и 0 — ее нулевой элемент.

Умножение в $\mathscr{L}$ ассоциативно. В самом деле, в силу (3) имеем

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

для любых a, b, c из L. В силу (3) и (4) $1_{\mathscr{L}} = 1$ и $a \odot 1_{\mathscr{L}} = a \odot 1 = a \cdot 1 = a$ для любого a из L. Следовательно, алгебра $\langle L, \odot, 1_{\mathscr{L}} \rangle$ является моноидом.

Умножение в $\mathscr{L}$ дистрибутивно относительно сложения. В самом деле, в силу (1) и (3) для любых a, b, c из L

$$(a \oplus b) \odot c = (a + b) \cdot c = a \cdot c + b \cdot c = a \odot b \oplus b \odot c$$

и, аналогично, $c \odot (a \oplus b) = c \odot a \oplus c \odot b$. Следовательно, алгебра $\mathscr{L}$ является кольцом. □

Пусть $\mathscr{K} = \langle K, +, -, \cdot, 1 \rangle$ — кольцо и A — произвольное непустое подмножество множества K, замкнутое относительно главных операций кольца $\mathscr{K}$. Пусть $\oplus, \ominus, \odot$ — ограничение главных операций кольца $\mathscr{K}$ множеством A, т. е.

$a \oplus b = a + b$ для любых a, b из A;

$\ominus a = -a$ для любого a из A;

$a \odot b = ab$ для любых a, b из A.

Тогда, по теоремам 2.6 и 4.4, алгебра $\mathscr{A}$,

(5) $\mathscr{A} = \langle A, \oplus, \ominus, \odot, 1 \rangle$,

является подкольцом кольца $\mathscr{K}$. Таким образом, подкольцо $\mathscr{A}$ кольца $\mathscr{K}$ однозначно определяется непустым подмножеством A множества K, замкнутым в $\mathscr{K}$. Поэтому вместо (5) пишут: «подкольцо $\mathscr{A} = \langle A, +, -, \cdot, 1 \rangle$» и говорят: «множество A является подкольцом кольца $\mathscr{K}$ относительно операций $+, -, \cdot, 1$».

ТЕОРЕМА 4.5. *Бинарное отношение $\prec$ («быть подкольцом») на множестве подколец данного кольца рефлексивно,*

транзитивно и антисимметрично, т. е. является отношением нестрогого порядка.

Эта теорема является частным случаем теоремы 2.8.

ТЕОРЕМА 4.6. *Пересечение произвольной (непустой) совокупности подколец кольца $\mathcal{K}$ является подкольцом кольца $\mathcal{K}$.*

Эта теорема является частным случаем теоремы 2.10.

Из теоремы 4.4 следует, что для любого множества M элементов кольца $\mathcal{K}$ существует наименьшее подкольцо $\mathcal{L}$, содержащее множество M. Нетрудно видеть, что $\mathcal{L}$ является пересечением всех подколец кольца $\mathcal{K}$, содержащих множество M. Это наименьшее подкольцо $\mathcal{L}$ называется *подкольцом, порожденным множеством M*, а *M — системой образующих* для кольца $\mathcal{L}$.

Примеры. 1. Пусть D — множество всех диагональных 2×2-матриц вида $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ над кольцом $\mathcal{K}$. Множество D замкнуто относительно главных операций кольца всех 2×2-матриц над кольцом K, $\mathcal{K}^{2\times 2} = \langle K^{2\times 2}, +, —, \cdot, I\rangle$. Следовательно, алгебра $\langle D, +, —, \cdot, 1\rangle$ является подкольцом кольца $\mathcal{K}^{2\times 2}$.

2. Матрицы вида $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ называются *верхнетреугольными*. Пусть L — множество всех верхнетреугольных матриц над данным кольцом $\mathcal{K} = \langle K, +, —, \cdot, 1\rangle$. Множество L замкнуто относительно главных операций кольца $\mathcal{K}^{2\times 2} = \langle K^{2\times 2}, +, —, \cdot, I\rangle$ 2×2-матриц над $\mathcal{K}$. Следовательно, алгебра $\langle L, +, —, \cdot, I\rangle$ является подкольцом кольца $\mathcal{K}^{2\times 2}$.

3. Пусть $\mathcal{K}$ — произвольное ненулевое кольцо и S — множество всех матриц вида $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ с элементами a, b из K. Непосредственная проверка показывает, что множество S замкнуто относительно главных операций кольца $\mathcal{K}^{2\times 2} = \langle K^{2\times 2}, +, —, \cdot, I\rangle$. Следовательно, алгебра $\langle S, +, —, \cdot, I\rangle$ является подкольцом кольца $\mathcal{K}^{2\times 2}$.

4. Пусть $\mathcal{K} = \langle K, +, —, \cdot, 1\rangle$ — кольцо всех действительных функций, определенных и непрерывных на множестве $\mathbf{R}$ действительных чисел. Пусть D — множество всех действительных функций, определенных и дифференцируемых на множестве $\mathbf{R}$. Множество D замкнуто относительно главных операций кольца $\mathcal{K}$. Следовательно, алгебра $\langle D, +, —, \cdot, 1\rangle$ является подкольцом кольца $\mathcal{K}$.

Упражнения

1. Выяснить, являются ли следующие множества рациональных чисел замкнутыми относительно главных операций кольца рациональных чисел:

(a) множество всех четных целых чисел;

(b) множество всех натуральных чисел;

(c) множество всех рациональных чисел, знаменатели которых суть единица или четные числа;

(d) множество всех рациональных чисел с нечетными знаменателями.

2. Выяснить, являются ли следующие множества действительных чисел замкнутыми относительно главных операций кольца всех действительных чисел:

(a) множество всех чисел вида $a+b\sqrt{2}$ с целыми a и b;

(b) множество всех чисел вида $a+b\sqrt{3}$ с целыми a и b;

(c) множество всех чисел вида $a+b\sqrt{5}$ с рациональными a и b.

3. Пусть $\mathscr{K}$ — ненулевое кольцо. Докажите, что кольцо 2×2-матриц над $\mathscr{K}$ является некоммутативным кольцом с делителями нуля.

4. Докажите, что в кольце, состоящем из n элементов, для каждого элемента a кольца $na=0$.

5. Докажите, что если элемент a кольца перестановочен с элементом b, т. е. $ab=ba$, то он перестановочен также с элементами $(-b)$, b^{-1} и nb, где n — целое число; если элемент a перестановочен с элементами b и c, то он перестановочен также с элементами $b+c$ и bc.

6. Пусть $a^2=a$ для каждого элемента a кольца $\mathscr{K}$. Покажите, что кольцо $\mathscr{K}$ коммутативно.

7. Пусть f — гомоморфизм кольца $\mathscr{K}$ в кольцо $\mathscr{K}'=\langle K', +, -, \cdot, 1\rangle$. Покажите, что алгебра $\langle \operatorname{Im} f, +, -, \cdot, 1\rangle$ является подкольцом кольца $\mathscr{K}'$.

8. Докажите, что для любых элементов x, y коммутативного кольца и любых целых положительных m и n

(a) $x^m\cdot x^n=x^{m+n}$; (b) $(x^m)^n=x^{mn}$; (c) $(xy)^n=x^ny^n$.

9. Докажите, что алгебра, изоморфная кольцу, сама является кольцом.

10. Для произвольного кольца докажите индукцией по n биномиальную теорему

$$(a+b)^n=a^n+C_n^1a^{n-1}b+C_n^2a^{n-2}b^2+\ldots+b^n,$$

где n — целое положительное и $C_n^k=\dfrac{n!}{k!\,(n-k)!}$.

§ 5. АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ

Понятие алгебраической системы. Пусть A — любое непустое множество.

ОПРЕДЕЛЕНИЕ. *Алгебраической системой* называется упорядоченная тройка

$$\mathscr{A}=\langle A,\ \Omega,\ \Omega_0\rangle,$$

где A — непустое множество, Ω — множество операции на A и Ω_0 — множество отношений на A.

Таким образом, алгебраическая система $\mathscr{A}$ определяется тремя множествами:

(a) непустым множеством A, обозначаемым также через $\mathscr{A}$|; это множество называется *основным множеством системы* $\mathscr{A}$, а его элементы — *элементами системы* $\mathscr{A}$;

(b) множеством операций Ω, определенных на A и называемых *главными операциями системы* $\mathscr{A}$;

(c) множеством отношений Ω_0, заданных на A и называемых *главными отношениями системы* $\mathscr{A}$.

Если $\langle A, \Omega, \Omega_0\rangle$ — алгебраическая система, то говорят также, что множество A есть алгебраическая система относительно операций Ω и отношений Ω_0.

Иногда под алгебраической системой понимают пару $\langle A, \Omega^*\rangle$, где $\Omega^* = \Omega \cup \Omega_0$, Ω — множество операций на A, Ω_0 — множество отношений на A. Тогда если $\Omega_0 = \emptyset$, то система $\langle A, \Omega^*\rangle = \langle A, \Omega\rangle$ является алгеброй. Таким образом, алгебру можно рассматривать как частный случай алгебраической системы.

ОПРЕДЕЛЕНИЕ. Алгебраические системы $\mathscr{A} = \langle A, \Omega, \Omega_0\rangle$ и $\mathscr{B} = \langle B, \Omega', \Omega_0'\rangle$ называются *однотипными*, если однотипны алгебры $\langle A, \Omega\rangle$ и $\langle B, \Omega'\rangle$ и существует инъективное отображение множества Ω_0 на Ω_0', при котором любое отношение $R_{\mathscr{A}}$ из Ω_0 и соответствующее ему при отображении отношение $R_{\mathscr{B}}$ из Ω_0' имеют один и тот же ранг.

Наиболее частым является случай, когда множества Ω и Ω_0 конечны: $\Omega = \{f_1, \ldots, f_s\}$, $\Omega_0 = \{R_1, \ldots, R_t\}$. В этом случае вместо записи

$$\mathscr{A} = \langle A, \{f_1, \ldots, f_s\}, \{R_1, \ldots, R_t\}\rangle$$

обычно употребляется запись

$$\mathscr{A} = \langle A, f_1, \ldots, f_s, R_1, \ldots, R_t\rangle.$$

При этом последовательность $(\mathrm{r}(f_1), \ldots, \mathrm{r}(f_s); \mathrm{r}(R_1), \ldots, \mathrm{r}(R_t))$, где $\mathrm{r}(f_i)$ — ранг операции f_i, $\mathrm{r}(R_k)$ — ранг отношения R_k, называется *типом системы* $\mathscr{A}$. Алгебраические системы $\mathscr{A}$ и $\mathscr{B}$,

$$\mathscr{B} = \langle B, f_1', \ldots, f_s', R_1', \ldots, R_t'\rangle$$

являются *однотипными*, если их типы совпадают, т. е. $\mathrm{r}(f_i) = \mathrm{r}(f_i')$ для $i = 1, \ldots, s$, $\mathrm{r}(R_1) = \mathrm{r}(R_k')$ для $k = 1, \ldots, t$. При этом операция f_i' системы $\mathscr{B}$ называется *соответст-*

вующей операции f_i системы $\mathscr{A}$, а отношение R'_k системы $\mathscr{B}$ — *соответствующим отношению* R_k системы $\mathscr{A}$.

Пример. Множество натуральных чисел **N** с обычными операциями сложения $+$, умножения $\cdot$ и отношением порядка $\leqslant$ является алгебраической системой $\langle \mathbf{N}, +, \cdot, \leqslant \rangle$ типа (2,2; 2).

Изоморфизмы алгебраических систем. Пусть $\mathscr{A}$ и $\mathscr{B}$ — однотипные алгебраические системы, $R_{\mathscr{A}}$ — произвольное главное отношение системы $\mathscr{A}$ и $R_{\mathscr{B}}$ — соответствующее ему главное отношение системы $\mathscr{B}$. Говорят, что отображение h множества $|\mathscr{A}|$ в $|\mathscr{B}|$ сохраняет отношение $R_{\mathscr{A}}$, если

$$(a_1, \ldots, a_n) \in R_{\mathscr{A}} \leftrightarrow (h(a_1), \ldots, h(a_n)) \in R_{\mathscr{B}}$$

для любых $a_1, \ldots, a_n$ из $|\mathscr{A}|$,

где n — ранг отношения $R_{\mathscr{A}}$.

ОПРЕДЕЛЕНИЕ. *Изоморфизмом алгебраической системы* $\mathscr{A}$ на однотипную ей систему $\mathscr{B}$ называется инъективное отображение множества $|\mathscr{A}|$ на $|\mathscr{B}|$, сохраняющее все главные операции и отношения системы $\mathscr{A}$. Системы $\mathscr{A}$ и $\mathscr{B}$ называются *изоморфными*, если существует изоморфизм системы $\mathscr{A}$ на $\mathscr{B}$.

Запись $\mathscr{A} \cong \mathscr{B}$ означает, что системы $\mathscr{A}$ и $\mathscr{B}$ изоморфны.

ОПРЕДЕЛЕНИЕ. *Мономорфизмом* или *вложением* алгебраической системы $\mathscr{A}$ в однотипную ей систему $\mathscr{B}$ называется инъективное отображение множества $|\mathscr{A}|$ в $|\mathscr{B}|$, сохраняющее все главные операции и отношения системы $\mathscr{A}$.

ОПРЕДЕЛЕНИЕ. *Гомоморфизмом алгебраической системы* $\mathscr{A}$ *в однотипную ей систему* $\mathscr{B}$ называется отображение h множества $|\mathscr{A}|$ в $|\mathscr{B}|$, сохраняющее все главные операции системы $\mathscr{A}$ и удовлетворяющее условию

$$(a_1, \ldots, a_n) \in R_{\mathscr{A}} \rightarrow (h(a_1), \ldots, h(a_n)) R_{\mathscr{B}}$$

для любых $a_1, \ldots, a_n$ из $|\mathscr{A}|$,

где $R_{\mathscr{A}}$ — любое главное отношение системы $\mathscr{A}$, n — его ранг, а $R_{\mathscr{B}}$ — главное отношение системы $\mathscr{B}$, соответствующее отношению $R_{\mathscr{A}}$.

Подсистемы. Пусть $\mathscr{A}$ и $\mathscr{B}$ — однотипные алгебраические системы, $f_{\mathscr{A}}$ — главная операция системы $\mathscr{A}$ и $f_{\mathscr{B}}$ — соответствующая ей главная операция системы $\mathscr{B}$, $R_{\mathscr{A}}$ — главное отношение системы $\mathscr{A}$ и $R_{\mathscr{B}}$ — соответствующее ему главное отношение системы $\mathscr{B}$.

ОПРЕДЕЛЕНИЕ. Система $\mathscr{A}$ называется *подсистемой системы* $\mathscr{B}$, если $|\mathscr{A}| \subset |\mathscr{B}|$ и для каждой главной операции $f_{\mathscr{A}}$ и каждого главного отношения $R_{\mathscr{A}}$ выполняются условия:

(1) $f_{\mathscr{A}}(a_1, \ldots, a_m) = f_{\mathscr{B}}(a_1, \ldots, a_m)$
для любых $a_1, \ldots, a_m$ из $|\mathscr{A}|$,

(2) $(a_1, \ldots, a_n) \in R_{\mathscr{A}} \leftrightarrow (a_1, \ldots, a_n) \in R_{\mathscr{B}}$
для любых $a_1, \ldots, a_n$ из $|\mathscr{A}|$,

где m — ранг операции $f_{\mathscr{A}}$ и n — ранг отношения $R_{\mathscr{A}}$.

Другими словами, система $\mathscr{A}$ называется *подсистемой системы* $\mathscr{B}$, если $|\mathscr{A}| \subset |\mathscr{B}|$ и тождественное отображение $|\mathscr{A}|$ в $|\mathscr{B}|$ является мономорфизмом системы $\mathscr{A}$ в систему $\mathscr{B}$. Запись $\mathscr{A} \rightarrowtail \mathscr{B}$ означает, что система $\mathscr{A}$ является подсистемой системы $\mathscr{B}$.

Из определения следует, что если $\mathscr{A} \rightarrowtail \mathscr{B}$, то множество $|\mathscr{A}|$ замкнуто в системе $\mathscr{B}$, значит применение любой главной операции $f_{\mathscr{B}}$ к элементам множества $|\mathscr{A}|$ приводит снова к элементам множества $|\mathscr{A}|$. В силу (1) каждая главная операция $f_{\mathscr{A}}$ алгебры $\mathscr{A}$ является ограничением соответствующей операции $f_{\mathscr{B}}$ множеством $|\mathscr{A}|$, т. е. $f_{\mathscr{A}} = f_{\mathscr{B}} | |\mathscr{A}|$.

Пусть R — отношение ранга n на множестве B и $A \subset B$.

ОПРЕДЕЛЕНИЕ. Отношение S ранга n на множестве A называется *ограничением отношения* R *множеством* A, если $S = R \cap A^n$, что эквивалентно условию

$(a_1, \ldots, a_n) \in S \leftrightarrow (a_1, \ldots, a_n) \in R$
для любых $a_1, \ldots, a_n$ из A.

Из этого определения следует в силу (2), что каждое главное отношение подалгебры является ограничением соответствующего ему отношения самой алгебры.

Пусть $\mathscr{B} = \langle B, f_1, \ldots, f_s, R_1, \ldots, R_t \rangle$ — алгебраическая система и C — произвольное непустое подмножество множества $|\mathscr{B}|$, замкнутое относительно главных операций системы $\mathscr{B}$. Обозначим через $f_i | C$ и $R_k | C$ ограничения множеством C соответственно операции f_i и отношения R_k ($i = 1, \ldots, s$; $k = 1, \ldots, t$). Система

(3) $\mathscr{C} = \langle C, f_1 | C, \ldots, f_s | C, R_1 | C, \ldots, R_t | C \rangle$

является подсистемой системы $\mathscr{B}$. Таким образом, подсистема $\mathscr{C}$ системы $\mathscr{B}$ однозначно определяется непустым

подмножестом C, замкнутым в системе $\mathscr{B}$. Поэтому вместо (3) пишут: «подсистема $\mathscr{C} = \langle C, f_1, \ldots, f_s; R_1, \ldots, R_t\rangle$» или «множество C является подсистемой относительно операций $f_1, \ldots, f_s$ и отношений $R_1, \ldots, R_t$».

Упражнения

1. Пусть h — изоморфизм алгебраической системы $\langle A, R\rangle$ на алгебраическую систему $\langle B, S\rangle$, где R и S — бинарные отношения. Докажите, что тогда:

(a) если R рефлексивно (на A), то и S рефлексивно (на B);

(b) если R антирефлексивно (на A), то и S антирефлексивно (на B);

(c) если отношение R симметрично, то и S симметрично;

(d) если R транзитивно, то и S транзитивно;

(e) если R антисимметрично, то и S антисимметрично;

(f) если R связанно, то и S связанно;

(g) если R — отношение строгого (нестрогого) порядка (на A), то и S — отношение строгого (нестрогого) порядка (на B);

(h) если R — отношение линейного порядка (на A), то и S — отношение линейного порядка (на B).

2. Покажите на примере систем $\langle \mathbf{N}, \sigma\rangle$ и $\langle \mathbf{N}, >\rangle$, где σ — пустое бинарное отношение на $\mathbf{N}$, а $\mathbf{N}$ — множество натуральных чисел, что не каждый взаимно однозначный гомоморфизм есть изоморфизм.

3. Приведите примеры изоморфизмов и гомоморфизмов алгебраических систем.

Глава четвертая

ОСНОВНЫЕ ЧИСЛОВЫЕ СИСТЕМЫ

§ 1. СИСТЕМА НАТУРАЛЬНЫХ ЧИСЕЛ

Алфавит и слова. *Алфавитом* называется произвольный набор символов, называемых *буквами*. При этом предполагается, что буквы можно воспроизводить в неограниченном количестве, подобно печатным буквам. Набор букв алфавита может быть задан в виде списка конкретных букв, заключенных в фигурные скобки. Можно считать, что в таком списке отсутствуют повторения, — любые две буквы, встречающиеся в алфавите, различны. Будем считать, что каждый алфавит содержит по крайней мере одну букву.

Буквы, входящие в алфавит $\mathfrak{A}$, называются *буквами алфавита* $\mathfrak{A}$. О буквах алфавита $\mathfrak{A}$ говорят также, что они принадлежат $\mathfrak{A}$.

Всякую конечную последовательность букв называют *словом*. Словом в данном алфавите $\mathfrak{A}$ называется слово, каждая буква которого принадлежит этому алфавиту. Например, слова a, ba, $baab$, $baaacb$ являются словами в алфавите $\{a, b, c\}$. Слова 0, 00, 0|, |, 0|0|, ||00 можно рассматривать как слова в алфавите $\{0, |\}$. Так как любая последовательность написанных друг за другом букв алфавита есть слово, то в любом данном алфавите есть сколь угодно длинные слова. Удобно ввести в рассмотрение слово, не содержащее никаких букв; такое слово называется *пустым словом*.

Два слова называют *равными* (графически равными), если они совпадают по написанию, т. е. состоят из одинаковых букв, одинаково расположенных.

Пусть символы A и B обозначают слова в каком-либо алфавите. Поставим в соответствие паре A, B слово AB, которое получается, если сначала написать слово A, а затем справа приписать к нему слово B. Слово AB называется *композицией* или *сочленением* слов A и B. Например, если

A обозначает слова *bac*, а B — слово *aba*, то AB есть слово *bacaba*. Композиция любого слова A с пустым словом считается, по определению, равной слову A.

Легко убедиться, что композиция слов обладает свойством ассоциативности, — для любых трех слов A, B, C композиция слов AB и C равна композиции слов A и BC. Поэтому и ту, и другую композицию будем записывать одинаково: ABC.

Слово B называется *обращением (зеркальным образом) слова* A, если B состоит из тех вхождений букв, что и A, но записанных в обратном порядке. Например, слово *bac* есть обращение слова *cab*, и наоборот. Слово называется *симметричным*, если оно совпадает со своим обращением; например, слова *шалаш*, *bab*, $0|0$ суть симметричные слова.

Слово A называется *подсловом слова* B, если найдутся такие слова C и E (возможно пустые), что $B=CAE$. Если A — подслово слова B, то говорят, что A входит в B. Для данных слов A и B слово A может иметь несколько вхождений в слово B. Ясно, что пустое слово является подсловом любого слова.

Слова в однобуквенном алфавите. Пусть $r=\{|\}$ — алфавит, состоящий из одной буквы «|», называемой вертикальной палочкой. Обозначим через N* множество всех слов в однобуквенном алфавите r. Множеству N* принадлежат пустое слово, обозначаемое символом 0*, слова $|$, $||$, $|||$, $||||$ и т. д. Если n — слово в алфавите r, то и $n|$ — тоже слово в этом алфавите.

Два элемента m и n из N* называют *равными* и пишут $m=n$, если они равны как слова (равны графически). Если слова m и n не равны, то пишут $m\neq n$.

ОПРЕДЕЛЕНИЕ. Пусть m и n — произвольные слова в алфавите r. Композиция слов m и n называется *суммой* m и n и обозначается $m\oplus n$. Операция $\oplus$ называется *операцией сложения*.

Например, композицией слов $||$ и $|||$ является слово $|||||$. Следовательно, $||\oplus|||=|||||$.

Композиция любого слова n из N* и пустого слова 0* есть, по определению, слово n. Следовательно, $n\oplus 0^*=n$, $0^*+n=n$.

Выше отмечалось, что композиция слов обладает свойством ассоциативности. В частности, для любых элементов m и n из N* верно равенство $m\oplus(n\oplus|)=(m\oplus n)\oplus|$ или, поскольку $n\oplus|=n|$, $m\oplus n|=(m\oplus n)|$. Свойство

ассоциативности композиции слов позволяет определить сумму трех слагаемых и более:

$$k \oplus m \oplus n = (k \oplus m) \oplus n,\ k \oplus m \oplus n \oplus l = (k \oplus m \oplus n) \oplus l \text{ и т. д.}$$

ОПРЕДЕЛЕНИЕ. *Произведением двух слов* m и n ($n \neq 0$) называется слово, равное сумме n слагаемых, каждое из которых равно m. Кроме того, полагаем $m \odot 0^* = 0^*$.

Произведение слов m и n обозначим $m \odot n$. Операция $\odot$ называется *умножением слов*. Таким образом,

$$m \odot n = \underbrace{m \oplus m \oplus \ldots \oplus m}_{n \text{ раз}}.$$

Например, для любого m из N^* имеем:

$$m \odot | = m,\ m \odot || = m \oplus m,\ m \odot ||| = m \oplus m \oplus m \text{ и т. д.}$$

Система натуральных чисел. Рассмотрим аксиоматический подход введения натуральных чисел.

ОПРЕДЕЛЕНИЕ. *Системой натуральных чисел* называется алгебра $\langle \mathbf{N}, +, \cdot, 0, 1 \rangle$, состоящая из некоторого множества $\mathbf{N}$, выделенных в $\mathbf{N}$ элементов 0 и 1, бинарных операций $+$ и $\cdot$ (называемых сложением и умножением соответственно), удовлетворяющих следующим условиям (аксиомам):

I. Для любого n из $\mathbf{N}$ $n + 1 \neq 0$.

II. Для любых m и n из $\mathbf{N}$, если $m + 1 = n + 1$, то $m = n$.

III. Для любого m из $\mathbf{N}$ $m + 0 = m$.

IV. Для любых m и n $m + (n + 1) = (m + n) + 1$.

V. Для любого m из $\mathbf{N}$ $m \cdot 0 = 0$.

VI. Для любых m и n из $\mathbf{N}$ $m \cdot (n + 1) = m \cdot n + m$.

VII. Если A — подмножество множества $\mathbf{N}$ такое, что (a) $0 \in A$, (b) для любого n, если $n \in A$, то $n + 1 \in A$, тогда $A = \mathbf{N}$.

Приведенную систему аксиом называют *системой аксиом Пеано*, так как она представляет собой несущественное изменение аксиоматики, предложенной итальянским математиком Пеано.

Условие I означает, что элемент 0 нельзя представить в виде суммы какого-нибудь элемента из $\mathbf{N}$ и элемента 1. Условие II означает, что элемент 1 является регулярным слева относительно сложения. Условие III означает, что 0 есть правый нейтральный элемент относительно сложения. Условие IV есть слабая форма ассоциативности сложения.

Условие VI есть слабая форма дистрибутивности умножения относительно сложения. Условие VII называется *аксиомой математической индукции*. Из этой аксиомы вытекает, что любое подмножество множества **N**, содержащее 0, 1 и замкнутое относительно сложения, совпадает с множеством **N**. Таким образом, из аксиомы математической индукции следует, что единственной подалгеброй алгебры $\mathscr{N} = \langle \mathbf{N}, +, \cdot, 0, 1 \rangle$ является сама алгебра $\mathscr{N}$.

Элементы множества **N** называются натуральными числами. Элементы 0 и 1 называются соответственно *нулем* и *единицей системы* $\mathscr{N}$.

Для записи чисел $1+1$, $(1+1)+1$, $((1+1)+1)+1$, $(((1+1)+1)+1)+1$, ... используется обычная десятичная символика: 2, 3, 4, 5, ...

Возникает вопрос: существует ли хотя бы одна система натуральных чисел, т. е. алгебра типа (2, 2, 0, 0), удовлетворяющая аксиомам I—VII? Следующий пример дает положительный ответ на поставленный вопрос.

Рассмотрим множество N* в однобуквенном алфавите r. Раньше уже были определены операции $\oplus$ и $\odot$ над словами алфавита r. Пустое слово 0* и слово $|$ играют роль нуля и единицы соответственно в алгебре:

$$\mathscr{N}^* = \langle \mathrm{N}^*, \oplus, \odot, 0^*, | \rangle.$$

Эта алгебра удовлетворяет системе аксиом I—VII. В самом деле, для любого n из N* слово $n|$ не является пустым; следовательно, $n \oplus | \neq 0^*$, значит выполнено условие I. Поскольку для любых m, $n \in \mathrm{N}^*$ из графического равенства слов $m|$ и $n|$ следует графическое равенство слов m и n, то выполнено и условие II. Композиция любого слова m из N* и пустого слова 0* есть слово m, $m \oplus 0^* = m$, т. е. выполнено условие III. Из свойства ассоциативности композиции слов следует выполнение условия IV. Выполнение условия V непосредственно следует из определения операции умножения слов. Из графического равенства слов

$$\underbrace{mm\ldots m}_{n+1 \text{ раз}} \quad \text{и} \quad \underbrace{mm\ldots mm}_{n \text{ раз}}$$

следует равенство $m \odot (n \oplus |) = (m \odot n) \oplus m$, т. е. условие VI также выполняется. Наконец, интуитивно ясно, что в алгебре $\mathscr{N}^*$ выполняется аксиома индукции: если множество $A \subset \mathrm{N}^*$ такое, что (a) $0^* \in A$ и (b) для каждого n, если $n \in A$, то и $n| \in A$, тогда $A = \mathrm{N}^*$. В самом деле,

обозначим через $A(n)$ предикат «$n \in A$»; запишем цепочку верных в силу (b) для любого n импликаций:

$$A(0^*) \to A(|),\ A(|) \to A(||),\ \ldots,\ A(n) \to A(n|).$$

Так как $A(0^*)$ истинно, то из первой импликации следует истинность $A(|)$; из истинности $A(|)$ и второй импликации следует истинность $A(||)$ и т. д. Через $n+1$ шагов мы получим истинность $A(n|)$ для любого n из $\mathbf{N}^*$.

Принцип математической индукции. Аксиома математической индукции является основой метода доказательства по индукции. Доказательство по индукции применимо, когда хотят доказать, что какой-нибудь одноместный предикат с натуральной свободной переменной (одноместное условие) истинен для всех натуральных чисел.

ТЕОРЕМА 1.1. *Пусть $A(n)$ — любой одноместный предикат на множестве* $\mathbf{N}$ *натуральных чисел, удовлетворяющий условиям: (α) $A(0)$ истинно (0 удовлетворяет предикату $A(n)$); (β) для каждого n из* $\mathbf{N}$, *если $A(n)$ истинно, то истинно $A(n+1)$. Тогда $A(n)$ истинно для любого натурального n.*

Доказательство. Пусть $A = \{n \in \mathbf{N} \mid A(n)\}$. В силу ($\alpha$) и ($\beta$) выполняются условия: (a) $0 \in A$, (b) для любого n из $\mathbf{N}$, если $n \in A$, то $n+1 \in A$. По аксиоме VII отсюда следует, что $A = \mathbf{N}$. Последнее равенство означает, что любое натуральное число n удовлетворяет условию $A(n)$. □

Теорема 1.1 есть, в сущности, другая формулировка аксиомы математической индукции, и ее будем называть *принципом математической индукции.* Принцип математической индукции можно записать в виде

$$A(0) \wedge \forall n\,(A(n) \to A(n+1)) \to \forall n A(n)$$

или в виде

$$\frac{A(0) \wedge \forall n\,(A(n) \to A(n+1)}{\forall n A(n)}.$$

Основные этапы доказательства по индукции: 1) доказывается, что 0 удовлетворяет условию A; 2) доказывается, что для всякого n из $A(n)$ следует $A(n+1)$. Переменную n называют *переменной, по которой производится индукция.* Часть доказательства «верно, что $A(0)$» называется *началом индукции* или *базисом индукции.* Вторая часть доказательства «для любого n из $A(n)$ следует $A(n+1)$» называется *индукционным шагом.* Посылка «$A(n)$» называется *индуктивным предположением.*

Для доказательства утверждения

$$\forall n\,(A(n) \to A(n+1))$$

берут произвольное натуральное число, обозначают его какой-нибудь буквой, например k, и доказывают импликацию $A(k) \to A(k+1)$ обычным путем: предполагают, что $A(k)$ истинно (индуктивное предположение), и показывают, что тогда истинно $A(k+1)$.

Упражнения

1. Докажите индукцией по n, что $1+2+\ldots+n=n(n+1)/2$.

2. Докажите индукцией по n, что множество из n элементов имеет 2^n подмножеств.

3. Пусть A и B — конечные множества, состоящие из m и n элементов соответственно. Докажите индукцией по n, что:

(a) число инъективных отображений множества A в B равно $n(n-1)\ldots(n-m+1)$,

(b) число всевозможных отображений множества A в B равно n^m.

4. Докажите, что если A — подмножество множества натуральных чисел и для некоторого n_0 из A выполняется условие: если для каждого натурального числа n при $n \geqslant n_0$ из $n \in A$ следует $n+1 \in A$, то каждое натуральное число $n \geqslant n_0$ принадлежит множеству A.

5. Докажите индукцией по n, что композиция инъективных функций $f_n \circ f_{n-1} \circ \ldots \circ f_1$ является инъективной функцией.

6. Докажите следующее утверждение (принцип Дирихле): если требуется разложить более чем n предметов по n местам, то по крайней мере на одно место придется положить более чем один предмет.

7. Запишите аксиомы I—VII системы натуральных чисел на языке логики предикатов (заменив аксиому VII эквивалентным ей принципом индукции).

8. Приведите пример алгебры типа (2, 2, 0, 0), которая:

(a) удовлетворяет аксиомам II, VII и не удовлетворяет аксиоме I (системы $\mathscr{N}^\circ$);

(b) удовлетворяет аксиомам I, VII и не удовлетворяет аксиоме II (системы $\mathscr{N}^\circ$);

(c) удовлетворяет аксиомам I, II и не удовлетворяет аксиоме VII (системы $\mathscr{N}^\circ$).

§ 2. СВОЙСТВА СЛОЖЕНИЯ И УМНОЖЕНИЯ НАТУРАЛЬНЫХ ЧИСЕЛ

Свойства сложения. Сложение натуральных чисел удовлетворяет следующим условиям (аксиомам):

IV. Для каждого m из $\mathbf{N}$ $m+0=m$.

V. Для любых m и n из $\mathbf{N}$ $m+(n+1)=(m+n)+1$.

Эти условия дают возможность для любого фиксированного натурального числа m вычислить значение суммы $m+n$ последовательно для значений n, равных 0, 1, 2, ... Следовательно, эти условия позволяют найти значение суммы $m+n$ для любых натуральных чисел m и n.

Например, пусть $m=5$ и $n=3$. Используя условия III, IV и V, можно выписать следующую цепочку равенств:

$5+0=5; 5+1=6; 5+2=5+(1+1)=(5+1)+1=6+1=7;$
$5+3=5+(2+1)=(5+2)+1=7+1=8;$ таким образом, $5+3=8$.

ТЕОРЕМА 2.1. *Сложение натуральных чисел ассоциативно, т. е. для любых натуральных a, b, c*

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

Доказательство. Зафиксируем произвольные натуральные числа a и b. Тогда формула (1) определяет предикат от одной свободной переменной c, обозначим его $A(c)$. Доказательство проводится индукцией по натуральной переменной c.

Базис индукции: $A(0)$ истинно, поскольку верно равенство $a+(b+0)=(a+b)+0$.

Индукционный шаг. Предположим, что для некоторого натурального n истинно $A(n)$, т. е. верна формула

$$a+(b+n)=(a+b)+n,$$

и докажем, что тогда истинно $A(n+1)$, т. е. верна формула

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

В самом деле,

$$\begin{aligned} a+(b+(n+1)) &= a+((b+n)+1) && \text{(по аксиоме IV);}\\ &= (a+(b+n))+1 && \text{(по аксиоме IV);}\\ &= ((a+b)+n)+1 && \text{(по индуктивному предположению);}\\ &= (a+b)+(n+1) && \text{(по аксиоме IV).} \end{aligned}$$

Согласно принципу индукции, предикат $A(c)$ истинен для любого натурального c. Поскольку при доказательстве фиксировались произвольные a и b, то формула (1) верна для любых натуральных a и b. □

ОПРЕДЕЛЕНИЕ. Алгебра $\langle \mathbf{N}, +, 0\rangle$ называется *аддитивным моноидом натуральных чисел.*

ЛЕММА 2.2. *Для любых натуральных a и b*

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

Доказательство. Проведем доказательство индукцией по b. Зафиксируем произвольное натуральное число a.

Обозначим через $B(b)$ предикат, определяемый формулой (1). Условимся в этой лемме и в дальнейшем в аналогичных случаях говорить, что $B(b)$ является и обозначением соответствующей формулы.

Легко видеть, что верна формула

$B(0)$: $(a+1)+0=a+(0+1)$.

Предположим, что для некоторого натурального числа n верна формула

$B(n)$: $(a+1)+n=a+(n+1)$,

и покажем, что верна формула $B(n+1)$. В самом деле,

$$\begin{aligned}(a+1)+(n+1)&=((a+1)+n)+1 \text{ (по аксиоме IV);}\\ &=(a+(n+1))+1 \text{ (по индуктивному предположению);}\\ &=a+((n+1)+1) \text{ (по аксиоме IV).}\end{aligned}$$

Согласно принципу индукции, формула $B(b)$ верна для любого натурального b. Так как при доказательстве фиксировалось произвольное значение a, то формула (1) верна для любых натуральных a и b. □

ТЕОРЕМА 2.3. *Сложение натуральных чисел коммутативно, т. е. для любых натуральных a, b*

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

Доказательство проводится индукцией по b. Докажем сначала, что верна формула

$A(0)$: $a+0=0+a$.

Проведем индукцию по a. Очевидно, формула верна при $a=0$. Далее, если для некоторого натурального числа n

$n+0=0+n$,

то

$$\begin{aligned}(n+1)+0&=n+(0+1) \text{ (по лемме 2.2);}\\ &=(n+0)+1 \text{ (по аксиоме IV);}\\ &=(0+n)+1 \text{ (по индуктивному предположению);}\\ &=0+(n+1) \text{ (по аксиоме IV).}\end{aligned}$$

Следовательно, по принципу индукции, формула $A(0)$ верна для любого a.

Зафиксируем произвольное a. Обозначим через $A(b)$ предикат, определяемый формулой (1). Предположим, что для некоторого натурального числа n верна формула

$A(n)$: $a+n=n+a$;

тогда

$$\begin{aligned} a+(n+1) &= (a+n)+1 \text{ (по аксиоме IV);} \\ &= (n+a)+1 \text{ (по индуктивному предположению);} \\ &= n+(a+1) \text{ (по аксиоме IV);} \\ &= (n+1)+a \text{ (по лемме 2.2),} \end{aligned}$$

т. е. верна формула $A(n+1)$. Согласно принципу индукции, формула $A(b)$ верна для любого b. Поскольку фиксировалось произвольное значение a, то формула (1) верна для любых натуральных a и b. □

ТЕОРЕМА 2.4 (ЗАКОН СОКРАЩЕНИЯ ДЛЯ СЛОЖЕНИЯ). *Для любых натуральных* a, b, c

(1) *если* $a+c=b+c$, то $a=b$.

Доказательство (проводится индукцией по c; при этом фиксируются произвольные значения a и b). Рассмотрим формулу

$A(c)$: $(a+c=b+c)\to(a=b)$.

Так как $a+0=a$ и $b+0=b$, то верно, что

$$(a+0=b+0)\to(a=b),$$

т. е. верна формула $A(0)$.

Предположим, что для некоторого натурального числа n

$A(n)$: $(a+n=b+n)\to(a=b)$,

и покажем, что тогда верна формула $A(n+1)$. По аксиоме IV,

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

Далее, по аксиоме II,

(3) $((a+n)+1=(b+n)+1)\to(a+n=b+n)$.

Из того, что $A(n)$ и (3) — верные формулы, следует, что верна формула

(4) $((a+n)+1=(b+n)+1)\to(a=b)$.

На основании (2) и (4) заключаем, что верна формула

$A(n+1)$: $(a+(n+1)=b+(n+1))\to(a=b)$.

Согласно принципу индукции, формула $A(c)$ верна для любого натурального c. Так как a и b фиксировались произвольно, утверждение (1) верно для любых натуральных a, b, c. □

СЛЕДСТВИЕ 2.5. *Для любых натуральных a и b, если $b\neq 0$, то $a\neq a+b$.*

ТЕОРЕМА 2.6. *Для любого натурального числа a либо $a=0$, либо существует такое натуральное число b, что $a=b+1$.*

Доказательство. Рассмотрим формулу

$A(a)$: $(a=0)\vee\exists b\,(a=b+1)$.

Доказательство этой формулы проводится индукцией по a. Очевидно, формула верна при $a=0$. Предположим, что для некоторого натурального числа n верна формула

$A(n)$: $(n=0)\vee\exists b\,(n=b+1)$.

Надо показать, что верна формула

$A(n+1)$: $(n+1=0)\vee\exists b\,(n+1=b+1)$.

Эта формула действительно верна, так как второй член дизъюнкции — истинная формула (при $b=n$, $n+1=b+1$). Согласно принципу индукции, формула $A(a)$ верна для любого натурального a. □

СЛЕДСТВИЕ 2.7. *Для любых натуральных a и b, если $a\neq 0$ или $b\neq 0$, то $a+b\neq 0$.*

Доказательство. Предположим, что $b\neq 0$. Тогда, по теореме 2.6, существует такое натуральное c, что $b=c+1$. В силу аксиомы IV

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

По аксиоме I, $(a+c)+1\neq 0$; следовательно, $a+b\neq 0$. □

СЛЕДСТВИЕ 2.8. *Для любых натуральных a и b, если $a+b=0$, то $a=0$ и $b=0$.*

ТЕОРЕМА 2.9. *Для любых натуральных a и b выполняется одно и только одно из трех условий:*
(α) $a=b$; (β) $a+k=b$ *(для некоторого $k\in\mathbf{N}\setminus\{0\}$)*;
(γ) $a=b+m$ *(для некоторого $m\in\mathbf{N}\setminus\{0\}$)*.

Доказательство. Из следствия 2.5 вытекает, что не может выполняться более чем одно из трех условий.

В самом деле, если бы выполнялись условия (α) и (β), то $a=a+k$ и $k\neq 0$, что невозможно по следствию 2.5. Если бы выполнялись условия (α) и (γ), то $b=b+m$ и $m\neq 0$, что невозможно. Если бы выполнялись условия (β) и (γ), то $a=a+(k+m)$ и $k+m\neq 0$, что также противоречит следствию 2.5.

Теперь покажем, что выполняется хотя бы одно из условий (α), (β), (γ). Фиксируем произвольное натуральное число a и обозначим через $A(b)$ дизъюнкцию условий (α), (β), (γ). Докажем индукцией по b верность формулы $A(b)$. Верна формула $A(0)$. В самом деле, если $b=0$, то либо $a=0$, либо $a\neq 0$. Если $a\neq 0$, то $a=0+m$, где $m=a\neq 0$. Следовательно, при $b=0$ выполняется условие (α) или условие (γ).

Предположим, что для некоторого числа n верна формула

$$A(n)\colon\ (a=n)\vee(a+k=n \text{ для некоторого } k\in\mathbf{N}\setminus\{0\})\vee(a=n+m \text{ для некоторого } m\in\mathbf{N}\setminus\{0\}),$$

и покажем, что тогда верна формула $A(n+1)$. В самом деле, если $a=n$, то $a+1=b+1$, — выполняется условие (β). Если $a+k=n$, $a+(k+1)=n+1$, выполняется условие (β). Если же $a=n+m$, то $a+1=(n+1)+m$ и $m\in\mathbf{N}\setminus\{0\}$. В этом случае если $m=1$, то $a+1=(n+1)+1$ и, по аксиоме II, $a=n+1$, — выполняется условие (α). Так как $m\neq 0$, то, по теореме 2.6, существует $k\neq 0$ такое, что $m=k+1$. Если $m\neq 1$, то $k\neq 0$, и из равенства $a+1=(n+1)+(k+1)=((n+1)+k)+1$ по аксиоме II получаем $a=(n+1)+k$, $k\neq 0$, — выполняется условие (γ). Итак, в любом случае верна формула $A(n+1)$. Согласно принципу индукции, формула $A(b)$ верна для любого натурального b. Поскольку a фиксировалось произвольно, то утверждение теоремы верно для любых натуральных a и b. □

ОПРЕДЕЛЕНИЕ. *Разностью двух натуральных чисел a и b* называется такое натуральное число k, что $b+k=a$.

Из теоремы 2.9 следует, что разность двух натуральных чисел a и b существует в том случае, когда выполнено условие (α) (при этом $k=0$) или (γ). В случае выполнения условия (β) разность чисел a и b не существует.

Легко показать, что если разность чисел a и b существует, то она единственна. В самом деле, если $b+k=a$ и $b+m=a$, то $b+k=b+m$, откуда, по закону сокращения для сложения, следует, что $k=m$.

Единственное натуральное число, являющееся разностью чисел a и b, обозначают $a-b$.

Свойства умножения. Пусть $\mathbf{N}$ — множество всех натуральных чисел.

Умножение натуральных чисел определяется следующими условиями (аксиомами):

V. $m \cdot 0 = 0$ для каждого m из $\mathbf{N}$.

VI. $m(n+1) = m \cdot n + m$ для любых m, n из $\mathbf{N}$.

Из этих условий следует, что

$m \cdot 1 = m$,

$m \cdot 2 = m(1+1) = m+m$,

$m \cdot 3 = m(2+1) = m \cdot 2 + m = (m+m)+m = m+m+m$ и т. д.

Таким образом, умножение является повторным сложением числа с самим собой.

ТЕОРЕМА 2.10 (ПРАВЫЙ ЗАКОН ДИСТРИБУТИВНОСТИ УМНОЖЕНИЯ ОТНОСИТЕЛЬНО СЛОЖЕНИЯ). *Для любых натуральных* a, b и c

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

Доказательство. Зафиксируем произвольные значения a и b. Определяемый при этом формулой (1) предикат обозначим через $A(c)$. Доказательство проводится индукцией по натуральной переменной c. По аксиоме V справедлива формула

$A(0)$: $(a+b) \cdot 0 = a \cdot 0 + b \cdot 0$.

Предположим, что для какого-нибудь натурального числа n верна формула

$A(n)$: $(a+b) \cdot n = a \cdot n + b \cdot n$.

Тогда имеем:

$$
\begin{aligned}
(a+b) \cdot (n+1) &= (a+b) \cdot n + (a+b) && \text{(по аксиоме VI);} \\
&= (a \cdot n + b \cdot n) + (a+b) && \text{(по индуктивному предположению);} \\
&= (a \cdot n + a) + (b \cdot n + b) && \text{(в силу ассоциативности и коммутативности сложения);} \\
&= a(n+1) + b(n+1) && \text{(по аксиоме VI),}
\end{aligned}
$$

т. е. верна формула $A(n+1)$. Согласно принципу индукции $A(c)$ верно для любого натурального c. Поскольку

фиксировались произвольные значения a и b, то формула (1) верна для любых натуральных a, b и c. □

ЛЕММА 2.11. *Для любого натурального числа* a $1 \cdot a = a$.

Доказательство (проводится индукцией по a). По аксиоме V, имеем $1 \cdot 0 = 0$. Предположим, что $1 \cdot n = n$ для какого-нибудь натурального числа n. Тогда $1 \cdot (n+1) = 1 \cdot n + 1 = n + 1$, т. е. $1 \cdot (n+1) = n+1$. Согласно принципу индукции, формула $1 \cdot a = a$ верна для любого натурального числа a. □

ТЕОРЕМА 2.12. *Умножение натуральных чисел коммутативно, т. е. для любых натуральных* a *и* b

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

Доказательство. Используя индукцию по a, покажем, что для любого a верна формула

$A(0)$: $a \cdot 0 = 0 \cdot a$.

Зафиксируем в формуле (1) произвольное значение a. Обозначим через $A(b)$ предикат, определяемый равенством (1). Предположим, что для какого-нибудь натурального числа n верна формула

$A(n)$: $a \cdot n = n \cdot a$.

Тогда имеем:

$$\begin{aligned} a \cdot (n+1) &= a \cdot n + a && \text{(по аксиоме VI);} \\ &= n \cdot a + a && \text{(по предположению индукции);} \\ &= n \cdot a + 1 \cdot a && \text{(по лемме 2.11);} \\ &= (n+1) \cdot a && \text{(по дистрибутивности умножения относительно сложения),} \end{aligned}$$

т. е. выполняется формула $A(n+1)$. Согласно принципу индукции, $A(b)$ верно для любого натурального b. Поскольку фиксировалось произвольное значение a, то формула (1) верна для любых натуральных a и b. □

Из теорем 2.10 и 2.12 вытекает следующая теорема.

ТЕОРЕМА 2.13 (ЛЕВЫЙ ЗАКОН ДИСТРИБУТИВНОСТИ УМНОЖЕНИЯ ОТНОСИТЕЛЬНО СЛОЖЕНИЯ). *Для любых натуральных* a, b, *и* c *выполняется равенство* $c(a+b) = c \cdot a + c \cdot b$.

ТЕОРЕМА 2.14. *Умножение натуральных чисел ассоциативно, т. е. для любых натуральных* a, b *и* c

(1) $a(bc) = (ab)c$.

Доказательство (проводится индукцией по c). Пусть $A(c)$ обозначает предикат, определяемый формулой (1) при фиксированных значениях a и b. По аксиоме V, имеем: $b \cdot 0 = 0$ и $(a \cdot b) \cdot 0 = 0$. Следовательно, верна формула

$A(0)$: $a(b \cdot 0) = (a \cdot b) \cdot 0$.

Предположим, что для какого-нибудь натурального числа n верна формула

$A(n)$: $a(b \cdot n) = (a \cdot b) \cdot n$.

Тогда имеем:

$$\begin{aligned} a \cdot (b \cdot (n+1)) &= a \cdot (b \cdot n + b) && \text{(по аксиоме VI);} \\ &= a \cdot (b \cdot n) + a \cdot b && \text{(по теореме 2.13);} \\ &= (a \cdot b) \cdot n + a \cdot b && \text{(по предположению индукции);} \\ &= (a \cdot b) \cdot n + (a \cdot b) \cdot 1 && \text{(по аксиоме V);} \\ &= (a \cdot b)(n+1) && \text{(по теореме 2.13),} \end{aligned}$$

т. е. верна формула $A(n+1)$. Согласно принципу индукции, формула $A(c)$ верна при любом натуральном c. Поскольку фиксировались произвольные значения a и b, то формула (1) верна для любых натуральных a, b и c. □

ОПРЕДЕЛЕНИЕ. Алгебра $\langle \mathbf{N}, \cdot, 1 \rangle$ называется *мультипликативным моноидом натуральных чисел.*

ТЕОРЕМА 2.15. *Для любых натуральных чисел a и b, если $a \neq b$ и $b \neq 0$, то $ab \neq 0$.*

Доказательство. Предположим, что $a \neq 0$ и $b \neq 0$. По теореме 2.6, существуют такие натуральные числа m и n, что $a = m + 1$ и $b = n + 1$. В силу аксиом VI и IV имеем

$$a \cdot b = a \cdot (n+1) = a \cdot n + a = a \cdot n + (m+1) = (a \cdot n + m) + 1.$$

По аксиоме I $(a \cdot n + m) + 1 \neq 0$. Следовательно, $a \cdot b \neq 0$. □

ТЕОРЕМА 2.16 (ЗАКОН СОКРАЩЕНИЯ ДЛЯ УМНОЖЕНИЯ). *Для любых натуральных a, b, c, если $ac = bc$ и $c \neq 0$, то $a = b$.*

Доказательство. По условию,

(1) $ac = bc$, $c \neq 0$.

Допустим, что $a \neq b$. По теореме 2.8, либо существует такое k, что $a + k = b$ и $k \neq 0$, либо существует такое m, что $a = b + m$ и $m \neq 0$. В первом случае $bc = ac + kc$ и в силу (1), $bc = bc + kc$, что (по следствию 2.5) невозможно,

так как $k \neq 0$, $c \neq 0$ и (по теореме 2.15) $kc \neq 0$. Во втором случае аналогичные рассуждения показывают, что допущение $a \neq b$ ведет к противоречию. □

Упражнения

1. Докажите формулы:

(a) $1+3+5+\ldots+(2n+1)=(n+1)^2$;

(b) $1^2+2^2+\ldots+n^2=n(n+1)(2n+1)/6$;

(c) $1\cdot 2+2\cdot 3+\ldots+(n-1)n=(n-1)n(n+1)/3$ для $n>1$;

(d) $(1+2+\ldots+n)^2=1^3+2^3+\ldots+n^3$;

(e) $1^2+3^2+\ldots+(2n-1)^2=n(2n-1)(2n+1)/3$.

2. Докажите, что число C_n^k подмножеств из k элементов множества из n элементов ($1 \leqslant k \leqslant n$) выражается формулой

$$C_n^k = \frac{n(n-1)\ldots(n-k+1)}{1\cdot 2\ldots k}.$$

3. Докажите, что $C_{n+1}^k = C_n^k + C_n^{k-1}$ для $n \geqslant k > 1$.

4. Докажите, что для любого натурального $n>1$

$$(x+1)^n = x^n + C_n^1 x^{n-1} + C_n^2 x^{n-2} + \ldots + C_n^n.$$

5. Докажите, что

$$1 + C_n^1 + C_n^2 + \ldots + C_n^n = 2^n.$$

6. Докажите, что $\sum\limits_{k=0}^{n} (C_n^k)^2 = C_{2n}^n$.

7. Докажите, что для любых натуральных чисел a, b, c и d сумма $a+b+c+d$ не зависит от порядка слагаемых.

§ 3. ОТНОШЕНИЕ ПОРЯДКА НА МНОЖЕСТВЕ НАТУРАЛЬНЫХ ЧИСЕЛ

Отношение порядка. Рассмотрим отношения порядка на множестве натуральных чисел.

ОПРЕДЕЛЕНИЕ. Если для натуральных чисел a и b существует такое натуральное число k, что $a+k=b$ и $k \neq 0$, то говорят, что «a меньше b», и пишут $a<b$. Говорят, что «a меньше или равно b», и пишут $a \leqslant b$, если $a<b$ или $a=b$.

Отношение, инверсное к отношению $<$, обозначают символом $>$. Таким образом, $a>b$ тогда и только тогда, когда $b<a$. Есла $a>b$ или $a=b$, то говорят, что «a больше или равно b», и пишут $a \geqslant b$. Отношение $\geqslant$ является *инверсией* к отношению $\leqslant$.

ТЕОРЕМА 3.1. *Для любых натуральных чисел a и b:*

(1) *если $a<b$, то $a+1 \leqslant b$;*

(2) $0 \leqslant a$;

(3) *если* $a \neq 0$, *то* $0 < a$;

(4) $a \leqslant b$ *тогда и только тогда, когда существует такое натуральное число* k, *что* $a + k = b$.

Доказательство теоремы легко следует из определений отношений $<$ и $\leqslant$ и предоставляется читателю.

ОПРЕДЕЛЕНИЕ. Алгебраическая система $\langle \mathbf{N}, +, \cdot, < \rangle$ называется *упорядоченной системой натуральных чисел.*

ТЕОРЕМА 3.2 (ЗАКОН ТРИХОТОМИИ ДЛЯ $<$). *Для любых натуральных чисел* a *и* b *выполняется одно и только одно из трех условий:* $a < b$, $a = b$, $a > b$.

Эта теорема непосредственно следует из определения отношения $<$ и теоремы 2.9.

СЛЕДСТВИЕ 3.3. *Для любых натуральных чисел* a *и* b *выполняются:*

(1) $a \leqslant a$ (*закон рефлексивности для* $\leqslant$);

(2) *либо* $a \leqslant b$, *либо* $b \leqslant a$ (*закон связанности для* $\leqslant$);

(3) *если* $a \leqslant b$ *и* $b \leqslant a$, *то* $a = b$ (*закон антисимметричности для* $\leqslant$).

ТЕОРЕМА 3.4. *Бинарное отношение* $<$ *на множестве натуральных чисел транзитивно, т. е. для любых натуральных чисел* a, b *и* c, *если* $a < b$ *и* $b < c$, *то* $a < c$.

Доказательство. Предположим, что $a < b$ и $b < c$. Тогда существуют натуральные числа k и m, удовлетворяющие условиям:

(1) $a + k = b$, $\quad b + m = c$;

(2) $k \neq 0$, $m \neq 0$.

В силу (1) $a + (k + m) = c$, причем в силу (2) и следствия 2.7 $k + m \neq 0$; следовательно, $a < c$. □

СЛЕДСТВИЕ 3.5. *Отношение* $<$ *на множестве натуральных чисел является отношением строгого линейного порядка. Система* $\langle \mathbf{N}, < \rangle$ *является линейно упорядоченным множеством.*

СЛЕДСТВИЕ 3.6. *Для любых натуральных чисел* a, b *и* c:

(1) *если* $a \leqslant b$ *и* $b < c$, *то* $a < c$;

(2) *если* $a < b$ *и* $b \leqslant c$, *то* $a < c$;

(3) *если* $a \leqslant b$ *и* $b \leqslant c$, *то* $a \leqslant c$.

СЛЕДСТВИЕ 3.7. *Бинарное отношение* $\leqslant$ *на множестве натуральных чисел является отношением нестрогого линейного порядка.*

ТЕОРЕМА 3.8. *Отношение* $<$ *монотонно относительно сложения и умножения, т. е. для любых натуральных чисел* a, b *и* c:

(1) $a<b$ *тогда и только тогда, когда* $a+c<b+c$;

(2) *если* $a<b$ *и* $c\neq 0$, *то* $ac<bc$.

Доказательство. Условие $a+c<b+c$ равносильно условию $a+c+k=b+c$ и $k\neq 0$ для некоторого натурального k, которое, по закону сокращения, равносильно условию $a+k=b$ и $k\neq 0$ для некоторого натурального k, т. е. условию $a<b$.

Предположим, что $a<b$ и $c\neq 0$. Существует такое натуральное число k, что $a+k=b$, $k\neq 0$. Умножив обе части равенства на c, получим $ac+kc=bc$. По теореме 2.15, $kc\neq 0$, поскольку $k\neq 0$ и $c\neq 0$; следовательно, $ac<bc$. □

СЛЕДСТВИЕ 3.9. *Отношение* $\leqslant$ *монотонно относительно сложения и умножения, т. е. для любых натуральных* a, b *и* c:

(1) $a\leqslant b$ *тогда и только тогда, когда* $a+c\leqslant b+c$;

(2) если $a\leqslant b$, *то* $ac\leqslant bc$.

ТЕОРЕМА 3.10. *Для любых натуральных чисел* a, b *и* c *из* $ac<bc$ *следует* $a<b$.

Доказательство. Согласно следствию 3.9, для любых натуральных a, b, c

если $b\leqslant a$, то $bc\leqslant ac$. Отсюда по закону контрапозиции вытекает утверждение:

если $ac<bc$, то $a<b$. □

Полная упорядоченность множества натуральных чисел.

ТЕОРЕМА 3.11. *Система* $\langle \mathbf{N}, <\rangle$ *является вполне упорядоченным множеством.*

Доказательство. По следствию 3.7, система $\langle \mathbf{N}, <\rangle$ есть линейно упорядоченное множество. Надо доказать, что любое непустое подмножество множества $\mathbf{N}$ натуральных чисел имеет наименьший элемент. Предположим, что существует непустое подмножество A множества $\mathbf{N}$, которое не имеет наименьшего элемента. Докажем индукцией по натуральной переменной b, что для всякого b верна формула

$A(b)$: $\quad a\in A\rightarrow b\leqslant a.$

Очевидно, формула верна при $b=0$, т. е.

$A(0)$: $\quad a\in A\rightarrow 0\leqslant a.$

Предположим, что для любого a и некоторого натурального числа n верна формула

$A(n)$: $a \in A \to n \leqslant a$.

Тогда $n \notin A$, ибо в противном случае n было бы наименьшим элементом множества A; поэтому $a \in A \to n < a$. Так как, по теореме 3.1, из $n < a$ следует $n+1 \leqslant a$, то

$A(n+1)$: $a \in A \to n+1 \leqslant a$.

Значит, для всякого натурального n верна импликация $A(n) \to A(n+1)$. Следовательно, доказано, что формула $A(b)$ верна для любого натурального b.

По предположению, множество A не пусто, следовательно, существует элемент $m \in A$. Полагая в формуле $A(b)$ $a = m$ и $b = m+1$, имеем $m \in A \to m+1 \leqslant m$. Отсюда, поскольку $m \in A$, получаем $m+1 \leqslant m$, т. е. получено противоречие. □

ТЕОРЕМА 3.12. *Пусть A — подмножество множества* **N** *всех натуральных чисел. Если для каждого натурального n выполняется условие*

(1) $(\forall m < n)(m \in A) \to n \in A$,

то $A = \mathbf{N}$.

Доказательство. Предположим, что $A \neq \mathbf{N}$. Тогда множество $\mathbf{N} \setminus A$ не пусто и (по теореме 3.11) имеет наименьший элемент; следовательно, существует натуральное число k, удовлетворяющее условиям:

(2) $k \in \mathbf{N} \setminus A$;

(3) $(\forall m < k)(m \in A)$.

В силу условия (1) верна импликация

(4) $(\forall m < k)(m \in A) \to k \in A$.

По правилу отделения из (3) и (4) следует $k \in A$, что в силу (2) невозможно. □

ТЕОРЕМА 3.13. *Пусть $A(x)$ — любой одноместный предикат на множестве* **N** *натуральных чисел. Если для всякого натурального числа n*

$(\forall m < n) A(m) \to A(n)$,

то $A(x)$ для любого натурального x.

Доказательство теоремы 3.13 легко следует из теоремы 3.12 и предоставляется читателю.

Упражнения

1. Покажите, что для любых натуральных чисел a, b, c и d:
(а) если $a < b$ и $c < d$, то $a+c < b+d$;
(б) если $a < b$ и $c < d$, то $ac < bd$.

2. Докажите, что для любых натуральных чисел a_i, b_i, если $a_1 < b_1$, $a_2 < b_2$, ..., $a_n < b_n$, то $a_1 a_2 \dots a_n < b_1 b_2 \dots b_n$.

3. Докажите, что для любых натуральных чисел a_i, b_i, если $0 < a_1 \leqslant b_1$, $0 < a_2 \leqslant b_2$, ..., $0 < a_n \leqslant b_n$, то

(1) $a_1 a_2 \dots a_n \leqslant b_1 b_2 \dots b_n$,

причем знак равенства в (1) имеет место тогда и только тогда, когда $a_1 = b_1$, ..., $a_n = b_n$.

4. Покажите, что для любых натуральных чисел a, b и c выполняется неравенство $ab + bc + ca \leqslant a^2 + b^2 + c^2$.

5. Докажите, что для любых натуральных чисел a, b и $n > 1$ верно неравенство $(a+b)^n \leqslant 2^{n-1}(a^n + b^n)$.

6. Докажите неравенства:

(a) $n^2 < 2^n$ для любого натурального $n \geqslant 4$;

(b) $2^n < n!$ для любого натурального $n \geqslant 4$;

(c) $n! < \left(\frac{n+1}{2}\right)^n$ для любого натурального $n > 1$.

7. Докажите индукцией по n неравенство Бернулли $(1+a)^n \geqslant 1 + na$, где a — любое действительное число, большее (-1).

§ 4. КОЛЬЦО ЦЕЛЫХ ЧИСЕЛ

Аддитивная группа целых чисел. Пусть $\mathscr{N} = \langle \mathbf{N}, +, \cdot, 0, 1 \rangle$ — система натуральных чисел. Операция вычитания в $\mathscr{N}$ не всегда выполнима, т. е. для данных натуральных чисел m и n уравнение $m + x = n$ относительно x не всегда имеет решение в $\mathbf{N}$. Только в том случае, когда $m \leqslant n$, уравнение имеет решение в $\mathbf{N}$, и притом единственное (по теореме 4.2.9); это решение называется *разностью чисел* n и m и обозначается через $n - m$.

Наша задача состоит в том, чтобы доказать существование такой аддитивной абелевой группы $\mathbb{Z}$, которая удовлетворяет условиям:

(1) множество $\mathbf{N}$ содержится в $|\mathbb{Z}|$ и сложение в группе $\mathbb{Z}$ продолжает сложение в $\mathscr{N}$;

(2) операция вычитания в $\mathbb{Z}$ всегда выполнима и всякий элемент группы $\mathbb{Z}$ можно представить в виде разности натуральных чисел.

Такую группу мы назовем *аддитивной группой целых чисел.*

ТЕОРЕМА 4.1. *Пусть* $\mathscr{N} = \langle \mathbf{N}, +, \cdot, 0, 1 \rangle$ — *система натуральных чисел. Существует абелева группа* $\mathbb{Z} = \langle \mathbf{Z}, +, - \rangle$, *удовлетворяющая условиям:*

(α) $\mathbf{N} \subset \mathbf{Z}$ *и сумма любых двух натуральных чисел* m *и* n *в группе* $\mathbb{Z}$ *совпадает с суммой этих элементов в* $\mathscr{N}$, *т. е.* $m + n = m + n$;

(β) *для любого элемента* a *из* $\mathbf{Z}$ *существуют такие натуральные числа* n *и* m, *что* $n + a = m$.

Доказательство. Рассмотрим множество $\mathbf{N}\times\mathbf{N}$ пар натуральных чисел. На нем определим бинарное отношение $\sim$ следующим образом:

(1) $\langle m, n\rangle \sim \langle r, s\rangle$ тогда и только тогда, когда $m+s = r+n$.

Непосредственная проверка показывает, что отношение $\sim$ является отношением эквивалентности на множестве $\mathbf{N}\times\mathbf{N}$.

На множестве $\mathbf{N}\times\mathbf{N}$ определим бинарную операцию $\oplus$ (сложение) и унарную операцию $\ominus$ формулами

(2) $\langle m, n\rangle \oplus \langle p, q\rangle = \langle m+p, n+q\rangle$;

(3) $\ominus \langle m, n\rangle = \langle n, m\rangle$.

Сложение пар коммутативно и ассоциативно. Это непосредственно следует из коммутативности и ассоциативности сложения натуральных чисел.

Непосредственная проверка показывает, что эквивалентность $\sim$ является конгруэнцией относительно операций $\oplus$ и $\ominus$, т. е. из

$$\langle m, n\rangle \sim \langle k, l\rangle \text{ и } \langle p, q\rangle \sim \langle r, s\rangle$$

следует

$$\langle m, n\rangle \oplus \langle p, q\rangle \sim \langle k, l\rangle \oplus \langle r, s\rangle$$

и из $\langle m, n\rangle \sim \langle k, l\rangle$ следует

$$\ominus \langle m, n\rangle \sim \ominus \langle k, l\rangle.$$

Обозначим через $[m, n]$ класс эквивалентности, содержащий пару $\langle m, n\rangle$. По теореме 3.1, операции $\oplus$, $\ominus$ (см. формулы (2) и (3)) индуцируют на фактор-множестве $Z_1 = \mathbf{N}\times\mathbf{N}/\sim$ операции $+$, $-$:

(4) $[m, n]+[p, q] = [m+p, n+q]$;

(5) $-[m, n] = [n, m]$.

В силу (1)

(6) $[m, n] = [r, s]$

тогда и только тогда, когда $m+s = r+n$.

Алгебра $\mathfrak{Z}_1 = \langle Z_1, +, -\rangle$ есть абелева группа. В самом деле, непосредственная проверка с помощью формул (4)—(6) показывает, что сложение в Z_1 коммутативно и ассоциативно. Элемент $[0, 0]$ является нейтральным относительно сложения в $\mathfrak{Z}_1$, так как ввиду (4) $[m, n]+[0, 0] = [m, n]$.

Элемент $-[m, n]$ противоположен элементу $[m, n]$, так как в силу (4)—(6)

$$[m, n]+(-[m, n])=[m, n]+[n, m]= \\ =[m+n, m+n]=[0, 0].$$

Это и означает, что алгебра $\mathfrak{Z}_1$ является абелевой группой.

Рассмотрим множество

$$\mathbf{N}^*=\{[0, k] \mid k \in \mathbf{N} \setminus \{0\}\}$$

Объединение множеств $\mathbf{N}$ и $\mathbf{N}^*$ обозначим через $\mathbf{Z}$:

$$\mathbf{Z}=\mathbf{N} \cup \mathbf{N}^*.$$

Определим отображение h множества Z_1 на $\mathbf{Z}$ следующим образом:

$h([m \pm k, m])=k$ для любого k из $\mathbf{N}$;

$h([n, n \pm k])=[n, n \pm k]$ для любого k из $\mathbf{N} \setminus \{0\}$.

Легко видеть, что h является инъективным отображением множества Z_1 на $\mathbf{Z}$. Следовательно, существует обратное отображение h^{-1}, инъективное отображение множества $\mathbf{Z}$ на Z_1, удовлетворяющее условиям

$$h \circ h^{-1}=i_{\mathbf{Z}}, \quad h^{-1} \circ h=i_{Z_1},$$

где $i_{\mathbf{Z}}$ и i_{Z_1} — тождественные отображения $\mathbf{Z}$ и Z_1 соответственно.

Сложение в $\mathbf{Z}$ определим для любых a, b из $\mathbf{Z}$ формулой

(I) $a+b=h(h^{-1}(a)+h^{-1}(b))$,

а унарную операцию — определим формулой

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

Из формул (I) и (II) следуют формулы

(III) $h^{-1}(a+b)=h^{-1}(a)+h^{-1}(b)$,

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

Рассмотрим алгебру $\mathfrak{Z}=\langle \mathbf{Z}, +, - \rangle$. В силу (III) и (IV) алгебра $\mathfrak{Z}$ изоморфна абелевой группе $\mathfrak{Z}_1$. Отсюда следует, что алгебра $\mathfrak{Z}$ есть абелева группа. В самом деле, сложение в $\mathfrak{Z}$ коммутативно, так как в силу (I) и коммутативности сложения в $\mathfrak{Z}_1$ имеем

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

Сложение в $\mathfrak{Z}$ ассоциативно, так как в силу (I) и (II) получаем

$$a+(b+c)=h(h^{-1}(a)+h^{-1}(b+c))=h(h^{-1}(a)+$$
$$+h^{-1}(b)+h^{-1}(c))=h(h^{-1}(a+b)+h^{-1}(c))=(a+b)+c.$$

Натуральное число 0 является нейтральным элементом относительно сложения в $\mathfrak{Z}$, так как для любого a из $\mathbf{Z}$ имеем

$$a+0=h(h^{-1}(a)+h^{-1}(0))=h(h^{-1}(a)+[0,\ 0])=$$
$$=h(h^{-1}(a))=a.$$

Для любого a из $\mathbf{Z}$ верно равенство $a+(-a)=0$, поскольку

$$a+(-a)=h(h^{-1}(a)+h^{-1}(-a))=$$
$$=h(h^{-1}(a)+(-h^{-1}(a))=h\ ([0,\ 0])=0.$$

Следовательно, алгебра $\mathfrak{Z}$ является абелевой группой.

Покажем, что выполняется условие (α). В самом деле, в силу (I) для любых m, n из $\mathbf{N}$

$$m+n=h(h^{-1}(m)+h^{-1}(n))=h([m,\ 0]+[n,\ 0])=$$
$$=h([m+n,\ 0])=m+n,$$

т. е. сложение в $\mathfrak{Z}$ продолжает сложение в $\mathcal{N}$.

Покажем, что выполняется условие (β). Пусть a — любой элемент из $\mathbf{Z}$ и $h^{-1}(a)=[m,\ n]$; тогда

$$n+a=h(h^{-1}(n)+h^{-1}(a))=h([n,\ 0]+[m,\ n])=$$
$$=h([n+m,\ n])=m,\ \text{т. е. } n+a=m.$$

Следовательно, всякий элемент из $\mathbf{Z}$ можно представить в виде разности натуральных чисел: $a=m-n$.

Итак, установлено, что алгебра $\mathfrak{Z}=\langle \mathbf{Z},\ +,\ -\rangle$ является абелевой группой, удовлетворяющей условиям (α) и (β). □

ОПРЕДЕЛЕНИЕ. *Аддитивной группой целых чисел* называется абелева группа $\mathfrak{Z}=\langle \mathbf{Z},\ +,\ -\rangle$, удовлетворяющая условиям (α) и (β) теоремы 4.1.

Естественное умножение в аддитивной группе целых чисел. Пусть $\mathfrak{Z}_+=\langle \mathbf{Z},\ +,\ -\rangle$ — аддитивная группа целых чисел. По теореме 4.1, $\mathbf{N}\subset\mathbf{Z}$ и всякий элемент из $\mathbf{Z}$ можно представить как разность натуральных чисел; следовательно,

$$\mathbf{Z}=\{m-n\mid m,\ n\in\mathbf{N}\}.$$

В группе $\mathfrak{Z}_+$ определим умножение следующим образом: для любых элементов $m-n$ и $p-q$ из $\mathbf{Z}$ полагаем

(1) $(m-n)\cdot(p-q)=(mp+nq)-(mq+np)$,

где m, n, p, $q \in \mathbf{N}$ и mp, nq, mq, np — произведения натуральных чисел в системе $\mathscr{N}$.

Любой элемент из $\mathbf{Z}$ представим в виде разности натуральных чисел неоднозначно. Поэтому нам надо проверить, что произведение целых чисел, определяемое формулой (1), не зависит от способа представления их в виде разности натуральных чисел. Покажем, что для любого элемента $p-q$ множества $\mathbf{Z}$ из равенства

(2) $m-n=m'-n'$ $(m,\ n,\ m',\ n' \in N)$

следует равенство

(3) $(m'-n')\cdot(p-q)=(m-n)\cdot(p-q)$.

В самом деле, согласно определению (1),

$$(m'-n')(p-q)=(m'p+n'q)-(m'q+n'p).$$

Ввиду (1) и (4) достаточно проверить, что

(4) $(mp+nq)+(m'q+n'p)=(m'p+n'q)+(mq+np)$,

или

(5) $(m+n')p+(n+m')q=(m'+n)p+(n'+m)q$.

Ввиду (2) $m+n'=m'+n$. Следовательно, верны равенства (5), (4) и (3).

Столь же простая непосредственная проверка показывает, что для любых элементов $m-n$ и $p-q$ множества $\mathbf{Z}$ из равенств

$$m-n=m'-n' \text{ и } p-q=p'-q'$$

следует равенство

$$(m'-n')\cdot(p'-q')=(m-n)(p-q).$$

Итак, установлено, что умножение в группе $\mathbb{Z}_+$, определяемое формулой (1), не зависит от способа представления множителей в виде разности натуральных чисел.

ОПРЕДЕЛЕНИЕ. Умножение в аддитивной группе целых чисел $\mathbb{Z}_+$, определяемое формулой (1), называется *естественным умножением*.

Кольцо целых чисел. Сначала дадим определение.

ОПРЕДЕЛЕНИЕ. Кольцо $\mathscr{K}$ называется *кольцом целых чисел*, если аддитивная группа кольца $\mathscr{K}$ является аддитивной группой целых чисел и умножение в кольце $\mathscr{K}$ коммутативно и продолжает умножение натуральных чисел (в системе $\mathscr{N}$ натуральных чисел).

ТЕОРЕМА 4.2. *Пусть* $\langle \mathbf{Z}, +, -\rangle$ *— аддитивная группа целых чисел,* $\cdot$ *есть естественное умножение в ней и* 1 *— единица системы* N *натуральных чисел. Тогда алгебра* $\mathfrak{Z} = \langle \mathbf{Z}, +, -, \cdot, 1\rangle$ *является кольцом целых чисел.*

Доказательство. Покажем, что алгебра $\mathfrak{Z}$ есть коммутативное кольцо. По условию, алгебра $\langle \mathbf{Z}, +, -\rangle$ — аддитивная группа кольца — есть абелева группа, как аддитивная группа целых чисел.

Пусть a, b, c — произвольные элементы множества $\mathbf{Z}$. По теореме 4.1, их можно представить в виде разности натуральных чисел. Пусть

$$(1)\quad a = m - n,\ b = p - q,\ c = r - s\ (m, n, p, q, r, s \in N).$$

Естественное умножение в $\mathbf{Z}$ определяется формулой

$$(2)\quad a \cdot b = (m-n)\cdot(p-q) = (mp + nq) - (mq + np).$$

Естественное умножение коммутативно, так как

$$b \cdot a = (p-q)\cdot(m-n) = (pm + qn) - (pn + qm),$$

и коммутативно сложение и умножение натуральных чисел.

Естественное умножение ассоциативно. В самом деле, в силу (1) и (2) имеем:

$$\begin{aligned} a\cdot(b\cdot c) &= (m-n)[(p-q)(r-s)] = \\ &= (m-n)[(pr+qs)-(ps+qr)] = \\ &= (mpr+mqs+nps+nqr) - \\ &- (mps+mqr+npr+nqs); \\ (a\cdot b)\cdot c &= [(m-n)(p-q)](r-s) = \\ &= [(mp+nq)-(mq+np)](r-s) = \\ &= (mpr+nqr+mqs+nps) - \\ &- (mps+nqs+mqr+npr). \end{aligned}$$

Следовательно, в силу коммутативности сложения натуральных чисел $a\cdot(b\cdot c) = (a\cdot b)\cdot c$.

Элемент 1 является нейтральным относительно естественного умножения. В самом деле, для любого a из $\mathbf{Z}$ имеем

$$a \cdot 1 = (m-n)(1-0) = m\cdot 1 - n\cdot 1 = m - n = a.$$

Следовательно, алгебра $\langle \mathbf{Z}, \cdot, 1\rangle$ является коммутативным моноидом.

Естественное умножение дистрибутивно относительно сложения. Действительно,

$$(a+b)\cdot c=[(m+p)-(n+q)](r-s)=$$
$$=(mr+pr+ns+qs)-(ms+ps+nr+qs);$$
$$ac+bc=[(mr+ns)-(ms+nr)]+[(pr+qs)-(ps+qr)]=$$
$$=(mr+ns+pr+qs)-(ms+nr+ps+qr).$$

Следовательно, $(a+b)\cdot c=a\cdot c+b\cdot c$. Поскольку естественное умножение коммутативно, то имеет место также равенство $c(a+b)=ca+cb$.

Итак, установлено, что алгебра $\mathbb{Z}$ является коммутативным кольцом.

Естественное умножение продолжает умножение натуральных чисел в системе $\mathscr{N}=\langle \mathbf{N}, +, \cdot, 0, 1\rangle$. В самом деле, для m и n из $\mathbf{N}$

$$m\cdot n=(m-0)(n-0)=(m\cdot n+0\cdot 0)-(m\cdot 0+n\cdot 0)=m\cdot n.$$

Кроме того, по условию, аддитивная группа кольца $\mathbb{Z}$ является аддитивной группой целых чисел. Следовательно, кольцо $\mathbb{Z}$ является кольцом целых чисел. □

ОПРЕДЕЛЕНИЕ. Если для целых чисел a и b существует такое натуральное число k, что $a+k=b$ и $k\neq 0$, то говорят, что «a меньше b», и пишут $a<b$. Говорят, что «a меньше или равно b», и пишут $a\leqslant b$, если $a<b$ или $a=b$.

Отношение, обратное к отношению $<$, обозначают символом $>$. Таким образом, $a>b$ тогда и только тогда, когда $b<a$.

ТЕОРЕМА 4.3. *Пусть* $\mathbb{Z}=\langle \mathbf{Z}, +, -, \cdot, 1\rangle$ *кольцо целых чисел. Тогда*

(1) *для любых целых чисел* a *и* b *выполняется одно и только одно из трех условий:* $a<b$, $a=b$, $b<a$;

(2) *для любого целого числа* a *выполняется одно и только одно из трех условий:* $a<0$, $a=0$, $0<a$;

(3) *отношение* $<$ *монотонно относительно сложения, т. е. для любых целых* a, b *и* c

$a<b$ *тогда и только тогда, когда* $a+c<b+c$;

(4) *отношение* $<$ *монотонно относительно умножения, т. е. для любых целых* a, b *и* c

если $a<b$ *и* $c>0$, *то* $ac<bc$.

Доказательство теоремы предоставляется читателю.

Теорема о делении с остатком. Пусть a — целое число и b — натуральное число, отличное от нуля. Разделить

число a на b с остатком — значит представить его в виде $a=bq+r$, где $0\leqslant r<b$, q и r — целые числа. При этом q называется *неполным частным*, а число r — *остатком* от деления a на b.

Деление с остатком всегда выполнимо, а неполное частное и остаток однозначно определяются делимым и делителем, как показывает следующая теорема.

ТЕОРЕМА 4.4. *Для любых целых чисел a, b при $b>0$ существует единственная пара целых чисел q и r, удовлетворяющая условиям*:

(1) $a=bq+r$ *и* $0\leqslant r<b$.

Доказательство. Докажем, что существует хотя бы одна пара чисел q, r, удовлетворяющая условиям (1). Вначале рассмотрим случай, когда a — натуральное число. Фиксируем b и индукцией по a докажем, что

(2) *существует пара целых чисел q, r, удовлетворяющая* (1).

Для $a=0$ утверждение (2) верно, так как $0=b\cdot 0+0$. Предположим, что (2) верно для $a=n$, т. е. существуют целые q, r такие, что

(3) $n=bq+r$ и $0\leqslant r<b$,

и докажем, что оно верно для $a=n+1$. Из (3) следует $n+1=bq+(r+1)$ и $0<r+1\leqslant b$. Если $r+1<b$, то пара чисел q, $r+1$ является искомой. Если же $r+1=b$, то $n+1=b(q+1)$ и пара чисел $q+1$, 0 является искомой.

Рассмотрим теперь случай, когда $a<0$; в этом случае $-a>0$. По доказанному выше, для пары чисел $-a$, b существуют такие целые числа q', r', что $-a=bq'+r'$ и $0\leqslant r'<b$. Если $r'=0$, то $a=b(-q')+0$. Если же $r'>0$, то $a=b(-q'-1)+(b-r')$ и $0<b-r'<b$.

Полагая $q=-q'-1$ и $r=b-r'$, получаем

$$a=bq+r \text{ и } 0<r<b.$$

Итак, доказано, что для любых целых чисел a, b при $b>0$ существует хотя бы одна пара целых чисел q, r, удовлетворяющая условиям (1).

Осталось доказать, что существует единственная пара целых чисел, удовлетворяющая условиям (1). Допустим, что для целого числа a существует два представления:

(4) $a=bq+r$, $0\leqslant r<b$;

(5) $a=bq_1+r_1$, $0\leqslant r_1<b$.

Допустим, что $r \neq r_1$. Тогда $r > r_1$ или $r_1 > r$. Если $r > r_1$, то в силу (4) и (5)

(6) $0 < r - r_1 < b$;

(7) $r - r_1 = b(q_1 - q)$.

Из (6) и (7) следует, что $q_1 - q > 0$ и, значит, $q_1 - q \geqslant 1$. Отсюда в силу (7) вытекает неравенство $r - r_1 \geqslant b$, которое противоречит (6). Аналогично убеждаемся, что невозможен случай $r_1 > r$. Следовательно, $r = r_1$ и в силу (4), (5) $b(q - q_1) = 0$. Так как $b \neq 0$, то $q - q_1 = 0$ и $q = q_1$. □

Отношение делимости в кольце целых чисел. Рассмотрим простейшие свойства делимости в кольце целых чисел.

Определение. Пусть a и b — целые числа. Говорят, что b делит a, если $a = bq$ для некоторого целого q. Вместо «b делит a» говорят также, что a делится на b, или что a кратно b, и пишут $b \mid a$ или $a \vdots b$. В противном случае говорят, что *a не делится на b, a не кратно b, b не делит a, b не является делителем a*, и пишут $b \nmid a$.

Теорема 4.5. *Пусть a, b, c, d, m, n — любые целые числа. Тогда*

(1) $a \mid a$;

(2) $a \mid 0$;

(3) *если* $0 \mid a$, *то* $a = 0$;

(4) $\pm 1 \mid a$;

(5) *если* $a \mid b$ *и* $b \mid c$, *то* $a \mid c$, т. е. *отношение делимости транзитивно*;

(6) *если* $c \mid a$, *то* $c \mid ab$;

(7) *если* $c \mid a$ *и* $c \mid b$, *то* $c \mid (a \pm b)$;

(8) *если* $b \mid a$, *то* $bc \mid ac$;

(9) *если* $c \neq 0$, *то из* $bc \mid ac$ *следует* $b \mid a$;

(10) *если* $a \mid c$ *и* $b \mid d$, *то* $ab \mid cd$;

(11) *если* $a \mid b$ *и* $a \mid c$, *то* $a \mid (mb + nc)$.

Свойства (1)—(11) отношения делимости легко следуют из определения делимости и свойств кольца $\mathbb{Z}$. Их доказательство предоставляется читателю.

Лемма 4.6. *Если произведение ab натуральных чисел равно единице, то $a = b = 1$.*

Доказательство. Из условия $ab = 1$ следует, что a и b отличны от нуля. По теореме 2.6, их можно представить в виде $a = c + 1$, $b = d + 1$. Следовательно, $ab = cd + c + d + 1 = 1$ и $cd + c + d = 0$. Если сумма натураль-

ных чисел равна нулю, то в силу следствия 2.8 каждое слагаемое равно нулю. В частности, $c = d = 0$; следовательно, $a = b = 1$. □

Теорема 4.7. *Если целое число a делит единицу, то* $a = \pm 1$.

Доказательство. Предположим, что a делит единицу, т. е. $ab = 1$ для некоторого целого b. Тогда $a^2 b^2 = 1$. Так как a^2 и b^2 — натуральные числа, то, по лемме 4.6, $a^2 = 1$. Следовательно, по теореме 4.1,

(1) $(-a)(-a) = 1$.

Поскольку a или $-a$ является натуральным числом, то, по лемме 4.6, из $a^2 = 1$ и равенства (1) следует, что $a = 1$ или $-a = 1$. □

Теорема 4.8. *Если целые числа a и b ассоциированы (т. е. $a \mid b$ и $b \mid a$), то* $a = \pm b$.

Доказательство. По условию a делит b и b делит a, т. е. $b = ac$ и $a = bd$ для некоторых целых c и d, поэтому

(1) $a = acd$.

Если $a = 0$, то $b = 0 \cdot c = 0$ и теорема верна. Если же $a \neq 0$, то из (1) следует $cd = 1$. По теореме 4.7, из равенства $cd = 1$ следует, что $d = \pm 1$. Кроме того, $a = bd$; следовательно, $a = \pm b$. □

Упражнения

1. Пусть $m\mathbf{Z} = \{mx \mid x \in \mathbf{Z}\}$, где m — натуральное число. Покажите, что при $m \neq 0$ существует инъективное отображение множества $\mathbf{Z}$ на $m\mathbf{Z}$.

2. Пусть $\mathbb{Z}' = \langle \mathbf{Z}, +, - \rangle$ — аддитивная группа целых чисел. Покажите, что множество $m\mathbf{Z}$, где m — целое число, замкнуто в группе $\mathbb{Z}$, т. е. замкнуто относительно операций $+$ и $-$.

3. Покажите, что непустое множество целых чисел, замкнутое относительно сложения, не обязательно состоит из кратных фиксированного целого числа.

4. Покажите, что непустое множество целых чисел, замкнутое в группе $\mathbb{Z}$ (замкнутое относительно операций $+$ и $-$), состоит из кратных некоторого фиксированного целого числа.

5. Выясните, являются ли подгруппами относительно операций $+$, $-$ в аддитивной группе целых чисел следующие множества целых чисел:
   (a) множество всех четных чисел;
   (b) множество натуральных чисел;
   (c) множество нечетных чисел.

6. Пусть $\mathbb{Z} = \langle \mathbf{Z}, +, - \rangle$ и m — фиксированное целое число. Покажите, что алгебра $m\mathbb{Z} = \langle m\mathbf{Z}, +, - \rangle$ является подгруппой группы $\mathbb{Z}$. Покажите, что любая подгруппа группы $\mathbb{Z}$ совпадает с группой $m\mathbb{Z}$ для некоторого натурального m.

7. Докажите, что аддитивная группа целых чисел $\mathbb{Z}$ изоморфна подгруппе $m\mathbb{Z}$ при любом целом m, отличном от нуля.

8. Покажите, что кольцо $\mathbb{Z}$ целых чисел не имеет автоморфизмов, отличных от тождественного.

9. Докажите, что кольцо $\mathbb{Z}$ целых чисел не имеет подколец, отличных от $\mathbb{Z}$.

10. Пусть $\mathscr{K}$ — произвольное кольцо. Докажите, что существует единственный гомоморфизм кольца $\mathbb{Z}$ целых чисел в кольцо $\mathscr{K}$.

11. Пусть $\mathbf{Z}[\sqrt{2}] = \{m + n\sqrt{2} \mid m, n \in \mathbf{Z}\}$. Докажите, что алгебра $\mathbb{Z}[\sqrt{2}] = \langle \mathbf{Z}[\sqrt{2}], +, -, \cdot, 1\rangle$ типа (2, 1, 2, 0,), где $+, -, \cdot$ суть обычные операции над действительными числами, является коммутативным кольцом. Укажите нетривиальный автоморфизм этого кольца.

12. Докажите, что не существует гомоморфизмов кольца $\mathbb{Z}[\sqrt{2}]$ в кольцо $\mathbb{Z}[\sqrt{3}]$ и эти кольца не изоморфны.

13. Пусть $K = \{\langle a, b\rangle \mid a, b \in \mathbf{Z}\}$ и операции $+, -, \cdot, e$ на множестве K определяются следующим образом:

$\langle a, b\rangle + \langle c, d\rangle = \langle a + c, b + d\rangle$;

$-\langle a, b\rangle = \langle -a, -b\rangle$;

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

$e = \langle 1, 1\rangle$.

Покажите, что алгебра $\langle K, +, -, \cdot, e\rangle$ является коммутативным кольцом с делителями нуля.

14. Докажите, что для любого натурального n:

(a) $5^{2n} - 1$ делится на 24;

(b) $4^n + 6n - 1$ делится на 9;

(c) $10^{3n} - 1$ делится на 3^3;

(d) $3^{2n} + 5$ не делится на 8.

15. Докажите, что произведение любых трех последовательных целых чисел делится на 6.

16. Докажите, что для любого целого n:

(a) $n^3 - n$ делится на 3;

(b) $n^5 - n$ делится на 5;

(c) $n^7 - n$ делится на 7;

(d) $n(n^2 + 5)$ делится на 6;

(e) $n^5 - n$ делится на 30.

17. Покажите, что если целое число n не делится на 7, то $n^3 - 1$ или $n^3 + 1$ делится на 7.

18. Докажите, что для любых целых a и b:

(1) если $a \mid b$ и $b \neq 0$, то $|a| \leqslant |b|$,

(2) если $a \mid b$ и $|b| < |a|$, то $b = 0$.

19. Докажите, что для любых целых a и b

$$|ab| = |a| \cdot |b|, \quad |a + b| \leqslant |a| + |b|.$$

20. Докажите индукцией по n, что для любых целых $a_1, \ldots, a_n$ выполняется неравенство $a_1^2 + \ldots + a_n^2 > 0$, за исключением случая, когда $a_1 = \ldots = a_n = 0$.

21. Докажите, что любое непустое множество целых чисел, ограниченное снизу (сверху), имеет наименьший (наибольший) элемент.

22. Докажите, что для любого целого a и любого целого положительного b существует единственное целое число n такое, что $nb \leqslant a < (n+1)b$.

23. Докажите следующее обобщение теоремы о делении с остатком: для любых целых a и b при $b \neq 0$ существует единственная пара целых чисел q, r такая, что $a = bq + r$ и $0 \leqslant r < |b|$.

§ 5. ПОЛЯ. ПОЛЕ РАЦИОНАЛЬНЫХ ЧИСЕЛ

Понятие поля. Дадим основные определения.

ОПРЕДЕЛЕНИЕ. Элемент a кольца $\mathscr{K}$ называется *обратимым элементом кольца*, если в кольце существует такой элемент b, что $ab = ba = 1_{\mathscr{K}}$. При этом элементы a и b называются *взаимно обратными*.

ОПРЕДЕЛЕНИЕ. *Полем* называется коммутативное кольцо, в котором нуль отличен от единицы, $0_{\mathscr{K}} \neq 1_{\mathscr{K}}$, и всякий ненулевой элемент является обратимым элементом кольца.

ОПРЕДЕЛЕНИЕ. Пусть $\mathscr{F} = \langle F, +, -, \cdot, 1\rangle$ — поле. Группа $\langle F, +, -\rangle$ называется *аддитивной группой поля*. Ее нейтральный элемент называется *нулем поля* и обозначается символом 0 или $0_{\mathscr{F}}$.

Элемент 1, нейтральный относительно умножения, называется *единицей поля* и обозначается также символом $1_{\mathscr{F}}$.

ОПРЕДЕЛЕНИЕ. *Подполем поля* $\mathscr{F}$ называется подкольцо поля $\mathscr{F}$, в котором всякий ненулевой элемент обратим. Подполе поля $\mathscr{F}$, отличное от $\mathscr{F}$, называется *собственным подполем*.

Ясно, что всякое подполе является полем.

ОПРЕДЕЛЕНИЕ. Поле называется *простым*, если оно не имеет собственных подполей.

Простейшие свойства поля. Пусть a, b — элементы поля $\mathscr{F}$ и $b \neq 0$. Уравнение $bx = a$ имеет в поле решение ab^{-1}; легко проверить, что ab^{-1} является единственным решением уравнения. Элемент ab^{-1} обозначается символом $\frac{a}{b}$ или a/b.

ТЕОРЕМА 5.1. *Пусть* $\mathscr{F} = \langle F, +, -, \cdot, 1\rangle$ — *поле. Тогда для любых элементов* a, b, c *поля*:

(1) *если* $ab = 1$, *то* $a \neq 0$ *и* $b = a^{-1}$;

(2) *если* $ac = bc$ *и* $c \neq 0$, *то* $a = b$;

(3) *если* $ab = 0$, *то* $a = 0$ *или* $b = 0$;

(4) *если* $a \neq 0$ *и* $b \neq 0$, *то* $ab \neq 0$;

(5) $\frac{a}{b}=\frac{c}{d}$ *тогда и только тогда, когда* $ad=bc$, $b\neq 0$ и $d\neq 0$;

(6) $\frac{a}{b}\pm\frac{c}{d}=\frac{ad\pm bc}{bd}$;

(7) $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$;

(8) $\frac{a}{b}+\frac{(-a)}{b}=0$ и $-\left(\frac{a}{b}\right)=\frac{-a}{b}$;

(9) *если* $a\neq 0$ и $b\neq 0$, *то* $\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}$;

(10) $\frac{ac}{bc}=\frac{a}{b}$.

Доказательство. (1) Если $ab=1$, то $a\neq 0$, так как при $a=0$ $0\cdot b=1$ и $0=1$, что в поле невозможно. Поскольку $a\neq 0$, существует элемент a^{-1}, обратный a, и $b=(a^{-1}a)\,b=a^{-1}(ab)=a^{-1}1=a^{-1}$.

(2) Если $ac=bc$ и $c\neq 0$, то в поле существует элемент c^{-1} и $a=(ac)c^{-1}=(bc)c^{-1}=b$, т. е. $a=b$.

(3) Из $ab=0$ следует $a=0$ или $b=0$. В самом деле, если $a\neq 0$, то существует элемент a^{-1} и $b=(a^{-1}a)\,b=a^{-1}(ab)=a^{-1}0=0$.

(4) По закону контрапозиции, из (3) следует, что

$$\neg(a=0\vee b=0)\rightarrow\neg(ab=0),\quad \text{т. е.}\quad (a\neq 0\wedge b\neq 0)\rightarrow(ab\neq 0).$$

(5) Пусть $a/b=c/d$, т. е. $ab^{-1}=cd^{-1}$. Тогда $b\neq 0$, $d\neq 0$ и $ad=(ab^{-1})(bd)=cd^{-1}\cdot bd=cb$, т. е. $ad=cb$. Обратно: из равенства $ad=cb$ при $b\neq 0$, $d\neq 0$ следуют равенства $adb^{-1}d^{-1}=cbb^{-1}d^{-1}$ и $ab^{-1}=cd^{-1}$.

(6) Так как $a/b=ab^{-1}$ и $c/d=cd^{-1}$, то $\frac{a}{b}\pm\frac{c}{d}=ab^{-1}\pm$
$\pm cd^{-1}=add^{-1}b^{-1}\pm cbb^{-1}d^{-1}=(ad\pm bc)(bd)^{-1}=\pm$
$=(ad\pm bc)/bd$.

(7) При $b\neq 0$ и $d\neq 0$

$$\frac{a}{b}\frac{c}{d}=ab^{-1}cd^{-1}=ac(bd)^{-1}=\frac{ac}{bd}.$$

(8) При $b\neq 0$

$$\frac{a}{b}+\frac{(-a)}{b}=ab^{-1}+(-a)\,b^{-1}=(a-a)\,b^{-1}=0,$$

следовательно, $-(a/b) = -a/b$.

(9) Если $a \neq 0$ и $b \neq 0$, то $(a/b)^{-1} = (ab^{-1})^{-1} = ba^{-1} = b/a$.

(10) При $b \neq 0$ и $c \neq 0$

$$ac/bc = ac\,(bc)^{-1} = acc^{-1}b^{-1} = ab^{-1} = a/b. \quad \square$$

Поле рациональных чисел. Введем понятие поля частных области целостности.

ОПРЕДЕЛЕНИЕ. Поле $\mathscr{F}$ называется *полем частных области целостности* $\mathscr{K}$, если выполнены условия:

(α) $\mathscr{K}$ есть подкольцо поля $\mathscr{F}$;

(β) для любого x из F существуют такие элементы a, b кольца $\mathscr{K}$, что $x = ab^{-1}$.

ТЕОРЕМА 5.2. *Для любой области целостности* $\mathscr{K}$ *существует поле частных. Если* $\mathscr{F}$ *и* $\mathscr{P}$ *— поля частных кольца* $\mathscr{K}$, *то существует изоморфизм поля* $\mathscr{F}$ *на поле* $\mathscr{P}$, *переводящий каждый элемент кольца* $\mathscr{K}$ *в себя.*

Доказательство этой теоремы дано в гл. 13 (см. теоремы 13.21 и 13.22).

Кольцо $\mathbb{Z}$ целых чисел есть область целостности. Следовательно, по теореме 5.2, для кольца $\mathbb{Z}$ существует поле частных и любые два поля частных кольца $\mathbb{Z}$ изоморфны.

ОПРЕДЕЛЕНИЕ. *Полем рациональных чисел* называется поле частных кольца целых чисел. Элементы поля рациональных чисел называются *рациональными числами.*

Из определения следует, что любое рациональное число можно представить в виде частного целых чисел.

Отметим, что любое поле, изоморфное полю рациональных чисел, также является полем рациональных чисел.

Отношение порядка на множестве $\mathbf{Q}$ рациональных чисел вводится с помощью отношения порядка $<$ на множестве $\mathbf{Z}$ целых чисел.

ОПРЕДЕЛЕНИЕ. *Отношение* $<$ *на множестве* $\mathbf{Q}$ рациональных чисел определяется следующим образом: для любых двух рациональных чисел p/q и r/s, где p, $r \in \mathbf{Z}$ и q, $s \in \mathbf{N} \setminus \{0\}$, $\frac{p}{q} < \frac{r}{s}$ тогда и только тогда, когда $ps < qr$.

Нетрудно проверить, что $<$ на множестве $\mathbf{Q}$ рациональных чисел является отношением строгого порядка, продолжающим отношение порядка на множестве $\mathbf{Z}$ целых чисел.

ТЕОРЕМА 5.3. *Бинарное отношение* $<$ *на множестве* $\mathbf{Q}$ *рациональных чисел обладает следующими свойствами:*

(1) *для любых* a, b, c *из* $\mathbf{Q}$, *если* $a<b$ *и* $b<c$, *то* $a<c$;

(2) *для любых* a, b *из* $\mathbf{Q}$ *имеет место одно и только одно из трех соотношений:* $a<b$, $a=b$, $b<a$;

(3) *для любых* a, b, c *из* $\mathbf{Q}$, *если* $a<b$, *то* $a+c<b+c$;

(4) *для любых* a, b, c *из* $\mathbf{Q}$, *если* $a<b$ и $0<c$, *то* $ac<bc$.

Доказательство теоремы предоставляется читателю.

Упражнения

1. Выясните, какие из следующих множеств действительных чисел являются полями относительно обычных операций $+$, $-$, $\cdot$ над ними:

(a) все натуральные числа;

(b) все рациональные числа с нечетными знаменателями;

(c) все числа вида $a+b\sqrt{2}$ с рациональными a и b;

(d) все числа вида $a+b\sqrt{5}$ с рациональными a и b;

(e) все числа вида $a+b\sqrt[3]{2}$ с рациональными a и b;

(f) все числа вида $a+b\sqrt[3]{2}+c\sqrt[3]{4}$ с рациональными a, b и c.

2. Пусть K — множество всех матриц вида $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ с рациональными a и b. Докажите, что алгебра $\langle K, +, -, \cdot, e\rangle$, где $+$, $-$, $\cdot$ суть операции над матрицами и $e=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, является полем. Покажите, что это поле содержит такой элемент x, что $x^2=-e$.

3. Пусть F — множество всех матриц вида $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$ с рациональными a и b. Докажите, что алгебра $\mathcal{F}=\langle F, +, -, \cdot, e\rangle$, где $e=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, является полем. Покажите, что отображение $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \longmapsto a+b\sqrt{2}$ является изоморфизмом поля $\mathcal{F}$ на поле $\mathcal{Q}(\sqrt{2})$.

4. Какие из колец $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$ и $\mathbb{Z}_6$ являются полями?

5. Докажите, что поле не имеет делителей нуля.

6. Покажите, что каждое подкольцо поля является областью целостности.

7. Пусть a — ненулевой элемент поля. Докажите, что для любых целых чисел m и n выполняются равенства $a^{m+n}=a^m a^n$ и $(a^m)^n=a^{mn}$.

8. Пусть a, b и c — любые элементы поля $\mathcal{F}$. Докажите, что из равенства $ab=ac$ следует $b=c$ тогда и только тогда, когда $a\neq 0$.

9. Докажите, что пересечение любой совокупности подполей поля $\mathcal{F}$ есть подполе поля $\mathcal{F}$.

10. Докажите, что любая конечная область целостности является полем.

11. Покажите, что поле $\mathcal{Q}$ рациональных чисел не имеет подполей, отличных от $\mathcal{Q}$.

12. Докажите, что любое подполе поля $\mathcal{Q}(\sqrt{2})$ есть либо $\mathcal{Q}$, либо $\mathcal{Q}(\sqrt{2})$.

13. Опишите все подкольца поля $\mathcal{Q}$ рациональных чисел.

14. Пусть $\varphi: \mathcal{F}\to\mathcal{F}'$ есть кольцевой гомоморфизм поля $\mathcal{F}$ в поле $\mathcal{F}'$. Покажите, что образ поля $\mathcal{F}$ при отображении φ является подполем поля $\mathcal{F}'$.

15. Докажите, что кольцевой гомоморфизм поля $\mathcal{F}$ есть либо нулевое отображение, либо изоморфизм поля $\mathcal{F}$ на его образ.

16. Пусть $\varphi : \mathcal{F} \to \mathcal{F}'$ есть кольцевой гомоморфизм. Если $\mathcal{F}$ — поле, $a,\ b \in F$ и $b \neq 0$, то $\varphi(a/b) = \varphi(a)/\varphi(b)$; докажите.

17. Докажите, что тождественное отображение является единственным автоморфизмом поля $\mathbb{Q}$ рациональных чисел.

18. Покажите, что любое поле, состоящее из двух элементов, изоморфно полю $\mathbb{Z}_2$.

19. Докажите, что кольцо, изоморфное полю, само является полем.

20. Покажите, что не существует гомоморфизмов кольца $\mathbb{Z}_4$ в поле $\mathbb{Z}_5$.

21. Докажите, что алгебра, изоморфная полю, сама является полем.

22. Покажите, что поле частных поля $\mathcal{F}$ изоморфно $\mathcal{F}$.

23. Докажите, что поле частных кольца $\mathbb{Z}[\sqrt{3}]$ изоморфно полю $\mathbb{Q}(\sqrt{3})$.

24. Пусть $\mathcal{K}$ и $\mathcal{K}'$ — изоморфные области целостности. Докажите, что изоморфны поля частных этих колец.

§ 6. СИСТЕМА ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ

Упорядоченные поля. Алгебраическая система $\langle F, < \rangle$ называется *линейно упорядоченным множеством,* если выполнены следующие условия:

(α) для любых a, b, c из F, если $a < b$ и $b < c$, то $a < c$;

(β) для любой пары элементов a, b из F выполняется одно и только одно из трех соотношений: $a < b$, $a = b$, $b < a$.

ОПРЕДЕЛЕНИЕ. *Упорядоченным полем* называется алгебраическая система $\langle F, +, -, \cdot, 1, < \rangle$, удовлетворяющая условиям:

(1) алгебра $\langle F, +, -, \cdot, 1 \rangle$ есть поле;

(2) система $\langle F, < \rangle$ есть линейно упорядоченное множество;

(3) для любых a, b, c из F, если $a < b$, то $a + c < b + c$ (монотонность сложения);

(4) для любых a, b, c из F, если $a < b$ и $0 < c$, то $ac < bc$ (монотонность умножения).

Элемент a упорядоченного поля называется *положительным*, если $0 < a$. По определению, $b > a$ тогда и только тогда, когда $a < b$. Далее, по определению, $a \leqslant b$ тогда и только тогда, когда $a < b$ или $a = b$.

Пример. Пусть $\langle \mathbf{Q}, +, -, \cdot, 1 \rangle$ — поле рациональных чисел и $<$ — обычное отношение порядка на множестве $\mathbf{Q}$. В силу теоремы 5.3 условия (1) — (4) приведенного выше определения выполняются. Следовательно, система $\langle \mathbf{Q}, +, -, \cdot, 1 \rangle$ есть упорядоченное поле. Эта система называется *упорядоченным полем рациональных чисел.*

ТЕОРЕМА 6.1. *Пусть* $\mathcal{F} = \langle F, +, -, \cdot, 1, < \rangle$ *— упорядоченное поле и* a, b, c, d *— любые его элементы. Тогда*

(1) $a < b$ в том и только в том случае, *когда* $b - a > 0$;

(2) *для любого* a *из* F *выполняется одно и только одно из трех условий:* $a < 0$, $a = 0$, $0 < a$;

(3) *если* $a > 0$ *и* $b > 0$, *то* $a + b > 0$ *и* $ab > 0$, *т. е. множество положительных элементов упорядоченного поля замкнуто относительно сложения и умножения*;

(4) *если* $a < b$ *и* $c < d$, *то* $a + c < b + d$;

(5) *если* $a < b$ *и* $c < 0$, *то* $ac > bc$;

(6) *если* $a \neq 0$, *то* $a^2 > 0$;

(7) $1 > 0$ *и* $n \cdot 1 > 0$ *для всякого натурального* $n \neq 0$;

(8) *поле* $\langle F, +, -, \cdot, 1 \rangle$ *есть область целостности.*

Доказательство. (1) В силу монотонности сложения $a < b$ в том и только в том случае, когда $a + (-a) < b + (-a)$. Следовательно, $a < b$ тогда и только тогда, когда $b - a > 0$.

(2) Утверждение (2) справедливо в силу того, что $\langle F, < \rangle$ — линейно упорядоченное множество (см. условие (β)).

(3) Ввиду монотонности сложения из $a > 0$ и $b > 0$ следует $a + b > b$ и $a + b > 0$. В силу монотонности умножения из $a > 0$ и $b > 0$ следует $ab > 0 \cdot b$ и $ab > 0$.

(4) В силу монотонности сложения если $a < b$ и $c < d$, то $a + c < b + c$ и $b + c < b + d$. Следовательно, $a + c < b + d$.

(5) В силу (1) если $a < b$ и $c < 0$, то $b - a > 0$ и $-c > 0$. В силу монотонности умножения отсюда получаем $(b - a)(-c) > 0$ и $ac - bc > 0$. Следовательно, $ac > bc$.

(6) В силу монотонности умножения если $a > 0$, то $a^2 > 0$. Если же $-a > 0$, то $(-a)(-a) > 0$ и $a^2 > 0$.

(7) В поле $1 \neq 0$. В силу (6) $1^2 = 1 > 0$. Так как множество положительных элементов упорядоченного поля замкнуто относительно сложения, из $1 > 0$ следует, что $n \cdot 1 > 0$ для всякого отличного от нуля натурального n.

(8) В силу теоремы 5.1 для любых элементов a, b поля, если $a \neq 0$ и $b \neq 0$, то $ab \neq 0$. Следовательно, по закону контрапозиции, если $ab = 0$, то $a = 0$ или $b = 0$. Таким образом, поле $\langle F, +, -, \cdot, 1 \rangle$ является областью целостности. □

ОПРЕДЕЛЕНИЕ. *Абсолютное значение элемента* a упорядоченного поля обозначается через $|a|$ и определяется

следующим образом:

$$|a|=\begin{cases} a, \text{ если } a\geqslant 0, \\ -a, \text{ если } (-a)>0. \end{cases}$$

ТЕОРЕМА 6.2. *Пусть a и b — произвольные элементы упорядоченного поля; тогда*

(1) $|a|=|-a|$;

(2) $|a|\pm a\geqslant 0$;

(3) $|a+b|\leqslant|a|+|b|$;

(4) $|ab|=|a|\cdot|b|$;

(5) $|b|\leqslant a$ в том и только в том случае, когда $-a\leqslant b\leqslant a$.

Доказательство. (1) Равенство (1) непосредственно следует из определения абсолютного значения элемента.

(2) Если $a\geqslant 0$, то $|a|=a$, $|a|+a\geqslant 0$ и $|a|-a=0$. Если же $(-a)>0$, то $|a|=-a$, $|a|-a=|a|+(-a)>0$ и $|a|+a=0$.

(3) Если $|a+b|=a+b$, то в силу неравенства (2)

$$|a|+|b|-|a+b|=(|a|-a)+(|b|-b)\geqslant 0.$$

Если же $|a+b|=-(a+b)$, то также в силу (2)

$$|a|+|b|-|a+b|=(|a|+a)+(|b|+b)\geqslant 0.$$

Следовательно, в любом случае верно неравенство (3).

(4) Равенство (4) верно, если a или b равно нулю. Если элементы a и b положительны, то $|ab|=ab=|a|\cdot|b|$. Если $a<0$ и $b<0$, то $ab=(-a)(-b)>0$ и $|ab|=ab=(-a)(-b)=|a|\cdot|b|$. Если $a>0$ и $b<0$, то $(-ab)>0$ и $|ab|=-ab=a\cdot(-b)=|a|\cdot|b|$. Наконец, если $a<0$ и $b>0$, то $(-ab)>0$ и $|ab|=-ab=(-a)b=|a|\cdot|b|$.

(5) Неравенство $|b|\leqslant a$ имеет место тогда и только тогда, когда $(-b)\leqslant a$ и $b\leqslant a$. Поэтому $|b|\leqslant a$ тогда и только тогда, когда $-a\leqslant b$ и $b\leqslant a$, т. е. при $-a\leqslant b\leqslant a$. □

Система действительных чисел.

ОПРЕДЕЛЕНИЕ. Упорядоченное поле $\mathscr{F}$ называется *архимедовски упорядоченным*, если для любых положительных элементов a и b поля существует такое натуральное число n, что $na>b$.

Пусть $\langle a_0, a_1, a_2, \ldots\rangle$ — бесконечная последовательность элементов упорядоченного поля $\mathscr{F}$. Ее обозначают также через $\langle a_k\rangle_{k\in N}$ или $\langle a_k\rangle$.

ОПРЕДЕЛЕНИЕ. Элемент a упорядоченного поля $\mathscr{F}$ называется *пределом последовательности* $\langle a_k\rangle$ *элементов*

поля, если для каждого положительного элемента ε поля существует (зависящее от ε) натуральное число n_0 такое, что $|a_k - a| < \varepsilon$ для любого натурального $k \geqslant n_0$. Последовательность $\langle a_k \rangle$, имеющая предел в поле $\mathscr{F}$, называется *сходящейся* в этом поле.

ОПРЕДЕЛЕНИЕ. Последовательность $\langle a_k \rangle$ элементов упорядоченного поля $\mathscr{F}$ называется *фундаментальной* над $\mathscr{F}$, если для каждого положительного элемента ε поля существует (зависящее от ε) натуральное число n_0 такое, что $|a_k - a_n| < \varepsilon$ для любых натуральных k и n, больших, чем n_0.

ОПРЕДЕЛЕНИЕ. Упорядоченное поле называется *полным*, если всякая фундаментальная последовательность элементов поля сходится в этом поле.

ОПРЕДЕЛЕНИЕ. *Системой действительных чисел* называется полное архимедовски упорядоченное поле.

Пусть $\langle \mathbf{R}, +, -, \cdot, 1, < \rangle$ — система действительных чисел. Тогда алгебра $\langle \mathbf{R}, +, -, \cdot, 1 \rangle$ есть поле, называемое *полем действительных чисел*. Множество $\mathbf{R}$ называется *множеством действительных чисел*.

Можно доказать, что любые две системы действительных чисел изоморфны. Следовательно, изоморфны любые два поля действительных чисел.

ТЕОРЕМА 6.3. *Для любых действительных чисел a и b при $b > 0$ существует целое число m и действительное число r такие, что*

$$a = mb + r, \quad 0 \leqslant r < b.$$

Доказательство. 1°. Если $a = 0$, то полагаем $m = r = 0$. Предположим, что $a > 0$. Множество

$$M = \{n \in \mathbf{N} \mid (n+1)\, b > a\}$$

натуральных чисел не пусто, поскольку система действительных чисел архимедовски упорядочена. Так как множество натуральных чисел вполне упорядочено и M — непустое подмножество множества $\mathbf{N}$, то в M существует наименьший элемент. Пусть m — наименьший элемент множества M, тогда

$$mb \leqslant a < (m+1)\, b, \quad 0 \leqslant a - mb < b.$$

Полагая $a - mb = r$, получим $a = mb + r$, $0 \leqslant r < b$.

2°. Предположим, что $a < 0$. Тогда, по доказанному в п. 1°, для положительных чисел $(-a)$ и b существуют

натуральное число k и действительное число s такие, что

$$-a = kb + s,\ 0 \leqslant s < b.$$

Следовательно, $a = (-k)b + (-s)$. Если $s = 0$, то мы имеем искомое представление. Если же $s > 0$, то

$$a = (-k-1)\cdot b + (b-s).$$

Полагая $m = -k-1$ и $r = b-s$, имеем

$a = mb + r,\ 0 \leqslant r < b$. □

Пусть n — натуральное число, отличное от нуля. Введем понятие арифметического корня n-й степени из положительного действительного числа. Предварительно докажем следующую теорему.

ТЕОРЕМА 6.4. *Для любого положительного числа a существует единственное положительное действительное число c такое, что $c^n = a$.*

Доказательство. Рассмотрим функцию $f = x^n - a$, определенную на замкнутом интервале $[0, b]$, где $b = a + 1$. Функция f непрерывна на этом интервале и на его концах принимает значения разных знаков, так как $f(0) < 0 < f(b)$. Применим теорему о промежуточном значении к функции f на интервале $[0, b]$. По этой теореме, существует действительное число $c \in [0, b]$, для которого $c^n - a = 0$ и, значит,

(1) $c^n = a$.

Очевидно, $c > 0$. Предположим, что $d^n = a$ для какого-нибудь положительного числа d. Если при этом $c < d$, то $c^n < d^n = a$, что противоречит (1). Если же $c > d$, то $c^n > d^n = a$, что также противоречит (1). Следовательно, $d = c$. □

ОПРЕДЕЛЕНИЕ. Пусть a — положительное действительное число и n — натуральное число, отличное от нуля. Единственное положительное действительное число c такое, что $c^n = a$, называется *арифметическим* или *главным корнем n-й степени* из a и обозначается символом $c^{1/n}$ или $\sqrt[n]{c}$.

Построение системы действительных чисел. Последовательность $\langle a_0, a_1, a_2, \ldots \rangle$ рациональных чисел будем обозначать через $\langle a_k \rangle_{k \in \mathbf{N}}$ или $\langle a_k \rangle$. На множестве $\mathbf{Q}^{\mathbf{N}}$ всех последовательностей рациональных чисел определим бинарные операции $\oplus$, $\odot$, унарную операцию $\ominus$ и нульместную операцию $\bar{1}$:

$$\langle a_k \rangle \oplus \langle b_k \rangle = \langle a_k + b_k \rangle;$$

$$\ominus \langle a_k \rangle = \langle -a_k \rangle;$$

$$\langle a_k \rangle \odot \langle b_k \rangle = \langle a_k \cdot b_k \rangle;$$

$\bar{1} = \langle a_k \rangle$, где $a_k = 1$ для всякого натурального k.

Обозначим через $F(\mathbf{Q})$ множество всех фундаментальных последовательностей над полем $\mathbb{Q}$ рациональных чисел. Если $\langle a_k \rangle$ и $\langle b_k \rangle$ — произвольные элементы множества $F(\mathbf{Q})$, то последовательности $\langle a_k \rangle \oplus \langle b_k \rangle$, $\ominus \langle a_k \rangle$, $\langle a_k \rangle \odot \langle b_k \rangle$ также принадлежат множеству $F(\mathbf{Q})$. Следовательно, множество $F(\mathbf{Q})$ замкнуто относительно операций $\oplus$, $\ominus$, $\odot$. Нетрудно проверить, что алгебра $\langle F(\mathbf{Q}), \oplus, \ominus, \odot, \bar{1} \rangle$ является коммутативным кольцом.

На множестве $F(\mathbf{Q})$ введем бинарное отношение $\equiv$: $\langle a_k \rangle \equiv \langle b_k \rangle$ тогда и только тогда, когда последовательность $\langle a_k - b_k \rangle$ сходится к нулю.

Отношение $\equiv$ рефлексивно, транзитивно и симметрично, т. е. является отношением эквивалентности на множестве $F(\mathbf{Q})$. Условимся обозначать символом $[\langle a_k \rangle]$ класс эквивалентности, которому принадлежит последовательность $\langle a_k \rangle$. Множество всех классов эквивалентности обозначим через $\bar{F}$, $\bar{F} = F/\equiv$.

Нетрудно показать, что отношение $\equiv$ является отношением конгруэнтности в кольце $\langle F(\mathbf{Q}), \oplus, \ominus, \odot, 1 \rangle$. Это дает возможность определить на множестве $\bar{F}$ операции $+$, $-$, $\cdot$, 1 следующим образом:

$[\langle a_k \rangle] + [\langle b_k \rangle] = [\langle a_k + b_k \rangle]$;

$-[\langle a_k \rangle] = [\langle -a_k \rangle]$;

$[\langle a_k \rangle] \cdot [\langle b_k \rangle] = [\langle a_k \cdot b_k \rangle]$;

$1 = [\bar{1}]$.

Алгебра $\langle \bar{F}, +, -, \cdot, 1 \rangle$ есть фактор-алгебра кольца $\langle F(\mathbf{Q}), \oplus, \ominus, \odot, 1 \rangle$ по отношению конгруэнтности $\equiv$. Можно доказать, что алгебра $\langle \bar{F}, +, -, \cdot, 1 \rangle$ является полем.

На множестве $F(\mathbf{Q})$ введем *отношение порядка*: для любых $\langle a_k \rangle$ и $\langle b_k \rangle$ из $F(\mathbf{Q})$ полагаем

$$\langle a_k \rangle < \langle b_k \rangle,$$

если существуют натуральное число n_0 и положительное рациональное число ε такие, что $b_k - a_k \geqslant \varepsilon$ для всякого $k \geqslant n_0$.

Бинарное отношение $\equiv$ является отношением конгруэнтности относительно $<$, т. е. для любых $\langle a_k \rangle$, $\langle b_k \rangle$, $\langle c_k \rangle$ и $\langle d_k \rangle$ из $F(\mathbf{Q})$, если

$$\langle a_k \rangle < \langle b_k \rangle,\ \langle a_k \rangle \equiv \langle c_k \rangle \text{ и } \langle b_k \rangle \equiv \langle d_k \rangle,$$

то $\langle c_k \rangle < \langle d_k \rangle$.

Это дает возможность ввести на множестве $\bar{F}$ отношение порядка: для любых $[\langle a_k\rangle]$ и $[\langle b_k\rangle]$ из $\bar{F}$ полагаем

$[\langle a_k\rangle] < [\langle b_k\rangle]$, если $\langle a_k\rangle < \langle b_k\rangle$.

Можно доказать, что система $\bar{F} = \langle \bar{F}, +, -, \cdot, \mathbf{1}, < \rangle$ есть архимедовски упорядоченное поле и всякая фундаментальная последовательность над полем $\bar{\mathcal{F}}$ сходится к элементу этого поля. Таким образом, поле $\bar{\mathcal{F}}$ является полем действительных чисел.

Упражнения

1. Пусть $\mathcal{F} = \langle F, +, -, \cdot, 1, < \rangle$ — упорядоченное поле и $a, b, c, d \in F$. Докажите, что тогда:

(a) если $a + c < b + c$, то $a < b$;

(b) если $a - b < a - c$, то $b > c$;

(c) если $0 < c$ и $ac < bc$, то $a < b$;

(d) $0 < \frac{1}{a} \leftrightarrow a > 0$;

(e) если $0 < a < b$, то $0 < \frac{1}{b} < \frac{1}{a}$;

(f) если $a < b < 0$, то $0 > \frac{1}{a} > \frac{1}{b}$;

(g) если хотя бы одно из чисел a, b, c отлично от нуля, то $a^2 + b^2 + c^2 > 0$.

2. Пусть a, b — элементы упорядоченного поля $\mathcal{F}$ и $a < b$. Докажите, что в $\mathcal{F}$ существует такой элемент c, что $a < c < b$.

3. Докажите, что уравнение $x^2 = 2$ не имеет решений в поле рациональных чисел.

4. Докажите, что для любого положительного действительного числа a уравнение $x^2 = a$ имеет решение в поле действительных чисел.

5. Покажите, что уравнение $x^2 + 1 = 0$ не имеет решений в поле действительных чисел.

6. Пусть $\mathbf{R}^+$ — множество всех положительных действительных чисел. Докажите, что алгебра $\langle \mathbf{R}^+, \cdot, ^{-1} \rangle$ является группой; она называется *мультипликативной группой положительных действительных чисел.*

7. Пусть a, b, c и d — положительные действительные числа. Докажите, что $a/b = c/d$ тогда и только тогда, когда для любых целых положительных чисел m и n $na > mb \rightarrow nc > md$ и $na < mb \rightarrow nc < md$.

8. Докажите, что тождественное отображение является единственным изоморфизмом поля действительных чисел в себя.

9. Докажите, что алгебраическая система, изоморфная системе действительных чисел, является системой действительных чисел.

10. Пусть $\mathbf{Q}^{\mathbf{N}}$ — множество всех последовательностей рациональных чисел. Покажите, что алгебра $\bar{\mathcal{Q}}^{\mathbf{N}} = \langle \mathbf{Q}^{\mathbf{N}}, \oplus, \ominus, \odot, \bar{1} \rangle$, где

$\langle a_k\rangle \oplus \langle b_k\rangle = \langle a_k + b_k\rangle$;

$\ominus \langle a_k\rangle = \langle -a_k\rangle$;

$\langle a_k\rangle \odot \langle b_k\rangle = \langle a_k \cdot b_k\rangle$;

$\bar{1} = \langle a_k\rangle$ где $a_k = 1$ для всякого натурального k,

является коммутативным кольцом.

11. Пусть $F(\mathbf{Q})$ — множество всех фундаментальных последовательностей над полем $\mathcal{Q} = \langle \mathbf{Q}, +, -, \cdot, 1 \rangle$. Покажите, что $F(\mathbf{Q})$ замкнуто в кольце $\mathcal{Q}^{\mathbf{N}}$ всех последовательностей рациональных чисел и алгебра $\mathcal{F}(\mathbf{Q}) = \langle F(\mathbf{Q}), \oplus, \ominus, \odot, \bar{1} \rangle$ является коммутативным кольцом.

12. Пусть $\langle a_k \rangle \equiv \langle b_k \rangle$ означает, что последовательность $\langle a_k - b_k \rangle$ сходится к нулю. Докажите, что:

(a) отношение $\equiv$ на множестве $F(\mathbf{Q})$ есть отношение эквивалентности;

(b) отношение $\equiv$ является отношением конгруэнтности в кольце $\mathcal{F}(\mathbf{Q})$.

13. Покажите, что если $\langle a_k \rangle \in F(\mathbf{Q})$, $a_k \neq 0$ для всех $k \in \mathbf{N}$ и последовательность $\langle a_k \rangle$ не сходится к нулю, то

$\langle 1 / a_k \rangle \in F(\mathbf{Q})$ и $\langle a_k \rangle \odot \langle 1 / a_k \rangle = \bar{1}$.

14. Докажите, что фактор-алгебра кольца $\mathcal{F}(\mathbf{Q})$ по отношению конгруэнтности $\equiv$ является полем.

15. Пусть $\bar{F}$ — фактор-множество $F(\mathbf{Q})/\equiv$. Докажите, что система $\langle \bar{F}, +, -, \cdot, 1, < \rangle$ есть архимедовски упорядоченное поле.

16. Докажите, что в системе $\langle \bar{F}, +, -, \cdot, 1, < \rangle$ всякая фундаментальная последовательность элементов множества $\bar{F}$ сходится к элементу из $\bar{F}$.

§ 7. ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ

Комплексное расширение поля. Пусть $\mathcal{F} = \langle F, +, -, \cdot, 1 \rangle$ — поле и t — элемент (символ), не принадлежащий полю $\mathcal{F}$. Выражение вида $a + bt$, где a и b — произвольные элементы поля $\mathcal{F}$, назовем *линейным многочленом от t над полем $\mathcal{F}$* (или формой). Элементы a и b называются *коэффициентами многочлена $a + bt$*.

Два линейных многочлена от t называются *равными*, если они имеют одни и те же слагаемые (одни и те же коэффициенты), с точностью до слагаемых с нулевыми коэффициентами, которые могут быть удалены из выражения (для формы). В частности, для любых элементов a и b поля $\mathcal{F}$

(I) $a + 0 \cdot t = a, \quad 0 + bt = bt.$

Обозначим через K множество всех линейных многочленов от t над полем $\mathcal{F}$:

$$K = \{a + bt \mid a,\ b \in F\}.$$

На множестве K определим операции $+$, $-$, $\cdot$ следующими формулами:

(II) $(a + bt) + (c + dt) = (a + c) + (b + d)t;$

(III) $-(a + bt) = (-a) + (-b)t;$

(IV) $(a + bt) \cdot (c + dt) = (ac - bd) + (ad + bc)t.$

Алгебру $\mathscr{K} = \langle K, +, —, \cdot, 1\rangle$, где 1 — единица поля $\mathscr{F}$, назовем *алгеброй линейных многочленов*.

ТЕОРЕМА 7.1. *Пусть* $\mathscr{F} = \langle F, +, —, \cdot, 1\rangle$ — *поле. Алгебра* $\mathscr{K} = \langle K, +, —, \cdot, 1\rangle$ *линейных многочленов над полем* $\mathscr{F}$ *есть коммутативное кольцо, и поле* $\mathscr{F}$ *является его подкольцом.*

Доказательство. Главные операции алгебры $\mathscr{K}$ являются продолжениями соответствующих главных операций поля $\mathscr{F}$. Действительно, в силу формул (I)—(IV) для любых a, b из F

$$a + b = (a + 0 \cdot t) + (b + 0 \cdot t) = (a + b) + 0 \cdot t = a + b;$$
$$-a = -(a + 0 \cdot t) = (-a) + 0 \cdot t = -a;$$
$$a \cdot b = (a + 0 \cdot t) \cdot (b + 0 \cdot t) = a \cdot b + 0 \cdot t = a \cdot b.$$

Кроме того, элемент 1 алгебры $\mathscr{K}$ есть единица поля $\mathscr{F}$. Следовательно, поле $\mathscr{F}$ является подалгеброй алгебры $\mathscr{K}$:

(1) $\mathscr{F} \rightarrow \mathscr{K}$.

Алгебра $\langle K, +, —\rangle$ есть абелева группа. Действительно, сложение в алгебре $\mathscr{K}$ (по формуле (II)) коммутативно и ассоциативно, так как коммутативно и ассоциативно сложение в поле $\mathscr{F}$. Нуль поля $\mathscr{F}$ является нейтральным элементом относительно сложения в алгебре $\mathscr{K}$, поскольку в силу формул (I), (II) для всякого элемента $a + bt$ из K

$$(a + b \cdot t) + 0 = (a + b \cdot t) + (0 + 0 \cdot t) = (a + bt).$$

Всякий элемент $a + b \cdot t$ из K обладает противоположным, так как $(a + b \cdot t) + ((-a) + (-b) \cdot t) = 0 + 0 \cdot t = 0$. Таким образом, установлено, что алгебра $\langle K, +, —\rangle$ является абелевой группой.

Алгебра $\langle K, \cdot, 1\rangle$ есть коммутативный моноид. В самом деле, умножение в алгебре $\mathscr{K}$ (по формуле (IV)) коммутативно в силу коммутативности умножения в поле $\mathscr{F}$. Проверим ассоциативность умножения в алгебре $\mathscr{K}$:

$$\begin{aligned}(a + b \cdot t) \cdot [(c + dt) \cdot (e + ft)] &= (a + bt)\,[(ce - df) + \\ &+ (cf + de)\,t] = \\ &= (ace - adf - bcf - bde) + \\ &+ (acf + ade + bce - bdf)\,t;\end{aligned}$$

$$\begin{aligned}[(a + bt) \cdot (c + dt)] \cdot (e + ft) &= [(ac - bd) + \\ &+ (ad + bc)\,t]\,(e + ft) = \\ &= (ace - bde - adf - bcf) + \\ &+ (acf - bdf + ade + bce)\,t.\end{aligned}$$

Следовательно,

$$(a+bt)\cdot[(c+dt)\cdot(e+ft)]=[(a+bt)(c+dt)](e+ft).$$

Единица поля $\mathscr{F}$ есть нейтральный элемент относительно умножения в алгебре $\mathscr{K}$,

так как $(a+bt)\cdot 1=(a+bt)(1+0\cdot t)=a+bt$.

Таким образом, установлено, что алгебра $\langle K,\ \cdot,\ 1\rangle$ является коммутативным моноидом.

Умножение в алгебре $\mathscr{K}$ дистрибутивно относительно сложения. В самом деле,

$$\begin{aligned}[(a+bt)+(c+dt)]\cdot(e+ft)&=[(a+c)+(b+d)t](e+ft)=\\&=(ae+ce-bf-df)+\\&+(af+cf+be+de)\,t;\end{aligned}$$

$$\begin{aligned}(a+bt)\cdot(e+ft)+(c+dt)\cdot(e+ft)&=[(ae-bf)+(af+be)\,t]+\\&+[(ce-df)+(cf+de)\,t]=\\&=(ae-bf+ce-df)+\\&+(af+be+cf+de)\,t.\end{aligned}$$

Следовательно,

$$\begin{aligned}[(a+bt)+(c+dt)]\cdot(e+ft)=(a+bt)\cdot(e+ft)&+\\+(c+dt)\cdot(e+ft).&\end{aligned}$$

Итак, доказано, что алгебра $\mathscr{K}$ является коммутативным кольцом. В силу (1) поле $\mathscr{F}$ является подкольцом кольца $\mathscr{K}$. □

ОПРЕДЕЛЕНИЕ. Пусть $\mathscr{F}=\langle F,\ +,\ -,\ \cdot,\ 1\rangle$ — поле, в котором квадрат каждого элемента отличен от -1. Поле $\mathscr{K}$ называется *комплексным расширением поля* $\mathscr{F}$, если выполняются следующие условия:

(1) $\mathscr{F}$ есть подполе поля $\mathscr{K}$;

(2) в $\mathscr{K}$ имеется такой элемент u, что $u^2=-1$;

(3) каждый элемент z поля $\mathscr{K}$ можно представить в виде $z=a+bu$, где $a,\ b\in F$.

ПРЕДЛОЖЕНИЕ 7.2. *Пусть $\mathscr{F}$ — поле, в котором квадрат каждого элемента отличен от -1. Пусть $\mathscr{K}$ — комплексное расширение поля $\mathscr{F}$ и u — элемент поля $\mathscr{K}$, удовлетворяющий условиям* (2) *и* (3) *предыдущего определения. Тогда любой элемент z поля $\mathscr{K}$ можно единственным образом представить в виде $z=a+bu$, где $a,\ b\in F$.*

Доказательство. Пусть z — любой элемент поля $\mathscr{K}$. Рассмотрим два произвольных представления z в виде

$$(4)\quad z=a+bu,\quad z=c+du,$$

где a, b, c, $d \in F$. Если $b \neq d$, то $a+bu=c+du$ и $u=\frac{c-a}{b-d}$. Следовательно, $u=\frac{c-a}{b-d} \in F$ и $u^2=-1$. Однако это противоречит условию, согласно которому квадрат каждого элемента поля F отличен от -1. Таким образом, случай, когда $b \neq d$, невозможен. Следовательно, $b=d$ и в силу (4) $a=c$. □

ТЕОРЕМА 7.3. *Пусть* $\mathscr{F}=\langle F, +, -, \cdot, 1\rangle$ — *поле, в котором квадрат всякого элемента отличен от* -1. *Тогда существует комплексное расширение поля* $\mathscr{F}$.

Доказательство. Пусть K — множество всех линейных многочленов над полем $\mathscr{F}$ от переменной t:

(1) $K=\{a+bt \mid a, b \in F\} \quad (t \notin F)$.

На множестве K отношение равенства и операции $+$, $-$, $\cdot$ определяются с помощью формул (I)—(V). По теореме 7.1, алгебра $\mathscr{K}$

$$\mathscr{K}=\langle K, +, -, \cdot, 1\rangle$$

есть коммутативное кольцо, и поле $\mathscr{F}$ является подкольцом кольца $\mathscr{K}$:

(2) $\mathscr{F} \rightarrow \mathscr{K}$.

Докажем, что кольцо $\mathscr{K}$ является полем. В силу (2) нуль и единица поля $\mathscr{F}$ являются нулем и единицей кольца $\mathscr{K}$; поэтому $0_{\mathscr{K}} \neq 1_{\mathscr{K}}$. Нам остается показать, что для всякого ненулевого элемента из K существует в $\mathscr{K}$ обратный ему. Пусть $a+bt \neq 0$, где a, $b \in F$. Тогда $a \neq 0$ или $b \neq 0$. Поэтому $a^2+b^2 \neq 0$, ибо в противном случае $a^2+b^2=0$ и $(a/b)^2=-1$ (при $b \neq 0$) или $(b/a)^2=-1$, что по условию теоремы невозможно. В силу формул (II) и (V) имеем

$$(a+bt)\cdot\left(\frac{a}{a^2+b^2}+\frac{(-b)}{a^2+b^2}\,t\right)=1,$$

т. е. элемент $a+bt$ обратим в $\mathscr{K}$. Следовательно, кольцо $\mathscr{K}$ является полем.

Элемент t из K удовлетворяет условию $t^2=-1$. В самом деле, в силу формул (V) и (II) имеем

$$t\cdot t=(0+1\cdot t)(0+1\cdot t)=-1+0\cdot t=-1.$$

Наконец, в силу (2) поле $\mathscr{F}$ является подполем поля $\mathscr{K}$. Следовательно, поле $\mathscr{K}$ является комплексным расширением поля $\mathscr{F}$. □

ТЕОРЕМА 7.4. *Пусть* $\mathscr{F} = \langle F, +, -, \cdot, 1\rangle$ — *поле, в котором квадрат любого элемента отличен от* -1. *Пусть* $\mathscr{K}$ *и* $\mathscr{K}'$ — *комплексные расширения поля* $\mathscr{F}$. *Тогда существует изоморфизм поля* $\mathscr{K}$ *на поле* $\mathscr{K}'$, *оставляющий неизменными все элементы поля* $\mathscr{F}$.

Доказательство. В $\mathscr{K}$ существует элемент u такой, что $u^2 = -1$, и всякий элемент поля $\mathscr{K}$ единственным образом представим в виде $a + bu$, где $a, b \in F$. Аналогично, в $\mathscr{K}'$ имеется элемент t такой, что $t^2 = -1$, и каждый элемент поля $\mathscr{K}'$ единственным образом представим в виде $a + bt$, где $a, b \in F$. Обозначим через ψ отображение K на K', ставящее в соответствие элементу $a + bu$ из K элемент $a + bt$ из K'. Это отображение является инъективным отображением K на K'. Кроме того, ψ сохраняет главные операции поля $\mathscr{K}$. Действительно, так как

$$(a + bu) + (c + du) = (a + c) + (b + d)\,u,$$
$$-(a + bu) = (-a) + (-b)\,u;$$
$$(a + bu)(c + du) = (ac - bd) + (ad + bc)\,u,$$

то

$$\psi((a + bu) + (c + du)) = (a + c) + (b + d)\,t = (a + bt) + (c + dt) = \psi(a + bu) + \psi(c + du),$$
$$\psi(-(a + bu)) = (-a) + (-b)\,t = -(a + bt) = -\psi(a + bu),$$
$$\psi((a + bu)(c + du)) = (ac - bd) + (ad + bc)\,t = (a + bt)\cdot(c + dt) = \psi(a + bu)\cdot\psi(c + du).$$

Кроме того, $\psi(1) = 1$ и $\psi(a) = a$ для любого элемента a поля $\mathscr{F}$. Таким образом, ψ есть изоморфное отображение поля $\mathscr{K}$ на поле $\mathscr{K}'$, оставляющее неизменными все элементы поля $\mathscr{F}$. □

Поле комплексных чисел. В упорядоченном поле квадрат любого ненулевого элемента положителен. Следовательно, в поле действительных чисел квадрат любого действительного числа отличен от -1. В силу теоремы 7.3 существует комплексное расширение поля действительных чисел $\mathscr{R}$. По теореме 7.4, изоморфны любые два комплексных расширения поля $\mathscr{R}$ действительных чисел.

ОПРЕДЕЛЕНИЕ. *Полем комплексных чисел* называется комплексное расширение поля действительных чисел.

Пусть $\mathscr{R} = \langle \mathbf{R}, +, -, \cdot, 1\rangle$ — поле действительных чисел. Пусть $\mathscr{C}$ — поле комплексных чисел, комплексное расширение поля $\mathscr{R}$. Основное множество поля $\mathscr{C}$ обозна-

чим через $\mathbf{C}$. Элементы множества $\mathbf{C}$ называются *комплексными числами*. Обозначим через i такое комплексное число, что $i^2=-1$ и любое комплексное число z из $\mathbf{C}$ можно представить в виде $z=a+bi$, где $a, b\in\mathbf{R}$. Это представление называется *алгебраической формой числа* z. Число i называется *мнимой единицей поля комплексных чисел*.

ТЕОРЕМА 7.5. *Пусть* $\mathscr{C}=\langle\mathbf{C}, +, -, \cdot, 1\rangle$ — *поле комплексных чисел, комплексное расширение поля* $\mathscr{R}$ *действительных чисел, и* a, b, c, d — *любые действительные числа. Тогда*

(1) $a+bi=c+di$ тогда и только тогда, когда $a=c$ и $b=d$;

(2) $(a+bi)+(c+di)=(a+c)+(b+d)i$;

(3) $-(a+bi)=(-a)+(-b)i$;

(4) $(a+bi)(c+di)=(ac-bd)+(ad+bc)i$;

(5) если $a+bi\neq 0$, то $(a+bi)^{-1}=\frac{a}{a^2+b^2}+\frac{(-b)}{a^2+b^2}\cdot i$.

Доказательство. Пусть $a+bi=c+di$. Если $b=d$, то $a=c$. Если же $b\neq d$, то $i=\frac{c-a}{b-d}\in\mathbf{R}$ и $\left(\frac{c-a}{b-d}\right)^2=-1$, что невозможно. Следовательно, случай, когда $b\neq d$, невозможен. Поскольку $\mathscr{C}$ — поле, то имеют место равенства (2), (3) и (4).

Пусть $a+bi\neq 0$. В силу (1) $a\neq 0$ или $b\neq 0$ и $a-bi\neq\neq 0$. Так как произведение любых двух ненулевых элементов поля $\mathscr{C}$ отлично от нуля, то $(a+bi)(a-bi)=\\=a^2+b^2\neq 0$. Следовательно,

$$(a+bi)^{-1}=\frac{a-bi}{a^2+b^2}=\frac{a}{a^2+b^2}+\frac{(-b)}{a^2+b^2}i. \quad \square$$

ОПРЕДЕЛЕНИЕ. *Числовым полем* называется любое подполе поля комплексных чисел.

Любое числовое поле содержит подполе рациональных чисел. В самом деле, пусть $\mathscr{F}=\langle F, +, -, \cdot, 1\rangle$ — любое числовое поле. Так как $0, 1\in F$ и множество F замкнуто относительно операций $+$, $-$, то $n=1+\ldots+1\in F$ и $-n\in F$. Следовательно, F содержит все целые числа. Множество F замкнуто относительно деления и, значит, содержит все элементы вида mn^{-1}, обозначаемые символом m/n. Следовательно, F содержит множество $\mathbf{Q}$ всех рациональных чисел. Множество $\mathbf{Q}$ замкнуто относительно главных операций поля $\mathscr{F}$ и всякий ненулевой элемент из $\mathbf{Q}$ обратим в $\mathbf{Q}$. Значит, алгебра $\mathscr{Q}$, $\mathscr{Q}=\langle\mathbf{Q}, +, -, \cdot, 1\rangle$,

является подполем поля $\mathscr{F}$. Следовательно, числовое поле $\mathscr{F}$ содержит подполе $\mathbb{Q}$ рациональных чисел.

ОПРЕДЕЛЕНИЕ. *Числовым кольцом* называется любое подкольцо поля комплексных чисел.

Так, например, кольца $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ являются числовыми. Подкольцо поля $\mathbb{C}$, порожденное элементом i и обозначаемое $\mathbb{Z}[i]$, есть числовое поле.

Сопряженные комплексные числа. Если $z=a+bi$, где $a,\ b\in\mathbf{R}$, то число $a-bi$ обозначается через $\bar{z}$.

ОПРЕДЕЛЕНИЕ. Комплексные числа $z=a+bi$ и $\bar{z}=a-bi$ называются *сопряженными*.

Напомним, что изоморфное отображение поля на себя называется автоморфизмом поля.

ТЕОРЕМА 7.6. *Если z и z' — любые комплексные числа, то*

(1) $\overline{z+z'}=\bar{z}+z'$;

(2) $\overline{(-z)}=-\bar{z}$;

(3) $\overline{z\cdot z'}=\bar{z}\cdot z'$;

(4) $\overline{(\bar{z})}=z$;

(5) $z=\bar{z}$ *тогда и только тогда, когда* $z\in\mathbf{R}$,

(6) *если* $z=a+bi$, *то* $z\cdot\bar{z}=a^2+b^2$.

Доказательство теоремы предоставляется читателю.

СЛЕДСТВИЕ 7.7. *Отображение поля комплексных чисел $\mathbb{C}$ в себя, ставящее в соответствие любому комплексному числу z сопряженное число $\bar{z}$, является автоморфизмом поля $\mathbb{C}$, оставляющим неизменными действительные числа.*

Модуль комплексного числа. Введем понятие модуля комплексного числа.

ОПРЕДЕЛЕНИЕ. *Модулем комплексного числа* $a+bi$ ($a,\ b\in\mathbf{R}$) называется арифметический квадратный корень из числа a^2+b^2, т. е. число $(a^2+b^2)^{1/2}$. Модуль комплексного числа $z=a+bi$ обозначается через $|z|$ или $|a+bi|$. Таким образом, согласно определению, $|z|^2=a^2+b^2$.

ТЕОРЕМА 7.8. *Для любых комплексных чисел z и u*

(1) $|z|^2=z\cdot\bar{z}$;

(2) $|z|=0$ *тогда и только тогда, когда* $z=0$;

(3) $|zu|=|z|\cdot|u|$;

(4) $|z^{-1}|=|z|^{-1}$ *при* $z\neq 0$;

(5) $|z+u|\leqslant|z|+|u|$;

(6) $|z|-|u|\leqslant|z+u|$;

(7) $||z|-|u||\leqslant|z+u|$.

Доказательство. (1) Если $z=a+bi$, то $\bar{z}=a-bi$ и $z\cdot\bar{z}=a^2+b^2=|z|^2$.

(2) Если $|z|=|a+bi|=0$, то $|z|^2=a^2+b^2=0$. Так как a и b — действительные числа, то из $a^2+b^2=0$ следует $a=b=0$, т. е. $z=0$.

(3) В силу (1)

$$|zu|^2=(zu)(\overline{zu})=(zu)(\bar{z}\bar{u})=(z\bar{z})(u\bar{u})=|z|^2|u|^2=(|z|\cdot|u|)^2.$$

Из равенства $|zu|^2=(|z|\cdot|u|)^2$ следует формула (3).

(4) Согласно (3), при $z\neq 0$

$$|z\cdot z^{-1}|=|z|\cdot|z^{-1}|=1.$$

Следовательно, $|z^{-1}|=|z|^{-1}$.

(5) На основании (1) имеем

$$|z+1|^2=(z+1)\cdot(\bar{z}+1)=|z|^2+z+\bar{z}+1.$$

Кроме того, если $z=a+bi$, то $z+\bar{z}=2a\leqslant 2(a^2+b^2)^{1/2}=2|z|$. Поэтому $|z+1|^2\leqslant(|z|+1)^2$; следовательно, $|z+1|\leqslant|z|+1$. На основании формулы (3) и последнего неравенства заключаем, что при $u\neq 0$

$$|z+u|=|u(zu^{-1}+1)|=|u||zu^{-1}+1|\leqslant|u|(|zu^{-1}|+1)=$$
$$=|u|(|z||u|^{-1}+1).$$

Следовательно, $|z+u|\leqslant|z|+|u|$.

(6) Так как $z=-u+(z+u)$ и $|-u|=|u|$, то в силу (5) $|z|\leqslant|-u|+|z+u|=|u|+|z+u|$. Следовательно, $|z|-|u|\leqslant|z+u|$.

(7) Поскольку число $||z|-|u||$ равно $|z|-|u|$ или $|u|-|z|$, то неравенство (7) следует из неравенства (6). □

Геометрическое представление комплексных чисел. Каждому комплексному числу $z=a+bi$ поставим в соответствие точку $M(a, b)$ плоскости (с прямоугольной системой координат) с абсциссой a и ординатой b. Точка $M(a, b)$ называется *точкой, изображающей число* $a+bi$.

Для любых двух комплексных чисел $a+bi$ и $c+di$ равенство $a+bi=c+di$ имеет место тогда и только тогда, когда $a=c$ и $b=d$. Поэтому отображение, ставящее в соответствие каждому комплексному числу $a+bi$ точку $M(a, b)$ координатной плоскости, является инъективным отображением множества $\mathbb{C}$ комплексных чисел на множество всех точек координатной плоскости. Координатная плоскость, точки которой изображают комплексные числа, называется *комплексной плоскостью*.

Пусть r и φ — полярные координаты точки M (точка O — начало, Ox — полярная ось). Тогда $r=(a^2+b^2)^{1/2}$, т. е. r — модуль комплексного числа $a+bi$.

Действительные числа изображаются точками оси абсцисс; поэтому ось абсцисс называется *действительной осью*. Точки оси ординат изображают *чисто мнимые числа*, т. е. числа вида bi, где $b \in \mathbf{R}$, поэтому ось ординат называется *мнимой осью*.

Сопряженные комплексные числа z и $\bar{z}$ изображаются точками, симметричными относительно действительной оси. *Взаимно противоположные числа* z и $-z$ изображаются точками, симметричными относительно начала координат.

Точки, изображающие комплексные числа с одним и тем же модулем r, $r>0$, расположены на окружности радиуса r с центром в начале координат.

Изобразим на комплексной плоскости комплексные числа $z_1=a_1+b_1i$, $z_2=a_2+b_2i$ и их сумму $z_3=(a_1+a_2)+(b_1+b_2)i$ соответственно точками M_1, M_2 и M_3. Геометрически направленный отрезок OM_3 получается из направленных отрезков OM_1 и OM_2 по «правилу параллелограмма».

Упражнения

1. Найдите на плоскости точки, изображающие комплексные числа 1, i, $1+i$, $1-i$, $-1-i$, $1+i\sqrt{3}$, $\sqrt{3}-i$.

2. Пусть даны положительное действительное число a и комплексное число c. Найдите множество точек плоскости, которые изображают комплексные числа z, удовлетворяющие условиям:

(a) $|z|=a$; (b) $|z-c|=a$;
(c) $|z|<a$; (d) $|z-c|<a$;
(e) $|z-1|\leqslant 1$; (f) $|z-1-i|<\sqrt{2}$;
(g) $|z-1|+|z+1|=2$.

3. Решите уравнения:

(a) $(1-i)\,\bar{z}-3iz=2-i$;

(b) $z\cdot\bar{z}-2\bar{z}=3-i$;

(c) $z\cdot\bar{z}+3(z-\bar{z})=4+3i$;

(d) $z\cdot\bar{z}+3(z+\bar{z})=7$;

(e) $z\cdot\bar{z}+3(z+\bar{z})=3i$.

4. Покажите, что для любых комплексных чисел z_1 и z_2 выполняется равенство $|z_1+z_2|^2+|z_1-z_2|^2=2(|z_1|^2+|z_2|^2)$. Выясните геометрический смысл этого равенства.

5. Решите систему уравнений:

(a) $ix+(1+i)\,y=3-i$; $(1-i)\,x-(6-i)\,y=4$;

(b) $(2+i)\,x-(3+i)\,y=i$; $(3-i)\,\bar{x}+(2+i)\,\bar{y}=-i$.

6. Решите уравнения (в поле комплексных чисел):

(a) $z^2-(4+3i)z+1+5i=0$;
(b) $z^2+5z+9=0$;
(c) $z^2+z+1+i=0$;
(d) $z^3+1=0$;
(e) $z^4+1=0$.

7. Докажите, что в поле комплексных чисел имеется только один отличный от тождественного автоморфизм, переводящий действительные числа снова в действительные.

8. Докажите, что каждое числовое кольцо содержит подкольцо целых чисел.

9. Пусть $\mathbf{C}_1$ — множество всех квадратных матриц второго порядка вида $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ с действительными a и b. Докажите, что алгебра $\langle \mathbf{C}_1, +, -, \cdot, e\rangle$ типа (2, 1, 2, 0), где $+$, $-$, $\cdot$ суть обычные операции над матрицами и $e=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, есть поле, изоморфное полю комплексных чисел.

10. Пусть K — множество всех комплексных чисел вида $m+ni$ с целыми m и n. Покажите, что алгебра $\langle K, +, -, \cdot, 1\rangle$ является областью целостности (целостным кольцом). Это кольцо называется *кольцом целых гауссовых чисел*.

11. Опишите подполе поля комплексных чисел, порожденное числом i и рациональными числами.

§ 8. ТРИГОНОМЕТРИЧЕСКАЯ ФОРМА КОМПЛЕКСНОГО ЧИСЛА. ИЗВЛЕЧЕНИЕ КОРНЕЙ ИЗ КОМПЛЕКСНЫХ ЧИСЕЛ

Тригонометрическая форма комплексного числа. Наряду с алгебраической формой комплексного числа широко применяется тригонометрическая форма.

ПРЕДЛОЖЕНИЕ 8.1. *Для любых действительных чисел x и y, удовлетворяющих условию*

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

существует единственное действительное число φ такое, что

(2) $x=\cos\varphi$, $y=\sin\varphi$, $0\leqslant\varphi<2\pi$.

Доказательство. Предположим, что действительные числа x и y удовлетворяют условию (1), тогда

(3) $|x|\leqslant 1$.

Любое действительное число, удовлетворяющее условию (3), принадлежит области значений функции cos в замкнутом

интервале $[0, \pi]$. Следовательно, существует такое действительное число ψ, что

(4) $x = \cos\psi$, $0 \leqslant \psi \leqslant \pi$.

В силу (1) и (4) $y^2 = \sin^2\psi$ и $y = \pm\sin\psi$. Если $y = \sin\psi$, то положим $\varphi = \psi$. Если же $y = -\sin\psi$, то положим $\varphi = 2\pi - \psi$. В любом случае действительное число φ удовлетворяет условиям (2).

Предположим, что θ — произвольное действительное число, удовлетворяющее условиям

(5) $x = \cos\theta$, $y = \sin\theta$, $0 \leqslant \theta < 2\pi$.

Допустим, что $\theta \leqslant \varphi$, тогда

$$\sin(\varphi - \theta) = \sin\varphi\cos\theta - \cos\varphi\sin\theta = yx - xy = 0.$$

Но $0 \leqslant \varphi - \theta < 2\pi$, поэтому равенство $\sin(\varphi - \theta) = 0$ возможно лишь в случае $\varphi - \theta = 0$ или $\varphi - \theta = \pi$. Если $\varphi - \theta = \pi$, то $\cos\varphi = -\cos\theta = -x = -\cos\varphi$, $\sin\varphi = -\sin\theta = -y = -\sin\varphi$; из равенств $\cos\varphi = -\cos\varphi$, $\sin\varphi = -\sin\varphi$ следует $\cos\varphi = \sin\varphi = 0$, что невозможно. Таким образом, случай, когда $\varphi - \theta = \pi$, невозможен. Следовательно, $\varphi - \theta = 0$ и $\varphi = \theta$. □

ТЕОРЕМА 8.2. *Для любого комплексного числа z, отличного от нуля, существует единственная пара действительных чисел r и φ такая, что*

(1) $z = r(\cos\varphi + i\sin\varphi)$, $0 < r$, $0 \leqslant \varphi < 2\pi$.

Доказательство. Если r удовлетворяет условиям (1), то $|z|^2 = r^2(\cos^2\varphi + \sin^2\varphi) = r^2$ и $r = |z|$. Следовательно, существует не более одного действительного числа r, удовлетворяющего условиям (1).

Пусть $z = a + bi \neq 0$, где a, b — действительные числа. Положим $r = (a^2 + b^2)^{1/2}$, $r > 0$. Тогда $(a/r)^2 + (b/r)^2 = 1$. В силу предложения 8.1 существует единственное действительное число φ, удовлетворяющее условиям

(2) $a/r = \cos\varphi$, $b/r = \sin\varphi$, $0 \leqslant \varphi < 2\pi$.

Так как $r > 0$ и $z = r\left(\frac{a}{r} + \frac{b}{r}i\right)$, то из (2) следует

(3) $z = r(\cos\varphi + i\sin\varphi)$, $0 \leqslant \varphi < 2\pi$.

С другой стороны, из (3) следуют равенства $a + bi = r\cos\varphi + r\sin\varphi \cdot i$, $a = r\cos\varphi$, $b = r\sin\varphi$. Поэтому из условий (3) следуют условия (2). Таким образом, условия (2) и (3) при $r > 0$ равносильны. Следовательно, сущест-

вует единственная пара действительных чисел, удовлетворяющих условиям (1). □

ОПРЕДЕЛЕНИЕ. *Тригонометрической формой комплексного числа* z называется его представление в виде $z=r(\cos\varphi+i\sin\varphi)$, где r и φ — действительные числа и $r\geqslant 0$.

ТЕОРЕМА 8.3. *Пусть*

(1) $z=r(\cos\varphi+i\sin\varphi)$, $r>0$,

(2) $z=r_1(\cos\psi+i\sin\psi)$, $r_1>0$,

— два представления комплексного числа z *в тригонометрической форме. Тогда* $r=r_1=|z|$ *и существует такое целое число* k, *что* $\varphi-\psi=2\pi k$.

Доказательство. В теореме 8.2 установлено, что из (1) и (2) следуют соответственно равенства $r=|z|$ и $r_1=|z|$, или $r=r_1=|z|$. По теореме 6.3, для пары чисел φ и 2π существуют действительное число α и целое число m такие, что

(3) $\varphi=2\pi m+\alpha$, $0\leqslant\alpha<2\pi$.

Аналогично, для чисел ψ и 2π существуют действительно число β и целое число n такие, что

(4) $\psi=2\pi n+\beta$, $0\leqslant\beta<2\pi$.

На основании формул (1), (3) имеем $r=|z|$ и

(5) $z=|z|(\cos\alpha+i\sin\alpha)$.

В силу формул (2), (4) получаем $r_1=|z|$ и

(6) $z=|z|(\cos\beta+i\sin\beta)$.

Поскольку $|z|\neq 0$, из (5) и (6) следует, что

(7) $\cos\alpha+i\sin\alpha=\cos\beta+i\sin\beta$.

Так как $0\leqslant\alpha$, $\beta<2\pi$, то, по теореме 8.2, из (7) получаем

(8) $\alpha=\beta$.

На основании (3), (4) и (8) заключаем, что $\varphi-\psi=2\pi k$, где $k=m-n$. □

ТЕОРЕМА 8.4. *Пусть* $z=|z|(\cos\varphi+i\sin\varphi)$, $z_1=|z_1|(\cos\psi+i\sin\psi)$, *где* φ *и* ψ *— действительные числа;*

тогда

(1) $zz_1 = |z||z_1|[\cos(\varphi+\psi)+i\sin(\varphi+\psi)]$;

(2) $\frac{z}{z_1} = \frac{|z|}{|z_1|}[\cos(\varphi-\psi)+i\sin(\varphi-\psi)]$ *при* $z_1 \neq 0$;

(3) $z^n = |z|^n(\cos n\varphi + i\sin n\varphi)$ *для любого натурального* n;

(4) $(\cos\varphi + i\sin\varphi)^n = \cos n\varphi + i\sin n\varphi$.

Доказательство. В силу дистрибутивности умножения комплексных чисел относительно сложения имеем

$$z\cdot z_1 = |z|\cdot|z_1|[(\cos\varphi\cos\psi - \sin\varphi\sin\psi)+(\cos\varphi\sin\psi + \cos\psi\sin\varphi)i].$$

Отсюда следует формула (1), поскольку

$$\cos\varphi\cos\psi - \sin\varphi\sin\psi = \cos(\varphi+\psi);$$

$$\cos\varphi\sin\psi + \cos\psi\sin\varphi = \sin(\varphi+\psi).$$

В силу формулы (1) получаем

$$(\cos\psi + i\sin\psi)(\cos(-\psi)+i\sin(-\psi)) = \cos 0 + i\sin 0 = 1,$$

поэтому

$$\frac{1}{\cos\psi + i\sin\psi} = \cos(-\psi)+i\sin(-\psi)$$

и при $z_1 \neq 0$

$$\frac{1}{z_1} = \frac{1}{|z_1|}(\cos(-\psi)+i\sin(-\psi)).$$

Следовательно, по формуле (1),

$$\frac{z}{z_1} = z\cdot\frac{1}{z_1} = \frac{|z|}{|z_1|}\cdot[\cos(\varphi-\psi)+i\sin(\varphi-\psi)].$$

Формула (3) доказывается индукцией по n на основании формулы (1). Формула (4) получается из формулы (3) при $|z|=1$. □

Формулы (3) и (4) называются *формулами Муавра.*

Корни n-й степени из единицы. Пусть n — любое натуральное число, отличное от нуля.

ОПРЕДЕЛЕНИЕ. Комплексное число w, удовлетворяющее условию $w^n = 1$, называется *корнем* n-й *степени из единицы.*

ТЕОРЕМА 8.5. *Существует точно n различных корней n-й степени из единицы и все они получаются по формуле*

$$w_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} \text{ при } k = 0,\ 1,\ \ldots,\ n-1.$$

Доказательство. Каждое из чисел w_k есть корень n-й степени из единицы, так как согласно формуле Муавра

$$w_k^n = \left(\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}\right)^n = \cos 2\pi k + i\sin 2\pi k = 1.$$

Действительные числа $\frac{2\pi\cdot 0}{n}$, $\frac{2\pi\cdot 1}{n}$, $\ldots$, $\frac{2\pi(n-1)}{n}$ неотрицательны, меньше числа 2π и попарно различны. Следовательно, по теореме 8.2, комплексные числа w_0, w_1, $\ldots$ $\ldots$, w_{n-1} попарно различны.

Нам остается показать, что произвольный корень n-й степени из единицы принадлежит множеству $\{w_0, w_1, \ldots, w_{n-1}\}$. По теореме 8.2, число w можно представить в виде $w = |w|(\cos\varphi + i\sin\varphi)$, причем действительное число φ удовлетворяет условиям

(1) $0 \leqslant \varphi < 2\pi$.

Так как $w^n = 1$, то $|w|^n = 1$ и, по теореме 6.4, $|w| = 1$. Следовательно, $w = \cos\varphi + i\sin\varphi$. По формуле Муавра $w^n = \cos n\varphi + i\sin n\varphi$. Поэтому равенство $w^n = 1$ можно записать в виде

(2) $\cos n\varphi + i\sin n\varphi = \cos 0 + i\sin 0$.

По теореме 8.3, из (2) следует, что $n\varphi - 0 = 2\pi k$ для некоторого целого числа k, поэтому $\varphi = \frac{2\pi k}{n}$. Кроме того, в силу (1) $0 \leqslant \varphi = \frac{2\pi k}{n} < 2\pi$ и, значит, $0 \leqslant k < n$. Следовательно,

$$w = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = w_k \in \{w_0, w_1, \ldots, w_{n-1}\}. \quad \square$$

СЛЕДСТВИЕ 8.6. *Точки комплексной плоскости, изображающие корни n-й степени из единицы, являются вершинами правильного n-угольника, вписанного в окружность единичного радиуса с центром в начале координат, причем одна из вершин находится в точке* (0, 1).

ОПРЕДЕЛЕНИЕ. Комплексное число w называется *первообразным корнем n-й степени из единицы* ($n \geqslant 1$), если

множество чисел $\{w^0, w^1, \ldots, w^{n-1}\}$ является множеством всех решений уравнения $z^n = 1$.

Так, например, при любом натуральном $n \geqslant 1$ число $w_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ в силу теоремы 8.5 является первообразным корнем n-й степени из единицы.

Корни n-й степени из произвольного комплексного числа. Тригонометрическая форма комплексного числа позволяет полностью решить вопрос об извлечении корней из комплексных чисел.

ТЕОРЕМА 8.7. *Пусть $c = |c|(\cos\varphi + i\sin\varphi)$ — отличное от нуля комплексное число и n — ненулевое натуральное число. Существует n различных корней n-й степени из числа c и все они получаются по формуле*

$$u_k = |c|^{1/n}\left(\cos\frac{\varphi+2\pi k}{n} + i\sin\frac{\varphi+2\pi k}{n}\right),\ k = 0, 1, \ldots, n-1.$$

Доказательство. Покажем, что

(1) $u_k = u_0 w_k$, $k = 0, 1, \ldots, n-1$,

где $w_0, \ldots, w_{n-1}$ — корни n-й степени из единицы и

$$u_0 = |c|^{1/n}\left(\cos\frac{\varphi}{n} + i\sin\frac{\varphi}{n}\right).$$

В самом деле, в силу формулы Муавра

$$u_k = |c|^{1/n}\left(\cos\frac{\varphi}{n} + i\sin\frac{\varphi}{n}\right)\left(\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}\right) = u_0 w_k.$$

Каждое из чисел u_k есть корень n-й степени из числа c, так как в силу (1)

$$u_k^n = u_0^n w_k^n = u_0^n = (|c|^{1/n})^n\left(\cos\frac{\varphi}{n} + i\sin\frac{\varphi}{n}\right)^n = \\ = |c|(\cos\varphi + i\sin\varphi) = c.$$

Если u — произвольный корень n-й степени из числа c, то $(uu_0^{-1})^n = u^n(u_0^n)^{-1} = cc^{-1} = 1$. Поэтому

$$uu_0^{-1} \in \{w_0, \ldots, w_{n-1}\}$$

и в силу (1)

$$u \in \{u_0 w_0, \ldots, u_0 w_{n-1}\} = \{u_0, \ldots, u_{n-1}\}.$$

Следовательно, множество $\{u_0, \ldots, u_{n-1}\}$ является множеством всех корней n-й степени из числа c. Это множество содер-

жит в точности n различных элементов, поскольку

$$\{u_0, \ldots, u_{n-1}\} = \{u_0 w_0, \ldots, u_0 w_{n-1}\},$$

$u_0 \neq 0$ и числа $w_0, \ldots, w_{n-1}$ попарно различны (по теореме 8.2). □

Упражнения

1. Представьте в тригонометрической форме комплексные числа:

$$1,\ i,\ -1,\ -i,\ 1+i,\ 1-i,\ -\frac{1}{2}+i\frac{\sqrt{3}}{2},\ \sqrt{3}+i.$$

2. Найдите множество точек плоскости, изображающих комплексные числа z, для которых:

(a) $\arg z = 0$; (b) $\arg z = \frac{\pi}{3}$; (c) $\arg z = \pi$; (d) $\arg z = \frac{\pi}{2}$.

3. При каких условиях модуль суммы двух комплексных чисел равен сумме модулей слагаемых?

4. При каких условиях модуль суммы двух комплексных чисел равен разности модулей слагаемых?

5. Опишите следующие отображения ($\mathbf{C} \to \mathbf{C}$):

(a) $z \longmapsto \bar{z}$; (b) $z \longmapsto \frac{1}{z}$ $(z \neq 0)$; (c) $z \longmapsto iz$; (d) $z \longmapsto i\bar{z}$;

(e) $z \longmapsto rz$, где r — положительное число;

(f) $z \longmapsto (\cos\varphi + i\sin\varphi)$; (g) $z \longmapsto -\bar{z}$;

(h) $z \longmapsto r(\cos\varphi + i\sin\varphi)$; (i) $z \longmapsto \bar{z}^{-1}$.

6. Пусть $w = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$ и n — натуральное число. Вычислите: (a) $(1+w)^n$; (b) $w^n + \bar{w}^n$.

7. Вычислите сумму $\frac{1}{2} + \cos x + \cos 2x + \ldots + \cos nx$.

8. Покажите, что $\sin x + \sin 2x + \ldots + \sin nx = \dfrac{\sin\frac{n+1}{2}x \cdot \sin\frac{nx}{2}}{\sin\frac{x}{2}}$.

9. Выразите через $\cos x$ и $\sin x$:

(a) $\cos 5x$; (b) $\sin 5x$; (c) $\cos 6x$; (d) $\sin 6x$; (e) $\cos 8x$.

10. Найдите формулы, выражающие $\cos nx$ и $\sin nx$ через $\cos x$ и $\sin x$.

11. Выразите в виде многочлена первой степени от косинусов и синусов углов, кратных x:

(a) $\sin^3 x$; (b) $\cos^5 x$; (c) $\sin^5 x$; (d) $\cos^6 x$.

12. Найдите все корни из единицы степени: (a) 2; (b) 3; (c) 6; (d) 8; (e) 12; (f) 24.

13. Найдите все комплексные корни уравнений:

(a) $z^3 + i = 0$; (b) $z^3 + 2 + 2i = 0$; (c) $z^4 + \frac{1}{2} + i\frac{\sqrt{3}}{2} = 0$;

(d) $z^6 + i = 0$; (e) $z^5 - 1 = 0$.

14. Найдите сумму и произведение всех корней n-й степени из 1.

15. Пусть $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, где n — целое положительное число. Покажите, что комплексное число z является первообразным корнем n-й степени из единицы тогда и только тогда, когда $z = \varepsilon^m$ для некоторого натурального числа m, взаимно простого с n.

16. Найдите первообразные корни степени:

(a) 2; (b) 3; (c) 4; (d) 5; (e) 6; (f) 8; (g) 12; (h) 24.

17. Найдите все комплексные числа, удовлетворяющие условию $\bar{z} = z^{n-1}$, где n — целое положительное число и $\bar{z}$ — сопряженное с z.

18. Докажите следующие утверждения:

(a) произведение корня степени m из 1 на корень степени n из 1 есть корень степени mn из 1;

(b) если m и n взаимно простые, то существует только одно комплексное число z, удовлетворяющее условиям $z^m = 1$ и $z^n = 1$;

(c) если числа m и n взаимно простые, то все корни степени mn из 1 получаются умножением корней степени m из 1 на корни степени n из 1;

(d) если m и n взаимно простые, то произведение первообразного корня степени m из 1 на первообразный корень степени n из 1 есть первообразный корень степени mn из 1 и обратно.

Глава пятая

АРИФМЕТИЧЕСКИЕ ВЕКТОРНЫЕ ПРОСТРАНСТВА И СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ

§ 1. АРИФМЕТИЧЕСКИЕ ВЕКТОРНЫЕ ПРОСТРАНСТВА

Арифметическое n-мерное векторное пространство. Пусть $\mathcal{F}$ — произвольное фиксированное поле, $\mathcal{F} = \langle F, +, —, \cdot, 1\rangle$, и F — его основное множество. Элементы множества F назовем скалярами, F — множеством скаляров, а $\mathcal{F}$ — полем скаляров. Пусть n — фиксированное натуральное число, отличное от нуля.

ОПРЕДЕЛЕНИЕ. *n-мерным вектором над полем $\mathcal{F}$* называется любой кортеж из n элементов поля $\mathcal{F}$. Множество всех n-мерных векторов над полем $\mathcal{F}$ обозначается символом F^n.

Вектор обычно записывается в виде строки или столбца. В этом параграфе n-мерный вектор записывается в виде строки

$$(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

где $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$.

На множестве n-мерных векторов над полем $\mathcal{F}$ введем отношение равенства, операцию сложения векторов и операцию умножения вектора на скаляр.

ОПРЕДЕЛЕНИЕ. Векторы $(\alpha_1, \ldots, \alpha_n)$ и $(\beta_1, \ldots, \beta_n)$ называются *равными*, если $\alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n$.

ОПРЕДЕЛЕНИЕ. *Суммой векторов* $(\alpha_1, \ldots, \alpha_n)$ и $(\beta_1, \ldots, \beta_n)$ называется вектор $(\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$, т. е.

$$(\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n).$$

ОПРЕДЕЛЕНИЕ. *Произведением скаляра λ на вектор* $(\alpha_1, \ldots, \alpha_n)$ называется вектор $(\lambda\alpha_1, \ldots, \lambda\alpha_n)$, т. е.

$$\lambda(\alpha_1, \ldots, \alpha_n) = (\lambda\alpha_1, \ldots, \lambda\alpha_n).$$

Операцию умножения на скаляр λ обозначим символом ω_λ, т. е.

$$\omega_\lambda(\alpha_1, \ldots, \alpha_n) = \lambda(\alpha_1, \ldots, \alpha_n).$$

Для каждого λ из F ω_λ есть унарная операция на множестве F^n n-мерных векторов.

Вектор $(0, \ldots, 0)$ называется *нулевым вектором* и обозначается символом $\mathbf{0}$. Нулевой вектор является нейтральным элементом относительно сложения.

Вектор $(-1)\cdot(\alpha_1, \ldots, \alpha_n)$ называется *вектором, противоположным вектору* $\boldsymbol{a}=(\alpha_1, \ldots, \alpha_n)$, и обозначается символом $-\boldsymbol{a}$. Очевидно, $\boldsymbol{a}+(-\boldsymbol{a})=\mathbf{0}$.

ОПРЕДЕЛЕНИЕ. *Арифметическим n-мерным векторным пространством над полем $\mathcal{F}$* называется множество F^n с заданными на нем бинарной операцией сложения и унарными операциями ω_λ, т. е. алгебра $\langle F^n, +, \{\omega_\lambda \mid \lambda \in F\}\rangle$.

Арифметическое n-мерное векторное пространство над полем $\mathcal{F}$ обозначается символом $\mathcal{F}^n$.

Операция сложения векторов и унарные операции ω_λ являются главными операциями векторного пространства $\mathcal{F}^n$.

ТЕОРЕМА 1.1. *Главные операции векторного пространства $\mathcal{F}^n$ обладают следующими свойствами:*

(1) *алгебра $\langle F^n, +, -\rangle$, где $-\boldsymbol{a}=\omega_{-1}(\boldsymbol{a})$ для любого $\boldsymbol{a}$ из F^n, есть абелева группа;*

(2) *умножение на скаляры ассоциативно, т. е. $(\alpha\beta)\boldsymbol{a}=\alpha(\beta\boldsymbol{a})$ для любых α, β из F и любого $\boldsymbol{a}$ из F^n;*

(3) *умножение на скаляр дистрибутивно относительно сложения, т. е. $\alpha(\boldsymbol{a}+\boldsymbol{b})=\alpha\boldsymbol{a}+\alpha\boldsymbol{b}$ для любого α из F и любых $\boldsymbol{a}$, $\boldsymbol{b}$ из F^n;*

(4) *умножение на вектор дистрибутивно относительно сложения скаляров, т. е. $(\alpha+\beta)\boldsymbol{a}=\alpha\boldsymbol{a}+\beta\boldsymbol{a}$ для любых α, β из F и любого $\boldsymbol{a}$ из F^n;*

(5) $1\cdot\boldsymbol{a}=\boldsymbol{a}$ *для любого $\boldsymbol{a}$ из F^n.*

Доказательство. Докажем, что алгебра $\langle F^n, +, -\rangle$ есть коммутативная группа. Коммутативность сложения векторов непосредственно следует из определения сложения и того, что $\mathcal{F}$ — поле. Ассоциативность сложения следует из ассоциативности сложения скаляров:

$$\begin{aligned}(\boldsymbol{a}+\boldsymbol{b})+\boldsymbol{c}&=((\alpha_1, \ldots, \alpha_n)+(\beta_1, \ldots, \beta_n))+(\gamma_1, \ldots, \gamma_n)=\\&=(\alpha_1+\beta_1, \ldots, \alpha_n+\beta_n)+(\gamma_1, \ldots, \gamma_n)=\\&=((\alpha_1+\beta_1)+\gamma_1, \ldots, (\alpha_n+\beta_n)+\gamma_n)=\\&=(\alpha_1+(\beta_1+\gamma_1), \ldots, \alpha_n+(\beta_n+\gamma_n))=\\&=(\alpha_1, \ldots, \alpha_n)+(\beta_1+\gamma_1, \ldots, \beta_n+\gamma_n)=\\&=\boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{c}).\end{aligned}$$

Вектор 0 является нейтральным элементом относительно сложения, т. е. $\boldsymbol{a}+0=0+\boldsymbol{a}=\boldsymbol{a}$ для любого вектора $\boldsymbol{a}$. Вектор $-\boldsymbol{a}=(-\alpha_1, \ldots, -\alpha_n)$ является противоположным вектору $\boldsymbol{a}$, т. е. $\boldsymbol{a}+(-\boldsymbol{a})=0=(-\boldsymbol{a})+\boldsymbol{a}$. Таким образом, $\langle F^n, +, -\rangle$ есть группа. Ее коммутативность следует из коммутативности сложения скаляров.

Легко проверить также выполнимость свойств (2)—(5). □

Линейная зависимость и независимость системы векторов. Пусть $\mathcal{F}$ — поле скаляров и F — его основное множество. Пусть $\mathcal{V}=\mathcal{F}^n$ — n-мерное арифметическое пространство над $\mathcal{F}$ и $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ — произвольная система векторов пространства $\mathcal{V}$.

ОПРЕДЕЛЕНИЕ. *Линейной комбинацией системы векторов* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ называется сумма вида $\lambda_1\boldsymbol{a}_1+\ldots+\lambda_m\boldsymbol{a}_m$, где $\lambda_1, \ldots, \lambda_m \in F$. Скаляры $\lambda_1, \ldots, \lambda_m$ называются *коэффициентами линейной комбинации*. Линейная комбинация называется *нетривиальной*, если хотя бы один ее коэффициент отличен от нуля. Линейная комбинация называется *тривиальной*, если все ее коэффициенты равны нулю.

ОПРЕДЕЛЕНИЕ. Множество всех линейных комбинаций векторов системы $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ называется *линейной оболочкой* этой системы и обозначается через $L(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$. Линейной оболочкой пустой системы считается множество, состоящее из нулевого вектора.

Итак, по определению,

$$L(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)=\{\lambda_1\boldsymbol{a}_1+\lambda_2\boldsymbol{a}_2+\ldots+\lambda_m\boldsymbol{a}_m \mid \lambda_1, \ldots, \lambda_m \in F\}.$$

Легко видеть, что линейная оболочка данной системы векторов замкнута относительно операций сложения векторов, вычитания векторов и умножений векторов на скаляры.

ОПРЕДЕЛЕНИЕ. Система векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ называется *линейно независимой*, если для любых скаляров $\lambda_1, \ldots, \lambda_m$ из равенства $\lambda_1\boldsymbol{a}_1+\ldots+\lambda_m\boldsymbol{a}_m=0$ следуют равенства $\lambda_1=0, \ldots, \lambda_m=0$. Пустая система векторов считается линейно независимой.

Другими словами, конечная система векторов линейно независима в том и только в том случае, когда всякая нетривиальная линейная комбинация векторов системы не равна нулевому вектору.

ОПРЕДЕЛЕНИЕ. Система векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ называется *линейно зависимой*, если существуют скаляры $\lambda_1, \ldots, \lambda_m$, не все равные нулю, такие, что

$\lambda_1\boldsymbol{a}_1+\ldots+\lambda_m\boldsymbol{a}_m=0$.

Другими словами, конечная система векторов называется линейно зависимой, если существует нетривиальная линейная комбинация векторов системы, равная нулевому вектору.

Система векторов

$$\boldsymbol{e}_1=(1,\ 0,\ \ldots,\ 0),\ \boldsymbol{e}_2=(0,\ 1,\ 0,\ \ldots,\ 0),\ \ldots,\ \boldsymbol{e}_n=(0,\ 0,\ \ldots,\ 0,\ 1)$$

называется *системой единичных векторов* векторного пространства $\mathcal{F}^n$. Эта система векторов линейно независима. В самом деле, для любых скаляров $\lambda_1, \ldots, \lambda_n$ из равенства $\lambda_1\boldsymbol{e}_1+\ldots+\lambda_n\boldsymbol{e}_n=\boldsymbol{0}$ следует равенство $(\lambda_1, \ldots, \lambda_n)=\boldsymbol{0}$ и, значит, равенства $\lambda_1=0, \ldots, \lambda_n=0$.

Рассмотрим свойства линейной зависимости и независимости системы векторов.

СВОЙСТВО 1.1. *Система векторов, содержащая нулевой вектор, линейно зависима.*

Доказательство. Если в системе векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k, \ldots, \boldsymbol{a}_m$ один из векторов, например вектор $\boldsymbol{a}_k$, нулевой, то линейная комбинация векторов системы, все коэффициенты которой нулевые, за исключением коэффициента при $\boldsymbol{a}_k$, равна нулевому вектору. Следовательно, такая система векторов линейно зависима. □

СВОЙСТВО 1.2. *Система векторов линейно зависима, если какая-нибудь ее подсистема линейно зависима.*

Доказательство. Пусть $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ — линейно зависимая подсистема системы $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$, т. е. $\lambda_1\boldsymbol{a}_1+\ldots+\lambda_k\boldsymbol{a}_k=\boldsymbol{0}$, причем хотя бы один из коэффициентов $\lambda_1, \lambda_2, \ldots, \lambda_k$ отличен от нуля. Тогда $\lambda_1\boldsymbol{a}_1+\ldots+\lambda_k\boldsymbol{a}_k+0\,\boldsymbol{a}_{k+1}+\ldots+0\cdot\boldsymbol{a}_m=\boldsymbol{0}$. Следовательно, система векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ линейно зависима. □

СЛЕДСТВИЕ. *Любая подсистема линейно независимой системы линейно независима.*

СВОЙСТВО 1.3. *Система векторов*

(1) $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$,

в которой $\boldsymbol{u}_1\neq\boldsymbol{0}$, линейно зависима тогда и только тогда, когда хотя бы один из векторов $\boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$ является линейной комбинацией предшествующих векторов.

Доказательство. Пусть система (1) линейно зависима и $\boldsymbol{u}_1\neq\boldsymbol{0}$. Тогда существуют скаляры $\lambda_1, \ldots, \lambda_m$, не все равные нулю, такие, что

(2) $\lambda_1\boldsymbol{u}_1+\ldots+\lambda_m\boldsymbol{u}_m=\boldsymbol{0}$.

Обозначим через k наибольшее из чисел $1, 2, \ldots, m$, удовлетворяющее условию $\lambda_k \neq 0$. Тогда равенство (2) можно записать в виде

(3) $\lambda_1 u_1 + \ldots + \lambda_k u_k = 0$.

Отметим, что $k > 1$, ибо в противном случае $\lambda_2 = 0, \ldots, \lambda_m = 0$, $\lambda_1 u_1 = 0$; следовательно, $\lambda_1 = 0$, поскольку $u_1 \neq 0$. Из (3) следует равенство

$$u_k = (-\lambda_k^{-1}\lambda_1) u_1 + \ldots + (-\lambda_k^{-1}\lambda_{k-1}) u_{k-1}.$$

Предположим теперь, что вектор u_s, $1 < s \leqslant m$, есть линейная комбинация предшествующих ему векторов, т. е. $u_s = \lambda_1 u_1 + \ldots + \lambda_{s-1} u_{s-1}$. Тогда $\lambda_1 u_1 + \ldots + \lambda_{s-1} u_{s-1} + (-1) u_s = 0$, т. е. подсистема $u_1, \ldots, u_s$ системы (1) линейно зависима. Следовательно, по свойству 1.2, линейно зависима и исходная система (1). □

СВОЙСТВО 1.4. *Если система векторов* $u_1, \ldots, u_m$ *линейно независима, а система векторов*

(2) $u_1, u_2, \ldots, u_m, v$

линейно зависима, то вектор v *линейно выражается через векторы*

(1) $u_1, \ldots, u_m$,

и притом единственным образом.

Доказательство. По условию система (2) линейно зависима, т. е. существуют скаляры $\lambda_1, \ldots, \lambda_m, \lambda$, не все равные нулю, такие, что

(3) $\lambda_1 u_1 + \ldots + \lambda_m u_m + \lambda v = 0$.

При этом $\lambda \neq 0$, так как при $\lambda = 0$ $\lambda_1 u_1 + \ldots + \lambda_m u_m = 0$, что противоречит линейной независимости системы (1). Из (3) следует равенство

$$v = (-\lambda^{-1}\lambda_1) u_1 + \ldots + (-\lambda^{-1}\lambda_m) u_m.$$

Если $v = \lambda_1' u_1 + \ldots + \lambda_m' u_m$ и $v = \mu_1 u_1 + \ldots + \mu_m u_m$, то $(\lambda_1' - \mu_1) u_1 + \ldots + (\lambda_m' - \mu_m) u_m = 0$.

В силу линейной независимости системы (1) отсюда следует, что

$\lambda_1' - \mu_1 = 0, \ldots, \lambda_m' - \mu_m = 0$ и $\lambda_1' = \mu_1, \ldots, \lambda_m' = \mu_m$. □

СВОЙСТВО 1.5. *Если* $u \in L(v_1, v_2, \ldots, v_m)$ и $v_1, \ldots, v_m \in L(w_1, \ldots, w_s)$, *то* $u \in L(w_1, \ldots, w_s)$.

Доказательство. Условие $u \in L(v_1, \ldots, v_m)$ означает, что найдутся такие скаляры $\alpha_1, \ldots, \alpha_m$, что

1) $u = \alpha_1 v_1 + \ldots + \alpha_m v_m$.

Условие $v_i \in L(w_1, \ldots, w_s)$ означает, что существуют такие скаляры λ_{ik}, что

2) $v_i = \lambda_{i1} w_1 + \ldots + \lambda_{is} w_s \quad (i = 1, \ldots, m)$.

В силу (1) и (2) получаем

$$u = \alpha_1 (\lambda_{11} w_1 + \ldots + \lambda_{1s} w_s) + \ldots + \alpha_m (\lambda_{m1} w_1 + \ldots + \lambda_{ms} w_s) = (\alpha_1 \lambda_{11} + \ldots + \alpha_m \lambda_{m1}) w_1 + \ldots + (\alpha_1 \lambda_{1s} + \ldots + \alpha_m \lambda_{ms}) w_s,$$

т. е. $u \in L(w_1, \ldots, w_s)$. □

ТЕОРЕМА 1.2. *Если*

(1) $u_1, \ldots, u_{m+1} \in L(v_1, \ldots, v_m)$,

то система векторов $u_1, \ldots, u_{m+1}$ *линейно зависима.*

Доказательство (проводится индукцией по m). Будем считать, что векторы $u_1, \ldots, u_{m+1}$ — ненулевые, так как в противном случае теорема очевидна. Предположим, что $m = 1$ и $u_1, u_2 \in L(v_1)$, т. е. $u_1 = \alpha v_1$ и $u_2 = \beta v_1$. Тогда $\alpha \neq 0$, $\beta \neq 0$ и $\alpha^{-1} u_1 + (-\beta^{-1}) u_2 = 0$. Следовательно, система векторов u_1, u_2 линейно зависима.

Предположим, что теорема верна при $m = n - 1$, и докажем, что тогда она верна при $m = n$. Пусть $u_1, \ldots, u_{n+1} \in L(v_1, \ldots, v_n)$, т. е.

$$\begin{aligned} u_1 &= \lambda_{11} v_1 + \ldots + \lambda_{1n} v_n; \\ &\ldots\ldots\ldots\ldots\ldots \\ u_n &= \lambda_{n1} v_1 + \ldots + \lambda_{nn} v_n; \\ u_{n+1} &= \lambda_{n+1,1} v_1 + \ldots + \lambda_{n+1,n} v_n. \end{aligned} \tag{2}$$

Если в правых частях равенств (2) все коэффициенты при v_n равны нулю, то $u_1, \ldots, u_n \in L(v_1, \ldots, v_{n-1})$ и, по индуктивному предположению, система векторов $u_1, \ldots, u_n$ линейно зависима, а значит, линейно зависима и система $u_1, \ldots, u_n, u_{n+1}$. Если же хотя бы один из коэффициентов при v_n, например $\lambda_{n+1,n}$, отличен от нуля, то исключим вектор v_n из первых n равенств. В результате получим

$$\begin{aligned} u_1 - \beta_1 u_{n+1} &= \lambda'_{11} v_1 + \ldots + \lambda'_{1,n-1} v_{n-1}; \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ u_n - \beta_n u_{n+1} &= \lambda'_{n1} v_1 + \ldots + \lambda'_{n,n-1} v_{n-1}. \end{aligned}$$

По индуктивному предположению, из (3) следует, что система векторов $\boldsymbol{u}_1 - \beta_1 \boldsymbol{u}_{n+1}, \ldots, \boldsymbol{u}_n - \beta_n \boldsymbol{u}_{n+1}$ линейно зависима. Следовательно, существуют скаляры $\lambda_1, \ldots, \lambda_n$, не все равные нулю, такие, что

$$\lambda_1 (\boldsymbol{u}_1 - \beta_1 \boldsymbol{u}_{n+1}) + \ldots + \lambda_n (\boldsymbol{u}_n - \beta_n \boldsymbol{u}_{n+1}) = \boldsymbol{0}$$

или

$$\lambda_1 \boldsymbol{u}_1 + \ldots + \lambda_n \boldsymbol{u}_n + \lambda_{n+1} \boldsymbol{u}_{n+1} = \boldsymbol{0},$$

где $\lambda_{n+1} = -(\lambda_1 \beta_1 + \ldots + \lambda_n \beta_n)$. Следовательно, система векторов $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{n+1}$ линейно зависима. □

СЛЕДСТВИЕ 1.3. *Если* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \in L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ *и* $k > m$, *то система векторов* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ *линейно зависима.*

СЛЕДСТВИЕ 1.4. *Если* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \in L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ *и система векторов* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ *линейно независима, то* $k \leqslant m$.

СЛЕДСТВИЕ 1.5. *В* n*-мерном арифметическом векторном пространстве линейно зависима любая система векторов, состоящая из* $n+1$ *или большего числа векторов.*

Следствие 1.5 вытекает из теоремы 1.2, так как любой n-мерный вектор $(\alpha_1, \ldots, \alpha_n)$ является линейной комбинацией единичных векторов $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$:

$$(\alpha_1, \ldots, \alpha_n) = \alpha_1 \boldsymbol{e}_1 + \ldots + \alpha_n \boldsymbol{e}_n \in L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n).$$

Эквивалентные системы векторов. На множестве конечных систем векторов данного векторного пространства V введем бинарное отношение $\sim$.

ОПРЕДЕЛЕНИЕ. Пусть S и T — системы векторов; $S \sim T$, если каждый ненулевой вектор любой из этих систем можно представить в виде линейной комбинации векторов другой системы.

Легко проверить, что бинарное отношение $\sim$ рефлексивно, транзитивно и симметрично, а значит, является отношением эквивалентности. В связи с этим системы векторов S и T называются *эквивалентными*, если $S \sim T$. Отметим, что пустая система векторов эквивалентна как пустой системе векторов, так и системе, состоящей из нулевых векторов.

Рассмотрим некоторые свойства эквивалентных систем векторов.

ТЕОРЕМА 1.6. *Две системы векторов эквивалентны тогда и только тогда, когда равны их линейные оболочки.*

Доказательство. Пусть $S \sim T$. Тогда каждый вектор системы S принадлежит множеству $L(T)$, а каждый вектор системы T принадлежит множеству $L(S)$. Поэтому

в силу свойства 1.5 $L(S) \subset L(T)$ и $L(T) \subset L(S)$, т. е. $L(S) = L(T)$.

Обратно: если $L(S) = L(T)$, то, очевидно, $S \sim T$. □

ТЕОРЕМА 1.7. *Если две конечные системы векторов эквивалентны и каждая из них линейно независима, то эти системы состоят из одинакового числа векторов.*

Доказательство. Теорема, очевидно, верна, если обе системы векторов пустые. Пусть $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r$ и $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s$ — две непустые эквивалентные системы векторов, каждая из которых линейно независима. Тогда в силу следствия 1.4 $r \leqslant s$ и $s \leqslant r$. Следовательно, $r = s$. □

ОПРЕДЕЛЕНИЕ. *Элементарными преобразованиями конечной системы векторов* называются следующие преобразования:

(α) умножение какого-нибудь вектора системы на отличный от нуля скаляр;

(β) прибавление (вычитание) к одному из векторов системы другого вектора системы, умноженного на скаляр;

(γ) исключение из системы или введение в систему нулевого вектора.

Элементарные преобразования (α) и (β) называются *неособенными*, преобразование (γ) называется *особенным*.

ТЕОРЕМА 1.8. *Если одна конечная система векторов получается из другой системы векторов в результате цепочки элементарных преобразований, то эти две системы эквивалентны.*

Доказательство. Пусть

(1) $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m$

— исходная система векторов. Если умножить один из векторов системы, например первый, на отличный от нуля скаляр λ, то получим систему $\lambda\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m$, эквивалентную исходной системе.

Если прибавить к одному из векторов системы другой вектор, умноженный на скаляр, например прибавить к первому вектору k-й вектор, умноженный на λ, то получим систему $\boldsymbol{a}_1 + \lambda\boldsymbol{a}_k, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m$, эквивалентную исходной системе.

Применение к исходной системе векторов преобразования (γ), очевидно, приводит к системе векторов, эквивалентной исходной системе. Следовательно, в силу транзитивности отношения эквивалентности система векторов, получающаяся из системы (1) в результате цепочки эле-

ментарных преобразований, эквивалентна исходной системе векторов (1). □

Базис конечной системы векторов. Введем одно из основных понятий теории векторных пространств.

ОПРЕДЕЛЕНИЕ. *Базисом конечной системы векторов* называется непустая линейно независимая ее подсистема, эквивалентная всей системе.

Другими словами, базис системы векторов — это непустая линейно независимая ее подсистема, через векторы которой линейно выражается каждый вектор данной системы.

ТЕОРЕМА 1.9. *Конечная система векторов, содержащая хотя бы один ненулевой вектор, обладает базисом. Любые два базиса данной конечной системы векторов состоят из одинакового числа векторов.*

Доказательство. Пусть задана система векторов

(1) $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k, \ldots, \boldsymbol{u}_m,$

содержащая ненулевой вектор. Нулевые векторы можно исключить из системы (1), так как получающаяся при этом система эквивалентна исходной. Поэтому будем считать, что $\boldsymbol{u}_1 \neq \boldsymbol{0}$. Если система (1) линейно независима, то она есть базис этой системы.

Если система (1) линейно зависима, то, по свойству 1.3, существует вектор, например вектор $\boldsymbol{u}_k$, равный линейной комбинации предшествующих ему векторов. Следовательно, подсистема

(2) $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{k-1}, \boldsymbol{u}_{k+1}, \ldots, \boldsymbol{u}_m$

эквивалентна исходной системе и содержит ненулевой вектор. Если система (2) линейно независима, то она есть базис системы (1). Если же система (2) линейно зависима, то из нее можно вычеркнуть вектор, являющийся линейной комбинацией предшествующих ему векторов, и т. д. После конечного числа вычеркиваний получается подсистема векторов, ни один вектор которой не выражается линейно через предшествующие векторы; эта подсистема является базисом системы (1), так как она линейно независима и не пуста (содержит вектор $\boldsymbol{u}_1$).

Пусть $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r$ и $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_s$ — два базиса системы векторов (1). Эти базисы эквивалентны, так как каждый из них эквивалентен системе (1). Следовательно, по теореме 1.7, эти базисы состоят из одинакового числа векторов, т. е. $r = s$. □

Ранг конечной системы векторов. Теперь введем понятие ранга системы векторов.

ОПРЕДЕЛЕНИЕ. *Рангом конечной системы векторов* называется число векторов, входящих в какой-нибудь базис системы. Ранг системы нулевых векторов и ранг пустой системы векторов считаются равными нулю.

Рассмотрим некоторые свойства ранга системы векторов.

ТЕОРЕМА 1.10. *Если* $u_1, \ldots, u_k \in L(v_1, \ldots, v_m)$, *то ранг системы векторов* $u_1, \ldots, u_k$ *меньше или равен рангу системы векторов* $v_1, v_2, \ldots, v_m$.

Доказательство. Если первая система $u_1, \ldots, u_k$ состоит из нулевых векторов, то ее ранг равен нулю и поэтому не превосходит ранга второй системы $v_1, \ldots, v_m$. Предположим, что первая система векторов содержит хотя бы один ненулевой вектор. Тогда из условия теоремы следует, что и вторая система имеет ненулевые векторы. Следовательно, по теореме 1.9, эти системы обладают базисами. Предположим, что $u_1, \ldots, u_r$ — базис первой системы, а $v_1, \ldots, v_s$ — базис второй системы. Тогда система $v_1, \ldots, v_s$ эквивалентна системе $v_1, \ldots, v_m$ и, по теореме 1.6,

$$L(v_1, \ldots, v_m) = L(v_1, \ldots, v_s).$$

Кроме того, по условию теоремы, $u_1, \ldots, u_k \in L(v_1, \ldots, v_m)$, поэтому $u_1, \ldots, u_r \in L(v_1, \ldots, v_s)$. По следствию 1.4, в силу линейной независимости системы векторов $u_1, \ldots, u_r$ отсюда следует, что $r \leqslant s$. Следовательно, ранг первой системы векторов не больше ранга второй системы. □

ПРЕДЛОЖЕНИЕ 1.11. *Ранг любой подсистемы конечной системы векторов не больше ранга всей системы.*

Доказательство. Это утверждение, очевидно, верно, если подсистема пуста. Если же подсистема не пуста, то предложение 1.11 непосредственно следует из теоремы 1.10. □

ПРЕДЛОЖЕНИЕ 1.12. *Эквивалентные конечные системы векторов имеют один и тот же ранг.*

Это предложение следует из теоремы 1.10.

ПРЕДЛОЖЕНИЕ 1.13. *Ранг любой конечной системы векторов n-мерного арифметического векторного пространства не больше n.*

Доказательство. Пусть $e_1, \ldots, e_n$ — единичные векторы арифметического векторного пространства $\mathcal{F}^n$. Любая система $a_1, \ldots, a_m$ векторов этого пространства содержится в линейной оболочке единичных векторов, $a_1, \ldots, a_m \in$

$\in L(e_1, \ldots, e_n) = F^n$. Следовательно, в силу теоремы 1.10 ранг системы векторов $a_1, \ldots, a_m$ не больше n.

ПРЕДЛОЖЕНИЕ 1.14. *Если конечная система векторов имеет ранг r, то любая ее подсистема из k векторов при $k > r$ линейно зависима.*

Доказательство. Это утверждение, очевидно, верно, если система состоит из нулевых векторов. Предположим, что $v_1, \ldots, v_m$ — данная система векторов, $v_1, \ldots, v_r$ — ее базис, $u_1, \ldots, u_k$ — подсистема данной системы; тогда

$$u_1, \ldots, u_k \in L(v_1, \ldots, v_r) = L(v_1, \ldots, v_m).$$

По следствию 1.3, при $k > r$ отсюда следует, что система векторов $u_1, \ldots, u_k$ линейно зависима. □

ПРЕДЛОЖЕНИЕ 1.15. *Пусть ранг системы векторов*

(1) $a_1, \ldots, a_m$

равен рангу системы векторов

(2) $a_1, \ldots, a_m, b$.

Тогда вектор b можно представить в виде линейной комбинации векторов системы (1).

Доказательство. Предложение, очевидно, верно, если ранги систем (1) и (2) равны нулю. Предположим, что ранг r системы (1) отличен от нуля и $a_1, \ldots, a_r$ — базис системы (1). Так как, по условию, ранг системы (2) также равен r, то ее подсистема $a_1, \ldots, a_r, b$ линейно зависима. По свойству 1.4, отсюда следует, что $b \in L(a_1, \ldots, a_r)$. Следовательно, $b \in L(a_1, \ldots, a_m)$, т. е. существуют такие скаляры $\lambda_1, \ldots, \lambda_m$, что

$$b = \lambda_1 a_1 + \ldots + \lambda_m a_m. \quad \square$$

Упражнения

1. Пусть (α, β) и (γ, δ) — векторы пространства $\mathcal{F}^2$. Покажите, что эти векторы тогда и только тогда линейно зависимы, когда $\alpha\delta - \beta\gamma = 0$.

2. Покажите, что арифметические n-мерные векторы a, b линейно зависимы тогда и только тогда, когда a и b пропорциональны, т. е. для некоторого скаляра λ $a = \lambda b$ или $b = \lambda a$.

3. Каким условиям должны удовлетворять скаляры β и γ, чтобы векторы (α, β) и (α, γ) были линейно зависимыми?

4. Докажите, что если к линейно независимой системе векторов $a_1, \ldots, a_m$ приписать слева или справа какой-нибудь вектор b, то не более чем один вектор полученной системы будет линейно выражаться через предыдущие.

5. Пусть $a_1, \ldots, a_m$ и $b_1, \ldots, b_m$ — две системы линейно независимых векторов. Докажите, что если $a_1, \ldots, a_m \in L(b_1, \ldots, b_m)$, то $b_1, \ldots, b_m \in L(a_1, \ldots, a_m)$.

6. Пусть $\mathcal{F}=\mathbb{Z}_2$ — поле вычетов по модулю 2 и $\mathcal{V}=\mathcal{F}^n$. Покажите, что $a+a=0$ для любого вектора $a\in V=F^n$.

7. Пусть $\mathcal{F}=\mathbb{Z}_3$ — поле классов вычетов по модулю 3 и $\mathcal{V}=\mathcal{F}^n$. Покажите, что $a+a+a=0$ для любого вектора $a\in V$.

8. Пусть $\mathcal{F}=\mathbb{Z}_3$ — поле классов вычетов по модулю 3 и n — целое положительное число. Сколько векторов содержит векторное пространство $\mathcal{F}^n$?

9. В каком случае система векторов обладает единственным базисом?

10. Докажите, что всякая линейно независимая подсистема r векторов системы векторов ранга r является базисом системы.

11. Пусть $a_1, \ldots, a_m$ — линейно независимая система векторов. Докажите, что $b\in L(a_1, \ldots, a_m)$ тогда и только тогда, когда система векторов $a_1, \ldots, a_m, b$ линейно зависима.

12. Докажите, что $b\in L(a_1, \ldots, a_m)$ тогда и только тогда, когда ранг системы векторов $a_1, \ldots, a_m$ равен рангу системы векторов $a_1, \ldots, a_m, b$.

13. Докажите, что две непустые эквивалентные линейно независимые системы векторов содержат одинаковое число векторов.

14. Покажите, что если две системы векторов имеют одинаковый ранг и векторы одной из этих систем линейно выражаются через векторы другой системы, то эти системы эквивалентны.

§ 2. СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ

Следствия системы линейных уравнений. Всюду ниже $\mathcal{F}$ — поле, поле скаляров.

ОПРЕДЕЛЕНИЕ. *Системой линейных уравнений над полем $\mathcal{F}$ с переменными $x_1, \ldots, x_n$* называется система вида

$$\alpha_{11}x_1+\ldots+\alpha_{1n}x_n=\beta_1,$$
$$\ldots\ldots\ldots\ldots$$
$$\alpha_{m1}x_1+\ldots+\alpha_{mn}x_n=\beta_m,$$

где $\alpha_{ik}, \beta_l\in F$.

Эту систему m линейных уравнений будем кратко записывать в виде

$$(1)\quad \alpha_{i1}x_1+\ldots+\alpha_{in}x_n=\beta_i \quad (i=1, \ldots, m).$$

Система линейных уравнений (1) является предикатом (условием) с n свободными переменными $x_1, \ldots, x_n$. Допустимыми значениями свободных переменных всюду ниже считаются элементы поля скаляров $\mathcal{F}$. Этот n-местный предикат является конъюнкцией m более простых n-местных предикатов, каждый из которых определяется одним из уравнений системы (1).

ОПРЕДЕЛЕНИЕ. Вектор $(\xi_1, \ldots, \xi_n)$ из F^n называется *решением системы уравнений* (1), если верны равенства

$$\alpha_{i1}\xi_1+\ldots+\alpha_{in}\xi_n=\beta_i \quad (i=1, \ldots, m).$$

ОПРЕДЕЛЕНИЕ. Система линейных уравнений называется *совместной*, если она имеет хотя бы одно решение. Система линейных уравнений называется *несовместной*, если она не имеет решений, т. е. множество всех ее решений пусто.

Наряду с системой (1) рассмотрим систему (над $\mathcal{F}$)

$$(2)\quad \gamma_{i1}x_1 + \ldots + \gamma_{in}x_n = \delta_i \quad (i = 1, \ldots, s).$$

Отметим, что система линейных уравнений может состоять из одного уравнения.

ОПРЕДЕЛЕНИЕ. Система уравнений (2) называется *следствием системы уравнений* (1), если каждое решение системы (1) является также решением системы (2).

Запись $(1) \Rightarrow (2)$ означает, что система (2) есть следствие системы (1).

Любая система линейных уравнений (над $\mathcal{F}$) с n переменными является следствием несовместной системы уравнений (над $\mathcal{F}$) с теми же переменными.

Система линейных уравнений (2) есть следствие системы уравнений (1) тогда и только тогда, когда множество всех решений системы (1) является подмножеством множества всех решений системы (2).

Легко убедиться, что бинарное отношение следования на множестве систем линейных уравнений (над $\mathcal{F}$) рефлексивно и транзитивно, т. е. является предпорядком.

ОПРЕДЕЛЕНИЕ. Линейное уравнение

$$(\lambda_1\alpha_{11} + \ldots + \lambda_m\alpha_{m1})x_1 + \ldots + (\lambda_1\alpha_{1n} + \ldots + \lambda_m\alpha_{mn})x_n = \\ = \lambda_1\beta_1 + \ldots + \lambda_m\beta_m,$$

где $\lambda_1, \ldots, \lambda_m$ — произвольные элементы поля $\mathcal{F}$, называется *линейной комбинацией уравнений системы* (1) с коэффициентами $\lambda_1, \ldots, \lambda_m$.

ПРЕДЛОЖЕНИЕ 2.1. *Любая линейная комбинация линейных уравнений системы уравнений (1) является следствием этой системы.*

Доказательство этого предложения предоставляется читателю.

Равносильные системы линейных уравнений и элементарные преобразования системы. Ниже рассматриваются системы линейных уравнений над полем $\mathcal{F}$ с n переменными $x_1, \ldots, x_n$.

ОПРЕДЕЛЕНИЕ. Две системы линейных уравнений называются *равносильными*, если каждое решение любой из этих систем является решением другой системы.

Следующие предложения выражают свойства равносильности, вытекающие из определения равносильности и отмеченных выше свойств следования систем.

ПРЕДЛОЖЕНИЕ 2.2. *Две системы линейных уравнений равносильны тогда и только тогда, когда каждая из этих систем является следствием другой системы.*

ПРЕДЛОЖЕНИЕ 2.3. *Две системы линейных уравнений равносильны тогда и только тогда, когда множество всех решений одной системы совпадает с множеством всех решений другой системы.*

ПРЕДЛОЖЕНИЕ 2.4. *Две системы линейных уравнений равносильны в том и только в том случае, если равносильны предикаты, определяемые этими системами.*

ОПРЕДЕЛЕНИЕ. *Элементарными преобразованиями системы линейных уравнений* называются следующие преобразования:

(α) умножение обеих частей какого-нибудь уравнения системы на отличный от нуля скаляр;

(β) прибавление (вычитание) к обеим частям какого-либо уравнения системы соответствующих частей другого уравнения системы, умноженных на скаляр;

(γ) исключение из системы или присоединение к системе линейного уравнения с нулевыми коэффициентами и нулевым свободным членом.

ТЕОРЕМА 2.5. *Если одна система линейных уравнений получается из другой системы линейных уравнений в результате цепочки элементарных преобразований, то эти две системы равносильны.*

Доказательство. Пусть дана система

$$(1)\quad \begin{aligned} &\alpha_{11}x_1+\ldots+\alpha_{1n}x_n=\beta_1,\\ &\ldots\ldots\ldots\ldots\ldots\\ &\alpha_{m1}x_1+\ldots+\alpha_{mn}x_n=\beta_m. \end{aligned}$$

Если умножить одно из ее уравнений, например первое, на отличный от нуля скаляр λ, то получим систему

$$(2)\quad \begin{aligned} &\lambda\alpha_{11}x_1+\ldots+\lambda\alpha_{1n}x_n=\lambda\beta_1,\\ &\ldots\ldots\ldots\ldots\ldots\\ &\alpha_{m1}x_1+\ldots+\alpha_{mn}x_n=\beta_m. \end{aligned}$$

Каждое решение системы (1) есть также решение системы (2).

Обратно: если $(\xi_1, \ldots, \xi_n)$ — любое решение системы (2), т. е.

$$\lambda\alpha_{11}\xi_1 + \ldots + \lambda\alpha_{1n}\xi_n = \lambda\beta_1,$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\alpha_{m1}\xi_1 + \ldots + \alpha_{mn}\xi_n = \beta_m,$$

то, умножив первое равенство на λ^{-1} и не изменяя последующих равенств, получим равенства, показывающие, что вектор $(\xi_1, \ldots, \xi_n)$ является решением системы (1). Следовательно, система (2) равносильна исходной системе (1). Так же легко проверить, что однократное применение к системе (1) элементарного преобразования (β) или (γ) приводит к системе, равносильной исходной системе (1). Так как отношение равносильности транзитивно, то многократное применение элементарных преобразований приводит к системе уравнений, равносильной исходной системе (1). □

СЛЕДСТВИЕ 2.6. *Если к одному из уравнений системы линейных уравнений прибавить линейную комбинацию других уравнений системы, то получится система уравнений, равносильная исходной.*

СЛЕДСТВИЕ 2.7. *Если исключить из системы линейных уравнений или присоединить к ней уравнение, являющееся линейной комбинацией других уравнений системы, то получится система уравнений, равносильная исходной системе.*

Равенство строчечного и столбцового рангов матрицы. Пусть $\mathcal{F}$ — поле. Таблица вида

$$(1) \qquad A = \begin{bmatrix} \alpha_{11} \ldots \alpha_{1n} \\ \ldots\ldots\ldots \\ \alpha_{m1} \ldots \alpha_{mn} \end{bmatrix},$$

где $\alpha_{ik} \in F$, называется *матрицей* над полем $\mathcal{F}$ или $m \times n$-матрицей над $\mathcal{F}$. Введем следующие обозначения для строк и столбцов матрицы: i-я строка матрицы обозначается через A_i, $A_i = [\alpha_{i1}, \ldots, \alpha_{in}]$; k-й столбец матрицы обозначается через A^k:

$$A^k = \begin{bmatrix} \alpha_{1k} \\ \vdots \\ \alpha_{mk} \end{bmatrix}.$$

Строки матрицы A можно рассматривать как n-мерные

арифметические векторы над $\mathcal{F}$. Столбцы матрицы A можно рассматривать как m-мерные векторы над $\mathcal{F}$.

ОПРЕДЕЛЕНИЕ. *Строчечным рангом матрицы* A называется ранг системы ее строк $A_1, \ldots, A_m$, рассматриваемых как n-мерные векторы над $\mathcal{F}$. *Столбцовым рангом матрицы* A называется ранг системы ее столбцов $A^1, \ldots, A^n$, рассматриваемых как m-мерные векторы над $\mathcal{F}$.

Строчечный ранг матрицы A обозначается через $r(A)$, столбцовый ранг матрицы A обозначим через $\rho(A)$.

Матрица, получающаяся из матрицы A в результате замены ее строк соответствующими столбцами, называется *транспонированной* к A и обозначается ${}^tA$,

$$ {}^tA = \begin{bmatrix} \alpha_{11} \ldots \alpha_{m1} \\ \cdots\cdots \\ \alpha_{1n} \ldots \alpha_{mn} \end{bmatrix}. $$

Символами $r({}^tA)$ и $\rho({}^tA)$ обозначаются соответственно строчечный и столбцовый ранги матрицы ${}^tA$.

Пусть

$$ (1) \quad \begin{aligned} &\alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = 0, \\ &\cdots\cdots\cdots\cdots \\ &\alpha_{m1}x_1 + \ldots + \alpha_{mn}x_n = 0 \end{aligned} $$

— однородная система линейных уравнений. Матрица A

$$ A = \begin{bmatrix} \alpha_{11} \ldots \alpha_{1n} \\ \cdots\cdots \\ \alpha_{m1} \ldots \alpha_{mn} \end{bmatrix} $$

называется *матрицей* или *основной матрицей системы уравнений* (1).

ТЕОРЕМА 2.8. *Если однородная система линейных уравнений над полем* $\mathcal{F}$

$$ (1) \quad \begin{aligned} &\alpha_{11}\lambda_1 + \ldots + \alpha_{1n}\lambda_n = 0, \\ &\cdots\cdots\cdots\cdots \\ &\alpha_{k1}\lambda_1 + \ldots + \alpha_{kn}\lambda_n = 0, \\ &\cdots\cdots\cdots\cdots \\ &\alpha_{m1}\lambda_1 + \ldots + \alpha_{mn}\lambda_n = 0 \end{aligned} $$

с переменными $\lambda_1, \ldots, \lambda_n$ *равносильна системе*

$$ (2) \quad \begin{aligned} &\alpha_{11}\lambda_1 + \ldots + \alpha_{1n}\lambda_n = 0, \\ &\cdots\cdots\cdots\cdots \\ &\alpha_{k1}\lambda_1 + \ldots + \alpha_{kn}\lambda_n = 0, \end{aligned} $$

состоящей из первых k уравнений системы (1), *то столбцовые ранги основных матриц этих систем равны.*

Доказательство. Пусть A и $\bar{A}$ — основные матрицы систем уравнений (1) и (2) соответственно. Если матрица $\bar{A}$ — нулевая, то всякий вектор из F^n является решением системы (2). В силу равносильности систем (1) и (2) отсюда вытекает, что всякий вектор из F^n является решением системы (1). Следовательно, матрица A — нулевая и ее ранг равен нулю.

Предположим теперь, что $\bar{A}$ — ненулевая матрица и

(3) $\bar{A}^1, \ldots, \bar{A}^r$

— базис системы столбцов матрицы $\bar{A}$. Тогда в силу равносильности систем (1) и (2) система $A^1, \ldots, A^r$ первых r столбцов матрицы A линейно независима. Если $r < s \leqslant n$, то система столбцов $A^1, \ldots, A^r, A^s$ линейно зависима. В противном случае в силу равносильности (1) и (2) была бы линейно независима система $\bar{A}^1, \ldots, \bar{A}^r, \bar{A}^s$ столбцов матрицы $\bar{A}$, что противоречило бы предположению (3). Таким образом, система $A^1, \ldots, A^r$ есть базис системы столбцов матрицы A. Следовательно, столбцовые ранги матриц A и $\bar{A}$ равны. □

ТЕОРЕМА 2.9. *Строчечный ранг матрицы равен ее столбцовому рангу.*

Доказательство. Теорема, очевидно, верна для нулевых матриц. Предположим, что $A = \|\alpha_{ik}\|$ — ненулевая матрица над полем $\mathcal{F}$ и первые r строк образуют базис системы строк этой матрицы. Рассмотрим однородную систему линейных уравнений над $\mathcal{F}$

$$\begin{aligned}
&\alpha_{11}\lambda_1 + \ldots + \alpha_{1n}\lambda_n = 0,\\
&\ldots\ldots\ldots\ldots\\
(1)\quad &\alpha_{r1}\lambda_1 + \ldots + \alpha_{rn}\lambda_n = 0,\\
&\ldots\ldots\ldots\ldots\\
&\alpha_{m1}\lambda_1 + \ldots + \alpha_{mn}\lambda_n = 0
\end{aligned}$$

относительно переменных $\lambda_1, \ldots, \lambda_n$, для которой A является основной матрицей. Рассмотрим также однородную систему

$$\begin{aligned}
&\alpha_{11}\lambda_1 + \ldots + \alpha_{1n}\lambda_n = 0,\\
(2)\quad &\ldots\ldots\ldots\ldots\\
&\alpha_{r1}\lambda_1 + \ldots + \alpha_{rn}\lambda_n = 0,
\end{aligned}$$

состоящую из первых r уравнений системы (1); ее основную матрицу обозначим через $\bar{A}$. Так как первые r строк

матрицы A образуют базис системы ее строк, то каждое уравнение системы (1) есть линейная комбинация уравнений системы (2). Следовательно, системы уравнений (1) и (2) равносильны. По теореме 2.8, из равносильности систем (1) и (2) следует равенство столбцовых рангов основных матриц этих систем, т. е.

(3) $\rho(A)=\rho(\bar{A})$.

Поскольку столбцы матрицы $\bar{A}$ суть r-мерные векторы над полем $\mathcal{F}$, то, по следствию 1.6, $\rho(\bar{A})\leqslant r=r(A)$. Следовательно, в силу (3)

(4) $\rho(A)\leqslant r(A)$.

Аналогичное неравенство верно также для транспонированной матрицы ${}^tA$, т. е.

(5) $\rho({}^tA)\leqslant r({}^tA)$.

Легко видеть, что $\rho({}^tA)=r(A)$, $r({}^tA)=\rho(A)$. Отсюда в силу (5) получим, что

(6) $r(A)\leqslant\rho(A)$.

На основании (4) и (6) заключаем, что $r(A)=\rho(A)$. □

Критерий совместности системы линейных уравнений. Рассмотрим систему линейных уравнений над полем $\mathcal{F}$:

(1) $\alpha_{i1}x_1+\ldots+\alpha_{in}x_n=\beta_i \quad (i=1, \ldots, m)$.

Матрицы

$$A=\begin{bmatrix}\alpha_{11}\ldots\alpha_{1n}\\ \cdots\cdots\\ \alpha_{m1}\ldots\alpha_{mn}\end{bmatrix} \quad \text{и} \quad B=\begin{bmatrix}\alpha_{11}\ldots\alpha_{1n}\beta_1\\ \cdots\cdots\cdots\\ \alpha_{m1}\ldots\alpha_{mn}\beta_m\end{bmatrix}$$

называются соответственно *основной* и *расширенной матрицами* системы уравнений (1). Вектор $\boldsymbol{b}$

$$\boldsymbol{b}=\begin{bmatrix}\beta_1\\ \vdots\\ \beta_m\end{bmatrix}$$

называется *столбцом свободных членов*.

Рассмотрим уравнение (над полем $\mathcal{F}$)

(2) $x_1A^1+\ldots+x_nA^n=\boldsymbol{b}$,

где $A^1, \ldots, A^n$ — вектор-столбец матрицы A.

ТЕОРЕМА 2.10. *Уравнение* (2) *равносильно системе уравнений* (1).

Доказательство. Пусть $(\xi_1, \ldots, \xi_n)$ — любое решение системы (1), т. е.

(3) $\alpha_{i1}\xi_1 + \ldots + \alpha_{in}\xi_n = \beta_i \quad (i = 1, \ldots, m)$.

Учитывая, что

$$(4)\quad \xi_1 A^1 + \ldots + \xi_n A^n = \begin{bmatrix} \alpha_{11}\xi_1 + \ldots + \alpha_{1n}\xi_n \\ \cdots\cdots\cdots\cdots \\ \alpha_{m1}\xi_1 + \ldots + \alpha_{mn}\xi_n \end{bmatrix},$$

равенства (3) можно записать в виде одного равенства

(2′) $\xi_1 A^1 + \ldots + \xi_n A^n = \boldsymbol{b}$.

Обратно: предположим, что вектор $(\xi_1, \ldots, \xi_n)$ есть решение уравнения (2), т. е. имеет место равенство (2′). Тогда в силу (4) из (2′) вытекают равенства (3). Таким образом, любое решение уравнения (2) является решением системы (1). Следовательно, уравнение (2) равносильно системе уравнений (1). □

СЛЕДСТВИЕ 2.11. *Однородная система линейных уравнений*

$$\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \quad (i = 1, \ldots, m)$$

равносильна уравнению

$$x_1 A^1 + \ldots + x_n A^n = \mathbf{0},$$

где $\mathbf{0}$ *— нулевой* m*-мерный вектор-столбец.*

Уравнение (2) называется *векторной формой записи системы линейных уравнений* (1).

ТЕОРЕМА 2.12. *Пусть* A *и* B *— соответственно основная и расширенная матрицы системы линейных уравнений* (1). *Равносильны следующие утверждения*:

I. *Система линейных уравнений (1) совместна.*

II. *Уравнение (2) имеет решение (над полем* $\mathcal{F}$*).*

III. *Вектор* $\boldsymbol{b}$ *есть линейная комбинация столбцов матрицы* A, т. е. $\boldsymbol{b} \in L(A^1, \ldots, A^n)$.

IV. *Столбцовые* (*строчечные*) *ранги матриц* A *и* B *равны,* $r(A) = r(B)$.

Доказательство. В силу теоремы 2.10 утверждение I влечет утверждение II.

Если уравнение (2) имеет решение, то вектор $\boldsymbol{b}$ можно представить в виде линейной комбинации (с коэффициен-

тами из поля $\mathscr{F}$) столбцов матрицы A. Следовательно, из II следует III.

Если $\boldsymbol{b} \in L(A^1, \ldots, A^n)$, то система столбцов $A^1, \ldots, A^n$ матрицы A эквивалентна системе столбцов $A^1, \ldots, A^n, b$ матрицы B. По предложению 1.12, это влечет равенство столбцовых рангов матриц A и B. Следовательно, утверждение III влечет IV.

Предположим, что столбцовые ранги матриц A и B равны. Тогда базис системы столбцов матрицы A является также базисом системы столбцов матрицы B. Следовательно, $\boldsymbol{b} \in L(A^1, \ldots, A^n)$, т. е. существуют такие скаляры $\lambda_1, \ldots, \lambda_n \in F$, что $\lambda_1 A^1 + \ldots + \lambda_n A^n = \boldsymbol{b}$. Последнее равенство означает, что вектор $(\lambda_1, \ldots, \lambda_n)$ есть решение уравнения (2) и в силу теоремы 2.10 — решение системы уравнений (1). Таким образом, из утверждения IV следует утверждение I. Следовательно, утверждения I, II, III и IV равносильны. □

ТЕОРЕМА 2.13 (КРОНЕКЕР — КАПЕЛЛИ). *Система линейных уравнений совместна тогда и только тогда, когда ранг основной матрицы системы равен рангу расширенной матрицы.*

Эта теорема непосредственно следует из предыдущей теоремы.

СЛЕДСТВИЕ 2.14. *Если ранг основной матрицы системы линейных уравнений равен числу уравнений системы, то система уравнений совместна.*

Доказательство. Пусть A и B — соответственно основная и расширенная матрицы системы m линейных уравнений с n переменными. Тогда $\rho(B) \geqslant \rho(A) = m$. С другой стороны, $\rho(B) \leqslant m$, так как матрица B имеет m строк. Поэтому $\rho(B) = \rho(A)$. Следовательно, по теореме 2.13, рассматриваемая система линейных уравнений совместна. □

Связь между решениями неоднородной линейной системы и решениями ассоциированной с ней однородной системы. Пусть дана неоднородная линейная система

$$(1)\quad \alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = \beta_i \qquad (i = 1, \ldots, m)$$

над полем $\mathscr{F}$. Система линейных уравнений

$$(2)\quad \alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \qquad (i = 1, \ldots, m)$$

называется *однородной системой*, ассоциированной с системой (1).

Пусть L — множество всех решений однородной системы (2) и $\boldsymbol{c}$ — какое-нибудь решение системы (1). Мно-

жество $\{c+d \mid d \in L\}$ обозначим через $c+L$:

$$c+L=\{c+d \mid d \in L\}.$$

ПРЕДЛОЖЕНИЕ 2.15. *Если решение неоднородной системы* (1) *сложить с решением однородной системы* (2), *то получится решение системы* (1).

Доказательство. Пусть $(\gamma_1, \ldots, \gamma_n)$ — решение системы (1) и $(\delta_1, \ldots, \delta_n)$ — решение системы (2), т. е.

$$\alpha_{i1}\gamma_1+\ldots+\alpha_{in}\gamma_n=\beta_i \qquad (i=1, \ldots, m);$$
$$\alpha_{i1}\delta_1+\ldots+\alpha_{in}\delta_n=0 \qquad (i=1, \ldots, m).$$

Почленно складывая эти равенства, получим равенства

$$\alpha_{i1}(\gamma_1+\delta_1)+\ldots+\alpha_{in}(\gamma_n+\delta_n)=\beta_i \qquad (i=1, \ldots, m),$$

которые показывают, что вектор $(\gamma_1+\delta_1, \ldots, \gamma_n+\delta_n)$ является решением системы (1). □

ПРЕДЛОЖЕНИЕ 2.16. *Разность любых двух решений неоднородной системы линейных уравнений является решением ассоциированной с ней однородной системы.*

Доказательство. Пусть $(\gamma_1, \ldots, \gamma_n)$ и $(\gamma_1', \ldots, \gamma_n')$ — решения неоднородной системы уравнений (1), т. е.

$$\alpha_{i1}\gamma_1+\ldots+\alpha_{in}\gamma_n=\beta_i \qquad (i=1, \ldots, m),$$
$$\alpha_{i1}\gamma_1'+\ldots+\alpha_{in}\gamma_n'=\beta_i \qquad (i=1, \ldots, m).$$

Почленное вычитание приводит к равенствам

$$\alpha_{i1}(\gamma_1-\gamma_1')+\ldots+\alpha_{in}(\gamma_n-\gamma_n')=0 \qquad (i=1, \ldots, m),$$

которые показывают, что вектор $(\gamma_1-\gamma_1', \ldots, \gamma_n-\gamma_n')$ является *решением однородной системы уравнений* (2). □

ТЕОРЕМА 2.17. *Пусть* c — *решение неоднородной системы линейных уравнений* (1) *и* L — *множество всех решений однородной системы* (2), *ассоциированной с системой* (1). *Тогда* $c+L$ *является множеством всех решений системы* (1).

Доказательство. Пусть M — множество всех решений системы (1) и $c \in M$. Каждый элемент множества $c+L$ можно представить в виде суммы $c+l$, где $l \in L$. В силу предложения 2.15 $c+l \in M$. Следовательно,

(3) $c+L \subset M$.

Верно и обратное включение. В самом деле, если $\boldsymbol{d}$ — любое решение системы (1), $\boldsymbol{c} \in M$, то в силу предложения 2.16 $\boldsymbol{d} - \boldsymbol{c} \in L$. Поэтому $\boldsymbol{d} \in \boldsymbol{c} + L$; следовательно,

(4) $M \subset \boldsymbol{c} + L$.

На основании (3) и (4) заключаем, что $M = \boldsymbol{c} + L$. □

СЛЕДСТВИЕ 2.18. *Совместная неоднородная система линейных уравнений имеет единственное решение тогда и только тогда, когда ассоциированная с нею однородная система уравнений имеет единственное решение (нулевое).*

СЛЕДСТВИЕ 2.19. *Если две неоднородные системы линейных уравнений (над полем $\mathscr{F}$) с n переменными $x_1, \ldots, x_n$ совместны и равносильны, то ассоциированные с ними однородные системы уравнений равносильны.*

Теоремы о следствиях системы линейных уравнений. Рассмотрим систему линейных уравнений

(I) $\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = \beta_i \qquad (i = 1, \ldots, m)$

над полем $\mathscr{F}$. Линейное уравнение

(II) $\gamma_1 x_1 + \ldots + \gamma_n x_n = \beta,$

где $\gamma_1, \ldots, \gamma_n \in F$, называется *следствием системы* (I), если каждое решение системы (I) является решением этого уравнения.

Согласно предложению 2.1, любая линейная комбинация (с коэффициентами из поля $\mathscr{F}$) уравнений системы (I) является следствием этой системы. Верно ли обратное утверждение? Ответ на этот вопрос дают следующие ниже теоремы.

ТЕОРЕМА 2.20. *Линейное уравнение*

(2) $\gamma_1 x_1 + \ldots + \gamma_n x_n = 0,$

являющееся следствием однородной системы уравнений

(1) $\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \qquad (i = 1, \ldots, m),$

есть линейная комбинация уравнений этой системы.

Доказательство. По условию, уравнение (2) есть следствие системы (1). Следовательно, система

$$
(3)\quad \begin{array}{l}
\alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = 0, \\
\ldots\ldots\ldots\ldots \\
\alpha_{m1}x_1 + \ldots + \alpha_{mn}x_n = 0, \\
\gamma_1 x_1 + \ldots + \gamma_n x_n = 0
\end{array}
$$

равносильна системе (1). По теоремам 2.8 и 2.9, отсюда вытекает, что ранг матрицы A системы (1) равен рангу матрицы $\bar{A}$ системы (3). Поэтому если $c=(\gamma_1, \ldots, \gamma_n)$, то

$$\text{ранг } \{A_1, \ldots, A_m, c\} = \text{ранг } \{A_1, \ldots, A_m\},$$

где A_i есть i-я строка матрицы A. На основании этого равенства заключаем, что c есть линейная комбинация строк $A_1, \ldots, A_m$ матрицы A. Следовательно, уравнение (2) является линейной комбинацией уравнений системы (1). □

ТЕОРЕМА 2.21. *Две однородные системы линейных уравнений над полем $\mathcal{F}$ с n переменными $x_1, \ldots, x_n$ равносильны тогда и только тогда, когда матрицы этих систем строчечно эквивалентны.*

Эта теорема легко следует из теоремы 2.20.

ТЕОРЕМА 2.22. *Линейное уравнение, являющееся следствием совместной системы линейных уравнений, есть линейная комбинация уравнений этой системы.*

Доказательство. Предположим, что уравнение (II) есть следствие совместной системы (I). Тогда система уравнений

$$(3)\quad \begin{aligned} &\alpha_{11}x_1+\ldots+\alpha_{1n}x_n=\beta_1,\\ &\ldots\ldots\ldots\ldots\ldots\\ &\alpha_{m1}x_1+\ldots+\alpha_{mn}x_n=\beta_m,\\ &\gamma_1x_1+\ldots+\gamma_nx_n=\beta \end{aligned}$$

совместна и равносильна системе (I). По следствию 2.19, отсюда вытекает равносильность соответствующих однородных систем, т. е. система уравнений

$$4)\quad \alpha_{i1}x_1+\ldots+\alpha_{in}x_n=0 \qquad (i=1, \ldots, m)$$

равносильна системе уравнений

$$(5)\quad \begin{aligned} &\alpha_{11}x_1+\ldots+\alpha_{1n}x_n=0,\\ &\ldots\ldots\ldots\ldots\ldots\\ &\alpha_{m1}x_1+\ldots+\alpha_{mn}x_n=0,\\ &\gamma_1x_1+\ldots+\gamma_nx_n=0. \end{aligned}$$

В силу теорем 2.8 и 2.9 ранг основной матрицы A системы (4) равен рангу основной матрицы $\bar{A}$ системы (5). Следовательно, равны ранги основных матриц систем (I) и (3). Поскольку системы (1) и (3) совместны, то по критерию совместности отсюда вытекает, что строчечный ранг расширенной матрицы B системы (1) равен строчечному

рангу расширенной матрицы $\bar{B}$ системы (3). На основании равенства этих рангов заключаем, что последняя строка матрицы $\bar{B}$ является линейной комбинацией строк матрицы B, т. е.

$$(\gamma_1, \ldots, \gamma_n, \beta) \in L(B_1, \ldots, B_n).$$

Следовательно, уравнение (II) является линейной комбинацией уравнений системы (I). □

Упражнения.

1. Пусть A — $n \times m$-матрица с линейно независимыми строками. Докажите, что $m \geqslant n$.

2. Докажите, что ранг r $m \times n$-матрицы не больше m и n, $r \leqslant \min(m, n)$.

3. Докажите, что вычеркивание одной строки (столбца) матрицы тогда и только тогда не изменяет ее ранга, когда вычеркнутая строка (столбец) линейно выражается через остальные строки (столбцы).

4. Докажите, что приписывание к матрице одной строки (или одного столбца) либо не изменяет ранга матрицы, либо увеличивает его на единицу.

5. Докажите, что если ранг матрицы A не изменяется от приписывания к ней любого столбца матрицы B с тем же числом строк, то он не меняется от приписывания к матрице A всех столбцов матрицы B.

6. Пусть матрица B получается из матрицы A в результате цепочки неособенных строчечных линейных преобразований. Докажите, что строки матрицы A линейно независимы тогда и только тогда, когда линейно независимы строки матрицы B.

7. Пусть A и B — матрицы с n столбцами. Докажите, что матрицы A и B строчечно эквивалентны, когда линейная оболочка строк матрицы A совпадает с линейной оболочкой строк матрицы B.

8. Пусть A — $m \times n$-матрица и B — $m \times (n+k)$-матрица, получающаяся из матрицы A в результате приписывания k новых столбцов. Докажите, что:

(a) если строки матрицы B линейно зависимы, то строки матрицы A линейно зависимы;

(b) если строки матрицы A линейно независимы, то строки матрицы B линейно независимы;

(c) ранг матрицы A не превосходит ранга матрицы B.

9. Ранг основной матрицы однородной системы линейных уравнений на единицу меньше числа переменных. Докажите, что любые два решения этой системы пропорциональны (т. е. отличаются лишь скалярным множителем).

10. Найдите условия, при которых в любом решении однородной системы линейных уравнений k-е переменное равно нулю.

11. Докажите, что если система линейных уравнений над полем $\mathbb{Q}$ рациональных чисел не имеет решений в $\mathbb{Q}$, то она не имеет решений в любом числовом поле.

12. Пусть дана однородная система линейных уравнений (1) (над полем $\mathbb{Q}$ рациональных чисел), имеющая ненулевые решения. Любая фундаментальная система решений системы (1) над $\mathbb{Q}$ является фундаментальной системой над любым числовым полем.

13. Пусть

(1) $\alpha_{i1}x_1+\ldots+\alpha_{in}x_n=0 \qquad (i=1, \ldots, m)$

— однородная система линейных уравнений (над полем $\mathcal{F}$). Докажите, что уравнение

$$\beta_1x_1+\ldots+\beta_nx_n=0$$

является следствием системы (1) тогда и только тогда, когда оно является линейной комбинацией уравнений (1).

§ 3. СТУПЕНЧАТЫЕ МАТРИЦЫ И СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ

Ступенчатые матрицы. Пусть

$$A=\begin{bmatrix}\alpha_{11} & \ldots & \alpha_{1n}\\ \cdot & \cdots & \cdot\\ \alpha_{m1} & \ldots & \alpha_{mn}\end{bmatrix}$$

— $m\times n$-матрица над полем $\mathcal{F}$. *Ведущим элементом строки матрицы* называется первый (считая слева направо) ненулевой элемент строки. Столбец матрицы называется *основным*, если он содержит ведущий элемент какой-либо строки матрицы.

ОПРЕДЕЛЕНИЕ. Матрица A называется *ступенчатой*, если она удовлетворяет условиям:

(1) нулевые строки матрицы (если они есть) расположены ниже всех ненулевых строк;

(2) если α_{1k_1}, α_{2k_2}, ..., α_{rk_r} — ведущие элементы ненулевых строк матрицы, то $k_1<k_2<\ldots<k_r$.

Примеры ступенчатых матриц: 1) нулевая матрица, 2) однострочная матрица, 3) единичная матрица, 4) верхнетреугольная матрица

$$\begin{bmatrix}\alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n}\\ 0 & \alpha_{22} & \ldots & \alpha_{2n}\\ \cdot & \cdot & \cdots & \cdot\\ 0 & 0 & \ldots & \alpha_{nn}\end{bmatrix}.$$

Над системой вектор-строк (столбцов) данной матрицы можно проводить элементарные преобразования.

ОПРЕДЕЛЕНИЕ. Элементарные преобразования над системой строк (столбцов) матрицы называются *элементарными преобразованиями матрицы*. Две матрицы называются *строчечно-эквивалентными*, если одна получается из дру-

гой при помощи цепочки элементарных преобразований над строками.

Отношение строчечной эквивалентности рефлексивно, симметрично и транзитивно, т. е. является отношением эквивалентности.

ОПРЕДЕЛЕНИЕ. *Строчечным рангом матрицы* называется ранг системы ее строк. *Столбцовым рангом матрицы* называется ранг системы ее столбцов.

Из этого определения в силу теоремы 1.8 следует предложение 3.1.

ПРЕДЛОЖЕНИЕ 3.1. *Если одна матрица получается из другой в результате цепочки элементарных преобразований над строками, то строчечные ранги этих матриц равны.*

ТЕОРЕМА 3.2. *Любая $m \times n$-матрица строчечно эквивалентна ступенчатой $m \times n$-матрице.*

Доказательство (проводится индукцией по числу строк матрицы). Если число строк матрицы равно единице, то матрица ступенчатая. Предполагая, что теорема верна для матриц с $m-1$ строками, докажем, что тогда она верна для матриц с m строками. Пусть A есть m-строчная матрица:

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

Если в первом столбце матрицы есть элемент, отличный от нуля, то строку с этим ненулевым элементом можно переставить с первой строкой. Легко показать, что перестановка строк — результат цепочки элементарных преобразований над строками. Поэтому будем считать, что $\alpha_{11} \neq 0$. Матрицу A можно преобразовать в матрицу B:

$$B = \begin{bmatrix} 1 & \beta_{12} & \dots & \beta_{1n} \\ 0 & \beta_{22} & \dots & \beta_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & \beta_{m2} & \dots & \beta_{mn} \end{bmatrix}$$

при помощи цепочки элементарных преобразований. Для этого первую строку матрицы A надо умножить на α_{11}^{-1}. Затем полученную первую строку, умноженную на $(-\alpha_{ik})$, прибавить к i-й строке для $i = 2, \dots, m$. Матрица, полу-

ченная из матрицы B вычеркиванием первой строки, содержит $m-1$ строк и, по индуктивному предположению, строчечно эквивалентна некоторой ступенчатой $(m-1)\times$ $\times n$-матрице C^*:

$$\begin{bmatrix} 0 & \beta_{22} & \dots & \beta_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & \beta_{m2} & \dots & \beta_{mn} \end{bmatrix} \sim C^* = \begin{bmatrix} 0 & \gamma_{22} & \dots & \gamma_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & \gamma_{m2} & \dots & \gamma_{mn} \end{bmatrix}.$$

На основании этого и строчечной эквивалентности матриц A и B заключаем, что матрица A строчечно эквивалентна ступенчатой матрице C:

$$C = \begin{bmatrix} 1 & \beta_{12} & \dots & \beta_{1n} \\ 0 & \gamma_{22} & \dots & \gamma_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & \gamma_{m2} & \dots & \gamma_{mn} \end{bmatrix}.$$

Матрица C — ступенчатая, потому что матрица C^* является ступенчатой.

Если первый столбец или несколько первых столбцов матрицы A — нулевые, то рассмотрим матрицу, получающуюся в результате вычеркивания этих столбцов. Эта матрица содержит в первом столбце ненулевой элемент. Поэтому из первой части доказательства следует, что она строчечно эквивалентна ступенчатой матрице. Легко видеть, что, приписав слева к этой ступенчатой матрице вычеркнутые прежде нулевые столбцы, получим матрицу, строчечно эквивалентную исходной матрице A. □

ТЕОРЕМА 3.3. *Строчечный ранг ступенчатой матрицы равен числу ее ненулевых строк.*

Доказательство. Теорема, очевидно, верна для нулевой матрицы. Предположим, что A — ступенчатая матрица с r ненулевыми строками. Для удобства записи будем считать, что ведущие элементы матрицы A расположены в первых r столбцах, т. е.

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1r} & \dots \\ 0 & \alpha_{22} & \dots & \alpha_{2r} & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_{rr} & \dots \\ 0 & 0 & \dots & 0 & \dots \end{bmatrix},$$

где $\alpha_{ii} \neq 0$ для $i = 1, \dots, r$. Таким образом, первые r строк $A_1, \dots, A_r$ матрицы A ненулевые, а остальные (если

они есть) — нулевые. Покажем, что строки $A_1, \ldots, A_r$ линейно независимы. Надо показать, что для любых скаляров $\lambda_1, \ldots, \lambda_r$ из равенства

$$(1)\quad \lambda_1 A_1 + \ldots + \lambda_r A_r = 0$$

следуют равенства

$$(2)\quad \lambda_1 = 0, \ldots, \lambda_r = 0.$$

Так как $\lambda_1 A_1 + \ldots + \lambda_r A_r =$
$= (\lambda_1 \alpha_{11}, \lambda_1 \alpha_{12} + \lambda_2 \alpha_{22}, \ldots, \lambda_1 \alpha_{1r} + \ldots + \lambda_r \alpha_{rr}, \ldots),$
то из (1) следуют равенства

$$(3)\quad \begin{aligned} &\lambda_1 \alpha_{11} = 0, \\ &\lambda_1 \alpha_{12} + \lambda_2 \alpha_{22} = 0, \\ &\ldots\ldots\ldots\ldots \\ &\lambda_1 \alpha_{1r} + \ldots + \lambda_r \alpha_{rr} = 0. \end{aligned}$$

Поскольку $\alpha_{ii} \neq 0$ при $i = 1, \ldots, r$, из (3) следуют равенства (2). Таким образом, система $A_1, \ldots, A_r$ ненулевых строк матрицы A линейно независима. Следовательно, строчечный ранг матрицы A равен r. В общем случае доказательство проводится аналогично. □

На основании теоремы 3.3 приходим к следующему правилу вычисления ранга матрицы. *Для вычисления строчечного ранга матрицы A надо привести ее к ступенчатому виду C при помощи цепочки элементарных преобразований над строками. Число ненулевых строк матрицы C равно строчечному рангу матрицы A.*

Приведенные ступенчатые матрицы. При решении и исследовании системы линейных уравнений важную роль играют приведенные ступенчатые матрицы.

ОПРЕДЕЛЕНИЕ. Ступенчатая матрица называется *приведенной*, если матрица, составленная из всех ее основных столбцов, является единичной матрицей.

Приведенная ступенчатая матрица не имеет нулевых строк, и все ведущие элементы ее строк равны единице.

ТЕОРЕМА 3.4. *Любая ненулевая матрица строчечно эквивалентна приведенной ступенчатой матрице.*

Доказательство. Пусть A — ненулевая матрица ранга r. По теоремам 3.2 и 3.3, она строчечно эквивалентна ступенчатой матрице, например матрице B, состоящей из r ненулевых строк. Разделим каждую строку матрицы B на ее ведущий элемент. В результате получим

ступенчатую матрицу C, у которой все ведущие элементы строк равны единице. Далее, при помощи цепочки строчечных элементарных преобразований матрицы C обращаем в нуль все ненулевые элементы, расположенные над ведущими элементами. В результате получим матрицу D, основные столбцы которой образуют единичную матрицу. Следовательно, D есть искомая приведенная ступенчатая матрица, строчечно эквивалентная исходной матрице A. □

ТЕОРЕМА 3.5. *Всякая квадратная $n\times n$-матрица с линейно независимыми строками строчечно эквивалентна единичной $n\times n$-матрице E.*

Доказательство. Пусть $A-n\times n$-матрица с линейно независимыми строками. При помощи цепочки неособенных элементарных строчечных преобразований ее можно привести к некоторой ступенчатой $n\times n$-матрице $C=\|\gamma_{ik}\|$. Пусть $\gamma_{1k_1}, \gamma_{2k_2}, \ldots, \gamma_{nk_n}$ — ведущие элементы матрицы C. Тогда

(1) $\gamma_{1k_1}\neq 0, \ldots, \gamma_{nk_n}\neq 0$,

(2) $1\leqslant k_1<k_2<\ldots<k_n\leqslant n$.

Из неравенств (2) следует, что $k_1=1$, $k_2=2, \ldots, k_n=n$. Поэтому матрица C имеет вид

$$C=\begin{bmatrix}\gamma_{11} & \gamma_{12} & \cdots & \gamma_{1n}\\ 0 & \gamma_{22} & \cdots & \gamma_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & \ldots & \gamma_{nn}\end{bmatrix},$$

т. е. является верхнетреугольной матрицей с ненулевыми элементами на главной диагонали. Умножим первую строку матрицы на γ_{11}^{-1}, вторую — на γ_{22}^{-1} и т. д. В результате получим строчечно эквивалентную матрицу

$$C'=\begin{bmatrix}1 & \gamma'_{12} & \cdots & \gamma'_{1n}\\ 0 & 1 & \ldots & \gamma'_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & \ldots & 1\end{bmatrix}.$$

Легко видеть, что матрица C' строчечно эквивалентна единичной $n\times n$-матрице E. Таким образом, существует цепочка (неособенных) строчечных элементарных преобразований, которая переводит матрицу A в единичную матрицу E. □

Однородные системы линейных уравнений. Рассмотрим однородную систему уравнений над полем $\mathcal{F}$

$$(1)\quad \begin{aligned} &\alpha_{11}x_1+\ldots+\alpha_{1n}x_n=0,\\ &\ldots\ldots\ldots\ldots\\ &\alpha_{m1}x_1+\ldots+\alpha_{mn}x_n=0. \end{aligned}$$

Пусть

$$A=\begin{bmatrix} \alpha_{11}\ldots\alpha_{1n}\\ \ldots\ldots\\ \alpha_{m1}\ldots\alpha_{mn} \end{bmatrix}$$

— матрица, составленная из коэффициентов при переменных и называемая основной *матрицей системы* (1), и $A^1, \ldots, A^n$ — столбцы этой матрицы. Уравнение (над $\mathcal{F}$).

$$(2)\quad x_1A^1+\ldots+x_nA^n=\mathbf{0},$$

где $\mathbf{0}$ — нулевой вектор-столбец, называется *векторной формой записи системы уравнений* (1).

По следствию 2.11, однородная система уравнений (1) равносильна уравнению (2).

ПРЕДЛОЖЕНИЕ 3.6. *Если матрица A однородной системы уравнений (1) имеет ранг $r>0$ и $A_1, \ldots, A_r$ — базис системы ее строк, то система (1) равносильна системе*

$$(3)\quad \begin{aligned} &\alpha_{11}x_1+\ldots+\alpha_{1n}x_n=0,\\ &\ldots\ldots\ldots\ldots\\ &\alpha_{r1}x_1+\ldots+\alpha_{rn}x_n=0, \end{aligned}$$

состоящей из первых r уравнений системы (1).

Доказательство. Так как первые r строк матрицы A образуют базис системы строк этой матрицы, то каждое уравнение системы (1) есть линейная комбинация уравнений (3). Кроме того, система (3) есть следствие системы (1). Следовательно, системы (1) и (3) равносильны. □

ПРЕДЛОЖЕНИЕ 3.7. *Однородная система линейных уравнений с матрицей A имеет ненулевые решения тогда и только тогда, когда столбцы матрицы A линейно зависимы.*

Это предложение непосредственно вытекает из следствия 2.11.

СЛЕДСТВИЕ 3.8. *Однородная система линейных уравнений с n переменными имеет ненулевые решения тогда и только тогда, когда ранг матрицы системы меньше n.*

СЛЕДСТВИЕ 3.9. *Если число уравнений однородной системы линейных уравнений меньше числа переменных, то система имеет ненулевые решения.*

ПРЕДЛОЖЕНИЕ 3.10. *Множество всех решений однородной системы замкнуто относительно сложения, вычитания и умножения на скаляры. Любая линейная комбинация решений однородной системы уравнений является решением этой системы.*

Доказательство предложения 3.10 предоставляется читателю.

Фундаментальная система решений. Пусть

$$(1)\ \alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0\ \ (i = 1, \ldots, m)$$

— однородная система линейных уравнений над полем $\mathcal{F}$.

ОПРЕДЕЛЕНИЕ. *Фундаментальной системой решений системы уравнений* (1) называется непустая линейно независимая система ее решений, линейная оболочка которой совпадает с множеством всех решений системы (1).

Отметим, что однородная система линейных уравнений, имеющая только нулевое решение, не имеет фундаментальной системы решений.

ПРЕДЛОЖЕНИЕ 3.11. *Любые две фундаментальные системы решений однородной системы линейных уравнений состоят из одинакового числа решений.*

Доказательство. В самом деле, любые две фундаментальные системы решений однородной системы уравнений (1) эквивалентны и линейно независимы. Поэтому в силу предложения 1.12 их ранги равны. Следовательно, число решений, входящих в одну фундаментальную систему, равно числу решений, входящих в любую другую фундаментальную систему решений. □

Если основная матрица A однородной системы уравнений (1) нулевая, то любой вектор из F^n является решением системы (1); в этом случае любая совокупность n линейно независимых векторов из F^n является фундаментальной системой решений. Если же столбцовый ранг матрицы A равен n, то система (1) имеет только одно решение — нулевое; следовательно, в этом случае система уравнений (1) не обладает фундаментальной системой решений.

ТЕОРЕМА 3.12. *Если ранг r основной матрицы однородной системы линейных уравнений* (1) *меньше числа переменных n, то система* (1) *обладает фундаментальной системой решений, состоящей из $n - r$ решений.*

Доказательство. Если ранг основной матрицы A однородной системы (1) равен нулю или n, то выше было показано, что теорема верна. Поэтому ниже предполагается, что $0<r(A)<n$. Полагая $r=r(A)$, будем считать, что первые r столбцов матрицы A линейно независимы. В этом случае матрица A строчечно эквивалентна приведенной ступенчатой матрице, а система (1) равносильна следующей приведенной ступенчатой системе уравнений:

$$
(2)\qquad
\begin{array}{l}
x_1 - \quad \ldots - \gamma_{11}x_{r+1} - \ldots - \gamma_{1,n-r}x_n = 0, \\
\quad x_2 - \ldots - \gamma_{21}x_{r+1} - \ldots - \gamma_{2,n-r}x_n = 0, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\qquad x_r - \gamma_{r1}x_{r+1} - \ldots - \gamma_{r,n-r}x_n = 0.
\end{array}
$$

Легко проверить, что любой системе значений свободных переменных $x_{r+1}, \ldots, x_n$ системы (2) соответствует одно и только одно решение системы (2) и, значит, системы (1). В частности, системе нулевых значений $x_{r+1}=0, \ldots, x_n=0$ соответствует только нулевое решение системы (2) и системы (1).

Будем в системе (2) придавать одному из свободных переменных значение, равное 1, а остальным переменным — нулевые значения. В результате получим $n-r$ решений системы уравнений (2), которые запишем в виде строк следующей матрицы C:

$$
C = \begin{bmatrix}
\gamma_{11} & \gamma_{21} & \ldots & \gamma_{r1} & 1 & 0 & \ldots & 0 \\
\gamma_{12} & \gamma_{22} & \ldots & \gamma_{r2} & 0 & 1 & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\gamma_{1n} & {}_r\gamma_{2n-r} & \ldots & \gamma_{r,n-r} & 0 & 0 & \ldots & 1
\end{bmatrix}.
$$

Система строк $C_1, \ldots, C_{n-r}$ этой матрицы линейно независима. В самом деле, для любых скаляров $\lambda_1, \ldots, \lambda_{n-r}$ из равенства

$$\lambda_1 C_1 + \ldots + \lambda_{n-r} C_{n-r} = (0, 0, \ldots, 0)$$

следует равенство

$$(\ldots, \lambda_1, \lambda_2, \ldots, \lambda_{n-r}) = (0, 0, \ldots, 0)$$

и, значит, равенства

$$\lambda_1 = 0, \lambda_2 = 0, \ldots, \lambda_{n-r} = 0.$$

Докажем, что линейная оболочка системы строк матрицы C совпадает с множеством всех решений системы (1).

Пусть

$$\boldsymbol{a} = (\alpha_1, \ldots, \alpha_r, \alpha_{r+1}, \ldots, \alpha_n)$$

— произвольное решение системы (1). Тогда вектор

$$\boldsymbol{d} = \boldsymbol{a} - (\alpha_{r+1}C_1 + \alpha_{r+2}C_2 + \ldots + \alpha_n C_{n-r})$$

также является решением системы (1), причем

$$\boldsymbol{d} = (\delta_1, \ldots, \delta_r, 0, 0, \ldots, 0);$$

это решение соответствует нулевым значениям свободных переменных $x_{r+1}, \ldots, x_n$. Поэтому $\boldsymbol{d}$ является нулевым решением системы (2) и системы (1); следовательно,

$$\boldsymbol{a} = \alpha_{r+1}C_1 + \ldots + \alpha_n C_{n-r} \in L(C_1, \ldots, C_{n-r}).$$

Итак, доказано, что множество всех решений системы (1) совпадает с линейной оболочкой системы векторов $C_1, \ldots, C_{n-r}$. Следовательно, эта система $n - r$ векторов является фундаментальной системой решений для системы уравнений (1). □

СЛЕДСТВИЕ 3.13. *Пусть* $\boldsymbol{d}$ *— решение неоднородной системы линейных уравнений (над полем* $\mathscr{F}$*)*

$$\text{(I)}\quad \alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = \beta_i \quad (i = 1, \ldots, m)$$

и $C_1, \ldots, C_{n-r}$ *— фундаментальная система решений однородной системы уравнений*

$$\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \quad (i = 1, \ldots, m).$$

Тогда множество

$$\{\boldsymbol{d} + \lambda_1 C_1 + \ldots + \lambda_{n-r}C_{n-r} \mid \lambda_1, \lambda_2, \ldots, \lambda_{n-r} \in F\}$$

является множеством всех решений системы (I).

Решение системы линейных уравнений методом последовательного исключения переменных. Пусть дана система линейных уравнений (над полем $\mathscr{F}$)

$$\text{(1)}\quad \begin{aligned} &\alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = \beta_1, \\ &\ldots\ldots\ldots\ldots\ldots \\ &\alpha_{m1}x_1 + \ldots + \alpha_{mn}x_n = \beta_m. \end{aligned}$$

Пусть

$$A = \begin{bmatrix} \alpha_{11} \ldots \alpha_{1n} \\ \ldots\ldots \\ \alpha_{m1} \ldots \alpha_{mn} \end{bmatrix}, \quad B = \begin{bmatrix} \alpha_{11} \ldots \alpha_{1n}\beta_1 \\ \ldots\ldots\ldots \\ \alpha_{m1} \ldots \alpha_{mn}\beta_m \end{bmatrix}.$$

Матрица A называется *основной матрицей системы* (1), матрица B — *расширенной матрицей системы* (1).

Система линейных уравнений называется *ступенчатой*, если расширенная матрица системы есть ступенчатая матрица без нулевых строк. Система линейных уравнений называется *приведенной ступенчатой*, если расширенная матрица системы есть приведенная ступенчатая матрица.

Если B — нулевая матрица, то любой n-мерный вектор из F^n является решением системы (1). Если же A — нулевая матрица, а B — ненулевая, то система уравнений (1) несовместна.

Предположим, что матрица A — ненулевая. Тогда систему уравнений (1) можно при помощи элементарных преобразований привести к ступенчатой системе, а затем к приведенной ступенчатой системе, причем эти системы будут равносильны исходной системе (1). Предположим, что столбцы $A^1, \ldots, A^r$ образуют базис системы столбцов матрицы A. При помощи цепочки элементарных преобразований приведем систему уравнений (1) к ступенчатому виду без нулевых строк. Если последнее уравнение полученной ступенчатой системы имеет вид

$$0 \cdot x_1 + \ldots + 0 \cdot x_n = \beta, \text{ где } \beta \neq 0,$$

то полученная ступенчатая система уравнений несовместна и, следовательно, несовместна равносильная ей исходная система уравнений (1). Если же в левой части последнего уравнения полученной ступенчатой системы есть коэффициенты, отличные от нуля, то полученная ступенчатая система имеет вид

$$\begin{aligned} &\alpha'_{11}x_1 + \alpha'_{12}x_2 + \ldots + \alpha'_{1r}x_r + \ldots + \alpha'_{1n}x_n = \beta'_1, \\ &\alpha'_{22}x_2 + \ldots + \alpha'_{2r}x_r + \ldots + \alpha'_{2n}x_n = \beta'_2, \\ &\qquad\qquad \ldots\ldots\ldots\ldots\ldots\ldots \\ &\alpha'_{rr}x_r + \ldots + \alpha'_{rn}x_n = \beta'_r, \end{aligned} \tag{2}$$

где коэффициенты $\alpha'_{11}, \alpha'_{22}, \ldots, \alpha'_{rr}$ отличны от нуля. Система (2) совместна и равносильна исходной системе (1).

От ступенчатой системы (2) при помощи цепочки элементарных преобразований переходим к ступенчатой системе уравнений

$$\begin{aligned} x_1 \quad &- \gamma_{1r+1}x_{r+1} - \ldots - \gamma_{1n}x_n = \delta_1, \\ x_2 \quad &- \gamma_{2r+1}x_{r+1} - \ldots - \gamma_{2n}x_n = \delta_2, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ x_r &- \gamma_{rr+1}x_{r+1} - \ldots - \gamma_{rn}x_n = \delta_r. \end{aligned} \tag{3}$$

Система (3) совместна и равносильна исходной системе уравнений (1). Если при этом $r=n$, то система уравнений (3) (и система (1)) имеет единственное решение $(\delta_1, \delta_2, \ldots, \delta_n)$. Если же $r(A)=r(B)<n$, то система (3) равносильна системе

$$
\begin{aligned}
&x_1=\gamma_{1r+1}x_{r+1}+\ldots+\gamma_{1n}x_n+\delta_1,\\
&x_2=\gamma_{2r+1}x_{r+1}+\ldots+\gamma_{2n}x_n+\delta_2,\\
&\qquad\ldots\ldots\ldots\ldots\ldots\ldots\\
&x_r=\gamma_{rr+1}x_{r+1}+\ldots+\gamma_{rn}x_n+\delta_r.
\end{aligned}
\tag{4}
$$

Уравнения системы (4) дают явное выражение переменных $x_1, \ldots, x_r$, называемых *главными*, через переменные $x_{r+1}, \ldots, x_n$, называемые *свободными*. Придавая в уравнениях (4) свободным переменным любые значения из поля скаляров, находим соответствующие значения главных переменных. Таким образом можно получить любое частное решение исходной системы уравнений (1), поскольку она равносильна системе (4). Поэтому вектор

$$
(\gamma_{1r+1}x_{r+1}+\ldots+\gamma_{1n}x_n+\delta_1, \ldots, \gamma_{rr+1}x_{r+1}+\ldots \ldots+\gamma_{1n}x_n+\delta_r, x_{r+1}, \ldots, x_n) \tag{5}
$$

называется *общим решением системы уравнений* (1). Вектор (5) можно записать в виде

$$
x_{r+1}C_{r+1}+\ldots+x_nC_n+\delta, \tag{6}
$$

где $C_{r+1}, \ldots, C_n \in F^n$ и $\delta=(\delta_1, \ldots, \delta_r, 0, \ldots, 0)$ — частное решение системы (1). Вектор (6) также называется *общим решением системы* (1). Легко видеть, что векторы $C_{r+1}, \ldots, C_n$ образуют фундаментальную систему решений однородной системы уравнений, ассоциированной с системой (1).

Множество $\{x_{r+1}C_{r+1}+\ldots+x_nC_n+\delta \mid x_{r+1}, \ldots, x_n \in F\}$ является множеством всех решений системы уравнений (1).

Для исследования совместности данной системы линейных уравнений (1) надо расширенную матрицу B системы при помощи цепочки элементарных преобразований над строками привести к ступенчатой матрице B'. Система линейных уравнений (1′) с расширенной матрицей B' равносильна исходной системе уравнений (1). Система уравнений (1′) несовместна тогда и только тогда, когда строчечный ранг ее основной матрицы A' меньше строчечного ранга расширенной матрицы B', т. е. когда в последней строке ступенчатой матрицы B' все элементы, кроме последнего, равны нулю.

Упражнения

1. Докажите, что ненулевая матрица строчечно эквивалентна одной и только одной приведенной ступенчатой матрице.

2. Докажите, что $m \times n$-матрица A строчечно эквивалентна единичной $n \times n$-матрице тогда и только тогда, когда ранг матрицы A равен n.

3. Покажите, что две линейные однородные системы над полем $\mathcal{F}$ с переменными $x_1, \ldots, x_n$ равносильны тогда и только тогда, когда строчечно эквивалентны основные матрицы этих систем.

4. Пусть $\mathcal{F}$ — конечное поле, состоящее из k элементов. Покажите, что данная однородная система линейных уравнений над полем $\mathcal{F}$ с n переменными имеет k^{n-r} решений, где r — ранг основной матрицы данной системы уравнений.

5. Докажите, что совместная система линейных уравнений с ненулевой основной матрицей равносильна одной и только одной приведенной ступенчатой системе линейных уравнений.

6. Докажите, что если равносильны две совместные системы линейных уравнений, то равносильны ассоциированные с ними однородные системы линейных уравнений.

7. Докажите, что две совместные системы линейных уравнений над полем $\mathcal{F}$ с переменными $x_1, \ldots, x_n$ равносильны тогда и только тогда, когда строчечно эквивалентны расширенные матрицы этих систем.

Глава шестая

МАТРИЦЫ И ОПРЕДЕЛИТЕЛИ

§ 1. ОПЕРАЦИИ НАД МАТРИЦАМИ И ИХ СВОЙСТВА

Операции над матрицами. Всюду в этой главе $\mathscr{F} = \langle F, +, -, \cdot, 1\rangle$ есть фиксированное поле, которое будем называть *полем скаляров*. Элементы множества F будем называть *скалярами*.

Пусть m и n — целые положительные числа. Таблицу

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

с элементами из F называют *матрицей над полем* $\mathscr{F}$ или $m \times n$-*матрицей* над $\mathscr{F}$, кратко обозначают через $\|\alpha_{ik}\|$ и пишут $A = \|\alpha_{ik}\|$. Если $m = n$, то матрицу A называют *квадратной матрицей* порядка n. Множество всех $m \times n$-матриц над полем $\mathscr{F}$ обозначается через $F^{m\times n}$. В частности, множество всех квадратных матриц над $\mathscr{F}$ порядка n обозначается через $F^{n\times n}$.

Сохраним прежние обозначения для строк и столбцов матрицы A: i-я строка матрицы A обозначается через A_i:

$$A_i = [\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{in}];$$

k-й столбец матрицы обозначается через A^k:

$$A^k = \begin{bmatrix} \alpha_{1k} \\ \alpha_{2k} \\ \vdots \\ \alpha_{nk} \end{bmatrix}.$$

Две $m \times n$-матрицы $A = \|\alpha_{ik}\|$ и $B = \|\beta_{ik}\|$ называют *равными* и пишут $A = B$, если $\alpha_{ik} = \beta_{ik}$ для любых индексов i и k.

Матрица называется *нулевой* и обозначается через O, если все ее элементы равны нулю.

Суммой двух $m\times n$*-матриц* A *и* B называется $m\times n$-матрица, ik-й элемент которой равен $\alpha_{ik}+\beta_{ik}$, т. е.

$$A+B=\|\alpha_{ik}+\beta_{ik}\|.$$

Произведением скаляра λ *на матрицу* $A=\|\alpha_{ik}\|$ называется $m\times n$-матрица $\|\lambda\alpha_{ik}\|$, обозначаемая через λA:

$$\lambda A=\|\lambda\alpha_{ik}\|.$$

Для матрицы $(-1)A$ выполняется равенство

$$A+(-1)A=0.$$

Поэтому матрицу $(-1)A$ обозначают также через $-A$ и называют *противоположной матрице* A.

Пусть $A\in F^{m\times n}$ и $B\in F^{n\times p}$:

$$A=\begin{bmatrix}\alpha_{11} & \dots & \alpha_{1n}\\ \dots & \dots & \dots\\ \alpha_{m1} & \dots & \alpha_{mn}\end{bmatrix},\qquad B=\begin{bmatrix}\beta_{11} & \dots & \beta_{1p}\\ \dots & \dots & \dots\\ \beta_{n1} & \dots & \beta_{np}\end{bmatrix}.$$

Таким образом, мы предполагаем, что число столбцов матрицы A равно числу строк матрицы B. *Произведение строки* A_i *на столбец* B_k определяется так:

$$A_iB^k=[\alpha_{i1},\ \dots,\ \alpha_{in}]\cdot\begin{bmatrix}\beta_{1k}\\ \vdots\\ \beta_{nk}\end{bmatrix}=$$

$$=\alpha_{i1}\beta_{1k}+\dots+\alpha_{in}\beta_{nk}=\sum_{j=1}^{n}\alpha_{ij}\beta_{jk}.$$

Произведением матриц A *и* B называется $m\times p$-матрица, ik-й элемент которой равен A_iB^k, т. е.

$$A\cdot B=\begin{bmatrix}A_1B^1 & A_1B^2 & \dots & A_1B^p\\ A_2B^1 & A_2B^2 & \dots & A_2B^p\\ \dots & \dots & \dots & \dots\\ A_mB^1 & A_mB^2 & \dots & A_mB^p\end{bmatrix}.$$

Итак, если A есть $m\times n$-матрица и B есть $n\times p$-матрица, то AB является $m\times p$-матрицей.

ТЕОРЕМА 1.1. *Умножение матриц ассоциативно, т. е. для любых матриц* A, B *и* C $A(BC)=(AB)C$, *если произведения* AB *и* BC *существуют.*

Доказательство. По условию, произведения AB и BC существуют. Поэтому можно считать, что $A \in F^{m\times n}$, $B \in F^{n\times p}$, $C \in F^{p\times q}$. Следовательно, произведения $A(BC)$ и $(AB)C$ существуют и принадлежат множеству $F^{m\times q}$. Пусть $H = A(BC)$, $H' = (AB)C$ и h_{ik}, h'_{ik} — ik-е элементы матриц H и H' соответственно. Докажем, что $h_{ik} = h'_{ik}$ для любых индексов i и k. В самом деле,

$$h_{ik} = A_i (BC)^k = [\alpha_{i1}, \ldots, \alpha_{in}] \begin{bmatrix} B_1 C^k \\ \vdots \\ B_n C^k \end{bmatrix} =$$

$$= \alpha_{i1} B_1 C^k + \ldots + \alpha_{in} B_n C^k =$$

$$= \alpha_{i1} \sum_{s=1}^{p} \beta_{1s}\gamma_{sk} + \ldots + \alpha_{in} \sum_{s=1}^{p} \beta_{ns}\gamma_{sk} =$$

$$= \sum_{\substack{j=1,\ldots,n \\ s=1,\ldots,p}} \alpha_{ij}\beta_{js}\gamma_{sk};$$

$$h'_{ik} = (AB)_i C^k = [A_i B^1, \ldots, A_i B^p] \begin{bmatrix} \gamma_{1k} \\ \vdots \\ \gamma_{pk} \end{bmatrix} =$$

$$= A_i B^1 \gamma_{1k} + \ldots + A_i B^p \gamma_{pk} =$$

$$= \left(\sum_{j=1}^{n} \alpha_{ij}\beta_{j1} \right) \gamma_{1k} + \ldots + \left(\sum_{j=1}^{n} \alpha_{ij}\beta_{jp} \right) \gamma_{pk} =$$

$$= \sum_{\substack{j=1,\ldots,n \\ s=1,\ldots,p}} \alpha_{ij}\beta_{js}\gamma_{sk}.$$

Следовательно, $h_{ik} = h'_{ik}$ для любых индексов i и k, т. е. $A(BC) = (AB)C$. □

ТЕОРЕМА 1.2. *Операции над матрицами обладают следующими свойствами*:

(1) *алгебра* $\langle F^{m\times n}, +, - \rangle$ *есть абелева группа*;

(2) $\alpha(A+B) = \alpha A + \alpha B$ $\quad (\alpha, \beta \in F,\ A, B \in F^{m\times n})$;

(3) $(\alpha+\beta)A = \alpha A + \beta A$;

(4) $(\alpha\beta)A = \alpha(\beta A)$;

(5) $1 \cdot A = A$;

(6) *умножение матриц ассоциативно*;

(7) *умножение матриц дистрибутивно относительно сложения, т. е.* $A(B+C) = AB + AC$, *если произведение*

AB и сумма $B+C$ существуют, и $(B+C)A=BA+CA$, если произведение BA и сумма $B+C$ существуют;

(8) *для любого скаляра λ и любых матриц A, B*

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

если произведение AB существует.

Доказательство. Свойства (1)—(5) доказываются аналогично доказательству соответствующих свойств сложения векторов и умножения на скаляр векторов арифметических векторных пространств.

По теореме 1.1, умножение матриц ассоциативно.

Докажем, что умножение матриц дистрибутивно относительно сложения. Пусть $A\in F^{m\times n}$, B, $C\in F^{n\times p}$. Легко проверить, что AB, $AC\in F^{m\times p}$, $B+C\in F^{n\times p}$. Отсюда следует, что $A(B+C)$ и $AB+AC$ суть $m\times p$-матрицы. Покажем, что ik-е элементы этих матриц равны, т. е. $A_i(B+C)^k=A_iB^k+A_iC^k$. В самом деле,

$$A_i(B+C)^k=\sum_{j=1,\ldots,n}\alpha_{ij}(\beta_{jk}+\gamma_{jk});$$

$$A_iB^k+A_iC^k=\sum_{j=1,\ldots,n}\alpha_{ij}\beta_{jk}+\sum_{j=1,\ldots,n}\alpha_{ij}\gamma_{jk}=$$

$$=\sum_{j=1,\ldots,n}\alpha_{ij}(\beta_{jk}+\gamma_{jk}).$$

Следовательно, $A(B+C)=AB+BC$. Аналогично доказывается, что $(B+C)A=BA+CA$, если произведение BA и сумма $B+C$ существуют.

Для доказательства свойства (8) найдем ik-е элементы матриц $\lambda(AB)$, $(\lambda A)B$, $A(\lambda B)$:

$$\lambda(A_iB^k)=\lambda\sum_{j=1}^{n}\alpha_{ij}\beta_{jk};\quad(\lambda A_i)B^k=\sum_{j=1}^{n}(\lambda\alpha_{ij})\beta_{jk};$$

$$A_i(\lambda B^k)=\sum_{j=1}^{n}\alpha_{ij}(\lambda\beta_{jk}).$$

Эти три выражения равны между собой в силу свойств сложения и умножения скаляров. Следовательно, $\lambda(AB)=(\lambda A)B=A(\lambda B)$. □

Транспонирование произведения матриц. Пусть $A=\|\alpha_{ik}\|$ есть $m\times n$-матрица над полем $\mathcal{F}$. Тогда $n\times m$-матрица $\|\beta_{ik}\|$ такая, что $\beta_{ik}=\alpha_{ik}$, называется *матрицей, транспонированной* к A, и обозначается через ${}^tA$. Таким образом, транспонированная матрица получается в резуль-

тате замены строк данной матрицы соответствующими столбцами. В частности,

$$({}^tA)^i = {}^t[\alpha_{i1}, \ldots, \alpha_{in}] = \begin{bmatrix} \alpha_{i1} \\ \vdots \\ \alpha_{in} \end{bmatrix};$$

$$({}^tA)_k = {}^t\begin{bmatrix} \alpha_{1k} \\ \vdots \\ \alpha_{mk} \end{bmatrix} = [\alpha_{1k}, \ldots, \alpha_{mk}].$$

ТЕОРЕМА 1.3. *Если существует произведение AB матриц A и B, то существует произведение ${}^tB \cdot {}^tA$ и ${}^t(AB) = {}^tB \cdot {}^tA$.*

Доказательство. Предположим, что $A \in F^{m\times n}$ и $B \in F^{n\times p}$. Тогда если $C = AB$, то $AB \in F^{m\times p}$ и ${}^t(AB) \in F^{p\times m}$. Кроме того, ${}^tB \in F^{p\times n}$ и ${}^tA \in F^{p\times n}$. Следовательно, существует произведение ${}^tB \cdot {}^tA$ и ${}^tB{}^tA \in F^{p\times m}$. Таким образом, матрицы $C = {}^t(AB)$ и $C' = {}^tB \cdot {}^tA$ являются $p \times m$-матрицами. Проверим, что ik-е элементы c_{ik} и c'_{ik} этих матриц равны. В самом деле,

$$c_{ik} = A_k B^i = [\alpha_{k1}, \ldots, \alpha_{kn}] \begin{bmatrix} \beta_{1i} \\ \vdots \\ \beta_{ni} \end{bmatrix} = \alpha_{k1}\beta_{1i} + \ldots + \alpha_{kn}\beta_{ni};$$

с другой стороны,

$$c'_{ik} = ({}^tB)_i ({}^tA)^k = [\beta_{1i}, \ldots, \beta_{ni}] \begin{bmatrix} \alpha_{k1} \\ \vdots \\ \alpha_{kn} \end{bmatrix} =$$

$$= \alpha_{k1}\beta_{1i} + \ldots + \alpha_{kn}\beta_{ni}.$$

Следовательно, $c_{ik} = c'_{ik}$ для любых индексов i и k, т. е. ${}^t(AB) = {}^tB \cdot {}^tA$. □

Упражнения

1. Пусть $A = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$. Найдите A^n для любого положительного целого n.

2. Докажите, что если для матриц A и B произведения AB и BA существуют и $AB = BA$, то матрицы A и B — квадратные и имеют одинаковый порядок.

3. Пусть A, B — квадратные матрицы одинакового порядка и $AB = BA$. Докажите, что для любого целого положительного числа n справедлива формула

$$(A+B)^n = A^n + n \cdot A^{n-1} \cdot B + \frac{n(n-1)}{2} A^{n-2} \cdot B^2 + \ldots + B^n.$$

4. Покажите, что операция транспонирования обладает следующими свойствами:
(a) ${}^t(A+B)={}^tA+{}^tB$; (b) ${}^t(\lambda A)=\lambda\cdot{}^tA$, где λ — скаляр; (c) ${}^t(A^{-1})=({}^tA)^{-1}$; (d) ${}^t(ABC)={}^tC\cdot{}^tB\cdot{}^tA$, если произведение ABC существует.

5. Квадратная матрица A называется *симметрической*, если $A={}^tA$. Покажите, что если A — квадратная матрица, то матрица $A+{}^tA$ является симметрической.

6. Квадратная матрица A называется *кососимметрической*, если $A=-{}^tA$. Докажите, что любую квадратную матрицу можно представить, и притом единственным образом, в виде суммы симметрической и кососимметрической матриц.

7. Докажите, что элементарные преобразования над столбцами матрицы осуществляются посредством умножения матрицы справа на соответствующие элементарные матрицы.

§ 2. ОБРАТИМЫЕ МАТРИЦЫ

Обратимые матрицы. Пусть A есть $n\times n$-матрица над полем скаляров $\mathscr{F}$. Если E — единичная $n\times n$-матрица, то

(1) $AE=A=EA.$

Квадратная матрица называется *обратимой*, если существует матрица B, удовлетворяющая условиям

(2) $AB=E,\quad BA=E.$

Матрица B, удовлетворяющая этим условиям, называется *обратной к* A. Матрицы A и B называются *взаимно обратными*.

ПРЕДЛОЖЕНИЕ 2.1. *Если матрица A обратима, то существует только одна матрица, обратная к A.*

Доказательство. Предположим, что B и C — матрицы, обратные к A. Тогда $AC=E=BA$ и $B=BE=$ $=B(AC)=(BA)C=E\cdot C=C$, т. е. $B=C$. □

Если матрица A обратима, то обратная к A матрица обозначается через A^{-1}. Таким образом, для любой обратимой матрицы выполняются равенства

(3) $AA^{-1}=E,\quad A^{-1}A=E.$

Множество всех обратимых $n\times n$-матриц над полем $\mathscr{F}$ обозначается через $GL(n,\mathscr{F})$.

ТЕОРЕМА 2.2. *Алгебра $\langle GL(n,\mathscr{F}),\ \cdot,\ ^{-1}\rangle$ есть группа.*

Доказательство. Единичная матрица E, очевидно, обратима и ввиду (1) является нейтральным элементом.

Если матрица A обратима, то в силу (2) матрица A^{-1} также обратима.

Множество $GL(n, \mathscr{F})$ обратимых $n \times n$-матриц замкнуто также относительно умножения. Действительно, если $A, B \in GL(n, \mathscr{F})$, то

$$(AB)(B^{-1}A^{-1}) = E = (B^{-1}A^{-1})(AB),$$

т. е. матрица AB обратима над $\mathscr{F}$ и поэтому принадлежит множеству $GL(n, \mathscr{F})$.

Наконец, по теореме 1.1, умножение матриц ассоциативно. □

СЛЕДСТВИЕ 2.3. *Произведение любого числа обратимых матриц есть обратимая матрица.*

Элементарные матрицы. Введем понятие элементарной матрицы.

ОПРЕДЕЛЕНИЕ. Квадратная матрица, получающаяся из единичной матрицы в результате неособенного элементарного преобразования над строками (столбцами), называется *элементарной матрицей*, соответствующей этому преобразованию.

Так, например, элементарными матрицами второго порядка являются матрицы

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \lambda & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & \lambda \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix},$$

где λ — любой ненулевой скаляр.

Элементарная матрица получается из единичной матрицы E в результате одного из следующих неособенных преобразований:

1) умножение строки (столбца) матрицы E на отличный от нуля скаляр;

2) прибавление (или вычитание) к какой-либо строке (столбцу) матрицы E другой строки (столбца), умноженной на скаляр.

Обозначим через $E_{\lambda(i)}$ матрицу, получающуюся из матрицы E в результате умножения i-й строки на ненулевой скаляр λ:

$$E_{\lambda(i)} = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & \lambda & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{bmatrix}.$$

Обозначим через $E_{(i)+\lambda(k)}$ ($E_{(i)-\lambda(k)}$) матрицу, получающуюся из матрицы E в результате прибавления (вычитания) к i-й строке k-й строки, умноженной на λ;

$$E_{(i)+\lambda(k)} = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & \lambda & & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{bmatrix}; \quad E_{(i)-\lambda(k)} = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & -\lambda & & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{bmatrix}.$$

Через E_φ будем обозначать матрицу, получающуюся из единичной матрицы E в результате применения элементарного преобразования φ над строками; таким образом, E_φ есть матрица, соответствующая преобразованию φ.

Рассмотрим некоторые свойства элементарных матриц.

СВОЙСТВО 2.1. *Любая элементарная матрица обратима. Матрица, обратная к элементарной, является элементарной.*

Доказательство. Непосредственная проверка показывает, что для любого отличного от нуля скаляра λ и произвольных i и k выполняются равенства

$$E_{\lambda(i)}E_{\lambda^{-1}(i)} = E = E_{\lambda^{-1}(i)}E_{\lambda(i)};$$

$$E_{(i)+\lambda(k)}E_{(i)-\lambda(k)} = E = E_{(i)-\lambda(k)}E_{(i)+\lambda(k)}.$$

На основании этих равенств заключаем, что имеет место свойство 2.1. □

СВОЙСТВО 2.2. *Произведение элементарных матриц является обратимой матрицей.*

Это свойство непосредственно следует из свойства 2.1 и следствия 2.3.

СВОЙСТВО 2.3. *Если необособенное строчечное элементарное преобразование φ переводит $m \times n$-матрицу A в матрицу B, то $B = E_\varphi A$ ($E_\varphi \in F^{m\times m}$). Верно и обратное утверждение.*

Доказательство. Если φ есть умножение i-й строки $A = \|\alpha_{ik}\|$ на ненулевой скаляр λ, то

$$E_{\lambda(i)}A = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \dots & \dots & \dots \\ \lambda\alpha_{i1} & \dots & \lambda\alpha_{in} \\ \dots & \dots & \dots \\ \alpha_{m1} & \dots & \alpha_{mn} \end{bmatrix},$$

т. е. $B = E_{\varphi}A$. Если же $E_{\varphi} = E_{(i)+\lambda(k)}$, то

$$E_{(i)+\lambda(k)}A = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \dots & \dots & \dots \\ \alpha_{i1}+\lambda\alpha_{k1} & \dots & \alpha_{in}+\lambda\alpha_{kn} \\ \dots & \dots & \dots \\ \alpha_{m1} & \dots & \alpha_{mn} \end{bmatrix},$$

т. е. $B = E_{(i)+\lambda(k)} \cdot A$.

Легко проверить, что верно также обратное утверждение. □

СВОЙСТВО 2.4. *Если матрица C получается из матрицы A при помощи цепочки неособенных строчечных элементарных преобразований $\varphi_1, \dots, \varphi_s$, то $C = E_{\varphi_s} \dots E_{\varphi_1} \cdot A$. Верно и обратное утверждение.*

Доказательство. По свойству 2.3, преобразование φ_1 переводит матрицу A в матрицу $E_{\varphi_1} \cdot A$, φ_2 переводит матрицу $E_{\varphi_1} \cdot A$ в матрицу $E_{\varphi_2}E_{\varphi_1} \cdot A$ и т. д. Наконец, φ_s переводит матрицу $E_{\varphi_{s-1}} \dots E_{\varphi_1} \cdot A$ в матрицу $E_{\varphi_s}E_{\varphi_{s-1}} \dots$ $\dots E_{\varphi_1} \cdot A$. Следовательно, $C = E_{\varphi_s} \dots E_{\varphi_2}E_{\varphi_1} \cdot A$.

Легко проверить, что верно и обратное утверждение.

Условия обратимости матрицы. Для доказательства теоремы 2.8 необходимы следующие три леммы.

ЛЕММА 2.4. *Квадратная матрица с нулевой строкой (столбцом) необратима.*

Доказательство. Пусть A — квадратная матрица с нулевой строкой, B — любая матрица, A, $B \in F^{n \times n}$. Пусть A_i — нулевая строка матрицы A; тогда

$$(AB)_i = [A_iB^1, \dots, A_iB^n] = [0, \dots, 0],$$

т. е. i-я строка матрицы AB является нулевой. Следовательно, матрица A необратима. □

ЛЕММА 2.5. *Если строки квадратной матрицы линейно зависимы, то матрица необратима.*

Доказательство. Пусть A — квадратная матрица с линейно зависимыми строками. Тогда существует цепочка неособенных строчечных элементарных преобразований, переводящих A в ступенчатую матрицу; пусть $\varphi_1, \dots, \varphi_s$ — такая цепочка. По свойству 2.4 элементарных матриц, имеет место равенство

$$(1)\quad E_{\varphi_s} \dots E_{\varphi_1} \cdot A = C,$$

где C — матрица с нулевой строкой. Следовательно, по

лемме 2.4 матрица C необратима. С другой стороны, если бы матрица A была обратимой, то произведение слева в равенстве (1) было бы обратимой матрицей, как произведение обратимых матриц (см. следствие 2.3), что невозможно. Следовательно, матрица A необратима. □

СЛЕДСТВИЕ 2.6. *Если квадратная матрица обратима, то ее строки линейно независимы.*

ЛЕММА 2.7. *Квадратную матрицу с линейно независимыми строками можно представить в виде произведения элементарных матриц.*

Доказательство. Пусть A — квадратная матрица с линейно независимыми строками. Существует цепочка строчечных неособенных элементарных преобразований $\varphi_1, \ldots, \varphi_s$, переводящая матрицу A в единичную матрицу E. По свойству 2.4 элементарных матриц отсюда следует, что $E_{\varphi_s} \ldots E_{\varphi_1} \cdot A = E$. Следовательно, $A = E_{\varphi_s}^{-1} \ldots E_{\varphi_1}^{-1}$, причем, по свойству 2.1 элементарных матриц, множители $E_{\varphi_1}^{-1}, \ldots, E_{\varphi_s}^{-1}$ являются элементарными матрицами. □

ТЕОРЕМА 2.8. *Для любой квадратной матрицы A ($A \in F^{n \times n}$) равносильны следующие три утверждения:*

(a) *матрица A обратима;*

(b) *строки (столбцы) матрицы A линейно независимы;*

(c) *матрицу A можно представить в виде произведения элементарных матриц.*

Доказательство. По следствию леммы 2.5, из (a) следует (b). Далее, по лемме 2.7, из (b) следует (c). Наконец, в силу свойства 2.2 элементарных матриц и следствия 2.3 из (c) следует (a). Следовательно, утверждения (a), (b) и (c) равносильны. □

Вычисление обратной матрицы. Теперь можно обосновать наиболее простое правило вычисления обратной матрицы.

ТЕОРЕМА 2.9. *Если какая-либо цепочка неособенных строчечных элементарных преобразований переводит квадратную матрицу A в единичную матрицу E, то матрица A обратима и эта же цепочка преобразований переводит матрицу E в матрицу A^{-1}.*

Доказательство. Предположим, что $\varphi_1, \ldots, \varphi_s$ есть цепочка неособенных строчечных элементарных преобразований, переводящая квадратную матрицу A в единичную матрицу E. Тогда, по свойству 2.4 элементарных матриц,

$$E = E_{\varphi_s} \ldots E_{\varphi_1} A.$$

В силу предложения 2.1 отсюда следует, что матрица A обратима и

$$A^{-1} = E_{\varphi_s} \dots E_{\varphi_1} E.$$

По свойству 2.4 элементарных матриц, из последнего равенства следует, что цепочка строчечных элементарных преобразований $\varphi_1, \dots, \varphi_s$ переводит матрицу E в матрицу A^{-1}. □

Теорема 2.9 дает возможность сформулировать следующее правило нахождения обратной матрицы. *Для нахождения матрицы, обратной к $n \times n$-матрице A, надо прямоугольную $n \times 2n$-матрицу $(A \mid E)$ при помощи цепочки неособенных строчечных элементарных преобразований привести к виду $(E \mid C)$; получающаяся при этом матрица C является обратной к матрице A.*

Запись и решение системы n линейных уравнений с n переменными в матричной форме. Рассмотрим систему линейных уравнений

$$\text{(I)} \quad \begin{aligned} &\alpha_{11}x_1 + \dots + \alpha_{1n}x_n = \beta_1, \\ &\dots\dots\dots\dots\dots \\ &\alpha_{n1}x_1 + \dots + \alpha_{nn}x_n = \beta_n \end{aligned}$$

над полем $\mathscr{F}$. Если ввести обозначения

$$A = \begin{bmatrix} \alpha_{11} \dots \alpha_{1n} \\ \dots\dots \\ \alpha_{n1} \dots \alpha_{nn} \end{bmatrix}, \quad b = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}, \quad \mathscr{X} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix},$$

то систему (I) можно записать в виде матричного уравнения

$$\text{(2)} \quad A\mathscr{X} = b.$$

Легко видеть, что уравнение (2) равносильно системе уравнений (I). Уравнение (2) называется *матричной формой записи системы уравнений* (I).

ТЕОРЕМА 2.10. *Если строки матрицы A линейно независимы, то вектор $A^{-1}b$ является единственным решением уравнения* (2).

Доказательство. Предположим, что какой-либо вектор-столбец $\mathscr{X}_0$ есть решение уравнения (2), т. е. $A\mathscr{X}_0 = b$. Умножив слева обе части равенства $A\mathscr{X}_0 = b$ на A^{-1}, получим

$$\text{(3)} \quad \mathscr{X}_0 = A^{-1} \cdot b.$$

Таким образом, либо уравнение (2) имеет решение $A^{-1}b$, либо оно не имеет решений. Однако равенство $A(A^{-1} \cdot b) = b$

показывает, что вектор $A^{-1} \cdot b$ является решением уравнения (2). Следовательно, вектор $A^{-1} \cdot b$ является единственным решением уравнения (2). □

СЛЕДСТВИЕ 2.11. *Если строки основной матрицы A системы* (I) *линейно независимы, то система совместна и вектор $A^{-1} \cdot b$ является ее единственным решением.*

Упражнения

1. Пусть $A = \|\alpha_{ij}\|$ — квадратная матрица порядка n (над полем $\mathcal{F}$). Обозначим через E_{ik} ($i, k = 1, \ldots, n$) матрицу, у которой в i-й строке и k-м столбце стоит 1, а все остальные элементы равны нулю. Покажите, что

(*) $AE_{ik} = \alpha_{1i}E_{ik} + \ldots + \alpha_{ni}E_{nk}$, $E_{ik}A = \alpha_{k1}E_{i1} + \ldots + \alpha_{kn}E_{in}$.

2. На основании равенства (*) докажите, что матрица A тогда и только тогда перестановочна с каждой из матриц E_{ik}, когда A имеет вид λE, где $\lambda \in F$.

3. Пользуясь результатом предыдущей задачи, покажите, что матрица A тогда и только тогда перестановочна с произвольной квадратной матрицей порядка n (над полем $\mathcal{F}$), когда $A = \lambda E$, где $\lambda \in F$.

4. Пусть A — квадратная матрица порядка n. Докажите, что матрица A перестановочна с произвольной диагональной матрицей порядка n тогда и только тогда, когда матрица A сама диагональна.

5. Пусть A — диагональная матрица и все элементы ее главной диагонали различны между собой. Покажите, что любая матрица, перестановочная с A, также диагональна.

6. Покажите, что квадратная матрица A порядка n, перестановочная со всякой симметрической матрицей того же порядка, является *скалярной*, т. е. $A = \lambda E$, где λ — скаляр и E — единичная матрица порядка n.

7. Пусть A — квадратная матрица порядка n (над полем $\mathcal{F}$). Докажите, что множество всех матриц (над $\mathcal{F}$), перестановочных с матрицей A, замкнуто относительно сложения и умножения.

§ 3. ПОДСТАНОВКИ

Подстановки. Группа подстановок. Рассмотрим подстановки множества $M = \{1, \ldots, n\}$, где n — натуральное число, отличное от нуля. *Подстановкой множества M* называется инъективное отображение множества M на себя.

Всякое отображение φ множества M на себя удобно записать в виде таблицы

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

Порядок чисел в первой строке этой таблицы несущественен, его можно как угодно изменить. Однако надо следить за тем, чтобы для всякого k число $\varphi(k)$ было записано непосредственно под k.

Множество всех подстановок множества M обозначим через S_n; элементы этого множества называются *подстановками степени n*.

Если $\varphi \in S_n$, то: (1) φ есть инъективное отображение, т. е. для любых i, $k \in M$ из $\varphi(i) = \varphi(k)$ следует $i = k$; (2) φ есть отображение M на M, т. е. $\{\varphi(1), \ldots, \varphi(n)\} = \{1, \ldots, n\}$. Так как M — конечное множество, то из условия (1) следует условие (2), и наоборот.

Произведение $\varphi\psi$ двух подстановок φ и ψ множества M определяется как композиция отображений φ и ψ ($\varphi\psi = \varphi \cdot \psi$). Таким образом, по определению

$$\varphi\psi(i) = \varphi(\psi_{(i)}) \quad \text{для } i = 1, \ldots, n.$$

Композиция любых двух инъективных отображений множества M на себя есть инъективное отображение множества M на себя. Следовательно, для любых двух подстановок φ, ψ из S_n имеем $\varphi\psi \in S_n$.

Обозначим через ε тождественное отображение множества M на себя:

$$\varepsilon(i) = i \text{ для } i = 1, \ldots, n, \text{ т. е. } \varepsilon = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Легко видеть, что для любой подстановки φ из S_n $\varphi\varepsilon = \varepsilon\varphi = \varphi$, т. е. ε является нейтральным элементом относительно умножения.

Если φ — подстановка множества M, то φ^{-1} — также подстановка множества M и $\varphi\varphi^{-1} = \varepsilon = \varphi^{-1}\varphi$. При этом

$$\varphi^{-1} = \begin{pmatrix} \varphi(1) & \ldots & \varphi(n) \\ 1 & \ldots & n \end{pmatrix} = \begin{pmatrix} 1 & \ldots & n \\ \varphi^{-1}(1) & \ldots & \varphi^{-1}(n) \end{pmatrix}.$$

ТЕОРЕМА 3.1. *Алгебра* $\langle S_n, \cdot, {}^{-1} \rangle$ *является группой.*

Доказательство. Выше мы установили, что множество S_n замкнуто относительно главных операций $\cdot$, $^{-1}$. По теореме 2.3, композиция функций ассоциативна. Следовательно, операция умножения подстановок ассоциативна. Тождественная подстановка ε есть нейтральный элемент относительно умножения, и для любой подстановки φ из S_n выполняется равенство $\varphi\varphi^{-1} = \varepsilon = \varphi^{-1}\varphi$. Таким образом, алгебра $\langle S_n, \cdot, {}^{-1} \rangle$ является группой. □

ОПРЕДЕЛЕНИЕ. Группа $\langle S_n, \cdot, {}^{-1} \rangle$ называется *симметрической группой степени n* и обозначается через $\mathfrak{S}_n$. Элемент ε называется *единичным элементом* этой *группы*.

Четные и нечетные подстановки. Пусть дана подстановка множества $M=\{1, \ldots, n\}$

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

Рассмотрим какую-нибудь неупорядоченную пару $\{i, k\}$ различных элементов множества M. Пара $\{i, k\}$ называется *правильной* по отношению к подстановке φ, если разности $i-k$ и $\varphi(i)-\varphi(k)$ имеют один и тот же знак. Говорят, что пара $\{i, k\}$ *неправильна* по отношению к подстановке φ или образует в ней *инверсию*, если разности $i-k$ и $\varphi(i)-\varphi(k)$ имеют разные знаки. Так, например, в тождественной подстановке $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ нет инверсий. В подстановке $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ есть только одна инверсия. В подстановке $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ имеется две инверсии.

Подстановка называется *четной*, если она содержит четное число инверсий; подстановка называется *нечетной*, если она содержит нечетное число инверсий. Так, например, тождественная подстановка есть четная.

Подстановка φ вида

$$\begin{pmatrix} 1 & \ldots & i & \ldots & k & \ldots & n \\ 1 & \ldots & k & \ldots & i & \ldots & n \end{pmatrix}$$

называется *транспозицией*. Другими словами, подстановка φ называется *транспозицией*, если существует пара $\{i, k\}$ различных элементов из M, удовлетворяющих условиям

(1) $\varphi(i)=k$, $\varphi(k)=i$, $\varphi(s)=s$ для каждого $s \in M \setminus \{i, k\}$.

ЛЕММА 3.2. *Любая транспозиция есть нечетная подстановка.*

Доказательство. Пусть φ — транспозиция, переводящая i в k $(i \neq k)$, т. е. удовлетворяющая условиям (1). Будем предполагать, что $i<k$. Легко видеть, что пара $\{s, t\} \subset M$ может образовать инверсию, если хотя бы один из ее элементов есть i или k; в противном случае обе разности $s-t$ и $\varphi(s)-\varphi(t)$ совпадают.

Если $i<s$ или $k<s$, то среди пар $\{s, i\}$ и $\{k, s\}$ нет инверсий, так как обе разности отрицательны.

Если $i<s \leqslant k$, то среди пар $\{i, s\}$ инверсиями являются следующие: $\{i, i+1\}, \ldots, \{i, k\}$, всего $k-i$ инверсий.

Если $i < s < k$, то среди пар $\{s, k\}$ инверсиями являются пары $\{i+1, k\}, \ldots, \{k-1, k\}$; имеется всего $k-i-1$ инверсий.

Итак, транспозиция φ содержит всего $(k-i)+(k-i-1) = 2(k-i)-1$ инверсий, значит, φ есть нечетная подстановка. □

Знак подстановки. Знак любого рационального числа a определяется следующим образом:

$$\operatorname{sign}(a) = \begin{cases} 1 & \text{для } a > 0, \\ 0 & \text{для } a = 0, \\ -1 & \text{для } a < 0. \end{cases}$$

Легко видеть, что *для любых рациональных чисел* a и b

$$\operatorname{sign}(ab) = \operatorname{sign}(a) \cdot \operatorname{sign}(b).$$

Это свойство знака, называемое *свойством мультипликативности,* будет использовано при доказательстве леммы 3.3.

Обозначим через sgn отображение множества S_n в множество $\{1, -1\}$, определяемое равенством:

$$\operatorname{sgn}\varphi = \begin{cases} 1, & \text{если } \varphi - \text{четная подстановка}, \\ -1, & \text{если } \varphi - \text{нечетная подстановка}. \end{cases}$$

Нетрудно видеть, что знак $(\operatorname{sgn}\varphi)$ подстановки φ равен произведению знаков всех чисел $\frac{i-k}{\varphi(i)-\varphi(k)}$, соответствующих всевозможным парам $\{i, k\}$ различных элементов множества M, т. е.

$$\operatorname{sgn}\varphi = \prod_{\substack{\{i,\,k\} \subset M \\ i \neq k}} \operatorname{sign} \frac{i-k}{\varphi(i)-\varphi(k)}.$$

ЛЕММА 3.3. *Знак произведения двух подстановок равен произведению знаков этих подстановок,* т. е.

(1) $\operatorname{sgn}(\varphi\psi) = \operatorname{sgn}\varphi \cdot \operatorname{sgn}\psi \quad (\varphi, \psi \in S_n)$.

Доказательство. Подстановку φ можно представить в виде

$$\varphi = \begin{pmatrix} \psi(1) & \ldots & \psi(n) \\ \varphi\psi(1) & \ldots & \varphi\psi(n) \end{pmatrix}; \text{ поэтому}$$

$$\operatorname{sgn}\varphi = \prod_{\substack{\{i,\,k\} \subset M \\ i \neq k}} \operatorname{sign} \frac{\psi(i)-\psi(k)}{\varphi\psi(i)-\varphi\psi(k)};$$

следовательно, имеем

$$(2)\quad \operatorname{sgn}\varphi\cdot\operatorname{sgn}\psi=\prod_{\substack{\{i,\,k\}\subset M\\ i\neq k}}\operatorname{sign}\frac{\psi(i)-\psi(k)}{\varphi\psi(i)-\varphi\psi(k)}\times$$

$$\times\prod_{\substack{\{i,\,k\}\subset M\\ i\neq k}}\operatorname{sign}\frac{i-k}{\psi(i)-\psi(k)}.$$

В силу свойства мультипликативности знака sign

$$\operatorname{sign}\frac{\psi(i)-\psi(k)}{\varphi\psi(i)-\varphi\psi(k)}\cdot\operatorname{sign}\frac{i-k}{\psi(i)-\psi(k)}=$$

$$=\operatorname{sign}\left(\frac{\psi(i)-\psi(k)}{\varphi\psi(i)-\varphi\psi(k)}\cdot\frac{i-k}{\psi(i)-\psi(k)}\right)=\operatorname{sign}\frac{i-k}{\varphi\psi(i)-\varphi\psi(k)}.$$

Поэтому из (2) следует, что

$$\operatorname{sgn}\varphi\cdot\operatorname{sgn}\psi=\prod_{\substack{\{i,\,k\}\subset M\\ i\neq k}}\operatorname{sign}\frac{i-k}{\varphi\psi(i)-\varphi\psi(k)}=\operatorname{sgn}(\varphi\psi).\ \square$$

ТЕОРЕМА 3.4. *Знак подстановки (функция* sgn*) обладает следующими свойствами:*

(1) *функция* sgn *мультипликативна, т. е.* $\operatorname{sgn}(\varphi\psi)=\operatorname{sgn}\varphi\cdot\operatorname{sgn}\psi$ *для любых* φ, ψ *из* S_n;

(2) *знак транспозиции равен* (-1);

(3) *взаимно обратные подстановки имеют один и тот же знак;*

(4) *если* τ *— транспозиция и* φ *— любая подстановка из* S_n, *то* $\operatorname{sgn}(\tau\varphi)=\operatorname{sgn}(\varphi\tau)=-\operatorname{sgn}\varphi$.

Доказательство. Свойство (1) выполняется в силу леммы 3.3. Свойство (2) непосредственно следует из леммы 3.2. В силу свойства (1)

$$\operatorname{sgn}(\varphi\varphi^{-1})=\operatorname{sgn}\varphi\cdot\operatorname{sgn}\varphi^{-1}=\operatorname{sgn}\varepsilon=1$$

для любой подстановки φ. Следовательно, $\operatorname{sgn}\varphi=\operatorname{sgn}\varphi^{-1}$. Свойство (4) непосредственно следует из свойств (1) и (2). $\square$

СЛЕДСТВИЕ 3.5. *Произведение двух (или четного числа) подстановок одинаковой четности есть четная подстановка.*

СЛЕДСТВИЕ 3.6. *Произведение двух подстановок различной четности есть нечетная подстановка.*

Упражнения

1. Докажите, что существует $n!$ подстановок множества, состоящего из n элементов.

2. Покажите, что при $n>1$ число четных подстановок множества $\{1, 2, \ldots, n\}$ равно числу нечетных подстановок.

3. Докажите, что множество всех четных подстановок из S_n замкнуто относительно умножения и операции образования обратного элемента.

4. Покажите, что каждую подстановку из S_n при $n > 1$ можно представить в виде произведения транспозиций вида $(k, k+1)$, где $1 \leqslant k < n$.

5. Покажите, что каждую подстановку из S_n при $n > 1$ можно записать в виде произведения транспозиций вида $(1, k)$, где $1 < k \leqslant n$.

§ 4. ОПРЕДЕЛИТЕЛИ

Определитель квадратной матрицы. Пусть $\mathscr{F}$ — коммутативное кольцо или поле, элементы которого будем называть *скалярами*. Пусть

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{bmatrix}$$

— матрица над $\mathscr{F}$, $A \in F^{n \times n}$. Пусть S_n — множество всех подстановок множества $\{1, \dots, n\}$.

Рассмотрим множество $M(A)$ всех произведений элементов матрицы A, взятых по одному из каждой строки и каждого столбца. Всякий элемент множества $M(A)$ содержит n сомножителей и может быть записан в виде (1) $a_{1i_1} \cdot a_{2i_2} \dots a_{ni_n}$.

Элементу (1) поставим в соответствие подстановку

$$(2) \quad \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

множества $\{1, \dots, n\}$. Обратно: каждой подстановке τ из S_n,

$$(3) \quad \tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix},$$

соответствует единственный элемент множества $M(A)$, а именно

$$(4) \quad a_{1\tau(1)} \cdot a_{2\tau(2)} \dots a_{n\tau(n)}.$$

Таким образом, отображение, ставящее в соответствие каждой подстановке τ из S_n элемент (4) множества $M(A)$, есть *инъективное отображение* множества S_n на $M(A)$.

ОПРЕДЕЛЕНИЕ. *Определителем матрицы* A называется сумма

$$\sum_{\tau \in S_n} \operatorname{sgn}(\tau)\ a_{1\tau(1)} \cdot a_{2\tau(2)} \dots a_{n\tau(n)}.$$

Сумма содержит $n!$ слагаемых, причем каждой подстановке τ из S_n в этой сумме соответствует в точности одно слагаемое.

Определитель матрицы A будем обозначать $|A|$, или $\det A$, или

$$\begin{vmatrix} \alpha_{11} \dots \alpha_{1n} \\ \dots\dots \\ \alpha_{n1} \dots \alpha_{nn} \end{vmatrix}.$$

Если $n=1$, то $\det[\alpha_{11}]=\alpha_{11}$. Для $n=2$

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

Если $n=3$, то

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

ПРЕДЛОЖЕНИЕ 4.1. *Определитель матрицы с нулевой строкой (столбцом) равен нулю.*

Квадратная матрица называется *диагональной*, если равны нулю все ее элементы, расположенные вне главной диагонали.

ПРЕДЛОЖЕНИЕ 4.2. *Определитель диагональной матрицы равен произведению элементов ее главной диагонали.*

Квадратная матрица называется *треугольной*, если равны нулю все ее элементы, расположенные выше (ниже) главной диагонали.

ПРЕДЛОЖЕНИЕ 4.3. *Определитель треугольной матрицы равен произведению элементов ее главной диагонали.*

Доказательство предложений 4.1—4.3 предоставляется читателю.

Основные свойства определителей. Сформулируем и докажем наиболее часто встречающиеся свойства.

СВОЙСТВО 4.1. *Определители квадратной матрицы* A *и транспонированной матрицы* ${}^tA$ *равны.*

Доказательство. Пусть $A = \| \alpha_{ik} \|$ — квадратная матрица порядка n и ${}^tA = \| \beta_{ik} \|$, где $\beta_{ik} = \alpha_{ki}$. Тогда имеем:

$$|{}^tA| = \sum_{\tau \in S_n} (\operatorname{sgn} \tau)\, \beta_{1\tau(1)} \dots \beta_{n\tau(n)};$$

$$|{}^tA| = \sum_{\tau \in S_n} (\operatorname{sgn} \tau)\, \alpha_{\tau(1)1} \dots \alpha_{\tau(n)n}. \quad (1)$$

Так как $\tau = \begin{pmatrix} 1 & \dots & n \\ \tau(1) & \dots & \tau(n) \end{pmatrix}$, то $\tau^{-1} = \begin{pmatrix} \tau(1) & \dots & \tau(n) \\ 1 & \dots & n \end{pmatrix}$, или, если расположить в верхней строке числа в порядке возрастания, $\tau^{-1} = \begin{pmatrix} 1 & \dots & n \\ \tau^{-1}(1) & \dots & \tau^{-1}(n) \end{pmatrix}$. В произведении $\alpha_{\tau(1)1} \dots \alpha_{\tau(n)n}$ множители расположим так, чтобы первые индексы шли в порядке возрастания; в результате получим

$$\alpha_{\tau(1)1} \dots \alpha_{\tau(n)n} = \alpha_{1\tau^{-1}(1)} \dots \alpha_{n\tau^{-1}(n)}$$

и равенство (1) можно записать в виде

$$|{}^tA| = \sum_{\tau^{-1} \in S_n} (\operatorname{sgn} \tau^{-1})\, \alpha_{1\tau^{-1}(1)} \dots \alpha_{n\tau^{-1}(n)}. \quad (2)$$

Так как подстановка τ^{-1} пробегает все элементы множества S_n по одному разу, когда τ пробегает все элементы этого множества по одному разу, то сумма в равенстве (2) равна определителю матрицы A. Следовательно, $|{}^tA| = |A|$. □

СВОЙСТВО 4.2. *При перестановке двух столбцов (строк) матрицы ее определитель меняет знак.*

Доказательство. Пусть $A = \| \alpha_{ik} \|$ есть $n \times n$-матрица и $B = \| \beta_{ik} \|$ — матрица, полученная из матрицы A в результате перестановки двух столбцов с индексами s и t. Пусть σ — транспозиция из S_n, переводящая s в t, $\sigma = (st)$, тогда

$$\beta_{ik} = \alpha_{i\sigma(k)} \text{ для } i,\ k \in \{1, \dots, n\},$$

поэтому

$$|B| = \sum_{\tau \in S_n} (\operatorname{sgn} \tau)\, \beta_{1\tau(1)} \dots \beta_{n\tau(n)} = \sum_{\tau \in S_n} (\operatorname{sgn} \tau)\, \alpha_{1\sigma\tau(1)} \dots \alpha_{n\sigma\tau(n)}.$$

По теореме 3.4, $\operatorname{sgn}(\sigma\tau) = -\operatorname{sgn} \tau$. Кроме того, когда подстановка τ пробегает все элементы множества S_n по одному разу, подстановка $\tau' = \sigma\tau$ также пробегает все элементы

этого множества по одному разу. Следовательно, получаем

$$|B| = -\sum_{\tau' \in S_n} (\operatorname{sgn} \tau')\, \alpha_{1\tau'(1)} \dots \alpha_{n\tau'(n)} = -|A|,$$

т. е. $|B| = -|A|$.

СВОЙСТВО 4.3. *Определитель матрицы, имеющий два одинаковых столбца (строки), равен нулю.*

Доказательство. Предположим, что матрица $A = \|\alpha_{ik}\|$ имеет два одинаковых столбца, например $A^s = A^t$. Обозначим транспозицию (st) через σ. Тогда равенство $A^s = A^t$ влечет равенство

(1) $\alpha_{1\tau(1)} \dots \alpha_{n\tau(n)} = \alpha_{1\sigma\tau(1)} \dots \alpha_{n\sigma\tau(n)}$.

Каждой подстановке τ из S_n поставим в соответствие подстановку $\sigma\tau$. Тогда подстановке $\sigma\tau$ соответствует подстановка τ, так как $\sigma(\sigma\tau) = \tau$. Назовем множество $\{\tau, \sigma\tau\}$ *парой соответствующих друг другу подстановок*. Множество S_n распадается на попарно непересекающиеся пары таких подстановок. Следовательно, мы получаем разбиение множества S_n:

$$S_n = \bigcup_{\tau \in A_n} \{\tau,\ \sigma\tau\},$$

где A_n — множество всех четных подстановок степени n. Поэтому равенство

$$|A| = \sum_{\tau \in S_n} (\operatorname{sgn} \tau)\, \alpha_{1\tau(1)} \dots \alpha_{n\tau(n)}$$

можно записать в виде

(2) $|A| = \sum_{\tau \in A_n} [(\operatorname{sgn} \tau)\, \alpha_{1\tau(1)} \dots \alpha_{n\tau(n)} + (\operatorname{sgn} \sigma\tau)\, \alpha_{1\sigma\tau(1)} \dots \alpha_{n\sigma\tau(n)}]$.

Кроме того, по теореме 3.4,

(3) $\operatorname{sgn}(\sigma\tau) = -\operatorname{sgn} \tau$.

На основании (1) и (3) заключаем, что

$$(\operatorname{sgn} \tau)\, \alpha_{1\tau(1)} \dots \alpha_{n\tau(n)} + (\operatorname{sgn} \sigma\tau)\, \alpha_{1\sigma\tau(1)} \dots \alpha_{n\sigma\tau(n)} = 0.$$

Таким образом, каждое слагаемое в сумме (2) равно нулю; следовательно, $|A| = 0$. □

СВОЙСТВО 4.4. *Если все элементы какой-либо строки (столбца) матрицы A умножить на скаляр λ, то на скаляр λ умножится определитель матрицы A.*

Доказательство. Пусть $A=\|\alpha_{ik}\|$ — квадратная матрица порядка n и B — матрица, получающаяся из матрицы A в результате умножения i-й строки на скаляр λ:

$$B=\begin{bmatrix} \alpha_{11}\dots\alpha_{1n} \\ \dots\dots \\ \lambda\alpha_{i1}\dots\lambda\alpha_{in} \\ \dots\dots \\ \alpha_{n1}\dots\alpha_{nn} \end{bmatrix}.$$

Тогда, по определению определителя,

$$|B|=\sum_{\tau\in S_n}(\operatorname{sgn}\tau)\,\alpha_{1\tau(1)}\dots(\lambda\alpha_{i\tau(i)})\dots\alpha_{n\tau(n)}=$$

$$=\lambda\sum_{\tau\in S_n}(\operatorname{sgn}\tau)\,\alpha_{i\tau(1)}\dots\alpha_{i\tau(i)}\dots\alpha_{n\tau(n)},\ \text{т. е. } |B|=\lambda|A|.$$

СЛЕДСТВИЕ 4.4. *Определитель матрицы, у которой какие-либо две строки (столбца) пропорциональны, равен нулю.*

СВОЙСТВО 4.5. *Если каждый элемент i-й строки (столбца) квадратной матрицы A есть сумма m слагаемых, то определитель матрицы A равен сумме m определителей, причем в матрице первого определителя в i-й строке (i-м столбце) стоят первые слагаемые, в матрице второго — вторые и т. д., а остальные строки те же, что и в матрице A.*

Доказательство. Предположим, что каждый элемент i-й строки матрицы A есть сумма m слагаемых:

$$(1)\quad \alpha_{ik}=\alpha_{ik}^{(1)}+\dots+\alpha_{ik}^{(m)}\quad (k=1,\ \dots,\ m).$$

В равенстве

$$|A|=\sum_{\tau\in S_n}(\operatorname{sgn}\tau)\,\alpha_{1\tau(1)}\dots\alpha_{i\tau(i)}\dots\alpha_{n\tau(n)}$$

в каждом слагаемом суммы заменим множитель $\alpha_{i\tau(i)}$ суммой m слагаемых по формуле (1) и представим всю сумму в виде m слагаемых;

$$|A|=\sum_{\tau\in S_n}(\operatorname{sgn}\tau)\,\alpha_{1\tau(1)}\dots\alpha_{i\tau(i)}^{(1)}\dots\alpha_{n\tau(n)}+\dots$$

$$\dots+\sum_{\tau\in S_n}(\operatorname{sgn}\tau)\,\alpha_{1\tau(1)}\dots\alpha_{i\tau(i)}^{(m)}\dots\alpha_{n\tau(n)}.$$

Заменив каждую из m сумм определителем, получим искомое равенство

$$|A| = \begin{vmatrix} \alpha_{11} \dots \alpha_{1n} \\ \dots\dots \\ \alpha_{i1}^{(1)} \dots \alpha_{in}^{(1)} \\ \dots\dots \\ \alpha_{n1} \dots \alpha_{nn} \end{vmatrix} + \dots + \begin{vmatrix} \alpha_{11} \dots \alpha_{1n} \\ \dots\dots \\ \alpha_{i1}^{(m)} \dots \alpha_{in}^{(m)} \\ \dots\dots \\ \alpha_{n1} \dots \alpha_{nn} \end{vmatrix}. \quad \square$$

СВОЙСТВО 4.6. *Если к какому-нибудь столбцу (строке) матрицы определителя прибавить другой столбец (строку) матрицы, умноженный на произвольный скаляр, то определитель матрицы не изменится.*

Доказательство. Запишем $n \times n$-матрицу A в виде

$$A = (A^1, A^2, \dots, A^n).$$

Предположим, что матрица B получается из матрицы A в результате прибавления к первому столбцу k-го столбца, умноженного на скаляр λ, т. е.

$$B = (A^1 + \lambda A^k, A^2, \dots, A^n) \quad (k \neq 1).$$

По свойству 4.5, определитель матрицы B можно представить в виде суммы двух слагаемых:

$$|B| = |(A^1, A^2, \dots, A^n)| + \lambda |(A^k, A^2, \dots, A^n)|.$$

В этой сумме второй определитель равен нулю, так как имеет два одинаковых столбца; следовательно, $|B| = |A|$. $\square$

СЛЕДСТВИЕ 4.5. *Если к какому-нибудь столбцу (строке) матрицы определителя прибавить линейную комбинацию других столбцов (строк) матрицы, то определитель матрицы не изменится.*

СВОЙСТВО 4.7. *Если какой-нибудь столбец (строка) квадратной матрицы есть линейная комбинация других столбцов (строк) матрицы, то определитель матрицы равен нулю.*

Это свойство легко вытекает из следствия 4.5.

Упражнения

1. Как изменится определитель квадратной матрицы порядка n, если каждый элемент матрицы заменить на противоположный?

2. Пусть A — квадратная матрица порядка n над полем $\mathcal{F}$ и λ — элемент этого поля. Докажите, что $|\lambda A| = \lambda^n |A|$.

3. Как изменится определитель квадратной матрицы порядка n с комплексными элементами, если каждый элемент матрицы заменить комплексно-сопряженным?

4. Элементы квадратной матрицы A порядка n удовлетворяют условию $\alpha_{ik}=\bar{\alpha}_{ki}$, где $\bar{\alpha}_{ki}$ — комплексное число, сопряженное с α_{ik}. Докажите, что $|A|$ есть действительное число.

5. Докажите, что определитель треугольной матрицы равен произведению элементов, расположенных на главной диагонали матрицы.

6. Как изменится определитель квадратной матрицы порядка n, если первый столбец матрицы переставить на последнее место, а остальные столбцы передвинуть влево, сохраняя их расположение?

7. Как изменится определитель квадратной матрицы порядка n, если столбцы матрицы написать в обратном порядке?

8. Пусть в поле $\mathcal{F}$ выполняется равенство $1+1=0$. Докажите, что определитель любой кососимметрической матрицы над $\mathcal{F}$ нечетного порядка равен нулю.

9. Докажите, что

$$\begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{vmatrix} = (x_2-x_1)(x_3-x_2)(x_3-x_2).$$

10. Докажите, что имеет место следующее разложение на линейные множители определителя Вандермонда n-го порядка:

$$\begin{vmatrix} 1 & x_1 & x_1^2 \dots x_1^{n-1} \\ 1 & x_2 & x_2^2 \dots x_2^{n-1} \\ \dots & \dots & \dots \\ 1 & x_n & x_n^2 \dots x_n^{n-1} \end{vmatrix} = \prod_{n \geqslant i > k \geqslant 1} (x_i - x_k),$$

11. Покажите, что если квадратная матрица A обратима, то $|A^{-1}|=|A|^{-1}$.

12. Пусть A — квадратная матрица. Докажите, что $|A^k|=|A|^k$ для каждого целого положительного числа k. Покажите, что если матрица A — неособенная, то $|A^k|=|A|^k$ для любого целого числа k.

§ 5. МИНОРЫ И АЛГЕБРАИЧЕСКИЕ ДОПОЛНЕНИЯ. ТЕОРЕМЫ ОБ ОПРЕДЕЛИТЕЛЯХ

Миноры и алгебраические дополнения. Пусть $\mathcal{F}$ — поле скаляров и $A=\|\alpha_{ik}\| \in F^{m\times n}$;

$$A = \begin{bmatrix} \alpha_{11} \dots \alpha_{1n} \\ \dots \dots \\ \alpha_{m1} \dots \alpha_{mn} \end{bmatrix}$$

ОПРЕДЕЛЕНИЕ. *Подматрицей матрицы* A называется матрица, которая получается из A в результате вычеркивания какой-либо совокупности ее строк и столбцов. Подматрица, состоящая из k строк и k столбцов, называется *подматрицей k-го порядка.*

ОПРЕДЕЛЕНИЕ. Определитель подматрицы k-го порядка матрицы A называется *минором k-го порядка матрицы A.*

Минорами первого порядка матрицы A являются ее элементы.

ОПРЕДЕЛЕНИЕ. Определитель матрицы, полученной из квадратной матрицы A вычеркиванием i-й строки и k-го столбца, называется *минором элемента* α_{ik} и обозначается через M_{ik}. Произведение $(-1)^{i+k} M_{ik}$ называется *алгебраическим дополнением* элемента α_{ik} и обозначается через A_{ik}.

Отметим, что M_{ik} и $A_{ik} = (-1)^{i+k} M_{ik}$ не зависят от элемента α_{ik}, однако A_{ik} зависит от четности суммы $i+k$.

ЛЕММА 5.1. *Пусть* $A \in F^{n \times n}$. *Если равны нулю все элементы последней строки (столбца) матрицы* A, *за исключением, быть может, элемента* α_{nn}, *то* $|A| = \alpha_{nn} M_{nn}$.

Доказательство. Предположим, что

(1) $\alpha_{nk} = 0$ для $k \in \{1, \ldots, n-1\}$.

По определению определителя,

$$(2)\quad |A| = \sum_{\tau \in S_n} (\operatorname{sgn} \tau)\, \alpha_{1\tau(1)} \ldots \alpha_{n-1\tau(n-1)} \cdot \alpha_{n\tau(n)}.$$

Определим множество S_n' равенством

$$(3)\quad S_n' = \{\tau \in S_n \mid \tau(n) = n\}.$$

Если $\tau \in S_n \setminus S_n'$, то в силу (1) $\alpha_{n\tau(n)} = 0$. Следовательно, в сумме (2) равны нулю все слагаемые, которые соответствуют подстановкам τ из $S_n \setminus S_n'$. Опуская в сумме (2) эти слагаемые, получаем

$$(4)\quad |A| = \alpha_{nn} \sum_{\tau \in S_n'} (\operatorname{sgn} \tau)\, \alpha_{1\tau(1)} \ldots \alpha_{(n-1)\tau(n-1)}.$$

Рассмотрим следующее отображение φ множества S_n' на S_{n-1}:

$$\tau = \begin{pmatrix} 1 & \ldots & (n-1) & n \\ \tau(1) & \ldots & \tau(n-1) & n \end{pmatrix} \xrightarrow[\varphi]{} \begin{pmatrix} 1 & \ldots & (n-1) \\ \tau(1) & \ldots & \tau(n-1) \end{pmatrix} = \tau'.$$

Таким образом, τ' есть ограничение τ множеством $\{1, \ldots, n-1\}$:

$$(5)\quad \tau'(i) = \tau(i) \text{ для } i \in \{1, \ldots, n-1\},\ \tau' = \begin{pmatrix} 1 & \ldots n-1 \\ \tau'(1) \ldots \tau'(n-1) \end{pmatrix}.$$

Отображение φ есть инъективное отображение множества S_n' на S_{n-1}. Так как $\tau(n) = n$ для $\tau \in S_n'$, то число инвер-

сий в подстановке τ равно числу инверсий в подстановке τ'; следовательно,

(6) $\operatorname{sgn}\tau' = \operatorname{sgn}\tau$ $(\tau' \in S_{n-1})$.

На основании (5) и (6) равенство (4) можно записать в виде

$$|A| = \alpha_{nn} \sum_{\tau' \in S_{n-1}} (\operatorname{sgn}\tau')\ \alpha_{1\tau'(1)} \dots \alpha_{n-1\tau'(n-1)}.$$

В последнем равенстве сумма есть минор M_{nn}, соответствующий элементу α_{nn}, т. е. $|A| = \alpha_{nn} \cdot M_{nn}$. □

ЛЕММА 5.2. *Если равны нулю все элементы какой-либо строки (столбца) квадратной матрицы A, за исключением, быть может, одного элемента, то $|A|$ равен произведению этого элемента на его алгебраическое дополнение.*

Доказательство. Пусть $A = \|\alpha_{ij}\| \in F^{n\times n}$. Предположим, что равны нулю все элементы i-й строки матрицы A, за исключением, быть может, элемента α_{ik}:

(1) $\alpha_{ij} = 0$, $j \in \{1, \dots, n\} \setminus \{k\}$.

В матрице A будем смещать i-ю строку вниз до тех пор, пока она не станет последней, переставляя ее последовательно с соседней (снизу) строкой. Затем k-й столбец полученной матрицы будем смещать вправо, последовательно переставляя его с соседним (справа) столбцом, пока он не станет последним. В результате матрица A перейдет в матрицу

$$B = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} & \alpha_{1k} \\ \dots & \dots & \dots & \dots \\ \alpha_{i-1,1} & \dots & \alpha_{i-1,n} & \alpha_{i-1,k} \\ \alpha_{i+1,1} & \dots & \alpha_{i+1,n} & \alpha_{i+1,k} \\ \dots & \dots & \dots & \dots \\ \alpha_{n1} & \dots & \alpha_{nn} & \alpha_{nk} \\ \alpha_{i1} \dots \alpha_{i,k-1} & & \alpha_{i,k+1} \dots \alpha_{in} & \alpha_{ik} \end{bmatrix}.$$

Ввиду условия (1) равны нулю все элементы последней строки матрицы B, за исключением, быть может, элемента α_{ik}. Следовательно, по лемме 5.1,

(2) $|B| = \alpha_{ik} \cdot M_{ik}$,

где M_{ik} — минор матрицы A, соответствующий элементу α_{ik}. Матрица B получилась из матрицы A в результате

$n-i$ перестановок строк и $n-k$ перестановок столбцов; следовательно, по свойству 4.3 определителей,

$$|B|=(-1)^{n-i+n-k}|A|$$

и

(3) $|A|=(-1)^{i+k}|B|$.

Из (2) и (3) получаем $|A|=(-1)^{i+k}\cdot\alpha_{ik}\cdot M_{ik}=\alpha_{ik}A_{ik}$, т. е. $|A|=\alpha_{ik}A_{ik}$. □

Разложение определителя по строке или столбцу. При вычислении определителей часто используется следующая теорема.

ТЕОРЕМА 5.3. *Пусть* $A\in F^{n\times n}$. *Определитель матрицы* A *равен сумме произведений элементов какого-либо столбца (строки) на их алгебраические дополнения*, т. е.

(1) $|A|=\alpha_{1k}A_{1k}+\ldots+\alpha_{nk}A_{nk}$

$(i,\ k\in\{1,\ \ldots,\ n\})$.

(2) $|A|=\alpha_{i1}A_{i1}+\ldots+\alpha_{in}A_{in}$

Доказательство. Представим в виде суммы n столбцов k-й столбец A^k матрицы A:

$$A^k=\begin{bmatrix}\alpha_{1k}\\0\\\vdots\\0\end{bmatrix}+\begin{bmatrix}0\\\alpha_{2k}\\\vdots\\0\end{bmatrix}+\cdots+\begin{bmatrix}0\\0\\\vdots\\\alpha_{nk}\end{bmatrix}.$$

По свойству 4.5 определителей, этому представлению соответствует представление $|A|$ в виде суммы n определителей:

$$|A|=\begin{vmatrix}\alpha_{11}\ldots\alpha_{1k}\ldots\alpha_{1n}\\\alpha_{21}\ldots0\quad\ldots\alpha_{2n}\\\cdots\cdots\cdots\\\alpha_{n1}\ldots0\quad\ldots\alpha_{nn}\end{vmatrix}+\cdots+\begin{vmatrix}\alpha_{11}\ldots0\quad\ldots\alpha_{1n}\\\alpha_{21}\ldots0\quad\ldots\alpha_{2n}\\\cdots\cdots\cdots\\\alpha_{n1}\ldots\alpha_{nk}\ldots\alpha_{nn}\end{vmatrix}.$$

По лемме 5.2, первое слагаемое этой суммы равно $\alpha_{1k}A_{1k}$, второе — $\alpha_{2k}A_{2k}$ и т. д. Следовательно,

$$|A|=\alpha_{1k}A_{1k}+\alpha_{2k}A_{2k}+\ldots+\alpha_{nk}A_{nk}.$$

Аналогично доказывается формула (2). □

Формула (1) называется *разложением определителя по k-му столбцу*. Формула (2) называется *разложением определителя по i-й строке*.

ТЕОРЕМА 5.4. *Пусть* $A=\|\alpha_{ij}\|\in F^{n\times n}$. *Сумма произведений элементов какого-либо столбца (строки) матрицы* A *на алгебраические дополнения соответствующих элементов другого столбца (строки) равна нулю, т. е.*

(3) $\alpha_{1k}A_{1s}+\ldots+\alpha_{nk}A_{ns}=0$ $(k\neq s)$,

(4) $\alpha_{i1}A_{m1}+\ldots+\alpha_{in}A_{mn}=0$ $(m\neq i)$.

Доказательство. Докажем формулу (3). Запишем A в виде

$$A=(A^1,\ \ldots,\ A^k,\ \ldots,\ A^s,\ \ldots,\ A^n).$$

Заменив в матрице A s-й столбец A^s произвольным вектором $b=\begin{bmatrix}\beta_1\\ \vdots\\ \beta_n\end{bmatrix}$, получим матрицу

$$B=(A^1,\ \ldots,\ A^k,\ \ldots,\ b,\ \ldots,\ A^n).$$

Разложим $|B|$ по s-му столбцу:

$$|B|=\beta_1A_{1s}+\ldots+\beta_nA_{ns}.$$

Отметим, что это равенство верно для любого набора скаляров $\beta_1,\ \ldots,\ \beta_n$. В частности, положив в нем $\beta_1=\alpha_{1k},\ \ldots,\ \beta_n=\alpha_{nk}$, получим равенство

$$0=\alpha_{1k}A_{1s}+\ldots+\alpha_{nk}A_{ns}\quad(k\neq s),$$

так как матрица B будет иметь два одинаковых столбца.

Аналогично доказывается формула (4). □

Определитель произведения матриц. Сначала докажем две леммы.

ЛЕММА 5.5. *Если* E_φ *— элементарная матрица, имеющая тот же порядок, что и квадратная матрица* B, *то*

(1) $|E_\varphi B|=|E_\varphi||B|$ и $|E_\varphi|\neq 0$.

Доказательство. Всякая элементарная матрица треугольна, и поэтому ее определитель равен произведению элементов главной диагонали. Следовательно,

$$(2)\quad |E_\varphi|=\begin{cases}\lambda, & \text{если } E_\varphi=E_{\lambda(i)}\ (\lambda\neq 0),\\ 1, & \text{если } E_\varphi=E_{(i)+\lambda(k)};\end{cases}$$

кроме того,

$$(3)\quad |E_\varphi B|=\begin{cases}\lambda|B|, & \text{если } E_\varphi=E_{\lambda(i)},\\ |B|, & \text{если } E_\varphi=E_{(i)+\lambda(k)}.\end{cases}$$

На основании (2) и (3) заключаем, что имеет место (1). □

ЛЕММА 5.6. *Если* $E_1, \ldots, E_s$ *— элементарные матрицы, имеющие тот же порядок, что и квадратная матрица* B, *то*

$$(4)\quad |E_1E_2\ldots E_sB| = |E_1||E_2|\ldots|E_s||B|.$$

Доказательство (ведется индукцией по числу s). По лемме 5.5, лемма 5.6 верна при $s=1$. Предположим, что лемма верна для $s-1$ элементарных сомножителей, и докажем, что тогда она верна для s сомножителей. По лемме 5.5 имеем

$$|E_1(E_2\ldots E_sB)| = |E_1||E_2\ldots E_sB|.$$

По индуктивному предположению,

$$|E_2\ldots E_sB| = |E_2||E_3|\ldots|E_s||B|;$$

следовательно,

$$|E_1E_2\ldots E_sB| = |E_1||E_2|\ldots|E_s||B|.$$

Таким образом, равенство (4) верно для любого s. □

СЛЕДСТВИЕ 5.7. *Если* $E_1, \ldots, E_s$ *— элементарные матрицы одного и того же порядка, то*

$$|E_1E_2\ldots E_s| = |E_1||E_2|\ldots|E_s|.$$

ТЕОРЕМА 5.8. *Определитель произведения двух квадратных матриц равен произведению определителей этих матриц*, т. е. $|AB| = |A||B|$.

Доказательство. Первый случай: строки матрицы A линейно независимы. По теореме 2.8, матрицу A можно представить в виде произведения элементарных матриц, $A = E_1, \ldots, E_s$, поэтому $AB = E_1\ldots E_sB$. По лемме 5.6 имеем

$$|AB| = |E_1|\ldots|E_s||B|.$$

Кроме того, по следствию 5.7,

$$|A| = |E_1\ldots E_s| = |E_1||E_2|\ldots|E_s|;$$

следовательно, $|AB| = |A||B|$.

Второй случай: строки матрицы A линейно зависимы. В этом случае матрицу A при помощи цепочки строчечных неособенных элементарных преобразований можно привести к ступенчатой матрице, которую обозначим через C; так как строки матрицы линейно зависимы, то C имеет нулевую строку. Если

$$A \underline{\quad} \overset{\varphi_1 \cdots \varphi_s}{\underline{\quad}} C,$$

то, по свойству 2.4 элементарных матриц, $E_{\varphi_1}\dots E_{\varphi_s}\cdot A=C$. Умножим это равенство справа на матрицу B:

$$E_{\varphi_1}\dots E_{\varphi_s}AB=CB.$$

По лемме 5.6, $|E_{\varphi_1}|\dots|E_{\varphi_s}||AB|=|CB|$. Так как C и, значит, CB — матрицы с нулевой строкой, то $|CB|=0$. Кроме того (по лемме 5.5),

$$|E_{\varphi_1}|\neq 0,\ \dots,\ |E_{\varphi_s}|\neq 0,\ |E_{\varphi_1}|\dots|E_{\varphi_s}|\neq 0;$$

следовательно, $|AB|=0$. Так как строки матрицы A линейно зависимы, то одна из строк матрицы A есть линейная комбинация других строк. Поэтому (согласно свойству 4.7 определителей) $|A|=0$. Следовательно, $|A||B|=0$.

Итак, $|AB|=|A||B|$. □

Необходимые и достаточные условия равенства нулю определителя. Как показывают следующие две теоремы, существуют различные эквивалентные между собой условия равенства нулю определителя.

ТЕОРЕМА 5.9. *Определитель квадратной матрицы равен нулю тогда и только тогда, когда строки (столбцы) матрицы линейно зависимы.*

Доказательство. Пусть $A\in F^{n\times n}$. Докажем, что если строки матрицы A линейно независимы, то $|A|\neq 0$. В самом деле, если строки матрицы A линейно независимы, то, по теореме 2.8, ее можно представить в виде произведения элементарных матриц, т. е. $A=E_1\dots E_s$. По следствию 5.7, $|A|=|E_1|\dots|E_s|$. Кроме того, по лемме 5.5, определитель любой элементарной матрицы отличен от нуля. Следовательно, $|A|\neq 0$. По закону контрапозиции, доказанное сейчас утверждение равносильно утверждению: если $|A|=0$, то строки матрицы A линейно зависимы.

Докажем теперь обратное утверждение: если строки квадратной матрицы A линейно зависимы, то $|A|=0$. В самом деле, если первая строка A_1 матрицы A — ненулевая, то хотя бы одна из строк $A_2, \dots, A_n$ является линейной комбинацией других строк этой матрицы. Следовательно, по свойству 4.7 определителей, $|A|=0$. □

ТЕОРЕМА 5.10. *Для любой квадратной матрицы A равносильны следующие четыре утверждения:*

(a) $|A|\neq 0$;

(b) *строки (столбцы) матрицы A линейно независимы;*

(c) *матрица A обратима;*

(d) *матрица A представима в виде произведения элементарных матриц.*

Эта теорема непосредственно следует из теорем 5.9 и 2.8.

Упражнения

1. Пусть A и C — квадратные матрицы. Докажите, что

$$\begin{vmatrix} A & 0 \\ B & C \end{vmatrix} = |A| \cdot |C|,$$

2. Докажите, что

$$\begin{vmatrix} a & b & c \\ c & a & b \\ b & c & a \end{vmatrix} = f(\omega_1) f(\omega_2) f(\omega_3),$$

где $f = a + bx + cx^2$ и ω_1, ω_2, ω_3 — различные корни третьей степени из единицы.

3. Вычислите определитель

$$\begin{vmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{vmatrix}.$$

4. Докажите, что

$$\begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{vmatrix} = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2).$$

5. Пользуясь только определением определителя, вычислите определитель треугольной матрицы A:

$$A = \begin{bmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & 0 & \dots & 0 \\ a_{31} & a_{32} & a_{33} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix}.$$

6. Сколько квадратных подматриц k-го порядка имеет $m \times n$-матрица?

§ 6. ТЕОРЕМЫ О МАТРИЦАХ. ПРАВИЛО КРАМЕРА

Теорема о ранге матрицы. Рассмотрим связь ранга матрицы с порядками ее ненулевых миноров.

ТЕОРЕМА 6.1. *Ранг ненулевой матрицы равен наибольшему из порядков ненулевых миноров матрицы.*

Доказательство. Пусть A — ненулевая матрица и $A \in F^{m \times n}$. Тогда ее ранг $r = r(A) > 0$. Докажем, что матрица A имеет хотя бы один ненулевой минор порядка

r. Так как $r=r(A)>0$, то матрица A имеет r линейно независимых строк. Пусть B — подматрица матрицы A, состоящая из r линейно независимых строк матрицы A, т. е. $B\in F^{r\times n}$, $r(B)=r$. Из равенства $r(B)=r$ следует, что матрица B имеет r линейно независимых столбцов. Пусть C — подматрица матрицы B, состоящая из r линейно независимых столбцов матрицы B, тогда $C\in F^{r\times r}$, $r(C)=r$. По теореме 5.10, $|C|\neq 0$, так как столбцы матрицы C линейно независимы. Таким образом, $|C|$ есть ненулевой минор порядка r матрицы A.

Легко проверить, что при $k>r(A)$ равен нулю любой минор порядка k матрицы A. В самом деле, при $k>r(A)$ линейно зависимы любые k строк матрицы A. Поэтому линейно зависимы строки любой квадратной $k\times k$ подматрицы матрицы A. Следовательно, по теореме 5.9, равен нулю любой минор порядка k матрицы A. □

Обратная матрица. Пусть $A\in F^{n\times n}$,

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

и A_{ik} — алгебраическое дополнение элемента α_{ik}.

Присоединенной для матрицы A называется матрица

$$A^*=\begin{bmatrix}A_{11} & A_{21} & \dots & A_{n1}\\ A_{12} & A_{22} & \dots & A_{n2}\\ \dots & \dots & \dots & \dots\\ A_{1n} & A_{2n} & \dots & A_{nn}\end{bmatrix}.$$

В силу теорем 5.3 и 5.4

$$A_i(A^*)^k=(\alpha_{i1},\dots,\alpha_{in})\begin{bmatrix}A_{k1}\\ \vdots\\ A_{kn}\end{bmatrix}=\alpha_{i1}A_{k1}+\dots+\alpha_{in}A_{kn}=$$

$$=\begin{cases}|A|, & \text{если } i=k,\\ 0, & \text{если } i\neq k,\end{cases}$$

поэтому

$$AA^*=\begin{vmatrix}|A| & 0 & \dots & 0\\ 0 & |A| & \dots & 0\\ \dots & \dots & \dots & \dots\\ 0 & 0 & & |A|\end{vmatrix}=|A|E\ \ (E\text{ — единичная матрица});$$

(1) $A(|A|^{-1}A^*)=E$, если $|A|\neq 0$.

Аналогичные вычисления приводят к равенствам

$$A^*A = |A|E,$$

(2) $(|A|^{-1}A^*)A = E$, если $|A| \neq 0$.

Равенства (1) и (2) показывают, что матрицы A и $|A|^{-1}A^*$ взаимно обратны. Таким образом доказана следующая теорема.

ТЕОРЕМА 6.2. *Если определитель квадратной матрицы A отличен от нуля, то матрица A обратима и $A^{-1} = |A|^{-1}A^*$.*

Правило Крамера. Рассмотрим систему n линейных уравнений с n переменными

$$\begin{aligned} &\alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = \beta_1, \\ &\ldots\ldots\ldots\ldots\ldots \\ &\alpha_{n1}x_1 + \ldots + \alpha_{nn}x_n = \beta_n \end{aligned} \tag{1}$$

над полем $\mathcal{F}$. Обозначим через A основную матрицу этой системы: $A = \|\alpha_{ik}\|$.

ТЕОРЕМА 6.3. *Если $|A| \neq 0$, то система линейных уравнений* (1) *имеет единственное решение, выражаемое формулами*

$$x_1 = |A|^{-1}(\beta_1 A_{11} + \ldots + \beta_n A_{n1}), \ \ldots,$$
$$\ldots, \ x_n = |A|^{-1}(\beta_1 A_{1n} + \ldots + \beta_n A_{nn}). \tag{2}$$

Доказательство. Полагая $\mathcal{X} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, $b = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$, запишем систему (1) в виде матричного уравнения

$$A\mathcal{X} = b, \tag{3}$$

равносильного системе (1). По теореме 5.9, из условия $|A| \neq 0$ следует, что строки матрицы A линейно независимы и системы (3) и (1) имеют единственное решение $\mathcal{X} = A^{-1}b$.

Отсюда, поскольку (по теореме 6.2) $A^{-1} = |A|^{-1}A^*$, получаем

$$A^{-1}b = |A|^{-1}\begin{bmatrix} A_{11} \ldots A_{n1} \\ \ldots\ldots \\ A_{1n} \ldots A_{nn} \end{bmatrix}\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} =$$

$$= |A|^{-1}\begin{bmatrix} \beta_1 A_{11} + \ldots + \beta_n A_{n1} \\ \ldots\ldots\ldots\ldots \\ \beta_1 A_{1n} + \ldots + \beta_n A_{nn} \end{bmatrix}$$

и

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} |A|^{-1}(\beta_1 A_{11} + \ldots + \beta_n A_{n1}) \\ \cdots\cdots\cdots\cdots \\ |A|^{-1}(\beta_1 A_{1n} + \ldots + \beta_n A_{nn}) \end{bmatrix}.$$

Из последнего равенства следуют формулы (2). □

Формулы (2) обычно называют *формулами Крамера*, а теорему 6.3 — *правилом Крамера*.

Обозначим через $A(k)$ матрицу, которая получается из матрицы A в результате замены k-го столбца столбцом свободных членов системы (1):

$$A(1) = \begin{bmatrix} \beta_1 & \alpha_{12} \ldots \alpha_{1n} \\ \cdots\cdots\cdots \\ \beta_n & \alpha_{n2} \ldots \alpha_{nn} \end{bmatrix}, \ldots, A(n) = \begin{bmatrix} \alpha_{11} \ldots \alpha_{1n-1} & \beta_1 \\ \cdots\cdots\cdots\cdots \\ \alpha_{n1} \ldots \alpha_{n\,n-1} & \beta_n \end{bmatrix}.$$

Разлагая определитель матрицы $A(k)$ по k-му столбцу, получаем

$$|A(k)| = \beta_1 A_{1k} + \ldots + \beta_n A_{nk} \quad (k = 1, \ldots, n).$$

Эти равенства позволяют переформулировать теорему 6.3 следующим образом.

ТЕОРЕМА 6.4. *Если* $|A| \neq 0$, *то система линейных уравнений* (1) *имеет единственное решение, выражаемое формулами*

$$(2) \quad x_1 = \frac{|A(1)|}{|A|}, \ \ldots, \ x_n = \frac{|A(n)|}{|A|}.$$

Условия, при которых система n линейных однородных уравнений с n переменными имеет ненулевые решения.

ТЕОРЕМА 6.5. *Система n линейных однородных уравнений с n переменными имеет ненулевые решения тогда и только тогда, когда определитель матрицы системы равен нулю.*

Доказательство. Пусть дана система линейных однородных уравнений

$$(1) \quad \begin{aligned} &\alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = 0, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &\alpha_{n1}x_1 + \ldots + \alpha_{nn}x_n = 0 \end{aligned}$$

и $A = \|\alpha_{ik}\|$ — матрица этой системы. Система (1) имеет ненулевые решения в том и только в том случае, когда столбцы матрицы A линейно зависимы. Столбцы матрицы A линейно зависимы тогда и только тогда, когда $|A| = 0$.

Следовательно, система (1) имеет ненулевые решения в том и только в том случае, когда $|A|=0$. □

СЛЕДСТВИЕ 6.6. *Матричное уравнение* $A\mathcal{X}=\begin{bmatrix}0\\ \vdots\\ 0\end{bmatrix}$, *где* $A\in F^{n\times n}$, $\mathcal{X}=\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}$, *имеет ненулевые решения тогда и только тогда, когда* $|A|=0$.

Упражнения

1. Покажите, что ранг произведения матриц не превосходит ранга каждого сомножителя.

2. Пусть A, B — квадратные матрицы порядка n. Покажите, что уравнения $A\mathcal{X}=B$ и $\mathcal{X}A=B$, где $\mathcal{X}$ — искомая матрица, неразрешимы, когда ранг матрицы B больше ранга матрицы A.

3. Пусть A, B — прямоугольные матрицы, имеющие одинаковое число строк, и C — матрица, получаемая из матрицы A приписыванием к ней справа матрицы B. Докажите, что матричное уравнение $A\mathcal{X}=B$, где $\mathcal{X}$ — искомая матрица, разрешимо тогда и только тогда, когда ранг матрицы A равен рангу матрицы C.

4. Пусть $A\mathcal{X}=B$ — матричное уравнение, где $\mathcal{X}$ — искомая матрица, и $\mathcal{X}_0$ — какое-нибудь его решение. Докажите, что каждое решение матричного уравнения может быть записано в виде $\mathcal{X}_0+\mathcal{Y}$, где $\mathcal{Y}$ — решение однородного уравнения $A\mathcal{Y}=0$, и обратно.

5. Найдите все комплексные матрицы, квадраты которых равны нулевой матрице.

6. Исследуйте уравнение $\mathcal{X}A=0$, где A — данная и $\mathcal{X}$ — искомая матрицы второго порядка.

7. Найдите все комплексные матрицы второго порядка, квадраты которых равны единичной матрице.

8. Пусть A и B — $m\times n$-матрицы. Докажите, что $r(A+B)\leqslant r(A)+r(B)$ *).

9. Пусть A и B — матрицы, имеющие одинаковое число строк, и C — матрица, получающаяся из A приписыванием к ней всех столбцов матрицы B. Докажите, что $r(C)\leqslant r(A)+r(B)$.

10. Покажите, что если произведение AB есть неособенная матрица, то матрицы A и B — также неособенные.

11. Пусть A — неособенная квадратная матрица порядка n. Покажите, что для любой квадратной матрицы B порядка n матрицы AB, B и BA имеют один и тот же ранг.

12. Пусть A, B — $n\times n$-матрицы рангов r и s соответственно. Докажите, что $r(AB)\leqslant r+s-n$.

13. Докажите, что матрица $\begin{bmatrix}a & b\\ c & d\end{bmatrix}$ обратима тогда и только тогда, когда $ad-bc\neq 0$.

---

*) Здесь $r(A)$ — ранг матрицы A.

14. Докажите, что если матрица $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ обратима, то $A^{-1}=$ $=(ad-bc)^{-1}\cdot\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

15. Докажите, что каждая треугольная матрица A (над полем $\mathcal{F}$) с ненулевыми элементами на главной диагонали обратима и матрица A^{-1} треугольна.

16. Пусть A, B — неособенные $n\times n$-матрицы над полем $\mathcal{F}$. Покажите, что равенства $AB=BA$, $AB^{-1}=B^{-1}A$, $A^{-1}B=BA^{-1}$, $A^{-1}B^{-1}=$ $=B^{-1}A^{-1}$ равносильны между собой.

17. Пусть A — $m\times n$-матрица над полем $\mathcal{F}$. Докажите, что:

(a) существует такая $n\times m$-матрица $\mathcal{X}$, что $\mathcal{X}A=E$, где E — единичная $n\times n$-матрица, тогда и только тогда, когда ранг A равен n;

(b) существует $n\times m$-матрица такая, что $A\mathcal{Y}=E$, где E — единичная $m\times m$-матрица, тогда и только тогда, когда ранг A равен m.

18. Пусть A — треугольная $n\times n$-матрица (над полем $\mathcal{F}$), у которой все элементы на главной диагонали равны единице. Пусть $B=$ $=A-E$, где E — единичная $n\times n$-матрица. Докажите, что:

(a) $B^{n+1}=0$;

(b) матрица A обратима и $A^{-1}=(E+B)^{-1}=E-B+B^2-\ldots$ $\ldots+(-1)^n B^n$;

(c) $(E-B)^{-1}=E+B+B^2+\ldots+B^n$.

19. Пусть A — треугольная матрица (над полем) с ненулевыми элементами на главной диагонали. Докажите, что матрица A обратима.

20. Найдите условия, которым должна удовлетворять квадратная матрица с целыми элементами, чтобы все элементы обратной матрицы были целыми.

21. Пусть A — квадратная $n\times n$-матрица и A^* — матрица, присоединенная к A. Докажите, что:

(a) если A — особенная матрица, то матрица AA^* нулевая;

(b) $A^*=|A|A^{-1}$, если A — обратимая матрица;

(c) A^* есть особенная матрица тогда и только тогда, когда матрица A является особенной;

(d) $|A^*|=|A|^{n-1}$;

(e) если матрица A симметрическая или кососимметрическая, то A^* — также симметрическая или кососимметрическая;

(f) если A — треугольная матрица, то A^* — также треугольная.

22. Пусть A^* — матрица, присоединенная к $n\times n$-матрице A. Докажите, что:

(a) если ранг $A<n-1$, то A^* есть нулевая матрица;

(b) если A имеет ранг $n-1$, то ранг A^* равен 1;

(c) если A имеет ранг n, то ранг A^* равен n.

23. Пусть A есть треугольная $n\times n$-матрица над полем $\mathcal{F}$. Докажите, что матрица A обратима тогда и только тогда, когда отличны от нуля все элементы матрицы A, расположенные на главной диагонали.

Глава седьмая

ВЕКТОРНЫЕ ПРОСТРАНСТВА

§ 1. ВЕКТОРНЫЕ ПРОСТРАНСТВА

Понятие векторного пространства. Пусть $\mathscr{F}$ — поле и F — его основное множество. Элементы множества F будем называть *скалярами*, а $\mathscr{F}$ — *полем скаляров*.

Пусть V — непустое множество и $F \times V$ — прямое произведение множеств F и V. Пусть задано отображение

$$\omega : F \times V \to V,$$

ставящее в соответствие каждой паре $\langle \lambda, a \rangle$ из $F \times V$ единственный элемент множества V, который будем обозначать через λa и называть *произведением скаляра* λ *и элемента* a. Если фиксировать скаляр λ, то отображение ω индуцирует отображение

$$\omega_\lambda : \{\lambda\} \times V \to V,$$

которое является ограничением ω на множество $\{\lambda\} \times V$. Отображение ω_λ при фиксированном λ можно рассматривать также как одноместную (унарную) операцию $V \to V$, ставящую в соответствие каждому элементу a из V элемент λa из V. Таким образом, $\omega_\lambda a = \lambda a$ для любого a из V.

Пример. Пусть $\mathscr{F}$ — поле, $V = F^n$ и λ — фиксированный элемент из F. Обозначим через ω_λ отображение V в V, ставящее в соответствие каждому вектору $(\alpha_1, \ldots, \alpha_n)$ из F^n вектор $(\lambda\alpha_1, \ldots, \lambda\alpha_n)$ из F^n, который называется *произведением скаляра* λ *и арифметического вектора* $(\alpha_1, \ldots, \alpha_n)$.

ОПРЕДЕЛЕНИЕ. Множество V с заданными на нем бинарной операцией $+$ (называемой сложением) и операциями умножения элементов поля скаляров $\mathscr{F}$ на элементы множества V называется *векторным пространством над полем* $\mathscr{F}$, если для любых $\boldsymbol{a}$, $\boldsymbol{b}$ из V и α, β из F выполнены следующие условия (аксиомы):

(1) алгебра $\langle V, +, -\rangle$, где $-$ есть операция умножения на скаляр (-1) элементов из V, является абелевой группой;

(2) $(\alpha\beta)\boldsymbol{a} = \alpha(\beta\boldsymbol{a})$;
(3) $\alpha(\boldsymbol{a}+\boldsymbol{b}) = \alpha\boldsymbol{a}+\alpha\boldsymbol{b}$;
(4) $(\alpha+\beta)\boldsymbol{a} = \alpha\boldsymbol{a}+\beta\boldsymbol{a}$;
(5) $1\cdot\boldsymbol{a} = \boldsymbol{a}$.

Векторное пространство с основным множеством V обозначается через $\mathfrak{V}$. Таким образом, векторное пространство $\mathfrak{V}$ есть алгебра с основным множеством V, в котором бинарная операция $+$ и унарные операции ω_λ (умножение на скаляр λ из F) суть главные операции, т. е.

$$\mathfrak{V} = \langle V, +, \{\omega_\lambda \mid \lambda \in F\}\rangle;$$

при этом главные операции удовлетворяют условиям (1)—(5), называемым *аксиомами векторного пространства.*

Группа $\langle V, +, -\rangle$ называется *аддитивной группой векторного пространства* $\mathfrak{V}$. Нуль $\mathbf{0}$ этой группы называется *нулевым вектором пространства* $\mathfrak{V}$. Элементы множества V называются *векторами векторного пространства* $\mathfrak{V}$. Векторы $\boldsymbol{a}$ и $(-1)\,\boldsymbol{a}$ являются *взаимно противоположными.*

Примеры векторных пространств. 1. Пусть $\mathscr{F}^n$ — n-мерное арифметическое пространство над полем $\mathscr{F}$; $\mathscr{F}^n$ является векторным пространством над полем $\mathscr{F}$. Важные частные случаи: $\mathscr{Q}^m$, $\mathscr{R}^n$, $\mathscr{C}^n$.

2. Множество всех векторов плоскости есть векторное пространство над полем $\mathscr{R}$ действительных чисел относительно операций сложения и умножения на действительные числа.

3. Пусть $F^{m\times n}$ — множество всех $m\times n$-матриц над полем $\mathscr{F}$. Алгебра $\langle F^{m\times n}, +, \{\omega_\lambda \mid \lambda \in F\}\rangle$, где $+$ есть операция сложения матриц и ω_λ — операция умножения матриц на скаляр λ, является векторным пространством над $\mathscr{F}$. Его называют *векторным пространством* $m\times n$-матриц над полем $\mathscr{F}$.

4. Множество всех отображений множества $\mathbf{R}$ в $\mathbf{R}$ является векторным пространством над полем $\mathscr{R}$ относительно операций сложения отображений и умножения отображений на действительные числа.

5. Множество $\mathbf{C}$ всех комплексных чисел есть векторное пространство над полем $\mathscr{R}$ относительно операций

сложения комплексных чисел и умножений их на действительные числа.

Простейшие свойства векторных пространств.

ТЕОРЕМА 7.1. *Пусть* $\mathcal{V}$ *— векторное пространство над полем* $\mathcal{F}$, $\boldsymbol{a}, \boldsymbol{b} \in V$ *и* $\alpha, \beta \in F$. *Тогда*

(1) *если* $\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{a}$, *то* $\boldsymbol{b}=0$;

(2) $0 \cdot \boldsymbol{a}=0$;

(3) $\alpha \cdot 0=0$;

(4) *если* $\boldsymbol{a}+\boldsymbol{b}=0$, *то* $\boldsymbol{b}=(-1)\boldsymbol{a}=-\boldsymbol{a}$;

(5) *если* $\alpha \cdot \boldsymbol{a}=\alpha \cdot \boldsymbol{b}$ *и* $\alpha \neq 0$, *то* $\boldsymbol{a}=\boldsymbol{b}$;

(6) *если* $\alpha \cdot \boldsymbol{a}=0$, *то* $\alpha=0$ *или* $\boldsymbol{a}=0$;

(7) *если* $\alpha \boldsymbol{a}=\beta \boldsymbol{a}$ и $\boldsymbol{a} \neq 0$, *то* $\alpha=\beta$.

Доказательство. (1) Так как 0 — нуль аддитивной группы пространства $\mathcal{V}$, то $\boldsymbol{a}+0=\boldsymbol{a}$. Поэтому равенство $\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{a}$ можно записать в виде $\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{a}+0$. По закону сокращения (для групп), отсюда следует $\boldsymbol{b}=0$.

(2) По аксиоме 4 векторного пространства имеем

$$0 \cdot \boldsymbol{a}+0 \cdot \boldsymbol{a}=(0+0)\boldsymbol{a}=0 \cdot \boldsymbol{a}, \text{ т. е. } 0 \cdot \boldsymbol{a}+0 \cdot \boldsymbol{a}=0 \cdot \boldsymbol{a}.$$

По свойству (1), отсюда следует, что $0 \cdot \boldsymbol{a}=0$.

(3) По аксиоме (3) векторного пространства,

$$\alpha \cdot 0+\alpha \cdot 0=\alpha(0+0)=\alpha \cdot 0, \text{ т. е. } \alpha \cdot 0+\alpha \cdot 0=\alpha \cdot 0.$$

По свойству (1), отсюда следует равенство $\alpha \cdot 0=0$.

(4) Так как $\boldsymbol{a}+(-1)\boldsymbol{a}=0$, то равенство $\boldsymbol{a}+\boldsymbol{b}=0$ можно записать в виде $\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{a}+(-1)\boldsymbol{a}$. По закону сокращения (для групп), отсюда следует $\boldsymbol{b}=(-1) \cdot \boldsymbol{a}$.

(5) При $\alpha \neq 0$ из $\alpha \boldsymbol{a}=\alpha \boldsymbol{b}$ следует $\alpha^{-1}(\alpha \boldsymbol{a})=\alpha^{-1}(\alpha \boldsymbol{b})$ и в силу аксиомы (2), $\boldsymbol{a}=\boldsymbol{b}$.

(6) Так как $\alpha 0=0$, то равенство $\alpha \boldsymbol{a}=0$ можно записать в виде $\alpha \boldsymbol{a}=\alpha \cdot 0$. При $\alpha \neq 0$, по свойству (5), отсюда следует, что $\boldsymbol{a}=0$.

(7) Прибавив $(-\beta \boldsymbol{a})$ к обеим частям равенства $\alpha \boldsymbol{a}=\beta \boldsymbol{a}$, получим $\alpha \boldsymbol{a}+(-\beta)\boldsymbol{a}=0$, $(\alpha-\beta)\boldsymbol{a}=0$. При $\boldsymbol{a} \neq 0$, по свойству (6), отсюда следует, что $\alpha-\beta=0$ и $\alpha=\beta$.

Линейная зависимость и независимость системы векторов. Пусть $\mathcal{V}$ — векторное пространство над полем $\mathcal{F}$. Система векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ пространства называется *линейно зависимой*, если существуют скаляры $\lambda_1, \ldots, \lambda_m \in F$, не все равные нулю, такие, что $\lambda_1 \boldsymbol{a}_1+\ldots+\lambda_m \boldsymbol{a}_m=0$.

Система векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ пространства $\mathcal{V}$ называется *линейно независимой*, если для любых скаляров

$\lambda_1, \ldots, \lambda_m \in F$ из равенства $\lambda_1 a_1 + \ldots + \lambda_m a_m = 0$ следуют равенства $\lambda_1 = 0, \ldots, \lambda_m = 0$.

Для произвольных векторных пространств остаются в силе: формулировки и доказательства свойств и теорем § 5.1 о линейной зависимости и независимости систем (свойства 5.1.1 — 5.1.5, теоремы и следствия 5.1.2 — 5.1.5); определения и теоремы § 5.1 об эквивалентных системах векторов и их доказательства (теоремы 5.1.6 — 5.1.8); теоремы и предложения (и их доказательства) из § 5.1 о базисе и ранге конечной системы векторов (теорема 5.1.9, теоремы и предложения 5.1.10 — 5.1.15).

Упражнения

1. Пусть $\mathcal{F} = \mathbb{Z}_2$ — поле классов вычетов по модулю 2. Сколько векторов содержит векторное пространство $\mathcal{V} = \mathcal{F}^n$, n-мерное арифметическое пространство над полем $\mathcal{F}$?

2. Пусть $\mathcal{F}$ — поле скаляров и $F^{2\times 2}$ — множество всех 2×2-матриц над полем $\mathcal{F}$. Покажите, что алгебра

$$\langle F^{2\times 2}, +, -, \{\omega_\lambda \mid \lambda \in F\}\rangle,$$

где $+$ есть операция сложения матриц и ω_λ — операция умножения матриц на скаляр λ, есть векторное пространство над полем $\mathcal{F}$.

3. Пусть $\mathbf{C}^{\mathbf{R}}$ — множество всех отображений множества $\mathbf{R}$ действительных чисел в множество $\mathbf{C}$ комплексных чисел. Покажите, что алгебра

$$\langle \mathbf{C}^{\mathbf{R}}, +, -, \{\omega_\lambda \mid \lambda \in \mathbf{C}\}\rangle,$$

где $+$ есть операция сложения функций, ω_λ — операция умножения функции на скаляр λ, $((\lambda f)(x) = \lambda f(x)$, $\lambda \in \mathbf{C})$ и $-f = (-1)\cdot f$, является векторным пространством над полем комплексных чисел.

4. Пусть $\mathbf{R}^{\mathbf{C}}$ есть множество всех отображений множества $\mathbf{C}$ комплексных чисел в множество $\mathbf{R}$ действительных чисел. Покажите, что алгебра

$$\langle \mathbf{R}^{\mathbf{C}}, +, -, \{\omega_\lambda \mid \lambda \in \mathbf{R}\}\rangle,$$

где $+$ есть операция сложения функций и ω_λ — операция умножения на скаляр λ, является векторным пространством над полем $\mathscr{R}$ действительных чисел.

5. Пусть $\mathscr{R}$ — поле действительных чисел и $\mathscr{Q}$ — поле рациональных чисел. Покажите, что алгебра

$$\langle \mathbf{R}, +, -, \{\omega_\lambda \mid \lambda \in Q\}\rangle,$$

где $+$ есть обычная операция сложения действительных чисел и ω_λ — обычная операция умножения на рациональное число λ, является векторным пространством над полем $\mathscr{Q}$.

6. Пусть $\mathbf{C}$ — множество всех комплексных чисел и $\mathbf{Q}$ — множество всех рациональных чисел. Покажите, что алгебра

$$\langle \mathbf{C}, +, -, \{\omega_\lambda \mid \lambda \in \mathbf{Q}\}\rangle,$$

где $+$ есть обычное сложение комплексных чисел и ω_λ — операция умножения на скаляр λ (на рациональное число λ), есть векторное пространство над полем $\mathcal{Q}$.

7. Пусть V есть множество всех дважды дифференцируемых действительных функций $f: \mathbf{R} \to \mathbf{R}$, удовлетворяющих дифференциальному уравнению $f'' + f = 0$. Покажите, что алгебра

$$\langle V, +, -, \{\omega_\lambda \mid \lambda \in \mathbf{R}\}\rangle,$$

где $+$ есть операция сложения функций и ω_λ — операция умножения функции на скаляр (на действительное число), является векторным пространством над полем $\mathscr{R}$.

8. Пусть V есть множество всех n раз дифференцируемых действительных функций $f: \mathbf{R} \to \mathbf{R}$, удовлетворяющих условию (дифференциальному уравнению)

$$f^{(n)} + \lambda_{n-1} f^{(n-1)} + \ldots + \lambda_1 f' + \lambda_0 f = 0,$$

где $f^{(k)}$ есть k-я производная функции f и $\lambda_0, \ldots, \lambda_{n-1} \in \mathbf{R}$. Докажите, что алгебра $\langle V, +, -, \{\omega_\lambda \mid \lambda \in \mathbf{R}\}\rangle$, где $+$ есть операция сложения функций и ω_λ — операция умножения на скаляр λ, является векторным пространством над полем $\mathscr{R}$.

9. Покажите, что система, состоящая из одного вектора, линейно независима тогда и только тогда, когда вектор ненулевой.

10. Докажите, что система двух векторов линейно зависима тогда и только тогда, когда один из векторов получается из другого умножением на скаляр.

11. Покажите, что векторы (α, β), (γ, δ) двумерного арифметического векторного пространства линейно зависимы тогда и только тогда, когда $\alpha\delta - \beta\gamma = 0$.

12. Каким условиям должны удовлетворять скаляры α, β, γ, чтобы система векторов $(1, \alpha, \alpha^2)$, $(1, \beta, \beta^2)$, $(1, \gamma, \gamma^2)$ трехмерного арифметического векторного пространства над числовым полем $\mathscr{F}$ была линейно независимой?

13. Пусть $\mathscr{V}$ — векторное пространство над числовым полем $\mathscr{F}$. Покажите, что если векторы $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ пространства $\mathscr{V}$ линейно независимы, то векторы $\boldsymbol{a}+\boldsymbol{b}$, $\boldsymbol{a}+\boldsymbol{c}$, $\boldsymbol{b}+\boldsymbol{c}$ также линейно независимы. Верно ли это, если поле скаляров $\mathscr{F}$ состоит из двух элементов?

14. Пусть $\mathscr{V} = \mathscr{F}^n$ есть n-мерное арифметическое пространство над полем $\mathscr{F}$. Покажите, что система векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ пространства $\mathscr{V}$ линейно независима тогда и только тогда, когда ранг $m \times n$-матрицы со строками $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ равен m.

15. Покажите, что система ненулевых векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ векторного пространства $\mathscr{V}$ линейно независима тогда и только тогда, когда $\boldsymbol{a}_k \notin L(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{k-1})$ для всех $k = 2, 3, \ldots, m$.

16. Пусть $\mathscr{F}$ — конечное поле, состоящее из p элементов, и $\mathscr{V} = \mathscr{F}^n$. Сколько существует различных линейно независимых систем из k векторов $(k < n)$ пространства $\mathscr{V}$?

17. Пусть $\mathscr{F}$ — поле и A есть $n \times n$-матрица над $\mathscr{F}$. Докажите, что при достаточно большом m система матриц E, A, A^2, $\ldots$, A^m, где E — единичная $n \times n$-матрица, линейно зависима над полем $\mathscr{F}$.

18. Пусть $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \in \mathbf{Q}$. Докажите, что система векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ линейно независима в пространстве $\mathscr{R}^n$ тогда и только тогда, когда она линейно независима в пространстве $\mathcal{Q}^n$.

19. Пусть $\mathscr{F}$ — конечное поле, состоящее из p элементов. Сколько различных k-мерных подпространств $(k < n)$ имеет векторное пространство $\mathscr{F}^n$?

Подпространство. Пусть $\mathfrak{V}$ — векторное пространство над полем $\mathfrak{F}$ и $U \subset V$. Множество U называется *замкнутым* в $\mathfrak{V}$, если оно замкнуто относительно главных операций $\mathfrak{V}$, операций сложения и умножения на скаляры, т. е. для любых $\boldsymbol{a}$, $\boldsymbol{b}$ из U и любого λ из F $\boldsymbol{a}+\boldsymbol{b} \in U$ и $\lambda \boldsymbol{a} \in U$.

ОПРЕДЕЛЕНИЕ. *Подпространством векторного пространства* $\mathfrak{V}$ называется любая подалгебра пространства $\mathfrak{V}$, рассматриваемого как алгебра.

Пусть $\mathfrak{V}=\langle V, +, \{\omega_\lambda \mid \lambda \in F\}\rangle$ — векторное пространство над $\mathfrak{F}$. Пусть $\mathfrak{U}$ — подалгебра пространства $\mathfrak{V}$ и U — его основное множество. Тогда U — непустое подмножество множества V, замкнутое в $\mathfrak{V}$. Пусть $\oplus$ и ω'_λ — ограничения главных операций «$+$» и ω_λ пространства $\mathfrak{V}$ множеством U, т. е.

$\boldsymbol{a} \oplus \boldsymbol{b} = \boldsymbol{a} + \boldsymbol{b}$ для любых $\boldsymbol{a}$, $\boldsymbol{b}$ из U,

$\omega'_\lambda \boldsymbol{a} = \omega_\lambda \boldsymbol{a} = \lambda \boldsymbol{a}$ для любого $\boldsymbol{a}$ из U;

тогда

(1) $\mathfrak{U} = \langle U, \oplus, \{\omega'_\lambda \mid \lambda \in F\}\rangle$.

Однако вместо записи (1) обычно пишут

$\mathfrak{U} = \langle U, +, \{\omega_\lambda \mid \lambda \in F\}\rangle$.

Отметим следующие свойства подпространств.

СВОЙСТВО 2.1. *Если* $\mathfrak{V}$ *— векторное пространство над полем* $\mathfrak{F}$, *то любое его подпространство является векторным пространством над* $\mathfrak{F}$.

СВОЙСТВО 2.2. *Если* $\mathfrak{W}$ *— подпространство векторного пространства* $\mathfrak{U}$ *и* $\mathfrak{U}$ *— подпространство векторного пространства* $\mathfrak{V}$, *то* $\mathfrak{W}$ *является подпространством пространства* $\mathfrak{V}$.

Пересечением подпространств $\mathfrak{U}_1, \ldots, \mathfrak{U}_m$ векторного пространства $\mathfrak{V}$ называется подпространство $\mathfrak{V}$ с основным множеством $U_1 \cap U_2 \cap, \ldots, \cap U_m$. Аналогично определится пересечение бесконечного множества подпространств пространства $\mathfrak{V}$.

СВОЙСТВО 2.3. *Пересечение любого множества подпространств векторного пространства* $\mathfrak{V}$ *является подпространством пространства* $\mathfrak{V}$.

Свойства 2.2 и 2.3 следуют из теорем 3.1.7 и 3.1.9 соответственно.

Линейная оболочка множества векторов. Пусть $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\}$ — конечное множество векторов векторного про-

странства $\mathfrak{V}$. Вектор $\lambda_1 a_1 + \ldots + \lambda_n a_n$ называется *линейной комбинацией векторов* $a_1, \ldots, a_n$ с коэффициентами из F.

ОПРЕДЕЛЕНИЕ. Множество $\{\lambda_1 a_1 + \ldots + \lambda_n a_n \mid \lambda_1, \ldots, \lambda_n \in F\}$ всех линейных комбинаций векторов $a_1, \ldots, a_n$ с коэффициентами из F называется *линейной оболочкой векторов* $a_1, \ldots, a_n$ и обозначается через $L(a_1, \ldots, a_n)$.

Легко видеть, что линейная оболочка векторов замкнута в $\mathfrak{V}$, т. е. замкнута относительно всех главных операций пространства $\mathfrak{V}$ (сложения и умножений на скаляры).

ОПРЕДЕЛЕНИЕ. Подпространство векторного пространства $\mathfrak{V}$ с основным множеством $L(a_1, \ldots, a_n)$ обозначается через $\mathfrak{L}(a_1, \ldots, a_n)$ и называется *подпространством,* натянутым на векторы $a_1, \ldots, a_n$, или подпространством, порожденным векторами $a_1, \ldots, a_n$.

ОПРЕДЕЛЕНИЕ. *Линейной оболочкой множества* M, $M \subset V$, называется совокупность $L(M)$ всех линейных комбинаций векторов из M с коэффициентами из F. *Линейной оболочкой пустого множества* называется множество $\{0\}$.

Линейная оболочка множества M замкнута в $\mathfrak{V}$.

ОПРЕДЕЛЕНИЕ. Подпространство пространства $\mathfrak{V}$ с основным множеством $L(M)$ обозначается через $\mathfrak{L}(M)$ и называется *подпространством, натянутым на множество* M, или *подпространством, порожденным множеством* M.

Сумма подпространств. Пусть $\mathfrak{U}_1, \ldots, \mathfrak{U}_m$ — подпространства векторного пространства $\mathfrak{V}$ и $U_1, \ldots, U_m$ — их основные множества. Множество

$$\{a_1 + \ldots + a_m \mid a_1 \in U_1, \ldots, a_m \in U_m\}$$

обозначается через $U_1 + \ldots + U_m$. Легко проверить, что это множество замкнуто в пространстве $\mathfrak{V}$.

ОПРЕДЕЛЕНИЕ. Подпространство пространства $\mathfrak{V}$ с основным множеством $U_1 + \ldots + U_m$ называется *суммой подпространств* $\mathfrak{U}_1, \ldots, \mathfrak{U}_m$ и обозначается через $\mathfrak{U}_1 + \ldots + \mathfrak{U}_m$.

Отметим следующие свойства суммы подпространств, легко вытекающие из ее определения.

СВОЙСТВО 2.4. Если $\mathfrak{L}$ и $\mathfrak{U}$ — подпространства векторного пространства $\mathfrak{V}$, то $\mathfrak{U} + \mathfrak{L} = \mathfrak{L} + \mathfrak{U}$.

СВОЙСТВО 2.5. Если $\mathfrak{L}$, $\mathfrak{U}$, $\mathfrak{W}$ — подпространства векторного пространства $\mathfrak{V}$, то $\mathfrak{L} + (\mathfrak{U} + \mathfrak{W}) = (\mathfrak{L} + \mathfrak{U}) + \mathfrak{W}$.

СВОЙСТВО 2.6. Если $\mathscr{L}$ — подпространство пространства $\mathscr{U}$, то $\mathscr{L}+\mathscr{U}=\mathscr{U}$.

Пусть $\mathscr{L}_1, \ldots, \mathscr{L}_m$ — подпространства векторного пространства $\mathscr{V}$.

ОПРЕДЕЛЕНИЕ. Сумма $\mathscr{L}_1+\ldots+\mathscr{L}_m$ называется *прямой суммой подпространств* $\mathscr{L}_1, \ldots, \mathscr{L}_m$ и обозначается через $\mathscr{L}_1 \oplus \ldots \oplus \mathscr{L}_m$, если любой вектор $\boldsymbol{a}$ из $L_1+\ldots+L_m$ можно единственным образом представить в виде

$$\boldsymbol{a}=\boldsymbol{a}_1+\ldots+\boldsymbol{a}_m, \text{ где } \boldsymbol{a}_1 \in L_1, \ldots, \boldsymbol{a}_m \in L_m.$$

Другими словами, сумма $\mathscr{L}_1+\ldots+\mathscr{L}_m$ называется *прямой*, если для любых $\boldsymbol{a}_1, \boldsymbol{b}_1$ из $L_1, \ldots, \boldsymbol{a}_m, \boldsymbol{b}_m$ из L_m равенство $\boldsymbol{a}_1+\ldots+\boldsymbol{a}_m=\boldsymbol{b}_1+\ldots+\boldsymbol{b}_m$ влечет равенства $\boldsymbol{a}_1=\boldsymbol{b}_1, \ldots, \boldsymbol{a}_m=\boldsymbol{b}_m$.

ТЕОРЕМА 2.1. *Сумма подпространств* $\mathscr{L}$ и $\mathscr{U}$ *векторного пространства является прямой тогда и только тогда, когда* $L \cap U=\{\mathbf{0}\}$.

Доказательство. Предположим, что $\mathscr{L}+\mathscr{U}=\mathscr{L} \oplus \mathscr{U}$. Тогда для любого элемента $\boldsymbol{c}$ из $L \cap U$ верно равенство $\boldsymbol{c}+\mathbf{0}=\mathbf{0}+\boldsymbol{c}$, из которого следует равенство $\boldsymbol{c}=\mathbf{0}$, так как сумма $\mathscr{L}+\mathscr{U}$ прямая. Следовательно, $L \cap U=\{\mathbf{0}\}$.

Предположим теперь, что $L \cap U=\{\mathbf{0}\}$. Для любых векторов $\boldsymbol{a}_1$, $\boldsymbol{b}_1$ из L и $\boldsymbol{a}_2$, $\boldsymbol{b}_2$ из U равенство $\boldsymbol{a}_1+\boldsymbol{a}_2=\boldsymbol{b}_1+\boldsymbol{b}_2$ влечет соотношения $\boldsymbol{a}_1-\boldsymbol{b}_1=\boldsymbol{a}_2-\boldsymbol{b}_2 \in L \cap U=\{\mathbf{0}\}$, поэтому $\boldsymbol{a}_1=\boldsymbol{b}_1$ и $\boldsymbol{a}_2=\boldsymbol{b}_2$. Следовательно, сумма $\mathscr{L}+\mathscr{U}$ является прямой. □

ТЕОРЕМА 2.2. *Сумма подпространств* $\mathscr{L}_1, \ldots, \mathscr{L}_m$ *векторного пространства является прямой суммой, если для любых векторов* $\boldsymbol{a}_1$ *из* $L_1, \ldots, \boldsymbol{a}_m$ *из* L_m *равенство*

(1) $\boldsymbol{a}_1+\ldots+\boldsymbol{a}_m=\mathbf{0}$

влечет равенства

(2) $\boldsymbol{a}_1=\mathbf{0}, \ldots, \boldsymbol{a}_m=\mathbf{0}$.

Доказательство. Предположим, что сумма $\mathscr{L}_1+\ldots+\mathscr{L}_m$ прямая. Тогда из равенства (1), которое можно записать в виде $\boldsymbol{a}_1+\ldots+\boldsymbol{a}_m=\mathbf{0}+\ldots+\mathbf{0}$, следуют равенства $\boldsymbol{a}_1=\mathbf{0}, \ldots, \boldsymbol{a}_m=\mathbf{0}$.

Предположим теперь, что для любых векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ соответственно из $L_1, \ldots, L_m$ равенство (1) влечет равенства (2). Каковы бы ни были векторы $\boldsymbol{b}_1$, $\boldsymbol{c}_1$ из $L_1, \ldots, \boldsymbol{b}_m$, $\boldsymbol{c}_m$ из L_m, равенство

(3) $\boldsymbol{b}_1+\ldots+\boldsymbol{b}_m=\boldsymbol{c}_1+\ldots+\boldsymbol{c}_m$

влечет $(b_1-c_1)+\ldots+(b_m-c_m)=0$, из которого, по условию, следуют равенства

$$b_1-c_1=0,\ \ldots,\ b_m-c_m=0.$$

Таким образом, из (3) следуют равенства

$$b_1=c_1,\ \ldots,\ b_m=c_m.$$

Следовательно, сумма $\mathscr{L}_1+\ldots+\mathscr{L}_m$ является прямой. □

Линейные многообразия. Пусть $\mathscr{L}$ — подпространство векторного пространства $\mathscr{V}$ и L — его основное множество. На множестве V определим бинарное отношение $\sim$, считая, что $a\sim b$ тогда и только тогда, когда $a-b\in L$. Назовем это бинарное отношение *отношением сравнения по* $\mathscr{L}$.

ПРЕДЛОЖЕНИЕ 2.3. *Отношение сравнения на множестве* V *по* $\mathscr{L}$ *является отношением эквивалентности на* V.

Доказательство. Отношение сравнения по $\mathscr{L}$, очевидно, рефлексивно. Отношение по $\mathscr{L}$ симметрично, так как из $a-b\in L$ следует $b-a\in L$. Отношение сравнения по $\mathscr{L}$ транзитивно, так как для любых a, b, $c\in V$ из $a-b\in L$ и $b-c\in L$ следует, что $a-c=(a-b)+(b-c)\in L$. Следовательно, отношение сравнения по $\mathscr{L}$ является отношением эквивалентности на множестве V. □

Отношение эквивалентности $\sim$ на V определяет разбиение множества V на классы эквивалентности.

ОПРЕДЕЛЕНИЕ. Пусть $\mathscr{L}$ — подпространство векторного пространства $\mathscr{V}$. Любой класс эквивалентности отношения сравнения по $\mathscr{L}$ называется *линейным многообразием пространства* $\mathscr{V}$ *с направлением* $\mathscr{L}$.

Пример. Множество всех решений совместной системы линейных уравнений с n переменными является линейным многообразием с направлением $\mathscr{L}$ n-мерного арифметического векторного пространства, где $\mathscr{L}$ — пространство решений соответствующей однородной системы уравнений.

Из приведенного выше определения вытекают свойства 2.7 и 2.8.

СВОЙСТВО 2.7. *Два вектора векторного пространства* $\mathscr{V}$ *принадлежат одному и тому же линейному многообразию с направлением* $\mathscr{L}$ *тогда и только тогда, когда их разность принадлежит* L.

СВОЙСТВО 2.8. *Любые два линейных многообразия векторного пространства* $\mathscr{V}$ *с направлением* $\mathscr{L}$ *либо совпадают, либо не пересекаются. Объединение всех линейных*

многообразий пространства $\mathfrak{V}$ *с направлением* $\mathfrak{L}$ *равно множеству* V.

Обозначим через $\boldsymbol{a}+L$ ($\boldsymbol{a}\in V$) множество $\{\boldsymbol{a}+\boldsymbol{x}\mid \boldsymbol{x}\in L\}$.

СВОЙСТВО 2.9. *Если* H *— линейное многообразие векторного пространства* $\mathfrak{V}$ *с направлением* $\mathfrak{L}$ *и* $\boldsymbol{a}\in H$, *то* $H=\boldsymbol{a}+L$.

Доказательство. Так как любой элемент множества $\boldsymbol{a}+L$ сравним с $\boldsymbol{a}$ по $\mathfrak{L}$, то $\boldsymbol{a}+L\subset H$. Кроме того, любой элемент $\boldsymbol{c}$ из H сравним с $\boldsymbol{a}$ по $\mathfrak{L}$, т. е. $\boldsymbol{c}-\boldsymbol{a}\in L$ и $\boldsymbol{c}\in\boldsymbol{a}+L$. Поэтому $H\subset\boldsymbol{a}+L$. Следовательно, $H=\boldsymbol{a}+L$. □

СЛЕДСТВИЕ 2.4. *Если* $\boldsymbol{a}$ *и* $\boldsymbol{b}$ *— элементы одного и того же линейного многообразия пространства* $\mathfrak{V}$ *с направлением* $\mathfrak{L}$, *то* $\boldsymbol{a}+L=\boldsymbol{b}+L$.

СЛЕДСТВИЕ 2.5. *Если* $\mathfrak{L}\rightarrow\mathfrak{V}$ *и* $\boldsymbol{c}$ *— любой элемент пространства* $\mathfrak{V}$, *то* $\boldsymbol{c}+L$ *является линейным многообразием пространства* $\mathfrak{V}$ *с направлением* $\mathfrak{L}$.

СВОЙСТВО 2.10. *Пусть* $\mathfrak{L}$ *и* $\mathfrak{U}$ *— подпространства векторного пространства* $\mathfrak{V}$ *и* $\boldsymbol{a}$, $\boldsymbol{b}\in V$. *Включение* $\boldsymbol{a}+L\subset\boldsymbol{b}+U$ *имеет место тогда и только тогда, когда* $\boldsymbol{a}-\boldsymbol{b}\in U$ *и* $L\subset U$.

Доказательство. Предположим, что $\boldsymbol{a}+L\subset\boldsymbol{b}+U$. Тогда $\boldsymbol{a}\in\boldsymbol{b}+U$, $\boldsymbol{a}-\boldsymbol{b}\in U$ и $\boldsymbol{a}+U=\boldsymbol{b}+U$, поэтому $\boldsymbol{a}+L\subset\boldsymbol{a}+U$ и $L\subset U$.

Предположим теперь, что выполнены условия $\boldsymbol{a}-\boldsymbol{b}\in U$, $L\subset U$. Тогда $\boldsymbol{a}+U=\boldsymbol{b}+U$ и $\boldsymbol{a}+L\subset\boldsymbol{a}+U$; следовательно, $\boldsymbol{a}+L\subset\boldsymbol{b}+U$. □

СВОЙСТВО 2.11. *Пересечение линейных многообразий* $\boldsymbol{a}+L$ *и* $\boldsymbol{b}+U$ *векторного пространства не пусто тогда и только тогда, когда* $\boldsymbol{a}-\boldsymbol{b}\in L+U$.

Доказательство. Предположим, что пересечение $\boldsymbol{a}+L\cap\boldsymbol{b}+U$ не пусто и $\boldsymbol{c}$ — элемент пересечения. Тогда $\boldsymbol{c}=\boldsymbol{a}+\boldsymbol{l}=\boldsymbol{b}+\boldsymbol{u}$, где $\boldsymbol{l}\in L$ и $\boldsymbol{u}\in U$; поэтому $\boldsymbol{a}-\boldsymbol{b}=-\boldsymbol{l}+\boldsymbol{u}$ и $\boldsymbol{a}-\boldsymbol{b}\in L+U$.

Предположим теперь, что $\boldsymbol{a}-\boldsymbol{b}\in L+U$. Тогда $\boldsymbol{a}-\boldsymbol{b}=\boldsymbol{v}+\boldsymbol{u}$, где $\boldsymbol{v}\in L$, $\boldsymbol{u}\in U$, и $\boldsymbol{a}+(-\boldsymbol{v})=\boldsymbol{b}+\boldsymbol{u}$. Следовательно, многообразия $\boldsymbol{a}+L$ и $\boldsymbol{b}+U$ имеют общий элемент $\boldsymbol{b}+\boldsymbol{u}$. □

СВОЙСТВО 2.12. *Если пересечение линейного многообразия с направлением* $\mathfrak{L}$ *и линейного многообразия с направлением* $\mathfrak{U}$ *не пусто, то оно является линейным многообразием с направлением* $\mathfrak{L}\cap\mathfrak{U}$.

Доказательство. Предположим, что пересечение многообразий $\boldsymbol{a}+L$ и $\boldsymbol{b}+U$ не пусто и $\boldsymbol{c}$ — их общий

элемент; тогда $\boldsymbol{a}+L=\boldsymbol{c}+L$, $\boldsymbol{b}+U=\boldsymbol{c}+U$ и $\boldsymbol{a}+L\cap\boldsymbol{b}+U=\boldsymbol{c}+L\cap\boldsymbol{c}+U$. Легко проверить, что $\boldsymbol{c}+L\cap\boldsymbol{c}+U=\boldsymbol{c}+(L\cap U)$. Следовательно, $\boldsymbol{a}+L\cap\boldsymbol{b}+U=\boldsymbol{c}(L\cap U)$, т. е. пересечение двух рассматриваемых многообразий есть линейное многообразие с направлением $\mathscr{L}\cap\mathscr{U}$. □

СВОЙСТВО 2.13. *Если векторное пространство $\mathscr{V}$ есть прямая сумма подпространств $\mathscr{L}$ и $\mathscr{U}$, то пересечение линейного многообразия с направлением $\mathscr{L}$ и линейного многообразия с направлением $\mathscr{U}$ содержит только один элемент.*

Доказательство. Пусть $\mathscr{V}=\mathscr{L}\oplus\mathscr{U}$, тогда $V=L+U$, $L\cap U=\{\mathbf{0}\}$. Пусть $\boldsymbol{a}+L$ и $\boldsymbol{b}+U$ — линейные многообразия с направлениями $\mathscr{L}$ и $\mathscr{U}$ соответственно. По свойству 2.11, их пересечение не пусто, так как $\boldsymbol{a}-\boldsymbol{b}\in V=L+U$. Пусть $\boldsymbol{c}$ — общий элемент пересечения. По свойству 2.12, отсюда следует, что $\boldsymbol{a}+L\cap\boldsymbol{b}+U=\boldsymbol{c}+(L\cap U)=\boldsymbol{c}+\{\mathbf{0}\}=\boldsymbol{c}$. □

Упражнения

1. Каждое из следующих условий выделяет некоторое множество векторов $(x_1, \ldots, x_n)$ векторного пространства $\mathscr{V}=\mathscr{F}^n$. Какие из этих множеств замкнуты в $\mathscr{V}$ относительно сложения и умножений на скаляры:

(a) $x_1+x_2+\ldots+x_n=0$;
(b) $x_1+x_2+\ldots+x_n=1$;
(c) $x_1-x_2-\ldots-x_n=0$;
(d) $x_n=0$;
(e) $x_1=1$;
(f) $x_1=x_n=0$;
(g) $x_1\cdot x_n=0$;
(h) $x_1=x_2=\ldots=x_n$?

2. Пусть $\mathscr{V}=\mathscr{F}^{n\times n}$ — векторное пространство всех $n\times n$-матриц над полем. Покажите, что множество всех симметрических (кососимметрических) матриц пространства $\mathscr{V}$ есть подпространство пространства $\mathscr{V}$ относительно сложения и умножений на скаляры.

3. Пусть $\mathscr{V}=\mathscr{F}^{n\times n}$ над числовым полем $\mathscr{F}$, $\mathscr{L}$ — подпространство всех симметрических $n\times n$-матриц и $\mathscr{U}$ — подпространство всех кососимметрических матриц. Докажите, что $\mathscr{V}=\mathscr{L}\oplus\mathscr{U}$.

4. Пусть $\mathscr{V}$ есть векторное пространство (над $\mathscr{R}$) всех трижды дифференцируемых функций f: $\mathbf{R}\to\mathbf{R}$, удовлетворяющих условию $f'''+f'=0$. Покажите, что множество всех функций пространства, удовлетворяющих условию $f''+f=0$, образует подпространство пространства $\mathscr{V}$.

5. Пусть $\mathscr{V}=\mathscr{R}^{2\times 2}$ — векторное пространство 2×2-матриц над полем $\mathscr{R}$ действительных чисел. Покажите, что множество всех матриц над $\mathscr{R}$ вида $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ образует подпространство пространства $\mathscr{V}$.

6. Пусть $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k, \boldsymbol{b}_1 \ldots, \boldsymbol{b}_s$ — векторы векторного пространства $\mathscr{V}$. Докажите, что

$$L(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k)+L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_s)=L(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_s).$$

7. Докажите, что пересечение любого множества подпространств векторного пространства $\mathscr{V}$ является подпространством пространства $\mathscr{V}$.

8. Пусть $\mathscr{L}$ и $\mathscr{U}$ — подпространства векторного пространства $\mathscr{V}$. Докажите, что $\mathscr{L}+\mathscr{U}$ есть пересечение всех подпространств пространства $\mathscr{V}$, содержащих подпространства $\mathscr{L}$ и $\mathscr{U}$.

9. Пусть a, b, c — векторы, удовлетворяющие условию $a+\lambda b+\xi c=0$, где λ, ξ — ненулевые скаляры. Покажите, что $L(a, b)=L(b, c)=L(c, a)$.

10. Пусть векторы a, b линейно независимы. Покажите, что $\mathscr{L}(a, b)=\mathscr{L}(a)\oplus\mathscr{L}(b)$.

11. Пусть система векторов a, b, c линейно независима. Докажите, что $\mathscr{L}(a, b, c)=\mathscr{L}(a)\oplus\mathscr{L}(b)\oplus\mathscr{L}(c)$.

12. Покажите, что если вектор b есть линейная комбинация векторов $a_1, \ldots, a_m$, то $L(a_1, \ldots, a_m)=L(a_1, \ldots, a_m, b)$.

13. Предположим, что векторное пространство $\mathscr{V}$ порождается подпространством $\mathscr{U}$ и вектором a. Покажите, что если $b\in V\setminus U$, то $\mathscr{V}=\mathscr{U}\oplus\mathscr{L}(b)$.

14. Пусть $\mathscr{V}$ есть сумма подпространств $\mathscr{L}$ и $\mathscr{U}$. Покажите, что $\mathscr{V}=\mathscr{L}\oplus\mathscr{U}$, если хотя бы один вектор $c\in V$ можно однозначно представить в виде $c=a+b$, где $a\in L$, $b\in U$.

15. Пусть $\mathscr{V}$ есть прямая сумма подпространств $\mathscr{L}$ и $\mathscr{U}$. Покажите, что если $a_1, \ldots, a_m$ есть линейно независимая система векторов подпространства $\mathscr{L}$, а $b_1, \ldots, b_s$ — линейно независимая система векторов из $\mathscr{U}$, то $a_1, \ldots, a_m, b_1, \ldots, b_s$ есть линейно независимая система векторов пространства $\mathscr{V}$.

16. Пусть векторное пространство $\mathscr{V}$ есть сумма подпространств $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$. Докажите, что $\mathscr{V}=\mathscr{L}_1\oplus\mathscr{L}_2\oplus\mathscr{L}_3$ тогда и только тогда, когда $L_1\cap L_2=0$ и $(L_1+L_2)\cap L_3=0$.

17. Пусть $\mathscr{V}=\mathscr{F}^n$, где $\mathscr{F}$ — поле скаляров, состоящее из двух элементов, и $b_1, \ldots, b_m$ — линейно независимая система векторов пространства $\mathscr{V}$. Сколько векторов имеет линейная оболочка $L(b_1, \ldots, b_m)$ этих векторов?

§ 3. БАЗИС И РАЗМЕРНОСТЬ ВЕКТОРНОГО ПРОСТРАНСТВА

Базис векторного пространства. Пусть $\mathscr{V}$ — векторное пространство с основным множеством V. Если существует в V такое конечное множество $\{a_1, \ldots, a_m\}$ векторов, что $V=L(a_1, \ldots, a_m)$, то говорят, что пространство $\mathscr{V}$ порождается конечным множеством $\{a_1, \ldots, a_m\}$, и это множество называется *множеством* (или системой) *образующих пространства* $\mathscr{V}$.

ОПРЕДЕЛЕНИЕ. Векторное пространство называется *конечномерным*, если оно порождается конечным множеством векторов.

ОПРЕДЕЛЕНИЕ. *Базисом конечномерного векторного пространства* называется непустая конечная линейно независимая система векторов, порождающая это пространство.

Пример. Пусть $\mathcal{V} = \mathcal{F}^n$ — арифметическое векторное пространство над полем $\mathcal{F}$. Система единичных векторов

$$e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 0, 1)$$

линейно независима и порождает пространство $\mathcal{V}$, т. е. $V = L(e_1, \ldots, e_n)$. Следовательно, система векторов $e_1, \ldots, e_n$ является базисом пространства $\mathcal{F}^n$.

ТЕОРЕМА 3.1. *Любое ненулевое конечномерное векторное пространство обладает базисом. При этом если система векторов*

(1) $a_1, \ldots, a_m$

порождает векторное пространство $\mathcal{V}$, то базис системы векторов (1) *является базисом пространства $\mathcal{V}$.*

Доказательство. Предположим, что пространство $\mathcal{V}$ порождается системой векторов (1), т. е. $V = L(a_1, \ldots, a_m)$; мы можем считать, что векторы системы (1) ненулевые. По теореме 5.1, система (1) обладает базисом. Пусть

(2) $b_1, \ldots, b_n$

— базис системы (1). Тогда система (2) также порождает пространство $\mathcal{V}$, т. е. $V = L(b_1, \ldots, b_n)$. Кроме того, система (2) линейно независима. Следовательно, система (2) — базис системы (1) — является базисом пространства $\mathcal{V}$. □

ТЕОРЕМА 3.2. *Пусть $\mathcal{V}$ — конечномерное ненулевое векторное пространство. Тогда число элементов одного базиса пространства $\mathcal{V}$ равно числу элементов любого другого базиса этого пространства.*

Доказательство. По теореме 3.1, пространство $\mathcal{V}$ обладает базисом. Пусть

(1) $b_1, \ldots, b_n$

— один базис пространства $\mathcal{V}$ и

(2) $c_1, \ldots, c_s$

— любой другой базис этого пространства. Тогда $V = L(b_1, \ldots, b_n) = L(c_1, \ldots, c_s)$. Поэтому системы векторов (1) и (2) эквивалентны. Кроме того, каждая из этих систем линейно независима. Следовательно, по теореме 5.1.2, $n = s$. □

СЛЕДСТВИЕ 3.3. *Если базис векторного пространства $\mathcal{V}$ состоит из n элементов, то при $k > n$ любая система k векторов пространства $\mathcal{V}$ линейно зависима.*

Доказательство. Если $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ — базис пространства $\mathcal{V}$ и $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ — любые векторы из V, то $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k \in L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$. По теореме 5.1, отсюда при $k > n$ следует, что система векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ линейно зависима. □

СЛЕДСТВИЕ 3.4. *Если базис векторного пространства $\mathcal{V}$ состоит из n векторов, то любая система n векторов, порождающая пространство $\mathcal{V}$, является базисом этого пространства.*

ТЕОРЕМА 3.5. *Любое подпространство $\mathcal{U}$ конечномерного векторного пространства $\mathcal{V}$ является конечномерным. Если $\mathcal{V}$ обладает базисом, состоящим из n элементов, и $\mathcal{U}$ — ненулевое подпространство, то $\mathcal{U}$ обладает базисом и число элементов его базиса меньше или равно n.*

Доказательство. Пусть $\mathcal{V}$ — конечномерное векторное пространство и $\mathcal{U}$ — его подпространство. Если $\mathcal{U}$ — нулевое подпространство, то оно конечномерно. Предположим, что подпространство $\mathcal{U}$ ненулевое. Тогда $\mathcal{V}$ — ненулевое пространство и, по теореме 3.1, обладает базисом. Предположим, что базис пространства $\mathcal{V}$ состоит из n элементов. Тогда любая линейно независимая система векторов пространства $\mathcal{V}$ содержит не более n элементов.

Пусть $\boldsymbol{u}_1$ — ненулевой элемент пространства $\mathcal{U}$. Если $U \neq L(\boldsymbol{u}_1)$, то существует вектор $\boldsymbol{u}_2 \in U - L(\boldsymbol{u}_1)$, причем система векторов $\boldsymbol{u}_1$, $\boldsymbol{u}_2$ линейно независима. Если $U \neq L(\boldsymbol{u}_1, \boldsymbol{u}_2)$, то существует вектор $\boldsymbol{u}_3 \in U \setminus L(\boldsymbol{u}_1, \boldsymbol{u}_2)$, причем система векторов $\boldsymbol{u}_1$, $\boldsymbol{u}_2$, $\boldsymbol{u}_3$ линейно независима. Продолжая аналогичным образом, мы получим последовательность

(1) $\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \ldots$

линейно независимых элементов пространства $\mathcal{U}$. Эта последовательность содержит не более n элементов. Следовательно, существует такое натуральное число $m \leqslant n$ $(m > 0)$, что $U = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m)$. Таким образом, подпространство $\mathcal{U}$ конечномерно и система векторов $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m$ является его базисом. □

Дополнение независимой системы векторов до базиса. Возникает вопрос о возможности включения любой линейно независимой системы векторов в какой-нибудь базис.

ТЕОРЕМА 3.6. *Линейно независимую систему векторов ненулевого конечномерного векторного пространства $\mathcal{V}$,*

не являющуюся базисом пространства, можно дополнить до базиса пространства $\mathfrak{A}\mathcal{V}$.

Доказательство. Пусть

(1) $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$

— линейно независимая система, не являющаяся базисом пространства $\mathfrak{A}\mathcal{V}$. Пусть $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ — базис пространства $\mathfrak{A}\mathcal{V}$. Рассмотрим систему

(S) $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$.

По следствию 3.3, эта система линейно зависима. Поэтому хотя бы один из векторов $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ есть линейная комбинация предшествующих ему векторов в системе (S). Вычеркнем один из таких векторов из системы (S); получим систему

(S_1) $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m\ \boldsymbol{b}_1^{(1)}, \ldots, \boldsymbol{b}_{n-1}^{(1)}$,

эквивалентную системе S и поэтому порождающую пространство $\mathfrak{A}\mathcal{V}$. Если S_1 содержит более n элементов, то (по следствию 3.3) она линейно зависима и, значит, один из элементов $\boldsymbol{b}_1^{(1)}, \ldots, \boldsymbol{b}_{n-1}^{(1)}$ является линейной комбинацией предшествующих элементов. Вычеркнем этот элемент из S_1. Получающаяся при этом система S_2 эквивалентна системе S и поэтому порождает пространство $\mathfrak{A}\mathcal{V}$. Продолжая этот процесс, после m вычеркиваний мы получаем систему n векторов

(S_m) $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{b}_1^{(m)}, \ldots, \boldsymbol{b}_{n-m}^{(m)}$,

эквивалентную системе S и поэтому порождающую пространство $\mathfrak{A}\mathcal{V}$. По следствию 3.4, система S_m является базисом пространства $\mathfrak{A}\mathcal{V}$. Так как система S_m содержит исходную систему (1), то система S_m является искомым базисом пространства $\mathfrak{A}\mathcal{V}$. □

ТЕОРЕМА 3.7. *Если* $\mathcal{U}$ *— подпространство конечномерного векторного пространства* $\mathfrak{A}\mathcal{V}$, *то существует такое подпространство* $\mathcal{W}$ *пространства* $\mathfrak{A}\mathcal{V}$, *что*

(1) $\mathfrak{A}\mathcal{V} = \mathcal{U} \oplus \mathcal{W}$.

Доказательство. Равенство (1) верно, если $\mathcal{U}$ — тривиальное подпространство, т. е. нулевое или совпадающее с $\mathfrak{A}\mathcal{V}$. Предположим, что $\mathcal{U}$ — нетривиальное подпространство и

(2) $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$

— его базис. По теореме 3.6, систему (2) можно дополнить до базиса пространства $\mathcal{V}$, т. е. существуют такие векторы $a_{m+1}, \ldots, a_n$, что система

(3) $a_1, \ldots, a_m, a_{m+1}, \ldots, a_n$

является базисом пространства $\mathcal{V}$. Тогда

(4) $V = U + W$,

где $W = L(a_{m+1}, \ldots, a_n)$. Докажем, что

(5) $U \cap W = \{0\}$.

Действительно, если $c \in U \cap W$, то

$$c = \alpha_1 a_1 + \ldots + \alpha_m a_m \in U, \quad c = \alpha_{m+1} a_{m+1} + \ldots + \alpha_n a_n \in W$$

и поэтому

$$\alpha_1 a_1 + \ldots + \alpha_m a_m + (-\alpha_{m+1}) a_{m+1} + \ldots + (-\alpha_n) a_n = 0.$$

В силу линейной независимости системы (3) следует равенство нулю всех коэффициентов, в частности $\alpha_1 = 0, \ldots, \alpha_m = 0$. Следовательно, $c = 0$, т. е. выполняется (5).

На основании (4) и (5) заключаем, что при $\mathcal{W} = \mathcal{L}(a_{m+1}, \ldots, a_n)$ имеет место равенство (1). □

СЛЕДСТВИЕ 3.8. Если система (3) есть базис пространства $\mathcal{V}$, то

$$\mathcal{V} = \mathcal{L}(a_1, \ldots, a_m) \oplus \mathcal{L}(a_{m+1}, \ldots, a_n).$$

Размерность векторного пространства. Одним из самых важных инвариантов векторного пространства является его размерность.

ОПРЕДЕЛЕНИЕ. *Размерностью ненулевого конечномерного векторного пространства* называется число векторов какого-либо базиса пространства. Размерность нулевого векторного пространства считается равной нулю. Размерность векторного пространства обозначается через $\dim \mathcal{V}$.

Пример. Пусть $\mathcal{F}^n$ — арифметическое векторное пространство над полем $\mathcal{F}$. Векторы $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 0, 1)$ образуют базис пространства. Следовательно, $\dim \mathcal{F}^n = n$.

Рассмотрим некоторые свойства размерности.

СВОЙСТВО 3.1. Если $\mathcal{V}$ — конечномерное векторное пространство и $\dim \mathcal{V} = n$, то при $k > n$ любая система k векторов пространства $\mathcal{V}$ линейно зависима.

Доказательство. Если $n = 0$, то $\mathcal{V}$ — нулевое пространство и свойство 3.1 выполняется. Если же

$\dim \mathcal{V} = n > 0$, то базис пространства $\mathcal{V}$ состоит из n векторов. По следствию 3.3, отсюда следует, что при $k > n$ всякая система k векторов пространства $\mathcal{V}$ линейно зависима. □

СЛЕДСТВИЕ 3.9. *Если* $\dim \mathcal{V} = n$ *и система векторов* $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ *пространства* $\mathcal{V}$ *линейно независима, то* $m \leqslant n$.

СВОЙСТВО 3.2. *Если* $\mathcal{U}$ *— подпространство конечномерного векторного пространства* $\mathcal{V}$, *то*

(1) $\dim \mathcal{U} \leqslant \dim \mathcal{V}$.

Доказательство. Неравенство (1), очевидно, верно, если $\mathcal{U}$ есть нулевое подпространство. Если же подпространство $\mathcal{U}$ ненулевое, то (по теореме 3.5) оно конечномерно и (по теореме 3.1) обладает базисом. Пусть $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ — базис пространства $\mathcal{U}$. Тогда $\dim \mathcal{U} = m$. В пространстве $\mathcal{V}$ система векторов $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ линейно независима. Поэтому, по следствию 3.9, $m \leqslant n$. □

СВОЙСТВО 3.3. *Если* $\mathcal{U}$ *— подпространство конечномерного векторного пространства и* $\dim \mathcal{U} = \dim \mathcal{V}$, *то* $\mathcal{U} = \mathcal{V}$

Доказательство. Если подпространство $\mathcal{U}$ нулевое, то $\dim \mathcal{U} = 0$. Тогда в силу условия $\dim \mathcal{V} = 0$. Поэтому $\mathcal{V}$ — также нулевое векторное пространство. Следовательно, $\mathcal{U} = \mathcal{V}$.

Предположим, что $\mathcal{U}$ — ненулевое подпространство. Тогда оно, так же как и $\mathcal{V}$, конечномерно и, по теореме 3.1, обладает базисом. Пусть $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ — его базис. Тогда $\dim \mathcal{U} = n$ и, по условию, $\dim \mathcal{V} = n$. Поэтому система $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ является также базисом пространства $\mathcal{V}$. Следовательно, $\mathcal{U} = \mathcal{V}$. □

СВОЙСТВО 3.4. *Если конечномерное векторное пространство* $\mathcal{V}$ *есть прямая сумма подпространств* $\mathcal{U}$ *и* $\mathcal{L}$, *то*

(1) $\dim \mathcal{V} = \dim \mathcal{U} + \dim \mathcal{L}$.

Доказательство. По условию, $\mathcal{V} = \mathcal{U} \oplus \mathcal{L}$ и, значит,

(2) $U \cap L = \{0\}$,

(3) $V = U + L$.

Если $\mathcal{U}$ или $\mathcal{L}$ — нулевые подпространства, то равенство (1), очевидно, верно.

Предположим, что $\mathcal{U}$ и $\mathcal{L}$ — ненулевые подпространства. Пусть

(4) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$,

(5) $\boldsymbol{b}_{m+1}, \ldots, \boldsymbol{b}_{m+s}$

— базисы пространств $\mathcal{U}$ и $\mathcal{L}$ соответственно. Докажем, что система

(6) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m, \boldsymbol{b}_{m+1}, \ldots, \boldsymbol{b}_{m+s}$

является базисом пространства $\mathcal{V}$. Ввиду (2)

(7) $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m) \cap L(\boldsymbol{b}_{m+1}, \ldots, \boldsymbol{b}_{m+s}) = \{\mathbf{0}\}$.

Система (6) линейно независима. Действительно, для любых скаляров $\lambda_1, \ldots, \lambda_{m+s}$ из равенства

$$\lambda_1 \boldsymbol{b}_1 + \ldots + \lambda_m \boldsymbol{b}_m + \lambda_{m+1} \boldsymbol{b}_{m+1} + \ldots + \lambda_{m+s} \boldsymbol{b}_{m+s} = \mathbf{0}$$

в силу (7) следуют равенства

(8) $\lambda_1 \boldsymbol{b}_1 + \ldots + \lambda_m \boldsymbol{b}_m = \mathbf{0}$, $\lambda_{m+1} \boldsymbol{b}_{m+1} + \ldots + \lambda_{m+s} \boldsymbol{b}_{m+s} = \mathbf{0}$,

а так как системы (4) и (5) линейно независимы, из (8) следует, что $\lambda_1 = 0, \ldots, \lambda_m = 0, \ldots, \lambda_{m+s} = 0$. Далее, в силу (3)

$$V = U + L = L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m) + L(\boldsymbol{b}_{m+1}, \ldots, \boldsymbol{b}_{m+s}) = L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m, \boldsymbol{b}_{m+1}, \ldots, \boldsymbol{b}_{m+s}),$$

т. е. система (6) порождает пространство $\mathcal{V}$. Итак, доказано, что система (6) есть базис пространства $\mathcal{V}$. Следовательно, $\dim \mathcal{V} = m + s = \dim \mathcal{U} + \dim \mathcal{L}$. □

Теорема 3.10. *Если векторное пространство $\mathcal{V}$ есть сумма конечномерных подпространств $\mathcal{U}$ и $\mathcal{L}$, то*

(1) $\dim (\mathcal{U} + \mathcal{L}) + \dim (\mathcal{U} \cap \mathcal{L}) = \dim \mathcal{U} + \dim \mathcal{L}$.

Доказательство. Предположим, что

(2) $\mathcal{V} = \mathcal{U} + \mathcal{L}$.

Если $U \cap L = \{\mathbf{0}\}$, то сумма (2) прямая; следовательно, по свойству 3.4, теорема верна. □

Предположим, что $U \cap L \neq \emptyset$. Тогда пространство $\mathcal{U} \cap \mathcal{L}$, так же как и $\mathcal{U}$, конечномерно. Пусть

(2) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_s$

— базис пространства $\mathcal{U} \cap \mathcal{L}$. Дополним его до базисов пространств $\mathcal{U}$ и $\mathcal{L}$. Пусть

(3) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_s, \boldsymbol{b}_{s+1}, \ldots, \boldsymbol{b}_m$

— базис пространства $\mathcal{U}$ и

(4) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_s, \boldsymbol{b}_{m+1}, \ldots, \boldsymbol{b}_{m+k}$

— базис пространства $\mathscr{L}$. Тогда

(5) $\dim(\mathscr{U} \cap \mathscr{L}) = s$, $\dim \mathscr{U} = m$, $\dim \mathscr{L} = s + k$

и

(6) $U = L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m)$, $L = L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_s, \boldsymbol{b}_{m+1}, \ldots, \boldsymbol{b}_{m+k})$.

На основании (4) и (6) заключаем, что

$$V = U + L = L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m, \boldsymbol{b}_{m+1} \ldots, \boldsymbol{b}_{m+k}),$$

т. е. система

(7) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m, \boldsymbol{b}_{m+1}, \ldots, \boldsymbol{b}_{m+k}$

порождает пространство $\mathscr{V}$.

Покажем, что система (7) линейно независима. Предположим, что

(8) $\lambda_1 \boldsymbol{b}_1 + \ldots + \lambda_s \boldsymbol{b}_s + \ldots + \lambda_m \boldsymbol{b}_m + \lambda_{m+1} \boldsymbol{b}_{m+1} + \ldots + \lambda_{m+k} \boldsymbol{b}_{m+k} = \boldsymbol{0}$.

На основании (6) и (8) заключаем, что

$$\lambda_{m+1} \boldsymbol{b}_{m+1} + \ldots + \lambda_{m+k} \boldsymbol{b}_{m+k} \in U \cap L$$

и, значит,

$$\lambda_{m+1} \boldsymbol{b}_{m+1} + \ldots + \lambda_{m+k} \boldsymbol{b}_{m+k} \in L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_s).$$

В силу линейной независимости системы (5) отсюда следует, что

(9) $\lambda_{m+1} = 0, \ldots, \lambda_{m+k} = 0$.

Из (8) и (9) следует равенство

$$\lambda_1 \boldsymbol{b}_1 + \ldots + \lambda_m \boldsymbol{b}_m = \boldsymbol{0}.$$

Ввиду линейной независимости системы (3) следуют равенства

$$\lambda_1 = 0, \ldots, \lambda_m = 0.$$

Итак, установлено, что система (7) линейно независима. Таким образом, система (7) есть базис пространства $\mathscr{V}$ и

(10) $\dim(\mathscr{U} + \mathscr{L}) = m + k$.

Ввиду (5) и (10)

$$\dim(\mathscr{U} + \mathscr{L}) + \dim(\mathscr{U} \cap \mathscr{L}) = m + k + s = \dim \mathscr{U} + \dim \mathscr{L}. \quad \square$$

Упражнения.

1. Покажите, что система векторов (α, β), (γ, δ) двумерного арифметического векторного пространства $\mathscr{V}$ тогда и только тогда является базисом пространства $\mathscr{V}$, когда $\alpha\delta - \beta\gamma \neq 0$.

2. Покажите, что система векторов (1, 1, 1), (0, 1, 1), (1, 0, 1) есть базис пространства $\mathscr{V} = \mathscr{F}^3$. Найдите координатные строки единичных векторов $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$ относительно этого базиса.

3. Покажите, что для любых скаляров α, β, γ система векторов $(1, \alpha, \beta)$, $(0, 1, \gamma)$, $(0, 0, 1)$ является базисом пространства $\mathscr{V} = \mathscr{F}^3$.

4. Пусть $\mathscr{F}$ — числовое поле. Каким условиям должны удовлетворять скаляры α, β, $\gamma \in F$, чтобы система векторов $(1, \alpha, \alpha^2)$, $(1, \beta, \beta^2)$, $(1, \gamma, \gamma^2)$ была базисом пространства $\mathscr{F}^3$?

5. Каким условиям должен удовлетворять скаляр λ, чтобы система векторов $(\lambda, 1, 0)$, $(1, \lambda, 1)$, $(0, 1, \lambda)$ была базисом пространства $\mathscr{C}^3$; пространства $\mathscr{Q}^3$?

6. Пусть векторное пространство $\mathscr{V}$ есть прямая сумма конечномерных подпространств $\mathscr{L}_1$ и $\mathscr{L}_2$. Покажите, что в результате приписывания базиса подпространства $\mathscr{L}_2$ к базису подпространства $\mathscr{L}_1$ получается базис пространства $\mathscr{V}$.

7. Пусть $\mathscr{F}$ — поле, состоящее из двух элементов. Сколько различных базисов имеет пространство $\mathscr{F}^3$?

8. Пусть $\mathscr{V}$ есть n-мерное векторное пространство. Докажите, что система векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ есть базис пространства $\mathscr{V}$ тогда и только тогда, когда $\mathscr{V} = \mathscr{L}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$.

9. Пусть $\mathscr{V} = \mathscr{F}^{m \times n}$ — векторное пространство $m \times n$-матриц над полем $\mathscr{F}$. Найдите его базис и размерность.

10. Пусть $\mathscr{V}$ — ненулевое конечномерное векторное пространство. Докажите, что размерность подпространства $\mathscr{L}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$ натянутого на данные векторы $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ пространства $\mathscr{V}$, равна рангу матрицы, составленной из координатных строк данных векторов в каком-нибудь базисе.

11. Докажите, что система $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ ненулевых векторов n-мерного векторного пространства $\mathscr{V}$ тогда и только тогда является базисом пространства $\mathscr{V}$, когда $\boldsymbol{a}_k \notin L(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{k-1})$ для $k = 2, 3, \ldots, n$.

12. Пусть $\mathscr{F}$ — конечное поле, состоящее из p элементов, и $\mathscr{V} = \mathscr{F}^n$. Сколько различных базисов имеет векторное пространство $\mathscr{V}$?

13. Пусть $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ — базис векторного пространства $\mathscr{V}$ и k — целое положительное число, меньшее n. Докажите, что $\mathscr{V} = \mathscr{L}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k) \oplus \mathscr{L}(\boldsymbol{a}_{k+1}, \ldots, \boldsymbol{a}_n)$.

14. Пусть $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ — стандартный базис векторного пространства $\mathscr{V} = \mathscr{F}^n$. Покажите, что система векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ пространства $\mathscr{V}$ тогда и только тогда является базисом пространства $\mathscr{V}$, когда $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n \in L(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$.

15. Докажите, что если сумма размерностей двух подпространств n-мерного пространства больше n, то эти подпространства имеют общий ненулевой вектор.

16. Докажите, что векторное пространство $\mathscr{V}$ имеет только два подпространства тогда и только тогда, когда пространство $\mathscr{V}$ одномерное.

17. Докажите, что двумерное векторное пространство над числовым полем имеет бесконечное множество различных одномерных подпространств.

18. Пусть $\mathscr{V} = \mathscr{U} \oplus \mathscr{L}$, где $\mathscr{V}$ — трехмерное пространство и $\mathscr{U}$, $\mathscr{L}$ — ненулевые подпространства, отличные от $\mathscr{V}$. Покажите, что одно из подпространств $\mathscr{U}$, $\mathscr{L}$ есть одномерное, а другое — двумерное.

19. Пусть $\mathscr{L}$ и $\mathscr{U}$ — различные одномерные подпространства двумерного векторного пространства $\mathscr{V}$. Докажите, что $\mathscr{V} = \mathscr{L} \oplus \mathscr{U}$.

20. Пусть $\mathscr{L}$ и $\mathscr{U}$ — различные двумерные подпространства трехмерного векторного пространства $\mathscr{V}$. Докажите, что $\mathscr{V}=\mathscr{L}+\mathscr{U}$ и $\mathscr{L}\cap\mathscr{U}$ есть одномерное подпространство.

21. Пусть $\mathscr{L}$ и $\mathscr{U}$ — подпространства n-мерного векторного пространства $\mathscr{V}$, имеющие размерности k и s соответственно. Докажите, что:

(a) если $L\cap V=\{0\}$ и $k+s=n$, то $\mathscr{V}=\mathscr{L}\oplus\mathscr{U}$;

(b) если $\mathscr{V}=\mathscr{L}+\mathscr{U}$ и $k+s=n$, то $\mathscr{V}=\mathscr{L}\oplus\mathscr{U}$.

22. Докажите, что n-мерное векторное пространство при $n>1$ можно представить в виде прямой суммы n одномерных подпространств.

23. Пусть $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ — базис векторного пространства $\mathscr{V}$. Покажите, что $\mathscr{V}=\mathscr{L}(\boldsymbol{b}_1)\oplus\ldots\oplus\mathscr{L}(\boldsymbol{b}_n)$.

24. Пусть $\mathscr{V}=\mathscr{L}_1+\mathscr{L}_2+\mathscr{L}_3$, где $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$ — подпространства n-мерного пространства $\mathscr{V}$, имеющие размерности r, s, t соответственно. Докажите, что $\mathscr{V}=\mathscr{L}_1\oplus\mathscr{L}_2\oplus\mathscr{L}_3$ тогда и только тогда, когда $r+s+t=n$.

§ 4. ИЗОМОРФИЗМЫ ВЕКТОРНЫХ ПРОСТРАНСТВ

Координатная строка вектора относительно данного базиса. Пусть ${}^{\mathscr{F}}\mathscr{V}$ — векторное пространство над полем $\mathscr{F}$

ТЕОРЕМА 4.1. *Пусть*

(1) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$

— базис векторного пространства ${}^{\mathscr{F}}\mathscr{V}$. *Для каждого вектора* $\boldsymbol{a}$ *из* V *существует в* F^n *единственный арифметический вектор* $(\alpha_1, \ldots, \alpha_n)$ *такой, что*

(2) $\boldsymbol{a}=\alpha_1\boldsymbol{b}_1+\ldots+\alpha_n\boldsymbol{b}_n$.

Доказательство. Так как система векторов (1) порождает пространство ${}^{\mathscr{F}}\mathscr{V}$, то любой вектор $\boldsymbol{a}$ из V можно представить в виде линейной комбинации векторов системы (1) — в виде (2). Такое представление единственно. В самом деле, если

$$\boldsymbol{a}=\beta_1\boldsymbol{b}_1+\ldots+\beta_n\boldsymbol{b}_n \quad (\beta_i\in F)$$

— любое представление $\boldsymbol{a}$ в виде линейной комбинации векторов системы (1), то

$$(\alpha_1-\beta_1)\boldsymbol{b}_1+\ldots+(\alpha_n-\beta_n)\boldsymbol{b}_n=\boldsymbol{0}.$$

В силу линейной независимости системы (1) отсюда вытекают равенства

$$\alpha_1-\beta_1=0, \ldots, \alpha_n-\beta_n=0 \text{ и } \alpha_1=\beta_1, \ldots, \alpha_n=\beta_n.$$

Следовательно, вектор $\boldsymbol{a}$ обладает единственным представлением в виде линейной комбинации векторов базиса (1). □

ОПРЕДЕЛЕНИЕ. Пусть $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ — фиксированный базис пространства $\mathscr{V}$, $\boldsymbol{a} \in V$ и $\boldsymbol{a} = \alpha_1 \boldsymbol{b}_1 + \ldots + \alpha_n \boldsymbol{b}_n$, где $\alpha_1, \ldots, \alpha_n \in F$. Коэффициенты $\alpha_1, \ldots, \alpha_n$ называются *координатами вектора* $\boldsymbol{a}$ *относительно фиксированного базиса.* Вектор $(\alpha_1, \ldots, \alpha_n) \in F^n$ называется *координатной строкой,* а вектор $\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$ — *координатным столбцом вектора* $\boldsymbol{a}$ относительно фиксированного базиса.

Изоморфизм векторных пространств. *Отображением векторного пространства* $\mathscr{U}$ *в* $\mathscr{V}$ называется отображение множества U в V.

ОПРЕДЕЛЕНИЕ. Отображение векторного пространства $\mathscr{U}$ на векторное пространство $\mathscr{V}$ называется *изоморфизмом,* если оно инъективно и удовлетворяет условиям линейности:

$$f(\boldsymbol{a}+\boldsymbol{b}) = f(\boldsymbol{a}) + f(\boldsymbol{b}), \quad f(\lambda \boldsymbol{a}) = \lambda f(\boldsymbol{a})$$

для любых $\boldsymbol{a}$, $\boldsymbol{b}$ из U и любого λ из F. Векторные пространства $\mathscr{U}$ и $\mathscr{V}$ называются *изоморфными,* если существует изоморфизм $\mathscr{U}$ на $\mathscr{V}$.

Другими словами, отображение f векторного пространства $\mathscr{U}$ и $\mathscr{V}$ называется изоморфизмом, если оно инъективно и сохраняет главные операции пространства $\mathscr{U}$, рассматриваемого как алгебра.

Запись $\mathscr{U} \cong \mathscr{V}$ означает, что векторные пространства $\mathscr{U}$ и $\mathscr{V}$ изоморфны.

ТЕОРЕМА 4.2. *Пусть* $\mathscr{V}$ *— n-мерное векторное пространство над полем* $\mathscr{F}$ *и* $n > 0$. *Тогда пространство* $\mathscr{V}$ *изоморфно арифметическому векторному пространству* $\mathscr{F}^n$.

Доказательство. Пусть

(1) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$

— фиксированный базис пространства $\mathscr{V}$. Пусть

$$f: V \to F^n$$

— отображение, ставящее в соответствие каждому вектору $\boldsymbol{a}$ из V его координатную строку $f(\boldsymbol{a})$ относительно фиксированного базиса. Пусть $(\gamma_1, \ldots, \gamma_n)$ — произвольный вектор из F^n. Вектор $\gamma_1 \boldsymbol{b}_1 + \ldots + \gamma_n \boldsymbol{b}_n$ является его прообразом при отображении f. Следовательно, f есть отображение V на F^n. Кроме того, по теореме 4.1, для любых $\boldsymbol{a}$, $\boldsymbol{b}$ из V, если $f(\boldsymbol{a}) = f(\boldsymbol{b})$, то $\boldsymbol{a} = \boldsymbol{b}$. Следовательно, f является

инъективным отображением V на F^n. Отображение f удовлетворяет условиям линейности. В самом деле, если $\boldsymbol{a}=\alpha_1\boldsymbol{b}_1+\ldots+\alpha_n\boldsymbol{b}_n$, $\boldsymbol{b}=\beta_1\boldsymbol{b}_1+\ldots+\beta_n\boldsymbol{b}_n$, то

$$\boldsymbol{a}+\boldsymbol{b}=(\alpha_1+\beta_1)\boldsymbol{b}_1+\ldots+(\alpha_n+\beta_n)\boldsymbol{b}_n$$

и

$$f(\boldsymbol{a}+\boldsymbol{b})=(\alpha_1+\beta_1,\ \ldots,\ \alpha_n+\beta_n)=$$
$$=(\alpha_1,\ \ldots,\ \alpha_n)+(\beta_1,\ \ldots,\ \beta_n)=f(\boldsymbol{a})+f(\boldsymbol{b}).$$

Далее, если $\lambda\in F$, то $\lambda\boldsymbol{a}=(\lambda\alpha_1)\boldsymbol{b}_1+\ldots+(\lambda\alpha_n)\boldsymbol{b}_n$ и

$$f(\lambda\boldsymbol{a})=(\lambda\alpha_1,\ \ldots,\ \lambda\alpha_n)=\lambda(\alpha_1,\ \ldots,\ \alpha_n)=\lambda f(\boldsymbol{a}).$$

Итак, f удовлетворяет условиям линейности. Следовательно, отображение f является изоморфизмом пространства $\mathscr{V}$ на пространство $\mathscr{F}^n$. □

ТЕОРЕМА 4.3. *Пусть $\mathscr{V}$ есть n-мерное векторное пространство над полем $\mathscr{F}$ с фиксированным базисом и $n>0$. Отображение $f: V\to F^n$, ставящее в соответствие каждому вектору $\boldsymbol{a}$ из V его координатную строку относительно фиксированного базиса, является изоморфизмом пространства $\mathscr{V}$ на арифметическое векторное пространство $\mathscr{F}^n$.*

Эта теорема непосредственно следует из теоремы 4.2 и ее доказательства.

СЛЕДСТВИЕ 4.4. *Пусть $\mathscr{V}$ — ненулевое конечномерное векторное пространство с фиксированным базисом. Система векторов пространства $\mathscr{V}$ линейно зависима тогда и только тогда, когда линейно зависима система координатных строк (столбцов) этих векторов относительно фиксированного базиса.*

СЛЕДСТВИЕ 4.5. *Пусть $\mathscr{V}$ — конечномерное векторное пространство с фиксированным базисом. Ранг системы векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ пространства $\mathscr{V}$ равен рангу матрицы, составленной из координатных строк (столбцов) этих векторов относительно фиксированного базиса.*

Рассмотрим свойства изоморфизмов векторных пространств.

СВОЙСТВО 4.1. *Если f — изоморфизм векторного пространства $\mathscr{U}$ на $\mathscr{V}$ и g — изоморфизм пространства $\mathscr{V}$ на $\mathscr{W}$, то их композиция является изоморфизмом $\mathscr{U}$ на $\mathscr{W}$.*

Доказательство. Из условия следует, что gf есть инъективное отображение U на W. Отображение gf удовлетворяет условиям линейности. В самом деле, в силу линейности отображений g и f для любых $\boldsymbol{a}$, $\boldsymbol{b}$ из V и

любого λ из F имеем:

$$(gf)(\boldsymbol{a}+\boldsymbol{b}) = g(f(\boldsymbol{a}+\boldsymbol{b})) = g(f(\boldsymbol{a})+f(\boldsymbol{b})) = \\ = g(f(\boldsymbol{a}))+g(f(\boldsymbol{b})) = (gf)(\boldsymbol{a})+(gf)(\boldsymbol{b}),$$

$$(gf)(\lambda\boldsymbol{a}) = g(f(\lambda\boldsymbol{a})) = g(\lambda f(\boldsymbol{a})) = \lambda g(f(\boldsymbol{a})) = \lambda(gf)(\boldsymbol{a}).$$

Следовательно, gf является изоморфизмом $\mathcal{U}$ на $\mathcal{V}$. □

СВОЙСТВО 4.2. *Если f — изоморфизм векторного пространства $\mathcal{U}$ на векторное пространство $\mathcal{V}$, то f^{-1} является изоморфизмом $\mathcal{V}$ на $\mathcal{U}$.*

Доказательство. Так как f — инъективное отображение U на V, то f^{-1} является инъективным отображением V на U. Кроме того, f^{-1} удовлетворяет условиям линейности. В самом деле, в силу линейности отображения f для любого $\boldsymbol{a}$ из V и любого λ из F имеем:

$$f(f^{-1}(\boldsymbol{a})+f^{-1}(\boldsymbol{b})) = f(f^{-1}(\boldsymbol{a}))+f(f^{-1}(\boldsymbol{b})) = \boldsymbol{a}+\boldsymbol{b},$$

$$f(\lambda f^{-1}(\boldsymbol{a})) = \lambda f(f^{-1}(\boldsymbol{a})) = \lambda\boldsymbol{a},$$

откуда

$$f^{-1}(\boldsymbol{a}+\boldsymbol{b}) = f^{-1}(\boldsymbol{a})+f^{-1}(\boldsymbol{b}), \quad f^{-1}(\lambda\boldsymbol{a}) = \lambda f^{-1}(\boldsymbol{a}).$$

Следовательно, f^{-1} является изоморфизмом $\mathcal{V}$ на $\mathcal{U}$. □

СВОЙСТВО 4.3. *Отношение изоморфизма на каком-либо множестве векторных пространств над полем $\mathcal{F}$ является отношением эквивалентности.*

Доказательство. Отношение изоморфизма, очевидно, рефлексивно. В силу свойства 4.1 оно транзитивно. В силу свойства 4.2 отношение изоморфизма симметрично. Следовательно, отношение изоморфизма является отношением эквивалентности.

СВОЙСТВО 4.4. *Пусть*

(1) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$

— базис векторного пространства $\mathcal{U}$ и f — изоморфизм $\mathcal{U}$ на векторное пространство $\mathcal{V}$. Тогда система векторов $f(\boldsymbol{b}_1), \ldots, f(\boldsymbol{b}_n)$ является базисом пространства $\mathcal{V}$.

Доказательство. Система векторов

(2) $f(\boldsymbol{b}_1), \ldots, f(\boldsymbol{b}_n)$

линейно независима. В самом деле, в силу линейности отображения f для любых $\lambda_1, \ldots, \lambda_n$ из F равенство

$$\lambda_1 f(\boldsymbol{b}_1)+\ldots+\lambda_n f(\boldsymbol{b}_n) = 0',$$

где $0'$ — нулевой вектор пространства $\mathcal{V}$, влечет равенства

$$f(\lambda_1 \boldsymbol{b}_1 + \ldots + \lambda_n \boldsymbol{b}_n) = 0' = f(\boldsymbol{0}),$$

В силу инъективности отображения f из последнего равенства следует, что

$$(3)\ \lambda_1 \boldsymbol{b}_1 + \ldots + \lambda_n \boldsymbol{b}_n = \boldsymbol{0}.$$

Так как система (1) линейно независима, то из (3) следуют равенства $\lambda_1 = 0, \ldots, \lambda_n = 0$.

Кроме того, система (1) порождает пространство $\mathcal{V}$. В самом деле, если $\boldsymbol{c} \in V$, то вектор $f^{-1}(\boldsymbol{c}) \in U$ и его можно представить в виде

$$(4)\ f^{-1}(\boldsymbol{c}) = \gamma_1 \boldsymbol{b}_1 + \ldots + \gamma_n \boldsymbol{b}_n \quad (\gamma_1, \ldots, \gamma_n \in F),$$

так как система (1) есть базис пространства $\mathcal{U}$. В силу линейности отображения f из (4) следуют равенства

$$\boldsymbol{c} = f(\gamma_1 \boldsymbol{b}_1 + \ldots + \gamma_n \boldsymbol{b}_n) = \gamma_1 f(\boldsymbol{b}_1) + \ldots + \gamma_n f(\boldsymbol{b}_n).$$

Следовательно, система (2) порождает пространство $\mathcal{V}$ и является его базисом.

ТЕОРЕМА 4.6. *Пусть $\mathcal{U}$ и $\mathcal{V}$ — конечномерные векторные пространства над полем $\mathcal{F}$. Пространства $\mathcal{U}$ и $\mathcal{V}$ изоморфны тогда и только тогда, когда равны их размерности.*

Доказательство. Предположим, что $\mathcal{U} \cong \mathcal{V}$. Если одно из этих пространств нулевое, то нулевым будет и другое, т. е. $\dim \mathcal{U} = \dim \mathcal{V} = 0$. Предположим теперь, что $\mathcal{U}$ и $\mathcal{V}$ — ненулевые пространства. Тогда, по свойству 4.4, число элементов базиса пространства $\mathcal{U}$ равно числу элементов базиса пространства $\mathcal{V}$ (равны размерности этих пространств).

Теперь предположим, что $\dim \mathcal{U} = \dim \mathcal{V} = n$. Если $n = 0$, то пространства $\mathcal{U}$, $\mathcal{V}$ — нулевые и поэтому изоморфны. Если же $n > 0$, то, по теореме 4.2, $\mathcal{U} \cong \mathcal{F}^n$ и $\mathcal{F}^n \cong \mathcal{V}$. В силу транзитивности изоморфизма отсюда следует, что векторные пространства $\mathcal{U}$ и $\mathcal{V}$ изоморфны. □

Упражнения

1. Пусть $\mathcal{U}$ и $\mathcal{V}$ — конечномерные векторные пространства над полем $\mathcal{F}$. Покажите, что существует мономорфизм пространства $\mathcal{U}$ в $\mathcal{V}$ тогда и только тогда, когда $\dim \mathcal{U} \leqslant \dim \mathcal{V}$.

2. Пусть $\mathcal{U}$ и $\mathcal{V}$ — конечномерные векторные пространства над полем $\mathcal{F}$. Докажите, что существует эпиморфизм пространства $\mathcal{U}$ на $\mathcal{V}$ тогда и только тогда, когда $\dim \mathcal{U} \geqslant \dim \mathcal{V}$.

3. Пусть $\mathcal{U}$ и $\mathcal{V}$ — n-мерные векторные пространства над конечным полем $\mathcal{F}$, состоящим из m элементов. Сколько существует изоморфизмов пространства $\mathcal{U}$ на пространство $\mathcal{V}$?

4. Приведите пример векторного пространства над полем $\mathcal{F}$, не являющегося конечномерным.

5. Пусть $\mathcal{W}$ — векторное пространство над полем $\mathcal{F}$, не являющееся конечномерным. Покажите, что существует мономорфизм любого конечномерного векторного пространства $\mathcal{V}$ над полем $\mathcal{F}$ в пространство $\mathcal{W}$.

§ 5. ВЕКТОРНЫЕ ПРОСТРАНСТВА СО СКАЛЯРНЫМ УМНОЖЕНИЕМ

Скалярное умножение в векторном пространстве. Пусть $^{\circ}\mathcal{V}$ — векторное пространство над полем $\mathcal{F}$, V — основное множество пространства $^{\circ}\mathcal{V}$ и F — основное множество поля $\mathcal{F}$, которое называется *множеством скаляров*.

ОПРЕДЕЛЕНИЕ. *Скалярным умножением в пространстве* $^{\circ}\mathcal{V}$ называется отображение $V \times V \to F$, ставящее в соответствие каждой паре элементов $\boldsymbol{a}$, $\boldsymbol{b}$ из V скаляр, обозначаемый через $\boldsymbol{a} \cdot \boldsymbol{b}$, и удовлетворяющее условиям:

(1) $\boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{b} \cdot \boldsymbol{a}$ для любых $\boldsymbol{a}$, $\boldsymbol{b}$ из V;

(2) $(\alpha \boldsymbol{a} + \beta \boldsymbol{b}) \cdot \boldsymbol{c} = \alpha (\boldsymbol{a} \cdot \boldsymbol{c}) + \beta (\boldsymbol{b} \cdot \boldsymbol{c})$ для любых $\boldsymbol{a}$, $\boldsymbol{b}$ из V и α, β из F.

Скаляр $\boldsymbol{a} \cdot \boldsymbol{b}$ называется *скалярным произведением* векторов $\boldsymbol{a}$ и $\boldsymbol{b}$.

ОПРЕДЕЛЕНИЕ. Скалярное умножение в пространстве $^{\circ}\mathcal{V}$ называется *невырожденным*, если $\boldsymbol{a} \cdot \boldsymbol{a} \neq 0$ для любого ненулевого вектора $\boldsymbol{a}$ из V. Скалярное умножение в пространстве $^{\circ}\mathcal{V}$ называется *нулевым, если* $\boldsymbol{a} \cdot \boldsymbol{b} = 0$ для любых $\boldsymbol{a}$, $\boldsymbol{b}$ из V.

ПРЕДЛОЖЕНИЕ 5.1. *Если* $^{\circ}\mathcal{V}$ *— векторное пространство со скалярным умножением, то* $\boldsymbol{a} \cdot \boldsymbol{0} = 0$ для любого $\boldsymbol{a}$ из V.

Доказательство. В силу условия (2) $\boldsymbol{a} \cdot \boldsymbol{0} = \boldsymbol{a} \cdot (\boldsymbol{0} + \boldsymbol{0}) = \boldsymbol{a} \cdot \boldsymbol{0} + \boldsymbol{a} \cdot \boldsymbol{0}$ и, значит, $\boldsymbol{a} \cdot \boldsymbol{0} + \boldsymbol{a} \cdot \boldsymbol{0} = \boldsymbol{a} \cdot \boldsymbol{0} + 0$. В силу правила сокращения отсюда следует, что $\boldsymbol{a} \cdot \boldsymbol{0} = 0 \cdot$ □

Отметим, что в любом конечномерном ненулевом векторном пространстве скалярное умножение можно ввести различными способами.

Пусть $^{\circ}\mathcal{V}$ — векторное пространство со скалярным умножением

(3) $V \times V \to F$,

удовлетворяющим условиям (1), (2) определения. Если $\mathscr{L}$ — подпространство пространства $\mathscr{V}$, то отображение (3) индуцирует отображение $L \times L \to F$, которое на L также удовлетворяет условиям (1), (2). Поэтому векторное пространство $\mathscr{L}$ также можно рассматривать как векторное пространство со скалярным умножением.

Ортогональная система векторов. Пусть $\mathscr{V}$ — векторное пространство (над полем $\mathscr{F}$) со скалярным умножением.

ОПРЕДЕЛЕНИЕ. Векторы $\boldsymbol{a}$, $\boldsymbol{b}$ из V называются *ортогональными* или *взаимно ортогональными*, если их скалярное произведение равно нулю.

Запись $\boldsymbol{a} \perp \boldsymbol{b}$ означает, что $\boldsymbol{a} \cdot \boldsymbol{b} = 0$.

ОПРЕДЕЛЕНИЕ. Система векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ пространства $\mathscr{V}$ называется *ортогональной*, если взаимно ортогональны любые два вектора системы. Система, состоящая из одного ненулевого вектора, считается ортогональной. Ортогональная система векторов, являющаяся базисом пространства $\mathscr{V}$, называется *ортогональным базисом пространства*.

ТЕОРЕМА 5.2. *Пусть $\mathscr{V}$ — векторное пространство с невырожденным скалярным умножением. Ортогональная система ненулевых векторов пространства $\mathscr{V}$ линейно независима.*

Доказательство. Пусть

(1) $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$

— ортогональная система ненулевых векторов пространства $\mathscr{V}$. Покажем, что для любых скаляров $\lambda_1, \ldots, \lambda_m$ (из F) из равенства

(2) $\lambda_1 \boldsymbol{a}_1 + \ldots + \lambda_m \boldsymbol{a}_m = \boldsymbol{0}$

следует равенство нулю всех коэффициентов. Умножив обе части равенства (2) на вектор $\boldsymbol{a}_k$, $k \in \{1, \ldots, m\}$, получим

$$\lambda_1 (\boldsymbol{a}_1 \boldsymbol{a}_k) + \ldots + \lambda_k (\boldsymbol{a}_k \boldsymbol{a}_k) + \ldots + \lambda_m (\boldsymbol{a}_m \boldsymbol{a}_k) = 0.$$

В силу ортогональности системы (1) отсюда получаем равенство

(3) $\lambda_k (\boldsymbol{a}_k \cdot \boldsymbol{a}_k) = 0.$

Так как, по условию, $\boldsymbol{a}_k \neq 0$ и скалярное умножение в $\mathscr{V}$ невырожденное, то $\boldsymbol{a}_k \boldsymbol{a}_k \neq 0$. Поэтому из (3) вытекают равенства

$\lambda_k = 0$ для $k = 1, \ldots, m$.

Следовательно, система векторов (1) линейно независима. □

СЛЕДСТВИЕ 5.3. *Если $\mathcal{V}$ — ненулевое n-мерное векторное пространство с невырожденным скалярным умножением, то любая ортогональная система n ненулевых векторов пространства является ортогональным базисом пространства $\mathcal{V}$.*

Процесс ортогонализации. Сущность процесса ортогонализации дана при доказательстве теоремы.

ТЕОРЕМА 5.4. *Пусть $\mathcal{V}$ — конечномерное векторное пространство с невырожденным скалярным умножением. Ортогональную систему ненулевых векторов, не являющуюся базисом пространства, можно дополнить до ортогонального базиса пространства.*

Доказательство. Пусть $\dim \mathcal{V} = n > 1$ и

(1) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$

— ортогональная система ненулевых векторов пространства $\mathcal{V}$, не являющаяся базисом пространства, т. е. $m < n$. По теореме 3.6, систему (1) можно дополнить до базиса. Пусть

(2) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m, \boldsymbol{c}_{m+1}, \ldots, \boldsymbol{c}_n$

— базис пространства $\mathcal{V}$. Положим

(3) $\boldsymbol{b}_{m+1} = \boldsymbol{c}_{m+1} - \lambda_1 \boldsymbol{b}_1 - \ldots - \lambda_m \boldsymbol{b}_m$

и найдем, при каких значениях скаляров $\lambda_1, \ldots, \lambda_m$ вектор $\boldsymbol{b}_{m+1}$ ортогонален ко всем векторам исходной системы (1), т. е. удовлетворяет условиям

(4) $\boldsymbol{b}_{m+1}\boldsymbol{b}_i = 0 \quad (i = 1, \ldots, m)$.

В силу (3) и ортогональности системы (1) эти условия можно записать в виде

$$\boldsymbol{c}_{m+1}\boldsymbol{b}_i - \lambda_i (\boldsymbol{b}_i \boldsymbol{b}_i) = 0.$$

Так как $\boldsymbol{b}_i \neq 0$ и $\boldsymbol{b}_i \cdot \boldsymbol{b}_i \neq 0$, эти условия можно записать в виде

$$\lambda_i = \frac{\boldsymbol{c}_{m+1}\boldsymbol{b}_i}{\boldsymbol{b}_i \boldsymbol{b}_i} \quad (i = 1, \ldots, m).$$

При таком выборе коэффициентов λ_i в равенстве (3) вектор $\boldsymbol{b}_{m+1}$ удовлетворяет условиям (4), т. е. ортогонален к каждому вектору системы (1). Из (3) в силу линейной независимости системы $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m, \boldsymbol{c}_{m+1}$ следует, что $\boldsymbol{b}_{m+1} \neq 0$. Следовательно, $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m, \boldsymbol{b}_{m+1}$ есть ортогональная система ненулевых векторов. Если $m+1 < n$, то аналогич-

ным образом находится ненулевой вектор $\boldsymbol{b}_{m+2}$, ортогональный к векторам $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m, \boldsymbol{b}_{m+1}$. Продолжая этот процесс, называемый *процессом ортогонализации* системы (2), получим ортогональную систему $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m, \boldsymbol{b}_{m+1}, \ldots, \boldsymbol{b}_n$ ненулевых векторов пространства $\mathcal{V}$. По следствию 5.3, эта система есть ортогональный базис пространства $\mathcal{V}$ и, следовательно, является искомым дополнением исходной системы (1) до ортогонального базиса пространства $\mathcal{V}$. □

Легко видеть, что применение процесса ортогонализации к линейно зависимой системе ненулевых векторов приведет к системе, содержащей нулевой вектор.

СЛЕДСТВИЕ 5.5. *Любое конечномерное ненулевое векторное пространство с невырожденным скалярным умножением обладает ортогональным базисом.*

Доказательство. В самом деле, по теореме 3.1, ненулевое конечномерное пространство обладает базисом. Пусть

(1) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$

— базис пространства $\mathcal{V}$. Считая $\boldsymbol{b}_1$ исходной ортогональной системой и применяя к системе (1) процесс ортогонализации, получаем ортогональный базис пространства $\mathcal{V}$.

Ортогональное дополнение к подпространству. Пусть $\mathcal{V}$ — векторное пространство со скалярным умножением и $M \subset V$. Если вектор $\boldsymbol{a}$ из V ортогонален к каждому вектору из M, то это записывается в виде $\boldsymbol{a} \perp M$. Символом $M^\perp$ обозначается множество всех элементов пространства $\mathcal{V}$, ортогональных к M:

$$M^\perp = \{\boldsymbol{a} \in V \mid \boldsymbol{a} \perp M\}.$$

Легко проверить, что множество $M^\perp$ не пусто и замкнуто в $\mathcal{V}$, замкнуто относительно сложения и умножения на скаляры.

ОПРЕДЕЛЕНИЕ. Подпространство пространства $\mathcal{V}$ с основным множеством $M^\perp$ называется *ортогональным к множеству* M.

Если $\mathcal{L}$ — подпространство пространства $\mathcal{V}$, то символом $\mathcal{L}^\perp$ обозначается подпространство с основным множеством $L^\perp$.

ОПРЕДЕЛЕНИЕ. Подпространство $\mathcal{L}^\perp$ называется *ортогональным к* $\mathcal{L}$ *в пространстве* $\mathcal{V}$ или *ортогональным дополнением к* $\mathcal{L}$ *в пространстве* $\mathcal{V}$.

Пример. Пусть $\mathcal{V} = \mathcal{F}^n$ — арифметическое векторное пространство над полем $\mathcal{F}$ со стандартным скалярным

умножением. Пусть $M=\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m\} \subset F^n$ и

$$\boldsymbol{a}_1=(\alpha_{11}, \ldots, \alpha_{1n}), \ldots, \boldsymbol{a}_m=(\alpha_{m1}, \ldots, \alpha_{mn}) \quad (\alpha_{ik} \in F).$$

Рассмотрим однородную систему линейных уравнений

$$\begin{array}{l} \alpha_{11}x_1+\ldots+\alpha_{1n}x_n=0, \\ \cdots\cdots\cdots\cdots \\ \alpha_{m1}x_1+\ldots+\alpha_{mn}x_n=0 \end{array} \tag{1}$$

над полем $\mathscr{F}$. Легко видеть, что множество $M^\perp$ совпадает с множеством всех решений системы (1). Пусть $\mathscr{L}=\mathscr{L}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$ и $L=L(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)=L(M)$. Легко проверить, что каждый вектор, ортогональный к M, ортогонален к любой линейной комбинации векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$, т. е. $M^\perp \subset L^\perp$. Обратно: каждый вектор из $L^\perp$ ортогонален к M, т. е. $L^\perp \subset M^\perp$. Таким образом, $M^\perp=L^\perp$. Следовательно, пространство решений однородной системы линейных уравнений (1) совпадает с пространством $\mathscr{L}^\perp$.

ТЕОРЕМА 5.6. *Пусть $\mathscr{V}$ — векторное пространство со скалярным умножением и $\mathscr{L}$ — его конечномерное подпространство, в котором скалярный квадрат любого ненулевого вектора отличен от нуля. Тогда $\mathscr{V}=\mathscr{L} \oplus \mathscr{L}^\perp$.*

Доказательство. Если $\mathscr{L}$ — нулевое подпространство, то, очевидно, теорема верна.

Предположим, что $\mathscr{L}$ — ненулевое подпространство. Докажем, что

$$L \cap L^\perp=\{0\}. \tag{1}$$

В самом деле, если $\boldsymbol{a} \in L \cap L^\perp$, то $\boldsymbol{a} \cdot \boldsymbol{a}=0$. По условию, $\boldsymbol{a} \cdot \boldsymbol{a} \neq 0$ при $\boldsymbol{a} \neq \boldsymbol{0}$. Поэтому для $\boldsymbol{a} \in L \cap L^\perp$ из $\boldsymbol{a} \cdot \boldsymbol{a}=0$ следует, что $\boldsymbol{a}=\boldsymbol{0}$.

Далее, докажем, что

$$\mathscr{V}=\mathscr{L} \oplus \mathscr{L}^\perp. \tag{2}$$

По условию, $\mathscr{L}$ — ненулевое конечномерное векторное пространство с невырожденным умножением. В силу следствия 5.5 $\mathscr{L}$ обладает ортогональным базисом. Пусть

$$\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m \tag{3}$$

— ортогональный базис пространства $\mathscr{L}$. Достаточно показать, что для всякого вектора $\boldsymbol{a}$ из L существуют скаляры $\lambda_1, \ldots, \lambda_m$ и вектор $\boldsymbol{x}$ такие, что

$$\boldsymbol{a}=\lambda_1\boldsymbol{b}_1+\ldots+\lambda_m\boldsymbol{b}_m+\boldsymbol{x}, \quad \boldsymbol{x} \in L^\perp. \tag{4}$$

Умножив обе части равенства (4) скалярно на вектор $\boldsymbol{b}_i$, получим $\boldsymbol{a}\cdot\boldsymbol{b}_i=\lambda_i(\boldsymbol{b}_i\cdot\boldsymbol{b}_i)$. Поскольку $\boldsymbol{b}_i\cdot\boldsymbol{b}_i\neq 0$, то отсюда следуют равенства

$$(5)\quad \lambda_i=\frac{\boldsymbol{a}\cdot\boldsymbol{b}_i}{\boldsymbol{b}_i\cdot\boldsymbol{b}_i}\qquad (i=1,\ \ldots,\ m).$$

При таком выборе скаляров λ_i вектор $\boldsymbol{x}=\boldsymbol{a}-\lambda_1\boldsymbol{b}_1-\ldots-\lambda_m\boldsymbol{b}_m$ ортогонален к каждому вектору базиса (3), так как в силу (4) и (5)

$$\boldsymbol{x}\boldsymbol{b}_i=\boldsymbol{a}\boldsymbol{b}_i-\lambda_i(\boldsymbol{b}_i\boldsymbol{b}_i)=0\qquad (i=1,\ \ldots,\ m).$$

Поэтому вектор $\boldsymbol{x}$ ортогонален к любой линейной комбинации векторов $\boldsymbol{b}_1,\ \ldots,\ \boldsymbol{b}_m$ и, значит, ортогонален к L; следовательно,

$$(6)\quad \boldsymbol{x}=\boldsymbol{a}-\lambda_1\boldsymbol{b}_1-\ldots-\lambda_m\boldsymbol{b}_m\in L^{\perp}.$$

На основании (4) и (6) заключаем, что имеет место прямое разложение (2). □

СЛЕДСТВИЕ 5.7. *Если $\mathscr{L}$ — конечномерное подпространство векторного пространства $\mathscr{V}$ с невырожденным скалярным умножением, то $\mathscr{V}=\mathscr{L}\oplus\mathscr{L}^{\perp}$.*

СЛЕДСТВИЕ 5.8. *Если $\mathscr{L}$ — подпространство конечномерного векторного пространства $\mathscr{V}$ с невырожденным скалярным умножением, то $\mathscr{V}=\mathscr{L}\oplus\mathscr{L}^{\perp}$.*

ТЕОРЕМА 5.9. *Если $\mathscr{L}$ — подпространство конечномерного векторного пространства $\mathscr{V}$ с невырожденным скалярным умножением, то $(\mathscr{L}^{\perp})^{\perp}=\mathscr{L}$.*

Доказательство теоремы 5.9 предоставляется читателю.

Упражнения.

1. Пусть $\boldsymbol{a}$ — ненулевой вектор векторного пространства $\mathscr{V}=\mathscr{R}^3$ со стандартным скалярным умножением. Какова размерность подпространства пространства $\mathscr{V}$, ортогонального к вектору $\boldsymbol{a}$?

2. Пусть $\boldsymbol{a}$, $\boldsymbol{b}$ — линейно независимые векторы пространства $\mathscr{V}=\mathscr{R}^3$ со стандартным скалярным умножением. Найдите размерность подпространства, ортогонального к векторам $\boldsymbol{a}$ и $\boldsymbol{b}$.

3. Пусть $\mathscr{V}=\mathscr{Q}^2$ — двумерное векторное пространство над полем рациональных чисел со стандартным скалярным умножением. Найдите в $\mathscr{V}$ ненулевое подпространство, в котором скалярный квадрат любого вектора отличен от единицы.

4. Пусть $\mathscr{V}$ — векторное пространство с невырожденным скалярным умножением. Докажите, что если ненулевой вектор $\boldsymbol{b}$ ортогонален к векторам $\boldsymbol{a}_1,\ \ldots,\ \boldsymbol{a}_m$ пространства $\mathscr{V}$, то $\boldsymbol{b}\notin L(\boldsymbol{a}_1,\ \ldots,\ \boldsymbol{a}_m)$.

5. Пусть $\mathscr{V}$ — векторное пространство с невырожденным скалярным умножением. Пусть $\boldsymbol{a}_1,\ \ldots,\ \boldsymbol{a}_m$ — линейно независимая система векторов пространства $\mathscr{V}$. Докажите, что если ненулевой вектор $\boldsymbol{b}$

ортогонален к векторам $a_1, \ldots, a_m$, то система $a_1, \ldots, a_m, b$ линейно независима.

6. Пусть $\mathscr{L}$ — ненулевое подпространство конечномерного векторного пространства $\mathscr{V}$ с невырожденным скалярным умножением. Пусть $a_1, \ldots, a_m$ — ортогональный базис пространства $\mathscr{L}$ и $b_1, \ldots, b_s$ — ортогональный базис пространства $\mathscr{L}^\perp$. Докажите, что $a_1, \ldots, a_m, b_1, \ldots, b_s$ является ортогональным базисом пространства $\mathscr{V}$.

7. Пусть $\mathscr{L}$, $\mathscr{U}$ — подпространства конечномерного векторного пространства $\mathscr{V}$ с невырожденным скалярным умножением. Докажите, что:

(a) $(\mathscr{L}^\perp)^\perp = \mathscr{L}$; (b) $(\mathscr{L}+\mathscr{U})^\perp = \mathscr{L}^\perp \cap \mathscr{U}^\perp$;

(c) $(\mathscr{L} \cap \mathscr{U})^\perp = \mathscr{L}^\perp + \mathscr{U}^\perp$.

8. Пусть $\mathscr{L}$, $\mathscr{U}$ — подпространства конечномерного векторного пространства $\mathscr{V}$ с невырожденным скалярным умножением и размерность $\mathscr{L}$ меньше размерности $\mathscr{U}$. Докажите, что в пространстве $\mathscr{U}$ есть ненулевой вектор, ортогональный к подпространству $\mathscr{L}$.

9. Пусть $\mathscr{L}$, $\mathscr{U}$ — подпространства конечномерного векторного пространства $\mathscr{V}$ с невырожденным скалярным умножением. Докажите, что существует в $\mathscr{V}$ ненулевой вектор, ортогональный к подпространствам $\mathscr{L}$ и $\mathscr{U}$, если $\mathscr{L} + \mathscr{U} \neq \mathscr{V}$.

§ 6. ЕВКЛИДОВЫ ВЕКТОРНЫЕ ПРОСТРАНСТВА

Евклидово векторное пространство. Пусть $\mathscr{V}$ — векторное пространство со скалярным умножением над полем $\mathscr{R}$ действительных чисел. Такое пространство называют также *действительным векторным пространством.*

ОПРЕДЕЛЕНИЕ. Векторное пространство над полем $\mathscr{R}$ с положительно определенным скалярным умножением (т. е. $a \cdot a > 0$ для любого $a \in V \setminus \{0\}$) называется *евклидовым векторным пространством.*

ТЕОРЕМА 6.1. *Арифметическое векторное пространство над полем $\mathscr{R}$ со стандартным скалярным умножением является евклидовым.*

Доказательство. Пусть $\mathscr{V} = \mathscr{R}^n$ — арифметическое векторное пространство со стандартным скалярным умножением и $a = (\alpha_1, \ldots, \alpha_n)$, $b = (\beta_1, \ldots, \beta_n)$ — векторы этого пространства. По определению стандартного скалярного умножения, $ab = \alpha_1\beta_1 + \ldots + \alpha_n\beta_n$. Следовательно, $aa = \alpha_1^2 + \ldots + \alpha_n^2$. А так как $\alpha_1, \ldots, \alpha_n$ — действительные числа, то $aa > 0$ для любого ненулевого вектора a пространства $\mathscr{V}$. □

ОПРЕДЕЛЕНИЕ. Арифметическое векторное пространство $\mathscr{R}^n$ со стандартным скалярным умножением называется *n-мерным стандартным евклидовым пространством* и обозначается через $\mathscr{E}_n$.

Пример. Рассмотрим множество V всех действительных функций одной действительной переменной x, непрерывных на отрезке $[0, 1]$. Множество V относительно сложения и умножений на действительные числа является (бесконечномерным) векторным пространством над $\mathscr{R}$. Формула $fg = \int_0^1 f(x)\, g(x)\, dx$ определяет в V скалярное умножение. Таким образом, получаем евклидово векторное пространство со скалярным умножением.

Норма вектора. Пусть $\mathscr{V}$ — евклидово векторное пространство.

ОПРЕДЕЛЕНИЕ. *Нормой вектора евклидова пространства* называется арифметический квадратный корень из скалярного квадрата вектора.

Норма вектора обозначается через $\|\boldsymbol{a}\|$.

По определению, $\|\boldsymbol{a}\| = \sqrt{\boldsymbol{a} \cdot \boldsymbol{a}}$. Следовательно, $\|\boldsymbol{a}\|^2 = \boldsymbol{a} \cdot \boldsymbol{a}$.

ОПРЕДЕЛЕНИЕ. Вектор $\boldsymbol{a}$ называется *нормированным*, если $\|\boldsymbol{a}\| = 1$.

Следующая теорема выражает основные свойства нормы вектора.

ТЕОРЕМА 6.2. *Если* $\boldsymbol{a}$, $\boldsymbol{b}$ — *векторы евклидова пространства и* $\lambda \in \mathbb{R}$, *то*:

(1) $\|\boldsymbol{a}\| \geqslant 0$, *причем* $\|\boldsymbol{a}\| = 0$ *тогда и только тогда, когда* $\boldsymbol{a} = \boldsymbol{0}$;

(2) $\|\lambda \boldsymbol{a}\| = |\lambda| \|\boldsymbol{a}\|$;

(3) $|\boldsymbol{a} \cdot \boldsymbol{b}| \leqslant \|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\|$ (*неравенство Коши — Буняковского*);

(4) $\|\boldsymbol{a} + \boldsymbol{b}\| \leqslant \|\boldsymbol{a}\| + \|\boldsymbol{b}\|$ (*неравенство треугольника*).

Доказательство. Скалярное умножение в евклидовом пространстве положительно определено, т. е. $\|\boldsymbol{a}\| = \sqrt{\boldsymbol{a} \cdot \boldsymbol{a}} > 0$ при $\boldsymbol{a} \neq \boldsymbol{0}$. Кроме того, $\|\boldsymbol{a}\| = 0$ при $\boldsymbol{a} = \boldsymbol{0}$. Согласно определению нормы,

$$\|\lambda \boldsymbol{a}\| = \sqrt{(\lambda \boldsymbol{a})(\lambda \boldsymbol{a})} = \sqrt{\lambda^2 (\boldsymbol{a}\boldsymbol{a})} = |\lambda| \sqrt{\boldsymbol{a}\boldsymbol{a}} = |\lambda| \cdot \|\boldsymbol{a}\|,$$

т. е. выполняется (2).

Неравенство (3) верно, если $\boldsymbol{a} = \boldsymbol{0}$ или $\boldsymbol{b} = \boldsymbol{0}$. Поэтому будем предполагать, что $\boldsymbol{a}$ и $\boldsymbol{b}$ — ненулевые векторы. Для любых действительных чисел α и β имеем неравенство

$$(\alpha \boldsymbol{a} - \beta \boldsymbol{b})(\alpha \boldsymbol{a} - \beta \boldsymbol{b}) \geqslant 0.$$

Раскрывая скобки в левой части неравенства $\alpha^2\boldsymbol{a}^2 - 2\alpha\beta\boldsymbol{ab} + \beta^2\boldsymbol{b}^2 \geqslant 0$ и полагая $\alpha = \|\boldsymbol{b}\|$ и $\beta = \|\boldsymbol{a}\|$, получаем:

$$2(\|\boldsymbol{a}\|\cdot\|\boldsymbol{b}\|)^2 - 2\|\boldsymbol{a}\|\cdot\|\boldsymbol{b}\|\cdot\boldsymbol{ab} \geqslant 0,$$

$$\|\boldsymbol{a}\|\cdot\|\boldsymbol{b}\|(\|\boldsymbol{a}\|\cdot\|\boldsymbol{b}\| - \boldsymbol{ab}) \geqslant 0.$$

Так как $\boldsymbol{a} \neq 0$ и $\boldsymbol{b} \neq 0$, то $\|\boldsymbol{a}\|\cdot\|\boldsymbol{b}\| \neq 0$, поэтому

(5) $\boldsymbol{ab} \leqslant \|\boldsymbol{a}\|\cdot\|\boldsymbol{b}\|$.

Заменим в этом неравенстве $\boldsymbol{a}$ на $-\boldsymbol{a}$:

$$-\boldsymbol{a}\cdot\boldsymbol{b} \leqslant \|\boldsymbol{a}\|\cdot\|\boldsymbol{b}\|.$$

На основании последних двух неравенств заключаем, что имеет место неравенство (3).

Для доказательства неравенства (4) достаточно показать, что $\|\boldsymbol{a}+\boldsymbol{b}\|^2 \leqslant (\|\boldsymbol{a}\|+\|\boldsymbol{b}\|)^2$. Легко видеть, что $\|\boldsymbol{a}+\boldsymbol{b}\|^2 = (\boldsymbol{a}+\boldsymbol{b})(\boldsymbol{a}+\boldsymbol{b}) = \|\boldsymbol{a}\|^2 + \|\boldsymbol{b}\|^2 + 2\boldsymbol{ab}$; поэтому

$$\|\boldsymbol{a}+\boldsymbol{b}\|^2 = (\|\boldsymbol{a}\|+\|\boldsymbol{b}\|)^2 + 2(\boldsymbol{ab} - \|\boldsymbol{a}\|\cdot\|\boldsymbol{b}\|).$$

В силу (5) второе слагаемое в правой части последнего равенства меньше или равно нулю, следовательно,

$$\|\boldsymbol{a}+\boldsymbol{b}\|^2 \leqslant (\|\boldsymbol{a}\|+\|\boldsymbol{b}\|)^2;$$

отсюда вытекает неравенство (4). □

Ортонормированный базис евклидова пространства. Для евклидовых пространств одним из основных является понятие ортонормированного базиса.

ОПРЕДЕЛЕНИЕ. Система векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ евклидова пространства называется *ортонормированной*, если она ортогональна и каждый ее вектор нормирован. Ортонормированная система векторов, являющаяся базисом пространства, называется *ортонормированным базисом пространства*.

ТЕОРЕМА 6.3. *Конечномерное ненулевое евклидово векторное пространство обладает ортонормированным базисом.*

Доказательство. Пусть $\mathcal{V}$ — n-мерное евклидово пространство и $n > 0$. По следствию 5.5, $\mathcal{V}$ обладает ортогональным базисом; пусть

(1) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$

— такой базис. Нормируем систему (1), т. е. образуем систему

$$\boldsymbol{e}_1 = \|\boldsymbol{b}_1\|^{-1}\boldsymbol{b}_1, \ldots, \boldsymbol{e}_n = \|\boldsymbol{b}_n\|^{-1}\boldsymbol{b}_n.$$

Легко видеть, что

$$e_i e_k = \begin{cases} 1, & \text{если } i = k, \\ 0, & \text{если } i \neq k. \end{cases}$$

Следовательно, система $e_1, \ldots, e_n$ является ортонормированным базисом пространства $\mathcal{V}$. □

Рассмотрим некоторые свойства ортонормированного базиса.

СВОЙСТВО 6.1. *Если $\mathcal{V}$ — n-мерное ненулевое евклидово пространство, то любая ортонормированная система n векторов является ортонормированным базисом пространства $\mathcal{V}$.*

Это свойство непосредственно вытекает из следствия 5.3.

СВОЙСТВО 6.2. *Ортонормированную систему векторов ненулевого конечномерного евклидова пространства, не являющуюся базисом, можно дополнить до ортонормированного базиса пространства.*

Доказательство. Согласно теореме 5.4, ортонормированную систему векторов $b_1, \ldots, b_m$, не являющуюся базисом, можно дополнить до ортогонального базиса

$$b_1, \ldots, b_m, b_{m+1}, \ldots, b_n$$

пространства. Нормируя векторы $b_{m+1}, \ldots, b_n$ этой системы, т. е. заменяя b_i на $\|b_i\|^{-1} \cdot b_i$ для $i = m+1, \ldots, n$, получаем ортонормированный базис пространства. □

СВОЙСТВО 6.3. Если $e_1, \ldots, e_n$ — ортонормированный базис евклидова пространства и

$$a = \alpha_1 e_1 + \ldots + \alpha_n e_n, \quad b = \beta_1 e_1 + \ldots + \beta_n e_n$$

— векторы пространства, то

$$ab = \alpha_1\beta_1 + \ldots + \alpha_n\beta_n \text{ и } \|a\|^2 = \alpha_1^2 + \ldots + \alpha_n^2.$$

Это свойство легко следует из свойства билинейности скалярного умножения.

СВОЙСТВО 6.4. *Если $e_1, \ldots, e_n$ — ортонормированный базис евклидова пространства и $a = \alpha_1 e_1 + \ldots + \alpha_n e_n$, то $\alpha_i = ae_i$ для $i = 1, \ldots, n$, т. е. координаты вектора a являются его проекциями на базисные векторы.*

Доказательство. Равенство $\alpha_i = ae_i$ получается из равенства $a = \alpha_1 e_1 + \ldots + \alpha_n e_n$ в результате умножения скалярно на вектор e_i. □

СВОЙСТВО 6.5. *Если $\mathcal{L}$ — подпространство конечномерного евклидова пространства $\mathcal{V}$, то $\mathcal{V} = \mathcal{L} \oplus \mathcal{L}^\perp$ и* $\dim \mathcal{V} = \dim \mathcal{L} + \dim \mathcal{L}^\perp$.

Это свойство непосредственно вытекает из следствия 5.8 и свойства 3.4, поскольку в евклидовом пространстве скалярное умножение является невырожденным.

Изоморфизмы евклидовых пространств. Пусть $\mathcal{U}$ и $\mathcal{V}$ — евклидовы пространства.

ОПРЕДЕЛЕНИЕ. Отображение f евклидова пространства $\mathcal{U}$ на $\mathcal{V}$ называется *изоморфизмом*, если оно инъективно и удовлетворяет условиям:

(1) $f(\boldsymbol{a}+\boldsymbol{b})=f(\boldsymbol{a})+f(\boldsymbol{b})$;

(2) $f(\lambda\boldsymbol{a})=\lambda f(\boldsymbol{a})$;

(3) $\boldsymbol{ab}=f(\boldsymbol{a})f(\boldsymbol{b})$

для любых $\boldsymbol{a}$, $\boldsymbol{b}$ из V и любого скаляра λ из $\mathbf{R}$. Евклидовы пространства называются *изоморфными*, если существует изоморфизм евклидова пространства $\mathcal{U}$ на $\mathcal{V}$.

Запись $\mathcal{U}\cong\mathcal{V}$ означает, что евклидовы пространства $\mathcal{U}$ и $\mathcal{V}$ изоморфны.

Отметим следующие свойства изоморфизмов.

СВОЙСТВО 6.6. *Отношение изоморфизма на какомлибо множестве евклидовых пространств является отношением эквивалентности.*

Доказательство. Легко видеть, что отношение изоморфизма рефлексивно.

Воспользуемся свойствами 4.2 и 4.3 изоморфизмов векторных пространств. Если f — изоморфизм евклидова пространства $\mathcal{U}$ на $\mathcal{V}$, то f^{-1} биективно и удовлетворяет условиям линейности. Далее, так как f удовлетворяет условию (3), то для любых $\boldsymbol{a}$, $\boldsymbol{b}$ из V

$$\boldsymbol{ab}=(ff^{-1})(\boldsymbol{a})(ff^{-1})(\boldsymbol{b})=f(f^{-1}(\boldsymbol{a}))f(f^{-1}(\boldsymbol{b}))=f^{-1}(\boldsymbol{a})f^{-1}(\boldsymbol{b}),$$

т. е. отображение f^{-1} также удовлетворяет условию (3). Таким образом, f^{-1} есть изоморфизм евклидова пространства $\mathcal{V}$ на $\mathcal{U}$. Следовательно, отношение изоморфизма евклидовых пространств симметрично.

Пусть $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$ — евклидовы пространства. Если f — изоморфизм $\mathcal{U}$ на $\mathcal{V}$ и g — изоморфизм $\mathcal{V}$ на $\mathcal{W}$, то, по свойству 4.1 изоморфизмов векторных пространств, композиция gf есть инъективное отображение $\mathcal{U}$ на $\mathcal{W}$, удовлетворяющее условиям линейности. Далее, так как

$$\boldsymbol{ab}=f(\boldsymbol{a})f(\boldsymbol{b}),\ f(\boldsymbol{a})f(\boldsymbol{b})=g(f(\boldsymbol{a}))g(f(\boldsymbol{b})),$$

то

$$\boldsymbol{ab}=(gf)(\boldsymbol{a})(gf)(\boldsymbol{b})$$

для любых $\boldsymbol{a}$, $\boldsymbol{b}$ из U. Поэтому gf является изоморфизмом евклидова пространства $\mathcal{U}$ на $\mathcal{W}$. Следовательно, отношение изоморфизма транзитивно. □

СВОЙСТВО 6.7. *Пусть $\mathcal{U}$, $\mathcal{V}$ — евклидовы пространства и f — изоморфизм $\mathcal{U}$ на $\mathcal{V}$. Если $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ — ортонормированный базис пространства $\mathcal{U}$, то система $f(\boldsymbol{e}_1), \ldots, f(\boldsymbol{e}_n)$ является ортонормированным базисом пространства $\mathcal{V}$.*

Доказательство. Так как f — изоморфизм, то $\boldsymbol{e}_i\boldsymbol{e}_k = f(\boldsymbol{e}_i)f(\boldsymbol{e}_k)$. Следовательно,

$$f(\boldsymbol{e}_i)f(\boldsymbol{e}_k) = \boldsymbol{e}_i\boldsymbol{e}_k = \begin{cases} 1, & \text{если } i = k, \\ 0, & \text{если } i \neq k. \end{cases}$$

Таким образом, система $f(\boldsymbol{e}_1), \ldots, f(\boldsymbol{e}_n)$ является ортонормированной. Кроме того, по свойству 4.4 изоморфизмов векторных пространств, система $f(\boldsymbol{e}_1), \ldots, f(\boldsymbol{e}_n)$ является базисом пространства $\mathcal{V}$. □

ТЕОРЕМА 6.4. *Любое ненулевое евклидово пространство размерности n изоморфно стандартному n-мерному евклидову пространству.*

Доказательство. Пусть $\mathcal{V}$ — n-мерное евклидово пространство и $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ — его фиксированный ортонормированный базис. Пусть $\mathcal{E}_n$ — стандартное n-мерное евклидово пространство. По теореме 4.3, отображение $f\colon V \to \mathbf{R}^n$, ставящее в соответствие каждому вектору $\boldsymbol{x} = \xi_1\boldsymbol{e}_1 + \ldots + \xi_n\boldsymbol{e}_n$ из V его координатную строку $(\xi_1, \ldots, \xi_n)$, является инъективным и удовлетворяет условиям линейности. Кроме того, если $\boldsymbol{y} = \eta_1\boldsymbol{e}_1 + \ldots + \eta_n\boldsymbol{e}_n$, то

$$\boldsymbol{x}\boldsymbol{y} = \xi_1\eta_1 + \ldots \xi_n\eta_n = (\xi_1, \ldots, \xi_n)(\eta_1, \ldots, \eta_n) = f(\boldsymbol{x})f(\boldsymbol{y}).$$

Следовательно, f является изоморфизмом евклидова пространства $\mathcal{V}$ на стандартное евклидово пространство $\mathcal{E}_n$ □

ТЕОРЕМА 6.5. *Два конечномерных евклидовых пространства изоморфны тогда и только тогда, когда равны их размерности.*

Доказательство. Пусть $\mathcal{U}$ и $\mathcal{V}$ — конечномерные евклидовы пространства. Если пространства $\mathcal{U}$ и $\mathcal{V}$ изоморфны, то, по теореме 4.6, $\dim \mathcal{U} = \dim \mathcal{V}$.

Предположим теперь, что $\dim \mathcal{U} = \dim \mathcal{V} = n$. Если $n = 0$, то пространство $\mathcal{U}$ и $\mathcal{V}$ — нулевые и поэтому изоморфны. Если же $n > 0$, то, по теореме 6.4, $\mathcal{U} \cong \mathcal{E}_n$ и $\mathcal{E}_n \cong \mathcal{V}$. В силу транзитивности изоморфизма отсюда следует, что евклидовы пространства $\mathcal{U}$ и $\mathcal{V}$ изоморфны. □

Упражнения.

1. Пусть $\boldsymbol{a}$, $\boldsymbol{b}$ — взаимно ортогональные векторы евклидова пространства. Покажите, что $\|\boldsymbol{a}+\boldsymbol{b}\|^2=\|\boldsymbol{a}\|^2+\|\boldsymbol{b}\|^2$.

2. Покажите, что для любых векторов $\boldsymbol{a}$, $\boldsymbol{b}$ евклидова пространства $\|\boldsymbol{a}+\boldsymbol{b}\|^2+\|\boldsymbol{a}-\boldsymbol{b}\|^2=2(\|\boldsymbol{a}\|^2+\|\boldsymbol{b}\|^2)$.

3. Пусть $\boldsymbol{a}$, $\boldsymbol{b}$ — такие векторы евклидова пространства, что $\|\boldsymbol{a}\|=\|\boldsymbol{b}\|$. Докажите, что векторы $\boldsymbol{a}-\boldsymbol{b}$ и $\boldsymbol{a}+\boldsymbol{b}$ взаимно ортогональны.

4. Докажите, что для любых векторов $\boldsymbol{a}$, $\boldsymbol{b}$ евклидова пространства $|\,\|\boldsymbol{a}\|-\|\boldsymbol{b}\|\,|\leqslant\|\boldsymbol{a}\pm\boldsymbol{b}\|$.

5. Пусть $\boldsymbol{a}$, $\boldsymbol{b}$ — ненулевые векторы евклидова пространства. Найдите вектор вида $\boldsymbol{a}+\lambda\boldsymbol{b}$, где $\lambda\in\mathbb{R}$, имеющий наименьшую норму, и покажите, что этот вектор ортогонален к вектору $\boldsymbol{a}$.

6. Пусть $\boldsymbol{a}$, $\boldsymbol{b}$ — линейно независимые векторы трехмерного евклидова пространства $\mathscr{V}$. Докажите, что в пространстве $\mathscr{V}$ существуют только два вектора с единичной нормой, ортогональных к векторам $\boldsymbol{a}$ и $\boldsymbol{b}$.

7. Пусть $\mathscr{V}=\mathbb{Q}^2$ — двумерное векторное пространство над полем рациональных чисел со стандартным скалярным умножением. Найдите в $\mathscr{V}$ ненулевое подпространство, в котором скалярный квадрат любого вектора отличен от единицы.

8. Пусть $\boldsymbol{a}$, $\boldsymbol{b}$ — линейно независимые векторы евклидова n-мерного пространства $\mathscr{V}$. Найдите размерность подпространства пространства $\mathscr{V}$, ортогонального к векторам $\boldsymbol{a}$ и $\boldsymbol{b}$.

9. Пусть $\mathscr{U}$ — подпространство n-мерного евклидова пространства $\mathscr{V}$ и $\mathscr{U}^\perp$ — его ортогональное дополнение. Пусть $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_s$ — ортонормированный базис пространства $\mathscr{U}$ и $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-s}$ — ортонормированный базис пространства $\mathscr{U}^\perp$. Докажите, что $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_s, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-s}$ есть ортонормированный базис пространства $\mathscr{V}$.

10. Пусть $\boldsymbol{a}$, $\boldsymbol{b}$ — векторы евклидова векторного пространства. Докажите, что $|\boldsymbol{a}\cdot\boldsymbol{b}|=\|\boldsymbol{a}\|\cdot\|\boldsymbol{b}\|$ тогда и только тогда, когда векторы $\boldsymbol{a}$ и $\boldsymbol{b}$ линейно зависимы.

11. Пусть $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ — ортонормированная система векторов евклидова пространства $\mathscr{V}$. Предположим, что для каждого вектора $\boldsymbol{c}$ пространства $\mathscr{V}$ $\|\boldsymbol{c}\|^2=(\boldsymbol{a}_1\boldsymbol{c})^2+\ldots+(\boldsymbol{a}_m\boldsymbol{c})^2$. Докажите, что система векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ является базисом пространства $\mathscr{V}$.

12. Пусть $\mathscr{L}$, $\mathscr{U}$ — подпространства конечномерного евклидова векторного пространства. Докажите, что:

(a) $(\mathscr{L}^\perp)^\perp=\mathscr{L}$; (b) $(\mathscr{L}+\mathscr{U})^\perp=\mathscr{L}^\perp\cap\mathscr{U}^\perp$; (c) $(\mathscr{L}\cap\mathscr{U})^\perp=\mathscr{L}^\perp+\mathscr{U}^\perp$.

Глава восьмая

ЛИНЕЙНЫЕ ОПЕРАТОРЫ

§ 1. ЛИНЕЙНЫЕ ОТОБРАЖЕНИЯ

Линейные отображения и операторы. Рассмотрим гомоморфизмы векторных пространств; они называются также линейными отображениями.

ОПРЕДЕЛЕНИЕ. Пусть $\mathcal{U}$ и $\mathcal{V}$ — векторные пространства над полем $\mathcal{F}$. Отображение f: $\mathcal{U} \to \mathcal{V}$ называется *линейным отображением* или *гомоморфизмом*, если оно удовлетворяет условиям линейности, т. е. для любых $\boldsymbol{a}$, $\boldsymbol{b} \in V$ и любого $\lambda \in F$ выполняются условия

$$f(\boldsymbol{a}+\boldsymbol{b}) = f(\boldsymbol{a}) + f(\boldsymbol{b}), \quad f(\lambda \boldsymbol{a}) = \lambda f(\boldsymbol{a}).$$

Если линейное отображение $\mathcal{U}$ на $\mathcal{V}$ инъективно, то оно называется *изоморфизмом* или *изоморфным отображением* $\mathcal{U}$ на $\mathcal{V}$.

Множество всех линейных отображений (гомоморфизмов) пространства $\mathcal{U}$ в пространство $\mathcal{V}$ будем обозначать $\mathrm{Hom}(\mathcal{U}, \mathcal{V})$.

Линейное отображение векторного пространства $\mathcal{V}$ в себя называется *линейным оператором пространства* $\mathcal{V}$. Множество всех линейных операторов пространства $\mathcal{V}$ обозначается $\mathrm{Hom}(\mathcal{V}, \mathcal{V})$.

Пусть φ — линейное отображение векторного пространства $\mathcal{U}$ на векторное пространство $\mathcal{V}$. Тогда для любых векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ из $\mathcal{U}$ и любых скаляров $\lambda_1, \ldots, \lambda_m \in F$

$$(1)\quad \varphi(\lambda_1 \boldsymbol{a}_1 + \ldots + \lambda_m \boldsymbol{a}_m) = \lambda_1 \varphi(\boldsymbol{a}_1) + \ldots + \lambda_m \varphi(\boldsymbol{a}_m).$$

Доказательство проводится индукцией по m. Если $m = 1$, то ввиду линейности отображения φ имеем $\varphi(\lambda_1 \boldsymbol{a}_1) = \lambda_1 \varphi(\boldsymbol{a}_1)$. Допустим, что предложение верно для $m-1$ векторов. Тогда, используя равенство

$$\lambda_1 \boldsymbol{a}_1 + \ldots + \lambda_{m-1} \boldsymbol{a}_{m-1} + \lambda_m \boldsymbol{a}_m = (\lambda_1 \boldsymbol{a}_1 + \ldots + \lambda_{m-1} \boldsymbol{a}_{m-1}) + \lambda_m \boldsymbol{a}_m,$$

получаем

$$\varphi(\lambda_1 a_1 + \ldots + \lambda_m a_m) = \varphi(\lambda_1 a_1 + \ldots + \lambda_{m-1} a_{m-1}) + \varphi(\lambda_m a_m).$$

По индуктивному предположению,

$$\varphi(\lambda_1 a_1 + \ldots + \lambda_{m-1} a_{m-1}) = \lambda_1 \varphi(a_1) + \ldots + \lambda_{m-1} \varphi(a_{m-1}).$$

Кроме того, $\varphi(\lambda_m a) = \lambda_m \varphi(a_m)$. Следовательно, выполняется равенство (1). □

Примеры. 1. Пусть $\mathcal{V}$ — векторное пространство. Отображение ε: $\mathcal{V} \to \mathcal{V}$, ставящее в соответствие каждому вектору x из V этот же вектор, т. е. $\varepsilon(x) = x$, есть линейный оператор. Он называется *тождественным* или *единичным оператором пространства*.

2. Пусть $\mathcal{V}$ — векторное пространство над полем $\mathcal{F}$ и λ — фиксированный элемент поля. Отображение $\lambda\varepsilon$: $\mathcal{V} \to \mathcal{V}$, ставящее в соответствие вектору x вектор λx, есть линейный оператор пространства $\mathcal{V}$. Он называется *оператором гомотетии* с коэффициентом λ. Оператор гомотетии с коэффициентом $\lambda = 0$ называется *нулевым оператором*. Оператор гомотетии с коэффициентом $\lambda = 1$ есть тождественный оператор.

3. Пусть $\mathcal{V} = \mathcal{L} \oplus \mathcal{U}$. Любой элемент x из $\mathcal{V}$ однозначно представим в виде $x = l + u$, где $l \in L$ и $u \in U$. Отображение $\mathcal{V} \to \mathcal{V}$, ставящее в соответствие вектору x его компоненту l в прямом слагаемом $\mathcal{U}$, есть линейный оператор пространства $\mathcal{V}$. Он называется *оператором проектирования*.

4. Пусть $\mathcal{V}$ — векторное пространство (над $\mathcal{R}$) действительных функций одной переменной x, определенных и неограниченно дифференцируемых на множестве $\mathbf{R}$ действительных чисел. Оператор $D: \mathcal{V} \to \mathcal{V}$, ставящий в соответствие каждому элементу $f \in V$ его производную $\frac{df}{dx}$, есть линейный оператор, так как удовлетворяет условиям линейности

$$D(f+g) = D(f) + D(g); \quad D(\lambda f) = \lambda D(f)$$

для любых $f, g \in V$ и любого $\lambda \in \mathbf{R}$. Этот оператор называется оператором *дифференцирования*.

5. Пусть $\mathcal{V} = \mathcal{F}^n$ — арифметическое пространство n-мерных вектор-столбцов и A — фиксированная квадратная $n \times n$-матрица над полем $\mathcal{F}$. Отображение пространства $\mathcal{V}$ в себя, ставящее в соответствие каждому вектору $X \in F^n$ вектор AX, есть линейный оператор пространства $\mathcal{V}$.

ТЕОРЕМА 1.1. *Пусть* $\mathcal{U}$ *и* $\mathcal{V}$ *— векторные пространства над полем* $\mathcal{F}$, $e_1, \ldots, e_n$ *— базис пространства* $\mathcal{U}$ *и* $c_1, \ldots, c_n$ *— произвольные векторы пространства* $\mathcal{V}$. *Тогда существует единственное линейное отображение* φ *пространства* $\mathcal{U}$ *в пространство* $\mathcal{V}$, *удовлетворяющее условиям* (1) $\varphi(e_1) = c_1, \ldots, \varphi(e_n) = c_n$.

Доказательство. Любой вектор пространства $\mathcal{U}$ можно представить в виде линейной комбинации базисных векторов, т. е. в виде $\lambda_1 e_1 + \ldots + \lambda_n e_n$. Обозначим через φ отображение $\mathcal{U}$ в $\mathcal{V}$, определяемое равенством

$$\varphi(\lambda_1 e_1 + \ldots + \lambda_n e_n) = \lambda_1 c_1 + \ldots + \lambda_n c_n \text{ для любых } \lambda_1, \ldots, \lambda_n \text{ из } F.$$

Легко видеть, что отображение φ удовлетворяет условиям (1).

Отображение φ удовлетворяет условиям линейности. Действительно, если

$$x = \alpha_1 e_1 + \ldots + \alpha_n e_n \text{ и } y = \beta_1 e_1 + \ldots + \beta_n e_n,$$

то

$$x + y = (\alpha_1 + \beta_1) e_1 + \ldots + (\alpha_n + \beta_n) e_n$$

$$\text{и } \lambda x = \lambda \alpha_1 e_1 + \ldots + \lambda \alpha_n x_n.$$

Следовательно, в силу определения отображения φ

$$\varphi(x + y) = (\alpha_1 + \beta_1) c_1 + \ldots + (\alpha_n + \beta_n) c_n =$$
$$= (\alpha_1 c_1 + \ldots + \alpha_n c_n) + (\beta_1 c_1 + \ldots + \beta_n c_n) = \varphi(x) + \varphi(y);$$
$$\varphi(\lambda x) = \lambda \alpha_1 c_1 + \ldots + \lambda \alpha_n c_n = \lambda(\alpha_1 c_1 + \ldots + \alpha_n c_n) = \lambda \varphi(x).$$

Предположим, что ψ — линейное отображение $\mathcal{U}$ в $\mathcal{V}$, удовлетворяющее условиям $\psi(e_1) = c_1, \ldots, \psi(e_n) = c_n$. Тогда для любого вектора $x = \alpha_1 e_1 + \ldots + \alpha_n e_n$ пространства $\mathcal{U}$ имеем

$$\psi(x) = \alpha_1 \psi(e_1) + \ldots + \alpha_n \psi(e_n) = \alpha_1 c_1 + \ldots + \alpha_n c_n = \varphi(x),$$

т. е. $\psi = \varphi$. □

СЛЕДСТВИЕ 1.2. *Пусть* $\mathcal{U}$ *и* $\mathcal{V}$ *— векторные пространства над* $\mathcal{F}$, $e_1, \ldots, e_n$ *— базис пространства* $\mathcal{U}$; φ *и* ψ *— такие линейные отображения* $\mathcal{U}$ *в* $\mathcal{V}$, *что* $\varphi(e_k) = \psi(e_k)$ *для* $k = 1, \ldots, n$. *Тогда* $\varphi = \psi$.

СЛЕДСТВИЕ 1.3. *Пусть* $e_1, \ldots, e_n$ *— базис векторного пространства* $\mathcal{V}$ *и* $c_1, \ldots, c_n$ *— произвольные векторы этого пространства. Тогда существует единственный линейный оператор* φ *пространства* $\mathcal{V}$, *удовлетворяющий условиям* (1).

Ядро и образ линейного оператора. Пусть φ — линейный оператор векторного пространства $\mathcal{V}$. Множество $\{x \in V \mid \varphi(x) = 0\}$ обозначается $\operatorname{Ker}\varphi$. Другими словами, множество $\operatorname{Ker}\varphi$ есть полный прообраз нулевого вектора при отображении φ, $\operatorname{Ker}\varphi = \varphi^{-1}(0)$. В силу линейности оператора φ это множество замкнуто относительно сложения и умножения на скаляры. Следовательно, существует подпространство пространства $\mathcal{V}$ с основным множеством $\operatorname{Ker}\varphi$.

ОПРЕДЕЛЕНИЕ. Подпространство векторного пространства $\mathcal{V}$ с основным множеством $\operatorname{Ker}\varphi$ называется *ядром линейного оператора* φ и обозначается $\mathcal{K}er\,\varphi$. Размерность ядра называется *дефектом оператора* φ, дефект $\varphi = \dim \mathcal{K}er\,\varphi$.

Множество $\{\varphi(x) \mid x \in V\}$ обозначается через $\operatorname{Im}\varphi$ или $\varphi(V)$. В силу линейности оператора φ это множество замкнуто относительно сложения и умножения на скаляры. Следовательно, существует подпространство пространства $\mathcal{V}$ с основным множеством $\operatorname{Im}\varphi$.

ОПРЕДЕЛЕНИЕ. Подпространство векторного пространства $\mathcal{V}$ с основным множеством $\operatorname{Im}\varphi$ называется *образом линейного оператора* φ и обозначается $\mathcal{I}m\,\varphi$. Размерность образа оператора φ называется *рангом оператора* φ, ранг $\varphi = \dim(\mathcal{I}m\,\varphi)$.

ТЕОРЕМА 1.4. *Пусть φ — линейный оператор конечномерного векторного пространства $\mathcal{V}$. Тогда*

(1) *сумма ранга и дефекта оператора φ равна* $\dim \mathcal{V}$.

Доказательство. Первый случай: $\operatorname{Ker}\varphi = \{0\}$. Если $\mathcal{V}$ — нулевое пространство, то легко видеть, что заключение теоремы выполняется.

Предположим, что $\mathcal{V}$ — ненулевое пространство. Пусть $\dim \mathcal{V} = n$ и $e_1, \ldots, e_n$ — базис пространства $\mathcal{V}$. Тогда система векторов $\varphi(e_1), \ldots, \varphi(e_n)$ порождает пространство $\mathcal{I}m\,\varphi$, т. е. $\operatorname{Im}\varphi = L(\varphi(e_1), \ldots, \varphi(e_n))$.

Эта система векторов линейно независима. Действительно, если

$$\lambda_1\varphi(e_1) + \ldots + \lambda_n\varphi(e_n) = 0,$$

то ввиду линейности оператора φ

$$\varphi(\lambda_1 e_1 + \ldots + \lambda_n e_n) = 0.$$

Так как $\operatorname{Ker}\varphi = \{0\}$, то отсюда следует, что

$$\lambda_1 e_1 + \ldots + \lambda_n e_n = 0$$

и в силу линейной независимости векторов $\lambda_1 = 0, \ldots, \lambda_n = 0$. Таким образом, система $\varphi(e_1), \ldots, \varphi(e_n)$ является базисом пространства $\mathscr{I}m\,\varphi$ и поэтому ранг φ равен n. Кроме того, дефект φ равен нулю. Следовательно, имеет место утверждение (1).

Второй случай: $\operatorname{Ker}\varphi \neq \{0\}$. Пусть дефект φ равен r и $e_1, \ldots, e_r$ — базис ядра оператора φ, базис пространства $\mathscr{K}er\,\varphi$. Если $r = \dim \mathscr{V}$, то, очевидно, утверждение (1) выполняется. Предположим, что $r < n = \dim \mathscr{V}$. В этом случае систему $e_1, \ldots, e_r$ можно дополнить до базиса пространства $\mathscr{V}$. Пусть $e_1, \ldots, e_r, e_{r+1}, \ldots, e_n$ — базис пространства $\mathscr{V}$; тогда

$$\operatorname{Im}\varphi = L(\varphi(e_1), \ldots, \varphi(e_n)).$$

Так как $\varphi(e_1) = 0, \ldots, \varphi(e_r) = 0$, то

$$\operatorname{Im}\varphi = L(\varphi(e_{r+1}), \ldots, \varphi(e_n)),$$

т. е. система векторов $\varphi(e_{r+1}), \ldots, \varphi(e_n)$ порождает пространство $\mathscr{I}m\,\varphi$.

Эта система линейно независима. Действительно, если

$$\lambda_{r+1}\varphi(e_{r+1}) + \ldots + \lambda_n\varphi(e_n) = 0,$$

то в силу линейности оператора φ

$$\varphi(\lambda_{r+1}e_{r+1} + \ldots + \lambda_n e_n) = 0,$$

откуда

$$\lambda_{r+1}e_{r+1} + \ldots + \lambda_n e_n \in \operatorname{Ker}\varphi.$$

Так как $e_1, \ldots, e_r$ — базис пространства $\mathscr{K}er\,\varphi$, то существуют такие скаляры $\lambda_1, \ldots, \lambda_r$, что

$$\lambda_{r+1}e_{r+1} + \ldots + \lambda_n e_n = \lambda_1 e_1 + \ldots + \lambda_r e_r$$

и

$$(-\lambda_1)e_1 + \ldots + (-\lambda_r)e_r + \lambda_{r+1}e_{r+1} + \ldots + \lambda_n e_n = 0.$$

В силу линейной независимости векторов $e_1, \ldots, e_n$ отсюда следует, что равны нулю все коэффициенты в левой части равенства, в частности и $\lambda_{r+1} = 0, \ldots, \lambda_n = 0$. Таким образом, система векторов $\varphi(e_{r+1}), \ldots, \varphi(e_n)$ является базисом пространства $\mathscr{I}m\,\varphi$ и ранг φ равен $n - r$. Следовательно, верно утверждение (1). □

Операции над линейными отображениями. Пусть $\mathscr{U}$ и $\mathscr{V}$ — векторные пространства над полем $\mathscr{F}$, φ, ψ — линейные отображения $\mathscr{U}$ в $\mathscr{V}$. Сумма $\varphi + \psi$ определяется как

отображение $\mathcal{U}$ в $\mathfrak{V}$, ставящее в соответствие элементу $\boldsymbol{x}$ из $\mathcal{U}$ элемент $\varphi(\boldsymbol{x})+\psi(\boldsymbol{x})$ из $\mathfrak{V}$, т. е.

$$(\varphi+\psi)(\boldsymbol{x})=\varphi(\boldsymbol{x})+\psi(\boldsymbol{x}).$$

Произведение скаляра $\lambda\in F$ и отображения φ определяется как отображение $\mathcal{U}$ в $\mathfrak{V}$, ставящее в соответствие элементу $\boldsymbol{x}\in\mathcal{U}$ элемент $\lambda\varphi(\boldsymbol{x})$ пространства $\mathfrak{V}$, т. е. $(\lambda\varphi)(\boldsymbol{x})=\lambda\varphi(\boldsymbol{x})$.

ПРЕДЛОЖЕНИЕ 1.5. *Пусть φ и ψ — линейные отображения векторного пространства $\mathcal{U}$ в векторное пространство $\mathfrak{V}$ и $\lambda\in F$. Тогда $\varphi+\psi$ и $\lambda\varphi$ являются линейными отображениями $\mathcal{U}$ в $\mathfrak{V}$.*

Доказательство. Сумма $\varphi+\psi$ удовлетворяет условиям линейности.. Действительно, для любых $\boldsymbol{a}, \boldsymbol{b}\in U$ и любого $\lambda\in F$ имеем:

$$\begin{aligned}(\varphi+\psi)(\boldsymbol{a}+\boldsymbol{b})&=\varphi(\boldsymbol{a}+\boldsymbol{b})+\psi(\boldsymbol{a}+\boldsymbol{b})=\varphi(\boldsymbol{a})+\varphi(\boldsymbol{b})+\\&+\psi(\boldsymbol{a})+\psi(\boldsymbol{b})=\varphi(\boldsymbol{a})+\psi(\boldsymbol{a})+\varphi(\boldsymbol{b})+\psi(\boldsymbol{b})=\\&=(\varphi+\psi)(\boldsymbol{a})+(\varphi+\psi)(\boldsymbol{b});\end{aligned}$$

$$\begin{aligned}(\varphi+\psi)(\lambda\boldsymbol{a})&=\varphi(\lambda\boldsymbol{a})+\psi(\lambda\boldsymbol{a})=\lambda\varphi(\boldsymbol{a})+\lambda\psi(\boldsymbol{a})=\\&=\lambda(\varphi(\boldsymbol{a})+\psi(\boldsymbol{a}))=\lambda((\varphi+\psi)(\boldsymbol{a})).\end{aligned}$$

Таким образом, $\varphi+\psi$ есть линейное отображение $\mathcal{U}$ в $\mathfrak{V}$.

Произведение $\lambda\varphi$ удовлетворяет условиям линейности. Действительно, для любых $\boldsymbol{a}, \boldsymbol{b}\in U$ и любого $\lambda\in F$ имеем:

$$\begin{aligned}(\lambda\varphi)(\boldsymbol{a}+\boldsymbol{b})&=\lambda(\varphi(\boldsymbol{a}+\boldsymbol{b}))=\lambda(\varphi(\boldsymbol{a})+\varphi(\boldsymbol{b}))=\\&=\lambda\varphi(\boldsymbol{a})+\lambda\varphi(\boldsymbol{b})=(\lambda\varphi)(\boldsymbol{a})+(\lambda\varphi)(\boldsymbol{b});\end{aligned}$$

$$\begin{aligned}(\lambda\varphi)(\mu\boldsymbol{a})&=\lambda\varphi(\mu\boldsymbol{a})=\lambda(\mu\varphi(\boldsymbol{a}))=(\lambda\mu)\varphi(\boldsymbol{a})=\\&=\mu(\lambda\varphi(\boldsymbol{a}))=\mu((\lambda\varphi)(\boldsymbol{a})).\end{aligned}$$

Следовательно, $\lambda\varphi$ есть линейное отображение $\mathcal{U}$ в $\mathfrak{V}$. □

СЛЕДСТВИЕ 1.6. *Множество* $\mathrm{Hom}(\mathcal{U}, \mathfrak{V})$ *замкнуто относительно сложения и умножения на скаляры.*

Упражнения

1. Пусть φ — линейный оператор одномерного векторного пространства $\mathcal{V}$ над полем $\mathcal{F}$. Докажите, что существует такой скаляр $\lambda\in F$, что $\varphi(x)=\lambda x$ для любого вектора $x\in V$.

2. Пусть φ и ψ — линейные операторы конечномерного векторного пространства и $\varphi\psi=0$. Будет ли $\psi\varphi=0$?

3. Пусть φ — линейное отображение векторного пространства $\mathcal{U}$ в пространстве $\mathcal{V}$ и $\boldsymbol{b}\in\mathrm{Im}\,\varphi$. Докажите, что множество $\varphi^{-1}(\boldsymbol{b})$ $(\varphi^{-1}(\boldsymbol{b})=\{x\in V\mid\varphi(x)=\boldsymbol{b}\})$ является линейным многообразием пространства $\mathcal{U}$ с направлением $\mathcal{K}er\,\varphi$.

4. Пусть φ — линейное отображение векторного пространства $\mathcal{U}$ в пространство $\mathcal{V}$ и $a_1, \ldots, a_m \in U$. Докажите, что если система $\varphi(a_1), \ldots, \varphi(a_m)$ линейно независима в $\mathcal{V}$, то система $a_1, \ldots, a_m$ линейно независима в $\mathcal{U}$.

5. Пусть φ — инъективное линейное отображение векторного пространства $\mathcal{U}$ в пространство $\mathcal{V}$. Докажите, что если система $a_1, \ldots, a_m$ линейно независима в $\mathcal{U}$, то система $\varphi(a_1), \ldots, \varphi(a_m)$ линейно независима в $\mathcal{V}$.

6. Докажите, что линейное отображение φ векторного пространства $\mathcal{U}$ в пространство $\mathcal{V}$ инъективно тогда и только тогда, когда $\mathcal{K}er\,\varphi = \{0\}$.

7. Пусть φ — линейное отображение n-мерного векторного пространства $\mathcal{U}$ на n-мерное пространство $\mathcal{V}$. Докажите, что φ есть изоморфизм.

8. Пусть φ — линейное отображение векторного пространства $\mathcal{U}$ на одномерное пространство $\mathcal{V}$ и $a \in U \setminus \operatorname{Ker}\varphi$. Докажите, что $\mathcal{U} = \mathcal{K}er\,\varphi \oplus \mathcal{L}(a)$.

9. Пусть φ, ψ — линейные операторы векторного пространства $\mathcal{V}$ такие, что $\operatorname{Ker}\varphi = \operatorname{Ker}\psi = \{0\}$. Докажите, что $\operatorname{Ker}(\varphi\psi) = \{0\}$.

10. Пусть φ есть линейный оператор векторного пространства $\mathcal{V}$, удовлетворяющий условию $\varphi \circ \varphi = \varphi$. Покажите, что $\mathcal{V} = \mathcal{K}er\,\varphi \oplus \mathcal{I}m\,\varphi$.

11. Пусть $\mathcal{U}$ и $\mathcal{V}$ — векторные пространства над полем $\mathcal{F}$, причем пространство $\mathcal{U}$ одномерное. Докажите, что всякое ненулевое отображение $\mathcal{U}$ в $\mathcal{V}$ является инъективным.

12. Пусть $\mathcal{H}om(\mathcal{U}, \mathcal{V})$ — векторное пространство всех линейных отображений конечномерного векторного пространства $\mathcal{U}$ в конечномерное пространство $\mathcal{V}$. Докажите, что

(a) если $\dim \mathcal{U} = 1$, то $\dim(\mathcal{H}om(\mathcal{U}, \mathcal{V})) = \dim \mathcal{V}$,

(b) если $\dim \mathcal{V} = 1$, то $\dim(\mathcal{H}om(\mathcal{U}, \mathcal{V})) = \dim \mathcal{U}$.

13. Пусть $\mathcal{U}$ и $\mathcal{V}$ — конечномерные векторные пространства, размерности которых m и n. Докажите, что размерность векторного пространства $\mathcal{H}om(\mathcal{U}, \mathcal{V})$ равна произведению mn.

14. Пусть φ — линейное отображение конечномерного векторного пространства $\mathcal{U}$ в векторное пространство $\mathcal{V}$. Докажите, что $\dim(\mathcal{K}er\,\varphi) + \dim(\mathcal{I}m\,\varphi) = \dim \mathcal{U}$.

15. Пусть φ — линейное отображение векторного пространства $\mathcal{U}$ в конечномерное векторное пространство $\mathcal{V}$. Пусть $a_1, \ldots, a_m$ — такая система векторов пространства $\mathcal{U}$, что система $\varphi(a_1), \ldots, \varphi(a_m)$ является базисом пространства $\mathcal{I}m\,\varphi$. Докажите, что $\mathcal{U} = \mathcal{K}er\,\varphi \oplus \mathcal{L}(a_1, \ldots, a_m)$.

16. Пусть φ — линейный оператор конечномерного векторного пространства $\mathcal{V}$ над полем $\mathcal{F}$. Докажите, что для достаточно большого натурального числа m линейные операторы $\varphi, \varphi^2, \ldots, \varphi^m$ линейно зависимы над полем $\mathcal{F}$.

§ 2. ПРЕДСТАВЛЕНИЕ ЛИНЕЙНЫХ ОПЕРАТОРОВ МАТРИЦАМИ

Матрица линейного оператора. Пусть $\mathcal{V}$ — конечномерное векторное пространство над полем $\mathcal{F}$,

(1) $e_1, \ldots, e_n$

— его базис и φ — линейный оператор пространства $\mathcal{V}$.

Представим векторы $\varphi(e_1), \ldots, \varphi(e_n)$ в виде линейных комбинаций векторов базиса (1):

$$(2)\quad \begin{aligned} \varphi(e_1) &= \alpha_{11}e_1 + \ldots + \alpha_{n1}e_n, \\ &\ldots\ldots\ldots\ldots\ldots \\ \varphi(e_n) &= \alpha_{1n}e_1 + \ldots + \alpha_{nn}e_n. \end{aligned}$$

ОПРЕДЕЛЕНИЕ. Матрица $M(\varphi)$

$$M(\varphi) = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \cdot & \cdot & \cdot \\ \alpha_{n1} & \ldots & \alpha_{nn} \end{bmatrix},$$

k-й столбец которой есть координатный столбец вектора $\varphi(e_k)$ относительно базиса (1), называется *матрицей линейного оператора* φ *относительно базиса* (1).

Напомним, что $F^{n\times n}$ обозначает множество всех $n\times n$-матриц над полем $\mathscr{F}$.

ТЕОРЕМА 2.1. *Пусть* $\mathscr{V}$ *— векторное пространство над полем* $\mathscr{F}$ *с фиксированным базисом* (1). *Отображение* Φ, *ставящее в соответствие каждому линейному оператору* φ *пространства* $\mathscr{V}$ *его матрицу* $M(\varphi)$ *относительно базиса* (1), *является биективным отображением множества* $\mathrm{Hom}(\mathscr{V}, \mathscr{V})$ *на множество* $F^{n\times n}$.

Доказательство. Ясно, что Φ — отображение на множество $F^{n\times n}$. Докажем, что отображение Φ инъективно, т. е. что для любых φ и ψ из равенства $M(\varphi) = M(\psi)$ следует равенство $\varphi = \psi$. Из $M(\varphi) = M(\psi)$ следуют равенства

$$M(\varphi(e_k)) = M(\psi(e_k)) \text{ для } k = 1, \ldots, n,$$

откуда

$$\varphi(e_k) = \psi(e_k) \text{ для } k = 1, \ldots, n.$$

Согласно следствию 1.2, отсюда следует равенство $\varphi = \psi$. □

Пусть λ — скаляр, $\lambda \in F$. Обозначим через ω'_λ унарную операцию в множестве $\mathrm{Hom}(\mathscr{U}, \mathscr{V})$, ставящую в соответствие каждому линейному отображению $\varphi \in \mathrm{Hom}(\mathscr{U}, \mathscr{V})$ линейное отображение $\lambda\varphi$:

$$\omega'_\lambda(\varphi) = \lambda\varphi.$$

Эту операцию будем называть *операцией умножения на скаляр* λ.

ТЕОРЕМА 2.2. *Пусть* $\mathcal{U}$, $\mathcal{V}$ — *векторные пространства над полем* $\mathcal{F}$. *Алгебра*

$$\langle \mathrm{Hom}(\mathcal{U}, \mathcal{V}),\ +,\ -,\ \{\omega'_\lambda \mid \lambda \in F\}\rangle$$

является векторным пространством над полем $\mathcal{F}$.

Доказательство. Согласно следствию 1.2, множество $\mathrm{Hom}(\mathcal{U}, \mathcal{V})$ замкнуто относительно сложения и унарных операций ω'_λ умножения на скаляры из поля $\mathcal{F}$.

Отметим, что через «—» обозначается унарная операция в множестве $\mathrm{Hom}(\mathcal{U}, \mathcal{V})$, ставящая в соответствие каждому оператору $\varphi \in \mathrm{Hom}(\mathcal{U}, \mathcal{V})$ оператор $-\varphi = (-1)\varphi$, и через $\bar{0}$ — нулевое отображение $\mathcal{U}$ в $\mathcal{V}$. Алгебра $\langle \mathrm{Hom}(\mathcal{U}, \mathcal{V}),\ +,\ -\rangle$ является абелевой группой. Действительно, легко проверить, что для любых φ, ψ, $\chi \in \mathrm{Hom}(\mathcal{U}, \mathcal{V})$ выполняются равенства

$$\varphi + \psi = \psi + \varphi, \qquad \varphi + \bar{0} = \varphi,$$
$$\varphi + (\psi + \chi) = (\varphi + \psi) + \chi, \qquad \varphi + (-\varphi) = \bar{0}.$$

Кроме того, легко проверить, что для любых λ, $\mu \in F$

$$\lambda(\varphi + \psi) = \lambda\varphi + \lambda\psi, \qquad (\lambda\mu)\varphi = \lambda(\mu\varphi),$$
$$(\lambda + \mu)\varphi = \lambda\varphi + \mu\varphi, \qquad 1 \cdot \varphi = \varphi.$$

Таким образом, выполняются все аксиомы векторного пространства. □

Векторное пространство

$$\langle \mathrm{Hom}(\mathcal{U}, \mathcal{V}),\ +,\ -,\ \{\omega'_\lambda \mid \lambda \in F\}\rangle$$

будем называть *векторным пространством линейных отображений* $\mathcal{U}$ в $\mathcal{V}$ и обозначать через $\mathcal{H}om(\mathcal{U}, \mathcal{V})$.

Связь между координатными столбцами векторов x и $\varphi(x)$. Пусть

(1) $e_1, \ldots, e_n$

— фиксированный базис векторного пространства $\mathcal{V}$ и φ — линейный оператор этого пространства. Пусть, далее,

$$x = \xi_1 e_1 + \ldots + \xi_n e_n \quad \text{и} \quad \varphi(x) = \eta_1 e_1 + \ldots + \eta_n e_n.$$

Обозначим через $M(x)$ и $M(\varphi(x))$ координатные столбцы соответственно векторов x и $\varphi(x)$ относительно фиксиро-

ванного базиса (1):

$$M(\boldsymbol{x})=\begin{bmatrix}\xi_1\\ \vdots\\ \xi_n\end{bmatrix},\quad M(\varphi(\boldsymbol{x}))=\begin{bmatrix}\eta_1\\ \vdots\\ \eta_n\end{bmatrix}.$$

Найдем связь между этими координатными столбцами.

ТЕОРЕМА 2.3. *Пусть* φ *— линейный оператор векторного пространства* $\mathcal{V}$ *и* $M(\varphi)$ *— матрица оператора* φ *относительно базиса* (1). *Тогда для любого вектора* $\boldsymbol{x}\in V$ *выполняется равенство*

$$M(\varphi(\boldsymbol{x}))=M(\varphi)\,M(\boldsymbol{x}).$$

Доказательство. Пусть

$$M(\varphi)=\begin{bmatrix}\alpha_{11} & \dots & \alpha_{1n}\\ \dots & \dots & \dots\\ \alpha_{n1} & \dots & \alpha_{nn}\end{bmatrix},$$

тогда выполняются равенства (2). Если $\boldsymbol{x}=\xi_1\boldsymbol{e}_1+\dots+\xi_n\boldsymbol{e}_n\in V$, то

$$\varphi(\boldsymbol{x})=\xi_1\varphi(\boldsymbol{e}_1)+\dots+\xi_n\varphi(\boldsymbol{e}_n).$$

Заменяя в этом равенстве векторы $\varphi(\boldsymbol{e}_1),\ \dots,\ \varphi(\boldsymbol{e}_n)$ на основании (2), получаем

$$\varphi(\boldsymbol{x})=\xi_1(\alpha_{11}\boldsymbol{e}_1+\dots+\alpha_{n1}\boldsymbol{e}_n)+\dots+\xi_n(\alpha_{1n}\boldsymbol{e}_1+\dots+\alpha_{nn}\boldsymbol{e}_n),$$

откуда

$$\varphi(\boldsymbol{x})=(\alpha_{11}\xi_1+\dots+\alpha_{1n}\xi_n)\,\boldsymbol{e}_1+\dots+(\alpha_{n1}\xi_1+\dots+\alpha_{nn}\xi_n)\,\boldsymbol{e}_n.$$

Следовательно,

$$M(\varphi(\boldsymbol{x}))=\begin{bmatrix}\alpha_{11}\xi_1+\dots+\alpha_{1n}\xi_n\\ \dots\dots\dots\dots\\ \alpha_{n1}\xi_1+\dots+\alpha_{nn}\xi_n\end{bmatrix}=\begin{bmatrix}\alpha_{11} & \dots & \alpha_{1n}\\ \dots & \dots & \dots\\ \alpha_{n1} & \dots & \alpha_{nn}\end{bmatrix}\cdot\begin{bmatrix}\xi_1\\ \vdots\\ \xi_n\end{bmatrix},$$

т. е. $M(\varphi(\boldsymbol{x}))=M(\varphi)\,M(\boldsymbol{x})$. □

ТЕОРЕМА 2.4. *Пусть* φ *— линейный оператор векторного пространства* $\mathcal{V}$ *и* $M(\varphi)$ *— матрица оператора* φ *относительно фиксированного базиса* (1). *Если для любого вектора* $\boldsymbol{x}\in V$

(3) $M(\varphi(\boldsymbol{x}))=BM(\boldsymbol{x})$,

то $B=M(\varphi)$.

Доказательство. Согласно определению матрицы $M(\varphi)$,

$$(4)\quad M(\varphi)=(M(\varphi(\boldsymbol{e}_1)),\ M(\varphi(\boldsymbol{e}_2)),\ \ldots,\ M(\varphi(\boldsymbol{e}_n))).$$

Подставив в (3) вместо $\boldsymbol{x}$ последовательно базисные векторы $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$, получим

$$M(\varphi(\boldsymbol{e}_1))=BM(\boldsymbol{e}_1)=B\begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}=B^1;$$

$$(5)\quad M(\varphi(\boldsymbol{e}_2))=BM(\boldsymbol{e}_2)=B\begin{bmatrix}0\\1\\\vdots\\0\end{bmatrix}=B^2;$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$M(\varphi(\boldsymbol{e}_n))=BM(\boldsymbol{e}_n)=B\begin{bmatrix}0\\0\\\vdots\\1\end{bmatrix}=B^n.$$

На основании (4) и (5) заключаем, что соответствующие столбцы матриц $M(\varphi)$ и B совпадают. Следовательно, $M(\varphi)=B$. □

ПРЕДЛОЖЕНИЕ 2.5. *Пусть* φ *и* ψ *— линейные операторы векторного пространства* $\mathcal{V}$ *с фиксированным базисом* $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ *и* $\lambda \in F$; *тогда*

(1) $M(\varphi+\psi)=M(\varphi)+M(\psi)$;

2) $M(\lambda\varphi)=\lambda M(\varphi)$.

Доказательство. Пусть $\boldsymbol{x}\in V$ и

$$(3)\quad \begin{aligned}\varphi(\boldsymbol{x})&=\xi_1\boldsymbol{e}_1+\ldots+\xi_n\boldsymbol{e}_n;\\ \psi(\boldsymbol{x})&=\eta_1\boldsymbol{e}_1+\ldots+\eta_n\boldsymbol{e}_n,\end{aligned}$$

тогда

$$(\varphi+\psi)(\boldsymbol{x})=(\xi_1+\eta_1)\boldsymbol{e}_1+\ldots+(\xi_n+\eta_n)\boldsymbol{e}_n.$$

Следовательно,

$$M((\varphi+\psi)(\boldsymbol{x}))=\begin{bmatrix}\xi_1+\eta_1\\ \dots\\ \xi_n+\eta_n\end{bmatrix}=\begin{bmatrix}\xi_1\\ \vdots\\ \xi_n\end{bmatrix}+\begin{bmatrix}\eta_1\\ \vdots\\ \eta_n\end{bmatrix}=$$
$$=M(\varphi(\boldsymbol{x}))+M(\psi(\boldsymbol{x}))$$

и, по теореме 2.3,

(4) $M((\varphi+\psi)(\boldsymbol{x}))=(M(\varphi)+M(\psi))\,M(\boldsymbol{x})$.

Равенство (4) верно для любого $\boldsymbol{x}\in V$. По теореме 2.4, из (4) следует равенство (1).

В силу (3) $(\lambda\varphi)(\boldsymbol{x})=\lambda\xi_1\boldsymbol{e}_1+\dots+\lambda\xi_n\boldsymbol{e}_n$; следовательно,

$M((\lambda\varphi)(\boldsymbol{x}))=\lambda M(\varphi(\boldsymbol{x}))$

и, по теореме 2.3, для любого $\boldsymbol{x}$

(5) $M((\lambda\varphi)(\boldsymbol{x}))=(\lambda M(\varphi))\,M(\boldsymbol{x})$.

Согласно теореме 2.4, из (5) следует (2). □

Ранг линейного оператора. Установим связь между рангом линейного оператора и рангом его матрицы.

ТЕОРЕМА 2.6. *Ранг линейного оператора конечномерного ненулевого векторного пространства равен рангу матрицы этого оператора.*

Доказательство. Пусть $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ — фиксированный базис векторного пространства $\mathscr{V}$. Пусть $M(\varphi(\boldsymbol{e}_1)), \dots$ $\dots, M(\varphi(\boldsymbol{e}_n))$ — координатные столбцы векторов $\varphi(\boldsymbol{e}_1), \dots$ $\dots, \varphi(\boldsymbol{e}_n)$ относительно фиксированного базиса. Они являются столбцами матрицы $M(\varphi)$ оператора φ относительно фиксированного базиса, т. е.

$$M(\varphi)=(M(\varphi(\boldsymbol{e}_1)),\ \dots,\ M(\varphi(\boldsymbol{e}_n))).$$

Следовательно,

(1) ранг $M(\varphi)=$ ранг $(M(\varphi(\boldsymbol{e}_1)),\ \dots,\ M(\varphi(\boldsymbol{e}_n)))$.

В силу следствия 7.3 ранг системы векторов $\varphi(\boldsymbol{e}_1), \dots$ $\dots, \varphi(\boldsymbol{e}_n)$ равен рангу системы столбцов этих векторов. Отсюда и из (1) следует, что

(2) ранг $M(\varphi)=$ ранг $(\varphi(\boldsymbol{e}_1),\ \dots,\ \varphi(\boldsymbol{e}_n))$.

Пусть $\boldsymbol{x}$ — произвольный вектор пространства $\mathscr{V}$ и $\boldsymbol{x}=\xi_1\boldsymbol{e}_1+\dots+\xi_n\boldsymbol{e}_n$. В силу линейности оператора φ выполняется равенство $\varphi(\boldsymbol{x})=\xi_1\varphi(\boldsymbol{e}_1)+\dots+\xi_n\varphi(\boldsymbol{e}_n)$. Поэтому

$$\operatorname{Im}(\varphi)=L(\varphi(\boldsymbol{e}_1),\ \dots,\ \varphi(\boldsymbol{e}_n)),$$

т. е. образ оператора φ порождается векторами $\varphi(e_1), \ldots, \varphi(e_n)$. Согласно следствию 7.3, отсюда следует, что

(3) $\text{ранг}\,\varphi = \text{ранг}\,(\varphi(e_1), \ldots, \varphi(e_n))$.

На основании (2) и (3) заключаем, что ранг φ равен рангу матрицы $M(\varphi)$. □

Связь между координатными столбцами вектора относительно различных базисов. Пусть $\mathcal{V}$ — ненулевое n-мерное векторное пространство над полем $\mathcal{F}$. Пусть даны два базиса этого пространства: $e_1, \ldots, e_n$ — первый базис, $e'_1, \ldots, e'_n$ — второй базис. Векторы второго базиса представим в виде линейных комбинаций первого базиса:

$$(1)\quad \begin{aligned} e'_1 &= t_{11}e_1 + \ldots + t_{n1}e_n \\ &\cdots\cdots\cdots\cdots \\ e'_n &= t_{1n}e_1 + \ldots + t_{nn}e_n \end{aligned} \qquad (t_{ik} \in F).$$

Матрицей перехода от первого базиса ко второму называется матрица T,

$$T = \begin{bmatrix} t_{11} & t_{12} \ldots t_{1n} \\ t_{21} & t_{22} \ldots t_{2n} \\ \cdots & \cdots\cdots \\ t_{n1} & t_{n2} \ldots t_{nn} \end{bmatrix},$$

k-й столбец которой является координатным столбцом вектора e'_k относительно первого базиса.

ПРЕДЛОЖЕНИЕ 2.7. *Матрица T обратима.*

Доказательство. Из линейной независимости векторов $e'_1, \ldots, e'_n$ следует линейная независимость координатных столбцов этих векторов, т. е. линейная независимость столбцов матрицы T (см. следствие 7.4). Согласно теореме 5.1, отсюда следует, что матрица T обратима. □

Координатный столбец вектора $x \in V$ относительно первого базиса обозначим через $M(x)$, относительно второго — через $M'(x)$. Найдем связь между $M(x)$ и $M'(x)$.

ТЕОРЕМА 2.8. *Пусть $M(x)$ и $M'(x)$ — координатные столбцы вектора x соответственно относительно первого и второго базисов и T — матрица перехода от первого базиса пространства ко второму. Тогда выполняются равенства*

(2) $M(x) = TM'(x)$;

(3) $M'(x) = T^{-1}M(x)$.

Доказательство. Пусть $x \in V$ и

(4) $x = \xi_1 e_1 + \ldots + \xi_n e_n$,

(5) $x = \xi'_1 e'_1 + \ldots + \xi'_n e'_n$;

следовательно,

$$M(x) = \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix}, \quad M'(x) = \begin{bmatrix} \xi'_1 \\ \vdots \\ \xi'_n \end{bmatrix}$$

Подставив в (5) выражения для $e'_1, \ldots, e'_n$ из равенств (1), получим

$$x = \xi'_1 (t_{11} e_1 + \ldots + t_{n1} e_n) + \ldots + \xi'_n (t_{1n} e_1 + \ldots + t_{nn} e_n),$$

откуда

(6) $x = (t_{11}\xi'_1 + \ldots + t_{1n}\xi'_n) e_1 + \ldots + (t_{n1}\xi'_1 + \ldots + t_{nn}\xi'_n) e_n$.

Из (4) и (6) следуют равенства

$$\xi_1 = t_{11}\xi'_1 + \ldots + t_{1n}\xi'_n;$$

$$\ldots\ldots\ldots\ldots$$

$$\xi_n = t_{n1}\xi'_1 + \ldots + t_{nn}\xi'_n.$$

Отсюда получаем равенство

$$\begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix} = T \begin{bmatrix} \xi'_1 \\ \vdots \\ \xi'_n \end{bmatrix},$$

т. е. $M(x) = TM'(x)$. Умножив слева обе части этого равенства на T^{-1}, получим (3). □

СЛЕДСТВИЕ 2.9. *Если* ${}^tM(x)$ и ${}^tM'(x)$ — *координатные строки вектора* x *соответственно относительно первого и второго базисов, то*

$${}^tM(x) = {}^tM'(x)\,{}^tT, \quad {}^tM'(x) = {}^tM(x)\,{}^t(T^{-1}).$$

Связь между матрицами линейного оператора относительно различных базисов. Пусть $\mathcal{V}$ — ненулевое конечномерное векторное пространство, $e_1, \ldots, e_n$ — первый базис пространства $\mathcal{V}$, $e'_1, \ldots, e'_n$ — второй базис пространства $\mathcal{V}$ и T — матрица перехода от первого базиса ко второму.

ТЕОРЕМА 2.10. *Пусть* φ — *линейный оператор векторного пространства* $\mathcal{V}$, $M(\varphi)$ и $M'(\varphi)$ — *матрицы этого оператора соответственно относительно первого и второго базисов и* T — *матрица перехода от первого базиса ко второму, тогда* $M'(\varphi) = T^{-1}M(\varphi)\,T$.

Доказательство. Согласно теореме 2.8, для всякого $x \in V$

(2) $M(x) = TM'(x)$;

(3) $M'(x) = T^{-1}M(x)$,

где $M(x)$ и $M'(x)$ — координатные столбцы вектора x соответственно относительно первого и второго базисов. Заменяя в (3) x на $\varphi(x)$, получаем

$$M'(\varphi(x)) = T^{-1}M(\varphi(x)).$$

По теореме 2.3, $M(\varphi(x)) = M(\varphi)M(x)$, следовательно,

$$M'(\varphi(x)) = T^{-1}M(\varphi)M(x).$$

Ввиду (2) отсюда получаем

$$M'(\varphi(x)) = [T^{-1}M(\varphi)T]M'(x).$$

Так как это равенство верно для любого x из V, то, по теореме 2.4, $M'(\varphi) = T^{-1}M(\varphi)T$. □

ОПРЕДЕЛЕНИЕ. Матрицы A и B из множества $F^{n\times n}$ называются *подобными над полем* $\mathcal{F}$, если существует такая обратимая матрица $T \in F^{n\times n}$, что $A = T^{-1}BT$.

Из теоремы 2.10 вытекает следующее следствие.

СЛЕДСТВИЕ 2.11. *Если* φ *— линейный оператор конечномерного ненулевого векторного пространства* $\mathcal{V}$, *то матрицы этого оператора относительно любых двух базисов пространства подобны.*

ПРЕДЛОЖЕНИЕ 2.12. *Отношение подобия матриц на множестве* $F^{n\times n}$ *есть отношение эквивалентности.*

Доказательство. Отношение подобия рефлексивно, так как $A = E^{-1}AE$, где E — единичная матрица. Отношение подобия симметрично, так как из равенства $A = T^{-1}BT$ следует $B = (T^{-1})^{-1}AT^{-1}$. Отношение подобия транзитивно, так как из $A = T^{-1}BT$ и $B = T_1^{-1}CT_1$ следует

$$A = (T_1T)^{-1}C(T_1T).$$

Отношение подобия матриц над полем $\mathcal{F}$ определяет разбиение множества $F^{n\times n}$ на классы эквивалентности, которые называются *классами подобных матриц*. Каждому линейному оператору векторного пространства $\mathcal{V}$ соответствует единственный класс подобных матриц.

Упражнения

1. Как изменится матрица линейного оператора, если в базисе $e_1, \ldots, e_n$ переставить какие-нибудь два вектора, например e_1 и e_2?

2. Докажите, что ранг линейного оператора конечномерного векторного пространства равен рангу матрицы этого оператора.

3. Покажите, что всякий линейный оператор ранга r конечномерного векторного пространства можно представить в виде суммы r линейных операторов ранга 1.

4. Пусть $\mathscr{V}$ — векторное пространство всех квадратных матриц второго порядка над полем $\mathscr{F}$. Покажите, что преобразование φ, состоящее в умножении матриц из $\mathscr{V}$ слева на матрицу $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$, есть линейный оператор. Найдите матрицу оператора φ в базисе $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$.

5. Докажите, что линейный оператор φ конечномерного векторного пространства $\mathscr{V}$, перестановочный с каждым линейным оператором пространства $\mathscr{V}$, есть скаляр, т. е. существует такой скаляр λ, что $\varphi(x) = \lambda x$ для любого вектора x из $\mathscr{V}$.

6. Пусть φ — произвольный, ψ — обратимый линейный оператор конечномерного векторного пространства. Докажите, что ранг $(\varphi\psi) = $ ранг $(\psi\varphi) =$ ранг φ.

7. Пусть φ, ψ — произвольные линейные операторы конечномерного векторного пространства. Докажите, что:

(a) ранг $(\varphi+\psi) \leqslant$ ранг $\varphi +$ ранг ψ;

(b) ранг $(\varphi\psi) \leqslant$ ранг φ, ранг $(\varphi\psi) \leqslant$ ранг ψ;

(c) деф $\varphi \leqslant$ деф $(\varphi\psi) \leqslant$ деф $\varphi +$ деф ψ.

8. Приведите пример линейных операторов φ, ψ двумерного векторного пространства, для которых ранг $(\varphi, \psi) \neq$ ранг $(\psi\varphi)$.

9. Докажите, что для любых линейных операторов φ, ψ n-мерного векторного пространства выполняется неравенство

ранг $(\varphi\psi) \geqslant$ ранг $\varphi +$ ранг $\psi - n$.

10. Пусть φ — линейный оператор векторного пространства $\mathscr{V}$. Подпространство $\mathscr{L}$ пространства $\mathscr{V}$ называется *инвариантным относительно* φ, если $\varphi(L) \subset L$. Пусть относительно базиса $e_1, \ldots, e_n$ оператор φ имеет диагональную матрицу с различными диагональными элементами. Найдите все подпространства пространства $\mathscr{V}$, инвариантные относительно φ, и покажите, что число их равно 2^n.

§ 3. ЛИНЕЙНЫЕ АЛГЕБРЫ

Линейная алгебра. Пусть $\mathscr{F}$ — поле скаляров.

ОПРЕДЕЛЕНИЕ. Алгебра $\langle V, +, \{\omega_\lambda \mid \lambda \in F\}, \cdot \rangle$ называется *линейной алгеброй*, если бинарные операции $+$, $\cdot$ и унарные операции ω_λ удовлетворяют следующим требованиям:

1) алгебра $\langle V, +, \{\omega_\lambda \mid \lambda \in F\} \rangle$ есть векторное пространство над полем $\mathscr{F}$;

2) выполняются условия билинейности, т. е.

$$(a+b)c = ac + bc, \quad c(a+b) = ca + cb,$$
$$\omega_\lambda(ab) = (\omega_\lambda a)b = a(\omega_\lambda b)$$

для любых a, b, $c \in V$ и любого $\lambda \in F$.

Рангом линейной алгебры называется размерность векторного пространства $\langle V, +, \{\omega_\lambda \mid \lambda \in F\}\rangle$

Примеры. 1. Пусть $\mathbf{C}$ — множество всех комплексных чисел. Алгебра

$$\langle \mathbf{C}, +, \{\omega_\lambda \mid \lambda \in \mathbf{R}\}, \cdot \rangle$$

есть линейная алгебра над полем $\mathscr{R}$ действительных чисел. Ее ранг равен двум.

2. Пусть $F^{n\times n}$ — множество всех $n\times n$-матриц над полем. Алгебра

$$\langle F^{n\times n}, +, \{\omega_\lambda \mid \lambda \in F\}, \cdot \rangle,$$

где ω_λ — унарная операция умножения на скаляр λ, является линейной алгеброй над полем $\mathscr{F}$ ранга n^2. Она называется *полной матричной алгеброй над полем* $\mathscr{F}$. Ее ранг равен n^2.

3. Алгебра кватернионов над полем $\mathscr{R}$. Пусть $\mathscr{V}$ — четырехмерное векторное пространство над полем $\mathscr{R}$ и $\boldsymbol{e}$, $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$ — его базис. Определим умножение базисных векторов следующими равенствами:

$$\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -\boldsymbol{e},\ \boldsymbol{ij} = -\boldsymbol{ji} = \boldsymbol{k},\ \boldsymbol{jk} = -\boldsymbol{kj} = \boldsymbol{i},$$
$$\boldsymbol{ki} = -\boldsymbol{ik} = \boldsymbol{j};$$
$$\boldsymbol{ae} = \boldsymbol{ea} \text{ для любого вектора } \boldsymbol{a} \in \{\boldsymbol{e}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}.$$

Произведение любых двух кватернионов определяется равенством

$$(\alpha\boldsymbol{e} + \beta\boldsymbol{i} + \gamma\boldsymbol{j} + \delta\boldsymbol{k})(\alpha_1\boldsymbol{e} + \beta_1\boldsymbol{i} + \gamma_1\boldsymbol{j} + \delta_1\boldsymbol{k}) =$$
$$= (\alpha\alpha_1 - \beta\beta_1 - \gamma\gamma_1 - \delta\delta_1)\boldsymbol{e} +$$
$$+ (\alpha\beta_1 + \beta\alpha_1 + \gamma\delta_1 - \delta\gamma_1)\boldsymbol{i} +$$
$$+ (\alpha\gamma_1 + \alpha_1\gamma + \delta\beta_1 - \beta\delta_1)\boldsymbol{j} +$$
$$+ (\alpha\delta_1 + \alpha_1\delta + \beta\gamma_1 - \gamma\beta_1)\boldsymbol{k}.$$

Кватернионы $\boldsymbol{q} = \alpha\boldsymbol{e} + \beta\boldsymbol{i} + \gamma\boldsymbol{j} + \delta\boldsymbol{k}$ и $\overline{\boldsymbol{q}} = \alpha\boldsymbol{e} - \beta\boldsymbol{i} - \gamma\boldsymbol{j} - \delta\boldsymbol{k}$ называются *сопряженными*. Действительное число

$$N(\boldsymbol{q}) = \boldsymbol{q}\cdot\overline{\boldsymbol{q}} = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$$

называется *нормой кватерниона*.

Непосредственная проверка показывает, что выполняются условия билинейности. Таким образом, алгебра

$$\langle V, +, \{\omega_\lambda \mid \lambda \in \mathbf{R}\}, \cdot \rangle$$

является линейной. Она называется *алгеброй кватернионов* над полем действительных чисел. Легко проверить, что

алгебра $\langle V, +, -, \cdot, e\rangle$ является некоммутативным кольцом, в котором для любых $a, b \in V$ при $a \neq 0$ уравнение $ax = b$ разрешимо.

Алгебра линейных операторов векторного пространства. Пусть $\mathcal{V}$ — векторное пространство над полем $\mathcal{F}$ и φ, ψ — линейные операторы этого пространства. Произведение $\varphi\psi$ определяется как композиция φ и ψ, т. е. как отображение пространства $\mathcal{V}$ в себя, ставящее в соответствие элементу x из V элемент $\varphi(\psi(x))$:

$$(\varphi\psi)(x) = \varphi(\psi(x)).$$

ПРЕДЛОЖЕНИЕ 3.1. *Произведение любых двух линейных операторов векторного пространства $\mathcal{V}$ есть линейный оператор этого пространства.*

Доказательство. Пусть φ и ψ — линейные операторы пространства $\mathcal{V}$. Произведение $\varphi\psi$ удовлетворяет условиям линейности. Действительно, если $x, y \in V$ и $\lambda \in F$, то

$$(\varphi\psi)(x+y) = \varphi(\psi(x+y)) = \varphi(\psi(x)+\psi(y)) =$$
$$= \varphi(\psi(x)) + \varphi(\psi(y)) = (\varphi\psi)(x) + (\varphi\psi)(y);$$
$$(\varphi\psi)(\lambda x) = \varphi(\psi(\lambda x)) = \varphi(\lambda\psi(x)) = \lambda(\varphi(\psi(x))) =$$
$$= \lambda((\varphi\psi)(x)).$$

Таким образом, произведение $\varphi\psi$ есть линейный оператор пространства $\mathcal{V}$. □

Пусть $\mathcal{V}$ — векторное пространство над полем $\mathcal{F}$. В силу следствия 1.6 $\mathcal{H}om(\mathcal{V}, \mathcal{V})$ есть векторное пространство над полем $\mathcal{F}$:

$$\mathcal{H}om(\mathcal{V}, \mathcal{V}) = \langle \mathrm{Hom}(\mathcal{V}, \mathcal{V}), +, \{\omega'_\lambda \mid \lambda \in F\}\rangle,$$

где ω'_λ — унарная операция умножения линейных операторов пространства $\mathcal{V}$ на скаляр λ. Рассмотрим алгебру

$$\langle \mathrm{Hom}(\mathcal{V}, \mathcal{V}), +, \{\omega'_\lambda \mid \lambda \in F\}, \cdot\rangle,$$

где бинарная операция «$\cdot$» есть операция умножения линейных операторов пространства $\mathcal{V}$; эта алгебра называется *алгеброй линейных операторов пространства* $\mathcal{V}$ и обозначается $End\,\mathcal{V}$.

ТЕОРЕМА 3.2. *Пусть $\mathcal{V}$ — векторное пространство над полем $\mathcal{F}$. Алгебра $End\,\mathcal{V}$ является линейной алгеброй над полем $\mathcal{F}$.*

Доказательство. Согласно теореме 2.2, алгебра

$$\langle \mathrm{Hom}(\mathcal{V}, \mathcal{V}), +, \{\omega'_\lambda \mid \lambda \in F\}\rangle$$

есть векторное пространство над полем $\mathscr{F}$. Кроме того, выполнены условия билинейности:

(1) $(\varphi+\psi)\chi=\varphi\chi+\psi\chi$;
(2) $\chi(\varphi+\psi)=\chi\varphi+\chi\psi$;
(3) $\lambda(\varphi\psi)=(\lambda\varphi)\psi=\varphi(\lambda\psi)$,

где $\varphi,\ \psi,\ \chi\subset \mathrm{Hom}(\mathscr{V},\ \mathscr{V})$ и $\lambda\in F$.

Докажем равенство (1). Если $\boldsymbol{x}\in V$, то

$$((\varphi+\psi)\chi)(\boldsymbol{x})=(\varphi+\psi)(\chi(\boldsymbol{x}))=\varphi(\chi(\boldsymbol{x}))+\psi(\chi(\boldsymbol{x}))=$$
$$=(\varphi\chi)(\boldsymbol{x})+(\psi\chi)(\boldsymbol{x})=(\varphi\chi+\psi\chi)(\boldsymbol{x}),$$

т. е. имеет место (1). Аналогично доказывается (2).

Докажем первое из равенств (3). Если $\boldsymbol{x}\in V$, то

$$(\lambda(\varphi\psi))(\boldsymbol{x})=\lambda((\varphi\psi)(\boldsymbol{x}))=\lambda(\varphi(\psi(\boldsymbol{x})))=(\lambda\varphi)(\psi(\boldsymbol{x}))=$$
$$=((\lambda\varphi)\psi)(\boldsymbol{x}),$$

т. е. $\lambda(\varphi\psi)=(\lambda\varphi)\psi$. Аналогично доказывается равенство $(\lambda\varphi)\psi=\varphi(\lambda\psi)$. □

Изоморфизм алгебры линейных операторов и полной матричной алгебры. Пусть $\mathfrak{A}$ и $\mathfrak{A}'$ — линейные алгебры над полем $\mathscr{F}$. Отображение Φ алгебры $\mathfrak{A}$ на алгебру $\mathfrak{A}'$ называется *изоморфизмом*, если оно инъективно и сохраняет главные операции алгебры $\mathfrak{A}$, т. е.

$$\Phi(\boldsymbol{a}+\boldsymbol{b})=\Phi(\boldsymbol{a})+\Phi(\boldsymbol{b}),\ \Phi(\lambda\boldsymbol{a})=\lambda\Phi(\boldsymbol{a}),$$
$$\Phi(\boldsymbol{ab})=\Phi(\boldsymbol{a})\Phi(\boldsymbol{b})$$

для любых $\boldsymbol{a},\ \boldsymbol{b}\in V$ и любого $\lambda\in F$. Алгебры $\mathfrak{A}$ и $\mathfrak{A}'$ называют *изоморфными*, если существует изоморфизм алгебры $\mathfrak{A}$ на алгебру $\mathfrak{A}'$

Легко проверить, что отношение изоморфизма на какой-либо совокупности алгебр над полем $\mathscr{F}$ есть отношение эквивалентности.

Пример. Алгебра комплексных чисел

$$\langle \mathbf{C},\ +,\ \{\omega_\lambda\mid\lambda\in\mathbf{R}\},\ \cdot\rangle$$

изоморфна алгебре всех матриц вида $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ над $\mathscr{R}$:

$$\left\langle\left\{\begin{bmatrix} a & -b \\ b & a \end{bmatrix}\middle|\ a,\ b\in\mathbf{R}\right\},\ +,\ \{\omega_\lambda\mid\lambda\in\mathbf{R}\},\ \cdot\right\rangle.$$

При этом соответствие

$$a+bi\mapsto\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

устанавливает изоморфизм рассматриваемых линейных алгебр.

Обозначим через $\mathfrak{M}(n, \mathscr{F})$ полную матричную алгебру над $\mathscr{F}$:

$$\mathfrak{M}(n, \mathscr{F}) = \langle F^{n \times n}, +, \{\omega_\lambda \mid \lambda \in F\}, \cdot \rangle.$$

ТЕОРЕМА 3.3. *Пусть $\mathscr{V}$ — конечномерное векторное пространство над полем $\mathscr{F}$ с фиксированным базисом $e_1, \ldots, e_n$. Отображение, ставящее в соответствие каждому линейному оператору φ пространства $\mathscr{V}$ его матрицу $M(\varphi)$ относительно фиксированного базиса, является изоморфизмом алгебры линейных операторов $End\,\mathscr{V}$ на полную матричную алгебру $\mathfrak{M}(n, \mathscr{F})$.*

Доказательство. Соответствие $\varphi \longmapsto M(\varphi)$ есть отображение множества $\mathrm{End}\,\mathscr{V} = \mathrm{Hom}(\mathscr{V}, \mathscr{V})$ на множество $\mathscr{F}^{n \times n}$ $n \times n$-матриц. В силу теоремы 2.1 это отображение биективно. Кроме того, оно сохраняет все главные операции алгебры $End\,\mathscr{V}$, т. е.

(1) $M(\varphi + \psi) = M(\varphi) + M(\psi)$,

(2) $M(\lambda\varphi) = \lambda M(\varphi)$,

(3) $M(\varphi\psi) = M(\varphi)\,M(\psi)$

для любых $\varphi, \psi \in \mathrm{Hom}(\mathscr{V}, \mathscr{V})$ и любого $\lambda \in F$. Равенства (1) и (2) были доказаны в предыдущем параграфе.

Докажем равенство (3). Пусть $\boldsymbol{x} \in V$. Тогда $(\varphi\psi)(\boldsymbol{x}) = \varphi(\psi(\boldsymbol{x}))$ и, по теореме 2.3,

$$M((\varphi\psi)(\boldsymbol{x})) = M(\varphi(\psi(\boldsymbol{x}))) = M(\varphi)\,M(\psi(\boldsymbol{x})) = [M(\varphi)\,M(\psi)]\,M(\boldsymbol{x}).$$

Таким образом, для любого вектора $\boldsymbol{x} \in V$

$$M((\varphi\psi)(\boldsymbol{x})) = [M(\varphi)\,M\psi]\,M(\boldsymbol{x}).$$

Согласно теореме 2.4, отсюда следует равенство (3).

Следовательно, рассматриваемое отображение является изоморфизмом алгебры $End\,\mathscr{V}$ на алгебру $\mathfrak{M}(n, \mathscr{F})$.

Упражнения

1. Докажите, что умножение кватернионов ассоциативно.
2. Докажите, что в алгебре кватернионов система уравнений

$$\boldsymbol{ix} + \boldsymbol{jy} = \boldsymbol{e},\ \boldsymbol{kx} - \boldsymbol{ey} = \boldsymbol{i}$$

имеет единственное решение, а система уравнений

$$\boldsymbol{xi} + \boldsymbol{yj} = \boldsymbol{e},\ \boldsymbol{xk} - \boldsymbol{ey} = \boldsymbol{i}$$

решений не имеет.

3. Пусть $a=\alpha e+\beta i+\gamma j+\delta k$ — кватернион и $a^*=\alpha e-\beta i-\gamma j-\delta k$. Покажите, что для любых кватернионов a, b

(a) $N(a)=aa^*=\alpha^2+\beta^2+\gamma^2+\delta^2$;

(b) $N(ab)=N(a)\,N(b)$;

(c) $(ab)^*=b^*a^*$.

4. Покажите, что существует бесконечно много кватернионов, удовлетворяющих уравнению $x^2+e=0$.

5. Пусть $a=\alpha e+\beta i+\gamma j+\delta k$ — любой кватернион. Проверьте, что кватернионы a и a^* являются корнями уравнения $x^2-2\alpha x+N(a)e=0$.

6. Покажите, что если кватернион a не является действительным числом, то существует только два кватерниона, удовлетворяющих уравнению $x^2=a$.

7. Докажите, что для любых двух кватернионов a и b

$$(aa^*)(bb^*)=(ab)(ab)^*,$$

Выведите отсюда, что если каждое из чисел m, n есть сумма квадратов четырех целых чисел, то произведение mn также есть сумма квадратов четырех целых чисел.

8. Докажите, что в алгебре кватернионов каждое из уравнений $ax=b$, $ya=b$ при $a\neq 0$ имеет единственное решение.

9. Покажите, что множество всех отличных от нуля кватернионов образует группу относительно умножения.

10. Покажите, что восемь кватернионов $\pm e$, $\pm i$, $\pm j$, $\pm k$ образуют мультипликативную группу (она называется *группой кватернионов*).

11. Пусть $\mathfrak{A}$ — алгебра ранга n над полем $\mathcal{F}$. Покажите, что при $k>n$ любые k элементов алгебры $\mathfrak{A}$ линейно зависимы над полем $\mathcal{F}$.

12. Пусть I, I, J, K — соответственно комплексные матрицы

$$\begin{bmatrix}1&0\\0&1\end{bmatrix},\ \begin{bmatrix}0&1\\-1&0\end{bmatrix},\ \begin{bmatrix}0&i\\i&0\end{bmatrix},\ \begin{bmatrix}i&0\\0&-i\end{bmatrix},$$

где $i=\sqrt{-1}$. Покажите, что $I^2=J^2=K^2=-I$, $IJ=-JI=K$, $JK=-KJ=I$, $KI=-IK=J$.

13. Докажите, что алгебра матриц вида

$$\begin{bmatrix}\alpha+\beta i&\gamma+\delta i\\-\gamma+\delta i&\alpha-\beta i\end{bmatrix}$$

с действительными α, β, γ, δ и $i=\sqrt{-1}$ изоморфна алгебре кватернионов над полем действительных чисел.

§ 4. ОБРАТИМЫЕ ОПЕРАТОРЫ

Обратимые операторы. Пусть φ — линейный оператор векторного пространства $\mathcal{V}$ и ε — тождественный оператор этого пространства. Оператор φ называется *обратимым*, если существует такой линейный оператор ψ пространства $\mathcal{V}$, что

(1) $\varphi\psi=\varepsilon$, $\psi\varphi=\varepsilon$,

Оператор ψ, удовлетворяющий условиям (1), существует только один. Действительно, если оператор ψ_1 удовлетворяет условиям $\varphi\psi_1 = \varepsilon$, $\psi_1\varphi = \varepsilon$, то

$$\psi_1 = \psi_1\varepsilon = \psi_1(\varphi\psi) = (\psi_1\varphi)\psi = \varepsilon\psi = \psi, \text{ т. е. } \psi_1 = \psi.$$

Линейный оператор ψ, удовлетворяющий условиям (1), называется *обратным к оператору* φ и обозначается φ^{-1}.

ТЕОРЕМА 4.1. *Пусть* φ *— линейный оператор конечномерного ненулевого векторного пространства* $\mathcal{V}$. *Тогда следующие условия равносильны:*

(a) *оператор* φ *обратим*;

(b) φ *есть инъективное отображение* $\mathcal{V}$ *на* $\mathcal{V}$;

(c) $\operatorname{Ker}\varphi = \{\mathbf{0}\}$;

(d) *дефект* $\varphi = 0$;

(e) *ранг* $\varphi = \dim \mathcal{V}$;

(f) *матрица оператора* φ *относительно любого базиса пространства* $\mathcal{V}$ *обратима.*

Доказательство. Пусть φ — обратимый оператор и ψ — оператор, обратный φ. Докажем, что φ инъективно, т. е. для любых $\boldsymbol{a}, \boldsymbol{b} \in V$, из $\varphi(\boldsymbol{a}) = \varphi(\boldsymbol{b})$ следует $\boldsymbol{a} = \boldsymbol{b}$. Действительно, если $\varphi(\boldsymbol{a}) = \varphi(\boldsymbol{b})$, то

$$\psi(\varphi(\boldsymbol{a})) = \psi(\varphi(\boldsymbol{b})),\ (\psi\varphi)(\boldsymbol{a}) = (\psi\varphi)(\boldsymbol{b}),\ \varepsilon(\boldsymbol{a}) = \varepsilon(\boldsymbol{b}),\ \boldsymbol{a} = \boldsymbol{b}.$$

Кроме того, φ есть отображение на V, т. е. для любого $\boldsymbol{a} \in V$ существует прообраз. Действительно,

$$\varphi(\psi(\boldsymbol{a})) = (\varphi\psi)\boldsymbol{a} = \varepsilon\boldsymbol{a} = \boldsymbol{a},$$

т. е. $\psi(\boldsymbol{a})$ есть прообраз элемента $\boldsymbol{a}$ при отображении φ.

Если φ есть инъекция, то нулевой вектор $\mathbf{0}$ имеет единственный прообраз при отображении φ, т. е. $\operatorname{Ker}\varphi = \{\mathbf{0}\}$.

Если $\operatorname{Ker}\varphi = \{\mathbf{0}\}$, то размерность ядра оператора φ равна нулю, т. е. дефект $\varphi = 0$.

Если дефект $\varphi = 0$, то по теореме 1.4, ранг $\varphi = \dim \mathcal{V}$.

Предположим, что ранг $\varphi = \dim \mathcal{V} = n$. Пусть $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ — фиксированный базис пространства $\mathcal{V}$. По теореме 2.6, ранг матрицы $M(\varphi)$ равен рангу оператора φ и, значит, равен n. Таким образом, строки матрицы $M(\varphi)$ линейно независимы. Следовательно, по теореме 5.1, матрица $M(\varphi)$ обратима.

Предположим, что матрица $M(\varphi)$ обратима и B — обратная к ней матрица, т. е.

$$M(\varphi)B = E \text{ и } BM(\varphi) = E.$$

По теореме 2.1, существует линейный оператор ψ пространства $\mathcal{V}$ такой, что B есть матрица оператора ψ относительно фиксированного базиса, т. е. $B = M(\varphi)$. Кроме того, $M(\varepsilon) = E$, следовательно,

$$M(\varphi)\,M(\psi) = M(\varepsilon) \text{ и } M(\psi)\,M(\varphi) = M(\varepsilon).$$

В силу теоремы 3.3 $M(\varphi)\,M(\psi) = M(\varphi\psi)$ и $M(\psi)\,M(\varphi) = M(\psi\varphi)$, поэтому

$$M(\varphi\psi) = M(\varepsilon),\ M(\psi\varphi) = M(\varepsilon).$$

Согласно теореме 2.1, отсюда следуют равенства $\varphi\psi = \varepsilon$ и $\psi\varphi = \varepsilon$, т. е. оператор φ обратим. □

Полная линейная группа. Согласно теореме 5.1, множество всех обратимых $n \times n$-матриц над полем $\mathcal{F}$ есть группа относительно операций умножения и образования обратного элемента.

ОПРЕДЕЛЕНИЕ. Мультипликативная группа всех обратимых $n \times n$-матриц над полем $\mathcal{F}$ называется *полной линейной группой степени n над полем* $\mathcal{F}$ и обозначается $GL(n, \mathcal{F})$.

Легко видеть, что любой обратимый оператор векторного пространства $\mathcal{V}$ есть автоморфизм этого пространства. Обратно: любой автоморфизм пространства $\mathcal{V}$ есть обратимый оператор. Множество всех обратимых операторов векторного пространства $\mathcal{V}$ обозначается $\mathrm{Aut}\,\mathcal{V}$.

Рассмотрим алгебру $\langle \mathrm{Aut}\,\mathcal{V}, \cdot, {}^{-1} \rangle$, где $\cdot$ есть бинарная операция умножения линейных операторов пространства $\mathcal{V}$ и ${}^{-1}$ есть операция образования оператора, обратного к данному оператору; эту алгебру будем обозначать символом $\mathcal{A}ut\,\mathcal{V}$.

ТЕОРЕМА 4.2. *Пусть* $\mathcal{V}$ *— векторное пространство над полем* $\mathcal{F}$. *Тогда алгебра* $\mathcal{A}ut\,\mathcal{V}$ *есть группа.*

Доказательство. Множество $\mathrm{Aut}\,\mathcal{V}$ обратимых операторов пространства $\mathcal{V}$ замкнуто относительно операций $\cdot$ и ${}^{-1}$. Действительно, если φ — обратимый оператор, то φ^{-1} есть обратимый оператор, так как $\varphi\varphi^{-1} = \varphi^{-1}\varphi = \varepsilon$. Кроме того, если φ и ψ — обратимые операторы, то их произведение есть обратимый линейный оператор, так как

$$(\varphi\psi)(\psi^{-1}\varphi^{-1}) = \varepsilon \text{ и } (\psi^{-1}\varphi^{-1})(\varphi\psi) = \varepsilon.$$

Согласно теореме 2.3, умножение линейных операторов ассоциативно. Тождественный оператор ε обратим и является нейтральным элементом относительно умножения,

т. е. $\varphi\varepsilon = \varepsilon\varphi = \varphi$ для любого линейного оператора φ. Наконец, для любого обратимого оператора φ выполняются равенства $\varphi\varphi^{-1} = \varphi^{-1}\varphi = \varepsilon$. Таким образом, главные операции алгебры $\mathscr{A}ut\,\mathscr{V}$ удовлетворяют всем групповым аксиомам. Следовательно, эта алгебра является группой. □

ТЕОРЕМА 4.3. *Пусть $\mathscr{V}$ есть n-мерное ненулевое векторное пространство над полем $\mathscr{F}$. Тогда группа $\mathscr{A}ut\,\mathscr{V}$ изоморфна полной линейной матричной группе $GL(n, \mathscr{F})$.*

Доказательство. Рассмотрим биективное отображение

$$\Phi\colon \operatorname{Aut}\mathscr{V} \to \operatorname{GL}(n, \mathscr{F}),$$

определяемое равенством $\Phi(\varphi) = M(\varphi)$, где $M(\varphi)$ — матрица линейного оператора φ относительно фиксированного базиса пространства $\mathscr{V}$. Согласно теореме 3.3, для любых $\varphi, \psi \in \operatorname{Aut}\mathscr{V}$

$$M(\varphi\psi) = M(\varphi)\,M(\psi).$$

Следовательно, для любых обратимых операторов φ, ψ имеем $\Phi(\varphi\psi) = \Phi(\varphi)\,\Phi(\psi)$. По теореме 3.3.1, отсюда следует, что Φ есть гомоморфизм. Следовательно, Φ есть изоморфизм группы $\mathscr{A}ut\,\mathscr{V}$ на группу $GL(n, \mathscr{F})$. □

Упражнения

1. Пусть φ, ψ — обратимые линейные операторы векторного пространства. Докажите, что $\varphi\psi$ есть обратимый линейный оператор и $(\varphi\psi)^{-1} = \psi^{-1}\varphi^{-1}$.

2. Покажите, что линейные операторы φ, ψ векторного пространства обратимы тогда и только тогда, когда обратимы операторы $\varphi\psi$ и $\psi\varphi$.

3. Пусть φ — обратимый оператор векторного пространства $\mathscr{V}$. Покажите, что φ есть изоморфизм $\mathscr{V}$ на $\mathscr{V}$.

4. Пусть φ, ψ — линейные операторы конечномерного векторного пространства $\mathscr{V}$. Покажите, что если $\varphi\psi$ есть тождественный оператор пространства $\mathscr{V}$, то φ и ψ обратимы.

5. Пусть φ, ψ — линейные операторы векторного пространства. Покажите, что если $\operatorname{Ker}\varphi = \operatorname{Ker}\psi = \{0\}$, то $\operatorname{Ker}(\varphi\psi) = \{0\}$.

6. Пусть φ есть линейное отображение векторного пространства $\mathscr{U}$ в векторное пространство $\mathscr{V}$ и ψ — линейное отображение $\mathscr{V}$ в векторное пространство $\mathscr{W}$. Докажите, что если $\operatorname{Ker}\varphi = \{0\}$ и $\operatorname{Ker}\psi = \{0'\}$, то $\operatorname{Ker}(\psi\varphi) = \{0\}$.

7. Пусть φ — обратимый и ψ — произвольный линейный оператор конечномерного векторного пространства. Покажите, что $\operatorname{ранг}(\varphi\psi) = \operatorname{ранг}(\psi\varphi) = \operatorname{ранг}\psi$.

8. Докажите, что линейный оператор конечномерного векторного пространства $\mathscr{V}$ обратим тогда и только тогда, когда он каждую линейно независимую систему векторов пространства $\mathscr{V}$ переводит в линейно независимую систему векторов этого пространства.

9. Пусть $\mathscr{H}om(\mathscr{V}, \mathscr{V})$ есть векторное пространство всех линейных операторов пространства $\mathscr{V}$. Пусть φ — фиксированный и ψ — произвольный линейный оператор пространства $\mathscr{V}$. Докажите, что отображение $\psi \longmapsto \varphi\psi$ является линейным оператором пространства $\mathscr{H}om(\mathscr{V}, \mathscr{V})$. Покажите, что множество $\{\varphi\psi \mid \psi \in \mathrm{Hom}(\mathscr{V}, \mathscr{V})\}$ совпадает с множеством всех линейных операторов векторного пространства $\mathscr{H}om(\mathscr{V}, \mathscr{V})$, если φ — обратимый оператор.

§ 5. СОБСТВЕННЫЕ ВЕКТОРЫ И СОБСТВЕННЫЕ ЗНАЧЕНИЯ. ХАРАКТЕРИСТИЧЕСКИЕ УРАВНЕНИЯ

Собственные векторы и собственные значения. Пусть $\mathscr{V}$ — векторное пространство над полем $\mathscr{F}$ и φ — линейный оператор этого пространства.

ОПРЕДЕЛЕНИЕ. Вектор $\boldsymbol{a} \in V$ называется *собственным вектором оператора* φ, если $\boldsymbol{a} \neq \mathbf{0}$ и вектор $\varphi(\boldsymbol{a})$ равен произведению скаляра и вектора $\boldsymbol{a}$.

Скаляр $\lambda \in F$ называется *собственным значением оператора* φ, если существует такой ненулевой вектор $\boldsymbol{a}$, что $\varphi(\boldsymbol{a}) = \lambda\boldsymbol{a}$.

Если $\boldsymbol{a}$ — собственный вектор оператора φ, то существует единственный скаляр $\lambda \in F$, удовлетворяющий условию $\varphi(\boldsymbol{a}) = \lambda\boldsymbol{a}$. Действительно, если $\boldsymbol{a} \neq \mathbf{0}$, то из равенства $\lambda\boldsymbol{a} = \lambda_1\boldsymbol{a}$ следует $\lambda = \lambda_1$. Поэтому, если $\varphi(\boldsymbol{a}) = \lambda\boldsymbol{a}$, говорят, что вектор $\boldsymbol{a}$ принадлежит собственному значению λ.

Примеры. 1. Пусть $\mathscr{V}$ есть ненулевое векторное пространство над полем $\mathscr{F}$ и λ — фиксированный скаляр. Определим отображение φ: $V \to V$, полагая $\varphi(\boldsymbol{a}) = \lambda\boldsymbol{a}$ для любого $\boldsymbol{a} \in V$. Легко видеть, что φ есть линейный оператор пространства $\mathscr{V}$; он называется *оператором гомотетии с коэффициентом* λ. Скаляр λ есть собственное значение оператора φ и притом единственное. Любой ненулевой вектор пространства $\mathscr{V}$ есть собственный вектор оператора φ, принадлежащий собственному значению λ.

2. Пусть $\mathscr{V}$ — векторное пространство действительных функций одной переменной, определенных на $\mathbf{R}$ и неограниченно дифференцируемых; $\mathscr{V}$ есть пространство над полем действительных чисел $\mathscr{R}$. Обозначим через $\frac{\mathrm{d}}{\mathrm{d}x}$ оператор дифференцирования, ставящий в соответствие каждому элементу $f \in V$ его производную $\frac{\mathrm{d}f}{\mathrm{d}x}$. Легко видеть, что оператор дифференцирования есть линейный оператор пространства $\mathscr{V}$. Если $\lambda \in \mathbf{R}$, то функция $\mathrm{e}^{\lambda x}$ есть собственный вектор оператора дифференцирования,

так как $\frac{de^{\lambda x}}{dx} = \lambda e^{\lambda x}$. Таким образом, любое действительное число является собственным значением оператора дифференцирования.

3. Пусть $\mathcal{V}$ — двумерное векторное пространство над полем действительных чисел $\mathcal{R}$, $\mathcal{V} = \mathcal{R}^2$, и $\alpha \in \mathbf{R}$. Обозначим через φ_α оператор поворота, ставящий в соответствие каждому вектору пространства $\mathcal{V}$ вектор, образующий с исходным вектором угол α. Легко видеть, что φ_α есть линейный оператор пространства $\mathcal{V}$, который не имеет собственных векторов, если $\alpha \neq k\pi$, где k — целое число.

Обозначим через ε тождественный оператор векторного пространства $\mathcal{V}$. Если φ — линейный оператор пространства $\mathcal{V}$ и λ — любой скаляр, $\lambda \in F$, то легко видеть, что $\lambda\varepsilon - \varphi$ является линейным оператором пространства $\mathcal{V}$.

ПРЕДЛОЖЕНИЕ 5.1. *Пусть φ — линейный оператор векторного пространства $\mathcal{V}$ и λ — собственное значение этого оператора. Множество всех собственных векторов оператора φ совпадает с множеством* $\operatorname{Ker}(\lambda\varepsilon - \varphi) \setminus \{0\}$.

Доказательство. Согласно определению ядра,

$$\operatorname{Ker}(\lambda\varepsilon - \varphi) = \{\boldsymbol{x} \in V \mid (\lambda\varepsilon - \varphi)(\boldsymbol{x}) = 0\}.$$

Если $\boldsymbol{a} \in \operatorname{Ker}(\lambda\varepsilon - \varphi) \setminus \{0\}$, то

$$(\lambda\varepsilon - \varphi)(\boldsymbol{a}) = 0,\ \lambda\varepsilon(\boldsymbol{a}) - \varphi(\boldsymbol{a}) = 0,\ \varphi(\boldsymbol{a}) = \lambda\boldsymbol{a}.$$

Таким образом, любой ненулевой вектор множества $\operatorname{Ker}(\lambda\varepsilon - \varphi)$ является собственным вектором оператора φ.

Пусть $\boldsymbol{b}$ — любой собственный вектор оператора φ, принадлежащий λ, т. е. $\varphi(\boldsymbol{b}) = \lambda\boldsymbol{b}$, тогда

$$\lambda\boldsymbol{b} - \varphi(\boldsymbol{b}) = 0,\ \lambda\varepsilon\boldsymbol{b} - \varphi(\boldsymbol{b}) = 0,\ (\lambda\varepsilon - \varphi)(\boldsymbol{b}) = 0.$$

Следовательно, $\boldsymbol{b} \in \operatorname{Ker}(\lambda\varepsilon - \varphi)$, и так как $\boldsymbol{b} \neq 0$, то

$$\boldsymbol{b} \in \operatorname{Ker}(\lambda\varepsilon - \varphi) \setminus \{0\}. \quad \square$$

Нахождение собственных векторов линейного оператора. Пусть $\mathcal{V}$ — векторное пространство над полем $\mathcal{F}$ с фиксированным базисом $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$, φ — линейный оператор этого пространства и $A = M(\varphi)$ — матрица оператора φ относительно фиксированного базиса, $A = \|a_{ik}\|$.

Для нахождения собственных векторов оператора φ, принадлежащих λ, надо найти $\operatorname{Ker}(\lambda\varepsilon - \varphi)$. Пусть $\boldsymbol{x}$ — вектор из V; в фиксированном базисе он имеет коорди-

натный столбец $\mathscr{X} = M(\boldsymbol{x})$:

$$\mathscr{X} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Согласно теореме 2.3, координатным столбцом вектора $(\lambda\varepsilon - \varphi)(\boldsymbol{x})$ является $(\lambda E - A)\mathscr{X}$, т. е. $M((\lambda\varepsilon - \varphi)(\boldsymbol{x})) = (\lambda E - A)\mathscr{X}$. Вектор $\boldsymbol{x} \in \operatorname{Ker}(\lambda\varepsilon - \varphi)$ тогда и только тогда, когда

(I) $(\lambda E - A)\mathscr{X} = \mathbf{0}$.

Условие (I) можно записать в виде однородной линейной системы относительно переменных $x_1, \ldots, x_n$:

$$(1)\quad \begin{aligned} &(\lambda - a_{11})x_1 - a_{12}x_2 - \ldots - a_{1n}x_n = 0; \\ &-a_{21}x_1 + (\lambda - a_{22})x_2 - \ldots - a_{2n}x_n = 0; \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &-a_{n1}x_1 - a_{n2}x_2 - \ldots + (\lambda - a_{nn})x_n = 0. \end{aligned}$$

Вектор $\boldsymbol{x} \in V$ тогда и только тогда есть собственный вектор оператора φ, принадлежащий собственному значению λ, когда координатная строка $(x_1, \ldots, x_n)$ вектора $\boldsymbol{x}$ является ненулевым решением линейной однородной системы (1). Таким образом, доказано следующее предложение.

ПРЕДЛОЖЕНИЕ 5.2. *Пусть φ — линейный оператор векторного пространства $\mathscr{V}$ с фиксированным базисом и $M(\varphi) = A$ — матрица оператора φ относительно фиксированного базиса. Вектор $\boldsymbol{x}$ тогда и только тогда есть собственный вектор оператора φ, принадлежащий собственному значению λ, когда координатная строка вектора $\boldsymbol{x}$ является ненулевым решением системы* (1).

Характеристическое уравнение. Пусть $\mathscr{V} = \mathscr{F}^n$ — пространство n-мерных арифметических векторов-столбцов над полем $\mathscr{F}$. Пусть A — фиксированная $n \times n$-матрица над $\mathscr{F}$. Рассмотрим отображение ψ: $X \to AX$ для любого $X \in \mathscr{F}^n$. Легко проверить, что ψ является линейным оператором пространства $\mathscr{V}$.

ОПРЕДЕЛЕНИЕ. Пусть A есть $n \times n$-матрица над полем $\mathscr{F}$. Вектор-столбец X называется *собственным вектором матрицы* A, если X — ненулевой вектор и AX можно представить в виде произведения скаляра и вектора X, т. е. в виде $AX = \lambda X$. При этом λ называется *собственным значением матрицы* A.

Легко видеть, что собственные векторы и собственные значения линейного оператора ψ суть собственные векторы и собственные значения матрицы A.

ТЕОРЕМА 5.3. *Пусть A — квадратная $n \times n$-матрица над полем $\mathscr{F}$. Элемент λ из F есть собственное значение матрицы тогда и только тогда, когда*

(1) $|\lambda E - A| = 0.$

Доказательство. Элемент λ, $\lambda \in F$, есть собственное значение матрицы A тогда и только тогда, когда существует такой ненулевой вектор-столбец $X_1 \in F^n$, что $AX_1 = \lambda X_1$ и, следовательно, $(\lambda E - A) X_1 = 0$. Другими словами, λ есть собственное значение матрицы A тогда и только тогда, когда уравнение

(2) $(A - \lambda E) X = 0$

имеет ненулевое решение. Уравнение (2) можно рассматривать, как матричную форму записи системы n линейных уравнений с n переменными с матрицей $(A - \lambda E)$. Уравнение (2) имеет ненулевое решение тогда и только тогда, когда определитель матрицы $(A - \lambda E)$ равен нулю. □

СЛЕДСТВИЕ 5.4. *Элемент λ поля $\mathscr{F}$ является собственным значением матрицы A тогда и только тогда, когда матрица $\lambda E - A$ необратима.*

ОПРЕДЕЛЕНИЕ. Пусть A — квадратная $n \times n$-матрица над полем $\mathscr{F}$. Уравнение $|\lambda E - A| = 0$ с переменной λ называется *характеристическим уравнением матрицы A.*

СЛЕДСТВИЕ 5.5. *Скаляр $\lambda \in F$ есть собственное значение квадратной матрицы A (над $\mathscr{F}$) тогда и только тогда, когда λ является корнем характеристического уравнения этой матрицы.*

Пример. Пусть $A = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$ — матрица над полем скаляров $\mathscr{R}$. Тогда

$$\lambda E - A = \begin{bmatrix} \lambda - 1 & -1 \\ -2 & \lambda - 1 \end{bmatrix}.$$

Уравнение

$$\begin{vmatrix} \lambda - 1 & -1 \\ -2 & \lambda - 1 \end{vmatrix} = 0, \text{ или } (\lambda - 1)^2 - 2 = 0,$$

есть характеристическое уравнение матрицы A. Его корни

$\lambda_1 = 1 + \sqrt{2}$, $\lambda_2 = 1 - \sqrt{2}$ являются собственными значениями матрицы A.

ПРЕДЛОЖЕНИЕ 5.6. *Пусть A и B — подобные $n \times n$-матрицы над полем скаляров $\mathcal{F}$. Тогда $|\lambda E - A| = |\lambda E - B|$ и характеристические уравнения этих матриц совпадают.*

Доказательство. Так как A и B подобны, то существует обратимая матрица T над $\mathcal{F}$ такая, что $A = T^{-1}BT$, поэтому

$$\lambda E - A = \lambda E - T^{-1}BT = T^{-1}(\lambda E - B)T;$$

следовательно,

$$|\lambda E - A| = |T^{-1}||\lambda E - B||T|.$$

Так как $|T^{-1}||T| = |T^{-1}T| = |E| = 1$, то $|\lambda E - A| = |\lambda E - B|$. Отсюда следует, что характеристические уравнения

$$|\lambda E - A| = 0 \quad \text{и} \quad |\lambda E - B| = 0$$

соответственно матриц A и B совпадают. □

ОПРЕДЕЛЕНИЕ. Пусть φ — линейный оператор конечномерного ненулевого векторного пространства $\mathcal{V}$ и $M(\varphi)$ — его матрица относительно какого-либо базиса. Уравнение $|\lambda E - M(\varphi)| = 0$ называется *характеристическим уравнением оператора* φ.

Линейные операторы с простым спектром. Изучим линейные операторы n-мерного векторного пространства, имеющие n различных собственных значений.

ТЕОРЕМА 5.7. *Если собственные векторы $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ линейного оператора имеют различные собственные значения, то система $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ линейно независима.*

Доказательство. Пусть φ — линейный оператор векторного пространства $\mathcal{V}$ и $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ — его собственные векторы, принадлежащие различным собственным значениям, т. е.

(1) $\varphi(\boldsymbol{a}_1) = \lambda_1 \boldsymbol{a}_1, \ldots, \varphi(\boldsymbol{a}_m) = \lambda_m \boldsymbol{a}_m$

и

(2) $\lambda_i \neq \lambda_k$ при $i \neq k$.

Доказательство проводится индукцией по числу m. Так как любой собственный вектор отличен от нулевого вектора, то теорема верна при $m = 1$. Предполагая, что теорема верна для $m - 1$ векторов, докажем, что она верна

для m векторов. Надо доказать, что для любых $\alpha_1, \ldots, \alpha_m \in F$ из равенства

(3) $\alpha_1 \boldsymbol{a}_1 + \ldots + \alpha_m \boldsymbol{a}_m = \boldsymbol{0}$

следуют равенства

(4) $\alpha_1 = 0, \ldots, \alpha_m = 0.$

Так как φ есть линейный оператор, то из (3) следует равенство $\alpha_1 \varphi(\boldsymbol{a}_1) + \ldots + \alpha_m \varphi(\boldsymbol{a}_m) = \boldsymbol{0}$ и в силу (1)

(5) $\alpha_1 \lambda_1 \boldsymbol{a}_1 + \ldots + \alpha_m \lambda_m \boldsymbol{a}_m = \boldsymbol{0}.$

Прибавив к обеим частям равенства (5) соответствующие части равенства (3), умноженные на $(-\lambda_m)$, получим

(6) $\alpha_1 (\lambda_1 - \lambda_m) \boldsymbol{a}_1 + \ldots + \alpha_{m-1} (\lambda_{m-1} - \lambda_m) \boldsymbol{a}_{m-1} = \boldsymbol{0}.$

По индуктивному предположению, система собственных векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{m-1}$ линейно независима. Поэтому из (6) следуют равенства

$$\alpha_1 (\lambda_1 - \lambda_m) = 0, \ \ldots, \ \alpha_{m-1} (\lambda_{m-1} - \lambda_m) = 0.$$

Ввиду (2) отсюда имеем

(7) $\alpha_1 = 0, \ \ldots, \ \alpha_{m-1} = 0.$

В силу (3) и (7) $\alpha_m \boldsymbol{a}_m = \boldsymbol{0}$, кроме того, $\boldsymbol{a}_m \neq \boldsymbol{0}$; следовательно, $\alpha_m = 0$.

Таким образом, доказано, что из (3) следует (4), т. е. система $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ линейно независима. □

ОПРЕДЕЛЕНИЕ. Линейный оператор n-мерного векторного пространства ($n > 0$), имеющий n различных собственных значений, называется *оператором с простым спектром*; набор всех собственных значений оператора называется *спектром оператора*.

ПРЕДЛОЖЕНИЕ 5.8. *Пусть φ — линейный оператор n-мерного векторного пространства $\mathcal{V}$ с простым спектром $\{\lambda_1, \ldots, \lambda_n\}$. Пусть $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ — собственные векторы оператора φ, принадлежащие соответственно $\lambda_1, \ldots, \lambda_n$. Тогда система $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ является базисом пространства $\mathcal{V}$.*

Доказательство. По условию, спектр $\lambda_1, \ldots, \lambda_n$ оператора φ состоит из попарно различных скаляров. По теореме 5.7, отсюда следует, что система собственных векторов $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ линейно независима. По следствию 7.3.4 отсюда вытекает, что система $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ есть базис пространства $\mathcal{V}$. □

ТЕОРЕМА 5.9. *Пусть* φ *— линейный оператор* n*-мерного векторного пространства* $\mathfrak{V}$ *с простым спектром* $\lambda_1, \ldots, \lambda_n$ *и* $e_1, \ldots, e_n$ *— собственные векторы оператора* φ*, принадлежащие соответственно собственным значениям* $\lambda_1, \ldots, \lambda_n$*. Тогда диагональная матрица*

$$(1) \quad \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}$$

является матрицей оператора φ *относительно базиса* $e_1, \ldots, e_n$ *и для любого вектора* $x = x_1e_1 + \ldots + x_ne_n$ *пространства* $\mathfrak{V}$

$$(2) \quad \varphi(x) = \lambda_1 x_1 e_1 + \ldots + \lambda_n x_n e_n.$$

Доказательство. По условию,

$$(3) \quad \varphi(e_1) = \lambda_1 e_1, \ \ldots, \ \varphi(e_n) = \lambda_n e_n.$$

Эти равенства показывают, что диагональная матрица (1) является матрицей оператора φ относительно базиса $e_1, \ldots, e_n$. Далее, если $x \in V$ и $x = x_1e_1 + \ldots + x_ne_n$, то ввиду линейности оператора φ имеем $\varphi(x) = x_1\varphi(e_1) + \ldots + x_n\varphi(e_n)$. В силу (3) отсюда следуют равенства (2). □

Условия, при которых матрица подобна диагональной матрице.

ТЕОРЕМА 5.10. *Пусть* A *есть* $n \times n$*-матрица над полем* $\mathfrak{F}$*, имеющая* n *линейно независимых собственных векторов, и* T *— матрица, столбцы которой суть линейно независимые собственные векторы матрицы* A*. Тогда матрица* $T^{-1}AT$ *диагональна и элементы ее главной диагонали являются собственными значениями матрицы* A*.*

Доказательство. Пусть

$$X_1, \ldots, X_n$$

— линейно независимые собственные векторы матрицы A, принадлежащие соответственно $\lambda_1, \ldots, \lambda_n$, т. е.

$$AX_1 = \lambda_1 X_1, \ \ldots, \ AX_n = \lambda_n X_n.$$

Обозначим через T такую матрицу, что $T^i = X_i$ для $i = 1, \ldots, n$, т. е.

$$T = [X_1, \ \ldots, \ X_n].$$

Так как столбцы матрицы T линейно независимы, то она обратима. Из определения произведения матриц следует,

что

$$AT=[AX_1,\ \ldots,\ AX_n];$$

откуда ввиду (1) имеем

$$AT=[\lambda_1X_1,\ \ldots,\ \lambda_nX_n]=[X_1,\ \ldots,\ X_n]\begin{bmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{bmatrix}=$$

$$=T\begin{bmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{bmatrix}.$$

Таким образом, получаем

$$T^{-1}AT=\begin{bmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{bmatrix}. \ \square$$

ТЕОРЕМА 5.11. *Если квадратная матрица A порядка n подобна над полем $\mathscr{F}$ диагональной матрице, то матрица A имеет n линейно независимых собственных векторов.*

Доказательство. Предположим, что матрица A подобна над $\mathscr{F}$ диагональной матрице, т. е. существует такая обратимая матрица T, что

$$(1)\quad T^{-1}AT=\begin{bmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{bmatrix},$$

причем $\lambda_1, \ldots, \lambda_n \in F$. Умножив слева обе части равенства (1) на T, получим

$$AT=T\begin{bmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{bmatrix}.$$

Следовательно,

$$[AT^1,\ \ldots,\ AT^n]=[\lambda_1T^1,\ \ldots,\ \lambda_nT^n],$$

поэтому

$$AT^1=\lambda_1T^1,\ \ldots,\ AT^n=\lambda_nT^n,$$

т. е. столбцы $T^1, \ldots, T^n$ матрицы T являются собственными векторами, принадлежащими соответственно $\lambda_1, \ldots, \lambda_n$. Так как матрица T обратима, то ее столбцы линейно независимы (по теореме 5.1). $\square$

Упражнения

1. Найдите собственные векторы и собственные значения следующих матриц над полем рациональных чисел:

(a) $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$; (b) $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$; (c) $\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$.

2. Пусть α — ненулевое действительное число. Покажите, что матрица $\begin{bmatrix} 0 & \alpha \\ -\alpha & 0 \end{bmatrix}$ не имеет действительных собственных значений.

3. Пусть α — действительное число, отличное от нуля. Найдите собственные значения и собственные векторы над полем комплексных чисел матрицы $\begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}$.

4. Найдите собственные векторы и собственные значения над полем комплексных чисел следующих матриц:

(a) $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$; (b) $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$; (c) $\begin{bmatrix} 1 & 2 \\ 2 & -2 \end{bmatrix}$; (d) $\begin{bmatrix} -1 & -2i \\ 2i & 2 \end{bmatrix}$.

5. Пусть $A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ — матрица над полем $\mathcal{F}$. Покажите, что скаляр $\lambda \in F$ есть собственное значение матрицы A, когда $\lambda^2 - (\alpha+\delta)\lambda + (\alpha\delta - \beta\gamma) = 0$.

6. Докажите, что собственными значениями действительной симметрической матрицы являются действительные числа.

7. Пусть A — квадратная матрица. Покажите, что транспонированная матрица ${}^tA$ имеет те же собственные значения, что и матрица A.

8. Покажите, что собственными значениями диагональной матрицы являются ее диагональные элементы.

9. Докажите, что собственными значениями треугольной матрицы являются ее диагональные элементы.

10. Докажите, что все собственные значения квадратной матрицы A отличны от нуля тогда и только тогда, когда матрица A обратима.

11. Пусть A — квадратная матрица и k — любое целое положительное число. Докажите, что если λ — собственное значение матрицы A, то λ^k является собственным значением матрицы A^k.

12. Зная собственные значения обратимой матрицы A, найдите собственные значения матрицы A^{-1}.

13. Пусть λ — собственное значение обратимой матрицы A. Докажите, что λ^n является собственным значением матрицы A^n для любого целого числа n.

14. Пусть A — квадратная матрица над полем $\mathcal{F}$:

$$f(\lambda) = \alpha_0 + \alpha_1\lambda + \ldots + \alpha_m\lambda^m, \text{ где } \alpha_0, \alpha_1, \ldots, \alpha_m \in F,$$

$$f(A) = \alpha_0 E + \alpha_1 A + \ldots + \alpha_m A^m \quad (E \text{ — единичная матрица}),$$

Докажите, что если λ — собственное значение матрицы A, то $f(\lambda)$ является собственным значением матрицы $f(A)$. Покажите, что любой собственный вектор матрицы A является собственным вектором матрицы $f(A)$.

15. Пусть A, B — квадратные $n \times n$-матрицы над полем $\mathcal{F}$, причем матрица A обратима. Докажите, что матрицы AB и BA имеют одно и то же характеристическое уравнение.

16. Найдите диагональную матрицу, подобную над полем рациональных чисел матрице:

(a) $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$; (b) $\begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}$; (c) $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$.

17. Найдите диагональную матрицу, подобную над полем действительных чисел матрице:

(a) $\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$; (b) $\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$; (c) $\begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix}$.

18. Найдите диагональную матрицу, подобную над полем комплексных чисел матрице $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.

19. Пусть α — действительное число, не являющееся целым кратным числа π. Докажите, что матрица $\begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}$ не подобна действительной диагональной матрице.

20. Покажите, что любая действительная диагональная матрица, определитель которой отрицателен, подобна действительной диагональной матрице.

21. Пусть $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ — матрица над полем $\mathcal{F}$ и $a \neq 0$. Докажите, что матрица A не подобна диагональной.

22. Докажите, что две диагональные матрицы подобны тогда и только тогда, когда они отличаются только порядком расположения диагональных элементов.

23. Пусть A — матрица, подобная диагональной матрице. Докажите, что матрица A^n подобно диагональной для всякого целого положительного числа.

24. Найдите все квадратные матрицы второго порядка над полем $\mathcal{Q}$ с собственными значениями 1 и -1.

Глава девятая

СИСТЕМЫ ЛИНЕЙНЫХ НЕРАВЕНСТВ

§ 1. СИСТЕМЫ ЛИНЕЙНЫХ НЕРАВЕНСТВ

Основные понятия. Система вида

(1) $\alpha_{i1}x_1+\ldots+\alpha_{in}x_n\leqslant\gamma_i \quad (i=1, \ldots, m)$,

где $\alpha_i\in\mathbf{R}$, $\gamma_i\in\mathbf{R}$, называется *системой линейных неравенств.*

Положим

$$\boldsymbol{a}_i=(\alpha_{i1}, \ldots, \alpha_{in}) \quad (i=1, \ldots, m).$$

Систему (1) можно записать в *векторной форме*:

(2) $\boldsymbol{a}_i\boldsymbol{x}\leqslant\gamma_i \qquad (i=1, \ldots, m)$,

где $\boldsymbol{x}=\begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix}$.

Обозначим через A матрицу, составленную из коэффициентов системы (1):

$$A=\begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{bmatrix}.$$

Систему (1) можно записать в *матричной форме*:

(3) $A\boldsymbol{x}\leqslant\boldsymbol{c}$, где $\boldsymbol{c}=\begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{bmatrix}$.

Пусть $\mathscr{R}^n$ есть n-мерное арифметическое пространство над полем действительных чисел $\mathscr{R}$ и $\mathbf{R}^n$ — его основное множество.

Вектор из $\mathbf{R}^n$ с координатами $\xi_1, \ldots, \xi_n$ называется *решением системы* (1), если

$$\alpha_{i1}\xi_1+\ldots+\alpha_{in}\xi_n\leqslant\gamma_i \qquad (i=1, \ldots, n).$$

Система (1) называется *совместной*, если она имеет хотя бы одно решение. Система (1) называется *несовместной*, если она не имеет решений.

Вектор $(\xi_1, \ldots, \xi_n) \in \mathbf{R}^n$ называется *неотрицательным*, если $\xi_i \geqslant 0$ для $i = 1, \ldots, n$. Неотрицательный вектор $(\xi_1, \ldots, \xi_n)$ называется *положительным*, если положительна хотя бы одна его координата.

Неравенство

$$(4)\quad \beta_1 x_1 + \ldots + \beta_n x_n \leqslant \gamma$$

называется *следствием системы* (1), если каждое решение системы (1) является решением неравенства (4).

Неравенство вида

$$(5)\quad (\lambda_1 a_1 + \ldots + \lambda_m a_m)\, x \leqslant \lambda_1 \gamma_1 + \ldots + \lambda_m \gamma_m,$$

где $\lambda_1 \geqslant 0, \ldots, \lambda_m \geqslant 0$, называется *неотрицательной линейной комбинацией неравенств системы* (2).

ПРЕДЛОЖЕНИЕ 1.1. *Любая неотрицательная линейная комбинация неравенств системы* (2) *является следствием этой системы.*

Доказательство. Пусть неравенство (5) есть неотрицательная линейная комбинация неравенств системы (2). Пусть $\xi \in \mathbf{R}^n$ есть любое решение системы (2),

$$(6)\quad a_i \xi \leqslant \gamma_i \qquad (i = 1, \ldots, m).$$

Умножив i-е неравенство (6) на λ_i для $i = 1, \ldots, m$ и сложив все эти неравенства, получим

$$(\lambda_1 a_1 + \ldots + \lambda_m a_m)\, \xi \leqslant \lambda_1 \gamma_1 + \ldots + \lambda_m \gamma_m.$$

Таким образом, неравенство (5) является следствием системы (2). □

Однородные системы линейных неравенств и выпуклые конусы. Пусть $\mathcal{V}$ — арифметическое векторное пространство над полем действительных чисел $\mathcal{R}$, $\mathcal{V} = \mathcal{R}^n$, и $a_1, \ldots, a_m$ — векторы пространства $\mathcal{V}$.

Система

$$(1)\quad a_i x \leqslant 0 \qquad (i = 1, \ldots, m)$$

называется *однородной линейной системой неравенств.*

ОПРЕДЕЛЕНИЕ. Непустое множество векторов векторного пространства $\mathcal{V}$, замкнутое относительно сложения и умножения на неотрицательные скаляры (неотрицательные действительные числа), называется *выпуклым конусом пространства* $\mathcal{V}$.

Примеры. 1. Пусть $\boldsymbol{a} \in \mathbf{R}^n$ и $\boldsymbol{a} \neq 0$. Множество

$$\{\lambda \boldsymbol{a} \mid \lambda \geqslant 0, \quad \lambda \in \mathbf{R}\}$$

есть выпуклый конус пространства $\mathscr{R}^n$. Этот конус называется *полупрямой, порожденной вектором* $\boldsymbol{a}$.

2. Множество всех неотрицательных комбинаций системы векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ пространства $\mathscr{R}^n$ есть выпуклый конус этого пространства; его мы будем обозначать через $L^+(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$.

3. Пусть $\mathscr{V} = \mathscr{R}^n$, $\mathscr{L}$ — подпространство пространства $\mathscr{V}$ и L — его основное множество. Тогда L есть выпуклый конус пространства $\mathscr{V}$.

4. Множество всех неотрицательных решений однородной линейной системы неравенств (1) есть выпуклый конус пространства $\mathscr{V}$.

5. Пусть $\boldsymbol{a} \in \mathbf{R}^n$ и $\boldsymbol{a} \neq \mathbf{0}$. Множество всех решений неравенства $\boldsymbol{a}\boldsymbol{x} \leqslant 0$ есть выпуклый конус пространства $\mathscr{V}$. Этот конус называется *полупространством пространства* $\mathscr{V}$, *определяемым вектором* $\boldsymbol{a}$.

ПРЕДЛОЖЕНИЕ 1.2. *Множество всех решений однородной линейной системы* (1) *есть выпуклый конус векторного пространства* $\mathscr{V}$.

Доказательство этого предложения предоставляется читателю.

СЛЕДСТВИЕ 1.3. *Если* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ — *ненулевые векторы, то конус всех решений однородной линейной системы* (1) *является пересечением* m *полупространств пространства* $\mathscr{V}$, *определяемых векторами* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$.

Следствия однородной системы линейных неравенств. Для доказательства теоремы Минковского необходимы следующие две леммы.

ЛЕММА 1.4. *Если*

(3) $\boldsymbol{b} \notin L(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$,

то неравенство

(2) $\boldsymbol{b}\boldsymbol{x} \leqslant 0$

не является следствием системы

(1) $\boldsymbol{a}_i\boldsymbol{x} \leqslant 0 \qquad (i = 1, \ldots, m)$.

Доказательство. Ранг системы векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ обозначим через r. Предположим, что выполняется условие (3), тогда

(4) ранг $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{b}\} =$ ранг $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m\} + 1 = r + 1$.

Пусть

$$\boldsymbol{a}_i=(\alpha_{i1},\ \ldots,\ \alpha_{in}) \qquad (i=1,\ \ldots,\ m);$$
$$\boldsymbol{b}=(\beta_1,\ \ldots,\ \beta_n).$$

Рассмотрим систему линейных уравнений

$$\begin{aligned}
&\alpha_{11}x_1+\ldots+\alpha_{1n}x_n=0,\\
&\qquad\ldots\ldots\ldots\ldots\\
&\alpha_{m1}x_1+\ldots+\alpha_{mn}x_n=0,\\
&\beta_1x_1+\ldots+\beta_nx_n=1.
\end{aligned} \tag{5}$$

На основании (4) заключаем, что ранги основной и расширенной матриц системы (5) равны $r+1$. Следовательно, система (5) совместна. Поэтому существует вектор ξ такой, что

$$\begin{aligned}
&\boldsymbol{a}_i\xi=0\\
&\boldsymbol{b}\xi=1
\end{aligned} \qquad (i=1,\ \ldots,\ m).$$

Вектор ξ является решением системы (1), не удовлетворяющим (2). Таким образом, неравенство (2) не является следствием системы (1). □

СЛЕДСТВИЕ 1.5. *Если неравенство* (2) *есть следствие системы* (1), *то*

$$\boldsymbol{b}\in L(\boldsymbol{a}_1,\ \ldots,\ \boldsymbol{a}_m).$$

По закону контрапозиции, это утверждение равносильно лемме 1.4.

ЛЕММА 1.6. *Пусть неравенство*

$$\boldsymbol{c}\boldsymbol{x}\leqslant 0 \tag{2}$$

есть следствие системы

$$\boldsymbol{a}_i\boldsymbol{x}\leqslant 0 \qquad (i=1,\ \ldots,\ m) \tag{1}$$

и

$$\boldsymbol{c}=\lambda_1\boldsymbol{a}_1+\ldots+\lambda_{m-1}\boldsymbol{a}_{m-1}+\lambda_m\boldsymbol{a}_m, \tag{3}$$
$$\lambda_1,\ \ldots,\ \lambda_{m-1}\geqslant 0,\quad \lambda_m\leqslant 0.$$

Тогда неравенство (2) *является следствием системы*

$$\boldsymbol{a}_i\boldsymbol{x}\leqslant 0 \qquad (i=1,\ \ldots,\ m-1). \tag{4}$$

Доказательство. Рассмотрим систему

$$\boldsymbol{a}_1\boldsymbol{x}\leqslant 0,\ \ldots,\ \boldsymbol{a}_{m-1}\boldsymbol{x}\leqslant 0,\quad (-\boldsymbol{a}_m)\,\boldsymbol{x}\leqslant 0. \tag{I}$$

Вектор $\boldsymbol{c}$ в силу (3) есть неотрицательная линейная комбинация векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{m-1}, (-\boldsymbol{a}_m)$,

$$\boldsymbol{c} = \lambda_1 \boldsymbol{a}_1 + \ldots + \lambda_{m-1} \boldsymbol{a}_{m-1} + (-\lambda_m)(-\boldsymbol{a}_m).$$

В силу предложения 1.1 отсюда следует, что (2) является следствием системы (II):

(5) $(\mathrm{II}) \to (2)$.

Надо доказать, что любое решение ξ системы (4) является решением неравенства (2). Возможны два случая: $\boldsymbol{a}_m \xi \leqslant 0$ или $(-\boldsymbol{a}_m)\xi \leqslant 0$. Если $\boldsymbol{a}_m \xi \leqslant 0$, то ξ есть решение системы (1) и, следовательно, по условию, ξ является решением неравенства (2). Если же $-\boldsymbol{a}_m \xi \leqslant 0$, то ξ есть решение системы (1′); следовательно, ввиду (4) является решением и неравенства (2). Итак, любое решение системы (4) является решением неравенства (2). □

Теорема Минковского. В теории линейных неравенств одной из основных является следующая теорема.

ТЕОРЕМА 1.7. *Пусть неравенство*

(2) $\boldsymbol{b}\boldsymbol{x} \leqslant 0$

есть следствие системы

(1) $\boldsymbol{a}_i \boldsymbol{x} \leqslant 0 \qquad (i = 1, \ldots, m)$.

Тогда $\boldsymbol{b} \in L^+(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$.

Доказательство*) (проводится индукцией по m). Теорема верна при $m = 1$. Действительно, пусть $\boldsymbol{b} \neq \boldsymbol{0}$. По условию, неравенство $\boldsymbol{b}\boldsymbol{x} \leqslant 0$ есть следствие неравенства $\boldsymbol{a}_1 x \leqslant 0$. По следствию 1.5, $\boldsymbol{b} = \lambda \boldsymbol{a}_1$, где $\lambda \in \mathbf{R}$. Так как $\boldsymbol{b} \neq \boldsymbol{0}$, то $\lambda \neq 0$, $\boldsymbol{a}_1 \neq \boldsymbol{0}$ и $\boldsymbol{a}_1 \boldsymbol{a}_1 > 0$. Поэтому вектор $(-\boldsymbol{a}_1)$ есть решение неравенства $\boldsymbol{a}_1 \boldsymbol{x} \leqslant 0$ и, по условию, решение неравенства (2), т. е. $\lambda \boldsymbol{a}_1 (-\boldsymbol{a}_1) \leqslant 0$. Следовательно, $\lambda > 0$. Теорема, очевидно, верна также при $\boldsymbol{b} = \boldsymbol{0}$.

Предположим, что теорема верна, когда система содержит $m - 1$ неравенств. Так как $(1) \to (2)$, то, по следствию 1.5, $\boldsymbol{b} \in L(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$. Среди представлений вектора $\boldsymbol{b}$ существует представление с наибольшим числом неотрицательных коэффициентов. Пусть

(3) $\boldsymbol{b} = \lambda_1 \boldsymbol{a}_1 + \ldots + \lambda_m \boldsymbol{a}_m$

— одно из таких представлений. Пусть s есть число неот-

*) Доказательство дано в работе С. Н. Черникова «Об основных теоремах теории линейных неравенств», Сибирск. матем. ж., 1964, № 5.

рицательных коэффициентов в (3), $s \leqslant m$. Надо доказать, что $s = m$. Допустим, что

(4) $s < m$.

Мы будем считать, что коэффициенты $\lambda_1, \ldots, \lambda_s$ неотрицательны. Рассмотрим вектор

$$\boldsymbol{c} = \sum_{1 \leqslant i \leqslant s} \lambda_i \boldsymbol{a}_i + \lambda_m \boldsymbol{a}_m;$$

тогда

(5) $$\boldsymbol{b} - \boldsymbol{c} = \sum_{s < k < m} \lambda_k \boldsymbol{a}_k.$$

Пусть M — множество всех решений системы (1) и ξ — любой вектор из M, тогда $\boldsymbol{a}_k \xi \leqslant 0$ и $\lambda_k (\boldsymbol{a}_k \xi) \geqslant 0$, если $s < k < m$; следовательно,

(6) $$(\boldsymbol{b} - \boldsymbol{c})\xi = \sum_{s < k < m} \lambda_k \boldsymbol{a}_k \xi \geqslant 0.$$

Кроме того, по условию, $\boldsymbol{b}\xi \leqslant 0$; поэтому

(7) $$\boldsymbol{c}\xi + (\boldsymbol{b} - \boldsymbol{c})\xi \leqslant 0.$$

На основании (6) и (7) заключаем, что $\boldsymbol{c}\xi \leqslant 0$ для любого ξ из M, т. е. неравенство $\boldsymbol{c}\boldsymbol{x} \leqslant 0$ есть следствие системы (1).

По лемме 1.6, отсюда вытекает, что неравенство $\boldsymbol{c}\boldsymbol{x} \leqslant 0$ есть следствие системы

$$\boldsymbol{a}_i \boldsymbol{x} \leqslant 0 \qquad (i = 1, \ldots, m-1),$$

состоящей из $m - 1$ неравенств. По индуктивному предположению, $\boldsymbol{c} \in L^+(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{m-1})$, т. е. $\boldsymbol{c}$ можно представить в виде

(8) $$\boldsymbol{c} = \gamma_1 \boldsymbol{a}_1 + \ldots + \gamma_{m-1} \boldsymbol{a}_{m-1}, \quad \text{где} \quad \gamma_1, \ldots, \gamma_{m-1} \geqslant 0.$$

Ввиду (5) и (8)

$$\boldsymbol{b} = \sum_{1 \leqslant i \leqslant s} \gamma_i \boldsymbol{a}_i + \sum_{s < k < m} (\gamma_k + \lambda_k) \boldsymbol{a}_k + 0 \cdot \boldsymbol{a}_m.$$

В этом представлении вектора $\boldsymbol{b}$ число неотрицательных коэффициентов больше, чем s. Это противоречит предположению, что представление (3) вектора $\boldsymbol{b}$ содержит наибольшее число неотрицательных коэффициентов. Мы пришли к противоречию, допустив, что $s < m$. Таким образом, этот случай невозможен. Следовательно, $s = m$, т. е. (3) есть искомое представление вектора $\boldsymbol{b}$ в виде неотрицательной комбинации векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$. □

Критерий несовместности системы линейных неравенств. Перейдем к рассмотрению неоднородных систем линейных неравенств.

ТЕОРЕМА 1.8. *Система неравенств*

$$(1)\quad \boldsymbol{a}_i\boldsymbol{x} \leqslant \gamma_i \qquad (i=1,\ \ldots,\ m)$$

несовместна тогда и только тогда, когда существуют действительные числа $\lambda_1, \ldots, \lambda_m$, *удовлетворяющие условиям*

$$(2)\quad \begin{array}{l} \lambda_1\boldsymbol{a}_1+\ldots+\lambda_m\boldsymbol{a}_m=\boldsymbol{0} \\ \lambda_1\gamma_1+\ldots+\lambda_m\gamma_m<0 \end{array} \qquad (\lambda_1\geqslant 0,\ \ldots,\ \lambda_m\geqslant 0).$$

Доказательство. Предположим, что система (1) несовместна, и докажем, что существуют действительные числа, удовлетворяющие условиям (2). Пусть

$$(3)\quad \boldsymbol{a}_i=(\alpha_{i1},\ \ldots,\ \alpha_{in}) \qquad (i=1,\ \ldots,\ m).$$

Рассмотрим однородную систему неравенств

$$(4)\quad \alpha_{i1}x_1+\ldots+\alpha_{in}x_n-\gamma_i x_{n+1}\leqslant 0 \qquad (i=1,\ \ldots,\ m)$$

с переменными $x_1, \ldots, x_n, x_{n+1}$. Неравенство

$$(5)\quad 0\cdot x_1+\ldots+0\cdot x_n+x_{n+1}\leqslant 0$$

есть следствие системы (4). Действительно, если $(\xi_1, \ldots, \xi_n, \xi_{n+1})$ — произвольное решение системы (4), то

$$(6)\quad \xi_{n+1}\leqslant 0,$$

ибо при $\xi_{n+1}>0$ вектор $(\xi_1\xi_{n+1}^{-1}, \ldots, \xi_n\xi_{n+1}^{-1}, 1)$ был бы решением системы (4), а вектор $(\xi_1\xi_{n+1}^{-1}, \ldots, \xi_n\xi_{n+1}^{-1})$ — решением исходной системы (1), что противоречило бы предположению о несовместности этой системы.

Так как неравенство (5) есть следствие системы (4), то, по теореме Минковского, вектор $(0, \ldots, 0, 1)$ можно представить в виде неотрицательной линейной комбинации векторов

$$\begin{array}{l} (\alpha_{11}, \ldots, \alpha_{1n}, -\gamma_1), \\ \ldots\ldots\ldots\ldots \\ (\alpha_{m1}, \ldots, \alpha_{mn}, -\gamma_m), \end{array}$$

т. е. существуют действительные числа $\lambda_1, \ldots, \lambda_m$ такие, что

$$\begin{aligned} &\lambda_1\alpha_{11} + \ldots + \lambda_m\alpha_{m1} = 0, \\ &\ldots\ldots\ldots\ldots\ldots \\ &\lambda_1\alpha_{1n} + \ldots + \lambda_m\alpha_{mn} = 0, \\ &\lambda_1(-\gamma_1) + \ldots + \lambda_m(-\gamma_m) = 1. \end{aligned} \qquad \lambda_1 \geqslant 0, \ \ldots, \ \lambda_m \geqslant 0,$$

Ввиду (3) отсюда следует, что

$$\begin{aligned} &\lambda_1\boldsymbol{a}_1 + \ldots + \lambda_m\boldsymbol{a}_m = \mathbf{0}, \\ &\lambda_1\gamma_1 + \ldots + \lambda_m\gamma_m < 0, \end{aligned} \qquad \lambda_1 \geqslant 0, \ \ldots, \ \lambda_m \geqslant 0,$$

т. е. выполняются условия (2).

Предположим теперь, что существуют действительные числа $\lambda_1, \ldots, \lambda_m$, удовлетворяющие условиям (2), и докажем, что система (1) несовместна. Рассмотрим неравенство

(7) $(\lambda_1\boldsymbol{a}_1 + \ldots + \lambda_m\boldsymbol{a}_m)\,\boldsymbol{x} \leqslant \lambda_1\gamma_1 + \ldots + \lambda_m\gamma_m$,

являющееся неотрицательной линейной комбинацией неравенств системы (1). Согласно предложению 1.1, это неравенство есть следствие системы (1). Ввиду (2) неравенство (7) можно записать в виде

$$\mathbf{0} \cdot \boldsymbol{x} < 0.$$

Это неравенство не имеет решений и является следствием системы (1), поэтому система (1) несовместна. □

Пусть $\boldsymbol{a}_i = (\alpha_{i1}, \ldots, \alpha_{in})$ для $i = 1, \ldots, m$,

$$A = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \ldots & \ldots & \ldots \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{bmatrix}, \quad {}^tA = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{m1} \\ \ldots & \ldots & \ldots \\ \alpha_{1n} & \ldots & \alpha_{mn} \end{bmatrix}.$$

ТЕОРЕМА 1.9. *Неравенство*

(2) $\boldsymbol{b}\boldsymbol{x} \leqslant 0$

является следствием неравенства

(1) $A\boldsymbol{x} \leqslant 0$

тогда и только тогда, когда совместна система

(3) ${}^tA\boldsymbol{y} = \boldsymbol{b}, \ \boldsymbol{y} \geqslant \mathbf{0}$.

Теорема 1.9 непосредственно следует из предложения 1.1 и теоремы 1.8.

ТЕОРЕМА 1.10. *Система*

$$A\boldsymbol{x} + \boldsymbol{b} = 0, \ \boldsymbol{x} \geqslant \mathbf{0}$$

(где $\boldsymbol{b}$ — столбец), совместна тогда и только тогда, когда для всякого $\boldsymbol{y}$ $^tA\boldsymbol{y} \geqslant \boldsymbol{0} \rightarrow {}^t\boldsymbol{b}\boldsymbol{y} \leqslant 0$.

Заменив в теореме 1.9 A, ^tA, $\boldsymbol{b}$, $^t\boldsymbol{b}$, $\boldsymbol{x}$, $\boldsymbol{y}$ соответственно на $-{}^tA$, $-A$, $^t\boldsymbol{b}$, $\boldsymbol{b}$, $\boldsymbol{y}$, $\boldsymbol{x}$, мы убедимся, что теорема 1.10 есть другая формулировка теоремы 1.9.

Неотрицательные решения системы линейных уравнений и системы линейных неравенств. Систему линейных уравнений

(1*) $\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n + \beta_i = 0 \qquad (i = 1, \ldots, m)$

можно записать в матричной форме

$$A\boldsymbol{x} + \boldsymbol{b} = \boldsymbol{0},$$

где $A = \|\alpha_{ik}\|$ — $m \times n$-матрица и $\boldsymbol{b} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix}$.

При рассмотрении задач линейного программирования возникает вопрос об условиях, при которых система (1*) имеет хотя бы одно неотрицательное решение. Этот вопрос равносилен вопросу о совместности системы

(1) $A\boldsymbol{x} + \boldsymbol{b} = \boldsymbol{0}, \ \boldsymbol{x} \geqslant \boldsymbol{0}$.

ТЕОРЕМА 1.11. *Система* (1) *совместна тогда и только тогда, когда несовместна система*

(2) $^tA\boldsymbol{y} \geqslant \boldsymbol{0}, \ {}^t\boldsymbol{b}\boldsymbol{y} > 0$.

Доказательство. Согласно теореме 1.10, система (1) совместна тогда и только тогда, когда

(3) $^t\forall \boldsymbol{y}\,(^tA\boldsymbol{y} \geqslant \boldsymbol{0} \rightarrow {}^t\boldsymbol{b}\boldsymbol{y} \leqslant 0)$.

Нетрудно видеть, что

$$\forall \boldsymbol{y}\,(^tA\boldsymbol{y} \geqslant \boldsymbol{0} \rightarrow {}^t\boldsymbol{b}\boldsymbol{y} \leqslant 0) \leftrightarrow \forall \boldsymbol{y}\,(\neg(^tA\boldsymbol{y} \geqslant \boldsymbol{0}) \vee ({}^t\boldsymbol{b}\boldsymbol{y} \leqslant 0)),$$
$$\leftrightarrow \forall \boldsymbol{y}\,\neg(^tA(\boldsymbol{y}) \geqslant \boldsymbol{0} \wedge {}^t\boldsymbol{b}\boldsymbol{y} > 0).$$

Таким образом, система (1) совместна тогда и только тогда, когда для каждого $\boldsymbol{y}$

$$\neg(^tA\boldsymbol{y} \geqslant \boldsymbol{0} \wedge {}^t\boldsymbol{b}\boldsymbol{y} > 0).$$

Следовательно, система (1) совместна тогда и только тогда, когда несовместна система (2). □

ТЕОРЕМА 1.12. *Система*

(1) $A\boldsymbol{x} + \boldsymbol{b} \leqslant \boldsymbol{0}, \ \boldsymbol{x} \geqslant \boldsymbol{0}$,

совместна тогда и только тогда, когда несовместна система

(2) ${}^tAy \geqslant 0,\ {}^tby > 0,\ y \geqslant 0.$

Доказательство. Пусть A — $m \times n$-матрица и $z = \begin{bmatrix} z_1 \\ \vdots \\ z_m \end{bmatrix}$. Нетрудно видеть, что система (1) совместна тогда и только тогда, когда совместна система

(1′) $Ax + z + b = 0,\ x \geqslant 0,\ z \geqslant 0.$

Пусть E — единичная $m \times m$-матрица, тогда

$$Ax + z + b = Ax + Ez + b = [A \mid E]\begin{bmatrix} x \\ z \end{bmatrix} + b.$$

Поэтому систему (1) можно записать в виде

$$[A \mid E]\begin{bmatrix} x \\ z \end{bmatrix} + b = 0,\ \begin{bmatrix} x \\ z \end{bmatrix} \geqslant 0.$$

Согласно теореме 1.11, система (1′) совместна тогда и только тогда, когда несовместна система

$$\begin{bmatrix} {}^tA \\ E \end{bmatrix} y \geqslant 0,\ {}^tby > 0,$$

т. е. несовместна система

$${}^tAy \geqslant 0,\ y \geqslant 0,\ {}^tby > 0.$$

Следовательно, система (1) совместна тогда и только тогда, когда несовместна система (2). □

Упражнения

1. Докажите, что любая система n однородных линейных неравенств с n переменными имеет ненулевые решения.

2. Докажите, что неравенство $Ax \leqslant 0$ имеет ненулевые решения тогда и только тогда, когда ненулевые решения имеет неравенство ${}^tAy \leqslant 0$.

3. Докажите, что любой выпуклый многогранник является множеством всех решений некоторой системы линейных неравенств.

4. Покажите, что множество всех решений совместной системы линейных неравенств можно представить в виде суммы выпуклого многогранника и выпуклого конуса, порожденного конечным множеством векторов.

§ 2. СТАНДАРТНЫЕ И КАНОНИЧЕСКИЕ ЗАДАЧИ ЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ. ТЕОРЕМЫ ДВОЙСТВЕННОСТИ

Стандартные и канонические задачи. Всюду ниже A есть $m \times n$-матрица над полем действительных чисел $\mathscr{R}$:

$$A = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ & \vdots & \\ \alpha_{m1} & \dots & \alpha_{mn} \end{bmatrix},$$

$\boldsymbol{b}$ и $\boldsymbol{c}$ — соответственно m-мерный и n-мерный векторы-столбцы над $\mathscr{R}$:

$$\boldsymbol{b} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix}, \quad \boldsymbol{c} = \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{bmatrix} \text{ и } {}^t\boldsymbol{b} = [\beta_1, \dots, \beta_m], \ {}^t\boldsymbol{c} = [\gamma_1, \dots, \gamma_n].$$

Линейную форму $\gamma_1 y_1 + \dots + \gamma_n y_n$ будем записывать в виде произведения строки ${}^t\boldsymbol{c}$ и столбца $\boldsymbol{y} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$, т. е.

$${}^t\boldsymbol{c}\boldsymbol{y} = \gamma_1 y_1 + \dots + \gamma_n y_n.$$

Линейную форму $\beta_1 z_1 + \dots + \beta_m z_m$ будем записывать в виде произведения строки ${}^t\boldsymbol{b}$ на столбец $\boldsymbol{z} = \begin{bmatrix} z_1 \\ \vdots \\ z_m \end{bmatrix}$;

$${}^t\boldsymbol{b}\boldsymbol{z} = \beta_1 z_1 + \dots + \beta_m z_m.$$

Основными задачами теории линейного программирования являются стандартные и канонические задачи на минимум и максимум.

Стандартная задача минимизации

С. *Найти решение системы*

$$(1) \quad \begin{array}{l} \alpha_{i1} y_1 + \dots + \alpha_{in} y_n + \beta_i \leqslant 0 \qquad (i = 1, \dots, m); \\ y_1 \geqslant 0, \dots, y_n \geqslant 0, \end{array}$$

которое минимизирует линейную форму $\gamma_1 y_1 + \dots + \gamma_n y_n$.

Стандартная задача максимизации

С*. *Найти решение системы*

$$(2) \quad \begin{array}{l} \alpha_{1k} z_1 + \dots + \alpha_{mk} z_m + \gamma_k \geqslant 0, \\ z_1 \geqslant 0, \dots, z_m \geqslant 0, \end{array}$$

которое максимизирует линейную форму $\beta_1 z_1 + \dots + \beta_m z_m$.

Условия (1) и (2) называются *линейными ограничениями* задач С и С* соответственно. Задачи С и С* называются *взаимно двойственными*.

В матричной форме эти задачи формулируются следующим образом:

С. *Найти решение системы*

$$(1)\quad A\boldsymbol{y}+\boldsymbol{b}\leqslant 0,\ \boldsymbol{y}\geqslant 0,$$

которое минимизирует линейную форму ${}^t\boldsymbol{cy}$.

С*. *Найти решение системы*

$$(2)\quad {}^tA\boldsymbol{z}+\boldsymbol{c}\geqslant 0,\ \boldsymbol{z}\geqslant 0,$$

которое максимизирует линейную форму ${}^t\boldsymbol{bz}$.

Каноническая задача минимизации

К. *Найти решение системы*

$$(I)\quad \begin{array}{l}\alpha_{i1}y_1+\ldots+\alpha_{in}y_n+\beta_i=0 \qquad (i=1,\ \ldots,\ m),\\ y_1\geqslant 0,\ \ldots,\ y_n\geqslant 0,\end{array}$$

которое минимизирует линейную форму $\gamma_1y_1+\ldots+\gamma_ny_n$.

Задача, двойственная к задаче К:

К*. *Найти решение системы*

$$(II)\quad \alpha_{1k}z_1+\ldots+\alpha_{mk}z_m+\gamma_k\geqslant 0 \qquad (k=i,\ \ldots,\ n),$$

которое максимизирует линейную форму $\beta_1z_1+\ldots+\beta_mz_m$.

Условия (I) и (II) называются *линейными ограничениями задач* К и К* соответственно. Задачи К и К* называются *взаимно двойственными*.

В матричной форме эти задачи формулируются следующим образом:

К. *Найти решение системы*

$$(I)\quad A\boldsymbol{y}+\boldsymbol{b}=0,\ \boldsymbol{y}\geqslant 0,$$

которое минимизирует линейную форму ${}^t\boldsymbol{cy}$.

К*. *Найти решение неравенства*

$$(II)\quad {}^tA\boldsymbol{z}+\boldsymbol{c}\geqslant 0,$$

которое максимизирует линейную форму ${}^t\boldsymbol{bz}$.

Допустимые и оптимальные векторы. Задача линейного программирования называется *допустимой*, если существует вектор, удовлетворяющий линейным ограничениям задачи. Если такой вектор существует, то он называется *допустимым вектором задачи*.

Допустимый вектор называется *решением задачи* или *оптимальным вектором задачи*, если он минимизирует (в задачах

С и К) или максимизирует (в задачах С* и К*) линейную форму задачи. Значение этого минимума или максимума называется *значением задачи линейного программирования.*

Обозначим через $x_1, \ldots, x_n$ левые части неравенств системы (II), т. е. положим

(3) $x_k = \alpha_{1k}z_1 + \ldots + \alpha_{mk}z_m + \gamma_k \qquad (k = 1, \ldots, n).$

ПРЕДЛОЖЕНИЕ 2.1. *Если вектор* $\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ *удовлетворяет неравенствам*

(1′) $\alpha_{i1}y_1 + \ldots + \alpha_{in}y_n + \beta_i \leqslant 0 \qquad (i = 1, \ldots, m),$

то

$$x_1y_1 + \ldots + x_ny_n \leqslant {}^t\boldsymbol{cy} - {}^t\boldsymbol{bz}.$$

Доказательство. Ввиду (3)

$$\begin{aligned} x_1y_1 + \ldots + x_ny_n &= (\alpha_{11}z_1 + \ldots + \alpha_{m1}z_m + \gamma_1)\,y_1 + \ldots \\ &\quad \ldots + (\alpha_{1n}z_1 + \ldots + \alpha_{mn}z_m + \gamma_n)\,y_n = \\ &= (\alpha_{11}y_1 + \ldots + \alpha_{1n}y_n)\,z_1 + \ldots + (\alpha_{m1}y_1 + \ldots \\ &\quad \ldots + \alpha_{mn}y_n)\,z_m + {}^t\boldsymbol{cy}. \end{aligned}$$

Отсюда в силу (1′)

$$\begin{aligned} x_1y_1 + \ldots + x_ny_n &\leqslant -(\beta_1z_1 + \ldots + \beta_mz_m) + {}^t\boldsymbol{cy} = \\ &= {}^t\boldsymbol{cy} - {}^t\boldsymbol{bz}. \quad \square \end{aligned}$$

СЛЕДСТВИЕ 2.2. *Если* $\boldsymbol{y}$ *— допустимый вектор стандартной задачи на минимум и* $\boldsymbol{z}$ *— допустимый вектор двойственной задачи, то*

$$0 \leqslant x_1y_1 + \ldots + x_ny_n \leqslant {}^t\boldsymbol{cy} - {}^t\boldsymbol{bz}.$$

ПРЕДЛОЖЕНИЕ 2.3. *Если вектор* $\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ *удовлетворяет системе уравнений*

(I′) $\alpha_{i1}y_1 + \ldots + \alpha_{in}y_n + \beta_i = 0 \qquad (i = 1, \ldots m),$

то

$$x_1y_1 + \ldots + x_ny_n = {}^t\boldsymbol{cy} - {}^t\boldsymbol{bz}.$$

Доказательство этого предложения аналогично доказательству предложения (2.1).

СЛЕДСТВИЕ 2.4. *Если* $\boldsymbol{y}$ *— допустимый вектор канонической задачи на минимум и* $\boldsymbol{z}$ *—* допустимый вектор двой-

ственной задачи, то

$$0 \leqslant x_1 y_1 + \ldots + x_n y_n = {}^t\boldsymbol{c}\boldsymbol{y} - {}^t\boldsymbol{b}\boldsymbol{z}.$$

ПРЕДЛОЖЕНИЕ 2.5. *Если* $\boldsymbol{y}$ *— допустимый вектор задачи на минимум* (С *или* К) *и* $\boldsymbol{z}$ *— допустимый вектор двойственной задачи* (С* *или* К*), *то* ${}^t\boldsymbol{c}\boldsymbol{y} - {}^t\boldsymbol{b}\boldsymbol{z} \geqslant 0$.

Предложение 2.5 непосредственно следует из следствий 2.2 и 2.4.

ПРЕДЛОЖЕНИЕ 2.6 (КРИТЕРИЙ ОПТИМАЛЬНОСТИ ВЕКТОРОВ). *Если* $\boldsymbol{y}$ *— допустимый вектор задачи на минимум,* $\boldsymbol{z}$ *— допустимый вектор двойственной задачи и* ${}^t\boldsymbol{c}\boldsymbol{y} = {}^t\boldsymbol{b}\boldsymbol{z}$, *то* $\boldsymbol{y}$ *и* $\boldsymbol{z}$ *являются оптимальными векторами соответствующих задач.*

Доказательство. Пусть $\boldsymbol{y}'$ — любой допустимый вектор задачи на минимум. Согласно предложению 2.5,

$${}^t\boldsymbol{c}\boldsymbol{y}' \geqslant {}^t\boldsymbol{b}\boldsymbol{z}.$$

Кроме того, по условию, ${}^t\boldsymbol{b}\boldsymbol{z} = {}^t\boldsymbol{c}\boldsymbol{y}$, поэтому ${}^t\boldsymbol{c}\boldsymbol{y}' \geqslant {}^t\boldsymbol{c}\boldsymbol{y}$ для любого допустимого вектора $\boldsymbol{y}'$ задачи на минимум. Следовательно, $\boldsymbol{y}$ является оптимальным вектором задачи на минимум.

Аналогично доказывается, что $\boldsymbol{z}$ является оптимальным вектором задачи на максимум. □

Теорема двойственности для стандартных задач. В теории линейного программирования основными являются теоремы двойственности 2.7 и 2.8.

ТЕОРЕМА 2.7. *Если обе взаимно двойственные стандартные задачи* (С *и* С*) *допустимы, то обе задачи имеют решения и значения этих задач совпадают. Если хотя бы одна из задач недопустима, то ни одна из задач не имеет решений.*

Доказательство. Предположим, что обе задачи допустимы. Тогда совместна система

(1) $\boldsymbol{A}\boldsymbol{y} + \boldsymbol{b} \leqslant 0$, $\boldsymbol{y} \geqslant 0$,

(2) ${}^t\boldsymbol{A}\boldsymbol{z} + \boldsymbol{c} \geqslant 0$, $\boldsymbol{z} \geqslant 0$.

Первая часть теоремы будет доказана, если мы докажем существование таких решений $\boldsymbol{y}$ и $\boldsymbol{z}$ соответственно (1) и (2) систем, что

(3) ${}^t\boldsymbol{c}\boldsymbol{y} - {}^t\boldsymbol{b}\boldsymbol{z} \leqslant 0$.

Действительно, в этом случае, по предложению 2.5, допустимые векторы $\boldsymbol{y}$ и $\boldsymbol{z}$ удовлетворяют неравенству

${}^tcy - {}^tbz \geqslant 0$. Поэтому если y и z удовлетворяют еще и (3), то ${}^tcy = {}^tbz$. Следовательно, в силу критерия оптимальности векторы y и z будут оптимальными векторами соответствующих задач (С и С*) и значения обеих задач будут совпадать. Таким образом, достаточно доказать совместность системы

$$(4)\quad \begin{cases} Ay + b \leqslant 0, & y \geqslant 0, \\ -{}^tAz - c \leqslant 0, & z \geqslant 0, \\ {}^tcy - {}^tbz \leqslant 0. \end{cases}$$

Запишем эту систему в матричной форме:

$$(4)\quad \begin{bmatrix} A & 0 \\ 0 & -{}^tA \\ {}^tc & -{}^tb \end{bmatrix} \cdot \begin{bmatrix} y \\ z \end{bmatrix} + \begin{bmatrix} b \\ -c \\ 0 \end{bmatrix} \leqslant 0, \quad \begin{bmatrix} y \\ z \end{bmatrix} \geqslant 0.$$

По теореме 2.6, система (4) совместна тогда и только тогда, когда несовместна система

$$(5)\quad \begin{bmatrix} {}^tA & 0 & c \\ 0 & -A & -b \end{bmatrix} \cdot \begin{bmatrix} u \\ v \\ \lambda \end{bmatrix} \geqslant 0, \ {}^tbu - {}^tcv > 0, \quad \begin{bmatrix} u \\ v \\ \lambda \end{bmatrix} \geqslant 0.$$

Эту систему можно записать в виде

$$(5)\quad \begin{aligned} & Av + b\lambda \leqslant 0, \\ & -{}^tAu - c\lambda \leqslant 0, \ u \geqslant 0, \ v \geqslant 0, \ \lambda \geqslant 0, \\ & {}^tcv - {}^tbu < 0. \end{aligned}$$

Покажем, что система (5) несовместна. Допустим, что существуют векторы u и v и действительное число λ, удовлетворяющие неравенствам (5). Тогда при $\lambda > 0$ имеем:

$$(5')\quad \begin{aligned} & A(v\lambda^{-1}) + b \leqslant 0, \ v\lambda^{-1} \geqslant 0, \\ & -{}^tA(u\lambda^{-1}) - c \leqslant 0, \ u\lambda^{-1} \geqslant 0, \\ & {}^tc(v\lambda^{-}) - {}^tb(u\lambda^{-1}) < 0. \end{aligned}$$

Первые четыре неравенства показывают, что векторы $v\lambda^{-1}$ и $u\lambda^{-1}$ удовлетворяют соответственно условиям (1) и (2), т. е. являются допустимыми векторами соответствующих задач. Следовательно, согласно предложению 2.5,

$${}^tc(v\lambda^{-1}) - {}^tb(u\lambda^{-1}) \geqslant 0,$$

что противоречит последнему неравенству (5').

Если же $\lambda=0$, то система (5) несовместна. Действительно, по условию, совместна система (1), (2), т. е. система

$$(6)\quad \begin{bmatrix} A & 0 \\ 0 & -{}^tA \end{bmatrix}\begin{bmatrix} y \\ z \end{bmatrix}+\begin{bmatrix} b \\ -c \end{bmatrix}\leqslant 0,\ \begin{bmatrix} y \\ z \end{bmatrix}\geqslant 0.$$

По теореме 2.6, из совместности системы (6) следует несовместность системы

$$\begin{bmatrix} {}^tA & 0 \\ 0 & -A \end{bmatrix}\begin{bmatrix} u \\ v \end{bmatrix}\geqslant 0,\ {}^tbu-{}^tcv>0,\ \begin{bmatrix} u \\ v \end{bmatrix}\geqslant 0,$$

т. е. несовместна система

$$Av\leqslant 0,$$
$$-{}^tAu\leqslant 0,\ u\geqslant 0,\ v\geqslant 0,$$
$${}^tcv-{}^tbu<0.$$

Таким образом, система (5) несовместна и поэтому совместна система (4).

Предположим теперь, что допустима только одна из двух взаимно двойственных стандартных задач, например допустима задача С, а задача С* недопустима. Докажем, что тогда задача С не имеет решений. Допустимость первой задачи означает, что существует решение y' системы (1), т. е.

$$(1')\quad Ay'+b\leqslant 0,\ y'\geqslant 0.$$

Недопустимость задачи С*, т. е. несовместность системы

$$(2)\quad -{}^tAz-c\leqslant 0,\ z\geqslant 0,$$

по теореме 1.12, влечет совместность системы

$$(2^*)\quad Ax\leqslant 0,\ {}^tcx<0,\ x\geqslant 0.$$

Следовательно, существует вектор x' такой, что

$$(2')\quad Ax'\leqslant 0,\ {}^tcx'<0,\ x'\geqslant 0.$$

На основании (1') и (2') заключаем, что для любого натурального n выполняются неравенства

$$(7)\quad A(y'+nx')+b\leqslant 0,\ y'+nx'\geqslant 0.$$

Значит, для любого натурального n вектор $y'+nx'$ является допустимым вектором первой задачи. Однако линейная форма ${}^tcy$ не имеет минимума. Действительно,

$${}^tc(y'+nx')={}^tcy'+n({}^tcx')$$

и в сумме справа первое слагаемое есть некоторое действительное число, а второе слагаемое ввиду ${}^tcx'<0$ может быть сделано при достаточно большом n меньше любого заданного числа. Следовательно, линейная форма ${}^tcy$ минимума не имеет, т. е. первая задача не имеет решений. □

Теорема двойственности для канонических задач. Рассмотрим канонические задачи К и К*:

К. *Найти решение системы* $Ay+b=0$, $y\geqslant 0$, *которое минимизирует линейную форму* ${}^tcy$.

К*. *Найти решение неравенства* ${}^tAz+c\geqslant 0$, *которое максимизирует линейную форму* ${}^tbz$.

Задача К равносильна следующей стандартной задаче:

C_1. *Найти решение системы*

$$\begin{bmatrix}-A\\ A\end{bmatrix}y+\begin{bmatrix}-b\\ b\end{bmatrix}\leqslant 0,\ y\geqslant 0,$$

которое минимизирует линейную форму ${}^tcy$.

Двойственной к C_1 является следующая задача:

C_1^*. *Найти решение системы*

$$[-{}^tA\,|\,{}^tA]\begin{bmatrix}z'\\ z''\end{bmatrix}+c\geqslant 0,\quad \begin{bmatrix}z'\\ z''\end{bmatrix}\geqslant 0,$$

где $z'=\begin{bmatrix}z_1\\ \vdots\\ z_m\end{bmatrix}$, $z''=\begin{bmatrix}z_{m+1}\\ \vdots\\ z_{2m}\end{bmatrix}$, *которое максимизирует линейную форму* $[-{}^tb\,|\,{}^tb]\begin{bmatrix}z'\\ z''\end{bmatrix}$.

Нетрудно убедиться, что задача C_1^* равносильна задаче К*. Действительно,

$$[-{}^tA\,|\,{}^tA]\begin{bmatrix}z'\\ z''\end{bmatrix}={}^tA(z''-z'),\ [-{}^tb\,|\,{}^tb]\begin{bmatrix}z'\\ z''\end{bmatrix}={}^tb(z''-z').$$

Любой m-мерный вектор можно представить в виде разности двух неотрицательных m-мерных векторов. Ввиду этого, если положить $z=z''-z'$, то z пробегает множество всех m-мерных векторов из $\mathbf{R}^m$, когда z'' и z' пробегают множество всех неотрицательных векторов из $\mathbf{R}^m$.

Следовательно, задача C_1^* равносильна следующей задаче (совпадающей с задачей К*). *Найти решение неравенства* ${}^t\boldsymbol{A}\boldsymbol{z}+\boldsymbol{c}\geqslant 0$, *которое максимизирует линейную форму* ${}^t\boldsymbol{b}\boldsymbol{z}$.

Стандартные задачи C_1 и C_1^* взаимно двойственны, и для них верна теорема двойственности. Задачи К и К* равносильны соответственно задачам C_1 и C_1^*. Поэтому теорема двойственности имеет место также для задач К и К*, т. е. верна следующая теорема.

ТЕОРЕМА 2.8. *Если обе взаимно двойственные канонические задачи* (К *и* К*) *допустимы, то обе задачи имеют решения и значения этих задач совпадают. Если хотя бы одна из задач недопустима, то ни одна из задач не имеет решений.*

Теорема равновесия. Напомним, что мы условились обозначать через $x_1, \ldots, x_n$ левые части неравенств системы (II),

$$x_k=\alpha_{1k}z_1+\ldots+\alpha_{mn}z_m \quad (k=1, \ldots, n).$$

ТЕОРЕМА 2.9. *Пусть* $\boldsymbol{y}=\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ *— допустимый вектор канонической задачи на минимум и* $\boldsymbol{z}=\begin{bmatrix} z_1 \\ \vdots \\ z_m \end{bmatrix}$ *— допустимый вектор двойственной задачи. Если*

(*) $x_1y_1=0, \ldots, x_ny_n=0,$

то $\boldsymbol{y}$ *и* $\boldsymbol{z}$ *являются оптимальными векторами соответствующих задач* (К *и* К*).

Доказательство. Предположим, что выполнены условия (*). По следствию 2.4 имеем

(1) $0\leqslant x_1y_1+\ldots+x_ny_n={}^t\boldsymbol{c}\boldsymbol{y}-{}^t\boldsymbol{b}\boldsymbol{z}.$

На основании (*) и (1) заключаем, что ${}^t\boldsymbol{c}\boldsymbol{y}-{}^t\boldsymbol{b}\boldsymbol{z}=0$. Согласно критерию оптимальности, векторы $\boldsymbol{y}$ и $\boldsymbol{z}$ являются оптимальными векторами соответственно задач К и К*. □

Замечание. Условие (*) также необходимо для оптимальности допустимых векторов $\boldsymbol{y}$ и $\boldsymbol{z}$. Действительно, по следствию 2.4, выполняется (1). Если векторы $\boldsymbol{y}$ и $\boldsymbol{z}$ оптимальны, то, по теореме 2.8,

(2) ${}^t\boldsymbol{c}\boldsymbol{y}={}^t\boldsymbol{b}\boldsymbol{z}.$

Из (1) и (2) следует

$$0 \leqslant x_1 y_1 + \ldots + x_n y_n = 0.$$

Поскольку y и z — допустимые векторы, то $x_1, \ldots, x_n \geqslant 0$ и $y_1, \ldots, y_n \geqslant 0$. Отсюда следуют равенства (*).

Упражнения

1. Покажите, что если одна из взаимно двойственных задач линейного программирования (канонических или стандартных) имеет решение, то другая задача также имеет решение.

2. Приведите пример такой стандартной (канонической) задачи на минимум с двумя переменными, чтобы ни сама задача, ни двойственная ей не были бы допустимыми.

3. Постройте пример стандартной задачи на минимум, которая имеет более одного оптимального решения.

§ 3. СИМПЛЕКС-МЕТОД

Симплекс-метод. Симплекс-метод для задач линейного программирования был разработан Данцигом. В изложенном ниже простом методе одновременного решения двух взаимно двойственных канонических задач мы следуем Холлу [27].

Рассмотрим взаимно двойственные канонические задачи.

K. *Найти решение системы*

$$\text{(I)} \quad \begin{array}{l} \alpha_{11} y_1 + \ldots + \alpha_{1n} y_n + \beta_1 = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \quad y_1 \geqslant 0, \ \ldots, \ y_n \geqslant 0, \\ \alpha_{m1} y_1 + \ldots + \alpha_{mn} y_n + \beta_m = 0, \end{array}$$

которое минимизирует линейную форму v:

$$\gamma_1 y_1 + \ldots + \gamma_n y_n = v.$$

K*. *Найти решение системы*

$$\text{(II)} \quad \begin{array}{l} \alpha_{11} z_1 + \ldots + \alpha_{m1} z_m + \gamma_1 \geqslant 0, \\ \ldots\ldots\ldots\ldots\ldots \\ \alpha_{1n} z_1 + \ldots + \alpha_{mn} z_m + \gamma_n \geqslant 0, \end{array}$$

которое максимизирует линейную форму u:

$$\beta_1 z_1 + \ldots + \beta_m z_m = u.$$

Симплекс-метод есть метод одновременного решения обеих взаимно двойственных канонических задач K и K*.

Пусть $A=\begin{bmatrix}\alpha_{11} & \dots & \alpha_{1n}\\ \dots & \dots & \dots\\ \alpha_{m1} & \dots & \alpha_{mn}\end{bmatrix}$ — матрица системы уравнений (I). Ниже мы будем предполагать, что ранг матрицы A равен m; это предположение несколько упрощает схему изложения симплекс-метода. Общий случай легко может быть сведен к этому случаю.

Рассмотрим таблицу

	η	η^*	
x^*	α	β	$=-y^*$
x	γ	δ	$=-y$
	$=z^*$	$=z$	

Эта таблица удобна для одновременного представления двух систем линейных уравнений. Она представляет линейную систему по строкам:

$$\begin{aligned}&\dots+\alpha\eta^*+\dots+\beta\eta+\dots=-y^*,\\ &\dots+\gamma\eta^*+\dots+\delta\eta+\dots=-y\end{aligned}\tag{1}$$

и по столбцам:

$$\begin{aligned}&\dots+\alpha x^*+\dots+\gamma x+\dots=z^*,\\ &\dots+\beta x^*+\dots+\delta x+\dots=z.\end{aligned}\tag{2}$$

Осевое преобразование таблицы с ведущим элементом α ($\alpha\neq 0$) — это такое преобразование, которое заменяет исходную таблицу таблицей, соответствующей решению системы (1) относительно $-\eta^*$ и решению системы (2) относительно x^*.

Решив уравнение системы (1), содержащее ведущий элемент α, относительно $-\eta^*$, имеем

$$\dots+\alpha^{-1}y^*+\dots+\alpha^{-1}\beta\eta+\dots=-\eta^*.$$

Подставив это выражение для $-\eta^*$ в другие уравнения системы (1), получим:

$$(1)\quad \begin{aligned} &\ldots+\alpha^{-1}y^*+\ldots+\alpha^{-1}\beta\eta+\ldots=-\eta^*,\\ &\ldots-\alpha^{-1}\gamma y^*+\ldots+(\delta-\alpha^{-1}\beta\gamma)\,\eta+\ldots=-y. \end{aligned}$$

Аналогично, решая систему (2) относительно x^*, получим

$$(2)\quad \begin{aligned} &\ldots+\alpha^{-1}z^*+\ldots+(-\alpha^{-1}\gamma)x+\ldots=x^*,\\ &\ldots+\alpha^{-1}\beta z^*+\ldots+(\delta-\alpha^{-1}\beta\gamma)\,x+\ldots=z. \end{aligned}$$

Таким образом, осевое преобразование таблицы с ведущим элементом α заменяет исходную таблицу следующей таблицей:

	y^*	η	
z^*	$\ldots\alpha^{-1}\ldots$	$\alpha^{-1}\beta\ \ldots$	$=-\eta^*$
x	$\ldots-\alpha^{-1}\gamma\ldots$	$\delta-\alpha^{-1}\beta\gamma\ldots$	$=-y$
	$\ldots=x^*$	$\ldots\ =z$	

соответствующей решению системы (1) по строкам относительно $-\eta^*$ и системы (2) по столбцам относительно x^*.

Обе взаимно двойственные канонические задачи K и K* представляет таблица

T_1

	y_1	$\ldots$	y_n	1	
z_1	α_{11}	$\ldots$	α_{1n}	β_1	$=0$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
z_m	α_{m1}	$\ldots$	α_{mn}	β_m	$=0$
1	γ_1	$\ldots$	γ_m	0	$=v$
	$=x_1$	$\ldots$	$=x_n$	$=u$	

Будем искать одновременно решение обеих задач. Вначале исключим переменные $z_1, \ldots, z_m$, на которые не наложены ограничения. Это первый этап решения. Он осуществляется при помощи цепочки осевых преобразований, исходя из таблицы T_1. Этот процесс продолжается до тех пор, пока в таблице можно найти ненулевой эле-

мент с y наверху и с нулем справа в строке. В результате приходим к таблице вида

	y'_{m+1}	…	y'_n	0	…	0	1	
x'_1								$=-y'_1$
⋮								⋮
x'_m								$=-y'_m$
1	γ'_{m+1}	…	γ'_n					$=v$
	$=x'_{m+1}$		$=x'_n=z'_1\ldots=z'_m=u$					

T'_1

$(x'_i \geqslant 0,\ y'_j \geqslant 0)$

В этой таблице переменные со штрихами — это размещенные иначе переменные, входящие в исходную таблицу T_1, а строки и столбцы переставлены в соответствии с положением нулей. Последние m столбцов представляют уравнения, выражающие переменные $z'_1, \ldots, z'_m$ через переменные $x'_1, \ldots, x'_m$. Эти уравнения надо выписать:

$$\text{(III)}\quad \begin{aligned} z'_1 &= d_{11}x'_1+\ldots+d_{1m}x'_m,\\ &\ldots\ldots\ldots\ldots\\ z'_m &= d_{m1}x'_1+\ldots+d_{mm}x'_m. \end{aligned}$$

Далее необходимо рассмотреть только те равенства, которые связывают переменные x'_i и y'_j и выражаются той частью таблицы T'_1, которая содержит первые $n-m$ столбцов. Таким образом, в результате исключения переменных $z_1, \ldots, z_m$ приходим к таблице

	y_{m+1}	…	y_n	1	
x_1				β_1	$=-y_1$
⋮				⋮	⋮
x_m				β_m	$=-y_m$
1	c_{m+1}	…	c_n	d	$=v$
	x_{m+1}		x_n	u	

T

Таблицу T называют *допустимой по строкам*, если выполнены условия

(1) $\beta_1 \leqslant 0, \ldots, \beta_m \leqslant 0.$

Эти условия означают, что вектор $(-\beta_1, \ldots, -\beta_m, 0, \ldots, 0)$ является допустимым вектором задачи K, т. е. удовлетворяет системе (I). Предположим, что таблица T допустима по строкам, т. е. выполнены условия (1). Цель

следующего этапа решения задачи состоит в том, чтобы по таблице, полученной из Т в результате цепочки осевых преобразований, найти допустимые векторы обеих задач (К и К*), которые удовлетворяют условиям

(*) $x_1y_1=0,\ \ldots,\ x_ny_n=0 \qquad (x_i\geqslant 0,\ y_j\geqslant 0).$

По теореме равновесия, такие векторы будут оптимальными векторами соответствующих задач.

Введем обозначения: $\oplus$ — неотрицательное число, $\ominus$ — неположительное число. Допустим, что мы, исходя из таблицы Т, сможем перейти к таблице вида

	$\ominus$ $\vdots$ $\ominus$
$\oplus \ldots \oplus$	

Тогда, придавая свободным переменным $x_1, \ldots, x_m$ и $y_{m+1}, \ldots, y_n$ значения, равные нулю, получим допустимые векторы для обеих задач (К и К*), которые являются оптимальными векторами этих задач.

Рассмотрим влияние осевого преобразования с ведущим элементом α_{rs} на столбец свободных членов и на значение линейной формы v, подлежащей минимизации:

$\alpha_{rs} \ldots \beta_r$	$\ldots\ \alpha_{rs}^{-1} \ldots \alpha_{rs}^{-1}\beta_r,$
. . . . .	. . . .
$\alpha_{is} \ldots \beta_i$	$\ldots -\alpha_{rs}^{-1}\alpha_{is} \ldots \beta_i-\alpha_{rs}^{-1}\beta_r\alpha_{is},$
. . . . .	. . . .
$\gamma_s \ldots \delta$	$\ldots -\alpha_{rs}^{-1}\gamma_s \ldots \delta-\alpha_{rs}^{-1}\beta_r\gamma_s.$

Мы предполагаем, что в таблице (слева) элементы β_i столбца свободных членов неположительны, т. е.

(1) $\beta_i\leqslant 0 \quad (i=1, \ldots, m).$

Мы хотим, чтобы новое значение линейной формы v не было больше предыдущего, т. е. $\delta-\alpha_{rs}^{-1}\beta_r\gamma_s\leqslant\delta$. Это неравенство выполняется, если выполняются условия

(α) $\alpha_{rs}>0,\ \gamma_s<0.$

При выполнении этих условий новое значение линейной формы v не больше предыдущего, причем новое значение формы v при $\beta_r<0$ строго меньше предыдущего.

Кроме того, мы хотим, чтобы новые элементы столбца свободных членов были неположительны, т. е.

$$\beta_i - \alpha_{rs}^{-1}\beta_r\alpha_{is} \leqslant 0.$$

При выполнении условий (α) и при $\alpha_{is} \leqslant 0$ это неравенство выполняется. Если же $\alpha_{is} > 0$, то неравенство можно записать в виде

(β) $\dfrac{\beta_r}{\alpha_{rs}} \geqslant \dfrac{\beta_i}{\alpha_{is}}$ при всех $\alpha_{is} > 0 \quad (i \neq r)$.

Таким образом, мы приходим к следующему *правилу выбора ведущего элемента* осевого преобразования таблицы, которая допустима по строкам.

Пусть таблица допустима по строкам. *В качестве ведущего элемента (при осевом преобразовании) следует выбирать элемент α_{rs}, если выполнены условия:*

(α) $\gamma_s < 0$, $\alpha_{rs} > 0$;

(β) $\dfrac{\beta_r}{\alpha_{rs}} \geqslant \dfrac{\beta_i}{\alpha_{is}}$ при $\alpha_{is} > 0 \quad (i \neq r)$.

Выбор ведущего элемента в соответствии с этим правилом обеспечивает допустимость новой таблицы по строкам и при $\beta_r < 0$ дает новое значение линейной формы v (подлежащей минимизации), строго меньшее, чем предыдущее.

Исходя из таблицы допустимой по строкам, осуществляют цепочку осевых преобразований, руководствуясь правилом выбора ведущего элемента. Процесс заканчивается, если в последней строке таблицы нет отрицательных элементов; это будет означать, что таблица допустима и по строкам и по столбцам, т. е. найдены решения обеих задач K и K* (найдены оптимальные векторы).

Процесс заканчивается также в том случае, когда в таблице встретится отрицательный (не последний) столбец вида

и, значит, правило выбора ведущего элемента неприменимо. Это будет означать, что задача K* недопустима, так как нельзя удовлетворить условию $x_s \geqslant 0$.

Таблица T может оказаться недопустимой и по строкам, и по столбцам. В этом случае, стремясь найти допустимое решение задачи K или установить недопустимость задачи K*, поступаем следующим образом. Строки таблицы T переставим так, чтобы все допустимые строки были расположены вверху таблицы:

	y_{m+1} … y_n	1	
x_1		$\ominus$	$= -y_1$
⋮		⋮	⋮
x_k		$\ominus$	$= -y_k$
x_{k+1}		$+$	$= -y_{k+1}$
⋮		⋮	⋮
x_m		$+$	$= -y_m$
1	γ_{m+1} … γ_n		

Первые $k+1$ строк этой таблицы будем рассматривать как таблицу, допустимую по строкам, и постараемся минимизировать $(-y_{k+1})$. Если на каком-либо шаге мы достигнем неположительного значения для $(-y_{k+1})$, то получим $k+1$ допустимых строк или больше. Продолжаем процесс аналогичным образом, стремясь представить в допустимой форме как можно больше строк. Если при этом в таблице появится плюсовая строка, т. е. (недопустимая) строка вида

$\oplus$ … $\oplus$	$+$

то это будет означать, что задача K недопустима, так как невозможно удовлетворить условию $-y_j \leqslant 0$.

Если же окажется, что минимальное значение $(-y_{k+1})$ положительно, то появляется таблица вида

		$\ominus$	
		⋮	
		$\ominus$	
$-$		$+$	$= -y_{k+1}$

В этом случае в качестве ведущего выбираем элемент, отмеченный стрелкой. Легко проверить, что такой выбор дает $k+1$ допустимых строк или еще больше. Таким

образом, описан способ нахождения допустимого решения задачи K во всех возможных случаях.

Задача. Найти решение системы

$$5y_1 - 4y_2 + 13y_3 - 2y_4 + y_5 - 20 = 0,$$

(I) $$y_1 - y_2 + 5y_3 - y_4 + y_5 - 8 = 0,$$

$$y_1 \geqslant 0,\ y_2 \geqslant 0,\ y_3 \geqslant 0,\ y_4 \geqslant 0,\ y_5 \geqslant 0,$$

которое минимизирует линейную форму v,

$$y_1 + 6y_2 - 7y_3 + y_4 + 5y_5 = v.$$

Задача, двойственная данной, формулируется так: найти решение системы

$$x_1 = 5z_1 + z_2 + 1 \geqslant 0,$$

$$x_2 = -4z_1 - z_2 + 6 \geqslant 0,$$

(II) $$x_3 = 13z_1 + 5z_2 - 7 \geqslant 0,$$

$$x_4 = -2z_1 - z_2 + 1 \geqslant 0,$$

$$x_5 = z_1 + z_2 + 5 \geqslant 0,$$

которое максимизирует линейную форму u,

$$-20z_1 - 8z_2 = u.$$

Обе эти задачи представляет следующая таблица:

	y_1	y_2	y_3	y_4	y_5	1	
z_1	5	−4	13	−2	1	−20	$=0$
z_2	1	−1	5	−1	1	−8	$=0$
1	1	6	−7	1	5	0	$=v$
	x_1	x_2	x_3	x_4	x_5	$=u$	

Будем искать одновременно решения обеих задач. Вначале исключим неизвестные z_1 и z_2. Исключая z_2 при помощи осевого преобразования с ведущим элементом 1, отмеченным жирным шрифтом, получим

	y_1	y_2	y_3	y_4	0	1	
z_1	4	−3	8	−1	−1	−12	$=0$
x_5	1	−1	5	−1	1	−8	$=-y_5$
1	−4	11	−32	6	−5	40	$=v$
	x_1	x_2	x_3	x_4	z_2	$=u$	

Теперь исключим z_2 осевым преобразованием с ведущим элементом 4 в первом столбце:

	0	y_2	y_3	y_4	0	1	
x_1	1/4	—3/4	2	—1/4	—1/4	—3	$=-y_1$
x_5	—1/4	—1/4	3	—3/4	5/4	—5	$=-y_5$
1	1	8	—24	5	—6	28	$=v$
	z_1	x_2	x_3	x_4	z_2	$=u$	

Из первого и пятого столбцов видно, что z_1 и z_2 выражаются через x_1 и x_5 следующим образом:

$$\text{(III)}\quad \begin{aligned} z_1 &= \tfrac{1}{4}x_1 - \tfrac{1}{4}x_5 + 1; \\ z_2 &= -\tfrac{1}{4}x_1 + \tfrac{5}{4}x_5 - 6. \end{aligned}$$

Исключая первый и пятый столбцы в предыдущей таблице, получим

	y_2	y_3	y_4	1	
x_1	—3/4	2	—1/4	—3	$=-y_1$
x_5	—1/4	3	—3/4	—5	$=-y_5$
1	8	—24	5	28	$=v$
	x_2	x_3	x_4	$=u$	

Эта таблица допустима по строкам. В соответствии с правилом выбора ведущего элемента выбираем элемент 2 во втором столбце и, произведя осевое преобразование, приходим к таблице

	y_2	y_1	y_4	1	
x_3	—3/8	1/2	—1/8	—3/2	$=-y_3$
x_5	7/8	—3/2	—3/8	—1/2	$=-y_5$
1	—1	12	2	—8	$=v$
	x_2	x_1	x_4	$=u$	

В полученной таблице выбираем элемент 7/8 в первом столбце в качестве ведущего элемента и, произведя осевое

преобразование, приходим к таблице

	y_5	y_1	y_4	1	
x_3	3/7	—1/7	—2/7	—12/7	$=-y_3$
x_2	8/7	—12/7	—3/7	—4/7	$=-y_2$
1	8/7	72/7	11/7	—60/7	$=v$
	x_5	x_1	x_4	$=u$	

Эта таблица допустима как по строкам, так и по столбцам. Полагая «свободные» переменные x_2, x_3, y_1, y_4, y_5 равными нулю, получим:

$$x_1=72/7,\ x_2=0,\ x_3=0,\ x_4=11/7,\ x_5=8/7,$$
$$y_1=0,\ y_2=4/7,\ y_3=12/7,\ y_4=0,\ y_5=0.$$

Подставляя найденные значения x_1 и x_5 в формулы (III), получим $z_1=23/7$, $z_2=-50/7$. Следовательно, вектор (0, 4/7, 12/7, 0, 0) есть решение первой задачи, а вектор $(23/7, -50/7)$ — решение двойственной задачи. При этом $u=v=-60/7$, т. е. минимальное значение линейной формы v и максимальное значение линейной формы u равно $(-60/7)$.

Упражнения

1. Максимизируйте линейную форму $2x_1+3x_2$ при условиях $4x_1+2x_2+x_3=4$, $x_1+3x_2=5$.

2. Максимизируйте линейную форму $x_1+3x_2+x_3$ при условиях $5x_1+3x_2\leqslant 3$, $x_1+2x_2+4x_3\leqslant 4$.

3. Разрешите вопрос о совместности системы линейных неравенств

$$5x_1+4x_2-7x_3\leqslant 1,$$
$$-x_1+2x_2-x_3\leqslant -4,$$
$$-3x_1-2x_2+4x_3\leqslant 3,$$
$$3x_1-2x_2-2x_3\leqslant -7.$$

4. Выясните, совместна ли следующая система линейных неравенств:

$$4x_1-5x_2\geqslant 3,$$
$$-2x_1-7x_2\geqslant 1,$$
$$-2x_1+x_2\geqslant -2?$$

5. Имеет ли система линейных уравнений

$$3x_1-5x_2+2x_3=0,$$
$$2x_1-4x_2+x_3=0$$

неотрицательные ненулевые решения?

6. Докажите, что система линейных неравенств

$$5x_1 - 4x_2 \leqslant 7,$$
$$-3x_1 + 3x_2 \leqslant -5$$

не имеет неотрицательных решений.

7. Найдите неотрицательное решение системы линейных уравнений:

$$5x_1 + x_2 + 6x_3 - 5x_5 = 2;$$
$$-7x_1 - x_2 - 2x_3 + x_4 + 2x_5 = -5.$$

Глава десятая

ГРУППЫ

§ 1. ПОЛУГРУППЫ И МОНОИДЫ

Полугруппы. Пусть A — непустое множество. Бинарная операция $*$ на множестве A называется *ассоциативной*, если $a*(b*c)=(a*b)*c$ для любых элементов a, b, c из A. Бинарная операция $*$ называется *коммутативной*, если для любых a, b из A $a*b=b*a$.

Так, например, операции сложения и умножения целых чисел ассоциативны и коммутативны. Операция вычитания целых чисел неассоциативна и некоммутативна.

ОПРЕДЕЛЕНИЕ. *Полугруппой* называется алгебра $\langle A, *\rangle$ типа (2) с бинарной ассоциативной операцией $*$. Подалгебра полугруппы называется *подполугруппой*.

Примеры. 1. Пусть $+$ есть операция сложения на множестве $\mathbf{N}$ натуральных чисел. Алгебра $\langle \mathbf{N}, +\rangle$ есть полугруппа, так как операция сложения ассоциативна. Эта полугруппа называется *аддитивной полугруппой натуральных чисел*.

2. Пусть M — непустое множество и A — совокупность всех отображений множества M в себя с законом композиции отображений $\circ$ в качестве бинарной операции. Алгебра $\langle A, \circ\rangle$ есть полугруппа, так как композиция отображений ассоциативна. Эта полугруппа называется *полугруппой отображений множества M в себя*.

Моноиды. Пусть A — множество с бинарной операцией $*$. Элемент e из A называется *нейтральным относительно операции* $*$, если $a*e=e*a=a$ для любого a из A.

ОПРЕДЕЛЕНИЕ. *Моноидом* называется алгебра $\langle A, *, e\rangle$ типа (2, 0), главные операции которой удовлетворяют условиям:

(1) бинарная операция $*$ ассоциативна:

(2) элемент e является нейтральным относительно операции $*$.

Примеры. 1. Пусть $+$ есть операция сложения на множестве $\mathbf{N}$ натуральных чисел. Алгебра $\langle \mathbf{N}, +, 0\rangle$ есть моноид, так как сложение ассоциативно и 0 является нейтральным элементом относительно сложения. Этот моноид называется *аддитивным моноидом натуральных чисел.*

2. Пусть $\cdot$ есть операция умножения на множестве $\mathbf{N}$ натуральных чисел. Алгебра $\langle \mathbf{N}, \cdot, 1\rangle$ есть моноид, так как умножение ассоциативно и 1 есть нейтральный элемент относительно умножения. Этот моноид называется *мультипликативным моноидом натуральных чисел.*

3. Пусть n — фиксированное натуральное число, отличное от нуля, A — совокупность всех отображений множества $\{1, \ldots, n\}$ в себя и ε — тождественное отображение этого множества. Алгебра $\langle A, \circ, \varepsilon\rangle$, где $\circ$ есть бинарная операция — композиция отображений, является моноидом, так как композиция отображений ассоциативна и ε есть нейтральный элемент относительно операции $\circ$. Этот моноид называется *моноидом отображений множества* $\{1, \ldots, n\}$ *в себя.*

4. Пусть $\mathcal{K} = \langle K, +, -, \cdot, 1\rangle$ — кольцо. Тогда алгебра $\langle K, \cdot, 1\rangle$ есть моноид. Он называется *мультипликативным моноидом кольца* $\mathcal{K}$.

Обобщенный закон ассоциативности. Пусть A — непустое множество и $*$ есть бинарная операция на нем. Пусть $a_1, a_2, \ldots, a_n$ — последовательность n элементов из A. Символом

$$a_1 * a_2 * \ldots * a_n$$

обозначим *композицию последовательности элементов*, определяемую индуктивно следующим образом:

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

Согласно этому определению,

$$a * b * c = (a * b) * c;\ a * b * c * d = (a * b * c) * d.$$

Если закон композиции — умножение, то композиция элементов $a_1, \ldots, a_n$ называется *произведением* и обычно обозначается через $\prod_{i=1}^{n} a_i$; при аддитивной записи композиция элементов $a_1, \ldots, a_n$ называется *суммой* и обычно обозначается через $\sum_{i=1}^{n} a_i$.

Если бинарная операция $*$ на множестве A ассоциативна, то легко показать, что

$$\begin{aligned} a*b*c*d &= (a*b)*(c*d) = \\ &= a*(b*c)*d = \\ &= (a*b*c)*d = \\ &= a*(b*c*d). \end{aligned}$$

В случае ассоциативной бинарной операции на A при рассмотрении композиции любой последовательности элементов из A можно любым образом расставлять скобки, как показывает следующая теорема.

ТЕОРЕМА 1.1. *Пусть A — множество с ассоциативной бинарной операцией $*$ и $a_1, \ldots, a_n$ — последовательность элементов из A. Пусть $1 < n_1 < n_2 < \ldots < n_k \leqslant n$, где $n_1, \ldots, n_k$ — натуральные числа, и*

$$b_0 = a_1 * \ldots * a_{n_1-1},\ b_1 = a_{n_1} * \ldots * a_{n_2-1}, \ldots, b_k = a_{n_k} * \ldots * a_n,$$

тогда $a_1 * \ldots * a_n = b_0 * \ldots * b_k$.

Доказательство (проводится индукцией по n). Если $n = 2$, то теорема, очевидно, верна. Предположим, что теорема верна, если последовательность содержит не более $n-1$ элементов.

Первый случай: $n_k = n$. В этом случае $b_k = a_n$. По определению,

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

По индуктивному предположению,

$$a_1 * \ldots * a_{n-1} = b_0 * \ldots * b_{k-1};$$

следовательно,

$$a_1 * \ldots * a_n = (b_0 * \ldots * b_{k-1}) * b_k = b_0 * \ldots * b_k.$$

Второй случай: $n_k < n$. В этом случае

$$b_k = (a_{n_k} * \ldots * a_{n-1}) * a_n = b_k' * a_n,$$

где $b_k' = a_{n_k} * \ldots * a_{n-1}$, и

$a_1 * \ldots * a_{n-1} = b_0 * \ldots * b_k'$ (по индуктивному предположению);

следовательно,

$$\begin{aligned} a_1 * \ldots * a_n &= (a_1 * \ldots * a_{n-1}) * a_n = \\ &= (b_0 * \ldots * b'_k) * a_n = \text{ (по индуктивному предположению)} \\ &= ((b_0 * \ldots * b_{k-1}) * b'_k) * a_n = \\ &= (b_0 * \ldots * b_{k-1}) * (b'_k * a_n) = \\ &= (b_0 * \ldots * b_{k-1}) * b_k = \\ &= b_0 * \ldots * b_k. \ \square \end{aligned}$$

Рассмотрим тот частный случай, когда бинарная ассоциативная операция на множестве A есть умножение и $a_1 = a_2 = \ldots = a_n = a$, где $a \in A$. Тогда, по определению,

$$a^n = a_1 \cdot a_2 \ldots a_n = \prod_{i=1}^{n} a_i.$$

СЛЕДСТВИЕ 1.2. *Пусть A — множество с заданной на нем бинарной ассоциативной операцией, умножением, и $a \in A$. Тогда для любых отличных от нуля натуральных чисел m и n имеем:*

$$a^{m+n} = a^m a^n, \ a^{mn} = (a^m)^n.$$

Рассмотрим также случай, когда бинарная ассоциативная операция на множестве A называется сложением и $a_1 = a_2 = \ldots = a_n = a$, где $a \in A$. Тогда, по определению,

$$na = a_1 + \ldots + a_n = \sum_{i=1}^{n} a_i.$$

СЛЕДСТВИЕ 1.3. *Пусть A — множество с заданной на нем бинарной ассоциативной операцией, сложением и $a \in A$. Тогда*

$$(m+n)a = ma + na, \ (mn)a = m(na)$$

для любых отличных от нуля натуральных чисел n и m.

Упражнения

1. Пусть $\langle A, \cdot, 1 \rangle$ — мультипликативный моноид. Докажите, что для всякого элемента a моноида и любых натуральных m и n выполняются соотношения

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

2. Пусть $\langle A, +, 0 \rangle$ — аддитивный моноид и $a \in A$. Покажите, что для любых натуральных m и n

$$ma + na = (m+n)a, \ n(ma) = (nm)a.$$

3. Пусть $\langle \mathbf{N}, + \rangle$ — аддитивная полугруппа натуральных чисел. Найдите систему образующих этой полугруппы.

4. Пусть $\langle \mathbf{N}, +, 0 \rangle$ — аддитивный моноид натуральных чисел. Опишите все подмоноиды этого моноида.

5. Пусть $\langle \mathbf{N}^*, \cdot \rangle$ — мультипликативная полугруппа натуральных чисел, отличных от нуля. Найдите минимальную систему образующих этой полугруппы.

6. Пусть $\langle \mathbf{N}, \cdot \rangle$ — мультипликативная полугруппа натуральных чисел. Найдите систему образующих полугруппы, которая содержится во всякой другой системе образующих этой полугруппы.

§ 2. ПОДГРУППЫ И СМЕЖНЫЕ КЛАССЫ

Подгруппы. Пусть M — непустое множество и S_M — множество всех подстановок множества M, т. е. совокупность всех инъективных отображений множества M на себя. Если f и g — подстановки множества M, то их композиция $f \circ g$ и обратное отображение f^{-1} суть подстановки множества M.

ТЕОРЕМА 2.1. *Алгебра* $\langle S_M, \circ, {}^{-1} \rangle$ *является группой.*

Доказательство. Бинарная операция $\circ$ на S_M, композиция подстановок множества M, ассоциативна в силу теоремы 2.2. Тождественная подстановка i_M есть нейтральный элемент относительно операции $\circ$. Для любой подстановки f множества M $f \circ f^{-1} = i_M$. Следовательно, алгебра $\langle S_M, \circ, {}^{-1} \rangle$ является группой. □

ОПРЕДЕЛЕНИЕ. Группа $\langle S_M, \circ, {}^{-1} \rangle$ называется *симметрической группой* на множестве M и обозначается через $\mathfrak{S}_M$. Если множество M конечно и состоит из n элементов, то группа $\mathfrak{S}_M$ называется *симметрической группой n-й степени* и обозначается также через $\mathfrak{S}_n$.

Пусть $\mathfrak{G} = \langle G, \cdot, {}^{-1} \rangle$ — мультипликативная группа. Каждому элементу a группы поставим в соответствие отображение t_a множества G на G, определяемое формулой

$$t_a(x) = ax \text{ для всякого } x \text{ из } G.$$

Отображение t_a есть подстановка множества G и называется *левой трансляцией* G. Множество $T(G) = \{t_a \mid a \in G\}$ называется *множеством левых трансляций* G.

ПРЕДЛОЖЕНИЕ 2.2. Пусть $\mathfrak{S}_G = \langle S_G, \cdot, {}^{-1} \rangle$ — *симметрическая группа на множестве* G. *Алгебра* $\mathfrak{T} = \langle T(G), \cdot, {}^{-1} \rangle$ *является подгруппой группы* $\mathfrak{S}_G$.

Доказательство. Для любых элементов a, b группы $\mathfrak{G}$ имеют место равенства

(1) $t_a \cdot t_b = t_{ab}$ и $t_a \cdot t_a^{-1} = i_G = t_e$,

где e — единица группы $\mathscr{G}$. В самом деле, для любого x из G

$(t_a \cdot t_b)(x) = t_a(t_b(x)) = t_a(bx) = abx = t_{ab}(x)$, т. е.
$t_a \cdot t_b = t_{ab}$.

Полагая в последнем равенстве $b = a^{-1}$, имеем $t_a \cdot t_a^{-1} = t_e = i_G$, где e — единица группы $\mathscr{G}$.

Кроме того, в силу (1) $t_a \cdot t_e = t_{ae} = t_a$ и

(2) $(t_a)^{-1} = t_a^{-1} \in T(G)$.

На основании (1) и (2) заключаем, что множество $T(G)$ замкнуто относительно главных операций группы $S(G)$. Следовательно, алгебра $\langle T(G), \cdot, {}^{-1}\rangle$ есть подгруппа группы S_G. □

ТЕОРЕМА 2.3 (КЭЛИ). *Любая группа $\mathscr{G} = \langle G, \cdot, {}^{-1}\rangle$ изоморфна подгруппе симметрической группы на множестве G. В частности, каждая конечная группа порядка n изоморфна подгруппе симметрической группы n-й степени.*

Доказательство. Пусть $T(G)$ — совокупность всех левых трансляций множества G. По теореме 2.2, группа $\mathscr{T} = \langle T(G), \cdot, {}^{-1}\rangle$ есть подгруппа группы S_G.

Пусть h — отображение множества G на $T(G)$, определяемое формулой

$h(a) = t_a$ для любого a из G.

Отображение h сохраняет главные операции группы $\mathscr{G}$. В самом деле, в силу (1) и (2)

$h(ab) = t_{ab} = t_a \cdot t_b = h(a) \cdot h(b)$,
$h(a^{-1}) = t_{a^{-1}} = (t_a)^{-1} = (h(a))^{-1}$.

Кроме того, h есть инъективное отображение. Действительно, для любых a, b множества G, если $h(a) = h(b)$, то $t_a = t_b$, $t_a(l) = t_b(e)$, где e — единица группы $\mathscr{G}$, $ae = be$, и, значит, $a = b$. Следовательно, h является изоморфизмом группы $\mathscr{G}$ на подгруппу $\mathscr{T}$ симметрической группы S_G на множество G. □

Смежные классы. Пусть $\mathscr{H} = \langle H, \cdot, {}^{-1}\rangle$ — подгруппа группы $\mathscr{G} = \langle G, \cdot, {}^{-1}\rangle$. На множестве G введем бинарное отношение $\equiv$:

$a \equiv b \pmod{H}$ тогда и только тогда, когда $ab^{-1} \in H$; назовем его *отношением сравнения по подгруппе* $\mathscr{H}$.

ПРЕДЛОЖЕНИЕ 2.4. *Пусть $\mathscr{H}$ — подгруппа группы $\mathscr{G}$. Отношение сравнения на G по подгруппе $\mathscr{H}$ является отношением эквивалентности.*

Доказательство. Так как $aa^{-1} \in H$, то $a \equiv a \pmod{H}$, т. е. отношение сравнения по $\mathscr{H}$ рефлексивно. Поскольку из $ab^{-1} \in H$ следует $ba^{-1} \in H$, то из $a \equiv b \pmod{H}$, следует $b \equiv a \pmod{H}$, — отношение сравнения по $\mathscr{H}$ симметрично. Далее, для любых элементов a, b, c из G, если $ab^{-1} \in H$ и $bc^{-1} \in H$, то $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$. Следовательно, если $a \equiv b$ и $b \equiv c \pmod{H}$, то $a \equiv c \pmod{H}$, — отношение сравнения по H транзитивно. Таким образом, отношение сравнения по $\mathscr{H}$ является отношением эквивалентности. □

ПРИМЕР. Пусть $\langle V, +, - \rangle$ — аддитивная группа векторного пространства $\mathscr{V}$, $\mathscr{L}$ — подпространство пространства $\mathscr{V}$ и $\langle L, +, - \rangle$ — его аддитивная группа. Рассмотрим на V бинарное отношение $\sim$:

$a \sim b$ тогда и только тогда, когда $a - b \in L$, называемое *отношением сравнения векторов из V по направлению $\mathscr{L}$*. Это отношение является отношением эквивалентности на V. Классы эквивалентности называются линейными многообразиями пространства $\mathscr{V}$ с направлением $\mathscr{L}$.

ОПРЕДЕЛЕНИЕ. Классы эквивалентности отношения сравнения по подгруппе $\mathscr{H}$ называются *правыми смежными классами группы $\mathscr{G}$* по подгруппе $\mathscr{H}$.

Отметим основные свойства смежных классов.

СВОЙСТВО 2.1. *Любые два правых смежных класса группы $\mathscr{G}$ по подгруппе $\mathscr{H}$ либо совпадают, либо не пересекаются. Множество G является объединением всех правых смежных классов группы $\mathscr{G}$ по подгруппе $\mathscr{H}$.*

Это свойство непосредственно следует из теоремы 2.4.1

Пусть $g \in G$. Обозначим через Hg множество, определяемое равенством $Hg = \{hg \mid h \in H\}$.

СВОЙСТВО 2.2. *Если $g \in G$, то Hg является правым смежным классом группы $\mathscr{G}$ по подгруппе $\mathscr{H}$.*

Доказательство. Пусть A — правый смежный класс группы $\mathscr{G}$ по подгруппе $\mathscr{H}$, содержащий g. Докажем, что $A = Hg$. Пусть hg — любой элемент из Hg. Тогда $hgg^{-1} \in H$ и $hg \equiv g \pmod{H}$. Поэтому $Hg \subset A$. Обратно: если $c \in A$, т. е. $c \equiv g \pmod{H}$, то $cg^{-1} = h \in H$ и $c = hg \in Hg$. Поэтому $A \subset Hg$. Следовательно, $A = Hg$. □

СВОЙСТВО 2.3. *Пусть A — правый смежный класс группы $\mathscr{G}$ по подгруппе $\mathscr{H}$ и $g \in A$, тогда $A = Hg$.*

Доказательство. Смежные классы A и Hg имеют общий элемент g. По свойству 2.1, они совпадают, т. е. $A = Hg$. □

СВОЙСТВО 2.4. *Пусть $\mathscr{H}$ — конечная подгруппа группы $\mathscr{G}$, $g \in \mathscr{G}$. Тогда число элементов смежного класса Hg равно числу элементов множества H.*

Доказательство. Пусть m — число элементов множества H: $H = \{h_1, \ldots, h_m\}$. Тогда $Hg = \{h_1 g, \ldots, h_m g\}$ и $h_i g \neq h_k g$ при $i \neq k$, так как из $h_i g = h_k g$, по закону сокращения, следовало бы равенство $h_i = h_k$. Следовательно, число элементов множества Hg равно m.

Пусть $\mathscr{H}$ — подгруппа группы $\mathscr{G}$. На множестве G введем бинарное отношение $\sim$ следующим образом:

$a \sim b \pmod{H}$ тогда и только тогда, когда $b^{-1}a \in H$; назовем его *отношением левого сравнения по подгруппе* $\mathscr{H}$. Непосредственная проверка показывает, что это отношение есть эквивалентность на множестве G. Классы эквивалентности этого отношения называются *левыми смежными классами группы* $\mathscr{G}$ по подгруппе $\mathscr{H}$. Нетрудно проверить, что левые смежные классы обладают свойствами, аналогичными свойствам 2.1 — 2.4.

Теорема Лагранжа. Пусть $\mathscr{G}$ — конечная группа. Число элементов ее основного множества G называется *порядком группы* $\mathscr{G}$.

ТЕОРЕМА 2.5 (ЛАГРАНЖА). *Порядок подгруппы конечной группы является делителем порядка группы.*

Доказательство. Пусть $\mathscr{H}$ — подгруппа конечной группы $\mathscr{G}$ и

$$H,\ Hg_2,\ \ldots,\ Hg_k$$

— множество всех различных правых смежных классов группы $\mathscr{G}$ по подгруппе $\mathscr{H}$. Тогда

$$(1)\quad G = H \cup Hg_2 \cup \ldots \cup Hg_k,$$

причем любые два смежных класса, входящих в это объединение, не пересекаются. Поэтому если n — число элементов множества G и m — число элементов множества H, то, по свойству 2.4, число элементов любого смежного класса Hg_i равно m и в силу (1) $n = mk$. □

СЛЕДСТВИЕ 2.6. *Если $\mathscr{G}$ — конечная группа порядка n и $g \in G$, то порядок элемента g делит n.*

СЛЕДСТВИЕ 2.7. *Любая конечная группа простого порядка является циклической.*

Упражнения

1. Пусть $\mathscr{S}_n = \langle S_n, \cdot, {}^{-1} \rangle$ — симметрическая группа подстановок n-й степени и A_n — множество всех четных подстановок из S_n. Покажите, что $\mathscr{A}_n = \langle A_n, \cdot, {}^{-1} \rangle$ есть подгруппа группы $\mathscr{S}_n$.

2. Покажите, что для произвольной подгруппы мультипликативной группы элементы, обратные к элементам левого смежного класса, образуют правый смежный класс.

3. Докажите, что при $n>1$ $n-1$ транспозиций (12), (13), ..., $(1n)$ порождают симметрическую группу $\mathcal{S}_n$.

4. Покажите, что при $n>2$ $n-2$ трехчленных циклов (123), ..., $(12n)$ порождают группу $\mathcal{A}_n$ четных подстановок.

5. Пусть $\mathcal{G}=\langle G, \cdot, ^{-1}\rangle$ — мультипликативная группа обратимых $n\times n$-матриц над полем $\mathcal{F}$. Пусть H — множество всех матриц из G, определитель которых равен единице поля $\mathcal{F}$. Покажите, что $\langle H, \cdot, ^{-1}\rangle$ есть подгруппа группы $\mathcal{G}$.

6. Пусть $\mathbf{R}^*$ — множество всех действительных чисел, отличных от нуля, и $\mathcal{R}^*=\langle \mathbf{R}^*, \cdot, ^{-1}\rangle$ — мультипликативная группа действительных чисел. Покажите, что для каждого натурального $n\geqslant 1$ мультипликативная группа корней n-й степени из единицы является единственной подгруппой n-го порядка группы $\mathcal{R}^*$.

§ 3. ЦИКЛИЧЕСКИЕ ГРУППЫ

Порядок элемента группы. Пусть $\mathcal{G}=\langle G, \cdot, ^{-1}\rangle$ — мультипликативная группа, e — ее единичный элемент и $a\in G$.

ОПРЕДЕЛЕНИЕ. *Порядком элемента a группы* называется наименьшее отличное от нуля натуральное число m такое, что $a^m=e$. Если же $a^n\neq e$ для любого ненулевого натурального числа n, то a называется элементом бесконечного порядка.

Порядок элемента a группы обозначается через $\mathcal{O}(a)$.

Пример. В мультипликативной группе комплексных чисел $\mathcal{O}(i)=4$, $\mathcal{O}(-1)=2$, $\mathcal{O}(1)=1$, $\mathcal{O}(2)=\infty$.

Ниже будет использована следующая теорема (см. теорему 4.4.4 о делении с остатком).

Для целых чисел n и $m>0$ существуют такие целые числа q и r, что

(1) $n=m\cdot q+r$, $0\leqslant r<m$.

ТЕОРЕМА 3.1. *Пусть m — порядок (конечный) элемента a мультипликативной группы. Равенство $a^n=e$, где n — целое число, выполняется тогда и только тогда, когда m делит n.*

Доказательство. Предположим, что $a^n=e$, и докажем, что m делит n. По теореме о делении с остатком, для чисел n и m существуют целые числа q и r, удовлетворяющие условиям (1). Надо показать, что $r=0$. По условию, $a^m=e$ и, по предположению, $a^n=e$. В силу (1) отсюда следует, что

$$a^n=a^{mq}\cdot a^r=(a^m)^q\cdot a^r=a^r=e.$$

Так как $\mathcal{O}(a)=m$ и $0\leqslant r<m$, то из $a^r=e$, следует $r=0$, т. е. m делит n.

Предположим теперь, что m делит n, и докажем, что $a^n=e$. Так как m делит n, то $n=mk$ для некоторого целого k. Следовательно, $a^n=a^{mk}=(a^m)^k=e^k=e$, т. е. $a^n=e$. □

ПРЕДПОЛОЖЕНИЕ 3.2. *Пусть a — элемент мультипликативной группы, имеющий конечный порядок m. Равенство $a^r=a^s$, где r и s — целые числа, выполняется тогда и только тогда, когда m делит $r-s$.*

Доказательство. Равенство $a^r=a^s$ имеет место тогда и только тогда, когда $a^{r-s}=e$. По теореме 3.1, $a^{r-s}=e$ в том и только в том случае, когда m делит $r-s$. Следовательно, $a^r=a^s$ тогда и только тогда, когда m делит $r-s$.

СЛЕДСТВИЕ 3.3. *Пусть a — элемент мультипликативной группы, имеющий конечный порядок m. Пусть r и s — целые числа; $\bar{r}=r+m\mathbf{Z}$ и $\bar{s}=s+m\mathbf{Z}$ — классы вычетов по модулю m. Равенство $a^r=a^s$ выполняется тогда и только тогда, когда $\bar{r}=\bar{s}$.*

СЛЕДСТВИЕ 3.4. *Пусть a — элемент мультипликативной группы, имеющий конечный порядок m. Тогда элементы $e(=a^0)$, a, a^2, ..., a^{m-1} различны.*

ПРЕДЛОЖЕНИЕ 3.5. *Пусть a — элемент бесконечного порядка мультипликативной группы и r, s — целые числа. Равенство $a^r=a^s$ имеет место тогда и только тогда, когда $r=s$.*

Доказательство. Из равенства $r=s$, очевидно, следует равенство $a^r=a^s$. Предположим, что $a^r=a^s$. Если $r\neq s$, например $r>s$, то $a^{r-s}=e$ и $r-s\neq 0$. Это невозможно, так как, по условию, элемент a имеет бесконечный порядок. Следовательно, $r=s$. □

Циклические группы. Ниже дано описание циклических групп.

ОПРЕДЕЛЕНИЕ. Мультипликативная (аддитивная) группа называется *циклической*, если основное множество группы состоит из степеней (кратных) какого-либо одного элемента группы; этот элемент называется *образующим элементом группы*.

Примеры. 1. Пусть $\mathbb{Z}=\langle \mathbf{Z}, +, -\rangle$ — аддитивная группа целых чисел. Каждый элемент группы является кратным 1 (или (—1)). Следовательно, $\mathbb{Z}$ есть циклическая группа с образующим элементом 1 (или (—1)).

2. Группа самосовмещений правильного m-угольника является циклической группой порядка m. Поворот m-

угольника вокруг центра на угол $2\pi/m$ есть образующий элемент этой группы.

3. Пусть m — целое положительное число, $\bar{k} = k + mZ$ и $\mathbf{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ — множество всех классов вычетов по модулю m. Операция сложения $+$ и унарная операция $-$ определяются так:

$$\bar{k} + \bar{s} = \overline{k+s}, \quad -(\bar{k}) = \overline{(-k)} = \overline{(m-k)}.$$

Операция сложения ассоциативна и коммутативна, $\bar{0}$ есть нейтральный элемент относительно сложения классов и $\bar{k} + (-\bar{k}) = \bar{0}$. Следовательно, алгебра $\mathbb{Z}_m = \langle \mathbf{Z}_m, +, - \rangle$ есть коммутативная группа порядка m. Она является циклической группой с образующим элементом $\bar{1}$. Группа $\mathbb{Z}_m$ называется *аддитивной группой классов вычетов по модулю* m.

ТЕОРЕМА 3.6. *Если образующий элемент циклической группы имеет бесконечный порядок, то группа изоморфна аддитивной группе целых чисел. Если же образующий элемент циклической группы имеет конечный порядок* m, *то группа изоморфна аддитивной группе классов вычетов по модулю* m.

Доказательство. Пусть $\mathcal{G} = \langle G, \cdot, {}^{-1} \rangle$ — мультипликативная циклическая группа с образующим элементом a, т. е. $G = \{a^n \mid n \in \mathbf{Z}\}$. Пусть $\mathbb{Z} = \langle \mathbf{Z}, +, - \rangle$ — аддитивная группа целых чисел и $\mathbb{Z} = \langle \mathbf{Z}_m, +, - \rangle$ — аддитивная группа классов вычетов по модулю m.

Первый случай: $\mathcal{O}(a) = \infty$. В этом случае в силу предложения 3.5 все целочисленные степени образующего элемента a различны. Поэтому отображение f множества G на $\mathbf{Z}$ такое, что $f(a^n) = n$ для всякого целого n, является инъективным. Отображение f сохраняет главные операции группы $\mathcal{G}$, так как для любых целых n и s:

$$f(a^n a^s) = f(a^{n+s}) = n + s = f(a^n) + f(a^s),$$
$$f(a^{-n}) = -n = -f(a^n).$$

Следовательно, f является изоморфным отображением группы $\mathcal{G}$ на группу $\mathbb{Z}$.

Второй случай: $\mathcal{O}(a) = m$, элемент a имеет конечный порядок m. Покажем, что в этом случае группа $\mathcal{G}$ изоморфна группе $\mathbb{Z}_m$. Докажем, что $G = \{e, a, a^2, \ldots, a^{m-1}\}$. Пусть a^k — любой элемент из G. По теореме о делении

с остатком, для чисел k и m существуют такие целые числа q и r, что

$$k = mq + r, \quad 0 \leqslant r < m.$$

Отсюда получаем

$$a^k = a^{mq} a^r = a^r \in \{e, a, \ldots, a^{m-1}\};$$

следовательно, $G = \{e, a, \ldots, a^{m-1}\}$.
Рассмотрим отображение φ множества G на множество $\mathbf{Z}_m$:

$\mathbf{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ такое, что

$$\varphi(a^k) = \bar{k} \text{ для } k = 0, 1, \ldots, m-1.$$

В силу предложения 3.2 φ является инъективным отображением множества G на $\mathbf{Z}_m$. Кроме того, φ сохраняет главные операции группы $\mathscr{G}$, так как

$$\varphi(a^k a^s) = \varphi(a^{k+s}) = \overline{k+s} = \bar{k} + \bar{s} = \varphi(a^k) + \varphi(a^s),$$
$$\varphi(a^{-k}) = \overline{m-k} = -(\bar{k}).$$

Следовательно, φ является изоморфным отображением группы $\mathscr{G}$ на группу $\mathbb{Z}_m$. □

Подгруппы циклической группы. Покажем, что всякая подгруппа циклической группы тоже циклическая.

ТЕОРЕМА 3.7. *Любая подгруппа циклической группы есть циклическая группа.*

Доказательство. Пусть $\mathscr{G}$ — мультипликативная циклическая группа с образующим элементом a. Пусть $\mathscr{H}$ — подгруппа группы $\mathscr{G}$. Теорема, очевидно, верна, если H содержит только один элемент. Предположим, что H содержит более одного элемента, Подгруппа $\mathscr{H}$ содержит хотя бы одну положительную степень элемента a, ибо если $a^{-k} \in H$, то $(a^{-k})^{-1} = a^k \in H$. Пусть a^s — элемент из H с наименьшим положительным показателем степени s. Всякий элемент из H есть элемент вида a^k. Если $a^k \in H$, то s делит k. В самом деле, по теореме о делении с остатком (теорема 4.4.4), для чисел k и s существуют такие целые числа q и r, что

(1) $k = sq + r$ и $0 \leqslant r < s$.

Ввиду (1) $a^r = a^{k-sq} = a^k (a^s)^{-q} \in H$. Так как $a^r \in H$ и $0 \leqslant r < s$, то в силу выбора числа s $r = 0$; значит, $k = sq$. Таким образом, множество H состоит из степеней элемента a^s. Следовательно, $\mathscr{H}$ является циклической группой с образующим элементом a^s. □

Упражнения

1. Найдите все подгруппы аддитивной группы $\mathbb{Z}$ всех целых чисел.

2. Найдите все подгруппы циклической группы порядка 12.

3. Найдите все подгруппы циклической группы порядка 24.

4. Докажите, что конечная группа простого порядка является циклической и любой ее элемент, отличный от нейтрального, является образующим.

5. Докажите, что существуют циклические группы произвольного порядка.

6. Докажите, что порядок любого элемента конечной группы есть делитель порядка группы.

7. Пусть m и n — взаимно простые натуральные числа. Покажите, что в мультипликативной абелевой группе произведение элемента a порядка m на элемент b порядка n есть элемент порядка mn.

8. Покажите, что любая группа порядка 15 — циклическая.

9. Пусть $\mathcal{G}$ — мультипликативная группа корней из 1 (корней n-й степени при всевозможных натуральных $n>0$). Покажите, что для всякого натурального числа m, отличного от нуля, группа $\mathcal{G}$ имеет только одну подгруппу порядка m и что каждая такая подгруппа циклическая.

§ 4. НОРМАЛЬНЫЕ ДЕЛИТЕЛИ И ФАКТОР-ГРУППЫ

Нормальные делители группы. Пусть $\mathcal{H}$ — подгруппа группы $\mathcal{G}$. Естественно возникает вопрос: при каких условиях разбиения множества G на правые и левые смежные классы по подгруппе $\mathcal{H}$ совпадают? Подгруппы, обладающие этим свойством, выделяются следующим определением.

Определение. Подгруппа $\mathcal{H}$ группы $\mathcal{G}$ называется *нормальным делителем группы* $\mathcal{G}$, если $g^{-1}hg \in H$ для любого элемента g из G и любого элемента h из H.

Запись $\mathcal{H} \lhd \mathcal{G}$ означает, что $\mathcal{H}$ есть нормальный делитель группы $\mathcal{G}$.

Примеры. 1. Пусть $\mathcal{S}_n$ — симметрическая группа подстановок n-й степени и $\mathcal{A}_n$ — ее подгруппа всех четных подстановок. Тогда $\mathcal{A}_n \lhd \mathcal{S}_n$.

2. Любая подгруппа абелевой группы является ее нормальным делителем.

3. Пусть $\mathcal{G}$ — мультипликативная группа обратимых $n \times n$-матриц над полем $\mathcal{F}$ и $\mathcal{H}$ — подгруппа матриц, определители которых равны единице. Тогда $\mathcal{H} \lhd \mathcal{G}$.

Рассмотрим некоторые свойства нормальных делителей группы.

СВОЙСТВО 4.1. *Подгруппа $\mathcal{H}$ группы $\mathcal{G}$ есть нормальный делитель группы $\mathcal{G}$ тогда и только тогда, когда*

каждый правый смежный класс группы $\mathcal{G}$ по подгруппе $\mathcal{H}$ является также левым смежным классом.

Доказательство. Предположим, что

(1) $\mathcal{H} \lhd \mathcal{G}$,

и докажем, что

(2) $Hg = gH$ для любого g из G.

В силу (1) $g^{-1}hg \in H$ для любого h из H. Поэтому $hg \in gH$ и $Hg \subset gH$. Далее, в силу (1) $(g^{-1})^{-1}hg^{-1} \in H$. Следовательно, $gH \in Hg$ для любого h из H, т. е. имеет место включение $gH \subset Hg$. Таким образом, из (1) следует (2).

Предположим теперь, что выполняется условие (2). Тогда для любого $h \in H$ найдется такое $h_1 \in H$, что $hg = gh_1$. Следовательно, $g^{-1}hg \in H$ для любого $g \in G$ и любого $h \in H$, т. е. $\mathcal{H} \lhd \mathcal{G}$. Таким образом, из (2) следует (1). □

СВОЙСТВО 4.2. *Пусть $\mathcal{A}$ — подгруппа группы $\mathcal{B}$, $\mathcal{B}$ — подгруппа группы $\mathcal{G}$ и $\mathcal{A} \lhd \mathcal{G}$; тогда $\mathcal{A} \lhd \mathcal{B}$.*

Доказательство. Пусть a и b — произвольные элементы из $|\mathcal{A}|$ и $|\mathcal{B}|$ соответственно. Тогда $b^{-1}ab \in |\mathcal{A}|$, так как, по условию, $\mathcal{A} \lhd \mathcal{G}$. Следовательно, $\mathcal{A} \lhd \mathcal{B}$. □

СВОЙСТВО 4.3. *Пересечение любой совокупности нормальных делителей группы $\mathcal{G}$ является нормальным делителем группы $\mathcal{G}$.*

Доказательство. Пусть $\mathcal{A} \lhd \mathcal{G}$ и $\mathcal{B} \lhd \mathcal{G}$. Тогда $\mathcal{A} \cap \mathcal{B}$ есть подгруппа группы $\mathcal{G}$. Если $c \in |\mathcal{A}| \cap |\mathcal{B}|$ и $g \in G$, то

$$g^{-1}cg \in |\mathcal{A}|, \quad g^{-1}cg \in |\mathcal{B}|,$$

так как $\mathcal{A}$ и $\mathcal{B}$, по условию, — нормальные делители группы $\mathcal{G}$. Следовательно, $g^{-1}cg \in |\mathcal{A}| \cap |\mathcal{B}|$ и $\mathcal{A} \cap \mathcal{B} \lhd \mathcal{G}$.

Аналогично доказывается, что свойство 4.3 имеет место для любой совокупности нормальных делителей группы $\mathcal{G}$. □

Фактор-группа. Пусть $\mathcal{G} = \langle G, \cdot, {}^{-1} \rangle$ — мультипликативная группа и A, $B \subset G$. Определим произведение $A \cdot B$ множеств A и B формулой

$$A \cdot B = \{x \cdot y \mid x \in A, \ y \in B\}.$$

ПРЕДЛОЖЕНИЕ 4.1. *Пусть $\mathcal{H}$ — нормальный делитель группы $\mathcal{G}$ и G/H — множество всех смежных классов группы $\mathcal{G}$ по подгруппе $\mathcal{H}$. Произведение любых двух смеж-*

ных классов $\mathcal{G}$ по $\mathcal{H}$ есть смежный класс, причем $Ha\ Hb = Hab$.

Доказательство. Пусть ha и h_1b, где $h,\ h_1 \in H$, — любые элементы из Ha и Hb соответственно. Тогда $ah_1a^{-1} \in H$, поскольку $\mathcal{H} \lhd \mathcal{G}$. Поэтому

$$ha \cdot h_1b = h(ah_1a^{-1})ab \in Hab;$$

следовательно, $(Ha)(Hb) \subset Hab$.

Докажем обратное включение. Пусть $hab \in Hab$. Тогда $hab = (ha)b \in Ha \cdot Hb$. Поэтому $Hab \subset (Ha) \cdot (Hb)$; следовательно, $(Ha) \cdot (Hb) = Hab$. □

На множестве G/H определим операции $\cdot$ и $^{-1}$ формулами

$$(Ha) \cdot (Hb) = Hab,\ (Ha)^{-1} = Ha^{-1}$$

и рассмотрим алгебру

$$\mathcal{G}/\mathcal{H} = \langle G/H,\ \cdot,\ ^{-1} \rangle.$$

ТЕОРЕМА 4.2. *Пусть $\mathcal{H}$ — нормальный делитель группы $\mathcal{G} = \langle G,\ \cdot,\ ^{-1} \rangle$. Алгебра $\mathcal{G}/\mathcal{H} = \langle G/H,\ \cdot,\ ^{-1} \rangle$ является группой.*

Доказательство. Пусть $Ha,\ Hb \in G/H$. Операции в G/H определяются равенствами

(1) $(Ha) \cdot (Hb) = Hab,\ (Ha)^{-1} = Ha^{-1}$.

Операция умножения смежных классов ассоциативна. В самом деле, если $A = Ha,\ B = Hb,\ C = Hc$, то в силу (1)

$$A \cdot (B \cdot C) = (Ha) \cdot (Hbc) = Habc,$$
$$(A \cdot B) \cdot C = (Hab) \cdot (Hc) = Habc.$$

Следовательно, $A(BC) = (AB)C$ для любых $A,\ B,\ C$ из G/H.

Элемент H из G/H является единичным относительно умножения, так как $A \cdot H = Ha \cdot He = Ha = A$, т. е. $A \cdot H = A$ для любого A из G/H. В силу (1) $A \cdot A^{-1} = Ha \cdot Ha^{-1} = Haa^{-1} = H$ для любого элемента A из G/H. Следовательно, алгебра $\mathcal{G}/\mathcal{H}$ является группой. □

ОПРЕДЕЛЕНИЕ. Алгебра $\mathcal{G}/\mathcal{H}$ называется *факторгруппой* группы $\mathcal{G}$ по подгруппе $\mathcal{H}$.

Примеры. 1. Пусть $\mathbb{Z}$ — аддитивная группа целых чисел, m — фиксированное натуральное число и $\bar{k} = k + m\mathbb{Z}$.

Тогда

$$\mathbf{Z}/m\mathbf{Z} = \{\bar{0},\ \bar{1},\ \ldots,\ \overline{m-1}\},$$

$$\bar{k}+\bar{n} = \overline{k+n},\ -(\bar{k}) = \overline{(-k)} = \overline{m-k}.$$

Алгебра $\mathbb{Z}/m\mathbb{Z} = \langle \mathbf{Z}/m\mathbf{Z},\ +,\ - \rangle$ является фактор-группой группы $\mathbb{Z}$ по подгруппе $m\mathbb{Z}$.

2. Пусть $\mathcal{S}_n$ — симметрическая группа подстановок степени $n\,(n > 1)$ и $\mathcal{A}_n$ — ее подгруппа четных подстановок. Тогда фактор-группа $\mathcal{S}_n/\mathcal{A}_n$ есть циклическая группа второго порядка, так как $S_n/A_n = \{A_n,\ A_n\sigma\}$, где σ — какая-нибудь нечетная подстановка.

Ядро гомоморфизма. Пусть $\mathcal{G} = \langle G,\ \cdot,\ ^{-1} \rangle$ и $\mathcal{G}' = \langle G',\ \circ,\ ^{-1} \rangle$ — мультипликативные группы.

ОПРЕДЕЛЕНИЕ. Пусть φ — гомоморфизм группы $\mathcal{G}$ в группу $\mathcal{G}'$. *Ядром гомоморфизма* φ называется множество

$$\operatorname{Ker}\varphi = \{x \in G \mid \varphi(x) = e'\},$$

где e' — единица группы $\mathcal{G}'$.

Множество $\operatorname{Ker}\varphi$ не пусто, так как $\varphi(e) = e'$. Множество $\operatorname{Ker}\varphi$ замкнуто в группе $\mathcal{G}$, так как для любых a, b из $\operatorname{Ker}\varphi$

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

т. е. элементы $a \cdot b$ и a^{-1} принадлежат множеству $\operatorname{Ker}\varphi$.

ОПРЕДЕЛЕНИЕ. Подгруппу группы $\mathcal{G}$ с основным множеством $\operatorname{Ker}\varphi$, где φ — гомоморфизм группы $\mathcal{G}$, обозначим $\mathcal{K}er\,\varphi$:

$$\mathcal{K}er\,\varphi = \langle \operatorname{Ker}\varphi,\ \cdot,\ ^{-1} \rangle$$

и назовем *ядерной группой гомоморфизма* φ или *ядром (гомоморфизма)* φ.

ПРЕДЛОЖЕНИЕ 4.3. *Если φ — гомоморфизм группы $\mathcal{G}$ в группу $\mathcal{G}'$, то $\mathcal{K}er\,\varphi$ является нормальным делителем группы $\mathcal{G}$.*

Доказательство. Выше было показано, что множество $\operatorname{Ker}\varphi$ замкнуто относительно главных операций группы $\mathcal{G}$. Кроме того, для любого g из G и любого h из $\operatorname{Ker}\varphi$

$$\varphi(g^{-1}hg) = \varphi(g^{-1}) \circ e' \circ \varphi(g) = \varphi(g^{-1}eg) = \varphi(e) = e',$$

т. е. $g^{-1}hg \in \operatorname{Ker}\varphi$. Следовательно, $\mathcal{K}er\,\varphi$ является нормальным делителем группы $\mathcal{G}$.

ПРЕДЛОЖЕНИЕ 4.4. *Пусть* φ — *гомоморфизм группы* $\mathcal{G}$ *в группу* $\mathcal{G}'$ *с ядром* $\mathcal{H} = \langle H, \cdot, {}^{-1}\rangle$. *Для любых* a, b *из* G, *если* $\varphi(a) = \varphi(b)$, *то* $Ha = Hb$.

Доказательство. Так как φ — гомоморфизм и $\varphi(a) = \varphi(b)$, то

$$\varphi(ab^{-1}) = \varphi(a) \circ \varphi(b^{-1}) = \varphi(a) \circ (\varphi(b))^{-1} = \varphi(a) \circ (\varphi(a))^{-1} = e'.$$

Следовательно, $a \cdot b^{-1} \in H$ и $Ha = Hb$. □

Теорема о гомоморфизмах. Одной из основных в теории групп является следующая теорема о гомоморфизмах.

ТЕОРЕМА 4.5. *Пусть* f — *гомоморфизм группы* $\mathcal{G}$ на *группу* $\mathcal{G}'$ *с ядром* $\mathcal{H}$. *Тогда фактор-группа* $\mathcal{G}/\mathcal{H}$ *изоморфна группе* $\mathcal{G}'$.

Доказательство. Пусть $\mathcal{H} = \mathcal{K}\mathrm{er}\, f$ и $H = \mathrm{Ker}\, f$. Пусть $\bar{G} = G/H$ — множество всех смежных классов группы $\mathcal{G}$ по подгруппе $\mathcal{H}$. Рассмотрим отображение

$$\varphi : G/H \to G',$$

определяемое следующим образом:

(1) $\varphi(Ha) = f(a)$ для любого смежного класса Ha из $\bar{G}$.

Так как $\mathrm{Ker}\, f = H$, то значение $\varphi(Ha)$ не зависит от выбора представителя a в смежном классе Ha. Отображение φ сохраняет операцию умножения в группе $\mathcal{G}/\mathcal{H}$, так как

$$\varphi(Ha \cdot Hb) = \varphi(Hab) = f(ab) = f(a) \cdot f(b) = \varphi(Ha)\varphi(Hb).$$

Следовательно, по теореме 3.3.1, φ является гомоморфизмом группы $\mathcal{G}/\mathcal{H}$ в группу $\mathcal{G}'$.

По условию, f есть отображение G на G'. В силу (1) отсюда следует, что φ есть отображение G/H на G'. Отображение φ является инъективным. В самом деле, в силу (1) из равенства $\varphi(Ha) = \varphi(Hb)$ следует $f(a) = f(b)$; согласно предложению 4.4, отсюда следует $Ha = Hb$. Итак, установлено, что φ есть инъективное отображение G/H на G'. Следовательно, φ является гомоморфизмом фактор-группы $\mathcal{G}/\mathcal{H}$ на группу $\mathcal{G}'$. □

Упражнения

1. Докажите, что любая фактор-группа аддитивной группы $\mathbb{Z}$ целых чисел является циклической.
2. Найдите все фактор-группы циклической группы порядка 12.
3. Докажите, что любая фактор-группа циклической группы является циклической.

4. Докажите, что фактор-группа симметрической группы $\mathfrak{S}_n$ подстановок n-й степени по подгруппе $\mathfrak{A}_n$ всех четных подстановок есть циклическая группа второго порядка.

5. Докажите, что аддитивная группа $\mathbb{Z}$ целых чисел изоморфна аддитивной группе $2\mathbb{Z}$ четных чисел.

6. Докажите, что аддитивная группа всех комплексных чисел изоморфна аддитивной группе всех векторов плоскости.

7. Пусть $\mathfrak{G}$ — группа подстановок. Рассмотрим отображение h группы $\mathfrak{G}$ в мультипликативную группу чисел $+1$ и -1, ставящее в соответствие каждой подстановке τ из $\mathfrak{G}$ ее знак $\operatorname{sgn}\tau$. Покажите, что h есть гомоморфизм.

8. Покажите, что мультипликативная группа корней m-й степени из 1 изоморфна аддитивной группе $\mathbb{Z}_m$ классов вычетов по модулю m.

9. Пусть $\mathfrak{G}$ — мультипликативная группа обратимых действительных $n \times n$-матриц и $\mathfrak{R}^*$ — мультипликативная группа действительных чисел, отличных от нуля. Пусть h — отображение $\mathfrak{G}$ в $\mathfrak{R}^*$, ставящее в соответствие каждому элементу g группы $\mathfrak{G}$ определитель $|g|$. Докажите, что h есть гомоморфизм, ядром которого является подгруппа группы $\mathfrak{G}$ всех $n \times n$-матриц с определителями, равными 1.

10. Пусть $\mathfrak{R}$ — аддитивная группа действительных чисел и $\mathfrak{K}$ — мультипликативная группа комплексных чисел, модуль которых равен 1. Докажите, что отображение f множества $\mathbf{R}$ в K, определяемое формулой $f(x) = \cos 2\pi x + i \sin 2\pi x$, есть гомоморфизм группы $\mathfrak{R}$ на группу $\mathfrak{K}$ с ядром $\mathbf{Z}$.

11. Пусть $\mathfrak{Q}$ — аддитивная группа рациональных чисел и $\mathbb{Z}$ — аддитивная группа целых чисел. Покажите, что каждый элемент фактор-группы $\mathfrak{Q}/\mathbb{Z}$ имеет конечный порядок. Докажите, что для всякого натурального n, отличного от нуля, $\mathfrak{Q}/\mathbb{Z}$ имеет только одну подгруппу порядка n и что каждая такая подгруппа циклическая.

Глава одиннадцатая

ТЕОРИЯ ДЕЛИМОСТИ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ

§ 1. РАЗЛОЖЕНИЕ ЦЕЛЫХ ЧИСЕЛ НА ПРОСТЫЕ МНОЖИТЕЛИ

Идеалы кольца целых чисел. Введем понятие идеала.

ОПРЕДЕЛЕНИЕ. Непустое множество I целых чисел называется *идеалом кольца* $\mathbb{Z}$ целых чисел, если оно замкнуто относительно сложения и умножения на любые целые числа, т. е. $a+b$, $ma \in \mathbf{Z}$ для любых a, $b \in I$ и любого $m \in \mathbf{Z}$.

Из определения следует, что любой идеал I замкнут относительно вычитания и, следовательно, содержит число нуль.

Пусть n — любое фиксированное целое число. Легко проверить, что множество $n\mathbf{Z}$, $n\mathbf{Z} = \{nx \mid x \in \mathbf{Z}\}$, является идеалом кольца $\mathbb{Z}$. Такой идеал называется *главным идеалом*, порожденным числом n. Идеал $0 \cdot \mathbf{Z}$ состоит только из нуля и называется *нулевым идеалом*. Легко видеть, что $n\mathbf{Z} = (-n)\mathbf{Z}$. Идеал, порожденный числом n, обозначают также через (n).

ТЕОРЕМА 1.1. *Каждый идеал кольца целых чисел является главным. Если I — ненулевой идеал кольца $\mathbb{Z}$ и d — наименьшее положительное число, содержащееся в I, то множество I состоит в точности из кратных числа d, т. е. $I = d\mathbf{Z}$.*

Доказательство. Нулевой идеал, очевидно, есть главный идеал, порожденный нулем. Пусть I — ненулевой идеал, т. е. он содержит хотя бы одно отличное от нуля число a. Тогда a, $-a \in I$ и одно из этих чисел положительно. Пусть d — наименьшее положительное число, содержащееся в I. Идеал I содержит все кратные числа d, т. е. $d\mathbf{Z} \subset I$. Надо еще показать, что каждое число c из I есть кратное числа d. Для этого разделим c на d с остатком:

$$c = dq + r, \quad 0 \leqslant r < d, \quad q, r \in \mathbf{Z}.$$

Так как c и dq принадлежат идеалу I, то $c-dq=r\in I$. Случай $r>0$ невозможен, так как d является наименьшим положительным числом, содержащимся в I. Следовательно, $r=0$ и $c=dq$. Таким образом, идеал I состоит в точности из кратных числа d, $I=d\mathbf{Z}$. □

Простые числа. Целое число p называется *простым*, если оно отлично от 0 и ± 1 и имеет делителями только ± 1 и $\pm p$. Целое число a, отличное от 0 и ± 1 и имеющее кроме ± 1 и $\pm a$ еще другие делители, называется *составным*.

Непосредственная проверка показывает, что первыми положительными простыми числами являются

2, 3, 5, 7, 11, 13, 17, 19, 23, 29;

первыми отрицательными простыми числами являются

$-2, -3, -5, -7, -11, -13, -17, -19, -23, -29.$

Разложение целых чисел на простые множители. Целые числа a и b называются *взаимно простыми*, если любой их общий делитель равен $+1$ или -1.

ПРЕДЛОЖЕНИЕ 1.2. *Если целые числа a и b взаимно простые, то существуют такие целые числа u, v, что $au+bv=1$.*

Доказательство. Рассмотрим множество

$$I=\{ax+by \mid x,\ y\in \mathbf{Z}\}.$$

Легко видеть, что это множество не пусто и замкнуто относительно сложения и умножения на целые числа. Следовательно, I есть идеал кольца $\mathbb{Z}$ целых чисел. Множество I содержит число a, $a=a\cdot 1+b\cdot 0$, и число b: $b=a\cdot 0+b\cdot 1$. Множество I содержит положительные числа, так как a и b взаимно простые и, значит, хотя бы одно из этих чисел отлично от нуля. Обозначим через d наименьшее положительное натуральное число, принадлежащее множеству I. Тогда согласно определению множества I существуют такие целые числа u, v, что $au+bv=d$. По теореме 4.4.5, d есть общий делитель чисел a и b. Так как a и b взаимно простые и $d>0$, то отсюда следует, что $d=1$. Таким образом, $au+bv=1$. □

ТЕОРЕМА 1.3. *Если произведение двух целых чисел делится на простое число p, то по меньшей мере один из сомножителей делится на p.*

Доказательство. Пусть произведение ab целых чисел делится на p и a не делится на p. Тогда числа a

и p взаимно простые. Согласно предложению 1.2, существуют такие целые числа u, v, что $au+pv=1$, откуда

$$abu+pbv=b.$$

Так как ab делится на p, то $abu+pbv$ делится на p, т. е. b делится на p. □

ТЕОРЕМА 1.4. *Если произведение нескольких целых чисел делится на простое число p, то по меньшей мере один из сомножителей делится на p.*

Доказательство проводится индукцией по числу сомножителей на основании теоремы 1.3. Предположим, что теорема верна для n сомножителей. Пусть $p \mid (a_1 \dots a_n \times \times a_{n+1})$; следовательно, $p \mid (a_1 \dots a_n) a_{n+1}$. Согласно теореме 1.3, по меньшей мере одно из двух чисел $a_1 \dots a_n$ и a_{n+1} делится на p. Если a_{n+1} не делится на p, то произведение $a_1 \dots a_n$ делится на p. Следовательно, по индуктивному предположению хотя бы одно из чисел $a_1 \dots a_n$ делится на p. □

ТЕОРЕМА 1.5. *Всякое целое положительное число, отличное от 1, представимо в виде произведения положительных простых чисел. Это представление единственно с точностью до порядка сомножителей.*

Доказательство. Пусть a — целое положительное число, отличное от 1. Докажем представимость a в виде произведения положительных простых множителей, предполагая, что это утверждение верно для всех целых положительных чисел, не равных единице и меньших a. Если a — простое число, то утверждение верно. Если a — составное, то его можно представить в виде произведения bc целых чисел b, c, меньших a и больших единицы. Согласно индуктивному предположению, b и c представимы в виде произведения положительных простых чисел:

$$b = p_1 \dots p_r, \quad c = p_{r+1} \dots p_m.$$

Подставив эти разложения в равенство $a=bc$, получим представление числа a

$$a = p_1 \dots p_r p_{r+1} \dots p_m$$

в виде произведения положительных простых чисел.

Докажем единственность представления, используя метод индукции. Если a — простое число, то, очевидно, единственность представления следует из определения простого числа. Предположим, что единственность представления для всех чисел, меньших a, имеет место. Предполо-

жим, что a составное, и рассмотрим два любых представления числа a в виде произведения положительных простых чисел:

(1) $a = p_1 \dots p_m = q_1 \dots q_n$.

Так как $p_1 \mid q_1 \dots q_n$, то согласно теореме 1.4 по меньшей мере один из сомножителей $q_1 \dots q_n$ делится на p_1; при соответствующей нумерации можно считать, что $p_1 \mid q_1$. Поскольку p_1 и q_1 — положительные простые числа, то $p_1 = q_1$. Сокращая обе части равенства (1) на p_1 и полагая $a/p_1 = a_1$, получим

$$a_1 = p_2 \dots p_m = q_2 \dots q_n.$$

Так как число a_1 меньше, чем a, то по индуктивному предположению число a_1 имеет единственное представление в виде произведения положительных простых чисел; следовательно, $m = n$ и при соответствующей нумерации $p_2 = q_2, \dots, p_m = q_m$. Таким образом, число a единственным образом представимо в виде произведения положительных простых чисел. □

СЛЕДСТВИЕ 1.6. *Всякое целое число c, отличное от нуля и ± 1, единственным образом представимо в виде произведения*

(1) $c = \varepsilon p_1 \dots p_m$,

где $p_1 \dots p_m$ — положительные простые числа и $\varepsilon = \pm 1$.

В представлении (1) могут встречаться равные простые числа. Если в представлении (1) объединить равные простые множители и изменить, если это необходимо, нумерацию, то представление (1) можно записать в виде

(2) $c = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$,

где $p_1, \dots, p_s$ — различные положительные простые числа, $\varepsilon = \pm 1$ и $\alpha_i > 0$ для $i = 1, 2, \dots, s$. Представление целого числа (отличного от нуля) в виде (2) называется его *каноническим разложением на простые множители*.

Делители целого числа. Зная каноническое разложение натурального числа, можно полностью описать делители этого числа.

ПРЕДЛОЖЕНИЕ 1.7. *Пусть n — натуральное число и*

(1) $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_s^{\alpha_s}$

— его каноническое разложение на простые множители. Тогда каждый натуральный делитель d числа n может быть записан в виде

(2) $d = p_1^{\delta_1} p_2^{\delta_2} \dots p_s^{\delta_s}$,

где δ_i — целые числа, удовлетворяющие условиям

(3) $\delta_i \in \{0, 1, \dots, \alpha_i\}$ для $i = 1, 2, \dots, s$.

Доказательство. Пусть d есть какой-либо натуральный делитель числа n. Так как каждый простой делитель числа d является делителем числа n, то ввиду (1) в разложении d на простые множители могут встречаться только числа множества $\{p_1, \dots, p_s\}$. Поэтому число d представимо в виде (2), причем показатели δ_i должны удовлетворять условиям (3).

С другой стороны, если d представимо в виде (2) и показатели δ_i удовлетворяют условиям (3), то

$$n = d\left(p_1^{\alpha_1 - \delta_1} \dots p_s^{\alpha_s - \delta_s}\right) \quad (\alpha_i - \delta_i \geqslant 0),$$

т. е. d является натуральным делителем числа n.

Число и сумма натуральных делителей числа. Предложение 1.7 позволяет подсчитать число и сумму натуральных делителей числа.

ПРЕДЛОЖЕНИЕ 1.8. *Пусть $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ — каноническое разложение на простые множители натурального числа n. Тогда число $\tau(n)$ натуральных делителей числа n выражается формулой $\tau(n) = (\alpha_1 + 1) \dots (\alpha_s + 1)$.*

Доказательство. Согласно предложению 1.7, любой натуральный делитель d числа n представим в виде

$$d = p_1^{\delta_1} \dots p_s^{\delta_s},$$

где

(3) $\delta_i \in \{0, 1, \dots, \alpha_i\}$ для $i = 1, 2, \dots, s$.

Поэтому, чтобы найти число всех натуральных делителей числа n, достаточно подсчитать число всевозможных упорядоченных наборов $\delta_1, \dots, \delta_s$, удовлетворяющих условиям (3). Ввиду (3) δ_i может принимать $\alpha_i + 1$ значений, выборы различных значений $\delta_1, \dots, \delta_s$ не зависят один от другого и в силу единственности разложения на простые множители разным наборам соответствуют различные делители n. Следовательно, число всех натуральных делителей числа n равно $(\alpha_1 + 1) \dots (\alpha_s + 1)$.

Примеры. 1. Пусть $n=180$. Тогда $180=2^2\cdot 3^2\cdot 5$ и $\tau(180)=(2+1)(2+1)(1+1)=18$.

2. Пусть $n=60$. Тогда $60=2^2\cdot 3\cdot 5$ и $\tau(60)=(2+1)(1+1)(1+1)=12$.

ПРЕДЛОЖЕНИЕ 1.9. *Пусть $n=p_1^{\alpha_1}\dots p_s^{\alpha_s}$ есть каноническое разложение натурального числа n на простые множители. Тогда сумма $\sigma(n)$ всех натуральных делителей числа n выражается формулой*

$$\sigma(n)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_s^{\alpha_s+1}-1}{p_s-1}. \tag{4}$$

Доказательство. Согласно предложению 1.7, каждый делитель числа n имеет вид $p_1^{\delta_1}\dots p_s^{\delta_s}$ и

$$\sigma(n)=\sum_{\substack{\delta_1\in\{0,\,1,\,\dots,\,\alpha_1\}\\ \dots\dots\dots\dots\\ \delta_s\in\{0,\,1,\,\dots,\,\alpha_s\}}} p_1^{\delta_1}\dots p_s^{\delta_s}. \tag{5}$$

Легко видеть, что каждое слагаемое в (5) в точности один раз встречается после раскрытия скобок произведения

$$\left(1+p_1+\dots+p_1^{\alpha_1}\right)\dots\left(1+p_s+\dots+p_s^{\alpha_s}\right). \tag{6}$$

Следовательно, сумма (5) равна произведению (6). Так как каждый сомножитель есть сумма членов геометрической прогрессии, то произведение (6) равно

$$\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_s^{\alpha_s+1}-1}{p_s-1}.$$

Таким образом, верна формула (4). □

Пример. Пусть $n=60$. Тогда $n=2^2\cdot 3\cdot 5$ и

$$\sigma(60)=\frac{2^3-1}{2-1}\cdot\frac{3^2-1}{3-1}\cdot\frac{5^2-1}{5-1}=7\cdot 4\cdot 6=168.$$

Бесконечность множества простых чисел. Следующая теорема была доказана Евклидом.

ТЕОРЕМА 1.10. *Множество положительных простых чисел бесконечно.*

Доказательство. Покажем, что для каждого данного конечного множества положительных простых чисел $p_1, \dots, p_n$ существует положительное простое число,

отличное от всех чисел этого множества. Для этого рассмотрим число

$$a = p_1 \cdot p_2 \dots p_n + 1.$$

Так как a есть натуральное число, большее единицы, то, по теореме 1.5, оно разложимо в произведение положительных простых чисел и поэтому обладает хотя бы одним положительным простым делителем p. Этот делитель отличен от $p_1 \cdot p_2, \dots, p_n$, так как в противном случае $p \mid p_1 \dots p_n$, $p \mid a$ и разность $a - p_1 \cdot p_2 \dots p_n = 1$ делилась бы на p, а это невозможно. Следовательно, множество всех простых чисел бесконечно. □

Решето Эратосфена. Рассмотрим метод нахождения положительных простых чисел, не превосходящих данного числа.

ПРЕДЛОЖЕНИЕ 1.11. *Положительное составное число a имеет по крайней мере один положительный простой делитель, не превосходящий $\sqrt{a}$.*

Доказательство. Среди отличных от единицы положительных делителей числа a существует наименьший; обозначим его через p. Если бы число p было составным, то оно имело бы положительный делитель q, удовлетворяющий условиям $1 < q < p$. В этом случае число q было бы положительным делителем числа a, меньшим p, что противоречит выбору числа p. Следовательно, p — простое число. Если $a = pb$, то $b \geqslant p$. Перемножая $a = pb$ и $b \geqslant p$ почленно и сокращая на b, получаем, $a \geqslant p^2$ и $p \leqslant \sqrt{a}$.

ПРЕДЛОЖЕНИЕ 1.12. *Если положительное число a, отличное от единицы, не делится ни на одно положительное простое число, не превосходящее $\sqrt{a}$, то оно простое.*

Это предложение непосредственно следует из предложения 1.11. Существует простой метод составления таблицы положительных простых чисел, не превосходящих данного целого числа. Этот метод носит название *решета Эратосфена*.

Предположим, что надо найти все положительные простые числа, не превосходящие данного натурального числа a. Для этого выпишем подряд последовательность всех натуральных чисел от 2 до a: 2, 3, 4, ..., a. В этой последовательности вычеркнем каждое второе число после 2. Первое незачеркнутое число — это простое число 3. Далее

вычеркнем каждое третье число после 3 (причем надо считать и те числа, которые уже вычеркнуты ранее). Первое следующее за 3 невычеркнутое число — это простое число 5. Вычеркнем каждое пятое число после 5, и т. п. Это вычеркивание продолжаем до тех пор, пока не дойдем до первого простого числа, не меньшего $\sqrt{a}$. В силу предложения 1.12 все числа, оставшиеся невычеркнутыми, будут положительными простыми, не превосходящими числа a.

Пример. Составим таблицу положительных простых чисел, не превосходящих 50. Для этого выпишем натуральные числа от 2 до 50 и произведем вычеркивание до встречи первого числа, большего или равного $\sqrt{50}$, т. е. до 11 (вычеркнутые числа — светлые):

2 **3** 4 **5** 6 **7** 8 **9** 10 **11** 12 **13** 14 15 16 **17** 18 **19** 20
21 22 **23** 24 25 26 27 28 **29** 30 **31** 32 33 34 35 36 **37** 38
39 40 **41** 42 **43** 44 45 46 **47** 48 49 50

Вычеркнем из этой последовательности каждое второе число после 2, далее — каждое третье число после трех, затем каждое пятое число после 5 и, наконец, каждое седьмое число после 7. Все числа, оставшиеся невычеркнутыми, будут простыми. Таким образом, получаем следующую таблицу положительных простых чисел, меньших 50:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

Упражнения

1. Покажите, что для любого целого n число $n(n+1)(n+2)$ делится на 6.

2. Покажите, что для любого целого n число $n(n+1)(2n+1)$ делится на 6.

3. Пусть m и n — взаимно простые целые числа. Покажите, что взаимно простыми являются следующие числа: m и $m+n$, m и $m-n$, $m+n$ и $2m+n$.

4. Пусть a, b, c, d — целые положительные числа и a/b, c/d — несократимые дроби. Покажите, что если $a/b=c/d$, то $a=c$ и $b=d$.

5. Покажите, что если 2^n+1 — простое число, то $n=2^m$.

6. Покажите, что если 2^n-1 — простое число, то n — простое.

7. Пусть a и n — целые положительные числа $a>1$. Докажите, что если a^n+1 — простое число, то $n=2^m$.

8. Разложите число 50! на простые множители.

9. Покажите, что при натуральном $n>1$ сумма $1+\frac{1}{2}+\ldots+\frac{1}{n}$ не может быть целым числом.

10. Натуральное число называется *совершенным*, если оно равно половине суммы своих положительных делителей. Докажите, что всякое четное совершенное число имеет вид $2^n(2^{n+1}-1)$, где $n \in \mathbb{N}$, причем $2^{n+1}-1$ — простое.

§ 2. НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ И НАИМЕНЬШЕЕ ОБЩЕЕ КРАТНОЕ

Наибольший общий делитель. Целое число c называется *общим делителем целых чисел* $a_1, \ldots, a_n$, если c есть делитель каждого из этих чисел.

ОПРЕДЕЛЕНИЕ. *Наибольшим общим делителем целых чисел* $a_1, \ldots, a_n$ называется такой их общий делитель, который делится на любой общий делитель этих чисел. Целые числа $a_1, \ldots, a_n$ называются *взаимно простыми*, если их наибольший общий делитель равен единице.

Наибольший общий делитель чисел $a_1, \ldots, a_n$ обозначается НОД$(a_1, \ldots, a_n)$, положительный наибольший общий делитель этих чисел обозначается нод$(a_1, \ldots, a_n)$.

СЛЕДСТВИЕ 2.1. *Если d есть наибольший общий делитель целых чисел $a_1, \ldots, a_n$, то множество всех общих делителей этих чисел совпадает с множеством всех делителей числа d.*

СЛЕДСТВИЕ 2.2. *Любые два наибольших общих делителя целых чисел $a_1, \ldots, a_n$ ассоциированы, т. е. могут отличаться только знаком. Если d есть наибольший общий делитель чисел $a_1, \ldots, a_n$, то число $(-d)$ также есть наибольший общий делитель этих чисел.*

ПРЕДЛОЖЕНИЕ 2.3. *Если* $a = \prod_{p \mid a} p^{\alpha_p}$ *и* $b = \prod_{p \mid b} p^{\beta_p}$ *суть канонические разложения целых положительных чисел a и b, то число d*

$$d = \prod_{\substack{p \mid a \\ p \mid b}} p^{\min(\alpha_p, \beta_p)}$$

является наибольшим общим делителем чисел a и b.

Доказательство. Число d является делителем как числа a, так и числа b в силу предложения 1.7, т. е. d есть общий делитель a и b. Далее, если c — любой положительный общий делитель a и b, то в силу предложения 1.7

$$c = \prod_{\substack{p \mid a \\ p \mid b}} p^{\gamma_p},$$

причем для каждого делителя a и b выполняются неравенства $\gamma_p \leqslant \alpha_p$, $\gamma_p \leqslant \beta_p$. Поэтому $c \mid d$. Следовательно, d есть наибольший общий делитель чисел a и b. □

Пусть $a_1, \ldots, a_n$ — любые целые числа. Рассмотрим множество

$$(1)\quad I = \{k_1a_1 + \ldots + k_na_n \mid k_1, \ldots, k_n \in \mathbf{Z}\}$$

всех целочисленных линейных комбинаций чисел $a_1, \ldots, a_n$. Легко проверить, что это множество есть идеал в кольце $\mathbb{Z}$. Этот идеал называется *идеалом, порожденным числами* $a_1, \ldots, a_n$, и обозначается через $(a_1, \ldots, a_n)$.

ТЕОРЕМА 2.4. *Для любой совокупности целых чисел* $a_1, \ldots, a_n$ *существует наибольший общий делитель. Число* d *является наибольшим общим делителем чисел* $a_1, \ldots, a_n$ *тогда и только тогда, когда идеал* $(a_1, \ldots, a_n)$ *равен идеалу* (d).

Доказательство. Если все числа $a_1, \ldots, a_n$ равны нулю, то единственным наибольшим общим делителем этих чисел является число нуль.

Предположим, что хотя бы одно из чисел $a_1, \ldots, a_n$ отлично от нуля. Рассмотрим множество I всех целочисленных линейных комбинаций чисел $a_1, \ldots, a_n$. Множество I содержит числа a_s, $s = 1, \ldots, n$, так как $a_s = k_1a_1 + \ldots + k_na_n$, где $k_s = 1$ и $k_i = 0$ для $i \neq s$. Поэтому множество I содержит числа, отличные от нуля. Множество I есть идеал кольца целых чисел, порожденный числами $a_1, \ldots, a_n$; $I = (a_1, \ldots, a_n)$. Согласно теореме 4.4, каждый идеал кольца $\mathbb{Z}$ является главным и, значит, состоит из кратных некоторого целого числа d, $I = dZ$. Докажем, что d есть НОД $(a_1, \ldots, a_n)$. Так как каждый элемент множества I делится на d, то $d \mid a_i$ для $i = 1, \ldots, n$, т. е. d есть общий делитель чисел $a_1, \ldots, a_n$. Далее, так как $d \in I$, то ввиду (1) существуют такие целые числа $k_1, \ldots, k_n$, что

$$d = k_1a_1 + \ldots + k_na_n.$$

Отсюда следует, что любой общий делитель c чисел $a_1, \ldots, a_n$ есть также делитель числа d. Таким образом, любой элемент d, порождающий идеал $I = (a_1, \ldots, a_n)$, является наибольшим общим делителем чисел $a_1, \ldots, a_n$. Из доказанного, в частности, следует, что любая конечная совокупность чисел $a_1, \ldots, a_n$ обладает наибольшим общим делителем.

Пусть d' — любой наибольший общий делитель чисел $a_1, \ldots, a_n$ и d — по-прежнему число, порождающее идеал I; докажем, что $(a_1, \ldots, a_n) = (d')$. Любые два НОД чисел $a_1, \ldots, a_n$ ассоциированы, т. е. могут отличаться только знаком. Ввиду этого $d' = \pm d$. Поэтому идеал (d') совпадает с идеалом (d). Следовательно, $(a_1, \ldots, a_n) = (d')$. □

Анализ доказательства предыдущей теоремы дает возможность формулировать также следующую теорему.

ТЕОРЕМА 2.5. *Наибольший общий делитель d целых чисел $a_1, \ldots, a_n$ представим в виде целочисленной линейной комбинации этих чисел, т. е. в форме $d = k_1a_1 + \ldots + k_na_n$ с целыми $k_1, \ldots, k_n$. При этом если не все числа $a_1, \ldots, a_n$ равны нулю, то $|d|$ есть наименьшее целое положительное число, представимое в этой форме. Все числа, представимые в этой форме, т. е. все числа идеала $(a_1, \ldots, a_n)$, являются кратными числу d.*

ПРЕДЛОЖЕНИЕ 2.6. *Если общий делитель d целых чисел $a_1, \ldots, a_n$ представим в виде целочисленной линейной комбинации этих чисел, то d есть наибольший общий делитель чисел $a_1, \ldots, a_n$.*

Доказательство. Предположим, что общий делитель d чисел $a_1, \ldots, a_n$ представим в виде

$$d = k_1a_1 + \cdots + k_na_n,$$

где $k_1, \ldots, k_n$ — целые числа. Тогда любой общий делитель чисел $a_1, \ldots, a_n$ делит сумму $k_1a_1 + \ldots + k_na_n$ и, значит, d. Таким образом, d есть наибольший общий делитель чисел $a_1, \ldots, a_n$. □

ПРЕДЛОЖЕНИЕ 2.7. *Для любых целых чисел a, b, c*

$$\text{НОД}(a, b, c) \sim \text{НОД}(\text{НОД}(a, b), c).$$

Доказательство. Пусть d_1 есть НОД(a, b) и d — НОД(d_1, c). Тогда d есть общий делитель чисел d_1 и c, а число d_1 есть общий делитель чисел a и b. Поэтому d есть общий делитель чисел a, b и c. Согласно теореме 2.5, числа d и d_1 можно представить в виде

$$d = kd_1 + k_3c, \quad d_1 = k_1a + k_2b,$$

где k, k_1, k_2, k_3 — целые числа; поэтому $d = kk_1a + kk_2b + k_3c$. Таким образом, общий делитель d чисел a, b, c можно линейно выразить через эти числа. Следовательно, согласно предложению 2.6, d является наибольшим делителем этих чисел. □

Это предложение дает возможность свести нахождение наибольшего общего делителя нескольких чисел к нахождению наибольшего общего делителя двух чисел.

ПРЕДЛОЖЕНИЕ 2.8. *Для любых целых чисел* a, b *и* c

$$\text{НОД}(ac,\ bc) \sim c \cdot \text{НОД}(a,\ b).$$

Доказательство. Пусть d есть НОД$(a,\ b)$. Тогда согласно теореме 2.5 d можно представить в виде

$$d = k_1 a + k_2 b,$$

где k_1 и k_2 — целые числа, поэтому $cd = k_1 ac + k_2 bc$. Кроме того, так как d есть общий делитель a и b, то cd есть общий делитель ac и bc. Следовательно, согласно предложению 2.6, число cd есть наибольший общий делитель чисел ac и bc. □

Взаимно простые числа. Рассмотрим свойства взаимно простых чисел.

ПРЕДЛОЖЕНИЕ 2.9. *Целые числа* $a_1, \ldots, a_n$ *взаимно простые тогда и только тогда, когда единица представима в виде целочисленной линейной комбинации этих чисел.*

Доказательство. Если числа $a_1, \ldots, a_n$ взаимно простые, то их наибольший общий делитель единица представим согласно теореме 2.5 в виде целочисленной линейной комбинации этих чисел.

Обратно: если единица представима в виде целочисленной линейной комбинации чисел $a_1, \ldots, a_n$, то в силу предложения 2.6 единица есть наибольший общий делитель этих чисел. Поэтому числа $a_1, \ldots, a_n$ взаимно простые. □

ПРЕДЛОЖЕНИЕ 2.10. *Целые числа* $a_1, \ldots, a_n$ *взаимно простые тогда и только тогда, когда они не имеют общего простого делителя.*

Доказательство предоставляется читателю.

ТЕОРЕМА 2.11. *Если целое число делит произведение двух целых чисел и взаимно простое с одним из сомножителей, то оно делит другой сомножитель.*

Доказательство. Пусть числа a и b взаимно простые и a делит bc. Докажем, что a делит c. Так как числа a и b взаимно простые, то существуют такие целые числа k_1 и k_2, что

$$k_1 a + k_2 b = 1.$$

Умножив обе части равенства на c, получим $k_1 ac + k_2 bc = c$. Кроме того, a делит bc. Поэтому a делит $k_1 ac + k_2 bc$, т. е. a делит c. □

ПРЕДЛОЖЕНИЕ 2.12. *Общий делитель d целых чисел $a_1, \ldots, a_n$, не равных одновременно нулю, тогда и только тогда является их наибольшим общим делителем, когда числа $a_1/d, \ldots, a_n/d$ взаимно простые.*

Доказательство. Так как, по условию, не все числа $a_1, \ldots, a_n$ равны нулю, то $d \neq 0$. Если d есть наибольший общий делитель чисел $a_1, \ldots, a_n$, то согласно теореме 2.5 его можно линейно выразить через $a_1, \ldots, a_n$:

$$(1) \quad k_1 a_1 + \ldots + k_n a_n = d,$$

где $k_1, \ldots, k_n$ — целые числа. Разделив обе части равенства на d, получим

$$(2) \quad k_1 \frac{a_1}{d} + \ldots + k_n \frac{a_n}{d} = 1.$$

Отсюда согласно предложению 2.9 следует, что числа $a_1/d, \ldots, a_n/d$ взаимно простые.

Обратно: если числа $a_1/d, \ldots, a_n/d$ взаимно простые, то согласно предложению 2.9 существуют такие целые числа $k_1, \ldots, k_n$, что выполняется равенство (2). Умножив обе части этого равенства на d, получим равенство (1). Так как общий делитель d чисел $a_1, \ldots, a_n$ представим в виде линейной комбинации этих чисел, то согласно предложению 2.6 число d есть наибольший делитель чисел $a_1, \ldots, a_n$. □

Наименьшее общее кратное. Целое число c называется *общим кратным целых чисел* $a_1, \ldots, a_n$, если оно делится на каждое из этих чисел.

ОПРЕДЕЛЕНИЕ. *Наименьшим общим кратным целых чисел* $a_1, \ldots, a_n$ называется такое их общее кратное, которое делит любое общее кратное этих чисел. Наименьшее общее кратное целых чисел $a_1, \ldots, a_n$ обозначается через НОК$(a_1, \ldots, a_n)$. Положительное наименьшее общее кратное чисел $a_1, \ldots, a_n$, отличных от нуля, обозначается через $[a_1, \ldots, a_n]$.

Из определения НОК$(a_1, \ldots, a_n)$ непосредственно вытекают следствия.

СЛЕДСТВИЕ 2.13. *Любые два наименьших общих кратных целых чисел $a_1, \ldots, a_n$ ассоциированы в $\mathfrak{Z}$, т. е. могут отличаться только знаком. Если число m есть* НОК$(a_1, \ldots, a_n)$, *то и число $(-m)$ есть* НОК$(a_1, \ldots, a_n)$.

СЛЕДСТВИЕ 2.14. *Если m — наименьшее общее кратное чисел $a_1, \ldots, a_n$, то множество всех общих кратных этих чисел совпадает с множеством всех кратных числа m.*

ПРЕДЛОЖЕНИЕ 2.15. *Пусть* $a = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ *и* $b = p_1^{\beta_1} \dots p_s^{\beta_s}$, *где* $p_1, \dots, p_s$ — *попарно различные положительные простые числа и* α_i, β_i — *целые неотрицательные числа. Тогда*

$$[a, b] = p^{\max(\alpha_1, \beta_1)} \dots p_s^{\max(\alpha_s, \beta_s)}.$$

Доказательство этого предложения предоставляется читателю.

ТЕОРЕМА 2.16. *Для любой совокупности целых чисел* $a_1, \dots, a_n$ *существует наименьшее общее кратное. Целое число* m *есть* НОК$(a_1, \dots, a_n)$ *тогда и только тогда, когда* $(a_1) \cap \dots \cap (a_n) = (m)$, *где* (a_i) — *идеал, порожденный числом* a_i.

Доказательство. Рассмотрим множество

$$(1) \quad I = (a_1) \cap \dots \cap (a_n).$$

Так как множества $(a_1), \dots, (a_n)$ замкнуты относительно сложения и умножения на целые числа, то легко проверить, что их пересечение I также замкнуто относительно сложения и умножения на целые числа. Кроме того, это множество не пусто, так как содержит нуль. Поэтому I есть идеал кольца целых чисел. Согласно теореме 4.4, любой идеал кольца целых чисел является главным, т. е. существует целое число m такое, что каждое число из I кратно m, $I = (m)$. Докажем, что m есть НОК$(a_1, \dots, a_n)$. Так как $m \in I$, то ввиду (1) $m \in (a_i)$ для $i = 1, \dots, m$, т. е. m есть общее кратное чисел $a_1, \dots, a_n$. Кроме того, если m' — любое общее кратное чисел $a_1, \dots, a_n$, то $m' \in (a_1), \dots, m' \in (a_n)$. Следовательно, $m' \in I = (a_1) \cap \dots \cap (a_m) = (m)$ и поэтому m' делится на m. Таким образом, m есть наименьшее общее кратное чисел $a_1, \dots, a_n$.

Предположим теперь, что m_1 есть наименьшее общее кратное чисел $a_1, \dots, a_n$ и докажем, что $(m_1) = (a_1) \cap \dots \cap (a_n)$. Так как числа m_1 и m суть наименьшие общие кратные одной и той же совокупности чисел $a_1, \dots, a_n$, то они ассоциированы в $\mathbb{Z}$, т. е. $m_1 = \pm m$. Следовательно, $(m_1) = (m)$ и поэтому $(a_1) \cap \dots \cap (a_n) = (m_1)$. □

ПРЕДЛОЖЕНИЕ 2.17. *Для любых отличных от нуля целых чисел* a, b *и* c *при* $c > 0$ *имеем*: $[ac, bc] = c[a, b]$.

Доказательство. Пусть $m = [a, b]$. Так как m есть общее кратное чисел a и b, то cm есть общее кратное

чисел ac и bc. Пусть m' — любое общее кратное чисел ac и bc, т. е.

$$m' = kac = sbc,$$

где k и s — целые числа. Так как $c \neq 0$, то $ka = sb$. Поэтому ka делится на m и, следовательно, m' делится на mc. Таким образом, cm есть наименьшее общее кратное чисел ac и bc. Кроме того, $cm > 0$; поэтому $[ac, bc] = cm = c[a, b]$. □

СЛЕДСТВИЕ 2.18. *Для любых отличных от нуля целых чисел a, b и c* $\text{НОК}(ac, bc) \sim c \cdot \text{НОК}(a, b)$.

ПРЕДЛОЖЕНИЕ 2.19. *Если целые числа a и b взаимно простые, то ab есть наименьшее общее кратное чисел a и b.*

Доказательство. Число ab есть общее кратное чисел a и b. Поэтому достаточно доказать, что любое общее кратное m чисел a и b делится на ab. Число m кратно b, т. е. $m = bc$, где c — целое число, и $a \mid bc$. Так как, по условию, a и b взаимно простые, то отсюда согласно теореме 2.11 следует, что a делит c, $c = ad$. Следовательно, $m = abd$, т. е. m делится на ab. Таким образом, ab есть наименьшее общее кратное чисел a и b. □

ПРЕДЛОЖЕНИЕ 2.20. *Если целые числа a и b отличны от нуля, то*

(1) $$\text{НОК}(a, b) \sim \frac{ab}{\text{НОД}(a, b)}.$$

Доказательство. Пусть d есть наибольший общий делитель чисел a и b. Так как числа a и b отличны от нуля, то $d \neq 0$. Согласно следствию 2.18,

(2) $$\text{НОК}(a, b) \sim d\,\text{НОК}(a/d, b/d).$$

Далее, в силу предложения 2.12 $\text{НОД}(a/d, b/d) = 1$. Отсюда согласно предложению 2.19

(3) $$\text{НОК}\left(\frac{a}{d}, \frac{b}{d}\right) \sim \frac{a}{d} \cdot \frac{b}{d}.$$

На основании (2) и (3) заключаем, что выполняется соотношение (1). □

ТЕОРЕМА 2.21. *Для любых целых чисел a, b и c*

(1) $$\text{НОК}(a, b, c) \sim \text{НОК}(\text{НОК}(a, b), c).$$

Доказательство. Пусть $m = \text{НОК}(a, b, c)$, $m_1 = \text{НОК}(a, b)$ и $m' = \text{НОК}(m_1, c)$. Согласно теореме 2.16,

(2) $$(m) = (a) \cap (b) \cap (c), \quad (m_1) = (a) \cap (b), \quad (m') = (m_1) \cap (c);$$

поэтому

(3) $(m') = ((a) \cap (b)) \cap (c) = (a) \cap (b) \cap (c)$.

Из (2) и (3) следует, что $(m) = (m')$. □

Упражнения

1. Пусть a и b — взаимно простые целые положительные числа. Покажите, что сумма $\frac{1}{a} + \frac{1}{a+b}$ после приведения к общему знаменателю есть несократимая дробь.

2. Докажите, что d есть наибольший общий делитель целых чисел a, b, c тогда и только тогда, когда a/d, b/d, c/d — целые взаимно простые числа.

3. Докажите, что для любых целых чисел a, b, c, k НОД $(ka, kb, kc) \sim k$ НОД (a, b, c).

4. Докажите, что общее кратное m целых чисел a, b, c есть наименьшее общее кратное тогда и только тогда, когда числа m/a, m/b, m/c взаимно простые ($a, b, c \neq 0$).

5. Пусть $a = m/n$, где m, n — целые взаимно простые числа, $m \neq 0$ и $n > 0$. Если $a = r/s$, где r, s — целые и $s > 0$, то существует натуральное число t такое, что $r = tm$ и $s = tn$. При этом t есть наибольший общий делитель чисел r и s.

§ 3. АЛГОРИТМ ЕВКЛИДА И КОНЕЧНЫЕ ЦЕПНЫЕ ДРОБИ

Алгоритм Евклида. Рассмотрим наиболее простой способ нахождения наибольшего общего делителя двух целых чисел.

ПРЕДЛОЖЕНИЕ 3.1. *Пусть a и b — два целых числа, $b \neq 0$ и*

(1) $a = bq + r \qquad (0 \leqslant r < |b|)$.

Тогда нод $(a, b) =$ нод (b, r).

Доказательство. Из (1) следует, что любой общий делитель чисел a и b есть делитель числа $r = a - bq$ и любой общий делитель чисел b и r есть делитель числа a. Поэтому множество всех общих делителей чисел a и b совпадает с множеством всех общих делителей чисел b и r. Отсюда следует, что положительный общий делитель чисел a и b совпадает с положительным общим делителем чисел b и r, т. е. нод $(a, b) =$ нод (b, r). □

Если $b \mid a$, где $b \geqslant 1$, то, очевидно, нод $(a, b) = b$. Для нахождения нод двух целых чисел применяют способ «*последовательного деления*», называемый *алгоритмом Евклида*. Сущность этого способа состоит в том, что в силу доказанного выше предложения задача нахождения нод чисел a

и b сводится к более простой задаче нахождения нод чисел b и r, где $0 \leqslant r < |b|$. Если $r = 0$, то нод$(a, b) = b$. Если же $r \neq 0$, то рассуждения повторяем, отправляясь от b и r. В результате получим цепочку равенств

$$
\begin{aligned}
&a = ba_0 + r_1, && 0 < r_1 < |b|,\\
&b = r_1a_1 + r_2 && 0 < r_2 < r_1,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&r_{n-2} = r_{n-1}a_{n-1} + r_n, && 0 < r_n < r_{n-1},\\
&r_{n-1} = r_n a_n + r_{n+1}.
\end{aligned}
\tag{2}
$$

Мы получили убывающую последовательность натуральных чисел

$$r_1 > r_2 > \ldots > r_n > \ldots \geqslant 0,$$

которая не может быть бесконечной. Поэтому существует остаток, равный нулю; пусть $r_{n+1} = 0$, $r_n \neq 0$.

На основании предложения 3.1 из равенств (2) следует, что

нод (a, b) = нод (b, r_1) = нод (r_1, r_2) = ... = нод (r_{n-1}, r_n) = = нод $(r_n, 0) = r_n$, т. е. r_n = нод (a, b). Итак, мы приходим к выводу: если к целым числам a, b, где $b \neq 0$, применить алгоритм Евклида, то последний ненулевой остаток в этом алгоритме есть нод (a, b).

Конечные цепные дроби. Любое рациональное число можно представить в виде a/b, где a и b — целые числа и $b \geqslant 1$. Применив к a и b алгоритм Евклида, получим цепочку равенств:

$$
\begin{aligned}
&a = ba_0 + r_1,\\
&b = r_1a_1 + r_2,\\
&r_1 = r_2a_2 + r_3,\\
&\ldots\ldots\ldots\ldots\\
&r_{n-3} = r_{n-2}a_{n-2} + r_{n-1},\\
&r_{n-2} = r_{n-1}a_{n-1} + r_n,\\
&r_{n-1} = r_n a_n,
\end{aligned}
$$

где $b > r_1 > r_2 \ldots > r_{n-1} > r_n > 0$. Эту цепочку равенств

можно записать в виде

$$\frac{a}{b} = a_0 + \frac{r_1}{b},$$

$$\frac{b}{r_1} = a_1 + \frac{r_2}{r_1},$$

$$\frac{r_1}{r_2} = a_2 + \frac{r_3}{r_2},$$

. . . . . .

$$\frac{r_{n-2}}{r_{n-1}} = a_{n-1} + \frac{r_n}{r_{n-1}},$$

$$\frac{r_{n-1}}{r_n} = a_n.$$

Пользуясь этими равенствами, можно выразить a/b через числа a_0, a_1, ..., a_n. Действительно, первое равенство запишем в виде

$$\frac{a}{b} = a_0 + \frac{1}{\frac{b}{r_1}};$$

заменяя здесь b/r_1 его выражением из второго равенства, имеем

$$\frac{a}{b} = a_0 + \frac{1}{a_1 + \frac{r_2}{r_1}} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{r_1}{r_2}}}$$

и т. д. В результате мы получаем

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}.$$

Выражение, стоящее справа в этом равенстве, называют конечной *цепной дробью*.

ОПРЕДЕЛЕНИЕ. *Конечной цепной дробью* называется выражение вида

$$(1)\quad a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}},$$

где a_0 — целое число, $a_1, \ldots, a_n$ — положительные целые числа и $a_n > 1$.

Цепную дробь (1) обычно сокращенно записывают в виде

$$|a_0;\ a_1,\ a_2,\ \ldots,\ a_n|.$$

Приведенные выше рассуждения показывают, что любое рациональное число можно представить в виде конечной цепной дроби.

Пример. Разложим в цепную дробь число $\frac{126}{37}$.

С помощью алгоритма Евклида находим:

$$\frac{126}{37} = 3 + \frac{15}{37} = 3 + \frac{1}{\frac{37}{15}} = 3 + \frac{1}{2 + \frac{1}{\frac{15}{7}}} = 3 + \frac{1}{2 + \frac{1}{2 + \frac{1}{7}}},$$

или

$$\frac{126}{37} = |3;\ 2,\ 2,\ 7|.$$

Можно показать, что всякое рациональное число обладает единственным представлением в виде конечной цепной дроби.

Подходящие дроби. Пусть

$$(1)\quad a_0 + \cfrac{1}{a_1 + \ddots} = |a_0;\ a_1,\ \ldots,\ a_n|$$

есть конечная цепная дробь. Цепная дробь

$$(2)\quad A_k = |a_0;\ a_1,\ \ldots,\ a_k|,$$

где $k \in \{0, 1, \ldots, n\}$, называется *k-й подходящей дробью* к дроби (1). По определению, *нулевой подходящей дробью* к дроби (1) называется число $A_0 = a_0$. Отметим, что $(k+1)$-я подходящая дробь A_{k+1} может быть получена из k-й подходящей дроби A_k в результате замены элемента a_k на $a_k + \frac{1}{a_{k+1}}$.

Определим числа P_k и Q_k ($k \in \{0, 1, \ldots, n\}$) индуктивно с помощью следующих формул:

$$(3)\quad \begin{array}{ll} P_0 = a_0, & Q_0 = 1, \\ P_1 = a_0 a_1 + 1, & Q_1 = a_1, \\ \ldots\ldots\ldots & \ldots\ldots \\ P_k = P_{k-1} a_k + P_{k-2}, & Q_k = Q_{k-1} a_k + Q_{k-2} \\ & (k \in \{2, 3, \ldots, n\}). \end{array}$$

ТЕОРЕМА 3.2. *Для любой подходящей дроби A_k к цепной дроби* (1) *имеет место равенство*

$$(4)\quad A_k=\frac{P_k}{Q_k}\qquad (k=0,\ 1,\ \ldots,\ n).$$

Доказательство. Формула (4) доказывается индукцией по k. Из формул (3) непосредственно следуют равенства

$$A_0=\frac{a_0}{1}=\frac{P_0}{Q_0},$$

$$A_1=a_0+\frac{1}{a_1}=\frac{a_0a_1+1}{a_1}=\frac{P_1}{Q_1},$$

т. е. утверждение теоремы верно для $k=0$ и $k=1$. Далее,

$$A_2=a_0+\frac{1}{a_1+\dfrac{1}{a_2}}=\frac{(a_0a_1+1)\,a_2+a_0}{a_1a_2+1}=\frac{P_1a_2+P_0}{Q_1a_2+Q_0},$$

значит, утверждение теоремы верно для $k=2$.

Предположим, что утверждение теоремы верно для m-й подходящей дроби, где $2\leqslant m<n$, т. е.

$$(5)\quad A_m=\frac{P_m}{Q_m},$$

и докажем, что утверждение теоремы верно для $(m+1)$-й подходящей дроби. На основании формул (3) равенство (5) можно записать в виде

$$(6)\quad A_m=\frac{P_{m-1}a_m+P_{m-2}}{Q_{m-1}a_m+Q_{m-2}}.$$

В обеих частях равенства (6) заменим элемент a_m на $a_m+\dfrac{1}{a_{m+1}}$. Эта замена переводит A_m в A_{m+1} и поэтому из (6) получаем

$$A_{m+1}=\frac{P_{m-1}\left(a_m+\dfrac{1}{a_{m+1}}\right)+P_{m-2}}{Q_{m-1}\left(a_m+\dfrac{1}{a_{m+1}}\right)+Q_{m-2}}=$$

$$=\frac{(P_{m-1}a_m+P_{m-2})\,a_{m+1}+P_{m-1}}{(Q_{m-1}a_m+Q_{m-2})\,a_{m+1}+Q_{m-1}}.$$

Отсюда в силу (3)

$$A_{m+1}=\frac{P_ma_{m+1}+P_{m-1}}{Q_ma_{m+1}+Q_{m-1}}=\frac{P_{m+1}}{Q_{m+1}}.$$

Таким образом, из верности формулы (4) для $k=m$ следует верность этой формулы для $k=m+1$. Поэтому формула (4) верна при всех $k \in \{0, 1, \ldots, n\}$.

Числа P_k и Q_k, определяемые формулами (3), называются соответственно *числителем и знаменателем k-й подходящей дроби*. Формулы (3) дают удобный способ для последовательного вычисления числителей P_k и знаменателей Q_k подходящих дробей. При этом вычисление удобно проводить по следующей схеме:

a_k		a_0	a_1	a_2	a_3	...	a_n
P_k	1	a_0	P_1	P_2	P_3	...	P_n
Q_k	0	1	Q_1	Q_2	Q_3	...	Q_n

Пример. Найдем подходящие дроби к цепной дроби $|2; 5, 7, 3|$:

a_k		2	5	7	3
P_k	1	2	11	79	248
Q_k	0	1	5	36	113

Таким образом, подходящими дробями цепной дроби $|2; 5, 7, 3|$ являются дроби

$$A_0=\frac{P_0}{Q_0}=\frac{2}{1},\quad A_1=\frac{P_1}{Q_1}=\frac{11}{5},\quad A_2=\frac{P_2}{Q_2}=\frac{79}{36},\quad A_3=\frac{P_3}{Q_3}=\frac{248}{113}.$$

ТЕОРЕМА 3.3. *Для* $k \in \{1, \ldots, n\}$ *выполняется равенство*

(7) $P_{k-1}Q_k - Q_{k-1}P_k = (-1)^k$.

Доказательство. Пусть $\Delta_k = P_{k-1}Q_k - Q_{k-1}P_k$. На основании формул (3) равенство (7) выполняется при $k=1$:

(8) $\Delta_1 = P_0Q_1 - Q_0P_1 = a_0a_1 - 1\ (a_0a_1+1) = -1$.

Кроме того, согласно (3),

$$\Delta_k = P_{k-1}Q_k - Q_{k-1}P_k = P_{k-1}(Q_{k-1}a_k + Q_{k-2}) - Q_{k-1}(P_{k-1}a_k + P_{k-2}) = P_{k-1}Q_{k-2} - Q_{k-1}P_{k-2} = -\Delta_{k-1}$$
$$(k \in \{2, \ldots, n\}).$$

В силу (8) отсюда следует, что

$$\Delta_k = (-1)^k \quad \text{для} \quad k \in \{1, 2, \ldots, n\},$$

т. е. выполняется равенство (7). □

СЛЕДСТВИЕ 3.4. *Числа P_k и Q_k взаимно простые и, значит, каждая дробь P_k/Q_k несократима.*

Доказательство. Ввиду (7) любой общий множитель P_k и Q_k есть делитель единицы. Поэтому числа P_k, Q_k взаимно простые и дробь P_k/Q_k несократима. □

Между двумя последовательными подходящими дробями имеется важное соотношение, которое вытекает из (7).

СЛЕДСТВИЕ 3.5. *Для $k \in \{1, \ldots, n\}$ выполняется равенство*

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{(-1)^k}{Q_{k-1}Q_k}.$$

Упражнения.

1. С помощью алгоритма Евклида найдите:
a) НОД (549, 387); b) НОД (589, 343); c) НОД (12 606, 64 994).
2. Разложите в цепную дробь следующие обыкновенные дроби:
a) 2,3547; b) $\frac{99}{170}$.
3. Сократите с помощью разложения в цепную дробь $\alpha = \frac{7857}{9153}$.
4. Зная, что $3{,}141592653 < \pi < 3{,}141592654$, найдите первые четыре подходящие дроби для числа π.
5. Зная, что $e = 2{,}71828182845\ldots$, найдите первые четыре подходящие дроби для числа e.
6. Решите в целых числах следующие уравнения:
a) $5x + 4y = 3$; b) $7x - 19y = 5$; c) $12x - 7y = 15$.

§ 4. ЦЕЛЫЕ СИСТЕМАТИЧЕСКИЕ ЧИСЛА

Целые систематические числа. Пусть g — натуральное число большее 1 и $M = \{0, 1, \ldots, g-1\}$. Говорят, что натуральное число a записано в позиционной системе с основанием g, если

$$(1) \quad a = a_s g^s + a_{s-1} g^{s-1} + \ldots + a_1 g + a_0,$$

где s — целое неотрицательное, $a_0, \ldots, a_s \in M$ и $a_s \neq 0$.

Если каждое число множества $M = \{0, 1, \ldots, g-1\}$ обозначено специальным символом, то эти символы называются *цифрами g-ичной позиционной системы.* Представление (1) записывается тогда сокращенно в виде

$$a = (a_s a_{s-1} \ldots a_1)_g$$

и называется *записью в g-ичной позиционной системе*. Так, например, запись

$a=(2315)_{10}$ означает, что $a=2\cdot 10^3+3\cdot 10^2+1\cdot 10+5$,

запись

$b=(101001)_2$ означает, что $b=1\cdot 2^5+0\cdot 2^4+$
$+1\cdot 2^3+0\cdot 2^2+0\cdot 2^1+1$.

ТЕОРЕМА 4.1. *Пусть g — данное натуральное число, большее единицы, и $M=\{0, 1, \ldots, g-1\}$. Всякое натуральное число a однозначно представимо в виде*

(1) $a=a_s g^s+a_{s-1}g^{s-1}+\ldots+a_1 g+a_0$,

где $a_i\in M$ и $a_s\neq 0$.

Доказательство. Существование представления (1) доказывается индукцией по a. Если $a=1$ или $a<g$, то равенство $a=a$ является искомым представлением. Пусть $a\geqslant g$; предположим, что возможность представления (1) уже установлена для всех натуральных чисел, меньших, чем a. Так как $a\geqslant g$, то разделив a на g с остатком, получим

(2) $a=bg+a_0$, где $a_0\in M$ и $1\leqslant b<a$.

Поскольку $b<a$, то согласно индуктивному предположению число b представимо в виде

(3) $b=a_s g^{s-1}+\ldots+a_2 g+a_1$, где $a_1, \ldots, a_s\in M$ и $a_s\neq 0$.

Подставив выражение (3) для b в правую часть (2), получим представление для числа a,

$a=a_s g^s+\ldots+a_1 g+a_0$, где $a_i\in M$ и $a_s\neq 0$,

которое называется *разложением числа a по степеням числа g*.

Докажем однозначность представления индукцией по a. Если $1\leqslant a<g$, то легко видеть, что единственность имеет место. Предположим, что единственность доказана для всех натуральных чисел, меньших, чем a. Предположим, что кроме (1) для a существует другое представление:

(4) $a=a'_{s'}g^{s'}+\ldots+a'_1 g+a'_0$.

Ввиду (1) и (4) имеем

(5) $a=g(a_s g^{s-1}+\ldots+a_2 g+a_1)+a_0=$
$=g(a'_{s'}g^{s'-1}+\ldots+a'_2 g+a'_1)+a'_0$.

Из (5) в силу однозначности деления с остатком следует, что

$$a_0 = a_0',$$
$$b = a_s g^{s-1} + \ldots + a_2 g + a_1 = a_{s'}' g^{s'-1} + \ldots + a_2' g + a_1'.$$

Так как $b < a$, то, по индуктивному предположению, $s = s'$ и $a_i = a_i'$ для $i = 1, \ldots, s$. □

Арифметические операции над целыми систематическими числами. Если натуральные числа записаны в десятичной системе счисления, то мы пользуемся правилами сложения и вычитания чисел «столбиком». Действия сложения и вычитания целых многозначных чисел в g-ичной системе счисления производятся по тем же правилам, что и в десятичной системе. В g-ичной системе, как и в десятичной, при сложении многозначных чисел мы складываем сначала единицы, затем переходим к следующему разряду и т. д. до тех пор, пока не дойдем до самого старшего из имеющихся разрядов. При этом всякий раз, когда при сложении в предыдущем разряде получается сумма, бо́льшая, чем основание g системы счисления или равная ему, надо сделать перенос в следующий разряд.

Следующие примеры иллюстрируют операции сложения в шестиричной и двоичной системах счисления:

$$\begin{array}{r} (4253)_6 \\ +\,(2542)_6 \\ \hline (11235)_6 \end{array} \qquad \begin{array}{r} (10011)_2 \\ +\,(11001)_2 \\ \hline (101100)_2 \end{array}$$

Вычитание в пятиричной системе иллюстрируется примером

$$\begin{array}{r} (42044)_5 \\ -\,(23141)_5 \\ \hline (13403)_5 \end{array}$$

Операция умножения целых многозначных чисел в g-ичной системе счисления производится по тем же правилам, что и в десятичной системе («столбиком»). При выполнении операции умножения удобно пользоваться таблицами умножения. Ниже приведена таблица умножения в шестиричной системе. В каждой клетке этой таблицы стоит произведение чисел, представляющих номера строки и столбца, на пересечении которых находится клетка, причем все числа записаны в шестиричной системе счисления.

Следующий пример иллюстрирует операцию умножения («столбиком») в шестиричной системе:

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	10	12	14
3	0	3	10	13	20	23
4	0	4	12	20	24	32
5	0	5	14	23	32	41

$$\begin{array}{r} \times 235 \\ 343 \\ \hline 1153 \\ 1432 \\ 1153 \\ \hline 135213 \end{array}$$

Перевод чисел из одной системы счисления в другую. Пусть число a записано в m-ичной системе. Это значит, что оно представлено в виде суммы:

$$(1)\quad a = b_k m^k + b_{k-1} m^{k-1} + \ldots + b_1 m + b_0.$$

Как записать это число в какой-либо другой системе, скажем, в g-ичной системе? Это значит, надо представить число a в виде

$$(2)\quad a = a_s g^s + a_{s-1} g^{s-1} + \ldots + a_1 g + a_0.$$

Для этого необходимо найти коэффициенты $a_0, a_1, \ldots, a_s$, каждый из которых является какой-либо цифрой от 0 до $g-1$ включительно. Разделим число a, заданное в m-ичной системе, на g, получим остаток a_0 и частное q_1. Затем разделим частное q_1 на g, получим остаток a_1 и частное q_2. Этот процесс мы продолжаем до тех пор, пока не получим остаток, равный нулю. В результате получим все цифры $a_0, a_1, \ldots, a_s$, входящие в g-ичное представление (2) числа a.

В качестве примера рассмотрим перевод числа $a = (5\,3\,7\,8)_{10}$ в шестиричную систему счисления. Разделив его на 6, получим частное 896 и остаток 2. Следовательно, в шестиричной записи числа a последняя цифра равна 2. Чтобы найти вторую цифру, разделим частное 896 на 6. Получим частное 149 и остаток 2. Следовательно, вторая цифра в шестиричной записи числа a есть 2. Затем, раз-

делив 149 на 6, получим частное 24 и остаток 5. Этот остаток 5 является третьей цифрой в шестиричной записи числа a. Наконец, разделим частное 24 на 6, получим частное 4 и остаток 0. Таким образом,

$$(5\ 3\ 7\ 8)_{10} = (4\ 0\ 5\ 2\ 2)_6.$$

Упражнения

1. Составьте таблицу умножения в семиричной системе счисления.
2. Докажите, что $A = (a_n a_{n-1} \dots a_1 a_0)_{12}$ делится на 8 (на 9), если на 8 (на 9) делится число $(a_1 a_0)_{12}$, образованное его двумя последними цифрами.
3. Покажите, что число $A = (a_n a_{n-1} \dots a_1 a_0)_g$, т. е. число $a_n g^n + a_{n-1} g^{n-1} + \dots + a_1 g + a_0$, делится на $g-1$, если на $g-1$ делится сумма его цифр, т. е. сумма $a_n + a_{n-1} + \dots + a_1 + a_0$.
4. Докажите, что натуральное число, десятичная запись которого состоит из 3^n единиц, делится на 3^n.
5. В десятичной записи некоторого натурального числа имеется 30 единиц, а остальные цифры равны нулю. Может ли это число быть полным квадратом?
6. Вы хотите узнать номер моего телефона, задавая мне вопросы, на которые я буду отвечать только «да» или «нет». Найдите способ, гарантирующий успех за наименьшее число вопросов (считая, что телефонный номер состоит из произвольных пяти цифр).

§ 5. РАСПРЕДЕЛЕНИЕ ПРОСТЫХ ЧИСЕЛ

Распределение простых чисел. Обозначим через $\pi(x)$ число положительных простых чисел, не превосходящих действительного числа x. В § 1 установлено, что существует бесконечно много простых чисел (теорема Евклида). Следовательно, $\pi(x) \to \infty$ при $x \to \infty$.

А. Лежандр в 1808 г. опубликовал найденную им эмпирически формулу для приближенного представления функции $\pi(x)$. Лежандр высказал утверждение, что для больших значений x $\pi(x)$ приближенно равно $\frac{x}{\log x - 1{,}08366}$.

П. Л. Чебышев в 1849 г. показал ошибочность этого утверждения. В работах, опубликованных в 1848 и 1850 гг., Чебышев установил связь функции $\pi(x)$ с отношением $\frac{x}{\log x}$. Он доказал следующую теорему: *существуют положительные постоянные a и b, $a < b$, такие, что для всех достаточно больших x*

$$(1)\quad a \cdot \frac{x}{\log x} < \pi(x) < b \frac{x}{\log x}.$$

Ниже приводится доказательство теоремы: *для всех* $x \geqslant 2$ *выполняются неравенства*

$$(2)\quad \log 2 \cdot \frac{x}{\log x} - 2 < \pi(x) < 4 \log 2 \frac{x}{\log x} + \log_2 x.$$

На основании неравенств (2) могут быть найдены константы a и b для неравенств (1).

Для доказательства неравенств (2) вводится функция $T(x) = \log [x]!$ и устанавливаются оценки сверху и снизу для функции $T(x) - 2T\left(\frac{x}{2}\right)$.

Функции $T(x)$ и $\Lambda(x)$. Символом $\Lambda(x)$ обозначается функция, которая имеет значение $\log p$, если n — простое число или положительная степень простого числа p, а в остальных случаях ее значение — нуль,

$$\Lambda(n) = \begin{cases} \log p, & \text{если } n = p^m \text{ для какого-либо натурального числа } m > 0, \\ 0, & \text{если } n \neq p^m. \end{cases}$$

Ниже будет нужно следующее свойство этой функции:

$$(1)\quad \sum_{d \mid n} \Lambda(d) = \log n.$$

Пусть $n = \prod_{p \mid n} p^{e_p}$ есть каноническое разложение натурального числа n. Легко видеть, что

$$\sum_{d \mid n} \Lambda(d) = \sum_{p^\alpha \mid n} \log p = \sum_{p \mid n} e_p \log p = \log n,$$

где p^α пробегает все степени простых чисел, входящих в n.

Символом $T(x)$ обозначается функция, которая для всякого действительного $x \geqslant 0$ принимает значение $\log [x]!$, т. е.

$$T(x) = \log [x]! = \sum_{n \leqslant x} \log n,$$

где $[x]$ есть целая часть числа x.

Просуммировав (1) по всем положительным целым $n \leqslant x$, получим

$$\sum_{m \leqslant x} \Lambda(m) \left[\frac{x}{m}\right] = \sum_{n \leqslant x} \log n = \log [x]! = T(x).$$

Таким образом, доказано следующее предложение.

ПРЕДЛОЖЕНИЕ 5.1. *Для любого действительного числа* $x \geqslant 1$

(1) $T(x) = \sum_{m \leqslant x} \Lambda(m) \left[\frac{x}{m}\right]$.

Неравенства для функции $T(x)$. Согласно определению функции $T(x)$

(1) $T(n) = \log n!$,

для любого действительного положительного x

(2) $T(x) = \log [x]!$

Ввиду (1)

(3) $T(2n) - 2T(n) = \log \frac{(2n)!}{(n!)^2} = \log C_{2n}^n$.

Докажем, что для любого натурального $n \geqslant 2$ выполняются неравенства

(4) $\frac{4^n}{2n} < C_{2n}^n < 4^n$.

Легко видеть, что $C_{2n}^n < (1+1)^{2n} = 4^n$. Следующие выкладки доказывают второе неравенство:

$$C_{2n}^n = \frac{2n\,(2n-1)\,(2n-2)\,\ldots\,2\cdot 1}{n^2\,(n-1)^2\,\ldots\,1^2} =$$

$$= \frac{2n\,(2n-1)}{n^2} \cdot \frac{(2n-2)\,(2n-3)}{(n-1)^2} \cdot \ldots \cdot \frac{2\cdot 1}{1^2} =$$

$$= 4^n \left(1 - \frac{1}{2n}\right)\left(1 - \frac{1}{2\,(n-1)}\right) \ldots \left(1 - \frac{1}{2}\right) =$$

$$= 4^n \cdot \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdot \ldots \cdot \frac{2n-1}{2n} > 4^n \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdot \ldots$$

$$\ldots \cdot \frac{2n-1}{2n} = \frac{4^n}{2n}.$$

Из (3) в силу (4) следуют для $n \geqslant 2$ неравенства

(5) $T(2n) - 2T(n) < \log 4^n = 2n \log 2$,

(6) $T(2n) - 2T(n) > \log \frac{4^n}{2n} = 2n \log 2 - \log 2n$.

Пусть x — произвольное действительное число, большее или равное 2, и пусть $2n$ есть наибольшее четное число, не превосходящее x. Тогда из равенства (2) следует, что

(7) $T(x) - T(2n) \leqslant \log x$.

Так как $T(x)$ есть неубывающая функция, то из (5) и (7) следует

(8) $T(x)-2T\left(\frac{x}{2}\right)<x\log 2+\log x.$

В силу (6)

$$T(x)-2T\left(\frac{x}{2}\right)>(x-2)\log 2-\log x.$$

Отсюда при $x\geqslant 4$ следует неравенство

(9) $T(x)-2T\left(\frac{x}{2}\right)>x\log 2-2\log x \quad (x\geqslant 4).$

Неравенства Чебышева. Выше (см. неравенство (8)) было получено неравенство

(1) $T(x)-2T\left(\frac{x}{2}\right)<x\log 2+\log x$

и доказано равенство

(2) $T(x)=\sum\limits_{m\leqslant x}\Lambda(m)\left[\frac{x}{m}\right].$

Если $\frac{x}{2}<m\leqslant x$, то $2m>x$. Поэтому из равенства $\left[\frac{x}{m}\right]=1$ следует, что $\left[\frac{x}{2m}\right]=0$. Отсюда и из (2) имеем:

(3) $T(x)-2T\left(\frac{x}{2}\right)=\sum\limits_{m\leqslant x}\Lambda(m)\left(\left[\frac{x}{m}\right]-2\left[\frac{x}{2m}\right]\right)\geqslant$

$$\geqslant\sum_{\frac{x}{2}<m\leqslant x}\Lambda(m)\geqslant\sum_{\frac{x}{2}<p\leqslant x}\log p\geqslant\log\left(\frac{x}{2}\right)\left[\pi(x)-\pi\left(\frac{x}{2}\right)\right].$$

В силу (2) и (3)

(4) $\left(\pi(x)-\pi\left(\frac{x}{2}\right)\right)\log\frac{x}{2}<x\log 2+\log x.$

Из этого неравенства выводим, заменяя x последовательно на $\frac{x}{2}$, $\frac{x}{4}$, $\frac{x}{8}$, ..., ряд неравенств:

(4′) $\left(\pi\left(\frac{x}{2}\right)-\pi\left(\frac{x}{4}\right)\right)\log\frac{x}{4}<\frac{x}{2}\log 2+\log\frac{x}{2},$

(4″) $\left(\pi\left(\frac{x}{4}\right)-\pi\left(\frac{x}{8}\right)\right)\log\frac{x}{8}<\frac{x}{4}\log 2+\log\frac{x}{4}.$

. . . . . .

Суммируя левые части неравенств (4), (4′), (4″), ..., получаем:

$$\pi(x)\log\frac{x}{2}-\pi\left(\frac{x}{2}\right)\left(\log\frac{x}{2}-\log\frac{x}{4}\right)-$$
$$-\pi\left(\frac{x}{4}\right)\left(\log\frac{x}{4}-\log\frac{x}{8}\right)-\ldots=$$
$$=\pi(x)\log x-\left(\pi(x)+\pi\left(\frac{x}{2}\right)+\pi\left(\frac{x}{4}\right)+\ldots\right)\log 2>$$
$$>\pi(x)\log x-\left(x+\frac{x}{2}+\frac{x}{4}+\ldots\right)\log 2=$$
$$=\pi(x)\log x-2x\log 2.$$

Сумма правых частей неравенств (4), (4′), (4″), ... будет меньше $2x\log 2+\log x\cdot\log_2 x$, так как число неравенств не превышает $\log_2 x$. Таким образом, приходим к неравенству

$$\pi(x)\log x-2x\log 2<2x\log 2+\log x\cdot\log_2 x,$$

откуда

$$\pi(x)<4\log 2\,\frac{x}{\log x}+\log_2 x.$$

При этом найденное неравенство имеет место для любого $x\geqslant 2$.

Выше было доказано неравенство

$$T(x)-2T\left(\frac{x}{2}\right)>x\log 2-2\log x.$$

Кроме того, так как $T(x)-2T\left(\frac{x}{2}\right)=$
$=\sum\limits_{m\leqslant x}\Lambda(m)\left(\left[\frac{x}{m}\right]-\left[\frac{x}{2m}\right]\right)$, то имеем

$$T(x)-2T\left(\frac{x}{2}\right)\leqslant\sum_{m\leqslant x}\Lambda(m)=\sum_{p\leqslant x}\left[\frac{\log x}{\log p}\right]\log p\leqslant$$
$$\leqslant\sum_{p\leqslant x}\frac{\log x}{\log p}\log p\leqslant\pi(x)\log x.$$

Таким образом, $x\log 2-2\log x<\pi(x)\log x$. Следовательно, для любого $x\geqslant 2$

$$\log 2\,\frac{x}{\log x}-2<\pi(x),$$

т. е. получена нижняя граница нужного вида для $\pi(x)$.

Таким образом, доказана следующая теорема.

ТЕОРЕМА 5.2. *Для всех* $x \geqslant 2$ *имеем*:

$$\log 2 \frac{x}{\log x} - 2 < \pi(x) < 4 \log 2 \frac{x}{\log x} + \log_2(x).$$

П. Л. Чебышев в 1850 г. доказал более точные неравенства. Он доказал, что для достаточно больших x выполняются неравенства

$$(0{,}92\ldots)\frac{x}{\log x} < \pi(x) \leqslant (1{,}105\ldots)\frac{x}{\log x}.$$

При доказательстве этих неравенств Чебышев вместо $T(x) - 2T\left(\frac{x}{2}\right)$ рассматривал более сложное выражение:

$$T(x) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) + T\left(\frac{x}{30}\right).$$

В 1851 г. Чебышев обосновал предположение о зависимости между $\pi(x)$ и $\frac{x}{\log x}$:

$$\underline{\lim} \frac{\pi(x)}{x/\log x} \leqslant 1 \leqslant \overline{\lim} \frac{\pi(x)}{x/\log x},$$

так что если предел отношения $\frac{\pi(x)}{x/\log x}$ существует, то он должен быть равен 1.

Центральным результатом в теории чисел является асимптотический закон распределения простых чисел, впервые доказанный в 1896 г. Адамаром и Валле-Пуссеном. Этот закон гласит, что *отношение* $\pi(x) : \frac{x}{\log x}$ *стремится к* 1 *при неограниченном возрастании* x, т. е.

$$\lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1.$$

Простые числа в арифметических прогрессиях. Рассмотрим три теоремы (5.3—5.5), которые являются частными случаями более общей теоремы — теоремы Дирихле.

ТЕОРЕМА 5.3. *Арифметическая последовательность* $4n+3$ $(n = 0, 1, \ldots)$ *содержит бесконечно много простых чисел.*

Доказательство. Рассмотрим число M, определяемое равенством $M = 4n! - 1$, где n — целое положительное число. M есть число вида $4k+3$, оно не может состоять только из простых множителей вида $4k+1$, потому что

произведение чисел вида $4k+1$ является числом такого же вида:

$$(4k+1)(4k_1+1)=4(4kk_1+k+k_1)+1.$$

Поэтому число M имеет хотя бы один простой множитель вида $4k+3$, который больше n. Таким образом, для каждого натурального числа n существует простое число, большее n, имеющее вид $4k+3$. □

ТЕОРЕМА 5.4. *Арифметическая последовательность* $6n+5$ $(n=0, 1, 2, \ldots)$ *содержит бесконечно много простых чисел.*

Доказательство этой теоремы аналогично доказательству предыдущей теоремы. Рассмотрим число M, определяемое равенством $M=6n!-1$, где n — любое целое положительное число; M есть число вида $6k+5$. Число M не может состоять только из простых множителей вида $6k+1$, так как произведение чисел вида $6k+1$ является числом такого же вида:

$$(6k+1)(6k_1+1)=6(6kk_1+k+k_1)+1.$$

Поэтому число M имеет хотя бы один простой множитель вида $6k+5$, который больше n. Итак, для каждого натурального числа n существует простое число, большее n, имеющее вид $6k+5$. □

ТЕОРЕМА 5.5. *Арифметическая последовательность*

$$4n+1 \quad (n=0, 1, 2, \ldots)$$

содержит бесконечно много простых чисел.

Доказательство. Пусть n — любое натуральное число, большее единицы. Тогда $(n!)^2+1$, как число нечетное, большее единицы, имеет нечетный простой делитель p; следовательно, p есть число вида $4k+1$ или $4k+3$. Предположим, что $p=4k+3$. Так как для натуральных a и нечетных m

$$a+1 \mid (a^m+1), \text{ то } (n!)^2+1 \mid (n!)^{2(2k+1)}+1.$$

Так как $2(2k+1)=4k+2=p-1$ и

$$p \mid (n!)^2+1, \text{ то } p \mid (n!)^{p-1}+1.$$

Следовательно,

(1) $p \mid (n!)^p+n!$

С другой стороны, по теореме Ферма,

(2) $p \mid (n!)^p-n!$

Из (1) и (2) следует $p \mid 2(n!)$, что невозможно, так как p есть простое нечетное число, большее n. Следовательно, p должно быть числом вида $4k+1$. Мы доказали, что для каждого натурального числа n существует простое число, большее n, имеющее вид $4k+1$. □

Доказанные выше теоремы являются частными случаями следующей теоремы Дирихле об арифметических прогрессиях: *каждая арифметическая последовательность* $a+km$ $(k=0, 1, 2, \ldots)$, *где* $(a, m)=1$, *содержит бесконечно много простых чисел.*

Упражнения

1. Покажите, что полином x^2+x+41 для последовательности натуральных чисел $x=0, 1, 2, \ldots, 39$ принимает значения, являющиеся различными простыми числами.

2. Пусть f — полином положительной степени от переменной x с целыми коэффициентами. Докажите, что для бесконечного множества натуральных чисел x число $f(x)$ является составным.

3. Опираясь на теорему Дирихле об арифметических прогрессиях, докажите, что для каждого натурального числа m существует простое число, в изображении которого (в десятичной системе счисления или в любой системе счисления с натуральным основанием $q>1$) имеется по крайней мере m нулей.

Глава двенадцатая

ТЕОРИЯ СРАВНЕНИЙ С АРИФМЕТИЧЕСКИМИ ПРИЛОЖЕНИЯМИ

§ 1. СРАВНЕНИЯ И ИХ СВОЙСТВА

Сравнения в кольце целых чисел. Пусть $\mathbb{Z}$ — кольцо целых чисел, m — фиксированное целое число и $m\mathbf{Z}$ — множество всех целых чисел, кратных m.

ОПРЕДЕЛЕНИЕ. Два целых числа a и b называют *сравнимыми по модулю* m, если m делит $a-b$.

Если a сравнимо с b по модулю m, то это записывается так:

(1) $a \equiv b \pmod{m}$.

Отношение сравнимости по модулю m обладает свойствами рефлексивности, симметричности и транзитивности, т. е. является отношением эквивалентности. Следовательно, отношение сравнимости индуцирует разбиение множества $\mathbf{Z}$ целых чисел на классы эквивалентности, которые называются *классами вычетов по модулю* m.

Отметим, что отношение сравнимости по модулю m совпадает с отношением сравнимости по модулю $(-m)$. Отношение сравнимости по модулю 0 совпадает с отношением равенства. Любые два целых числа сравнимы по модулю 1.

Так как отношение сравнимости по модулю m есть отношение эквивалентности на множестве $\mathbf{Z}$, то классы эквивалентности, т. е. классы вычетов по модулю m, обладают следующими свойствами:

СВОЙСТВО 1.1. *Любые два класса вычетов по модулю* m *либо совпадают, либо не пересекаются. Объединение всех классов вычетов по модулю* m *совпадает с множеством* $\mathbf{Z}$ *всех целых чисел.*

СВОЙСТВО 1.2. *Пусть* A *и* B — *классы вычетов по модулю* m, $a \in A$ *и* $b \in B$. *Смежные классы* A *и* B *совпадают тогда и только тогда, когда* $a \equiv b \pmod{m}$.

СВОЙСТВО 1.3. *Если A — класс вычетов по модулю m и a — любой элемент из A, то $A=a+m\mathbf{Z}$, т. е. $A=\{a+mk \mid k\in\mathbf{Z}\}$.*

ПРЕДЛОЖЕНИЕ 1.1. *Числа a и b сравнимы по модулю m ($m\neq 0$) тогда и только тогда, когда при делении на m они дают одинаковые остатки.*

Доказательство. Пусть при делении с остатком чисел a и b на m получаются частные q и q_1 и остатки r и r_1,

$$a=qm+r,\ 0\leqslant r<m;\quad b=q_1m+r_1,\ 0\leqslant r_1<m.$$

Предположим, что $r>r_1$. Вычитая из первого равенства второе, получим

$$(1)\quad a-b=(q-q_1)m+(r-r_1),\ 0\leqslant r-r_1<m.$$

Если $a\equiv b\,(\mathrm{mod}\,m)$, то согласно определению сравнимости $a-b$ делится на m и поэтому $r-r_1=0$ и $r=r_1$. С другой стороны, если $r=r_1$, то в силу (1) $a-b$ делится на m, т. е. $a\equiv b\ (\mathrm{mod}\,m)$. □

Простейшие свойства сравнений. Многие свойства сравнений аналогичны свойствам равенств.

СВОЙСТВО 1.4. *Сравнения можно почленно складывать и вычитать,* т. е. *если $a\equiv b\ (\mathrm{mod}\,m)$, $c\equiv d\ (\mathrm{mod}\,m)$, то $a+c\equiv b+d\ (\mathrm{mod}\,m)$.*

Доказательство. По условию, $m\mid(a-b)$ и $m\mid(c-d)$. Следовательно, $m\mid(a-b)\pm(c-d)$, $m\mid(a+c)-(b+d)$ и $m\mid(a-c)-(b-d)$. □

СВОЙСТВО 1.5. *Сравнения можно почленно перемножить, т. е. если $a\equiv b\,(\mathrm{mod}\,m)$, $c\equiv d\ (\mathrm{mod}\,m)$, то $ac\equiv bd\,(\mathrm{mod}\,m)$.*

В частности, обе части сравнения можно умножить на одно и то же целое число.

Доказательство. По условию, $a-b\in m\mathbf{Z}$ и $c-d\in m\mathbf{Z}$. Следовательно, $ac-bd=(ac-bc)+(bc-bd)=(a-b)c+b(c-d)\in m\mathbf{Z}$, т. е. $ac\equiv bd\,(\mathrm{mod}\,m)$. □

СВОЙСТВО 1.6. *Обе части сравнения можно разделить на их общий множитель, если он взаимно простой с модулем.*

Доказательство. Если $ca\equiv cb\,(\mathrm{mod}\,m)$, т. е. $m\mid c(a-b)$ и число c взаимно простое с m, то m делит $a-b$. Следовательно, $a\equiv b\,(\mathrm{mod}\,m)$. □

СВОЙСТВО 1.7. *Обе части сравнения и модуль можно разделить на их общий делитель.*

Доказательство. Если $ka \equiv kb \pmod{mk}$, то $k(a-b)$ делится на km. Следовательно, $a-b$ делится на m, т. е. $a \equiv b \pmod{m}$. □

СВОЙСТВО 1.8. *Пусть m_1 есть любой делитель числа m. Если $a \equiv b \pmod{m}$, то $a \equiv b \pmod{m_1}$.*

Доказательство. Если $a \equiv b \pmod{m}$, то $a-b$ делится на m. Так как m_1 — делитель m, то $a-b$ делится на m_1, т. е. $a \equiv b \pmod{m_1}$. □

Упражнения

1. Покажите, что любое натуральное число, записанное в десятичной системе, сравнимо по модулю 9 и по модулю 3 с суммой своих цифр.
2. Установите способ проверки арифметических действий при помощи числа 9.
3. Найдите признаки делимости чисел в десятичной системе счисления на 9 и 19.
4. Найдите признаки делимости чисел в десятичной системе счисления на 7 и 13.
5. Найдите признаки делимости на 2, 3, 4, 5, 7, 9 в восьмеричной системе счисления.
6. Найдите признаки делимости на 2, 3, 4, 5, 6, 7, 8, 9, 11, 13 в двенадцатиричной системе счисления.
7. Докажите, что если $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$ и m, n — взаимно простые, то $a \equiv b \pmod{mn}$.
8. Пусть d — наибольший общий делитель целых чисел m и n. Покажите, что если $a \equiv b \pmod{m}$ и $a \equiv b \pmod{n}$, то $a \equiv b \left(\mathrm{mod}\, \frac{mn}{d}\right)$.

§ 2. ПОЛНАЯ СИСТЕМА ВЫЧЕТОВ

Полная система вычетов. Согласно свойству 1.1, каждый класс вычетов по модулю m однозначно определяется любым принадлежащим ему числом a; этот класс является множеством всех чисел вида $a+km$, т. е. является множеством

$$\{a+km \mid k \in \mathbf{Z}\} = a+m\mathbf{Z}.$$

Класс вычетов по модулю m, содержащий число a, т. е. совокупность всех целых чисел b таких, что $b \equiv a \pmod{m}$, обозначается просто через $a \bmod m$:

$$a \bmod m = \{a+km \mid k \in \mathbf{Z}\}.$$

Любое число, принадлежащее классу вычетов $a \bmod m$, называется *представителем этого класса*.

ОПРЕДЕЛЕНИЕ. *Полной системой вычетов по модулю m* называется совокупность m целых чисел, содер-

жащая точно по одному представителю из каждого класса вычетов по модулю m.

Каждый класс вычетов по модулю m содержит в точности одно из чисел совокупности всех возможных остатков от деления на m, а именно $0, 1, 2, \ldots, m-1$.

ОПРЕДЕЛЕНИЕ. Совокупность чисел $0, 1, 2, \ldots, m-1$ называется *системой наименьших неотрицательных вычетов по модулю m.*

Всюду ниже запись $(a, m)=1$ будет означать, что числа a и m — взаимно простые.

ПРЕДЛОЖЕНИЕ 2.1. *Любая совокупность m чисел $(m>1)$, попарно несравнимых по модулю m, есть полная система вычетов по модулю m.*

Доказательство. Пусть M есть совокупность m чисел, попарно несравнимых по модулю m. Тогда эти числа принадлежат к различным классам вычетов. Кроме того, M содержит m чисел. Следовательно, множество M содержит по одному представителю из каждого класса вычетов по модулю m. □

ПРЕДЛОЖЕНИЕ 2.2. *Пусть a, b — целые числа и $(a, m)=1$. Если x пробегает полную систему вычетов по модулю m, то $ax+b$ тоже пробегает полную систему вычетов по модулю m.*

Доказательство. Пусть M — полная система вычетов. Тогда множество $M_1=\{ax+b \mid x \in M\}$, так же как и M, содержит m элементов. Любые два числа ax_1+b и ax_2+b из M несравнимы, если $x_1 \not\equiv x_2 \pmod m$. Следовательно, множество M_1 есть полная система вычетов по модулю m. □

Аддитивная группа классов вычетов. Обозначим через $\mathbf{Z}/m\mathbf{Z}$ множество всех классов вычетов по модулю m:

$$\mathbf{Z}/m\mathbf{Z}=\{0 \bmod m,\ 1 \bmod m,\ \ldots,\ (m-1) \bmod m\}.$$

Определим операции $+$, $-$ на множестве классов вычетов следующим образом:

$$a \bmod m + b \bmod m = (a+b) \bmod m,$$

$$-(a \bmod m) = (-a) \bmod m.$$

Согласно свойствам 1.4 и 1.5 сравнений, отношение сравнимости на множестве $\mathbf{Z}$ является конгруэнцией относительно операций сложения в $\mathbf{Z}$ и операций перехода к противоположному элементу. Таким образом, любым двум классам $a \bmod m$ и $b \bmod m$ независимо от выбора

в них представителей a, b однозначно соответствует класс $(a+b) \bmod m$, являющийся их суммой. Аналогично, класс $-(a \bmod m)$ не зависит от выбора представителя a. Так как сложение целых чисел коммутативно и ассоциативно, то коммутативно и ассоциативно сложение классов вычетов, т. е. для любых a, b, $c \in \mathbf{Z}$

$$a \bmod m + b \bmod m = b \bmod m + a \bmod m,$$
$$(a \bmod m + b \bmod m) + c \bmod m = a \bmod m + (b \bmod m + c \bmod m).$$

Класс вычетов $0 \bmod m$ является нейтральным относительно сложения, т. е. для любого класса вычетов $a \bmod m$

$$a \bmod m + 0 \bmod m = a \bmod m.$$

Далее, классы $a \bmod m$ и $(-a) \bmod m$ являются взаимно противоположными, т. е.

$$a \bmod m + (-a) \bmod m = 0 \bmod m.$$

Таким образом, имеет место следующая теорема.

ТЕОРЕМА 2.3. *Алгебра* $\langle \mathbf{Z}/m\mathbf{Z}, +, - \rangle$ *является группой. Эта группа является фактор-группой группы* $\mathbf{Z}$ *по подгруппе* $m\mathbf{Z}$.

ОПРЕДЕЛЕНИЕ. Группа $\langle \mathbf{Z}/m\mathbf{Z}, +, - \rangle$ называется *аддитивной группой классов вычетов по модулю* m.

Кольцо классов вычетов. На множестве классов вычетов по модулю m определим операцию умножения следующим образом:

$$(a \bmod m) \cdot (b \bmod m) = ab \bmod m.$$

Согласно свойству 1.5 сравнений, отношение сравнимости по модулю m на $\mathbf{Z}$ является конгруэнцией относительно операции умножения на $\mathbf{Z}$. Таким образом, каждым двум классам вычетов $a \bmod m$ и $b \bmod m$ независимо от выбора в них представителей a, b однозначно ставится в соответствие класс вычетов $ab \bmod m$, являющийся их произведением. Так как определение операций сложения и умножения классов вычетов сводится к соответствующим операциям над числами из классов вычетов, то при этом сохраняются законы сложения и умножения этих операций, в частности законы коммутативности, ассоциативности и

дистрибутивности:

$$(a \bmod m)(b \bmod m) = (b \bmod m)(a \bmod m),$$

$$(a \bmod m)[(b \bmod m)(c \bmod m)] = [(a \bmod m)(b \bmod m)](c \bmod m),$$

$$(a \bmod m)[(b \bmod m) + (c \bmod m)] = (a \bmod m)(b \bmod m) + (a \bmod m)(c \bmod m).$$

Кроме того, класс вычетов $1 \bmod m$ является нейтральным элементом относительно умножения:

$$(a \bmod m)(1 \bmod m) = a \bmod m.$$

Таким образом, верна следующая теорема.

ТЕОРЕМА 2.4. *Алгебра* $\langle \mathbf{Z}/m\mathbf{Z}, +, —, \cdot, 1 \bmod m \rangle$ *является коммутативным кольцом.*

ОПРЕДЕЛЕНИЕ. Кольцо $\langle \mathbf{Z}/m\mathbf{Z}, +, —, \cdot, 1 \bmod m \rangle$ называется *кольцом классов вычетов по модулю* m.

Упражнения

1. Найдите полную систему вычетов и полную систему абсолютно наименьших вычетов по модулю 30.

2. Найдите полную систему абсолютно наименьших вычетов по модулю 19.

3. Образуют ли степени $2^0, 2^1, 2^2, \ldots, 2^{10}$ вместе с числом 0 полную систему вычетов по модулю 11?

4. Подставляя в выражение $3x+7y$ значения $x=0, 1, 2, 3, 4, 5, 6$ и $y=0, 1, 2$, проверьте, что в результате получится полная система вычетов по модулю 21.

§ 3. ПРИВЕДЕННАЯ СИСТЕМА ВЫЧЕТОВ

Приведенная система вычетов. Пусть n — любое положительное число. Обозначим через $\varphi(n)$ число положительных целых чисел, не превосходящих n и взаимно простых с n. Наибольший общий делитель целых чисел a, b, являющийся натуральным числом, будем обозначать через (a, b).

ПРЕДЛОЖЕНИЕ 3.1. *Все числа из фиксированного класса вычетов* $a \bmod m$ *имеют с* m *один и тот же наибольший общий делитель, равный* (a, m).

Доказательство. Если b есть любое число класса вычетов $a \bmod m$, то $b = mq + a$, где q — некоторое целое число. Отсюда в силу предложения 11.3.1 следует, что $(b, m) = (a, m)$. □

Следовательно, (a, m) зависит только от класса вычетов $a \bmod m$ и не зависит от выбора представителя a

в этом классе. В частности, если $(a, m) = 1$, то класс $a \bmod m$ называется *классом вычетов, взаимно простым с модулем* m.

ПРЕДЛОЖЕНИЕ 3.2. *Число классов вычетов, взаимно простых с* m, *равно* $\varphi(m)$.

Доказательство. Из полной системы вычетов по модулю m

$$1, 2, \ldots, m$$

выделим систему всех вычетов, взаимно простых с m:

$$a_1, a_2, \ldots, a_{\varphi(m)}.$$

В силу предложения 3.1 классы вычетов

$$(1) \quad a_1 \bmod m, a_2 \bmod m, \ldots, a_{\varphi(m)} \bmod m$$

взаимно простые с модулем m. Всякий другой класс, не входящий в (1), не взаимно простой с модулем m, так как содержит элемент множества $\{1, 2, \ldots, m\} \setminus \{a_1, a_2, \ldots, a_{\varphi(m)}\}$. Классы, входящие в систему (1), различны. Следовательно, число классов, взаимно простых с m, равно $\varphi(m)$. □

ОПРЕДЕЛЕНИЕ. *Приведенной системой вычетов по модулю* m называется совокупность целых чисел, содержащая по одному представителю из каждого класса вычетов, взаимно простого с m.

ПРЕДЛОЖЕНИЕ 3.3. *Любая совокупность* $\varphi(m)$ *чисел* $m > 1$, *взаимно простых с* m *и попарно несравнимых по модулю* m, *есть приведенная система вычетов по модулю* m.

Доказательство. Пусть M есть совокупность $\varphi(m)$ чисел, взаимно простых с m и попарно несравнимых по модулю m. Тогда эти числа принадлежат к различным классам вычетов. Поэтому множество M содержит по одному представителю из каждого класса вычетов, взаимно простого с модулем m. Следовательно, M есть приведенная система вычетов по модулю m. □

ПРЕДЛОЖЕНИЕ 3.4. *Пусть* a — *целое число, взаимно простое с* m, *и* $b_1, b_2, \ldots, b_{\varphi(m)}$ — *приведенная система вычетов по модулю* m. *Тогда совокупность* $ab_1, ab_2, \ldots, ab_{\varphi(m)}$ *тоже есть приведенная система вычетов по модулю* m.

Доказательство. Ввиду предложения 3.3 достаточно показать, что числа совокупности $ab_1, ab_2, \ldots, ab_{\varphi(m)}$

попарно несравнимы по модулю m. Действительно, если $ab_i \equiv ab_k \pmod m$ при $i \neq k$, то ввиду условия $(a, m) = 1$, $b_i \equiv b_k \pmod m$, что невозможно, так как, по условию предложения, b_i и b_k — различные элементы приведенной системы вычетов по модулю m. □

Мультипликативная группа классов вычетов, взаимно простых с модулем. Рассмотрим теорему, выражающую весьма важное свойство классов вычетов, взаимно простых с модулем.

ТЕОРЕМА 3.5. *Множество классов вычетов по модулю m, взаимно простых с модулем, образуют относительно умножения абелеву группу.*

Доказательство. Пусть G_m — множество всех классов вычетов по модулю m, взаимно простых с m. Произведение любых двух классов вычетов по модулю m, взаимно простых с модулем, является классом вычетов взаимно простых с модулем, и, значит, множество G_m замкнуто относительно умножения. Далее, операция умножения классов коммутативна и ассоциативна. Класс $\bar{1}$, $\bar{1} = 1 \bmod m$, является нейтральным элементом относительно умножения. Докажем, что для любого класса $\bar{a} \in G_m$ существует в G_m обратный класс. Пусть

$$G_m = \{\bar{a}_1, \ldots, \bar{a}_{\varphi(m)}\},$$

т. е. $a_1, a_2, \ldots, a_{\varphi(m)}$ — приведенная система вычетов по модулю m. Тогда $aa_1, aa_2, \ldots, aa_{\varphi(m)}$ согласно предложению 3.4 также есть приведенная система вычетов по модулю m; следовательно, она содержит число, сравнимое с 1. Пусть $aa_k \equiv 1 \pmod m$. Тогда $\bar{a}\bar{a}_k = \bar{1}$, следовательно, $\bar{a}_k$ есть класс, обратный классу $\bar{a}$ в G_m. Таким образом, система $\langle G_m, \cdot, {}^{-1}\rangle$ является абелевой группой. □

ОПРЕДЕЛЕНИЕ. Группа $\mathscr{G}_m = \langle G_m, \cdot, {}^{-1}\rangle$ называется *мультипликативной группой классов вычетов по модулю m,* взаимно простых с модулем.

СЛЕДСТВИЕ 3.6. *Если p — простое число, то множество ненулевых классов вычетов является абелевой группой относительно умножения.*

ТЕОРЕМА 3.7. *Кольцо классов вычетов по модулю m тогда и только тогда является полем, когда m есть простое число.*

Доказательство. Пусть m — простое число. Тогда согласно следствию 3.6 множество всех ненулевых классов вычетов по модулю m есть группа относительно

умножения. Поэтому кольцо классов вычетов по модулю m является полем.

Пусть m — составное число, $m=ab$, $1<a$, $b<m$. Тогда $(a \bmod m)(b \bmod m)=0 \bmod m$, причем согласно условию

$$a \bmod m \neq 0 \bmod m,\ b \bmod m \neq 0 \bmod m.$$

Таким образом, кольцо классов вычетов содержит делители нуля и поэтому не может быть полем.

Если $m=1$, то кольцо классов вычетов по модулю m является нулевым. Если же $m=0$, то кольцо классов вычетов по модулю m, $\mathbb{Z}/(0)$, изоморфно кольцу $\mathbb{Z}$ и поэтому не является полем. □

ОПРЕДЕЛЕНИЕ. Число a называется *обратным к числу* b по модулю m, если $ab \equiv 1 \pmod m$. Числа a и b будем также называть *взаимно обратными по модулю* m.

ПРЕДЛОЖЕНИЕ 3.8. *Пусть число a взаимно простое с модулем m и P_{n-1} — числитель предпоследней подходящей дроби для числа $\frac{m}{a}$ $\left(\frac{m}{a}=\frac{P_n}{Q_n}\right)$. Тогда $a(-1)^{n-1}P_{n-1} \equiv 1 \pmod m$, т. е. число $(-1)^{n-1}P_{n-1}$ является обратным к элементу a по модулю m.*

Доказательство. Пусть $\frac{P_{n-1}}{Q_{n-1}}$ и $\frac{P_n}{Q_n}$ — две последние подходящие дроби для числа m/a. Тогда $m=P_n$, $a=Q_n$ и, согласно следствию 11.3.5,

$$\frac{P_n}{Q_n}-\frac{P_{n-1}}{Q_{n-1}}=\frac{(-1)^n}{Q_{n-1}Q_n}.$$

Следовательно,

$$\frac{m}{a}-\frac{P_{n-1}}{Q_{n-1}}=\frac{(-1)^n}{Q_{n-1}Q_n},\ Q_{n-1}m-aP_{n-1}=(-1)^n \text{ и}$$
$$a(-1)^{n-1}P_{n-1} \equiv 1 \pmod m. \ \square$$

Пример. Найдем число, обратное числу 79 по модулю $m=273$.

Разложим число $\frac{273}{79}$ в цепную дробь, тогда

$$\frac{273}{79}=|3;\ 2,\ 5,\ 7|.$$

Вычислим числители подходящих дробей к числу $\frac{273}{79}$ по схеме

k		1	2	3	4
q_k		3	2	5	7
p_k	1	3	7	38	273

$P_3 = 38$ есть числитель предпоследней подходящей дроби для числа 273/79. Следовательно, число $(-1)^3 P_3 = -38$ является обратным к числу 79, т. е. $79 \cdot (-38) \equiv 1 \pmod{273}$.

Функция Эйлера. Число положительных целых чисел, не превосходящих n и взаимно простых с n, обозначается через $\varphi(n)$; числовая функция φ, определенная на множестве всех целых положительных чисел, называется *функцией Эйлера*. Легко видеть, что $\varphi(n)$ равна числу неотрицательных целых чисел, меньших n и взаимно простых с n.

Пример: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(6) = 2$, $\varphi(5) = 4$, $\varphi(12) = 4$.

Числовая функция f называется *мультипликативной*, если для любых положительных взаимно простых целых чисел a и b выполняется равенство $f(ab) = f(a) f(b)$.

ТЕОРЕМА 3.9. *Функция Эйлера* φ *мультипликативна.*

Доказательство. Пусть a и b — взаимно простые положительные целые числа. Рассмотрим множество M всех неотрицательных целых чисел, меньших ab. Согласно теореме о делении с остатком, каждое число из M может быть единственным образом представлено в виде $bq + r$, где $r \in \{0, 1, \ldots, b-1\}$, $q \in \{0, 1, \ldots, a-1\}$. Число $bq + r$ взаимно простое с a тогда и только тогда, когда $(b, r) = 1$. Существует $\varphi(b)$ таких r. Пусть r_1 — одно из этих чисел. Тогда согласно предложению 2.2 числа r_1, $b + r_1$, $2b + r_1$, $\ldots$, $b(a-1) + r_1$ образуют полную систему вычетов по модулю a. Поэтому среди этих чисел имеется точно $\varphi(a)$ чисел, взаимно простых с a. Таким образом, каждому числу r_1, взаимно простому с b, соответствует точно $\varphi(a)$ чисел вида $bq + r_1$, взаимно простых с a, и, значит, с ab. Поэтому число чисел из M, взаимно простых с ab, равно $\varphi(a)\varphi(b)$, т. е. $\varphi(ab) = \varphi(a)\varphi(b)$.

ТЕОРЕМА 3.10. *Если* $n=\prod_{p\mid n} p^{\alpha_p}$ *— каноническое разложение натурального числа* n, *то*

$$(1)\quad \varphi(n)=n\prod_{p\mid n}\left(1-\frac{1}{p}\right).$$

Доказательство. Так как функция φ мультипликативна, то для вычисления $\varphi(n)$ достаточно уметь вычислять эту функцию для степени простого числа p. Число целых неотрицательных чисел, меньших p^{α} и не взаимно простых с p^{α}, равно $p^{\alpha-1}$, так как только числа kp, $0\leqslant k<p^{\alpha-1}$, не взаимно простые с p^{α}. Поэтому число чисел, меньших p^{α} и взаимно простых с p^{α}, равно $p^{\alpha}-p^{\alpha-1}$, т. е.

$$(2)\quad \varphi(p^{\alpha})=p^{\alpha}\left(1-\frac{1}{p}\right).$$

Так как $n=\prod_{p\mid n} p^{\alpha_p}$ и функция φ мультипликативна, то

$$(3)\quad \varphi(n)=\prod_{p\mid n}\varphi(p^{\alpha_p}).$$

Из (2) и (3) следует, что

$$\varphi(n)=\prod_{p\mid n} p^{\alpha_p}\left(1-\frac{1}{p}\right)=\prod_{p\mid n} p^{\alpha_p}\prod_{p\mid n}\left(1-\frac{1}{p}\right)=$$
$$=n\prod_{p\mid n}\left(1-\frac{1}{p}\right),$$

значит, верна формула (1). □

Пример: $\varphi(30)=30\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=$
$$=30\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}=8.$$

ТЕОРЕМА 3.11. *Сумма чисел* $\varphi(d)$ *по всем натуральным делителям* d *числа* n *равна* n, *т. е.* $\sum_{d\mid n}\varphi(d)=n$.

Доказательство. Если $n=\prod_i p_i^{\alpha_i}$ — каноническое разложение n, то

$$\sum_{d\mid n}\varphi(d)=\prod_i\left(1+\varphi(p_i)+\varphi(p_i^2)+\ldots+\varphi\left(p_i^{\alpha_i}\right)\right),$$

так как при раскрытии скобок получим сумму всех значений $\varphi(d)$. Далее,

$$\sum_{d \mid n} \varphi(d) = \prod_i \left(1 + (p_i - 1) + (p_i^2 - p_i) + \ldots + \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)\right) =$$

$$= \prod_i p_i^{\alpha_i} = n, \quad \text{т. е.} \quad \sum_{d \mid n} \varphi(d) = n.$$

Теоремы Эйлера и Ферма. В теории сравнений важную роль играет теорема Эйлера.

ТЕОРЕМА ЭЙЛЕРА. *Если целое число a взаимно простое с m, то*

(1) $a^{\varphi(m)} \equiv 1 \pmod m$.

Доказательство. Пусть

(2) $a_1, a_2, \ldots, a_{\varphi(m)}$

есть приведенная система вычетов по модулю m. Тогда согласно предложению 3.4

(3) $aa_1, aa_2, \ldots, aa_{\varphi(m)}$

также есть приведенная система вычетов по модулю m. Поэтому произведение чисел (3) сравнимо с произведением чисел (2), т. е.

(4) $a^{\varphi(m)} a_1 a_2 \ldots a_{\varphi(m)} \equiv a_1 a_2 \ldots a_{\varphi(m)} \pmod m$.

Произведение $a_1 a_2 \ldots a_{\varphi(m)}$ взаимно простое с m. Поэтому согласно свойству 1.6 обе части сравнения (4) можно разделить на это произведение, тогда $a^{\varphi(m)} \equiv 1 \pmod m$. □

ТЕОРЕМА ФЕРМА. *Если целое число a не делится на простое число p, то $a^{p-1} \equiv 1 \pmod p$.*

Эта теорема есть частный случай предыдущей теоремы при $m = p$. Теорема Ферма часто формулируется иначе.

ВТОРАЯ ФОРМУЛИРОВКА ТЕОРЕМЫ ФЕРМА. *Если p — простое и a — любое целое число, то $a^p \equiv a \pmod p$.*

Упражнения

1. Исходя из равенства $a^p = (1 + 1 + \ldots + 1)^p$, докажите, что для любого натурального a и простого p выполняется сравнение $a^p \equiv a \pmod p$.

2. Докажите, что число положительных приведенных дробей, имеющих знаменателями одно из чисел 1, 2, ..., n и не превосходящих единицы, равно $\varphi(1) + \varphi(2) + \ldots + \varphi(n)$.

3. Докажите, что при $n > 1$ сумма приведенных вычетов m по модулю n, находящихся в пределах $1 \leqslant m < n$, равна $\frac{1}{2} n\varphi(n)$.

4. Покажите на примерах, что сравнение $a^m \equiv a \pmod m$, где m — простое, может не выполняться при составном m.

5. Докажите, что если $a^{n-1} \equiv 1 \pmod n$ и $a^d \not\equiv 1$ для всякого положительного делителя d числа $(n-1)$, то n — простое число.

6. Сколько имеется натуральных чисел, меньших числа 234 000 000 и взаимно простых с ним?

§ 4. СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ. СРАВНЕНИЯ ВЫСШИХ СТЕПЕНЕЙ ПО ПРОСТОМУ МОДУЛЮ

Степень и число решений сравнения. Сравнение вида

$$(1)\quad a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \pmod m,$$

где $a_1, \ldots, a_n$ — целые числа, называется *алгебраическим сравнением*. Число n называется *степенью сравнения* (1), если a_n не делится на m.

Если число a удовлетворяет сравнению (1), то любое число b, сравнимое с a по модулю m, также удовлетворяет сравнению (1); два таких решения рассматриваются как одинаковые.

ОПРЕДЕЛЕНИЕ. *Числом решений сравнения по модулю m* называется число решений этого сравнения в какой-либо полной системе вычетов по модулю m.

Примеры. 1. Сравнению $3x^2 - 7 \equiv 0 \pmod 4$ среди чисел 0, 1, 2, 3 полной системы вычетов по модулю 4 удовлетворяют два числа: $x = 1$ и $x = 3$. Поэтому сравнение имеет два решения: $x \equiv 1 \pmod 4$ и $x \equiv 3 \pmod 4$.

2. Сравнению $x^2 \equiv 1 \pmod 8$ среди чисел 0, 1, 2, 3, 4, 5, 6, 7 полной системы вычетов по модулю 8 удовлетворяют четыре числа: 1, 3, 5, 7. Поэтому сравнение имеет четыре решения:

$$x \equiv 1 \pmod 8,\ x \equiv 3 \pmod 8,\ x \equiv 5 \pmod 8,\ x \equiv 7 \pmod 8.$$

Сравнения первой степени. Найдем условия разрешимости сравнения первой степени.

ТЕОРЕМА 4.1. *Если $(a, m) = 1$, то сравнение*

$$(1)\quad ax \equiv b \pmod m$$

имеет одно и только одно решение.

Доказательство. По условию, число a — взаимно простое с m. Согласно теореме 3.5, существует целое

число a', обратное к a по модулю m, т. е. $a'a \equiv 1 \pmod m$. Умножив обе части (1) на a', получим

(2) $x \equiv a'b \pmod m$.

Следовательно, сравнение (1) имеет не больше одного решения. С другой стороны, (2) есть решение сравнения (1), так как

$$a(a'b) \equiv (aa')\,b \equiv b \pmod m.$$

Таким образом, класс вычетов $a'b \bmod m$ является единственным решением сравнения (1). □

ТЕОРЕМА 4.2. *Пусть* $(a, m) = d$. *Сравнение*

(1) $ax \equiv b \pmod m$

разрешимо тогда и только тогда, когда $d \mid b$. *Если* $d \mid b$, *то сравнение* (1) *имеет своими решениями точно* d *классов вычетов по модулю* m, *которые составляют один класс вычетов по модулю* m/d.

Доказательство. Пусть $(a, m) = d > 1$. Если сравнение (1) имеет решение x_1, то $ax_1 - b = km$, где k — целое число. Так как $(a, m) = d$, то отсюда следует, что d делит b.

Предположим теперь, что b делится на d, и докажем, что сравнение (1) имеет d решений. Пусть $b = b_1 d$, $a = a_1 d$ и $m = m_1 d$. Сравнение (1) равносильно сравнению

(2) $a_1 x \equiv b_1 \pmod{m_1}$.

Согласно теореме 4.1, сравнение (2) имеет единственное решение $a_1' b_1 \bmod m_1$, где a_1' — число, обратное a_1 по модулю m_1. Пусть $x_0 = a_1' b_1$. Класс вычетов $x_0 \bmod m_1$ распадается на следующие d классов вычетов по модулю m:

(3) $x_0 \bmod m$, $(x_0 + m_1) \bmod m$, $(x_0 + 2m_1) \bmod m$, …, $(x_0 + (d-1)\,m_1) \bmod m$.

Легко видеть, что классы вычетов (3) являются различными по модулю m. Таким образом, сравнение (2) имеет своими решениями классы вычетов (3), т. е. точно d классов вычетов по модулю m, которые составляют один класс вычетов по модулю m/d. □

Отметим, что совокупность решений (3) сравнения (1) есть смежный класс аддитивной группы $\mathfrak{G}$ классов вычетов по модулю m по подгруппе $\frac{m}{d} \cdot \mathfrak{G}$. Обратно: любой смеж-

ный класс группы $\mathfrak{H}$ по подгруппе $\frac{m}{d}\cdot\mathfrak{H}$ можно задать как множество решений некоторого линейного сравнения по модулю m.

Сравнения высших степеней по простому модулю. Перейдем к рассмотрению вопроса о числе решений сравнения n-й степени по простому модулю.

ТЕОРЕМА 4.3. *Сравнение*

(1) $a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \pmod{p}$

степени n по простому модулю p имеет не более n решений.

Доказательство проводится индукцией по n. Если $n = 0$, то сравнение имеет вид $a_0 \equiv 0 \pmod{p}$, где $p \nmid a_0$; в этом случае сравнение имеет нуль решений. Предположим, что сравнение (1) имеет степень $n > 0$. Если сравнение имеет решения, то для некоторого целого числа x_1

(2) $a_n x_1^n + \ldots + a_1 x_1 + a_0 \equiv 0 \pmod{p}$.

Вычтем это сравнение из (1). Тогда разность членов степени k имеет вид

$$a_k\left(x^k - x_1^k\right) = a_k (x - x_1)\left(x^{k-1} + x_1 x^{k-2} + \ldots + x_1^{k-1}\right)$$

при $k = 1, \ldots, n$; каждая разность содержит линейный множитель $(x - x_1)$. Поэтому результат вычитания можно записать так:

(3) $(x - x_1)(b_{n-1} x^{n-1} + \ldots + b_0) \equiv 0 \pmod{p}$,

где $b_0, \ldots, b_{n-1}$ — некоторые целые числа, $b_{n-1} = a_n$. Любое другое решение сравнения (1), скажем x_2, будет решением сравнения

(4) $b_{n-1} x^{n-1} + \ldots + b_0 \equiv 0 \pmod{p}$.

Действительно, так как $x_2 \not\equiv x_1 \pmod{p}$ и модуль p простой, то из сравнения

$$(x_2 - x_1)(b_{n-1} x_2^{n-1} + \ldots + b_0) \equiv 0 \pmod{p}$$

следует, что

$$b_{n-1} x_2^{n-1} + \ldots + b_0 \equiv \pmod{p}.$$

Так как степень сравнения (4) равна $n - 1$, то, по индуктивному предположению, сравнение (4) имеет не более $n - 1$ решений. Следовательно, исходное сравнение (1) имеет не более n решений. □

СЛЕДСТВИЕ 4.4. *Если сравнение* $a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \pmod p$ *имеет более* n *решений, то все его коэффициенты делятся на* p.

ПРЕДЛОЖЕНИЕ 4.5. *Если* p *— простое число, то сравнение* $x^{p-1} - 1 \equiv 0 \pmod p$ *имеет точно* $p-1$ *решений.*

Это предложение непосредственно следует из теоремы Ферма, а сравнению удовлетворяют любые числа, не делящиеся на p; решениями являются числа $1, 2, \ldots, p-1$.

ТЕОРЕМА ВИЛЬСОНА. *Если* p *— простое число, то*

(1) $(p-1)! + 1 \equiv 0 \pmod p$.

Доказательство. Если $p = 2$, то теорема, очевидно, верна. Пусть $p > 2$. Рассмотрим сравнение

(2) $(x-1)(x-2)\ldots(x-(p-1)) - (x^{p-1} - 1) \equiv 0 \pmod p$.

Его степень меньше $p-1$ и в то же время это сравнение имеет $p-1$ решений: $1, 2, \ldots, p-1$. Поэтому согласно следствию 4.4 все коэффициенты сравнения (2) делятся на p. В частности, последний коэффициент, равный $(p-1)! + 1$, делится на p. □

ТЕОРЕМА 4.6. *Если* p *— простое число и* d *— натуральный делитель числа* $p-1$, *то сравнение*

(1) $x^d - 1 \equiv 0 \pmod p$

имеет точно d *решений.*

Доказательство. Пусть d — любой делитель $p-1$, $p-1 = kd$. Тогда сравнение

(2) $x^{p-1} - 1 \equiv 0 \pmod p$

можно записать в виде

(3) $(x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \ldots + x^d + 1) \equiv 0 \pmod p$.

Согласно предложению 4.5, сравнение (2) имеет $p-1$ решений: $1, 2, \ldots, p-1$. Каждое решение сравнения (2) должно удовлетворять одному из сравнений:

(1) $x^d - 1 \equiv 0 \pmod p$,

(4) $x^{d(k-1)} + \ldots + x^d + 1 \equiv 0 \pmod p$.

По теореме 4.3 сравнение (4) имеет не более $d(k-1) = p - 1 - d$ решений. Поэтому сравнение (1) должно иметь не менее d решений. Следовательно, ввиду предложения 4.5 сравнение (3) имеет точно d решений. □

Упражнения

1. Докажите, что если натуральное число $m > 1$, то сравнение $1 \cdot 2 \cdot 3 \ldots (m-1) \equiv -1 \pmod{m}$ выполняется тогда и только тогда, когда m — простое число.

2. Найдите решения сравнения $ax \equiv 1 \pmod{7}$ при $a = 2, 3, 4, 5, 6$.

3. Найдите число, кратное семи и дающее остаток 1 от деления на 2, 3, 4, 5, 6.

4. Докажите, что сравнению $x^2 + 1 \equiv 0 \pmod{p}$, где $p = 4n + 1$ — простое число, удовлетворяет число $(2n)!$

5. Решите сравнения:

$x^2 \equiv -1 \pmod{65}$; $x^2 \equiv -2 \pmod{33}$.

§ 5. ПЕРВООБРАЗНЫЕ КОРНИ И ИНДЕКСЫ

Порядок числа и класса вычетов по модулю. Пусть a — число, взаимно простое с m. *Порядком числа a по модулю m* называется наименьшее целое положительное число d такое, что $a^d \equiv 1 \pmod{m}$. Если $b \equiv a \pmod{m}$, то b имеет тот же порядок по модулю m, что и a. Таким образом, все элементы класса вычетов $a \bmod m$ имеют порядок d; число d называется *порядком класса вычетов* $a \bmod m$ и обозначается через $\mathcal{O}(a \bmod m)$.

ПРЕДЛОЖЕНИЕ 5.1. *Если $\mathcal{O}(a \bmod m) = d$, то числа a, a^2, ..., a^d попарно несравнимы по модулю m.*

Доказательство. Если $a^s \equiv a^k \pmod{m}$, где $k < s$, k, $s \in \{1, 2, \ldots, d\}$, то $a^{s-k} \equiv 1 \pmod{m}$, что противоречит условию, так как $0 < s - k < d$. □

ПРЕДЛОЖЕНИЕ 5.2. *Пусть $\mathcal{O}(a \bmod m) = d$ и n — любое целое неотрицательное число. Сравнение $a^n \equiv 1 \pmod{m}$ выполняется тогда и только тогда, когда n делится на d.*

Доказательство. Сначала покажем, что из $a^n \equiv 1 \pmod{m}$ следует, что n делится на d. По теореме о делении с остатком, для n и d существуют натуральные числа q и r такие, что

(1) $n = dq + r$, $0 \leqslant r < d$.

Покажем, что $r = 0$. Ввиду (1) и условия $a^d \equiv 1 \pmod{m}$

$$a^n \equiv a^{dq} a^r \equiv (a^d)^q a^r \equiv a^r \equiv 1 \pmod{m}.$$

Так как, по условию, $a^r \not\equiv 1 \pmod{m}$, если $0 < r < d$, то сравнение $a^r \equiv 1 \pmod{m}$ возможно лишь при $r = 0$. Следовательно, n делится на d. Теперь предположим, что n делится на d, $n = dk$ для некоторого k. Тогда

$$a^n \equiv a^{dk} \equiv (a^d)^k \equiv 1 \pmod{m}, \text{ т. е. } a^n \equiv 1 \pmod{m}. \square$$

ПРЕДЛОЖЕНИЕ 5.3. *Если* $\mathcal{O}(a \bmod m) = d$, *то* $\varphi(m)$ *делится на* d.

Доказательство. В силу предложения 5.2 из $a^{\varphi(m)} \equiv 1 \pmod m$ и условия $\mathcal{O}(a \bmod m) = d$ следует, что $\varphi(m)$ делится на d. □

ПРЕДЛОЖЕНИЕ 5.4. *Пусть* $\mathcal{O}(a \bmod m) = d$. *Сравнение* $a^s \equiv a^k \pmod m$ *имеет место тогда и только тогда, когда* $k \equiv s \pmod d$.

Доказательство. Если

(1) $a^k \equiv a^s \pmod m$, $k \geqslant s$,

то

(2) $a^{k-s} \equiv 1 \pmod m$

и поэтому в силу предложения 5.2 $k - s$ делится на d, т. е.

(3) $k \equiv s \pmod d$.

Обратно: из (3) следует (2) и (1). □

ПРЕДЛОЖЕНИЕ 5.5. *Пусть* a, b — *числа, взаимно простые с* m. *Если числа* $\mathcal{O}(a \bmod m)$ *и* $\mathcal{O}(b \bmod m)$ *взаимно простые, то*

$$\mathcal{O}(ab \bmod m) = \mathcal{O}(a \bmod m) \cdot \mathcal{O}(b \bmod m).$$

Доказательство. Пусть $\mathcal{O}(a) = d$, $\mathcal{O}(b) = e$ и $\mathcal{O}(ab) = f$. Докажем, что f делится на de. Так как $b^e \equiv 1 \pmod m$, то $a^e \equiv a^e b^e \equiv (ab)^e \pmod m$ и $a^{ef} \equiv (ab)^{ef} \equiv ((ab)^f)^e \equiv 1 \pmod m$. Из $a^{ef} \equiv 1 \pmod m$ в силу предложения 5.2 следует, что ef делится на d. Так как, по условию, $(d, e) = 1$, то f делится на d. Также находим, что f делится на e. Следовательно, f делится на de.

С другой стороны, $(ab)^{de} \equiv (a^d)^e (b^e)^d \equiv 1 \pmod m$. Согласно предложению 5.2, отсюда следует, что de делится на f. Следовательно, $f = de$. □

ПРЕДЛОЖЕНИЕ 5.6. *Если* $\mathcal{O}(a \bmod m) = n$ *и* d — *натуральный делитель числа* n, *то* $\mathcal{O}(a^d \bmod m) = n/d$.

Доказательство. Пусть $\mathcal{O}(a^d \bmod m) = f$. По условию, $a^n \equiv (a^d)^{n/d} \equiv 1 \pmod m$. Согласно предложению 5.2, отсюда следует, что n/d делится на f, т. е. $n/d = kf$, $n = kfd$ для некоторого натурального числа k. Следовательно, $a^{fd} \equiv (a^d)^f \equiv 1 \pmod m$. Отсюда следует, что fd делится на n. Поэтому $k = 1$, $n = fd$ и $f = n/d$. □

ПРЕДЛОЖЕНИЕ 5.7. *Если* $\mathcal{O}(a \bmod m) = n$ *и* $(k, n) = d$, *то* $\mathcal{O}(a^k \bmod m) = n/d$.

Доказательство. Пусть $\mathcal{O}(a^k \bmod m) = f$, $k = k_1 d$, $n = n_1 d$. Из условия следует, что

$$(a^k)^{n/d} \equiv (a^n)^{k/d} \equiv 1 \pmod{m}.$$

Следовательно, число $n/d = n_1$ делится на f. С другой стороны, $(a^k)^f \equiv a^{kf} \equiv 1 \pmod{m}$. Согласно предложению 5.2, отсюда следует, что kf делится на n. Поэтому $k_1 f$ делится на n_1. Так как $(k_1, n_1) = 1$, то f делится на n_1; следовательно, $f = n_1 = n/d$. □

ПРЕДЛОЖЕНИЕ 5.8. *Если* $\mathcal{O}(a \bmod m) = n$ *и* $(k, n) = 1$, *то* $\mathcal{O}(a^k \bmod m) = n$.

Это предложение непосредственно следует из предыдущего.

Первообразные корни по простому модулю. Для описания мультипликативной группы вычетов по простому модулю необходимо изучить числа, имеющие наибольший порядок по этому модулю.

ТЕОРЕМА 5.9. *Пусть* p — *простое число и* d — *натуральный делитель числа* $p - 1$. *В приведенной системе вычетов по модулю* p *существует точно* $\varphi(d)$ *чисел, имеющих порядок* d.

Доказательство. Пусть B — приведенная система вычетов по модулю p. Пусть d — некоторый натуральный делитель числа $p - 1$. Обозначим через $\psi(d)$ число элементов из B, порядок которых равен d. Допустим, что существует хотя бы один элемент $a \in B$, имеющий порядок p, т. е. $\psi(d) > 0$. Тогда a, a^2, ..., a^d — различные по модулю p решения сравнения

$$(1)\quad x^d \equiv 1 \pmod{p}$$

и, согласно теореме 4.6, других решений нет. Поэтому все вычеты порядка d должны принадлежать множеству

$$M = \{a, a^2, \ldots, a^d\}.$$

Согласно предложениям 5.7 и 5.8, число a^k имеет порядок d тогда и только тогда, когда $(d, k) = 1$. Отсюда следует, что $\psi(d) = \varphi(d)$, если существует хотя бы один элемент порядка d. Таким образом,

(2) $\psi(d) \leqslant \varphi(d)$ для любого делителя d числа $(p - 1)$.

Так как каждый вычет имеет некоторый порядок d, являющийся делителем $p - 1$, то

$$\sum_{d \mid (p-1)} \psi(d) = p - 1.$$

С другой стороны, согласно теореме 3.11,

$$\sum_{d \mid (p-1)} \varphi(d) = p - 1,$$

поэтому

$$(3) \quad \sum_{d \mid (p-1)} (\varphi(d) - \psi(d)) = 0.$$

На основании (2) и (3) заключаем, что $\psi(d) = \varphi(d)$ для любого натурального делителя d числа $p-1$. □

Если вычет a по модулю m имеет порядок $\varphi(m)$, то a называется *первообразным корнем по модулю* m.

ТЕОРЕМА 5.10. *Группа вычетов по модулю p, взаимно простых с модулем, циклична. Число первообразных корней по модулю p равно* $\varphi(p-1)$.

Эта теорема непосредственно следует из предыдущей теоремы, согласно которой существует $\varphi(p-1)$ образующих группы вычетов, взаимно простых с p.

Если g есть первообразный корень по модулю p, то $p-1$ степеней

$$(1) \quad g, \ g^2, \ \ldots, \ g^{p-1}$$

несравнимы по модулю p. Следовательно, верно следующее предложение.

ПРЕДЛОЖЕНИЕ 5.11. *Если g есть первообразный корень по модулю p, то* $p-1$ *степеней* $g, \ g^2, \ \ldots, \ g^{p-1}$ *представляют собой приведенную систему вычетов по модулю p.*

Первообразные корни существуют не для всякого модуля m, а лишь для $m = 2, \ 4, \ p^k, \ 2p^k$ (p — нечетное простое число).

Пример. Пусть $p = 13$. Найдем первообразные корни по этому модулю.

Число $p - 1 = 12$ имеет 6 натуральных делителей: 1, 2, 3, 4, 6, 12;

$$\varphi(1) = 1, \ \varphi(2) = 1, \ \varphi(3) = 2, \ \varphi(4) = 2, \ \varphi(6) = 2, \ \varphi(12) = 4.$$

Числа 2, 6, 7, 11 являются первообразными корнями по модулю 13. Число 12 имеет порядок 2; число 3 — порядок 3; числа 5,8 — порядок 4; числа 4,10 — порядок 6, число 1 — порядок 1.

Индексы по простому модулю. Пусть g есть первообразный корень по модулю p. Тогда числа

$$(1) \quad g, \ g^2, \ \ldots, \ g^{p-1}$$

образуют приведенную систему вычетов по модулю p. Поэтому любое число a, взаимно простое с p, сравнимо с одним и только с одним из чисел ряда (1).

Если $a \equiv g^k \pmod p$, то k называется *индексом числа a по модулю p* при основании g и обозначается символом $\operatorname{ind} a$ или $\operatorname{ind}_g a$. Если k' — другое число, для которого $a \equiv g^{k'} \pmod p$, то $g^k \equiv g^{k'} \pmod p$ и, согласно предложению 5.4, $k \equiv k' \pmod{(p-1)}$. Таким образом, множество индексов данного числа a образуют класс вычетов по модулю $p-1$. Из определения индекса вытекает, что из $a \equiv b \pmod p$ следует $\operatorname{ind} a \equiv \operatorname{ind} b \pmod{p-1}$.

Пример. Пусть $p = 13$. Число 2 есть первообразный корень по модулю 13. Индексы чисел 1, 2, ..., 12 при основании $g = 2$ таковы:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind} a$	0	1	4	2	9	5	11	3	8	10	7	6

С помощью этой таблицы по данному числу a находится его индекс по модулю 13. Следующая таблица позволяет по данному индексу находить соответствующее число:

$\operatorname{ind} a$	0	1	2	3	4	5	6	7	8	9	10	11
a	1	2	4	8	3	6	12	11	9	5	10	7

С помощью индексов умножение по модулю p можно свести к сложению по модулю $p-1$ аналогично тому, как, используя логарифмы, можно свести обычное умножение чисел к сложению.

ТЕОРЕМА 5.12. *Если числа a, b взаимно простые с p и n — любое натуральное число, то*

$$(1)\quad \begin{aligned} &\operatorname{ind} ab \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{p-1},\\ &\operatorname{ind} a^n \equiv n \operatorname{ind} a \pmod{p-1}. \end{aligned}$$

Доказательство. По определению индексов чисел a и b имеем:

$$a \equiv g^{\operatorname{ind} a} \pmod p,\quad b \equiv g^{\operatorname{ind} b} \pmod p,$$

отсюда находим произведение

$$ab \equiv g^{\operatorname{ind} a + \operatorname{ind} b} \pmod p.$$

Следовательно, $\operatorname{ind} a + \operatorname{ind} b$ есть один из индексов произведения ab, т. е.

$$\operatorname{ind} ab \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{p-1}.$$

Из сравнения $a \equiv g^{\operatorname{ind} a} \pmod p$ следует, что

$$a^n \equiv g^{n \operatorname{ind} a} \pmod p;$$

поэтому $n \operatorname{ind} a$ есть один из индексов степени a^n, т. е.

$$\operatorname{ind} a^n \equiv n \operatorname{ind} a \pmod{p-1}. \quad \square$$

Примеры. 1. Пусть $p = 13$, $a = 8$, $b = 6$; тогда $\operatorname{ind} 8 = 9$, $\operatorname{ind} 6 = 8$, $\operatorname{ind} 8 \cdot 6 \equiv 9 + 8 \equiv 5 \pmod{12}$.

2. Решить сравнение $6x \equiv 7 \pmod{13}$.

Данное сравнение равносильно такому:

$$\operatorname{ind} 6 + \operatorname{ind} x = \operatorname{ind} 7 \pmod{12}, \text{ или } \operatorname{ind} x \equiv$$
$$\equiv \operatorname{ind} 7 - \operatorname{ind} 6 = 11 - 5 = 6 \pmod{12}.$$

Отсюда следует, что $x \equiv 12 \pmod{13}$.

ТЕОРЕМА 5.12. *Пусть $\mathfrak{S}_p$ — мультипликативная группа классов вычетов, взаимно простых с p, и C есть аддитивная группа классов вычетов по модулю $p-1$. Отображение $a \bmod p \longmapsto \operatorname{ind} a \pmod{p-1}$, ставящее в соответствие каждому элементу a группы $\mathfrak{S}_p$ элемент $\operatorname{ind} a$ группы C, есть изоформизм группы $\mathfrak{S}_p$ на группу C.*

Доказательство. Согласно определению индекса, соответствие $a \bmod p \overset{\varphi}{\longmapsto} \operatorname{ind} a \pmod{p-1}$ является биективным. Кроме того, сохраняется операция умножения в группе $\mathfrak{S}_p$, так как из сравнения

$$\operatorname{ind} ab = \operatorname{ind} a + \operatorname{ind} b \pmod{p-1}$$

следует, что

$$[\operatorname{ind} ab] = [\operatorname{ind} a] + [\operatorname{ind} p].$$

Следовательно, φ есть изоморфизм группы $\mathfrak{S}_p$ на группу C. $\square$

В обычной арифметике основой теории логарифмов является изоморфизм мультипликативной группы положительных действительных чисел и аддитивной группы всех действительных чисел. Доказанная теорема, являющаяся основной в теории индексов, объясняет причину сходства теории логарифмов (в обычной арифметике) и теории индексов (по простому модулю).

Двучленные сравнения. *Двучленным сравнением* называется сравнение вида

(1) $ax^n \equiv b \pmod p$,

где степень n положительна. Если p — простое число, то сравнение (1) равносильно сравнению

(2) $n\xi \equiv \operatorname{ind} b - \operatorname{ind} a \pmod{p-1}$, где $\xi = \operatorname{ind} x$.

Для того чтобы сравнение (2) было разрешимо, необходимо и достаточно, чтобы число $d=(n,\ p-1)$ делило разность $\operatorname{ind} b-\operatorname{ind} a$. Если это условие выполнено, то сравнение (2) имеет d решений по модулю $p-1$; следовательно, сравнение (1) имеет точно d решений по модулю p.

Пример. Решим сравнение

(3) $6x^8\equiv 5 \pmod{13}$.

Сравнение (2) в этом случае имеет вид

$8\xi\equiv \operatorname{ind} 5-\operatorname{ind} 6 \pmod{12}$, или $8\xi\equiv 4 \pmod{12}$.

Последнее сравнение совместно, так как (8,12) делит 4, и имеет следующие четыре решения:

$\xi\equiv 2,\ 5,\ 8,\ 11 \pmod{12}$; $\operatorname{ind} x\equiv 2,\ 5,\ 8,\ 11 \pmod{12}$.

Поэтому сравнение (3) имеет четыре решения:

$x\equiv 4,\ 6,\ 9,\ 7 \pmod{13}$.

Двучленное сравнение (1) можно свести к более простому, умножив обе части сравнения на число a', обратное к a по модулю p, $a'a\equiv 1 \pmod{p}$. Умножив, получим $x^n\equiv a'b \pmod{p}$. Таким образом, любое двучленное сравнение можно привести к простейшему виду:

$x^m\equiv c \pmod{p}$.

ОПРЕДЕЛЕНИЕ. Число a называется *k-степенным вычетом по модулю m*, если сравнение $x^k\equiv a \pmod{m}$ имеет хотя бы одно решение.

Пусть p — простое число и $\bar{k}=(k,\ p-1)$.

ТЕОРЕМА 5.13. *Для любого вычета a по простому модулю p равносильны следующие утверждения*:

(α) *a есть k-степенной вычет по модулю p*;

(β) $a^{\frac{p-1}{\bar{k}}}\equiv 1 \pmod{p}$,

(γ) *порядок класса вычетов $a \bmod p$ есть делитель числа* $\frac{p-1}{\bar{k}}$, т. е. $\mathcal{O}(a \bmod p) \mid ((p-1)/\bar{k})$;

(δ) $\operatorname{ind} a$ *кратен* $\bar{k}$.

Доказательство. (α)$\rightarrow$(β). Пусть a есть k-степенной вычет; тогда существует вычет x_0, взаимно простой

с p, удовлетворяющий сравнению $x_0^k \equiv a \pmod p$. Следовательно,

$$a^{\frac{p-1}{\bar k}} \equiv \left(x_0^{\frac{k}{\bar k}}\right)^{\frac{p-1}{\bar k}} \equiv \left(x_0^{k/\bar k}\right)^{p-1} \equiv 1 \pmod p,$$

т. е. выполняется (β);

(β) $\to$ (γ). Согласно предложению 5.2, из сравнения (β) следует (γ);

(γ) $\to$ (δ). Из условия (γ) следует, что

(1) $a^{\frac{p-1}{\bar k}} \equiv 1 \pmod p$.

Пусть g есть первообразный корень по модулю p. Тогда $a = g^{\operatorname{ind} a}$ и в силу (1)

$$\left(g^{\operatorname{ind} a}\right)^{\frac{p-1}{\bar k}} \equiv g^{\operatorname{ind} a \cdot \frac{p-1}{\bar k}} \equiv 1 \pmod p.$$

Поэтому согласно предложению 5.2

$$\operatorname{ind} a \cdot \frac{p-1}{\bar k} \equiv 0 \pmod{p-1};$$

следовательно, $\bar k \mid \operatorname{ind} a$, т. е. выполняется ($\delta$).

(δ) $\to$ (α). Рассмотрим сравнение

$$k\xi \equiv \operatorname{ind} a \pmod{p-1}.$$

Так как $\bar k = (k, p-1) \mid \operatorname{ind} a$, то это сравнение имеет решение. Пусть ξ_0 — решение этого сравнения, $k\xi_0 \equiv \operatorname{ind} a \pmod{p-1}$. Тогда $g^{k\xi_0} \equiv g^{\operatorname{ind} a} \pmod p$, следовательно, $(g^{\xi_0})^k \equiv a \pmod p$, т. е. a есть k-степенной вычет по модулю p. Таким образом, (δ) $\to$ (α). □

Упражнения

1. Составьте таблицу индексов по модулю 19 с основанием 2.

2. Составьте таблицу индексов по модулю 29 с основанием 10.

3. Найдите первообразные корни чисел 41 и 49.

4. Пусть p — нечетное простое число и $n > 1$. Покажите, что существует ровно $(p-1)\cdot\varphi(p-1)$ различных первообразных корней числа p^n, несравнимых по модулю p^2.

5. Если p — простое нечетное число, $n > 1$, то существует ровно $\varphi(\varphi(p^n))$ различных первообразных корней числа p^n.

6. Покажите, что если p — нечетное простое число и $n > 1$, то существует ровно $\varphi(\varphi(p^n))$ различных первообразных корней числа $2p^n$.

7. Найдите индекс числа (-1) по нечетному простому модулю p при произвольном основании.

8. Покажите, что для простого числа вида 2^n+1 при $n>3$ число 3 является первообразным корнем.

9. Покажите, что если p — простое число вида $4k+1$ и g — первообразный корень по модулю p, то $p-g$ есть также первообразный корень по модулю p.

§ 6. ОБРАЩЕНИЕ ОБЫКНОВЕННОЙ ДРОБИ В СИСТЕМАТИЧЕСКУЮ И ОПРЕДЕЛЕНИЕ ДЛИНЫ ПЕРИОДА СИСТЕМАТИЧЕСКОЙ ДРОБИ

Периодическую m-ичную дробь

$$m^h\left(b_1m^{l-1}+\ldots+b_l+\frac{a_1}{m}+\ldots+\frac{a_k}{m^k}+\frac{a_1}{m^{k+1}}+\ldots+\frac{a_k}{m^{2k}}+\ldots\right)$$

кратко записывают в виде

$$(*)\quad m^h(b_1\ldots b_l,\ \overline{a_1\ldots a_k}).$$

При этом $a_1\ldots a_k$ называется *периодом дроби*, а $b_1\ldots b_l$ — *предпериодом дроби*. Число k называется *длиной периода*, число l — *длиной предпериода*.

Периодическая m-ичная дробь $(*)$ называется *нормированной*, если выполнены условия:

(α) $a_k\neq b_l$;

(β) период $a_1\ldots a_k$ имеет наименьшую возможную длину.

Если нормированная периодическая m-ичная дробь $(*)$ представляет число a, т. е. $a=m^h(b_1\ldots b_l,\ \overline{a_1\ldots a_k})$, то говорят, что дробь $m^h(b_1\ldots b_l,\ a_1\ldots a_k)$ есть *нормированное разложение числа a в периодическую m-ичную дробь*.

ПРЕДЛОЖЕНИЕ 6.1. *Пусть m — фиксированное натуральное, большее единицы число. Для любого заданного положительного рационального числа a существуют целое число h и натуральные числа c, n такие, что*

$$(\mathrm{I})\quad a=m^h\frac{c}{n},\ (m,\ n)=1,\ m\nmid c,\ (c,\ n)=1.$$

При этом если целое число h_1 и натуральные числа c_1, n_1 удовлетворяют условиям

$$(\mathrm{I}')\quad a=m^{h_1}\frac{c_1}{n_1},\ \ (m,\ n_1)=1,\ \ m\nmid c_1,\ \ (c_1,\ n_1)=1,$$

то $h=h_1$, $c=c_1$ и $n=n_1$.

Доказательство. Представим рациональное число a в виде несократимой дроби $a=u/v$, $(u, v)=1$, $u, v\in\mathbf{N}$. Обозначим через n наибольший натуральный делитель знаменателя v, взаимно простой с m, $v=qn$. Тогда каждый простой делитель числа q делит m; поэтому существуют целые числа t такие, что $\frac{m^t}{q}\in\mathbf{N}$. Обозначим через t_0 наименьшее целое число такое, что $\frac{m^{t_0}}{q}u\in\mathbf{N}$. Пусть $c=\frac{m^{t_0}}{q}\cdot u$, тогда

$$a=m^{-t_0}\cdot\frac{c}{n},\quad m\nmid c,\quad (c, n)=1.$$

Полагая $h=-t_0$, видим, что числа h, c, n удовлетворяют условиям (I).

Предположим, что числа h_1, c_1, n_1 удовлетворяют условиям (I′); тогда $a=m^h\cdot\frac{c}{n}=m^{h_1}\cdot\frac{c_1}{n_1}$. Пусть $h\geqslant h_1$, тогда $m^{h-h_1}cn_1=c_1n$. Так как, по условию, $(m, n)=1$ и $m\nmid c_1$, то $m\nmid c_1n$; поэтому $h-h_1=0$ и $cn_1=c_1n$, значит, $h=h_1$ и $\frac{c}{n}=\frac{c_1}{n_1}$. Так как $\frac{c}{n}=\frac{c_1}{n_1}$ несократимы, то $c=c_1$ и $n=n_1$ □

СЛЕДСТВИЕ 6.2. *Для фиксированного m и данного положительного рационального числа a существует единственное целое число h такое, что дробь a/m^h имеет взаимно простой с m знаменатель и не делящийся на m числитель.*

ОПРЕДЕЛЕНИЕ. *Представление положительного рационального числа a в виде*

$$(\mathrm{I})\quad a=m^h\cdot\frac{c}{n},$$

где $(m, n)=1$, $m\nmid c$, $(c, n)=1$, $(c, n)\in N$, будем называть *m-представлением числа a*. Число h будем обозначать также через $h(a)$.

ПРЕДЛОЖЕНИЕ 6.3. *Если периодическая m-ичная дробь*

$$m^h(b_1\dots b_l, \overline{a_1\dots a_k})$$

удовлетворяет условию $a_k\neq b_l$, то ее предпериод имеет наименьшую возможную длину.

Доказательство. Действительно, если $a_k = b_l$ и $l > 1$, то

$$m^h(b_1 \dots b_l,\ \overline{a_1 \dots a_k}) = m^{h+1}(b_1 \dots b_{l-1},\ \overline{a_k a_1 \dots a_{k-1}}),$$

т. е. можно уменьшить длину предпериода дроби. □

ПРЕДЛОЖЕНИЕ 6.4. *Пусть дробь*

(I) $m^h(b_1 \dots b_l,\ \overline{a_1 \dots a_k})$

есть разложение в периодическую m-ичную дробь положительного рационального числа a. Пусть

(II) $a = m^{h(a)} \cdot \frac{c}{n}$

есть m-представление числа a. Тогда равносильны следующие утверждения:

(α) $b_l \neq a_k$;

(β) $A \not\equiv B \pmod n$,

где $B = b_1 m^{l-1} + \dots + b_l$ и $A = a_1 m^{k-1} + \dots + a_k$;

(γ) $h = h(a)$;

(δ) $\frac{a}{m^h} = \frac{c}{n} = b_1 \dots b_l,\ \overline{a_1 \dots a_k}$.

Доказательство. (α)$\rightarrow$(β). Определим числа A и B следующими равенствами:

(1) $A = a_1 m^{k-1} + \dots + a_k,\ 0 \leqslant a_1, \dots, a_k < m,$

(2) $B = b_1 m^{l-1} + \dots + b_l,\ 0 \leqslant b_1, \dots, b_l < m,$

Так как $0 \leqslant b_l,\ a_k < m$, то из ($\alpha$) следует

(3) $a_k \not\equiv b_l \pmod m$.

На основании (1), (2) и (3) заключаем, что

$A \not\equiv B \pmod m$;

т. е. имеет место (β).

(β)$\rightarrow$(γ). Согласно условию,

$$a = m^h(b_1 \dots b_l\ \overline{a_1 \dots a_k}) =$$

$$= m^h\left(b_1 m^{l-1} + \dots + b_l + \frac{a_1 m^{k-1} + \dots + a_k}{m^k - 1}\right),$$

значит,

(4) $a = m^h\left(B + \frac{A}{m^k - 1}\right) = m^h \frac{B(m^k - 1) + A}{m^k - 1}$.

Легко видеть, что

$$B(m^k - 1) + A \equiv -B + A \equiv -b_l + a_k \pmod{m}.$$

Согласно условию (β) отсюда следует, что

(5) $B(m^k - 1) + A \not\equiv 0 \pmod{m}$,

т. е. $m \nmid (B(m^k - 1) + A)$. Кроме того, ввиду (II) и (4)

(6) $a = m^{h(a)} \cdot \frac{c}{n} = m^h \cdot \frac{B(m^k - 1) + A}{m^k - 1}$.

Согласно предложению 6.1 из (5) и (6) следует равенство

(7) $h = h(a)$;

(γ) → (δ). По условию,

(8) $a = m^{h(a)} \cdot \frac{c}{n} = m^h(b_1 \ldots b_l, \overline{a_1 \ldots a_k})$.

Из (7) и (8) следует

(9) $\frac{a}{m^h} = \frac{c}{n} = b_1 \ldots b_l, \overline{a_1 \ldots a_k}$,

значит, выполняется (δ);

(δ) → (α). Из условия (δ) следует, что

$$\frac{c}{n} = \frac{B(m^k - 1) + A}{m^k - 1},$$

т. е. $B(m^k - 1) + A = c \cdot \frac{m^k - 1}{n}$. Так как $(c, m) = 1$ и $\left(\frac{m^k - 1}{n}, m\right) = 1$, то $B(m^k - 1) + A \equiv -B + A \not\equiv 0 \pmod{m}$. Кроме того, $-B + A \equiv -b_l + a_k \pmod{m}$. Следовательно, $b_l \not\equiv a_k \pmod{m}$. В силу (1), (2) отсюда следует, что $b_l \neq a_k$. □

ПРЕДЛОЖЕНИЕ 6.5. *Пусть* $0, \overline{a_1 \ldots a_k}$ *есть разложение в периодическую* m*-ичную дробь положительного рационального числа* r/n, $(r, n) = 1$, т. е.

(1) $r/n = 0, \overline{a_1 \ldots a_k}$.

Тогда длина k *периода делится на порядок класса вычетов* $m \bmod n$, $\mathcal{O}(m \bmod n) \mid k$.

Доказательство. По условию,

$$(2)\quad \frac{r}{n}=\frac{a_1}{m}+\ldots+\frac{a_k}{m^k}+\frac{a_1}{m^{k+1}}+\ldots+\frac{a_k}{m^{2k}}+\ldots$$

Положим

$$A=a_1m^{k-1}+\ldots+a_k.$$

Тогда (2) можно записать в виде

$$\frac{r}{n}=\frac{A}{m^k}+\frac{A}{m^{2k}}+\ldots$$

Следовательно,

$$(3)\quad \frac{r}{n}=\frac{A}{m^k-1}$$

и $r(m^k-1)=nA$. А так как $(n, r)=1$, то $n\mid(m^k-1)$, т. е.

$$(4)\quad m^k\equiv 1 \pmod{n}.$$

В силу предложения 5.2 из (4) следует, что k делится на порядок класса вычетов $m \bmod n$. □

ТЕОРЕМА 6.6. *Рациональное число* $\frac{r}{n}>0$, $(r,\ n)=1$, *тогда и только тогда разлагается в чисто периодическую* m*-ичную дробь с наименьшим периодом*

$$(1)\quad 0,\ \overline{a_1\ldots a_k},$$

когда выполнены условия

$$(2)\quad 0<\frac{r}{n}\leqslant 1,\quad (m,\ n)=1.$$

При этом длина k *наименьшего периода равна порядку класса вычетов* $m \bmod n$ *и последовательность* $a_1, \ldots, a_k$ *совпадает с последовательностью цифр в* m*-адическом представлении числа* $(m^k-1)\cdot r/n$.

Доказательство. Пусть дано положительное рациональное число a, представленное несократимой дробью r/n, удовлетворяющей условиям (2). Положим $k=\mathcal{O}(m \bmod n)$. Умножив числитель и знаменатель дроби $\frac{r}{n}$ на $\frac{m^k-1}{n}$, получим

$$(3)\quad a=\frac{r}{n}=\frac{A}{m^k-1}.$$

Пусть

$$(4)\quad A=a_1m^{k-1}+\ldots+a_k$$

есть m-адическое представление числа a. Ввиду (3)

$$(5)\quad a=\frac{r}{n}=\frac{A}{m^k}+\frac{A}{m^{2k}}+\dots$$

Из (4) и (5) следует, что

$$a=\frac{a_1}{m}+\dots+\frac{a_k}{m^k}+\frac{a_1}{m^{k+1}}+\dots+\frac{a_k}{m^{2k}}+\dots,$$

т. е. получено разложение числа a в чисто периодическую дробь с периодом длины k:

$$a=0,\ \overline{a_1\dots a_k}.$$

При этом в силу предложения 6.5 длина k периода является минимальной и последовательность $a_1, \dots, a_k$ совпадает с последовательностью цифр в m-адическом представлении числа $(m^k-1)\cdot r/n$.

Теперь предположим, что дано разложение числа $\frac{r}{n}$, $(r,\ n)=1$, в чисто периодическую дробь с наименьшим периодом, $\frac{r}{n}=0,\ \overline{a_1\dots a_k}$, т. е.

$$(1)\quad \frac{r}{n}=\frac{a_1}{m}+\dots+\frac{a_k}{m^k}+\frac{a_1}{m^{k+1}}+\dots+\frac{a_k}{m^{2k}}+\dots$$

Пусть

$$(6)\quad A=a_1m^{k-1}+\dots+a_k.$$

Тогда

$$(7)\quad \frac{r}{n}=\frac{A}{m^k}+\frac{A}{m^{2k}}+\dots$$

и поэтому

$$(8)\quad \frac{r}{n}=\frac{A}{m^k-1}.$$

Ввиду (7) и (8) $0<A\leqslant m^k-1$. Отсюда и из (8) следует, что

$$0<\frac{r}{n}<1.$$

Из (8) имеем $r(m^k-1)=An$, а так как $(n,\ r)=1$, то $n\mid(m^k-1)$, т. е.

$$(9)\quad m^k\equiv 1 \pmod n.$$

и, значит, $(m, n)=1$. Из (9), согласно предложению 5.2, следует, что $\mathcal{O}(m \bmod n) \mid k$. По условию, k есть наименьший период, следовательно, в силу предложения 6.5 $k = \mathcal{O}(m \bmod n)$. Ввиду (8) $A=(m^k-1)\cdot\frac{r}{n}$. Далее, ввиду (2)

$$(m^k-1)\cdot\frac{r}{n}=a_1m^{k-1}+\ldots+a_k.$$

Таким образом, последовательность $a_1, \ldots, a_k$ цифр периода дроби $0, \overline{a_1\ldots a_k}$ совпадает с последовательностью цифр в m-адическом представлении числа $(m^k-1)\cdot\frac{r}{n}$. □

ТЕОРЕМА 6.7. *Любое положительное рациональное число a обладает нормированным разложением в периодическую m-ичную дробь $m^h(b_1\ldots b_l, \overline{a_1\ldots a_k})$. При этом если $a=m^{h(a)}\cdot\frac{c}{n}$ есть m-представление числа a, то:*

1) $h=h(a)$;

2) $k=\mathcal{O}(m \bmod n)$;

3) *последовательность $b_1, \ldots, b_l$ совпадает с последовательностью цифр в m-адическом представлении числа B, где*

$$B=\begin{cases}\left[\frac{a}{m^h}\right], & \text{если } \frac{a}{m^h}\notin\mathbf{Z},\\ \frac{a}{m^h}-1, & \text{если } \frac{a}{m^h}\in\mathbf{Z};\end{cases}$$

4) *последовательность $a_1, \ldots, a_k$ совпадает с последовательностью цифр в m-адическом представлении числа A, где*

$$A=(m^k-1)\left(\frac{a}{m^h}-B\right).$$

Доказательство. Согласно предложению 6.1, для числа a существуют целое число h и натуральные числа c, n такие, что

(1) $a=m^h\cdot\frac{c}{n}$, $(m, n)=1$, $m\nmid c$, $(c, n)=1$.

Число c можно представить в виде $c=Bn+r$, где $0<r\leqslant n$, $(r, n)=1$ и B — некоторое натуральное число, поэтому

(2) $\frac{c}{n}=B+\frac{r}{n}$, $0<\frac{r}{n}\leqslant 1$.

Следовательно, имеем:

$$B = \begin{cases} \left[\frac{a}{m^h}\right], & \text{если } \frac{a}{m^h} \notin \mathbf{Z}, \\ \frac{a}{m^h} - 1, & \text{если } \frac{a}{m^h} \in \mathbf{Z}. \end{cases}$$

По теореме 6.6, правильная дробь r/n разлагается в чисто периодическую m-ичную дробь

$$(3) \quad \frac{r}{n} = 0, \overline{a_1 \dots a_k}.$$

При этом длина k наименьшего периода равна порядку класса вычетов $m \bmod n$,

$$(4) \quad k = \mathcal{O}(m \bmod n),$$

и последовательность $a_1, \dots, a_k$ совпадает с последовательностью цифр в m-адическом представлении числа A, где

$$A = (m^k - 1) \cdot \frac{r}{n} = (m^k - 1)\left(\frac{a}{m^h} - B\right).$$

Пусть $B = b_1 m^{l-1} + \dots + b_l$ есть m-адическое представление числа B. Тогда в силу (I), (2) и (3) имеем

$$(5) \quad \frac{a}{m^h} = \frac{c}{n} = b_1 \dots b_l, \overline{a_1 \dots a_k},$$

поэтому

$$(6) \quad a = m^h (b_1 \dots b_l, \overline{a_1 \dots a_k}).$$

Так как $h = h(a)$, то из (6) согласно предложению 6.4 следует неравенство $b_l \neq a_k$. Кроме того, ввиду (4) и предложения 6.5 длина k периода в разложении (6) является наименьшей. Таким образом, (6) является нормированным разложением числа a в периодическую m-ичную дробь. □

Упражнения

1. Найдите число цифр в периоде десятичных дробей, в которые обращаются обыкновенные дроби со знаменателями: 3, 7, 11, 13, 17, 19, 21.

2. Обратите следующие периодические десятичные дроби в обыкновенные: 0,35 (62); 5,1 (538); 3, (27); 11,12 (31).

3. Найдите знаменатель дроби, обращающейся в чистую периодическую дробь с тремя цифрами в периоде.

4. Пусть p — простое число, отличное от 2 и 5. Покажите, что если дробь $1/p$ обращается в чистую периодическую десятичную

дробь с четным числом цифр в периоде, то цифры второй половины периода дополняют до девяти соответствующие цифры первой половины периода. Например, $1/7 = 0{,}\overline{142857}$.

5. Найдите число цифр в периоде десятичных дробей, в которые обращаются обыкновенные дроби со знаменателями: 41, $13 \cdot 37$, $11 \cdot 13 \cdot 17$, $5 \cdot 7 \cdot 19$, $2 \cdot 11 \cdot 13$.

6. Каким может быть знаменатель дроби, обращающейся в чистую периодическую десятичную дробь с тремя цифрами в периоде?

7. Каким может быть знаменатель дроби, обращающейся в чистую периодическую десятичную дробь с пятью цифрами в периоде?

Глава тринадцатая
КОЛЬЦА

§ 1. ИДЕАЛЫ КОЛЬЦА. ФАКТОР-КОЛЬЦО

Идеалы кольца. Пусть $\mathscr{K} = \langle K, +, -, \cdot, 1\rangle$ — кольцо и I — подмножество множества K. Множество I называется *замкнутым в $\mathscr{K}$ относительно вычитания*, если $a - b \in I$ для любых элементов a и b из I.

Множество I называется *устойчивым относительно умножения справа на элементы кольца $\mathscr{K}$*, если $ak \in I$ для любого a из I и любого k из K, т. е. если множество I вместе с каждым своим элементом a содержит все его правые кратные ak, где $k \in K$. Аналогично определяется множество, устойчивое относительно умножения слева на элементы кольца $\mathscr{K}$.

Множество I называется *устойчивым относительно умножения на элементы кольца $\mathscr{K}$*, если оно устойчиво относительно умножения справа и слева на элементы кольца $\mathscr{K}$.

ОПРЕДЕЛЕНИЕ. *Правым (левым) идеалом кольца $\mathscr{K}$* называется любое непустое подмножество множества K, замкнутое в $\mathscr{K}$ относительно вычитания и устойчивое относительно умножения справа (слева) на элементы кольца $\mathscr{K}$.

ОПРЕДЕЛЕНИЕ. *Двусторонним идеалом кольца $\mathscr{K}$* или просто *идеалом кольца $\mathscr{K}$* называется любое непустое подмножество множества K, если оно является одновременно правым и левым идеалом кольца $\mathscr{K}$.

Из определения следует, что любой идеал I кольца $\mathscr{K}$ содержит нуль кольца и замкнут относительно первых трех главных операций кольца. Алгебра $\langle I, +, -\rangle$ является *подгруппой* аддитивной группы $\langle K, +, -\rangle$ кольца. Множество $\{\mathscr{O}_{\mathscr{K}}\}$ есть идеал кольца $\mathscr{K}$, называемый *нулевым идеалом*. Множество K также есть идеал кольца $\mathscr{K}$; он состоит из кратных единицы кольца и поэтому называется *единичным идеалом кольца $\mathscr{K}$*. Нулевой и единичный идеалы называются *тривиальными идеалами кольца $\mathscr{K}$*.

Идеалы кольца, отличные от тривиальных, называются *собственными идеалами кольца.*

Примеры. 1. Пусть $\mathbb{Z}$ — кольцо целых чисел и n — фиксированное целое число. Множество $n\mathbf{Z}=\{nx \mid x \in \mathbf{Z}\}$ является идеалом кольца $\mathbb{Z}$.

2. Пусть $\mathcal{K}$ — произвольное кольцо и n — фиксированное целое число. Множество $nK=\{nx \mid x \in K\}$ является идеалом кольца $\mathcal{K}$.

3. Пусть $\mathcal{K}$ — коммутативное кольцо и a — фиксированный его элемент. Множество $\{ka \mid k \in K\}$, состоящее из кратных элемента a, есть идеал. Он называется *главным идеалом, порожденным элементом* a, и обозначается через (a). В некоммутативных кольцах необходимо различать правые и левые главные идеалы.

4. Пусть $\mathcal{K}$ — коммутативное кольцо и $a_1, \ldots, a_n \in K$. Множество $\{k_1a_1+\ldots+k_na_n \mid k_1, \ldots, k_n \in K\}$ есть идеал кольца $\mathcal{K}$. Он называется *идеалом, порожденным элементами* $a_1, \ldots, a_n$, и обозначается символом $(a_1, \ldots, a_n)$.

В некоммутативных кольцах необходимо различать правые и левые идеалы, порожденные элементами $a_1, \ldots, a_n$.

Рассмотрим операции над идеалами. *Пересечением идеалов* I и J кольца $\mathcal{K}$ называется множество $I \cap J$. Аналогично определяется пересечение любой совокупности идеалов кольца. Легко проверить, что пересечение любой совокупности идеалов кольца есть идеал этого кольца.

Суммой идеалов I и J называется множество $I+J$, определяемое равенством

$$I+J=\{x+y \mid x \in I,\ y \in J\}.$$

Легко проверить, что сумма идеалов кольца есть идеал этого кольца. Сложение идеалов обладает свойствами коммутативности и ассоциативности.

Произведением идеалов I и J кольца $\mathcal{K}$ называется множество всех элементов вида $x_1y_1+\ldots+x_ny_n$, где $x_i \in I$, $y_i \in J$ и n — любое целое положительное число. Произведение идеалов I и J обозначается через $I \cdot J$. Легко проверить, что произведение идеалов кольца есть идеал этого кольца.

Отметим, что главный идеал (a), порожденный элементом a коммутативного кольца $\mathcal{K}$, является *пересечением всех идеалов, содержащих элемент* a, и, значит, (a) есть наименьший среди идеалов, содержащих элемент a.

Аналогично, идеал $(a_1, \ldots, a_n)$, порожденный элементами $a_1, \ldots, a_n$ коммутативного кольца $\mathcal{K}$, является *пересечением всех идеалов, содержащих элементы* $a_1, \ldots, a_n$,

и, значит, $(a_1, \ldots, a_n)$ есть наименьший среди идеалов, содержащих элементы $a_1, \ldots, a_n$.

Сравнения и классы вычетов по идеалу. Пусть I — фиксированный произвольный идеал кольца $\mathcal{K}$.

ОПРЕДЕЛЕНИЕ. Элементы a, b кольца $\mathcal{K}$ называются *сравнимыми по идеалу* I, если $a-b \in I$.

Запись $a \equiv b \pmod{I}$ означает, что элементы a и b сравнимы по идеалу I.

ПРЕДЛОЖЕНИЕ 1.1. *Отношение сравнения по идеалу* I *в кольце* $\mathcal{K}$ (*на множестве* K) *является отношением эквивалентности.*

Доказательство. Отношение сравнения по идеалу I рефлексивно, так как $a-a \in I$ для любого элемента a из K. Отношение сравнения по идеалу I транзитивно, так как из того, что $a-b \in I$ и $b-c \in I$, следует, что

$$a-c=(a-b)+(b-c) \in I.$$

Отношение сравнения по идеалу I симметрично, так как из $a-b \in I$ следует $b-a \in I$. □

ОПРЕДЕЛЕНИЕ. Классы эквивалентности отношения сравнения по идеалу I в кольце $\mathcal{K}$ называются *классами вычетов по идеалу* I или *смежными классами кольца* $\mathcal{K}$ *по идеалу* I.

Класс вычетов, содержащий элемент a кольца $\mathcal{K}$, будем обозначать через $\bar{a}$. Очевидно, $\bar{a}=a+I$.

ТЕОРЕМА 1.2. *Классы вычетов кольца* $\mathcal{K}$ *по идеалу* I *обладают следующими свойствами*:

(1) *любые два класса вычетов либо совпадают, либо не пересекаются*;

(2) *объединение всех классов вычетов кольца* $\mathcal{K}$ *по идеалу* I *совпадает с множеством* $|\mathcal{K}|$;

(3) *классы вычетов* $\bar{a}$ *и* $\bar{b}$ *по идеалу* I *совпадают тогда и только тогда, когда* $a \equiv b \pmod{I}$;

(4) *если* $c \in \bar{a}$, *то* $\bar{a}=c+I$ (*в частности,* $\bar{a}=a+I$).

Свойства (1) — (4) теоремы выражают соответствующие свойства смежных классов группы $\langle K, +, - \rangle$ по подгруппе $\langle I, +, - \rangle$.

Рассмотрим следующие основные свойства сравнений по идеалу.

СВОЙСТВО 1.1. *Сравнения можно почленно складывать и вычитать, т. е. из*

$$a \equiv b \text{ и } c \equiv d \pmod{I}$$

следует, что

$$a+c \equiv b+d \text{ и } a-c \equiv b-d \pmod{I}.$$

Доказательство. В самом деле, если $a-b \in I$ и $c-d \in I$, то

$$a+c-(b+d) \in I \text{ и } (a-c)-(b-d) \in I.$$

Следовательно, $a+c \equiv b+d$, $a-c \equiv b-d \pmod{I}$. □

СВОЙСТВО 1.2. *Обе части сравнения можно умножить на любое целое число n, т. е. из $a \equiv b \pmod{I}$ следует сравнение $na \equiv nb \pmod{I}$, где $n \in \mathbf{Z}$.*

Доказательство. Из $a-b \in I$ следует, что $na-nb=n(a-b) \in I$. □

СВОЙСТВО 1.3. *Обе части сравнения можно умножить справа и слева на любой элемент кольца, т. е. из*

$$a \equiv b \pmod{I} \text{ и } c \in |\mathscr{K}|$$

следуют сравнения

$$ca \equiv cb \pmod{I},\ ac \equiv bc \pmod{I}.$$

Доказательство. Множество элементов идеала I устойчиво относительно умножения на элементы кольца. Следовательно, для любого элемента c кольца $\mathscr{K}$ из $a-b \in I$ следует, что $ca-cb \in I$ и $ac-bc \in I$. □

СВОЙСТВО 1.4. *Сравнения можно почленно перемножить, т. е. если*

$$a \equiv b,\ c \equiv d \pmod{I},\ \text{то } ac \equiv bd \pmod{I}.$$

Доказательство. В самом деле, если $a-b \in I$ и $c-d \in I$, то в силу устойчивости идеала I относительно сложения и умножения на элементы кольца имеем

$$ac-bd=ac-bc+bc-bd=(a-b)c+b(c-d) \in I. \quad \square$$

Фактор-кольцо. Пусть I — идеал кольца $\mathscr{K}=\langle K, +, -, \cdot, 1\rangle$. Выше было установлено, что отношение сравнения по идеалу I есть отношение эквивалентности на множестве K. Классы эквивалентности называются *классами вычетов* или *смежными классами кольца $\mathscr{K}$ по идеалу I*. Множество всех классов вычетов называется *фактор-множеством K по идеалу I* и обозначается через K/I.

Свойства 1.1 — 1.4 сравнений по идеалу показывают, что отношение сравнения по идеалу I является конгруэнцией в кольце $\mathscr{K}$ (конгруэнцией относительно всех главных операций кольца $\mathscr{K}$). Поэтому, согласно теореме 3.1.9,

на фактор-множестве K/I можно определить операции $+$, $-$, $\cdot$, $\bar{1}$, ассоциированные с главными операциями кольца $\mathscr{K}$, следующим образом:

$$\bar{a}+\bar{b}=\overline{a+b},\ -\bar{a}=\overline{(-a)},\ \bar{a}\bar{b}=\overline{ab},\ \bar{1}=I$$

для любых элементов $\bar{a}$, $\bar{b}$ из K/I.

Такое определение операций на фактор-множестве K/I является корректным, так как не зависит от выбора элементов a, b в смежных классах $\bar{a}$ и $\bar{b}$ соответственно.

ОПРЕДЕЛЕНИЕ. Алгебра $\langle K/I, +, -, \cdot, \bar{1}\rangle$ называется *фактор-кольцом кольца $\mathscr{K}$ по идеалу I* и обозначается через $\mathscr{K}/I$.

ТЕОРЕМА 1.3. *Пусть I — идеал кольца $\mathscr{K}$. Тогда алгебра $\mathscr{K}/I=\langle K/I, +, -, \cdot, \bar{1}\rangle$ является кольцом.*

Доказательство. Алгебра $\langle K/I, +, -\rangle$ есть абелева группа, так как она является фактор-группой аддитивной группы $\langle K, +, -\rangle$ кольца $\mathscr{K}$ по подгруппе $\langle I, +, -\rangle$ (см. теорему 10.4.2).

Алгебра $\langle K/I, \cdot, \bar{1}\rangle$ является *моноидом*. В самом деле, в силу ассоциативности умножения в $\mathscr{K}$ для любых $\bar{a}$, $\bar{b}$, $\bar{c}$ из K/I

$$\bar{a}\cdot(\bar{b}\cdot\bar{c})=\bar{a}\cdot\overline{(bc)}=\overline{a(bc)}=\overline{(ab)c}=\overline{(ab)}\cdot\bar{c}=(\bar{a}\cdot\bar{b})\cdot\bar{c},$$

т. е. умножение в алгебре $\mathscr{K}/I$ ассоциативно. Кроме того,

$$\bar{a}\cdot\bar{1}=\overline{a\cdot 1}=\bar{a}=\bar{1}\cdot\bar{a} \text{ для любого } \bar{a} \text{ из } K/I,$$

т. е. $\bar{1}$ является нейтральным элементом относительно умножения в алгебре $\mathscr{K}/I$.

Умножение в $\mathscr{K}/I$ дистрибутивно относительно сложения. В самом деле, в силу дистрибутивности умножения относительно сложения в кольце $\mathscr{K}$ для любых $\bar{a}$, $\bar{b}$, $\bar{c}$ из $\mathscr{K}/I$ имеем

$$(\bar{a}+\bar{b})\cdot\bar{c}=\overline{a+b}\cdot\bar{c}=\overline{(a+b)\cdot c}=\overline{ac+bc}=\overline{ac}+\overline{bc}=$$
$$=\bar{a}\cdot\bar{c}+\bar{b}\cdot\bar{c}.$$

Аналогично убеждаемся в том, что $\bar{c}(\bar{a}+\bar{b})=\bar{c}\cdot\bar{a}+\bar{c}\cdot\bar{b}$. □

Теорема об эпиморфизмах колец. Пусть $\mathscr{K}$ и $\mathscr{K}'$ — кольца:

$$\mathscr{K}=\langle K, +, -, \cdot, 1\rangle,\ \mathscr{K}'=\langle K', +, -, \cdot, 1'\rangle.$$

ТЕОРЕМА 1.4. *Ядро гомоморфизма кольца $\mathscr{K}$ в кольцо $\mathscr{K}'$ является идеалом кольца $\mathscr{K}$.*

Доказательство. Пусть $\operatorname{Ker} f$ — ядро гомоморфизма f кольца $\mathscr{K}$ в кольцо $\mathscr{K}'$, т. е. $\operatorname{Ker} f=\{x\in\mathscr{K}\mid f(x)=0'\}$,

где $0'$ — нуль кольца $\mathscr{K}'$. Множество $\operatorname{Ker} f$ не пусто, так как $0 \in \operatorname{Ker} f$. Для любых a, b из $\operatorname{Ker} f$ имеем

$$f(a-b)=f(a)-f(b)=0'-0'=0',$$

т. е. множество $\operatorname{Ker} f$ замкнуто в $\mathscr{K}$ относительно вычитания.

Для любого a из $\operatorname{Ker} f$ и любого k из K имеем

$$f(ka)=f(k)\cdot f(a)=f(k)\cdot 0'=0',$$

т. е. $ka \in \operatorname{Ker} f$. Аналогично убеждаемся, что $ak \in \operatorname{Ker} f$.

Таким образом, $\operatorname{Ker} f$ устойчиво относительно умножения на элементы K. Следовательно, ядро гомоморфизма f является идеалом кольца $\mathscr{K}$. □

ПРЕДЛОЖЕНИЕ 1.5. *Пусть f — гомоморфизм кольца $\mathscr{K}$ в кольцо $\mathscr{K}'$ с ядром I. Для любых a, b из K равенство $f(a)=f(b)$ выполняется тогда и только тогда, когда $\bar{a}=\bar{b}$.*

Доказательство. Пусть $f(a)=f(b)$. Тогда

(1) $f(a-b)=f(a)-f(b)=0'$,

поскольку f — гомоморфизм. Поэтому $a-b \in I$ и, следовательно, $\bar{a}=\bar{b}$.

Теперь допустим, что $\bar{a}=\bar{b}$. Тогда $a-b \in I$ и $f(a-b)=0'$, поскольку $I=\operatorname{Ker} f$. Отсюда, учитывая (1), получаем

$$f(a)-f(b)=0' \text{ и } f(a)=f(b). \quad \square$$

ТЕОРЕМА 1.6. *Пусть f — эпиморфизм кольца $\mathscr{K}$ на кольцо $\mathscr{K}'$ с ядром I. Тогда фактор-кольцо $\mathscr{K}/I$ изоморфно кольцу $\mathscr{K}'$.*

Доказательство. По условию, $I=\operatorname{Ker} f$. Пусть $\bar{K}=K/I$ — множество всех классов вычетов кольца $\mathscr{K}$ по идеалу I и

$$\mathscr{K}/I=\langle K/I, +, -, \cdot, \bar{1}\rangle,$$

где $\bar{1}=1+I$. Обозначим через h отображение K/I в $|\mathscr{K}'|$, определяемое следующим образом:

(1) $h(\bar{a})=f(\bar{a})$ для каждого элемента $\bar{a}$ из K.

В силу предложения 1.5 значение $h(\bar{a})$ не зависит от выбора представителя a в смежном классе $\bar{a}$. Далее, отображение h сохраняет главные операции кольца $\mathscr{K}/I$. В самом деле, $h(\bar{1})=1_{\mathscr{K}'}$ и для любых $\bar{a}$, $\bar{b}$ из K имеем:

$$h(\bar{a}+\bar{b})=h(\overline{a+b})=f(a+b)=f(a)+f(b)=h(\bar{a})+h(\bar{b});$$

$$h(-\bar{a})=h(\overline{(-a)})=f(-a)=-f(a)=-h(\bar{a});$$

$$h(\bar{a}\cdot\bar{b})=h(\overline{ab})=f(ab)=f(a)\cdot f(b)=h(\bar{a})\cdot h(\bar{b}).$$

По условию, f отображает $|\mathscr{K}|$ на $|\mathscr{K}'|$. В силу (1) отсюда следует, что h есть отображение множества K на множество $|\mathscr{K}'|$. Отображение h инъективно. В самом деле, в силу (1) из равенства $h(\bar{a})=h(\bar{b})$ следует $f(a)=f(b)$; в силу предложения 1.5 отсюда следует, что $\bar{a}=\bar{b}$. Следовательно, h является изоморфизмом фактор-кольца $\mathscr{K}/I$ на кольцо $\mathscr{K}'$. □

Характеристика кольца. Пусть $\mathscr{K}=\langle K, +, —, \cdot, e\rangle$ — кольцо с единицей e. В аддитивной группе $\langle K, +, -\rangle$ кольца элемент e имеет либо конечный порядок $\mathscr{O}(e)=m$, либо бесконечный порядок $\mathscr{O}(e)=\infty$.

ОПРЕДЕЛЕНИЕ. Говорят, что кольцо $\mathscr{K}$ имеет *конечную характеристику* m, если в аддитивной группе кольца единица кольца имеет конечный порядок m. Говорят, что кольцо $\mathscr{K}$ имеет *характеристику нуль,* если единица кольца $\mathscr{K}$ имеет бесконечный порядок.

Поскольку всякое поле $\mathscr{F}$ есть кольцо, мы можем говорить о характеристике поля $\mathscr{F}$. Условимся обозначать через $ch(\mathscr{K})$ характеристику кольца $\mathscr{K}$.

Примеры. 1. Пусть $\mathbb{Z}$ — кольцо целых чисел. Для любого целого положительного числа n выполняется условие $n\cdot 1\neq 0$, т. е. $\mathscr{O}(1)=\infty$. Следовательно, кольцо целых чисел имеет нулевую характеристику.

2. Пусть m — любое натуральное число, отличное от нуля. Фактор-кольцо $\mathbb{Z}_m=\mathbb{Z}/(m)$ имеет конечную характеристику m, так как 1 — единица кольца $\mathbb{Z}_m$, имеет порядок m.

3. Пусть $\mathscr{K}$ — любое числовое кольцо. Тогда для любого целого положительного числа n выполняется неравенство $n\cdot 1\neq 0$ и, значит, $\mathscr{O}(1)=\infty$. Следовательно, любое числовое кольцо имеет характеристику нуль.

4. Пусть $\mathscr{F}$ — поле характеристики m, $\mathscr{K}$ — кольцо квадратных матриц над $\mathscr{F}$ и E — единичная матрица, единица кольца. Кольцо $\mathscr{K}$ имеет характеристику m, так как $\mathscr{O}(E)=\mathscr{O}(1_{\mathscr{F}})=m$.

ТЕОРЕМА 1.7. *Характеристикой области целостности является либо нуль, либо простое число.*

Доказательство. Пусть $\mathscr{K}$ — область целостности и e — единица кольца $\mathscr{K}$. Если $\mathscr{O}(e)=\infty$, то $\mathscr{K}$ имеет характеристику нуль.

Если $\mathscr{O}(e)=1$, то $e=1_{\mathscr{K}}=0_{\mathscr{K}}$. Однако $1_{\mathscr{K}}\neq 0_{\mathscr{K}}$, так как $\mathscr{K}$ — область целостности. Значит, $\mathscr{O}(e)\neq 1$.

Предположим теперь, что $\mathscr{O}(e)=m$ есть положительное составное натуральное число: $m=st$, $1<s$, $t<m$. Следо-

вательно,

$$0 = m \cdot e = (st) \cdot e = (se) \cdot (t \cdot e).$$

Так как $\mathcal{O}(e) = m$ и $1 < s$, $t < m$, то $s \cdot e \neq 0$ и $t \cdot e \neq 0$, а поскольку $\mathcal{K}$ — область целостности, то $(s \cdot e) \cdot (t \cdot e) = m \cdot e \neq 0$. Мы пришли к противоречию, допустив, что m есть составное число. Следовательно, m является простым числом. □

ТЕОРЕМА 1.8. *Пусть p — простой элемент кольца $\mathbb{Z}$. Тогда фактор-кольцо $\mathbb{Z}_p = \mathbb{Z}/(p)$ является полем.*

Доказательство. Пусть $\bar{a}$ — любой ненулевой элемент кольца $\mathbb{Z}_p$. Надо доказать, что $\bar{a}$ обратим в кольце $\mathbb{Z}_p$. Условие $\bar{a} \neq \bar{0}$ означает, что p не делит a. Следовательно, p и a взаимно просты. Поэтому существуют такие целые числа m и n, что $mp + na = 1$. Следовательно, $\bar{n} \cdot \bar{a} = \bar{1}$, т. е. элемент $\bar{a}$ обратим в кольце $\mathbb{Z}_p$. Таким образом, кольцо $\mathbb{Z}_p$ является полем. □

Наименьшее подкольцо кольца. Подкольцо, порожденное единицей кольца $\mathcal{K}$, содержится в любом подкольце этого кольца.

ОПРЕДЕЛЕНИЕ. Подкольцо кольца $\mathcal{K}$, порожденное его единицей, называется *наименьшим* или *главным подкольцом кольца $\mathcal{K}$*.

Пусть e — единица кольца $\mathcal{K} = \langle K, +, —, \cdot, e\rangle$, $E = \{ne \mid n \in \mathbf{Z}\}$ и $\mathcal{E}$ — наименьшее подкольцо кольца $\mathcal{K}$. Тогда E является основным множеством кольца $\mathcal{E}$: $\mathcal{E} = \langle E, +, —, \cdot, e\rangle$. Легко проверить, что кольцо $\mathcal{E}$ является пересечением всех подколец кольца $\mathcal{K}$.

ТЕОРЕМА 1.9. *Пусть m — характеристика кольца $\mathcal{K}$ и $\mathcal{E}$ — наименьшее подкольцо этого кольца. Если $m = 0$, то $\mathcal{E}$ изоморфно кольцу $\mathbb{Z}$ целых чисел. Если же $m > 0$, то $\mathcal{E}$ изоморфно фактор-кольцу $\mathbb{Z}/(m)$.*

Доказательство. Рассмотрим отображение h множества $\mathbf{Z}$ в E такое, что

(1) $h(n) = ne$ для любого целого n.

В силу (1) h есть отображение множества $\mathbf{Z}$ на E и, кроме того, h сохраняет главные операции кольца $\mathbb{Z}$, т. е.

$$h(n+s) = h(n) + h(s),\ h(-n) = -h(n),$$
$$h(n \cdot s) = h(n) \cdot h(s),\ h(1) = e$$

для любых целых n и s. Следовательно, h является эпиморфизмом кольца $\mathbb{Z}$ на кольцо $\mathcal{E}$.

Покажем, что $\operatorname{Ker} h=(m)$. В самом деле, поскольку $h(m)=me=0$, то $(m)\subset\operatorname{Ker} h$. Далее, если $s\in\operatorname{Ker} h$, то $h(s)=0$, значит, $s\cdot e=0$. Кроме того, поскольку $\mathcal{O}(e)=m$, то $s\in(m)$ по теореме 10.3.1. Таким образом, $\operatorname{Ker} h\subset(m)$; следовательно, $\operatorname{Ker} h=(m)$.

По теореме о кольцевых эпиморфизмах, $\mathbb{Z}/\operatorname{Ker} h\cong\mathscr{E}$. А так как $\operatorname{Ker} h=(m)$, то $\mathscr{E}\cong\mathbb{Z}/(m)$. В частности, $\mathscr{E}\cong\mathbb{Z}/(0)$ при $m=0$. Следовательно, при $m=0$ кольцо $\mathscr{E}$ изоморфно кольцу $\mathbb{Z}$ целых чисел. □

СЛЕДСТВИЕ 1.10. *Пусть $\mathscr{K}$ — область целостности характеристики $m>0$. Тогда $\mathscr{E}$ — наименьшее подкольцо кольца $\mathscr{K}$ — является полем.*

Доказательство. Поскольку $m>0$, то, по теореме 1.7, m — простое число. Следовательно, по теореме 12.3.7, $\mathbb{Z}/(m)$ — поле. В силу теоремы 1.9 кольцо $\mathscr{E}$ изоморфно полю $\mathbb{Z}/(m)$ и, значит, само является полем. □

Упражнения

1. Пусть n — любое целое число и $n\mathbf{Z}=\{nx\ x\in\mathbf{Z}\}$. Покажите, что для всякого n множество $n\mathbf{Z}$ есть идеал кольца $\mathbb{Z}$. Покажите, что всякий идеал кольца $\mathbb{Z}$ есть множество $n\mathbf{Z}$ для некоторого натурального n.

2. Покажите, что бинарные операции пересечения и суммы идеалов коммутативны и ассоциативны.

3. Докажите, что пересечение левых (правых) идеалов кольца есть левый (правый) идеал кольца.

4. Покажите, что поле не имеет идеалов, отличных от нулевого и единичного.

5. Пусть $\mathscr{V}$ — конечномерное векторное пространство над полем $\mathscr{F}$. Пусть $\mathscr{K}$ — кольцо линейных операторов пространства $\mathscr{V}$. Докажите, что кольцо $\mathscr{K}$ не имеет двусторонних идеалов, отличных от нулевого и единичного.

6. Найдите все идеалы кольца $\mathbb{Z}_{12}$.

7. Докажите, что конечная область целостности является полем.

8. Пусть $\mathscr{K}$ — кольцо и n — целое число. Покажите, что множество $\{x\in K\mid nx=0_{\mathscr{K}}\}$ является идеалом кольца $\mathscr{K}$.

9. Пусть $\mathscr{F}$ — конечное поле, состоящее из m элементов. Докажите, что $a^m=a$ для любого элемента a поля $\mathscr{F}$.

10. Найдите все автоморфизмы поля комплексных чисел, оставляющие неизменными действительные числа.

11. Докажите, что при любом изоморфизме числовых полей подполе рациональных чисел отображается тождественно.

12. Докажите, что кольцо матриц вида

$$\begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix}$$

с действительными a, b, c, d изоморфно телу (кольцу с делением) кватернионов $a+bi+cj+dk$ над полем действительных чисел.

13. Докажите, что наименьшее подполе любого поля характеристики нуль изоморфно полю рациональных чисел.

14. Докажите, что $\mathbb{Z}_6/2\mathbf{Z}_6 \cong \mathbb{Z}_2$ и $\mathbb{Z}_6/3\mathbf{Z}_6 \cong \mathbb{Z}_3$.

15. Пусть n — положительный делитель натурального числа m. Докажите, что $\mathbb{Z}_m/n\mathbf{Z}_m \cong \mathbb{Z}_n$.

16. Докажите, что область целостности, содержащая только три элемента, изоморфна фактор-кольцу $\mathbb{Z}/3\mathbf{Z}$.

17. Докажите, что поля $\mathbb{Q}(\sqrt{7})$ и $\mathbb{Q}(\sqrt{11})$ не изоморфны.

§ 2. ПОЛЕ ЧАСТНЫХ ОБЛАСТИ ЦЕЛОСТНОСТИ

Поле частных области целостности. Весьма важным является вопрос о возможности вложения области целостности в поле.

ОПРЕДЕЛЕНИЕ. Поле $\mathscr{F}$ называется *полем частных области целостности* $\mathscr{K}$, если выполнены условия:

(α) $\mathscr{K}$ есть подкольцо поля $\mathscr{F}$;

(β) для любого x из F существуют в K такие элементы a и b, что $x = a \cdot b^{-1}$.

ТЕОРЕМА 2.1. *Для любой области целостности существует поле частных.*

Доказательство. Пусть $\mathscr{K} = \langle K, +, -, \cdot, 1\rangle$ — область целостности, $K^* = K \setminus \{0\}$ и

$$K \times K^* = \{\langle a, b\rangle \mid a \in K,\ b \in K^*\}.$$

На множестве $K \times K^*$ определим бинарное отношение $\equiv$ следующим образом:

$\langle a, b\rangle \equiv \langle c, d\rangle$ тогда и только тогда, когда $ad = bc$.

Его мы назовем *отношением сравнения на* $K \times K^*$. Отношение сравнения рефлексивно, симметрично и транзитивно.

Рефлексивность и симметричность очевидны. Свойство транзитивности также имеет место. В самом деле, из посылок следует, что $ad = bc$, $cf = de$, $d \neq 0$. Умножив обе части первого равенства на f, а второго на b, получим: $adf = bcf$, $bcf = bed$ и, значит, $adf = bed$. Последнее равенство влечет $af = be$, поскольку $\mathscr{K}$ — область целостности и $d \neq 0$. Следовательно, $\langle a, b\rangle \equiv \langle e, f\rangle$.

Таким образом, отношение сравнения является отношением эквивалентности на множестве $K \times K^*$. Класс эквивалентности, содержащий пару $\langle a, b\rangle$, обозначается через $[a, b]$, фактор-множество $K \times K^*/\equiv$ — через F_1. Отметим, что для любых $[a, b]$ и $[c, d]$ из F_1

(1) $[a, b] = [c, d]$ тогда и только тогда, когда $ad = bc$.

На множестве $K \times K^*$ определим операции $\oplus$, $\ominus$, $\odot$:

$\langle a, b\rangle \oplus \langle c, d\rangle = \langle ad + bc, bd\rangle$;

$\ominus \langle a, b\rangle = \langle -a, b\rangle$;

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

Так как $\mathscr{K}$ — область целостности, то из $b \neq 0$ и $d \neq 0$ следует, что $bd \neq 0$. Следовательно, множество $K \times K^*$ замкнуто относительно операций $\oplus$, $\ominus$ и $\odot$. Легко видеть, что операции сложения и умножения коммутативны.

Докажем, что отношение сравнения на $K \times K^*$ является конгруэнцией относительно операций $\oplus$, $\ominus$ и $\odot$. Учитывая, что операции сложения и умножения коммутативны, достаточно показать, что из условия

(2) $\langle a, b\rangle \equiv \langle a', b'\rangle$

следуют соотношения:

(3) $\langle a, b\rangle \oplus \langle c, d\rangle \equiv \langle a', b'\rangle \oplus \langle c, d\rangle$;

(4) $\ominus \langle a, b\rangle \equiv \ominus \langle a', b'\rangle$;

(5) $\langle a, b\rangle \odot \langle c, d\rangle \equiv \langle a', b'\rangle \odot \langle c, d\rangle$.

Проверка (3) сводится к установлению соотношения

$\langle ad + bc, bd\rangle \equiv \langle a'd + b'c, b'd\rangle$.

Это соотношение сводится к равенству

$(ad + bc)\, b'd = (a'd + b'c)\, bd$,

в свою очередь, сводящемуся к равенству $ab'd^2 = a'bd^2$, которое получается из равенства $ab' = a'b$. Последнее равенство следует из условия (2).

Проверка (4) сводится к установлению соотношения

$\langle -a, b\rangle \equiv \langle -a', b'\rangle$,

сводящегося к равенству $(-a)\, b' = (-a')\, b$, которое, в свою очередь, сводится к равенству $ab' = a'b$, верному в силу условия (2).

Проверка (5) сводится к установлению соотношения

$\langle ac, bd\rangle \equiv \langle a'c, b'd\rangle$,

сводящегося к равенству $ac \cdot b'd = a'c \cdot bd$, которое, в свою очередь, получается из равенства $ab' = a'b$, верного в силу условия (2).

Итак, установлено, что отношение сравнения на множестве $K \times K^*$ является конгруэнцией относительно операций $\oplus$, $\ominus$, $\odot$. По теореме 3.1.9 о конгруэнциях, на фактор-множестве F_1 определяются *операции* $+$, $-$, $\cdot$ следующими формулами:

(6) $[a, b]+[c, d]=[ad+bc, bd]$;

(7) $-[a, b]=[-a, b]$;

(8) $[a, b]\cdot[c, d]=[ac, bd]$,

причем значения так определенных операций не зависят от случайного выбора пар $\langle a, b\rangle$ и $\langle c, d\rangle$ из классов эквивалентности $[a, b]$ и $[c, d]$ соответственно.

Для любого элемента a из K положим $\bar{a}=[a, 1]$, в частности $\bar{0}=[0, 1]$, $\bar{1}=[1, 1]$. На основании (1) заключаем, что:

$[a, b]=\bar{0}$ тогда и только тогда, когда $a=0$;

$[a, b]=\bar{1}$ тогда и только тогда, когда $a=b$;

$[a, b]=[ac, bc]$ для любого $c\neq 0$.

Докажем, что алгебра $\mathscr{F}_1=\langle F_1, +, -, \cdot, \bar{1}\rangle$ является *полем*. Непосредственная проверка показывает, что сложение в $\mathscr{F}_1$ коммутативно и ассоциативно, $\bar{0}$ есть нейтральный элемент относительно сложения и для любого $[a, b]$ из F_1 имеем

$$[a, b]+(-[a, b])=\bar{0}.$$

Следовательно, алгебра $\langle F_1, +, -\rangle$ есть *абелева группа*.

Непосредственная проверка также показывает, что умножение в $\mathscr{F}_1$ коммутативно и ассоциативно и $\bar{1}$ есть нейтральный элемент относительно умножения. Следовательно, алгебра $\langle F_1, \cdot, \bar{1}\rangle$ является *коммутативным моноидом*.

Покажем, что умножение в $\mathscr{F}_1$ дистрибутивно относительно сложения, т. е. для любых $[a, b]$, $[c, d]$, $[e, f]$ из F_1

$$([a, b]+[c, d])[e, f]=[a, b][e, f]+[c, d][e, f].$$

Необходимо показать, что

$$[ade+bce, bdf]=[ae\cdot df+ce\cdot bf, bf\cdot df],$$

или

$$\langle ade+bce, bdf\rangle \equiv \langle (ade+bce)f, bdf\cdot f\rangle \quad (f\neq 0).$$

Последнее соотношение следует из того, что $\langle a_1, b_1\rangle \equiv \equiv \langle a_1 f, b_1 f\rangle$ для любых a_1, b_1, f при $f \neq \bar{0}$.

Таким образом, алгебра $\mathscr{F}_1$ является *коммутативным кольцом*. В кольце $\mathscr{F}_1$ выполняется условие $\bar{0} \neq \bar{1}$, так как $0 \cdot 1 \neq 1 \cdot 1$ в поле $\mathscr{F}$. В кольце $\mathscr{F}_1$ обратим любой элемент, отличный от $\bar{0}$. В самом деле, если $[a, b] \neq \bar{0}$, то $a \neq 0$, $[b, a] \in F_1$ и $[a, b] \cdot [b, a] = \bar{1}$. Итак, установлено, что алгебра $\mathscr{F}_1$ является полем.

Поле $\mathscr{F}_1$ содержит подкольцо, изоморфное кольцу $\mathscr{K}$. В самом деле, рассмотрим множество $K_1 = \{[a, 1] \mid a \in K\}$. Это множество замкнуто в $\mathscr{F}_1$, так как

$$(9)\quad [a, 1] + [b, 1] = [a + b, 1], \quad -[a, 1] = [-a, 1],$$
$$[a, 1]\,[b, 1] = [ab, 1], \quad [1, 1] \in K_1$$

для любых $[a, 1]$, $[b, 1]$ из K_1. Следовательно, алгебра $\mathscr{K}_1 = \langle K_1, +, -, \cdot, \bar{1}\rangle$ есть подкольцо поля $\mathscr{F}_1$. Определим *отображение* h_1 *множества* K_1 *в* K следующим образом:

$$h_1([a, 1]) = a \text{ для каждого } a \text{ из } K.$$

Очевидно, h_1 есть инъективное отображение множества K_1 на K. В силу (9) отображение h_1 сохраняет главные операции кольца $\mathscr{K}_1$, т. е.

$$h_1(\bar{a} + \bar{b}) = a + b,\ h_1(-\bar{a}) = -a,\ h_1(\bar{a}\bar{b}) = ab,\ h_1(\bar{1}) = 1.$$

Таким образом, h_1 есть *изоморфизм кольца* $\mathscr{K}_1$ на кольцо $\mathscr{K}$. Следовательно, поле $\mathscr{F}_1$ содержит подкольцо $\mathscr{K}_1$, изоморфное исходному кольцу $\mathscr{K}$.

Теперь по полю $\mathscr{F}_1$ необходимо построить новое поле, изоморфное полю $\mathscr{F}_1$ и содержащее подкольцо $\mathscr{K}$. Для этого заменим в множестве F_1 каждый элемент $[a, 1]$ элементом a (образом элемента $[a, 1]$ при отображении h_1), оставляя все остальные элементы множества F_1 неизменными. Положим $F = (F_1 \setminus K_1) \cup K$. Обозначим через h следующее отображение множества F_1 на F:

$$h(x) = \begin{cases} h_1(x), & \text{если } x \in K_1, \\ x, & \text{если } x \in F_1 \setminus K_1. \end{cases}$$

Отображение h является *инъективным отображением множества* F_1 на F, продолжающим отображение h_1.

На множестве F определим *операции* $+$, $-$, $\cdot$ формулами

$$\alpha+\beta=h(h^{-1}(\alpha)+h^{-1}(\beta)),$$
$$(*)\quad -\alpha=h(-h^{-1}(\alpha)),$$
$$\alpha\cdot\beta=h(h^{-1}(\alpha)\cdot h^{-1}(\beta))\quad(\alpha,\ \beta\in F).$$

Отметим, что $1=h(\bar{1})$. Рассмотрим алгебру $\mathscr{F}=\langle F,\ +,\ -,\ \cdot,\ 1\rangle$. На основании формул $(*)$ заключаем, что верны формулы

$$h^{-1}(\alpha+\beta)=h^{-1}(\alpha)+h^{-1}(\beta),$$
$$h^{-1}(-\alpha)=-h^{-1}(\alpha)\qquad(\alpha,\ \beta\in F),$$
$$h^{-1}(\alpha\beta)=h^{-1}(\alpha)\cdot h^{-1}(\beta),$$
$$h^{-1}(1)=\bar{1}.$$

Эти формулы показывают, что h^{-1} есть *изоморфизм алгебры* $\mathscr{F}$ на поле $\mathscr{F}_1$. Следовательно, алгебра $\mathscr{F}$ является полем. При этом $\mathscr{K}$ является подкольцом поля $\mathscr{F}$, так как $K\subset F$ и в силу формул $(*)$ операции $+$, $-$, $\cdot$ в $\mathscr{F}$ продолжают соответствующие главные операции кольца $\mathscr{K}$. В самом деле, для любых α, β из K имеем:

$$\alpha+\beta=h([\alpha,\ 1]+[\beta,\ 1])=h([\alpha+\beta,\ 1])=\alpha+\beta;$$
$$-\alpha=h(-[\alpha,\ 1])=h([-\alpha,\ 1])=-\alpha;$$
$$\alpha\cdot\beta=h([\alpha,\ 1]\cdot[\beta,\ 1])=h([\alpha\beta,\ 1])=\alpha\beta.$$

Каждый элемент x из F можно представить в виде частного элементов кольца $\mathscr{K}$. В самом деле, если $h^{-1}(x)=[a,\ b]$, где $a,\ b\in K$ и $b\neq 0$, то

$$[a,\ b]=[a,\ 1]\cdot[1,\ b]\ \text{ и }\ h^{-1}(x)=\bar{a}\cdot(\bar{b})^{-1}.$$

Следовательно,

$$x=h(\bar{a}\cdot\bar{b}^{-1})=h(\bar{a})\cdot h(\bar{b}^{-1})=a\cdot b^{-1},\ \text{ значит, }\ x=a\cdot b^{-1}.$$

Итак, установлено, что $\mathscr{F}$ — поле, удовлетворяющее условиям: (α) $\mathscr{K}$ есть подкольцо поля $\mathscr{F}$; (β) для всякого x из F существуют в K такие элементы a, b, что $x=a\cdot b^{-1}$. Следовательно, $\mathscr{F}$ является полем частных для области целостности $\mathscr{K}$. □

Изоморфизм полей частных. Покажем, что всякая область целостности имеет единственное поле частных с точностью до изоморфизма.

ТЕОРЕМА 2.2. *Пусть* $\mathscr{K} = \langle K, +, —, \cdot, 1\rangle$ *— область целостности. Пусть* $\mathscr{F} = \langle F, \overset{\mathscr{F}}{+}, \overset{\mathscr{F}}{—}, \cdot, 1\rangle$ и $\mathscr{P} = \langle P, \oplus, \ominus, \odot, 1\rangle$ *— поля частных кольца* $\mathscr{K}$. *Тогда существует изоморфизм поля* $\mathscr{F}$ *на поле* $\mathscr{P}$, *переводящий каждый элемент кольца* $\mathscr{K}$ *в себя.*

Доказательство. По условию, $\mathscr{F}$ — поле частных, значит выполняются условия:

(α) $\mathscr{K}$ есть подкольцо поля $\mathscr{F}$;

(β) для любого x из F существуют в K такие элементы a, b, что $x = a \cdot b^{-1}$. Далее, по условию, $\mathscr{P}$ — другое поле частных кольца $\mathscr{K}$, значит выполняются условия:

(γ) $\mathscr{K}$ есть подкольцо поля $\mathscr{P}$;

(δ) для любого y из P существуют в K такие элементы a_1, b_1, что $y = a_1 \odot b_1^{-1}$.

Определим *отношение* h следующим образом:

(1) $h(a \cdot b^{-1}) = a \odot b^{-1}$ для любых a, b из K.

Покажем, что h есть отображение из F в P. Надо показать, что равенство (1) определяет единственное значение $h(x)$, не зависящее от конкретного представления элемента x в виде $x = a \cdot b^{-1}$. В самом деле, если $x = c \cdot d^{-1}$ (c, $d \in K$) есть любое другое такое представление элемента x, то $a \cdot b^{-1} = c \cdot d^{-1}$. Следовательно, в силу (α) $a \cdot d = b \cdot c$. В силу (γ) отсюда следует, что $a \odot b^{-1} = c \odot b^{-1}$. Поэтому

$$h(a \cdot b^{-1}) = a \odot b^{-1} = c \odot d^{-1} = h(c \cdot d^{-1}).$$

Таким образом, установлено, что h является отображением (функцией). В силу (1) и условия (β) $\mathrm{Dom}\, h = F$. В силу (1) и условия (δ) $\mathrm{Im}\, h = P$. Следовательно, h является отображением множества F на P.

Непосредственная проверка показывает, что h есть гомоморфизм поля $\mathscr{F}$ на поле $\mathscr{P}$, т. е. для любых x, y из F выполняются условия

$$h(x \overset{\mathscr{F}}{+} y) = h(x) \oplus h(y), \quad h(\overset{\mathscr{F}}{—} x) = \ominus h(x),$$
$$h(x \cdot y)\, h(x) \odot h(y), \quad h(1_{\mathscr{F}}) = 1_{\mathscr{P}}.$$

Отображение h инъективно. В самом деле, если для каких-нибудь элементов $a \cdot b^{-1}$ и $c \cdot d^{-1}$ из F

(2) $h(a \cdot b^{-1}) = h(c \cdot d^{-1})$,

то согласно (1) в поле $\mathscr{P}$ выполняется равенство $a \odot b^{-1} = c \odot d^{-1}$. В силу ($\delta$) отсюда следует равенство $a \cdot d = b \cdot c$.

В силу (α) из последнего равенства следует, что

(3) $a \cdot b^{-1} = c \cdot d^{-1}$.

Итак, установлено, что для любых элементов $a \cdot b^{-1}$ и $c \cdot d^{-1}$ множества F из (2) следует (3). Следовательно, h есть инъективное отображение. Кроме того, h есть гомоморфизм. Следовательно, h является изоморфизмом поля $\mathscr{F}$ на поле $\mathscr{P}$. Наконец, в силу (1) $h(a) = a$ для любого a из K, т. е. h переводит каждый элемент кольца $\mathscr{K}$ в себя. □.

Упражнения

1. Пусть $\mathscr{K}$ — подкольцо поля $\mathscr{F}$ и K — его основное множество. Пусть $\mathscr{P}$ — подполе поля $\mathscr{F}$, порожденное множеством K, значит, $\mathscr{P}$ есть пересечение всех подполей поля $\mathscr{F}$, содержащих множество K. Докажите, что $\mathscr{P}$ является полем частных кольца $\mathscr{K}$.

2. Пусть $\mathbf{Z}[i] = \{m + ni \mid m,\ n \in \mathbf{Z}\}$ и $\mathbb{Z}[i]$ — подкольцо поля комплексных чисел с основным множеством $\mathbf{Z}[i]$. Пусть $\mathbb{Q}(i) = \{a + bi \mid a,\ b \in \mathbf{Q}\}$ и $\mathbb{Q}(i)$ — подполе поля комплексных чисел с основным множеством $\mathbf{Q}(i)$. Покажите, что $\mathbb{Q}(i)$ есть поле частных кольца $\mathbb{Z}[i]$.

3. Пусть $\mathscr{P}$ и $\mathscr{P}'$ — поля частных для областей целостности $\mathscr{K}$ и $\mathscr{K}'$ соответственно и h — изоморфизм $\mathscr{K}$ на $\mathscr{K}'$. Докажите, что существует единственный изоморфизм поля $\mathscr{P}$ на $\mathscr{P}'$, продолжающий изоморфизм h.

4. Пусть $\mathscr{P}$ — поле частных области целостности $\mathscr{K}$ и φ — мономорфизм $\mathscr{K}$ в поле $\mathscr{F}$. Докажите, что φ можно продолжить, и притом единственным образом, до мономорфизма поля $\mathscr{P}$ в поле $\mathscr{F}$.

§ 3. КОЛЬЦА ГЛАВНЫХ ИДЕАЛОВ

Простейшие свойства делимости в коммутативном кольце. Пусть $\mathscr{K}$ — коммутативное кольцо и a, b — его элементы.

ОПРЕДЕЛЕНИЕ. Элемент b называется *делителем* a, а элемент a — *кратным* b, если в $\mathscr{K}$ существует такой элемент c, что $a = bc$.

Запись $b \mid a$ означает, что b есть делитель a. Запись $a \vdots b$ означает, что a делится на b, или a кратно b.

Элемент c называется *общим делителем* a и b, если $c \mid a$ и $c \mid b$ (или $a \vdots c$ и $b \vdots c$). Аналогично определяется общий делитель нескольких элементов кольца.

Элементы a и b кольца $\mathscr{K}$ называются *ассоциированными* в $\mathscr{K}$, если $a \mid b$ и $b \mid a$.

Элемент a называется *обратимым* в $\mathscr{K}$ или *делителем единицы*, если существует в $\mathscr{K}$ такой элемент b, что $ab = 1$; в этом случае пишут $b = a^{-1}$.

Делитель единицы делит любой элемент кольца. Если $\mathscr{K}$ — поле, то обратим любой его элемент, отличный от нуля.

Рассмотрим простейшие свойства делимости в коммутативном кольце.

ПРЕДЛОЖЕНИЕ 3.1. *Отношение делимости в кольце рефлексивно и транзитивно, т. е. является предпорядком.*

ПРЕДЛОЖЕНИЕ 3.2. *Общий делитель двух или нескольких элементов кольца является делителем суммы и произведения этих элементов.*

ПРЕДЛОЖЕНИЕ 3.3. *Если элемент c делит хотя бы один из элементов $a_1, \ldots, a_n$, то он делит произведение этих элементов.*

ПРЕДЛОЖЕНИЕ 3.4. *Отношение ассоциированности в коммутативном кольце является отношением эквивалентности.*

ПРЕДЛОЖЕНИЕ 3.5. *Если a ассоциировано с b и $b \mid c$, то $a \mid c$.*

Доказательство предложений 3.1 — 3.5 предоставляется читателю.

ПРЕДЛОЖЕНИЕ 3.6. *В области целостности элементы a и b ассоциированы тогда и только тогда, когда существует такой обратимый в кольце элемент u, что $a = ub$.*

Доказательство. Пусть $\mathscr{K}$ — область целостности и a, b — элементы, ассоциированные в $\mathscr{K}$, $a \sim b$. Если один из элементов a, b равен нулю, то необходимо равен нулю и другой. Тогда $a = 1_{\mathscr{K}} \cdot b$.

Предположим, что $a \sim b$ и $a \neq 0$, $b \neq 0$. Тогда существуют такие ненулевые элементы u и v, что $a = ub$ и $b = va$. Следовательно, $a = uva$ и $a(uv - 1) = 0$. Поскольку $\mathscr{K}$ — область целостности и $a \neq 0$, из последнего равенства следует, что $uv - 1 = 0$ и $uv = 1$. Таким образом, элемент u обратим в $\mathscr{K}$ и $a = ub$.

Предположим теперь, что $a = \varepsilon b$, где ε — обратимый элемент кольца $\mathscr{K}$; тогда $b = \varepsilon^{-1} a$. Следовательно, a и b ассоциированы в $\mathscr{K}$. □

ПРЕДЛОЖЕНИЕ 3.7. *Пусть A — множество всех обратимых элементов коммутативного кольца $\mathscr{K}$, $\mathscr{K} = \langle K, +, —, \cdot, 1\rangle$. Тогда алгебра $\langle A, \cdot, {}^{-1}\rangle$, где ${}^{-1}$ — унарная операция, ставящая в соответствие элементу a из A обратный элемент a^{-1}, является группой.*

Доказательство предложения 3.7 предоставляется читателю.

Простые и составные элементы области целостности. Пусть $\mathscr{K}$ — область целостности. Всякий элемент a кольца

делится на любой обратимый элемент кольца (на любой делитель единицы кольца) и на каждый ассоциированный с a элемент кольца. Такие делители называются *тривиальными делителями элемента* a.

ОПРЕДЕЛЕНИЕ. *Собственным делителем элемента* a называется любой его нетривиальный делитель, т. е. делитель, не ассоциированный с a и необратимый в кольце $\mathcal{K}$.

ОПРЕДЕЛЕНИЕ. Элемент области целостности $\mathcal{K}$ называется *составным* или *приводимым в* $\mathcal{K}$, если он отличен от нуля и его можно представить в виде произведения двух необратимых элементов кольца $\mathcal{K}$.

Другими словами, элемент области целостности называется *составным*, если он отличен от нуля и его можно представить в виде произведения двух собственных делителей.

ОПРЕДЕЛЕНИЕ. Элемент области целостности $\mathcal{K}$ называется *простым* или *неприводимым в* $\mathcal{K}$, если он отличен от нуля, необратим и имеет только тривиальные делители.

Отметим, что в любом поле нет простых и нет составных элементов.

Примеры. 1. В кольце $\mathbb{Z}$ целых чисел элемент p, отличный от 0 и ± 1, является простым в том и только в том случае, когда его делителями являются только элементы ± 1, $\pm p$. Простыми в кольце $\mathbb{Z}$ являются числа ± 2, ± 3, ± 5, ...

2. В кольце $\mathbb{Z}$ элемент 6 составной, так как $6 = 2 \cdot 3$ и 2, 3 — необратимые элементы.

Множество всех элементов области целостности распадается на четыре класса: 1) множество, содержащее один элемент — нуль; 2) множество всех обратимых элементов (множество всех делителей единицы); 3) множество всех простых элементов; 4) множество всех составных элементов. Последние два класса могут быть пустыми (если область целостности — поле).

ТЕОРЕМА 3.8. *Пусть* $\mathcal{K}$ *— область целостности,* a, $b \in K$ *и* 1 *— единица кольца* $\mathcal{K}$. *Тогда*:

(1) $b \mid a$ *тогда и только тогда, когда* $(a) \subset (b)$;

(2) $a \mid 1$ *тогда и только тогда, когда* $(a) = (1)$;

(3) $a \sim b$ *тогда и только тогда, когда* $(a) = (b)$;

(4) *если* b *— собственный делитель* a, *то* $(a) \subsetneq (b)$;

(5) $(a) \subsetneq (b)$ *тогда и только тогда, когда* $b \mid a$ *и* a *не делит* b.

Доказательство. (1) Пусть $b \mid a$, т. е. существует такой элемент c из K, что $a = bc$; тогда $a \in (b)$;

$$(a) = \{ma \mid m \in K\} = \{mcb \mid m \in K\} \subset \{lb \mid l \in K\} = (b)$$

и, значит, $(a) \subset (b)$. Допустим теперь, что $(a) \subset (b)$; тогда $a \in (b)$ и, значит, $a = bc$ для некоторого c из K, т. е. $b \mid a$;

(2) если $a \mid 1$, то $(1) \subset (a)$ в силу (1). Кроме того, $(a) \subset (1)$, поскольку $(1) = K$; следовательно, $(a) = (1)$. Если $(a) = (1)$, то $a \mid 1$ в силу (1);

(3) если $a \sim b$, т. е. $a \mid b$ и $b \mid a$, то в силу (2) $(b) \subset (a)$ и $(a) \subset (b)$ и, значит, $(a) = (b)$. Если $(a) = (b)$, то $a \in (b)$ и $b \in (a)$ и поэтому $b \mid a$ и $a \mid b$, следовательно, $a \sim b$;

(4) пусть b есть собственный делитель a, т. е. $b \nmid 1$, $b \not\sim a$ и $b \mid a$. Тогда в силу (1) и (3) $(b) \neq (a)$ и $(a) \subset (b)$, значит, $(a) \subsetneq (b)$;

(5) если $(a) \subsetneq (b)$, то в силу (1) $b \mid a$ и в силу (3) $a \not\sim b$ и, значит, $b \nmid a$. Обратное следует из (1) и (3). □

Кольца главных идеалов. В классе областей целостности необходимо выделить и изучить такие кольца, у которых каждый идеал был бы главным.

ОПРЕДЕЛЕНИЕ. *Кольцом главных идеалов* называется область целостности, в которой каждый идеал является главным.

Примеры. 1. Любое поле есть кольцо главных идеалов.

2. Кольцо $\mathbb{Z}$ целых чисел является кольцом главных идеалов.

Напомним, что множество $(a, b) = \{ax + by \mid x, y \in K\}$, где a, b — фиксированные элементы K, является идеалом коммутативного кольца $\mathcal{K}$.

Рассмотрим свойства колец главных идеалов.

ПРЕДЛОЖЕНИЕ 3.9. *Пусть* p *— простой элемент кольца* $\mathcal{K}$ *главных идеалов и* $a \in K$. *Если* p *не делит* a, *то* $(p, a) = (1)$.

Доказательство. По условию, каждый идеал кольца $\mathcal{K}$ — главный. Следовательно, существует в $\mathcal{K}$ такой элемент c, что $(p, a) = (c)$. Элемент c делит элементы p и a:

(1) $c \mid p$, $c \mid a$.

Так как c — делитель простого элемента p, то $c \sim p$ или c делит 1. Если $c \sim p$, то $p \mid c$, и поскольку в силу (1) $c \mid a$, то $p \mid a$, что противоречит условию. Поэтому c делит 1. Следовательно, $(c) = (1)$ и $(p, a) = (1)$. □

ПРЕДЛОЖЕНИЕ 3.10. *Пусть p — простой элемент кольца главных идеалов $\mathcal{K}$ и $a, b \in K$. Если p делит ab, то p делит a или b.*

Доказательство. Если p не делит a, то в силу предложения 3.9 $(p, a) = (1)$. Следовательно, существуют в K такие элементы u, v, что $up + va = 1$. Умножив обе части равенства на b, имеем $upb + vab = b$. Следовательно, если p делит ab, то p делит $upb + vab$ и b. Таким образом, если $p \nmid a$, то $p \mid b$. □

ПРЕДЛОЖЕНИЕ 3.11. *Пусть p — простой элемент кольца $\mathcal{K}$ главных идеалов и $a_1, \ldots, a_n \in K$. Если p делит произведение $a_1 a_2 \ldots a_n$, то p делит хотя бы один из сомножителей $a_1, \ldots, a_n$.*

Доказательство этого предложения проводится индукцией по n на основании предложения 3.10.

ОПРЕДЕЛЕНИЕ. Последовательность $(a_1), (a_2), (a_3), \ldots$ главных идеалов кольца называется *возрастающей цепочкой идеалов*, если

$$(1) \quad (a_1) \subset (a_2) \subset (a_3) \subset \ldots$$
$$\neq \quad \neq \quad \neq$$

ПРЕДЛОЖЕНИЕ 3.12. *В кольце главных идеалов возрастающая цепочка идеалов не может быть бесконечной.*

Доказательство. Пусть (1) — возрастающая цепочка кольца $\mathcal{K}$ главных идеалов. Обозначим через I объединение всех идеалов цепочки (1), т. е.

$$(2) \quad I = \bigcup_i (a_i).$$

Непосредственная проверка показывает, что множество I замкнуто относительно вычитания и устойчиво относительно умножений на элементы кольца $\mathcal{K}$. Поэтому I есть идеал кольца $\mathcal{K}$ и притом главный. Следовательно, в K имеется такой элемент c, что $I = (c)$. В силу (2) найдется такой индекс m, что $c \in (a_m)$. Так как $c \in (a_m)$ и $a_m \in I = (c)$, то $I = (a_m) = (c)$. Следовательно, идеал (a_m) является последним звеном в цепочке (1). □

Факториальность кольца главных идеалов. Нашей целью является обобщение на кольца главных идеалов теоремы

о существовании и единственности разложения элементов кольца целых чисел $\mathbb{Z}$ на простые множители.

ОПРЕДЕЛЕНИЕ. Говорят, что элемент a области целостности $\mathscr{K}$ обладает однозначным разложением на простые множители, если выполняются условия:

(1) существуют в $\mathscr{K}$ такие простые элементы p_i, что $a = \prod_{i=1}^{m} p_i$;

(2) если $a = \prod_{i=1}^{n} q_i$ — другое разложение, в котором q_i — простые элементы $\mathscr{K}$, то $m = n$ и при соответствующей нумерации $p_i \sim q_i$ для $i = 1, \ldots, m$.

ОПРЕДЕЛЕНИЕ. Кольцо $\mathscr{K}$ называется *факториальным*, если оно есть область целостности и всякий отличный от нуля необратимый элемент кольца обладает однозначным разложением на простые множители.

Отметим, что любое поле есть факториальное кольцо, так как не имеет отличных от нуля необратимых элементов.

ТЕОРЕМА 3.13. *Кольцо главных идеалов факториально.*

Доказательство. Пусть $\mathscr{K}$ — кольцо главных идеалов. Нам надо доказать, что всякий отличный от нуля необратимый элемент кольца обладает разложением на простые множители. Допустим, что существует в $\mathscr{K}$ необратимый ненулевой элемент a, который неразложим на простые множители в $\mathscr{K}$. Тогда элемент a является составным. Следовательно, его можно представить в виде произведения двух собственных делителей $a = a_1 b_1$ и, по пункту (4) теоремы 3.8, $(a) \subset (a_1)$.

По крайней мере один из множителей a_1, b_1, например a_1, не обладает разложением на простые множители. Следовательно, a_1 можно представить в виде произведения двух собственных множителей:

$$a_1 = a_2 b_2, \quad (a_1) \subset (a_2)$$

и т. д. Таким образом, существует бесконечная возрастающая цепочка

$$(a) \subset (a_1) \subset (a_2) \subset \ldots$$

идеалов кольца $\mathscr{K}$, что невозможно в силу предложения 3.12. Следовательно, всякий необратимый отличный от нуля

элемент кольца $\mathscr{K}$ обладает разложением на простые множители.

Докажем однозначность разложения на простые множители. Если a — простой элемент, то теорема верна. Предположим, что теорема верна для элементов, представимых в виде произведения n простых множителей, и докажем, что тогда она верна для элементов, представимых в виде произведения $n+1$ простых множителей. Пусть даны любые два разложения элемента a на простые множители:

$$(1)\quad a = p_1 \dots p_n p_{n+1} = q_1 \dots q_s q_{s+1}.$$

Простой элемент p_{n+1} делит произведение $q_1 \dots q_{s+1}$. Следовательно, по предложению 3.14, он делит хотя бы один из множителей $q_1, \dots, q_{s+1}$, например q_{s+1}. Так как p_{n+1} и q_{s+1} — простые, то $q_{s+1} = up_{n+1}$, где u — обратимый элемент кольца. Сокращая обе части равенства (1) на p_{n+1}, имеем

$$p_1 \dots p_n = q_1 \dots (uq_s).$$

Следовательно, по индуктивному предположению, $n = s$ и при соответствующей нумерации $p_i \sim q_i$ для $i = 1, \dots, n$. Кроме того, $p_{n+1} \sim q_{n+1}$. Индукция проведена полностью. □

Евклидовы кольца. Пусть $\mathbf{N}$ — множество всех натуральных чисел, а K — основное множество кольца $\mathscr{K}$.

ОПРЕДЕЛЕНИЕ. Область целостности $\mathscr{K}$ называется *евклидовым кольцом*, если существует отображение h множества K в $\mathbf{N}$, удовлетворяющее условиям:

(α) для любых a, b из K при $b \neq 0$ существуют в K такие элементы q, r, что $a = bq + r$ и $h(r) < h(b)$;

(β) для любого a из K равенство $h(a) = 0$ выполняется тогда и только тогда, когда $a = 0$.

Пример. Пусть h — такое отображение множества $\mathbf{Z}$ целых чисел в $\mathbf{N}$, что $h(a) = |a|$. В силу теоремы о делении с остатком (см. теорему 4.4.4) h удовлетворяет условиям (α) и (β). Следовательно, $\mathbb{Z}$ есть евклидово кольцо.

ТЕОРЕМА 3.14. *Евклидово кольцо является кольцом главных идеалов.*

Доказательство. Пусть $\mathscr{K}$ — евклидово кольцо и h — отображение множества K в $\mathbf{N}$, удовлетворяющее условиям (α) и (β). Нулевой идеал, очевидно, — главный. Пусть M — ненулевой идеал кольца $\mathscr{K}$. Нам надо доказать, что идеал M — главный. Так как $M \setminus \{0\}$ — непустое множество, то в силу (β) $h(M \setminus \{0\})$ есть непустое подмножество множества $\mathbf{N} \setminus \{0\}$ и, значит, по теореме 4.3.11, $h(M \setminus \{0\})$

имеет наименьший элемент. Следовательно, существует в M такой ненулевой элемент b, что

(1) $h(b) \leqslant h(x)$ для любого x из $M \setminus \{0\}$.

Докажем, что $M = (b)$. Пусть a — произвольный элемент множества $M \setminus \{0\}$. В силу условия (α) существуют в K такие элементы q и r, что

(2) $a = bq + r$ и $h(r) < h(b)$.

Так как M — идеал и $a,\ b \in M$, то $r = a - bq \in M$ и в силу (1), (2) имеем

(3) $r \notin M \setminus \{0\}$.

Следовательно, $r = 0$ и $a = bq$. А так как a — произвольный ненулевой элемент множества M, то $M \subset (b)$. Поскольку $b \in M$, то $M = (b)$; следовательно, любой идеал евклидова кольца $\mathscr{K}$ является главным. □

СЛЕДСТВИЕ 3.15. *Любое евклидово кольцо факториально.*

СЛЕДСТВИЕ 3.16. *Кольцо $\mathbb{Z}$ целых чисел является кольцом главных идеалов и, значит, факториально.*

Пример. Пусть $\mathbf{Z}[i] = \{m + ni \mid m,\ n \in \mathbf{Z}\}$. Множество $\mathbf{Z}[i]$ замкнуто в кольце $\mathscr{C}$ комплексных чисел. Поэтому алгебра $\mathbb{Z}[i] = \langle \mathbf{Z}[i], +, -, \cdot, 1 \rangle$ есть подкольцо кольца $\mathscr{C}$. Это кольцо называется *кольцом целых гауссовых чисел*. Покажем, что кольцо $\mathbb{Z}[i]$ — евклидово. Рассмотрим отображение h множества $\mathbf{Z}[i]$ в $\mathbf{N}$ такое, что при $a = m + ni$ $h(a) = |a|^2 = m^2 + n^2$. Условие (β), очевидно, выполняется. Покажем, что для h выполняется условие (α). Пусть $a,\ b \in \mathbf{Z}[i]$ и $b \neq 0$. Тогда $a/b = \sigma + \tau i$, где $\sigma,\ \tau \in \mathbf{Q}$. Существуют такие целые числа s и t, что $|s - \sigma| \leqslant \frac{1}{2}$ и $|t - \tau| \leqslant \frac{1}{2}$. Положим $\alpha = \sigma - s$ и $\beta = \tau - t$. Тогда $a = b(s + \alpha + (t + \beta)i) = bq + r$, где $q = s + ti$ и $r = b(\alpha + \beta i)$; при этом $q = s + ti \in \mathbf{Z}[i]$ и $r = a - bq \in \mathbf{Z}[i]$. Поэтому $h(r) = |r|^2 = |b|^2(\alpha^2 + \beta^2) \leqslant \frac{1}{2}|b|^2 = \frac{1}{2}h(b)$ и $h(r) < h(b)$, т. е. h удовлетворяет также условию (α). Таким образом, кольцо целых гауссовых чисел является евклидовым.

Упражнения

1. Пусть K — множество всех рациональных чисел m/n с нечетными знаменателями n и $\mathscr{K} = \langle K, +, -, \cdot, 1 \rangle$ — подкольцо поля $\mathscr{Q}$

рациональных чисел. Покажите, что $\mathcal{K}$ есть кольцо главных идеалов.

2. Пусть $\mathbb{Z}[i]$ — кольцо целых гауссовых чисел. Найдите обратимые элементы этого кольца.

3. Докажите, что фактор-кольцо $\mathbb{Z}[i]/(3)$ кольца целых гауссовых чисел по идеалу (3) есть поле из девяти элементов.

4. Докажите, что фактор-кольцо $\mathbb{Z}[i]/(n)$ кольца целых гауссовых чисел по идеалу (n) является полем тогда и только тогда, когда n — простое число, не равное сумме двух квадратов целых чисел.

5. Пусть $K=\{a+bi\sqrt{3} \mid a,\ b\in \mathbf{Z}\}$ и $\mathcal{K}=\langle K, +, -, \cdot, 1\rangle$ — подкольцо поля комплексных чисел. Покажите, что в кольце $\mathcal{K}$ всякий необратимый элемент, отличный от нуля, разложим на простые множители, но не всегда однозначно. В частности, покажите, что $4=2\cdot 2=(1+i\sqrt{3})(1-i\sqrt{3})$ — два разложения числа 4 в произведение простых множителей, причем 2 не ассоциировано с $1\pm i\sqrt{3}$.

6. Пусть K — множество всех комплексных чисел вида $a+ib\sqrt{3}$, где a и b — либо оба целые, либо оба половины нечетных целых чисел. Пусть $\mathcal{K}$ — подкольцо поля комплексных чисел с основным множеством K. Докажите, что кольцо $\mathcal{K}$ является евклидовым.

7. Докажите, что элемент p кольца главных идеалов $\mathcal{K}$ простой тогда и только тогда, когда фактор-кольцо $\mathcal{K}/(p)$ является областью целостности.

8. Пусть $\mathbf{Z}[\sqrt{2}]=\{m+n\sqrt{2} \mid m,\ n\in \mathbf{Z}\}$ и $\mathbb{Z}[\sqrt{2}]$ — подкольцо поля действительных чисел с основным множеством $\mathbf{Z}[\sqrt{2}]$. Докажите, что кольцо $\mathbb{Z}[\sqrt{2}]$ является евклидовым.

§ 4. НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ. НАИМЕНЬШЕЕ ОБЩЕЕ КРАТНОЕ

Наибольший общий делитель. Пусть $\mathcal{K}$ — коммутативное кольцо. Элемент c называется *общим делителем элементов* $a_1, \ldots, a_m$ кольца $\mathcal{K}$, если c является делителем (в $\mathcal{K}$) каждого из этих элементов.

ОПРЕДЕЛЕНИЕ. *Наибольшим общим делителем элементов* $a_1, \ldots, a_m$ кольца $\mathcal{K}$ называется такой их общий делитель, который делится на любой общий делитель этих элементов.

Наибольший общий делитель элементов $a_1, \ldots, a_n$ обозначается через НОД $(a_1, \ldots, a_n)$.

Из данного определения непосредственно вытекает следующее предложение.

ПРЕДЛОЖЕНИЕ 4.1. *Если d наибольший общий делитель элементов $a_1, \ldots, a_n$ в $\mathcal{K}$, то множество всех общих делителей элементов $a_1, \ldots, a_n$ совпадает с множеством всех делителей элемента d.*

ОПРЕДЕЛЕНИЕ. Элементы a и b кольца $\mathcal{K}$ называются *взаимно простыми*, если единица (делитель единицы) кольца $\mathcal{K}$ является их наибольшим общим делителем в $\mathcal{K}$.

Ниже рассматриваются свойства наибольшего общего делителя в кольце главных идеалов. Предложение 4.2 имеет место в любом коммутативном кольце.

ПРЕДЛОЖЕНИЕ 4.2. *Любые два наибольших общих делителя элементов* $a_1, \ldots, a_n$ *кольца* $\mathcal{K}$ *ассоциированы в* $\mathcal{K}$. *Если* c *есть наибольший общий делитель элементов* $a_1, \ldots, a_n$ *и* c *ассоциировано с* d, *то* d *также является наибольшим общим делителем этих элементов.*

Это свойство непосредственно следует из определения наибольшего общего делителя.

ПРЕДЛОЖЕНИЕ 4.3. *Для любого набора* $a_1, \ldots, a_n$ *элементов кольца главных идеалов* $\mathcal{K}$ *существует наибольший общий делитель в* $\mathcal{K}$. *Элемент* d *является наибольшим общим делителем элементов* $a_1, \ldots, a_n$ *тогда и только тогда, когда* $(a_1, \ldots, a_n) = (d)$.

Доказательство. Предположим, что

(1) $(a_1, \ldots, a_n) = (d)$,

и докажем, что d есть НОД$(a_1, \ldots, a_n)$. Из условия (1) следует, что d есть общий делитель элементов $a_1, \ldots, a_n$ и

(2) $d = \lambda_1 a_1 + \ldots + \lambda_n a_n$, где $\lambda_1, \ldots, \lambda_n \in K$.

Кроме того, в силу (2), если c есть общий делитель $a_1, \ldots, a_n$, то c делит d. Следовательно, d есть НОД$(a_1, \ldots, a_n)$.

Предположим теперь, что d есть НОД$(a_1, \ldots, a_n)$, и докажем, что тогда $(a_1, \ldots, a_n) = (d)$. Так как $\mathcal{K}$ — кольцо главных идеалов, то существует в K такой элемент c, что $(a_1, \ldots, a_n) = (c)$. По только что доказанному, c есть НОД$(a_1, \ldots, a_n)$. В силу предложения 4.2 отсюда следует, что c и d ассоциированы и, значит, по теореме 3.8, $(c) = (d)$. Следовательно, $(a_1, \ldots, a_n) = (d)$. □

ТЕОРЕМА 4.4. *Пусть* d — *общий делитель элементов* $a_1, \ldots, a_n$ *кольца главных идеалов* $\mathcal{K}$. *Элемент* d *есть* НОД$(a_1, \ldots, a_n)$ *тогда и только тогда, когда его можно представить в виде* $d = \lambda_1 a_1 + \ldots + \lambda_n a_n$, *где* $\lambda_1, \ldots, \lambda_n \in K$.

Доказательство. Пусть d есть НОД$(a_1, \ldots, a_n)$. Тогда, по предложению 4.3, $(d) = (a_1, \ldots, a_n)$. Поэтому d можно представить в виде $d = \lambda_1 a_1 + \ldots + \lambda_n a_n$, где $\lambda_1, \ldots, \lambda_n \in K$.

Предположим теперь, что d можно представить в виде $d = \lambda_1 a_1 + \ldots + \lambda_n a_n$, $\lambda_i \in K$. Тогда любой общий делитель c элементов $a_1, \ldots, a_n$ делит сумму $\lambda_1 a_1 + \ldots + \lambda_n a_n$, т. е.

делит d. Следовательно, d есть наибольший общий делитель элементов $a_1, \ldots, a_n$. □

ПРЕДЛОЖЕНИЕ 4.5. *Для любых элементов $a_1, \ldots, a_n$ с кольца главных идеалов $\mathcal{K}$ имеем*

$$\text{НОД}(ca_1, \ldots, ca_n) \sim c \cdot \text{НОД}(a_1, \ldots, a_n).$$

Доказательство. Пусть d есть НОД$(a_1, \ldots, a_n)$. По теореме 4.4, в K существуют элементы $\lambda_1, \ldots, \lambda_n$ такие, что $d = \lambda_1 a_1 + \ldots + \lambda_n a_n$. Поэтому $cd = \lambda_1 (ca_1) + \ldots + \lambda_n (ca_n)$. Кроме того, так как d — общий делитель $a_1, \ldots, a_n$, то cd есть общий делитель $ca_1, \ldots, ca_n$. Следовательно, по теореме 4.4, cd является наибольшим общим делителем элементов $ca_1, \ldots, ca_n$. □

ПРЕДЛОЖЕНИЕ 4.6. *Если d — наибольший общий делитель элементов a и b в кольце главных идеалов $\mathcal{K}$ и $d \neq 0$, то элементы a/d и b/d — взаимно простые.*

Доказательство. По условию, НОД$(a, b) = d \neq 0$. По теореме 4.4, отсюда следует, что $\lambda_1 a + \lambda_2 b = d$ для некоторых $\lambda_1, \lambda_2 \in K$; поэтому $\lambda_1 \frac{a}{d} + \lambda_2 \frac{b}{d} = 1$. По теореме 4.4, отсюда следует, что 1 есть наибольший общий делитель элементов a/d и b/d, т. е. элементы a/d и b/d — взаимно простые. □

Очевидно, предложение 4.6 можно обобщить следующим образом: если d — наибольший общий делитель элементов $a_1, \ldots, a_n$ в кольце главных идеалов $\mathcal{K}$ и $d \neq 0$, то 1 есть наибольший общий делитель элементов $a_1/d, \ldots, an/d$.

ТЕОРЕМА 4.7. *Если в кольце главных идеалов a делит bc и элементы a, b — взаимно простые, то a делит c.*

Доказательство. По условию, НОД$(a, b) = 1$. По теореме 4.4, отсюда следует, что $\lambda_1 a + \lambda_2 b = 1$ для некоторых $\lambda_1, \lambda_2 \in K$. Умножив обе части равенства на c, получим $\lambda_1 ac + \lambda_2 bc = c$. Так как, по условию, a делит bc, то a делит $\lambda_1 ac + \lambda_2 bc$ и, значит, a делит c. □

Наименьшее общее кратное. Пусть $\mathcal{K}$ — кольцо главных идеалов. Элемент c называется *общим кратным элементов* $a_1, \ldots, a_n$ кольца $\mathcal{K}$, если c делится в $\mathcal{K}$ на каждый из этих элементов.

ОПРЕДЕЛЕНИЕ. *Наименьшим общим кратным элементов* $a_1, \ldots, a_n$ кольца $\mathcal{K}$ называется такое их общее кратное, которое делит любое общее кратное этих элементов.

Наименьшее общее кратное элементов $a_1, \ldots, a_n$ кольца $\mathcal{K}$ обозначается через НОК$(a_1, \ldots, a_n)$.

Из данного определения непосредственно вытекает следующее предложение.

ПРЕДЛОЖЕНИЕ 4.8. *Если m есть наименьшее общее кратное элементов $a_1, \ldots, a_n$ кольца $\mathcal{K}$, то множество всех общих кратных элементов $a_1, \ldots, a_n$ совпадает с множеством всех кратных элемента m.*

Рассмотрим свойства наименьшего общего кратного в кольце главных идеалов $\mathcal{K}$. Предложение 4.9 имеет место в любом коммутативном кольце.

ПРЕДЛОЖЕНИЕ 4.9. *Любые два наименьших общих кратных элементов $a_1, \ldots, a_n$ кольца $\mathcal{K}$ ассоциированы в $\mathcal{K}$. Если m — наименьшее общее кратное элементов $a_1, \ldots, a_n$ и m ассоциировано с m', то m' также является наименьшим общим кратным элементов $a_1, \ldots, a_n$.*

Это предложение непосредственно следует из определения наименьшего общего кратного.

ПРЕДЛОЖЕНИЕ 4.10. *Элемент m является наименьшим общим кратным элементов кольца $\mathcal{K}$ тогда и только тогда, когда*

$$(a_1) \cap (a_2) \cap \ldots \cap (a_n) = (m).$$

Доказательство. Предположим, что

(1) $(a_1) \cap \ldots \cap (a_n) = (m)$.

Тогда m является общим кратным элементов $a_1, \ldots, a_n$. Кроме того, если m' есть общее кратное элементов $a_1, \ldots, a_n$, то

$$m' \in (a_1), \ldots, m' \in (a_n), \text{ т. е. } m' \in (a_1) \cap \ldots \cap (a_n) = (m)$$

и, значит, m' кратно m. Следовательно, m является наименьшим общим кратным элементов $a_1, \ldots, a_n$.

Предположим, что m есть НОК$(a_1, \ldots, a_n)$. Поскольку $\mathcal{K}$ — кольцо главных идеалов, то существует в K такой элемент m_1, что

$$(a_1) \cap \ldots \cap (a_n) = (m_1).$$

По только что доказанному, m_1 является наименьшим общим кратным элементов $a_1, \ldots, a_n$. По предложению 4.9, m_1 ассоциировано с m. Следовательно,

$$(m_1) = (m) \text{ и } (a_1) \cap \ldots \cap (a_n) = (m). \quad \square$$

СЛЕДСТВИЕ 4.11. *Для любого набора $a_1, \ldots, a_n$ элементов кольца $\mathcal{K}$ существует наименьшее общее кратное в $\mathcal{K}$.*

ПРЕДЛОЖЕНИЕ 4.12. *Для любых элементов a, b, c кольца $\mathscr{K}$*

$$\text{НОК}(ac,\ bc) \sim c \cdot \text{НОК}(a,\ b).$$

Доказательство. Пусть m есть НОК(a, b). Надо доказать, что mc есть НОК(ac, bc). Это, очевидно, верно при $c=0$. Предположим, что $c \neq 0$. Так как m — общее кратное a и b, то mc является общим кратным ac и bc. Пусть m' — любое общее кратное элементов ac и bc, т. е. (2) $m' = kac$, $m' = sbc$, где $k, s \in K$.
Поскольку $\mathscr{K}$ — область целостности и $c \neq 0$, из $kac = sbc$ следует $ka = sb$. Поэтому ka кратно m, т. е. $ka = rm$, где $r \in K$. Следовательно, в силу (2) $m' = rmc$ и, значит, m' кратно mc. Таким образом, mc есть НОК(ac, bc) и, по предложению 4.9, НОК$(ac, bc) \sim cm$. □

ПРЕДЛОЖЕНИЕ 4.13. *Если a и b — взаимно простые элементы кольца $\mathscr{K}$, то ab является наименьшим общим кратным элементов a, b.*

Доказательство. Пусть m — любое общее кратное a и b. Докажем, что m кратно ab. Так как m кратно b, то $m = bc$, где $c \in K$. Поскольку a делит m и, по условию, a и b — взаимно простые в $\mathscr{K}$, то a делит c (см. теорему 4.7). Поэтому ab делит bc и, значит, m кратно ab. Следовательно, ab является наименьшим общим кратным элементов a, b. □

ПРЕДЛОЖЕНИЕ 4.14. *Если a, b — ненулевые элементы кольца $\mathscr{K}$, то* $\text{НОК}(a,\ b) \sim \dfrac{ab}{\text{НОД}(a,\ b)}$.

Доказательство. Пусть d есть НОД(a, b) в $\mathscr{K}$. Так как a, b — ненулевые элементы, то $d \neq 0$. По предложению 4.12,

$$(1)\quad \text{НОК}(a,\ b) \sim d \cdot \text{НОК}\left(\frac{a}{d},\ \frac{b}{d}\right).$$

В силу предложения 4.6 $\text{НОД}\left(\dfrac{a}{d},\ \dfrac{b}{d}\right) = 1$, т. е. элементы $\dfrac{a}{d}$ и $\dfrac{b}{d}$ — взаимно простые. Отсюда, по предложению 4.13, следует, что

$$(2)\quad \text{НОК}\left(\frac{a}{d},\ \frac{b}{d}\right) = \frac{a}{d} \cdot \frac{b}{d}.$$

На основании (1) и (2) заключаем, что $\text{НОК}(a,\ b) \sim \dfrac{ab}{d}$. □

ТЕОРЕМА 4.15. *Пусть* $a = u \cdot p_1^{\alpha_1} \dots p_m^{\alpha_m}$, $b = v \cdot p_1^{\beta_1} \dots p_m^{\beta_m}$, *где* $p_1, \dots, p_m$ — *попарно различные неприводимые элементы факториального кольца* $\mathcal{K}$, a *и,* v — *обратимые элементы кольца. Тогда имеем*:

(1) $\text{НОК}(a, b) = p_1^{\gamma_1} \dots p_m^{\gamma_m}$, где $\gamma_i = \max(\alpha_i, \beta_i)$:

(2) $\text{НОД}(a, b) = p_1^{\delta_1} \dots p_m^{\delta_m}$, где $\delta_i = \min(\alpha_i, \beta_i)$.

Доказательство формулы (1) аналогично доказательству предложения 11.3.8. Доказательство формулы (2) аналогично доказательству предложения 11.3.1.

Упражнения

1. Докажите теорему 4.15.

2. Докажите, что теорема 4.7 и предложение 4.6 верны для любого факториального кольца $\mathcal{K}$.

3. Покажите, что предложения 4.10—4.14 верны для любого факториального кольца $\mathcal{K}$.

4. Пусть a, b, c — элементы факториального кольца, $\text{НОД}(a, c) \sim 1$ и $\text{НОД}(b, c) \sim 1$. Докажите, что $\text{НОД}(ab, c) \sim 1$.

5. Пусть a, b, c — элементы факториального кольца. Докажите, что $\text{НОК}(a, \text{НОД}(b, c)) \sim \text{НОД}(\text{НОК}(a, b), \text{НОК}(a, c))$.

Глава четырнадцатая
ПОЛИНОМЫ ОТ ОДНОЙ ПЕРЕМЕННОЙ

§ 1. КОЛЬЦО ПОЛИНОМОВ

Простое трансцендентное расширение кольца. Пусть $\mathscr{K}$ и $\mathscr{L}$ — коммутативные кольца с основными множествами K и L соответственно.

ОПРЕДЕЛЕНИЕ. Кольцо $\mathscr{L}$ называется *простым расширением кольца* $\mathscr{K}$ с помощью элемента u, если выполняются условия:

(1) $\mathscr{K}$ — подкольцо кольца $\mathscr{L}$;

(2) любой элемент a из L можно представить в виде $a=\alpha_0+\alpha_1 u+\ldots+\alpha_n u^n$, где $\alpha_0, \alpha_1, \ldots, \alpha_n \in K$.

Запись $\mathscr{L}=\mathscr{K}[u]$ означает, что кольцо $\mathscr{L}$ есть простое расширение кольца $\mathscr{K}$ с помощью элемента u. В этом случае основное множество кольца $\mathscr{L}$ обозначают также через $K[u]$, $L=K[u]$.

ОПРЕДЕЛЕНИЕ. Кольцо $\mathscr{L}=\mathscr{K}[u]$ называется *простым трансцендентным расширением кольца* $\mathscr{K}$, если выполняется следующее условие:

(3) для любых элементов $\alpha_0, \alpha_1, \ldots, \alpha_n$ множества K из равенства $\alpha_0+\alpha_1 u+\ldots+\alpha_n u^n=0$ следуют равенства $\alpha_0=0, \alpha_1=0, \ldots, \alpha_n=0$.

Если $\mathscr{L}=\mathscr{K}[u]$ — простое расширение кольца $\mathscr{K}$ с помощью u и u удовлетворяет условиям (3), то элемент u называется *трансцендентным относительно* $\mathscr{K}$.

Если $\mathscr{K}[u]$ — простое трансцендентное расширение кольца $\mathscr{K}$ с помощью u, то кольцо $\mathscr{K}[u]$ называется также *кольцом полиномов от и над* $\mathscr{K}$, а элементы кольца $\mathscr{K}[u]$ — *полиномами от и над* $\mathscr{K}$ или *полиномами над* $\mathscr{K}$.

ПРЕДЛОЖЕНИЕ 1.1. *Пусть* $\mathscr{K}[u]$ — *простое трансцендентное расширение кольца* $\mathscr{K}$ *при помощи* u. *Тогда для любого элемента* a *кольца* $\mathscr{K}[u]$, *если* $a=a_0+a_1 u+\ldots+a_n u^n$ *и* $a=a'_0+a'_1 u+\ldots+a'_n u^n$, *где* $a_i, a'_i \in K$, *то* $a_i=a'_i$ *для* $i=1, \ldots, n$.

Доказательство. Если

$$a = a_0 + a_1 u + \ldots + a_n u^n = a_0' + a_1' u + \ldots + a_n' u^n \qquad (a_i,\ a_i' \in K),$$

то

$$(1)\quad a_0 - a_0' + (a_1 - a_1')\, u + \ldots + (a_n - a_n')\, u^n = 0.$$

По условию, элемент u является трансцендентным относительно $\mathscr{K}$. Поэтому из (1) следуют равенства $a_i - a_i' = 0$ и $a_i = a_i'$ для $i = 0, 1, \ldots, n$. □

ТЕОРЕМА 1.2. *Пусть $\mathscr{K}$ и $\mathscr{L}$ — коммутативные кольца, φ — изоморфизм $\mathscr{K}$ на $\mathscr{L}$, а $\mathscr{K}[x]$ и $\mathscr{L}[y]$ — простые трансцендентные расширения колец $\mathscr{K}$ и $\mathscr{L}$ соответственно. Тогда $\mathscr{K}[x] \cong \mathscr{L}[y]$, причем существует единственный изоморфизм кольца $\mathscr{K}[x]$ на кольцо $\mathscr{L}[y]$, переводящий x в y и продолжающий изоморфизм φ кольца $\mathscr{K}$ на $\mathscr{L}$.*

Доказательство. Обозначим через ψ отображение кольца $\mathscr{K}[x]$ в кольцо $\mathscr{L}[y]$, определяемое следующим образом: для любого $a = a_0 + \ldots + a_m x^m$ из $K[x]$

$$\psi(a_0 + \ldots + a_m x^m) = \varphi(a_0) + \ldots + \varphi(a_m)\, y^m.$$

Нетрудно видеть, что ψ удовлетворяет условиям: $\psi(a_0) = \varphi(a_0)$ для любого a_0 из K, $\psi(x) = y$ и $\operatorname{Im}\psi = L[y]$.

Кроме того, ψ сохраняет главные операции кольца $\mathscr{K}[x]$. Действительно, если $a = a_0 + \ldots + a_m x^m$ и $b = b_0 + \ldots + b_n x^n$ $(m \leqslant n)$, $a,\ b \in K[x]$, то

$$\begin{aligned}\psi(a+b) &= \psi((a_0 + b_0) + \ldots + (a_m + b_m)\, x^m + b_{m+1} x^{m+1} + \ldots \\ &\qquad \ldots + b_{n-1} x^{n-1} + b_n x^n) = \\ &= \varphi(a_0 + b_0) + \ldots + \varphi(a_m + b_m)\, y^m + \\ &\quad + \varphi(b_{m+1}) y^{m+1} + \ldots + \varphi(b_{n-1})\, y^{n-1} + \varphi(b_n)\, y^n = \\ &= (\varphi(a_0) + \ldots + \varphi(a_m)\, y^m) + (\varphi(b_0) + \ldots \\ &\qquad \ldots + \varphi(b_n)\, y^n) = \psi(a) + \psi(b).\end{aligned}$$

Аналогично можно показать, что

$$\psi(-a) = -\psi(a), \quad \psi(ab) = \psi(a)\psi(b), \quad \psi(1_{\mathscr{K}}) = 1_{\mathscr{L}}.$$

Следовательно, ψ есть изоморфизм $\mathscr{K}[x]$ на $\mathscr{L}[y]$, переводящий x в y и продолжающий изоморфизм φ.

Докажем, что существует единственный изоморфизм с указанными свойствами. Допустим, что ψ_1 — другой изоморфизм кольца $\mathscr{K}[x]$ на кольцо $\mathscr{L}[y]$ такой, что $\psi_1(a_0) =$

$= \varphi(a_0)$ для любого a_0 из K и $\psi_1(x) = y$. Тогда для любого $a = a_0 + \ldots + a_m x^m$ из $K[x]$

$$\psi_1(a) = \psi_1(a_0) + \ldots + \psi_1(a_m)\,\psi_1(x^m) = \varphi(a_0) + \varphi(a_1)\,y + \ldots$$
$$\ldots + \varphi(a_m)\,y^m = \psi(a);$$

таким образом, $\psi_1 = \psi$. □

СЛЕДСТВИЕ. *Пусть $\mathscr{K}[x]$ и $\mathscr{K}[y]$ — два простых трансцендентных расширения коммутативного кольца $\mathscr{K}$. Тогда $\mathscr{K}[x] \cong \mathscr{K}[y]$, причем существует единственный изоморфизм кольца $\mathscr{K}[x]$ на кольцо $\mathscr{K}[y]$, переводящий x в y и индуцирующий тождественное отображение на K.*

Теорема о существовании простого трансцендентного расширения коммутативного кольца. Пусть $\mathscr{K}$ — ненулевое коммутативное кольцо. Бесконечная последовательность $a = (a_0, a_1, \ldots,)$ элементов из K, у которой все члены a_i, кроме конечного их числа, равны нулю, называется *псевдобесконечной последовательностью над $\mathscr{K}$*. Для всякой псевдобесконечной последовательности a существует такое натуральное число n, что $a_i = 0$ для всех $i \geqslant n$. Множество всех псевдобесконечных последовательностей над $\mathscr{K}$ обозначим через L_1.

На множестве L_1 введем отношение равенства, считая, что $(a_0, a_1, \ldots) = (b_0, b_1, \ldots)$ тогда и только тогда, когда $a_i = b_i$ для любого натурального числа i.

Сумма любых двух элементов $a = (a_0, a_1, \ldots)$ и $b = (b_0, b_1, \ldots)$ определяется равенством

$$a \oplus b = (a_0 + b_0,\ a_1 + b_1,\ \ldots).$$

Ниже через $(a \oplus b)_i$ будем обозначать i-ю компоненту суммы $a + b$.

Произведение элемента λ из K на элемент a из L_1 определяется формулой $\lambda a = (\lambda a_0, \lambda a_1, \ldots)$. В частности, полагаем $\ominus a = (-1)a = (-a_0, -a_1, \ldots)$.

Сложение в L_1 коммутативно, ассоциативно, обладает нейтральным элементом $\bar{0} = (0, 0, \ldots)$ и для каждого a из L_1 элемент $\ominus a$ является противоположным, т. е. $a \oplus (\ominus a) = \bar{0}$. Следовательно, алгебра $\langle L_1, \oplus, \ominus \rangle$ является коммутативной группой.

Произведение любых двух элементов $a = (a_0, a_1, \ldots)$ и $b = (b_0, b_1, \ldots)$ из L_1 определяется формулой

$$(a_0, a_1, \ldots) \odot (b_0, b_1, \ldots) = (c_0, c_1, \ldots),$$

где $c_k \sum_{i+j=k} a_i b_j$ для любого натурального числа k. Ниже через $(a \odot b)_k$ будем обозначать k-ю компоненту произведения ab.

Таким образом, на множестве L_1 определены две бинарные операции (сложение $\oplus$ и умножение $\odot$) и унарная операция $\ominus$, ставящая в соответствие каждому a из L_1 противоположный элемент $\ominus a$. Всюду ниже 1 — единица кольца $\mathscr{K}$, $1 = 1_{\mathscr{K}}$ и $\bar{1} = (1, 0, 0, \ldots)$.

ЛЕММА 1.3. *Алгебра* $\mathscr{L}_1 = \langle L_1, \oplus, \ominus, \odot, \bar{1} \rangle$ *является коммутативным кольцом.*

Доказательство. Выше было установлено, что алгебра $\langle L_1, \oplus, \ominus \rangle$ есть абелева группа. Из определения умножения в L_1 непосредственно следует, что оно коммутативно. Умножение в L_1 ассоциативно. В самом деле, для любых a, b, c из L_1

$$(a \odot (b \odot c))_l = \sum_{j+s=i} a_j (b \cdot c)_s = \sum_{j+s=i} a_j \left(\sum_{k+l=s} b_k c_l \right) = \sum_{j+k+l=i} a_j b_k c_l,$$

$$((a \odot b) \odot c)_l = \sum_{t+l=i} (ab)_t c_l = \sum_{t+l=i} \left(\sum_{j+k=t} a_j b_k \right) c_l = \sum_{j+k+l=i} a_j b_k c_l.$$

Следовательно, $a \odot (b \odot c) = (a \odot b) \odot c$.

Умножение в L_1 дистрибутивно относительно сложения. В самом деле, для любых a, b, c из L_1

$$((a \oplus b) \odot c)_i = \sum_{j+k=i} (a \oplus b)_j c_k = \sum_{j+k=i} (a_j c_k + b_j c_k),$$

$$(a \odot c \oplus b \odot c)_i = (a \odot c)_i \oplus (b \odot c)_i = \sum_{j+k=i} a_j c_k + \sum_{j+k=i} b_j c_k = \sum_{j+k=i} (a_j c_k + b_j c_k).$$

Следовательно, $(a \oplus b) \odot c = a \odot c \oplus b \odot c$. Кроме того, $\bar{1}$ является нейтральным элементом относительно умножения в L_1.

Итак, установлено, что алгебра $\mathscr{L}_1$ является коммутативным кольцом. □

Положим

$$u_0=(1,\ 0,\ 0,\ \ldots),\ u_1=(0,\ 1,\ 0,\ 0,\ \ldots),\ \ldots,\ u_k=$$
$$=(\underbrace{0,\ \ldots,\ 0}_{k\text{ нулей}},\ 1,\ 0,\ \ldots).$$

Всякий элемент $a=(a_0,\ a_1,\ \ldots)$ из L_1 можно записать в виде

$$a=a_0(1,\ 0,\ 0,\ \ldots)\oplus a_1(0,\ 1,\ 0,\ \ldots)\oplus\ldots$$
$$\ldots\oplus a_n(0,\ \ldots,\ 0,\ 1,\ 0,\ \ldots)=a_0u_0\oplus a_1u_1\oplus\ldots\oplus a_nu_n,$$

т. е.

$$a=a_0u_0\oplus a_1u_1\oplus\ldots\oplus a_nu_n,$$

где n — такое натуральное число, что $a_i=0$ для всякого $i>n$.

Для любого натурального n система элементов $u_0,\ u_1,\ \ldots,\ u_n$ линейно независима над $\mathscr{K}$, т. е. для любых элементов $\lambda_0,\ \lambda_1,\ \ldots,\ \lambda_n$ множества K из равенства

(1) $\lambda_0u_0\oplus\lambda_1u_1\oplus\ldots\oplus\lambda_nu_n=\bar{0}$

следуют равенства $\lambda_0=0,\ \lambda_1=0,\ \ldots,\ \lambda_n=0$.

В самом деле, из (1) следует

$$\lambda_0u_0+\lambda_1u_1+\ldots+\lambda_nu_n=(\lambda_0,\ \lambda_1,\ \ldots,\ \lambda_n,\ 0,\ 0,\ \ldots)=$$
$$=(0,\ 0,\ 0,\ \ldots),$$

поэтому $\lambda_0=0,\ \lambda_1=0,\ \ldots,\ \lambda_n=0$.

Положим $x=u_1=(0,\ 1,\ 0,\ 0,\ \ldots)$. Из определения умножения в L_1 следует, что

$$x^2=u_2,\ x^3=u_2\odot u_1=u_3,\ \ldots,\ x^n=u_{n-1}\odot u_1=u_n.$$

Следовательно, всякий элемент a из L_1, для которого $a_i=0$ при любом $i>n$, можно представить в виде

$$a=a_0u_0\oplus a_1u_1\oplus\ldots\oplus a_nu_n=a_0u_0\oplus a_1x\oplus\ldots\oplus a_nx^n.$$

ТЕОРЕМА 1.4. *Для каждого ненулевого коммутативного кольца* $\mathscr{K}=\langle K,\ +,\ -,\ \cdot,\ 1\rangle$ *существует простое трансцендентное расширение.*

Доказательство. Пусть L_1 — множество всех псевдобесконечных последовательностей над $\mathscr{K}$. По лемме 1.3, алгебра

$$\mathscr{L}_1=\langle L_1,\ \oplus,\ \ominus,\ \odot,\ \bar{1}\rangle$$

является коммутативным кольцом. Множество

$$K_1 = \{a_0 u_0 \mid a_0 \in K\}, \text{ где } a_0 u_0 = \{a_0, 0, 0, \ldots\},$$

замкнуто в кольце $\mathscr{L}_1$ и не пусто. Следовательно, алгебра

$$\mathscr{K}_1 = \langle K, \oplus, \ominus, \odot, \bar{1} \rangle$$

является подкольцом кольца $\mathscr{L}_1$. Отображение h_1: $K_1 \to K$ такое, что

$$h_1(a_0 u_0) = a_0 \text{ для каждого } a_0 \text{ из } K,$$

очевидно, есть инъективное отображение множества K_1 на K. Кроме того, h_1 сохраняет главные операции кольца $\mathscr{K}_1$, так как для любых a_0, b_0 из K

$$h_1(a_0 u_0 \oplus b_0 u_0) = a_0 + b_0,$$
$$h_1(\ominus a_0 u_0) = -a_0,$$
$$h_1(a_0 u_0 \odot b_0 u_0) = a_0 \cdot b_0,$$
$$h_1(1 \odot u_0) = 1 \quad \text{(т. е. } h_1(\bar{1}) = 1_{\mathscr{K}}).$$

Следовательно, h_1 является изоморфизмом кольца $\mathscr{K}_1$ на $\mathscr{K}$. Таким образом, $\mathscr{L}_1$ содержит подкольцо $\mathscr{K}_1$, изоморфное кольцу $\mathscr{K}$.

Нам надо по кольцу $\mathscr{L}_1$ построить новое кольцо, изоморфное $\mathscr{L}_1$ и содержащее подкольцо $\mathscr{K}$. Для этого заменим в множестве L_1 каждый элемент $a_0 u_0$ из K_1 элементом a_0 из K (т. е. заменим $a_0 u_0$ элементом $h_1(a_0 u_0)$), оставляя все остальные элементы множества L_1 неизменными. Положим

$$L = (L_1 \setminus K_1) \cup K$$

и определим отображение h: $L_1 \to L$ следующим образом:

$$h(a) = \begin{cases} h_1(a), & \text{если } a \in K_1, \\ a, & \text{если } a \in L_1 \setminus K_1. \end{cases}$$

Нетрудно видеть, что h является инъективным отображением множества L_1 на L, продолжающим отображение h_1, т. е. $h_1 \subset h$.

На множестве L определим операции $+$, $-$, $\cdot$, 1 формулами

$$\text{(I)} \quad \begin{aligned} &\alpha + \beta = h(h^{-1}(\alpha) \oplus h^{-1}(\beta)) \quad (\alpha, \beta \in L); \\ &-\alpha = h(\ominus h^{-1}(\alpha)); \\ &\alpha \cdot \beta = h(h^{-1}(\alpha) \odot h^{-1}(\beta)); \\ &1 = h(\bar{1}) = 1_{\mathscr{K}}. \end{aligned}$$

Рассмотрим алгебру $\mathscr{L} = \langle L, \dotplus, \dot{-}, \cdot, 1\rangle$. Из формул (I) следуют формулы

$$\text{(II)}\quad \begin{aligned} &h^{-1}(\alpha \dotplus \beta) = h^{-1}(\alpha) \oplus h^{-1}(\beta);\\ &h^{-1}(\dot{-}\alpha) = \ominus h^{-1}(\alpha);\\ &h^{-1}(\alpha \cdot \beta) = h^{-1}(\alpha) \odot h^{-1}(\beta);\\ &h^{-1}(1) = \bar{1} \end{aligned}$$

Формулы (II) показывают, что h^{-1} есть изоморфизм алгебры $\mathscr{L}$ на кольцо $\mathscr{L}_1$. Отсюда следует, что алгебра $\mathscr{L}$ является коммутативным кольцом, изоморфным кольцу $\mathscr{L}_1$. Главные операции в кольце $\mathscr{L}$ являются продолжениями соответствующих операций в кольце $\mathscr{K}$. В самом деле, в силу (I) для любых α и β из K имеем:

$$\begin{aligned} \alpha \dotplus \beta &= h(h^{-1}(\alpha) \oplus h^{-1}(\beta)) = h(\alpha u_0 \oplus \beta u_0) =\\ &= h(\alpha u_0) \dotplus h(\beta u_0) = h_1(\alpha u_0) \dotplus h_1(\beta u_0) = \alpha \dotplus \beta;\\ \dot{-}\alpha &= h(\ominus h^{-1}(\alpha)) = h(\ominus \alpha u_0) = \dot{-} h(\alpha u_0) =\\ &= \dot{-} h_1(\alpha u_0) = \dot{-}\alpha;\\ \alpha \cdot \beta &= h(h^{-1}(\alpha) \odot h^{-1}(\beta)) = h(\alpha u_0 \odot \beta u_0) =\\ &= h(\alpha u_0) \cdot h(\beta u_0) = h_1(\alpha u_0) \cdot h_1(\beta u_0) = \alpha\beta. \end{aligned}$$

Следовательно, $\mathscr{K}$ является подкольцом кольца $\mathscr{L}$.

Любой элемент из $\mathscr{L}$ можно представить в виде линейной комбинации элементов $1, x, x^2, \ldots$ с коэффициентами из K, так как

$$\begin{aligned} h(a_0u_0 \oplus \ldots \oplus a_nu_n) &= a_0 \dotplus a_1u_1 \dotplus \ldots \dotplus a_nu_n =\\ &= a_0 \dotplus a_1x \dotplus \ldots \dotplus a_nx^n \quad (a_i \in K). \end{aligned}$$

Следовательно, $\mathscr{L} = \mathscr{K}[x]$.

Элемент x является трансцендентным относительно $\mathscr{K}$. В самом деле, равенство

$$a_0 \dotplus a_1x \dotplus \ldots \dotplus a_nx^n = 0$$

влечет равенство

$$h^{-1}(a_0 \dotplus a_1x \dotplus \ldots \dotplus a_nx^n) = a_0u_0 \oplus a_1u_1 \oplus \ldots \oplus a_nu_n = \bar{0}.$$

Поскольку элементы $u_0, \ldots, u_n$ линейно независимы над $\mathscr{K}_1$, отсюда следует, что $a_0 = 0$, $a_1 = 0$, $\ldots$, $a_n = 0$. Следовательно, x есть трансцендентный элемент относительно $\mathscr{K}$ и кольцо $\mathscr{L} = \mathscr{K}[x]$ является трансцендентным расширением кольца $\mathscr{K}$ с помощью x. □

Степень полинома. Пусть $\mathscr{K}$ — ненулевое коммутативное кольцо и $\mathscr{K}[x]$ — кольцо полиномов от x, т. е. простое

трансцендентное расширение $\mathscr{K}$ с помощью x. Любой ненулевой элемент a из $K[x]$ можно единственным образом представить в виде линейной комбинации степеней x с коэффициентами из K.

ОПРЕДЕЛЕНИЕ. Пусть a — полином из $K[x]$. Натуральное число n называется *степенью полинома* a, если $a = a_0 + a_1x + \ldots + a_nx^n$, где $a_n \neq 0$. При этом a_0, a_1, ..., a_n называются *коэффициентами полинома*, элемент a_n — *старшим коэффициентом*. Полином a называется *нормированным*, если его старший коэффициент равен единице кольца $\mathscr{K}$.

Обозначать степень полинома a будем через $\deg a$.

Таким образом, степень определена для всех полиномов, кроме нулевого; степень нулевого полинома не определяется. Степень полинома a_0, где a_0 — ненулевой элемент кольца $\mathscr{K}$, равна нулю.

Отметим некоторые свойства степени полинома.

ПРЕДЛОЖЕНИЕ 1.5. *Степень суммы двух ненулевых полиномов не больше максимальной степени слагаемых*, т. е. $\deg(a+b) \leqslant \max(\deg a, \deg b)$.

ПРЕДЛОЖЕНИЕ 1.6. *Степень произведения двух ненулевых полиномов не больше суммы степеней сомножителей*, т. е. при $ab \neq 0$ $\deg(ab) \leqslant \deg a + \deg b$.

Доказательство предложений 1.5 и 1.6 предоставляется читателю.

ПРЕДЛОЖЕНИЕ 1.7. *Если $\mathscr{K}$ — область целостности, то степень произведения двух ненулевых полиномов равна сумме степеней сомножителей*, т. е. $\deg(ab) = \deg a + \deg b$.

Доказательство. Пусть $a = a_0 + \ldots + a_mx^m$, $b = b_0 + \ldots + b_nx^n$ — полиномы над областью целостности $\mathscr{K}$ и $a_m \neq 0$, $b_n \neq 0$. Тогда $ab = a_0b_0 + (a_0b_1 + a_1b_0)x + \ldots + a_mb_nx^{m+n}$. Так как $\mathscr{K}$ — область целостности, то $a_mb_n \neq 0$. Следовательно, $\deg(ab) = m + n = \deg a + \deg b$. □

ТЕОРЕМА 1.8. *Если $\mathscr{K}$ — область целостности, то кольцо полиномов $\mathscr{K}[x]$ также является областью целостности.*

Эта теорема непосредственно следует из предложения 1.7.

Из теорем 1.8 и 13.2.1 вытекает следующее следствие.

СЛЕДСТВИЕ 1.9. *Для кольца полиномов $\mathscr{K}[x]$ над областью целостности $\mathscr{K}$ существует поле частных.*

Деление полинома на двучлен и корни полинома. Пусть $\mathscr{K}[x]$ — кольцо полиномов от x над ненулевым коммутативным кольцом $\mathscr{K}$. Если $f = a_0 + a_1x + \ldots + a_nx^n \in K[x]$ и $c_0 \in K$, то сумму $a_0 + a_1c_0 + \ldots + a_nc_0^n$ будем

обозначать через $f(c_0)$ и называть *значением полинома для аргумента* c_0.

ТЕОРЕМА 1.10 (Безу). *Пусть* f *— полином над кольцом* $\mathscr{K}$ *и* $c_0 \in K$. *В кольце* $\mathscr{K}[x]$ *существует такой полином* q, *что* $f=(x-c_0)\,q+a(c_0)$.

Доказательство. Теорема верна, если f — нулевой полином; в этом случае $f(c_0)=0$ и можно положить $q=0$. Пусть $f=a_0+a_1x_1+\ldots+a_nx^n$ — ненулевой полином, тогда

$$f-f(c_0)=a_1(x-c_0)+a_2(x^2-c_0^2)+\ldots+a_n(x^n-c_0^n)=$$
$$=(x-c_0)\left[a_1+a_2(x+c_0)+\ldots+a_n\left(x^{n-1}+c_0x^{n-2}+\ldots+c_0^{n-1}\right)\right];$$

следовательно, $f=(x-c_0)\,q+f(c_0)$, где

$$q=a_1+a_2(x+c_0)+\ldots+a_n\left(x^{n-1}+\ldots+c_0^{n-1}\right)\in K[x]. \quad \square$$

Часто теорему Безу формулируют следующим образом: *остаток от деления полинома* f *из* $K[x]$, *где* $\mathscr{K}$ *— коммутативное кольцо, на двучлен* $(x-c_0)$, $(c_0 \in K)$, *равен* $f(c_0)$.

Пусть f — полином над кольцом $\mathscr{K}$ и $c_0 \in K$.

ОПРЕДЕЛЕНИЕ. Элемент c_0 кольца $\mathscr{K}$ называется *корнем полинома* f *над кольцом* $\mathscr{K}$, если $f(c_0)=0$.

ТЕОРЕМА 1.11. *Пусть* f *— полином над кольцом* $\mathscr{K}$ *и* $c_0 \in K$. *Элемент* c_0 *является корнем полинома* f *тогда и только тогда, когда* $x-c_0$ *делит полином* f *в кольце* $\mathscr{K}[x]$.

Доказательство. Пусть c_0 — корень полинома f, $f(c_0)=0$. По теореме Безу, $f=(x-c_0)\,q$, где $q \in K[x]$. Следовательно, $x-c_0$ делит полином f в $\mathscr{K}[x]$.

Предположим теперь, что $x-c_0$ делит полином f в $\mathscr{K}[x]$, т. е. $f=(x-c_0)\,g$, где $g \in K[x]$. Тогда $f(c_0)=(c_0-c_0)\,g(c_0)=0$. $\square$

Теорема о наибольшем возможном числе корней полинома в области целостности. Пусть $\mathscr{K}[x]$ — кольцо полиномов над кольцом $\mathscr{K}$.

ТЕОРЕМА 1.12. *Пусть* $\mathscr{K}$ *— область целостности. Любой полином из* $K[x]$ *степени* n *имеет не более* n *различных корней в* $\mathscr{K}$.

Доказательство проводится индукцией по n. Если $\deg f=0$, т. е. $f=a_0$, где $a_0 \in K$ и $a_0 \neq 0$, то полином f имеет нуль корней. Предположим, что любой полином из $K[x]$ степени n имеет не более n корней. Пусть $f \in K[x]$ и $\deg f=n+1$. Если f не имеет корней в $\mathscr{K}$, то теорема верна. Если же f имеет корни в $\mathscr{K}$, то $f(c_0)=0$ для некоторого элемента c_0 из K. По теореме Безу, $f=(x-c_0)g$, где $g \in K[x]$; при этом, поскольку $\mathscr{K}$ — область

целостности, в силу предложения 1.7 степень полинома g равна n. Элемент b_0 кольца $\mathscr{K}$, отличный от c_0, есть корень полинома f тогда и только тогда, когда $f(b_0) = (b_0 - c_0)g(b_0) = 0$, т. е. когда $g(b_0) = 0$, поскольку $\mathscr{K}$ — область целостности. Так как степень g равна n, то, по индуктивному предположению, g имеет не более n различных корней в $\mathscr{K}$. Следовательно, полином f степени $n+1$ имеет в $\mathscr{K}$ не более $n+1$ различных корней. □

СЛЕДСТВИЕ 1.13. *Если полином* $f = a_0 + \ldots + a_n x^n \in K[x]$ *имеет в области целостности* $\mathscr{K}$ *более чем* n *различных корней, то* f *является нулевым полиномом.*

Алгебраическое и функциональное равенства полиномов. Пусть $\mathscr{K}[x]$ — кольцо полиномов над областью целостности $\mathscr{K}$ и $f = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$. Обозначим через f^* функцию

$$\{\langle \lambda,\ a_0 + a_1\lambda + \ldots + a_n\lambda^n\rangle \mid \lambda \in K\},$$

ставящую в соответствие каждому λ из K элемент $f(\lambda) = a_0 + a_1\lambda + \ldots + a_n\lambda^n$, т. е. значение полинома f для аргумента λ. Для некоторых колец $\mathscr{K}$ различные полиномы могут определять одну и ту же функцию. Так, например, если $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ и $\mathbb{Z}_2[x]$ — кольцо полиномов над полем $\mathbb{Z}_2$, то полиномы $x + x^2$, $x - x^2$ и 0 определяют одну и ту же функцию.

ТЕОРЕМА 1.14. *Пусть* $\mathscr{K}[x]$ *— кольцо полиномов над бесконечной областью целостности* $\mathscr{K}$. *Полиномы* f *и* g *из* $K[x]$ *равны тогда и только тогда, когда равны определяемые ими функции* f^* *и* g^*.

Доказательство. Пусть f и g — полиномы из $K[x]$ и f^*, g^* — определяемые ими функции. Предположим, что $f = g$. Если f и g — нулевые полиномы, то $f^* = g^*$. Предположим, что f и g — ненулевые полиномы степени n:

$$f = a_0 + a_1 x + \ldots + a_n x^n,\ g(x) = b_0 + b_1 x + \ldots + b_n x^n.$$

Поскольку $f = g$, то

(1) $a_0 = b_0,\ \ldots,\ a_n = b_n$.

Для любого λ из K имеем:

$$f^*(\lambda) = a_0 + a_1\lambda + \ldots + a_n\lambda^n,\ g^*(\lambda) = b_0 + b_1\lambda + \ldots + b_n\lambda^n.$$

Следовательно, в силу (1) $f^* = g^*$.

Предположим теперь, что $f^* = g^*$, т. е. для любого λ из K

$$f(\lambda) = a_0 + a_1\lambda + \ldots + a_n\lambda^n = g(\lambda) = b_0 + b_1\lambda + \ldots + b_n\lambda^n.$$

Тогда для полинома $h=f-g$ выполняется условие

(2) $h(\lambda)=0$ для всякого λ из K.

Так как множество K бесконечно, то (2) означает, что полином h имеет бесконечное множество различных корней. По следствию 1.13, h — нулевой полином, т. е. $f-g=0$ и $f=g$. Таким образом, из $f^*=g^*$ следует $f=g$. □

Упражнения

1. Докажите предложения 1.5 и 1.6.

2. Пусть $\mathcal{F}[x]$ — кольцо полиномов над полем $\mathcal{F}$ и I — непустое множество из $F[x]$, замкнутое относительно вычитания и удовлетворяющее условиям: если $f\in I$, то $x\cdot f\in I$ и $\lambda f\in I$ для любого λ из F. Докажите, что множество I является идеалом кольца $\mathcal{F}[x]$.

3. Найдите все автоморфизмы кольца полиномов $\mathbb{Z}[x]$.

4. Найдите все автоморфизмы кольца полиномов $\mathbb{Q}[x]$.

5. Найдите все автоморфизмы кольца полиномов $\mathbb{R}[x]$.

6. Найдите все автоморфизмы кольца полиномов $\mathbb{C}[x]$ над полем $\mathbb{C}$ комплексных чисел.

7. Пусть $\mathbb{Z}[x]$ — кольцо полиномов над кольцом $\mathbb{Z}$ целых чисел. Покажите, что множество всех полиномов из $\mathbf{Z}[x]$ с четными свободными членами есть идеал кольца $\mathbb{Z}[x]$, не являющийся главным идеалом.

§ 2. ПОЛИНОМЫ НАД ПОЛЕМ

Теорема о делении с остатком. Пусть $\mathcal{F}[x]$ — кольцо полиномов над полем $\mathcal{F}$ и $F[x]$ — его основное множество.

ТЕОРЕМА 2.1. *Пусть h — ненулевой полином из $F[x]$. Для каждого полинома f из $F[x]$ существует в $F[x]$ единственная пара полиномов q и r таких, что*

(1) $f=h\cdot q+r$ и $\deg r<\deg h$ или $r=0$.

Доказательство. Сначала докажем индукцией по степени n полинома f существование полиномов q и r, удовлетворяющих условиям (1). Пусть

$$\deg h=m,\quad h=b_0+\ldots+b_mx^m\qquad (b_m\neq 0).$$

Отметим, что если f — нулевой полином или $\deg f<m$, то $f=h\cdot 0+f$ и, значит, можно положить $q=0$ и $r=f$. Поэтому нам остается рассмотреть случай, когда $\deg f\geqslant m$. Допустим, что теорема верна для любого полинома f степени меньшей, чем n. Пусть $\deg f=n\geqslant m$. В этом случае полиномы f и $a_nb_m^{-1}x^{n-m}h$ имеют одинаковые старшие коэффициенты. Следовательно, полином

(2) $g=f-a_nb_m^{-1}x^{n-m}\cdot h$

либо нулевой степени, либо его степень меньше n. Если $g=0$, то $f=a_nb_m^{-1}x^{n-m}h+0$ и можно положить $q=a_nb_m^{-1}x^{n-m}$ и $r=0$. Если же $\deg g<n$, то, по индуктивному предположению, в $F[x]$ существуют полиномы $\bar{q}$ и r такие, что

(3) $g=h\bar{q}+r$ и $\deg r<\deg h$, или $r=0$.

В силу (2) и (3) $f=h\left(\bar{q}+a_nb_m^{-1}x^{n-m}\right)+r$, или если положить $q=\bar{q}+a_nb_m^{-1}x^{n-m}$,

(4) $f=h\cdot q+r$ и $r=0$ или $\deg r<\deg h$.

Докажем, что для заданных полиномов f и h «неполное частное» q и «остаток» r в (4) определяются однозначно. В самом деле, предположим, что

(5) $f=hq_1+r_1$ и $r_1=0$ или $\deg r_1<\deg h$ $(r_1,\ q_1\in F[x])$.

Тогда в силу (4) и (5) имеем

(6) $r_1-r=h(q-q_1)$, $r_1-r=0$ или $\deg(r_1-r)<\deg h$.

Если $r_1-r\neq 0$, то $q-q_1\neq 0$ и

$$\deg(r_1-r)=\deg h+\deg(q-q_1)\geqslant\deg h,$$

что противоречит условиям (6). Если же $r_1-r=0$, то $q-q_1=0$ и, следовательно, $q=q_1$. □

СЛЕДСТВИЕ 2.2. *Если $\mathcal{F}$ — поле, то кольцо полиномов $\mathcal{F}[x]$ является евклидовым кольцом.*

СЛЕДСТВИЕ 2.3. *Кольцо полиномов $\mathcal{F}[x]$ над полем $\mathcal{F}$ является кольцом главных идеалов.*

СЛЕДСТВИЕ 2.4. *Если $\mathcal{F}$ — поле, то кольцо полиномов $\mathcal{F}[x]$ факториально.*

Алгоритм Евклида. Пусть $\mathcal{K}$ — коммутативное кольцо.

ЛЕММА 2.5. *Пусть в коммутативном кольце $\mathcal{K}$ для элементов a, b, q и r выполняется равенство*

(1) $a=bq+r$;

тогда

(2) НОД$(a,\ b)\sim$ НОД$(b,\ r)$.

Доказательство. Пусть $d=$ НОД$(a,\ b)$, $d'=$ НОД$(b,\ r)$. Так как $d\mid a$, $d\mid b$, то ввиду (1) $d\mid r$. Поскольку d есть общий делитель b и r, то $d\mid d'$. Аналогично убеждаемся, что $d'\mid d$. Следовательно, $d\sim d'$. □

Для нахождения НОД двух элементов кольца полиномов $\mathcal{F}[x]$ (или любого евклидова кольца) применяют спо-

соб «последовательного деления», называемый *алгоритмом Евклида*. Смысл этого способа состоит в сведении вычисления НОД данных полиномов a, b из $F[x]$ к вычислению НОД полиномов b и r с меньшими степенями.

Предположим, что ни один из полиномов a, b не делится (в $\mathscr{F}[x]$) на другой, и положим $b = b_1$; тогда

$$a = b_1 q_1 + b_2; \quad \deg b_1 > \deg b_2,$$
$$b_1 = b_2 q_2 + b_3, \quad \deg b_2 > \deg b_3.$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$

Продолжаем этот процесс до тех пор, пока не получим при делении нулевой остаток:

$$b_{k-2} = b_{k-1} q_{k-1} + b_k, \quad \deg b_{k-1} > \deg b_k,$$
$$b_{k-1} = b_k q_k + 0.$$

Этот процесс последовательного деления называется *алгоритмом Евклида*.

Отметим, что последовательность $\deg b_1, \deg b_2, \ldots$ есть убывающая последовательность натуральных чисел. Поэтому она обрывается через конечное число шагов. Предположим, что $b_k \neq 0$ и $b_{k+1} = 0$; тогда

$$\deg b_1 > \deg b_2 > \deg b_3 > \ldots > \deg b_{k-1} > \deg b_k.$$

На основании леммы 2.5 из выписанных выше равенств следует:

$$\text{НОД}(a, b_1) \sim \text{НОД}(b_1, b_2) \sim \ldots \sim \text{НОД}(b_{k-1}, b_k) \sim$$
$$\sim \text{НОД}(b_k, 0) = b_k.$$

Таким образом, $\text{НОД}(a, b) \sim b_k$ и b_k есть $\text{НОД}(a, b)$.

Мы пришли к следующему выводу. *Если к полиномам a и b кольца $\mathscr{F}[x]$ применить алгоритм Евклида, то получающийся при этом последний ненулевой остаток есть* НОД *полиномов a и b.*

СЛЕДСТВИЕ 2.6. *Пусть $\mathscr{F}$ — подполе поля $\mathscr{P}$, $\mathscr{F}[x]$ и $\mathscr{P}[x]$ — кольца полиномов соответственно над $\mathscr{F}$ и над $\mathscr{P}$. Пусть a и b — не равные одновременно нулю полиномы из $\mathscr{F}[x]$. Если d и d' — нормированные наибольшие общие делители полиномов a и b соответственно в $\mathscr{F}[x]$ и $\mathscr{P}[x]$, то $d = d'$.*

Неприводимые над данным полем полиномы. Пусть $\mathscr{F}[x]$ — кольцо полиномов над полем $\mathscr{F}$. В кольце $\mathscr{F}[x]$ обратимы только полиномы нулевой степени (делители единицы поля $\mathscr{F}$), т. е. ненулевые элементы поля $\mathscr{F}$. Следо-

вательно, любой полином положительной степени из $F[x]$ необратим в кольце $\mathscr{F}[x]$.

Полином из $F[x]$ является *приводимым, или составным*, в кольце $\mathscr{F}[x]$ или приводимым над полем $\mathscr{F}$, если его можно представить в виде произведения двух полиномов положительной степени из $F[x]$.

Другими словами, полином приводим в $\mathscr{F}[x]$, если он имеет положительную степень и обладает нетривиальными делителями.

Полином из $F[x]$ является *неприводимым, или простым*, в кольце $\mathscr{F}[x]$ или неприводимым над полем $\mathscr{F}$, если он имеет положительную степень и обладает только тривиальными делителями, т. е. любой делитель полинома либо ассоциирован с ним, либо ассоциирован с единицей.

Другими словами, полином a неприводим в кольце $\mathscr{F}[x]$, если он имеет положительную степень и в любом разложении вида $a=bc$, где b, $c\in F[x]$, один из множителей (b или c) ассоциирован с единицей поля, а другой — ассоциирован с a.

Примеры. 1. Если $\mathscr{F}$ — поле, то в кольце полиномов $\mathscr{F}[x]$ неприводим любой полином первой степени.

2. В кольце полиномов $\mathscr{R}[x]$, где $\mathscr{R}$ — поле действительных чисел, полином второй степени неприводим тогда и только тогда, когда он не имеет действительных корней.

ПРЕДЛОЖЕНИЕ 2.7. *Пусть p — неприводимый и a — любой полином кольца $\mathscr{F}[x]$. Тогда либо p делит a, либо p и a — взаимно простые.*

Доказательство. Мы предполагаем, что $\mathscr{F}$ — поле. По следствию 2.3, $\mathscr{F}[x]$ является кольцом главных идеалов. Следовательно, в силу 13.3.9 если p не делит a, то $(p, a)=(1)$. Поэтому $\lambda_1 p+\lambda_2 a=1$ для некоторых λ_1, λ_2 из F. Следовательно, по теореме 13.4.4, наибольший общий делитель p и a равен 1, т. е. полиномы p и a — взаимно простые. □

ПРЕДЛОЖЕНИЕ 2.8. *Пусть p — полином, неприводимый в кольце $\mathscr{F}[x]$, и $a_1, \ldots, a_n\in F[x]$. Если p делит произведение $a_1, a_2 \ldots a_n$, то p делит хотя бы один из полиномов $a_1, a_2, \ldots, a_n$.*

Это предложение непосредственно вытекает из следствия 2.3 и предложения 13.3.11.

ТЕОРЕМА 2.9. *Пусть $\mathscr{R}[x]$ — кольцо полиномов над полем $\mathscr{R}$ действительных чисел. Фактор-кольцо $\mathscr{R}[x]/(x^2+1)$ изоморфно полю комплексных чисел.*

Доказательство. Пусть $\mathbf{C}$ — основное множество поля $\mathscr{C}$ комплексных чисел. Пусть h — отображение множества $\mathbf{R}[x]$ в $\mathbf{C}$ такое, что

$h(f)=f(i)$ для любого f из $\mathbf{R}[x]$.

Непосредственная проверка показывает, что h является эпиморфизмом кольца $\mathscr{R}[x]$ на поле $\mathscr{C}$ комплексных чисел с ядром (x^2+1), т. е. $\operatorname{Ker} h=(x^2+1)$. Следовательно, по теореме 13.1.6 о кольцевых эпиморфизмах получаем $\mathscr{R}[x]/(x^2+1)\cong\mathscr{C}$. □

ТЕОРЕМА 2.10. *Пусть $\mathscr{F}[x]$ — кольцо полиномов над полем $\mathscr{F}$ и p — полином, неприводимый в $\mathscr{F}[x]$. Тогда фактор-кольцо $\mathscr{F}[x]/(p)$ является полем.*

Доказательство этой теоремы предоставляется читателю.

Разложение полинома в произведение нормированных неприводимых множителей. Пусть $\mathscr{F}$ — поле, а $\mathscr{F}[x]$ — кольцо полиномов над $\mathscr{F}$.

ТЕОРЕМА 2.11. *Любой полином положительной степени из $F[x]$ можно единственным образом представить в виде произведения элемента поля $\mathscr{F}$ и нормированных неприводимых в кольце $\mathscr{F}[x]$ полиномов.*

Доказательство. Пусть a — полином положительной степени из $F[x]$. Так как кольцо $\mathscr{F}[x]$ факториально, то полином a можно представить в виде произведения $a=q_1\ldots q_s$ полиномов $q_1, \ldots, q_s$, неприводимых в кольце $\mathscr{F}[x]$. Пусть u_k — старший коэффициент полинома q_k, $u_k\in F$. Тогда $q_k=u_kp_k$, где p_k — нормированный полином, неприводимый в $\mathscr{F}[x]$. Следовательно,

(1) $a=up_1\ldots p_s$, где $u=u_1\ldots u_s\in F$.

Докажем единственность разложения. Пусть

(2) $a=vp_1^*\ldots p_s^*$, $v\in F$,

— произвольное разложение, в котором $p_1^*, \ldots, p_s^*$ — нормированные полиномы, неприводимые в кольце $\mathscr{F}[x]$. Так как кольцо $\mathscr{F}[x]$ факториально, то: 1) $u=v$, поскольку u, v — старшие коэффициенты одного и того же полинома a; 2) при соответствующей нумерации полиномы p_i и p_i^* ассоциированы. Поскольку p_i, p_i^* — нормированные полиномы, то из их ассоциированности следует, что $p_i=p_i^*$ для $i=1,\ldots, s$. □

Пусть $a \in F[x]$ и

(1) $a = up_1 \dots p_s$, где $u \in F$,

— разложение полинома a в произведение нормированных неприводимых в $\mathcal{F}[x]$ множителей. Пусть $p_1, \dots, p_k$ — все различные нормированные неприводимые множители полинома a и $\alpha_1, \dots, \alpha_k$ — кратности их вхождения в разложение (1). Тогда имеет место разложение

(I) $a = up_1^{\alpha_1} \dots p_k^{\alpha_k}$ $(u \in F)$.

ОПРЕДЕЛЕНИЕ. Разложение (I) называется *каноническим разложением полинома a из $\mathcal{F}[x]$* на неприводимые над $\mathcal{F}$ (нормированные) множители.

Упражнения

1. Укажите, при каком значении λ полиномы $x^3 - 2\lambda x + \lambda^3$ и $x^3 + \lambda^2 - 2$ имеют общий корень в поле комплексных чисел.

2. Найдите наибольший общий делитель полиномов $x^3 - 1$ и $x^4 + x^3 + 2x^2 + x + 1$ и его линейное представление через эти полиномы.

3. Найдите наибольший общий делитель и наименьшее общее кратное полиномов $x^4 - 4x^3 + 1$ и $x^3 - 3x^2 + 1$.

4. Найдите наименьшее общее кратное полиномов $x^{33} - 1$ и $x^{18} - 1$.

5. Пусть $\mathcal{F}[x]$ — кольцо полиномов над полем $\mathcal{F}$ и a, b, c — полиномы из $F[x]$. Найдите в $F[x]$ наименьший идеал, содержащий все эти полиномы.

6. Пусть $\mathcal{F}[x]$ — кольцо полиномов над полем $\mathcal{F}$. Докажите, что множество всех общих кратных двух данных полиномов f и g из $F[x]$ является идеалом кольца $\mathcal{F}[x]$.

7. Пусть x_0 и y_0 — полиномы из $F[x]$, удовлетворяющие равенству $ax_0 + by_0 = c$, где a, b, $c \in F[x]$. Найдите в $F[x]$ множество всех решений уравнения $ax + by = c$.

8. Докажите, что если полином h взаимно простой с полиномами f и g, то h взаимно простой с $f \cdot g$.

9. Докажите неприводимость над полем $\mathbb{Q}$ полинома $x^4 - 2x + 3$.

10. Пусть p — полином из $F[x]$ такой, что любой другой полином из $F[x]$ либо взаимно простой с p, либо делится на p. Докажите, что полином p неприводим над полем $\mathcal{F}$.

11. Пусть $\mathcal{F}[x]$ — кольцо полиномов над числовым полем $\mathcal{F}$. Пусть c — степень неприводимого над $\mathcal{F}$ полинома, a, $b \in F[x]$ и c делит ab. Докажите, что c делит a или c делит b^k для некоторого натурального k.

12. Пусть $f = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ — каноническое разложение полинома f над полем $\mathcal{F}$. Сколько нормированных делителей с коэффициентами из F имеет полином f?

13. Пусть $\mathcal{F}[x]$ — кольцо полиномов над числовым полем $\mathcal{F}$, p — неприводимый над $\mathcal{F}$ полином и I — идеал, порожденный полиномом p. Докажите, что фактор-кольцо $\mathcal{F}[x]/I$ является полем.

§ 3. ФАКТОРИАЛЬНОСТЬ КОЛЬЦА ПОЛИНОМОВ НАД ФАКТОРИАЛЬНЫМ КОЛЬЦОМ

Примитивные полиномы. Всюду ниже используются следующие обозначения: $\mathscr{K}$ — факториальное кольцо, $\mathscr{F}$ — поле частных кольца $\mathscr{K}$; $\mathscr{K}[x]$ — кольцо полиномов от x над $\mathscr{K}$; $\mathscr{F}[x]$ — кольцо полиномов от x над $\mathscr{F}$.

ОПРЕДЕЛЕНИЕ. Пусть $f = a_0 + a_1x + \ldots + a_nx^n$ — произвольный ненулевой полином из $K[x]$. Наибольший общий делитель коэффициентов a_0, a_1, ..., a_n в кольце $\mathscr{K}$ называется *содержанием полинома* f.

ОПРЕДЕЛЕНИЕ. Полином f, содержание которого есть единица или делитель единицы (в $\mathscr{K}$), называется *примитивным в кольце* $\mathscr{K}[x]$.

Содержание полинома f в $\mathscr{K}[x]$ определяется однозначно с точностью до множителей, являющихся делителями единицы. Другими словами, любые два содержания полинома f ассоциированы в $\mathscr{K}$.

ПРЕДЛОЖЕНИЕ 3.1. *Если d — содержание ненулевого полинома из $K[x]$, то $f = dg$, где g — примитивный в $\mathscr{K}[x]$ полином.*

Доказательство. В самом деле, если в правой части равенства $f = a_0 + a_1x + \ldots + a_nx^n$ вынести d за скобки, то получим равенство $f = d\left(\frac{a_0}{d} + \frac{a_1}{d}x + \ldots + \frac{a_n}{d}x^n\right) = dg$, причем в силу предложения 13.4.6 единица есть наибольший общий делитель коэффициентов $\frac{a_0}{d}$, $\frac{a_1}{d}$, ..., $\frac{a_n}{d}$ полинома g. Следовательно, g — примитивный в $\mathscr{K}[x]$ полином. □

Отметим, что *всякий неприводимый над кольцом $\mathscr{K}$ полином положительной степени примитивен в $\mathscr{K}[x]$*. Действительно, если f не примитивен, то, по предложению 3.1, $f = dg$, где g — примитивный в $\mathscr{K}[x]$ полином положительной степени, а d — содержание f. Поскольку f не примитивен, то d не является делителем единицы в $\mathscr{K}$ и, значит, d и g — необратимые элементы $\mathscr{K}[x]$. Следовательно, f приводим в $\mathscr{K}[x]$. Таким образом, всякий непримитивный полином положительной степени приводим в $\mathscr{K}[x]$, а, значит, всякий неприводимый в $\mathscr{K}[x]$ полином положительной степени примитивен в $\mathscr{K}[x]$.

Заметим также, что примитивный в $\mathscr{K}[x]$ полином приводим над $\mathscr{K}$ тогда и только тогда, когда его можно представить в виде произведения полиномов положительной степени (причем примитивных). Для произвольного непри-

митивного полинома f это неверно, так как возможно, что $f=dg$, где d — содержание f и $\deg d=0$, а g — примитивный неприводимый полином.

ЛЕММА 3.2. *Пусть f, h — примитивные в $\mathscr{K}[x]$ полиномы и*

(1) $cf=dh$, где $c,\ d\in K\setminus\{0\}$.

Тогда d ассоциирован с c в $\mathscr{K}$ и f ассоциирован с h в $\mathscr{K}[x]$.

Доказательство. Пусть

$$f=a_0+\ldots+a_nx^n,\quad h=b_0+\ldots+b_mx^m\quad (a_n\neq 0,\ b_m\neq 0);$$

тогда $cf=ca_0+\ldots+ca_nx^n$, $dh=db_0+\ldots+db_mx^m$. В силу

(1) $n=m$ и

(2) $ca_0=db_0,\ \ldots,\ ca_n=db_n$.

Поскольку 1 есть наибольший общий делитель коэффициентов $a_0,\ \ldots,\ a_n$, то в силу предложения 13.4.5 c — наибольший общий делитель коэффициентов $ca_0,\ \ldots,\ ca_n$. Аналогично, на основании примитивности h и равенств (2) заключаем, что d — наибольший общий делитель коэффициентов $ca_0,\ \ldots,\ ca_n$. Следовательно, c и d ассоциированы в $\mathscr{K}$ и поэтому $d=\varepsilon c$, где ε — обратимый элемент кольца $\mathscr{K}$. Разделив обе части равенства (1) на c, получим $f=\varepsilon h$, т. е. f и h ассоциированы в $\mathscr{K}[x]$. □

ЛЕММА 3.3. *Пусть f и h — примитивные в $\mathscr{K}[x]$ полиномы. Если полиномы f и h ассоциированы в $\mathscr{F}[x]$, то они ассоциированы также в $\mathscr{K}[x]$.*

Доказательство. Пусть f и h ассоциированы в $\mathscr{F}[x]$. Тогда $f=\alpha h$, где α — некоторый ненулевой элемент поля $\mathscr{F}$. Поскольку $\mathscr{F}$ — поле частных кольца $\mathscr{K}$, элемент α можно представить в виде $\alpha=dc^{-1}$, где $d,\ c\in K\setminus\{0\}$.

Таким образом, $f=dc^{-1}h$ и $cf=dh$. По лемме 3.2, отсюда следует, что полиномы f и g ассоциированы в кольце $\mathscr{K}[x]$. □

ЛЕММА 3.4 (Гаусса). *Произведение примитивных в $\mathscr{K}[x]$ полиномов является примитивным в $\mathscr{K}[x]$ полиномом.*

Доказательство. Пусть f и g — произвольные примитивные в $\mathscr{K}[x]$ полиномы:

$$f=a_0+a_1x+\ldots+a_mx^m\quad (a_m\in K\setminus\{0\}),$$
$$g=b_0+b_1x+\ldots+b_nx^n\quad (b_n\in K\setminus\{0\});$$

тогда

$$fg=c_0+c_1x+\ldots+c_{m+n}x^{m+n}\quad (c_{m+n}=a_mb_n\neq 0).$$

Покажем, что полином fg примитивен в кольце $\mathscr{K}[x]$. Предположим, что p — любой простой элемент кольца $\mathscr{K}$, и докажем, что хотя бы один коэффициент полинома fg не делится на p. В самом деле, в силу примитивности полинома f существует коэффициент a_r, не делящийся на p и имеющий наименьший индекс. Аналогично, существует b_s — коэффициент полинома g, не делящийся на p и имеющий наименьший индекс. Коэффициент c_{r+s} полинома fg можно представить в виде суммы:

(1) $c_{r+s} = a_r b_s + (a_{r+1} b_{s-1} + \ldots + a_{r-1} b_{s+1} + \ldots)$.

Первое слагаемое этой суммы не делится на p, а второе — делится на p или отсутствует. Таким образом, c_{r+s} не делится на p. Поэтому содержание полинома fg равно 1, т. е. полином fg является примитивным в $\mathscr{K}[x]$. □

ЛЕММА 3.5. *Пусть f — полином в $\mathscr{K}[x]$. Если полином f приводим в $\mathscr{F}[x]$, то он приводим также в $\mathscr{K}[x]$.*

Доказательство. Пусть полином f приводим в $\mathscr{F}[x]$, т. е.

(1) $f = gh$,

где g и h — полиномы положительной степени из $F[x]$. Допустим, что f неприводим в $\mathscr{K}[x]$ и, следовательно, примитивен в $\mathscr{K}[x]$. Пусть

$$g = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n.$$

Поскольку $\mathscr{F}$ — поле частных кольца $\mathscr{K}$, то каждый коэффициент α_i можно представить в виде

$$\alpha_i = a_i \cdot b_i^{-1}, \text{ где } a_i,\ b_i \in K \quad (i = 0,\ \ldots,\ n).$$

Положим $b = b_0 \cdot b_1 \ldots b_n$; тогда $bg \in K[x]$ и в силу предложения 3.1

(2) $bg = cg_1 \quad (b,\ c \in K \setminus \{0\})$,

где g_1 — примитивный в $\mathscr{K}[x]$ полином положительной степени, а c — содержание полинома g. Аналогично убеждаемся в том, что существуют элементы d и e такие, что

(3) $dh = eh_1 \quad (d,\ e \in K \setminus \{0\})$,

где h_1 — примитивный в $\mathscr{K}[x]$ полином положительной степени.

В силу (1), (2) и (3) имеем

(4) $(bd)f = (ce)g_1 h_1 \quad (bd,\ ce \in K \setminus \{0\})$,

причем, по лемме Гаусса, полином g_1h_1 примитивен в $\mathscr{K}[x]$. По лемме 3.2, из (4) следует, что полиномы f и g_1h_1 ассоциированы в $\mathscr{K}[x]$. Следовательно,

$$f=\varepsilon g_1h_1,$$

где ε — элемент, обратимый в K, и g_1, h_1 — полиномы положительной степени из $K[x]$, что противоречит нашему допущению. Таким образом, полином f приводим в $\mathscr{K}[x]$. □

СЛЕДСТВИЕ 3.6. *Если полином положительной степени неприводим в кольце $\mathscr{K}[x]$, то он неприводим также в кольце $\mathscr{F}[x]$.*

Факториальность кольца полиномов. Докажем основную теорему этого параграфа.

ТЕОРЕМА 3.7. *Если кольцо $\mathscr{K}$ факториально, то и кольцо полиномов $\mathscr{K}[x]$ факториально.*

Доказательство. Пусть $\mathscr{K}$ — факториальное кольцо. Докажем, что любой отличный от нуля необратимый элемент кольца $\mathscr{K}[x]$ однозначно с точностью до порядка сомножителей и обратимых множителей разложим в произведение простых множителей в $\mathscr{K}[x]$. Сначала докажем возможность разложения на простые множители. Пусть f — произвольный ненулевой полином из $K[x]$. Если f — полином нулевой степени, то $f\in K$. Поскольку кольцо $\mathscr{K}$ факториально, полином f можно представить в виде произведения простых множителей в $\mathscr{K}$ и, значит, в $\mathscr{K}[x]$. Предположим, что $\deg f=n>0$, и всякий полином, степень которого меньше n, разложим в произведение простых множителей. Пусть

$$(1)\quad f=dg(x),$$

где $d\in K$, $g(x)$ — полином положительной степени, примитивный в $\mathscr{K}[x]$. Если полином g неприводим над $\mathscr{K}$, то, разлагая в (1) множитель d на простые множители, получим разложение f на простые множители. Если же полином $g(x)$ приводим в $\mathscr{K}[x]$, то его можно представить в виде произведения двух полиномов положительной степени, меньшей, чем n: $g(x)=h(x)\varphi(x)$. По индуктивному предположению, $h(x)$ и $\varphi(x)$ можно представить в виде произведения простых множителей в $\mathscr{K}[x]$. Следовательно, g, а в силу (1) и f также можно представить в виде произведения простых множителей.

Докажем единственность разложения. Пусть даны любые два разложения f на простые множители в $\mathscr{K}[x]$:

$$(2)\quad f=p_1\dots p_kq_1\dots q_s=p'_1\dots p'_rq'_1\dots q'_t,$$

где p_i, $p_i' \in K$, и q_i, q_i' — неприводимые, а значит, и примитивные полиномы положительной степени. По леммам 3.2 и 3.4, из (2) следует, что

(3) $p_1 \dots p_k \sim p_1' \dots p_r'$ в $\mathscr{K}$;

(4) $q_1 \dots q_s \sim q_1' \dots q_t'$ в $\mathscr{K}[x]$.

Поскольку кольцо $\mathscr{K}$ факториально, то из (3) следует, что $k = r$ и при соответствующей нумерации

(5) $p_i \sim p_i'$ в $\mathscr{K}$ для $i = 1, \dots, k$.

Далее, по следствию 3.6, полиномы q_i и q_i' неприводимы в кольце $\mathscr{F}[x]$. В силу факториальности кольца $\mathscr{F}[x]$ из (4) следует, что $s = t$ и при соответствующей нумерации

$q_i \sim q_i'$ в $\mathscr{F}[x]$ для $i = 1, \dots, s$.

Полиномы q_i и q_i' неприводимы в $\mathscr{K}[x]$ и, значит, примитивны в $\mathscr{K}[x]$, кроме того, эти полиномы ассоциированы в $\mathscr{F}[x]$. Следовательно, по лемме 3.3, они ассоциированы в $\mathscr{K}[x]$,

(6) $q_i \sim q_i'$ в $\mathscr{K}[x]$ при $i = 1, \dots, s$.

В силу (5) и (6) полином f обладает однозначным разложением на простые множители в кольце $\mathscr{K}[x]$. Итак, показано, что кольцо $\mathscr{K}[x]$ факториально. □

Упражнения

1. Приводим или неприводим полином $x^2 + 2x + 2$: (a) в кольце $\mathbb{Q}[x]$; (b) в кольце $\mathscr{R}[x]$; (c) в кольце $\mathbb{C}[x]$?
2. Приводим или неприводим полином $2x + 6$: (a) в кольце $\mathbb{Q}[x]$; (b) в кольце $\mathbb{Z}[x]$?
3. Всякий неприводимый в кольце $\mathbb{Z}[x]$ полином является примитивным в $\mathbb{Z}[x]$. Верно ли обратное утверждение?

§ 4. ФОРМАЛЬНАЯ ПРОИЗВОДНАЯ ПОЛИНОМА. НЕПРИВОДИМЫЕ КРАТНЫЕ МНОЖИТЕЛИ

Формальная производная полинома. Пусть $\mathscr{K}$ — кольцо полиномов от x над полем $\mathscr{F}$: $\mathscr{K} = \mathscr{F}[x]$. Пусть $\mathscr{K}[y]$ — простое трансцендентное расширение кольца $\mathscr{K}$ при помощи y. Кольцо $\mathscr{K}[y]$ будем обозначать также через $\mathscr{F}[x, y]$. Здесь элементы кольца $\mathscr{F}[x, y]$, если они являются элементами кольца $\mathscr{F}[x]$, будем обозначать через $f(x)$, $g(x)$ и т. д.; если же они являются элементами кольца $\mathscr{F}[y]$, — то через $f(y)$, $g(y)$ и т. д.

В кольце $\mathscr{F}[x, y]$ рассмотрим полиномы

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \quad (a_i \in F),$$
$$f(y) = a_0 + a_1 y + \ldots + a_n y^n$$

и их разность $f(x) - f(y)$. Легко видеть, что

$$f(x) - f(y) = \sum_{k=1}^{n} a_k (x^k - y^k) =$$
$$= (x-y) \sum_{k=1}^{n} a_k (x^{k-1} + x^{k-2}y + \ldots + y^{k-1}) =$$
$$= (x-y)\,\Phi(x, y),$$

где $\Phi(x, y) = \sum_{k=1}^{n} a_k (x^{k-1} + x^{k-2}y + \ldots + y^{k-1})$. Отметим, что

$$\Phi(x, x) = \sum_{k=1}^{n} k a_k x^{k-1} = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}.$$

ОПРЕДЕЛЕНИЕ. Пусть $f = a_0 + a_1 x + \ldots + a_n x^n$ — полином над полем $\mathscr{F}$. Полином

$$\Phi(x, x) = \sum_{k=1}^{n} k a_k x^{k-1} = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}$$

называется *формальной производной полинома* f и обозначается через f' или $f'(x)$.

ТЕОРЕМА 4.1. *Пусть* $\mathscr{F}[x]$ *— кольцо полиномов над полем* $\mathscr{F}$, f, g *— любые полиномы из* $F[x]$ и $\lambda \in F$; тогда:

(1) $(f+g)' = f' + g'$;

(2) $(fg)' = fg' + f'g$;

(3) $(\lambda f)' = \lambda f'$;

(4) $(f^m)' = m f^{m-1} f'$ при любом натуральном m.

Доказательство. (1) Пусть $h = f + g$; тогда

$$f(x) - f(y) = (x-y)\,\Phi(x \cdot y),\ g(x) - g(y) = (x-y)\,G(x, y),$$
$$h(x) - h(y) = f(x) - f(y) + g(x) - g(y) =$$
$$= (x-y)[\Phi(x, y) + G(x, y)].$$

Поэтому $h' = \Phi(x, x) + G(x, x) = f' + g'$; следовательно,

$$(f+g)' = f' + g'.$$

(2) Положим $\varphi = fg$, тогда

$$\begin{aligned}\varphi(x) - \varphi(y) &= f(x)g(x) - f(y)g(y) = \\ &= f(x)(g(x) - g(y)) + g(y)(f(x) - f(y)) = \\ &= (x-y)[f(x)G(x, y) + g(y)\Phi(x, y)].\end{aligned}$$

Отсюда получаем

$$\varphi' = f(x)G(x, x) + g(x)\Phi(x, x) = f(x)g'(x) + g(x)f'(x);$$

следовательно,

$$(fg)' = fg' + f'g.$$

(3) Формула (3) непосредственно следует из формулы (2) при $g = \lambda$, так как в этом случае $g' = 0$.

(4) Доказательство формулы (4) проводится индукцией по m на основании формулы (2). □

Разложение полинома по степеням разности $x - c$. При делении полинома $f = a_0x^n + \ldots + a_n$ на двучлен вида $x - c$ вычисления удобнее всего располагать по следующей схеме (называемой *схемой Горнера*):

	a_0	a_1	a_2	$\ldots$	a_{n-1}	a_n
c	b_0	b_1	b_2	$\ldots$	b_{n-1}	r
	a_0	$cb_0 + a_1$	$cb_1 + a_2$	$\ldots$	$cb_{n-2} + a_{n-1}$	$cb_{n-1} + a_n$

Очевидно, $a_0 = b_0$; любой же следующий коэффициент частного и остаток r вычисляются по формулам

$$b_k = cb_{k-1} + a_k \quad (k = 1, \ldots, n-1);$$
$$r = cb_{n-1} + a_n.$$

Эти формулы получаются из равенства

$$\begin{aligned}a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = (x-c)(b_0x^{n-1} + \\ + b_1x^{n-2} + \ldots + b_{n-1}) + r,\end{aligned}$$

если раскрыть скобки и, сделав приведение подобных членов, приравнять друг другу коэффициенты при одинаковых степенях в обеих частях равенства.

Схема Горнера удобна при разложении данного полинома f по степеням двучлена $x - c$.

Пусть

$$
\begin{aligned}
f &= (x-c)\,q_1 + r_0,\\
q_1 &= (x-c)\,q_2 + r_1,\\
&\dots\dots\dots\dots\dots\dots\\
q_{n-2} &= (x-c)\,q_{n-1} + r_{n-2},\\
q_{n-1} &= (x-c)\,a_0 + r_{n-1},
\end{aligned}
\tag{1}
$$

где q_k и r_k обозначают частное и остаток, полученные при делении q_{k-1} на $x-c$. Если последнее выражение в (1) для q_{k-1} подставить в предыдущее равенство, а затем то, что при этом получится, подставить вместо q_{n-2} и т. д., то придем к равенству

$$
f = r_0 + r_1(x-c) + r_2(x-c)^2 + \dots + r_{n-1}(x-c)^{n-1} + a_0(x-c)^n. \tag{2}
$$

Это есть разложение данного полинома f по степеням $(x-c)$. Дифференцируя обе части равенства (2) и полагая $x=c$, получим

$$
f(c) = r_0,\ f'(c) = r_1,\ f''(c) = 2!\ r_2,\ \dots,\ f^{(n)}(c) = n!\ a_0.
$$

Поэтому равенство (2) можно записать в виде

$$
f = f(c) + f'(c)(x-c) + \frac{f''(c)}{2!}(x-c)^2 + \dots + \frac{f^{(n)}(c)}{n!}(x-c)^n,
$$

если только f — полином над полем нулевой характеристики. Это и есть *формула Тейлора* для полиномов. Деление по схеме Горнера f на $x-c$ дает коэффициенты частного q_1, которое в свою очередь надо делить на $x-c$ и т. д.; все вычисления удобно расположить в одну таблицу:

	a_0	a_1	…	a_{n-1}	a_n	
c	b_0	b_1	…	b_{n-1}	r_0	$r_0 = f(c)$
	c_0	c_1	…	r_1		$r_1 = f'(c)$
	d_0	d_1	…			$r_2 = f''(c)$
	…	…	…	…	…	…
	a_0	r_{n-1}				$r_{n-1} = \frac{f^{(n-1)}(c)}{(n-1)!}$

Неприводимые кратные множители полинома. Пусть $\mathcal{F}[x]$ — кольцо полиномов над полем $\mathcal{F}$ нулевой характеристики.

ОПРЕДЕЛЕНИЕ. Пусть f — полином из $F[x]$ и p — его неприводимый множитель. Полином p называется *множителем кратности* m (или m-кратным множителем) полинома f, если

(1) $f = p^m g,\ p \nmid g,\ g \in F[x]$.

При $m > 1$ полином p называется *кратным множителем*, а при $m = 1$ — *простым множителем полинома* f.

ТЕОРЕМА 4.3. *Пусть* $\mathscr{F}[x]$ — *кольцо полиномов над полем* $\mathscr{F}$ *нулевой характеристики и* $f \in F[x]$. *Пусть* p — *неприводимый множитель кратности* $m \geqslant 1$ *полинома* f. *Тогда* p *является множителем кратности* $m-1$ *производной* f'.

Доказательство. По условию, p есть m-кратный множитель полинома f, значит, выполняются условия (1). Используя свойства производной, находим

$$f' = mp^{m-1}p'g + p^m g',$$

(2) $f' = p^{m-1}(mp'g + pg')$.

Так как, по условию, поле $\mathscr{F}$ имеет нулевую характеристику, то $mp' \neq 0$ и $\deg(mp') < \deg p$; поэтому $p \nmid mp'$. Поскольку p — неприводимый полином и (ввиду (1)) $p \nmid g$, то $p \nmid (mp')g$, поэтому

(3) $p \nmid (mp'g + pg')$.

На основании (2) и (3) заключаем, что p является множителем кратности $m-1$ производной f'. □

СЛЕДСТВИЕ 4.4. *Полином* f *из* $F[x]$ *имеет кратные неприводимые множители тогда и только тогда, когда наибольший общий делитель полиномов* f *и* f' *имеет положительную степень.*

Кратные корни полинома. Пусть $\mathscr{F}[x]$ — кольцо полиномов над полем $\mathscr{F}$ и $F[x]$ — его основное множество.

ОПРЕДЕЛЕНИЕ. Пусть f — полином из $F[x]$ и c — его корень в $\mathscr{F}$. Элемент c называется *корнем кратности* m (*m-кратным корнем*), если $f = (x-c)^m g,\ g(c) \neq 0,\ g \in F[x]$; при $m > 1$ элемент c называется *кратным корнем*, а при $m = 1$ — *простым корнем полинома* f.

ПРЕДЛОЖЕНИЕ 4.5. *Пусть* $\mathscr{F}[x]$ — *кольцо полиномов над полем нулевой характеристики и* $f \in F[x]$. *Элемент* c *из* F *является кратным корнем полинома* f *тогда и только тогда, когда* $f(c) = f'(c) = 0$.

Это предложение непосредственно следует из теоремы 1.9 и следствия 4.4.

ПРЕДЛОЖЕНИЕ 4.6. *Пусть* $\mathcal{F}[x]$ *— кольцо полиномов над полем* $\mathcal{F}$ *нулевой характеристики и* $f \in F[x]$. *Элемент* c *является* m*-кратным корнем полинома* f *тогда и только тогда, когда*

(1) $f(c) = f'(c) = \ldots = f^{(m-1)}(c) = 0,\ f^{(m)}(c) \neq 0.$

Доказательство. По теореме 4.3, элемент c тогда и только тогда будет m-кратным корнем полинома f (т. е. $(x-c)$ — m-кратный множитель полинома f), когда

(2) $(x-c)$ делит f, f', ..., $f^{(m-1)}$ и $(x-c) \nmid f^{(m)}$.

В силу теоремы Безу условия (1) и (2) равносильны. □

Упражнения

1. Разложите полином $x^6 - 5x^5 + 3x^3 - 1$ по степеням $x-1$.

2. Разложите полином $x^5 + 4x^4 - x^3 - 29x^2 - 14x - 1$ по степеням разности $x-2$.

3. Разложите полином $x^5 - x^3 + 1$ по степеням $x+i$.

4. Вычислите значения полинома $x^4 + 3x^2 - 5x + 1$ и его производных при $x = -1$.

5. Определите кратность корня 1 полинома $x^6 - x^5 - x^4 + 2x^3 - x^2 - x + 1$.

6. Определите кратность корня i полинома $x^6 + x^5 + 3x^4 + 2x^3 + 3x^2 + x + 1$.

7. Определите коэффициенты a и b так, чтобы полином $ax^4 + bx^3 + 1$ из $\mathbf{Q}[x]$ делился на $(x-1)^2$.

8. Определите коэффициенты a и b так, чтобы полином $ax^{n+1} + bx^n + 1$ из $\mathbf{Q}[x]$ делился на $(x-1)^2$.

9. Определите коэффициент a так, чтобы полином $x^5 - ax^2 - ax + 1$ из $\mathbf{Q}[x]$ имел -1 корнем не ниже второй кратности.

10. Найдите условия, при которых полином $x^5 + ax^3 + b$ имеет в поле комплексных чисел двойной корень, отличный от нуля.

11. Имеет ли полином $x^n + a$, где n — натуральное число и a — отличное от нуля число, кратные корни в поле комплексных чисел?

12. Докажите, что полином $1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!}$ не имеет кратных корней в любом числовом поле.

13. Пусть $\mathcal{F}$ и $\mathcal{P}$ — числовые поля, причем $\mathcal{F}$ — подполе поля $\mathcal{P}$. Докажите, что если полином f неприводим в кольце полиномов $\mathcal{F}[x]$, то он не имеет кратных множителей в кольце $\mathcal{P}[x]$.

Глава пятнадцатая

ПОЛИНОМЫ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ

§ 1. КОЛЬЦО ПОЛИНОМОВ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ

Кратное расширение кольца. Пусть $\mathscr{K}$ — ненулевое подкольцо коммутативного кольца $\mathscr{L}$ и $x_1, \ldots, x_m$ — элементы кольца $\mathscr{L}$.

ОПРЕДЕЛЕНИЕ. Минимальное расширение кольца $\mathscr{K}$, являющееся подкольцом кольца $\mathscr{L}$ и содержащее элементы $x_1, \ldots, x_m$ из L, называется *подкольцом кольца* $\mathscr{L}$, порожденным кольцом $\mathscr{K}$ и элементами $x_1, \ldots, x_m$.

Это кольцо обозначается через $\mathscr{K}[x_1, \ldots, x_m]$, а его основное множество — через $K[x_1, \ldots, x_m]$.

Очевидно, кольцо $\mathscr{K}[x_1, \ldots, x_m]$ является пересечением всех подколец кольца $\mathscr{L}$, содержащих элементы $x_1, \ldots, x_m$ и имеющих кольцо $\mathscr{K}$ в качестве подкольца.

ОПРЕДЕЛЕНИЕ. Кольцо, обозначаемое через $\mathscr{K}[x_1]\ldots[x_m]$ и определяемое индуктивно формулами

$$\mathscr{K}[x_1][x_2] = (\mathscr{K}[x_1])[x_2],$$

$$\mathscr{K}[x_1][x_2]\ldots[x_m] = (\mathscr{K}[x_1][x_2]\ldots[x_{m-1}])[x_m],$$

называется *m-кратным расширением кольца* $\mathscr{K}$.

ТЕОРЕМА 1.1. *Пусть* $\mathscr{K}$ *— подкольцо коммутативного кольца* $\mathscr{L}$ *и* $x_1, \ldots, x_m \in L$; *тогда*

(1) $\mathscr{K}[x_1, x_2, \ldots, x_m] = \mathscr{K}[x_1][x_2]\ldots[x_m]$.

Доказательство. Теорема, очевидно, верна при $m = 1$. Предположим, что теорема верна, когда к кольцу $\mathscr{K}$ присоединяется $m-1$ элементов. Из определения следует, что

$$K[x_1, \ldots, x_{m-1}] \subset K[x_1, \ldots, x_m] \text{ и } x_m \in K[x_1, \ldots, x_m],$$

поэтому

(2) $(K[x_1, \ldots, x_{m-1}])[x_m] \subset K[x_1, \ldots, x_m]$.

С другой стороны, поскольку $x_1, \ldots, x_m \in (K[x_1, \ldots, x_m])[x_m]$, то

(3) $K[x_1, \ldots, x_m] \subset (K[x_1, \ldots, x_{m-1}])[x_m]$.

В силу (2) и (3) имеем

(4) $K[x_1, \ldots, x_{m-1}, x_m] = K[x_1, \ldots, x_{m-1}][x_m]$.

По индуктивному предположению,

(5) $K[x_1, \ldots, x_{m-1}] = K[x_1] \ldots [x_{m-1}]$.

На основании равенств (4) и (5) заключаем, что

$$K[x_1, x_2, \ldots, x_m] = K[x_1][x_2] \ldots [x_m].$$

Следовательно, верна формула (1). □

Кольцо полиномов от нескольких переменных. Пусть m — целое положительное число и $\mathbf{N}$ — множество всех натуральных чисел. Пусть $\mathbf{N}^1 = \mathbf{N}$ и при $m > 1$

$$\mathbf{N}^m = \{(i_1, \ldots, i_m) \mid i_1, \ldots, i_m \in \mathbf{N}\},$$

где $(i_1, \ldots, i_m)$ — m-мерный вектор.

По теореме 1.1, $\mathscr{K}[x_1, x_2] = (\mathscr{K}[x_1])[x_2]$. Поэтому элементы кольца $\mathscr{K}[x_1, x_2]$ суть суммы вида

$$\alpha_0 + \alpha_1 x_2 + \ldots + \alpha_n x_2^n,$$

где $\alpha_i = a_{i0} + a_{i1}x_1 + \ldots + a_{im}x_1^m$ $(a_{ik} \in K)$, а m — наибольшая из степеней полиномов $\alpha_0, \alpha_1, \ldots, \alpha_n$. Следовательно, элементы кольца $\mathscr{K}[x_1, x_2]$ можно записать в виде

$$\sum_{(i_1, i_2) \in M} a_{i_1 i_2} x_1^{i_1} x_2^{i_2} \qquad (a_{i_1 i_2} \in K),$$

где M — непустое конечное подмножество множества $\mathbf{N}^2 = \mathbf{N} \times \mathbf{N}$.

На основании теоремы 1.1 заключаем также, что элементы кольца $\mathscr{K}[x_1, \ldots, x_m]$ суть суммы вида

$$\sum_{(i_1, \ldots, i_m) \in M} a_{i_1 \ldots i_m} x_1^{i_1} \ldots x_m^{i_m},$$

где M — непустое конечное подмножество множества $\mathbf{N}^m$ и $a_{i_1 \ldots i_m} \in K$. Такую сумму будем кратко записывать в виде

$$\sum_{(i) \in M} a_{(i)} x_1^{i_1} \ldots x_m^{i_m}, \text{ где } (i) = (i_1, \ldots, i_m).$$

Напомним, что элемент x_1 кольца $\mathscr{K}[x_1]$ называется *трансцендентным над* $\mathscr{K}$, если для любых элементов $a_1, \ldots, a_n$ кольца $\mathscr{K}$ из равенства $\sum_{i=1}^{n} a_i x_1^i = 0$ следуют равенства $a_1 = 0, \ldots, a_n = 0$. Обобщением этого понятия является понятие алгебраической независимости совокупности элементов $x_1, \ldots, x_m$ над $\mathscr{K}$.

Пусть $\mathscr{K}$ — подкольцо коммутативного кольца $\mathscr{L}$.

ОПРЕДЕЛЕНИЕ. Элементы $x_1, \ldots, x_m$ кольца $\mathscr{L}$ называются *алгебраически независимыми над кольцом* $\mathscr{K}$, если для любых элементов $a_{(i)}$ кольца $\mathscr{K}$ из равенства

$$\text{(I)} \quad \sum_{(i)\in M} a_{(i)} x_1^{i_1} \ldots x_m^{i_m} = 0, \text{ где } M \subset \mathbf{N}^n,$$

следует равенство нулю всех коэффициентов $a_{(i)}$.

При $m = 1$ мы получаем определение элемента, алгебраически независимого над $\mathscr{K}$, которое совпадает с определением элемента, трансцендентного над $\mathscr{K}$.

ТЕОРЕМА 1.2. *Пусть* $\mathscr{K}$ *— подкольцо коммутативного кольца* $\mathscr{L}$ *и* $x_1, \ldots, x_m \in L$. *Элементы* $x_1, \ldots, x_m$ *алгебраически независимы над* $\mathscr{K}$ *тогда и только тогда, когда для каждого* $s \in \{1, \ldots, m\}$ *элемент* x_s *является трансцендентным над* $\mathscr{K}[x_1, \ldots, x_{s-1}]$.

Доказательство. Предположим, что элементы $x_1, \ldots, x_m$ алгебраически независимы над кольцом $\mathscr{K}$, и докажем, что для каждого $s \in \{1, \ldots, m\}$ элемент x_s является трансцендентным над кольцом $\mathscr{K}[x_1, \ldots, x_{s-1}]$.

Пусть

$$\text{(II)} \quad A_0 + A_1 x_s + \ldots + A_l x_s^l = 0, \text{ где } A_k \in K[x_1, \ldots, x_{s-1}].$$

Слагаемые $A_k x_s^k$ можно записать в виде

$$A_k x_s^k = \sum_{(i)\in M_k} a_{(i)} x_1^{i_1} \ldots x_{s-1}^{i_{s-1}} x_s^k x_{s+1}^0 \ldots x_m^0, \text{ где } M_k \subset \mathbf{N}^m,$$

$$k = 0, \ldots, l.$$

Тогда равенство (II) можно записать следующим образом:

$$\text{(3)} \quad \sum_{(i)\in \bigcup M_k} a_{(i)} x_1^{i_1} \ldots x_s^{i_s} x_{s+1}^0 \ldots x_m^0 = 0.$$

В силу алгебраической независимости элементов $x_1, \ldots, x_m$ над кольцом $\mathscr{K}$ из (3) следует равенство нулю всех коэффициентов $a_{(i)}$ для $(i) \in \bigcup M_k$, поэтому $A_k = 0$ для $k = 0,$

$1, \ldots, l$. Следовательно, для каждого $s \in \{1, \ldots, m\}$ элемент x_s является трансцендентным над $\mathscr{K}[x_1, \ldots, x_{s-1}]$.

Предположим, что для каждого $s \in \{1, \ldots, m\}$ элемент x_s трансцендентен над $\mathscr{K}[x_1, \ldots, x_{s-1}]$, и докажем индукцией по m, что из (I) следует равенство нулю всех коэффициентов $a_{(i)}$.

Для $m = 1$ утверждение, очевидно, верно. Предположим, что утверждение верно для совокупности элементов $x_1, \ldots, x_{m-1}$. Запишем равенство (I) в виде

$$A_0 + A_1 x_m + A_2 x_m^2 + \ldots + A_r x_m^r = 0, \tag{4}$$

где

$$A_k x_m^k = \sum_{(i) \in M_k} a_{(i)} x_1^{i_1} \ldots x_{m-1}^{i_{m-1}} x_m^k, \quad A_k \in K[x_1, \ldots, x_{m-1}],$$

$$M = \bigcup_k M_k.$$

По условию, элемент x_m трансцендентен над $\mathscr{K}[x_1, \ldots, x_{m-1}]$, поэтому из (4) следуют равенства $A_0 = 0$, $A_1 = 0, \ldots, A_r = 0$. По индуктивному предположению, отсюда вытекают равенства

$$a_{(i)} = 0 \quad \text{для} \quad (i) \in \bigcup M_k = M.$$

Следовательно, элементы $x_1, \ldots, x_m$ алгебраически независимы над $\mathscr{K}$. □

Пусть $\mathscr{K}$ — ненулевое коммутативное кольцо и $\mathscr{K}[x_1] \ldots [x_m]$ — k-кратное расширение кольца $\mathscr{K}$ элементами $x_1, \ldots, x_m$. По теореме 1.1, $\mathscr{K}[x_1 \ldots x_m] = \mathscr{K}[x_1] \ldots [x_m]$ и, значит, кольцо $\mathscr{K}[x_1, \ldots, x_m]$ также является k-кратным расширением кольца $\mathscr{K}$.

ОПРЕДЕЛЕНИЕ. Кольцо $\mathscr{K}[x_1, \ldots, x_m]$ называется *m-кратным трансцендентным расширением кольца $\mathscr{K}$*, если для любого $s \in \{1, \ldots, m\}$ кольцо $\mathscr{K}[x_1, \ldots, x_s]$ является простым трансцендентным расширением кольца $\mathscr{K}[x_1, \ldots, x_{s-1}]$ при помощи x_s.

Отметим, что при $m = 1$ m-кратное трансцендентное расширение кольца $\mathscr{K}$ является простым трансцендентным расширением кольца $\mathscr{K}$.

ТЕОРЕМА 1.3. *Пусть $\mathscr{K}$ — ненулевое коммутативное кольцо. Для любого натурального m, отличного от нуля, существует m-кратное трансцендентное расширение кольца $\mathscr{K}$. При этом если $\mathscr{K}$ — область целостности, то m-кратное трансцендентное расширение этого кольца также является областью целостности.*

Доказательство. На основании теоремы 14.1.2 о существовании простого трансцендентного расширения кольца можно последовательно строить кольца:

$$\mathscr{K}[x_1],$$
$$(\mathscr{K}[x_1])[x_2],$$
$$\ldots\ldots\ldots$$
$$(\mathscr{K}[x_1]\ldots[x_{m-1}])[x_m],$$

где $\mathscr{K}[x_1]$ — простое трансцендентное расширение кольца $\mathscr{K}$ при помощи x_1, $(\mathscr{K}[x_1])[x_2]$ — простое трансцендентное расширение кольца $\mathscr{K}[x_1]$ при помощи x_2 и т. д. Наконец, $(\mathscr{K}[x_1]\ldots[x_{m-1}])[x_m]$ — простое трансцендентное расширение кольца $\mathscr{K}[x_1]\ldots[x_{m-1}]$ при помощи x_m. Согласно определению, предшествующему теореме, последнее кольцо является m-кратным трансцендентным расширением кольца $\mathscr{K}$. При этом, по теореме 14.1.6, если $\mathscr{K}$ — область целостности, то все построенные выше кольца являются областями целостности. □

ОПРЕДЕЛЕНИЕ. Кольцо $\mathscr{K}[x_1, \ldots, x_m]$, являющееся m-кратным трансцендентным расширением ненулевого коммутативного кольца $\mathscr{K}$, называется *кольцом полиномов над* $\mathscr{K}$ *от* $x_1, \ldots, x_m$.

Иногда, если это требуется, элементы f, g и т. д. этого кольца будем также обозначать через $f(x_1, \ldots, x_m)$, $g(x_1, \ldots, x_m)$ и т. д.

Изоморфизм колец полиномов. Пусть $\mathscr{K}$ и $\mathscr{L}$ — ненулевые коммутативные кольца.

ТЕОРЕМА 1.4. *Пусть* $\mathscr{K}$ *и* $\mathscr{L}$ *— изоморфные кольца и* φ *— изоморфизм* $\mathscr{K}$ *на* $\mathscr{L}$, *а* $\mathscr{K}[x_1, \ldots, x_n]$, $\mathscr{L}[y_1, \ldots, y_n]$ *— кольца полиномов. Тогда существует изоморфизм кольца* $\mathscr{K}[x_1, \ldots, x_n]$ *на кольцо* $\mathscr{L}[y_1, \ldots, y_n]$, *переводящий* $x_1, \ldots, x_n$ *соответственно в* $y_1, \ldots, y_n$ *и продолжающий изоморфизм* φ.

Доказательство проведем индукцией по n. Если $n=1$, то, по теореме 14.1.2, существует изоморфизм φ_1 кольца $\mathscr{K}[x_1]$ на кольцо $\mathscr{L}[y_1]$ такой, что $\varphi_1(x_1)=y_1$ и $\varphi_1(a)=\varphi(a)$ для всякого элемента a из K.

Допустим, что существует изоморфизм φ_n кольца $\mathscr{K}[x_1, \ldots, x_n]$ на кольцо $\mathscr{L}[y_1, \ldots, y_n]$, переводящий $x_1, \ldots, x_n$ в $y_1, \ldots, y_n$ соответственно и продолжающий изоморфизм φ. Тогда, по теореме 14.1.2, существует изоморфизм φ_{n+1} кольца $(\mathscr{K}[x_1\ldots x_n])[x_{n+1}]$ на кольцо $(\mathscr{L}[y_1, \ldots, y_n])[y_{n+1}]$, переводящий x_{n+1} в y_{n+1} и продолжающий

изоморфизм φ_n. Учитывая, что, по теореме 1.1,

$$(\mathscr{K}[x_1, \ldots, x_n])[x_{n+1}] = \mathscr{K}[x_1, \ldots, x_{n+1}] \text{ и}$$

$$(\mathscr{L}[y_1, \ldots, y_n])[y_{n+1}] = \mathscr{L}[y_1, \ldots, y_{n+1}],$$

получаем, что φ_{n+1} — изоморфизм $\mathscr{K}[x_1, \ldots, x_{n+1}]$ на $\mathscr{L}[y_1, \ldots, y_{n+1}]$, переводящий элементы $x_1, \ldots, x_{n+1}$ в $y_1, \ldots, y_{n+1}$ соответственно и продолжающий изоморфизм φ.

Таким образом, утверждение теоремы верно для любого натурального числа n. □

СЛЕДСТВИЕ 1.5. *Пусть $\mathscr{K}[x_1, \ldots, x_n]$ и $\mathscr{K}[y_1, \ldots, y_n]$ — кольца полиномов над кольцом $\mathscr{K}$. Тогда существует изоморфизм φ кольца $\mathscr{K}[x_1, \ldots, x_n]$ на кольцо $\mathscr{K}[y_1, \ldots, y_n]$, переводящий $x_1, \ldots, x_n$ соответственно в $y_1, \ldots, y_n$ и такой, что $\varphi(a) = a$ для любого элемента кольца $\mathscr{K}$.*

Нормальное представление полинома и степень полинома. Пусть $\mathbf{N}$ — множество всех натуральных чисел и m — фиксированное натуральное число, отличное от нуля. Для любого натурального числа k определим множество S_k:

$$S_k = \{(i_1, \ldots, i_m) \in \mathbf{N}^k \mid i_1 + \ldots + i_m = k\}.$$

Отметим, что

(1) $S_l \cap S_k = \emptyset$ при $l \neq k$.

Полином $\sum\limits_{(i) \in M} a_{(i)} x_1^{i_1} \ldots x_m^{i_m}$ называется *нулевым*, если все его коэффициенты $a_{(i)}$ равны нулю.

ТЕОРЕМА 1.6. *Пусть f — ненулевой полином из кольца полиномов $\mathscr{K}[x_1, \ldots, x_m]$. Для полинома f существует натуральное число n и такое представление*

$$(2)\quad f = \sum_{k=0}^{n} \Big(\sum_{(i) \in S_k} a_{(i)} x_1^{i_1} \ldots x_m^{i_m} \Big), \text{ где } a_{(i)} \in K,$$

что хотя бы для одного ненулевого коэффициента $a_{(i)}$ $i_1 + \ldots + i_m = n$. Это представление единственно в том смысле, что если

$$(3)\quad f = \sum_{k=0}^{s} \Big(\sum_{(i) \in S_k} b_{(i)} x_1^{i_1} \ldots x_m^{i_m} \Big), \text{ где } b_{(i)} \in K,$$

— другое такое представление, то $s = n$ и $a_{(i)} = b_{(i)}$ для всех (i) из S_k при $k = 0, 1, \ldots, n$.

Доказательство. Пусть

$$(4)\quad f=\sum_{(i)\in M} a_{(i)}x_1^{i_1}\dots x_m^{i_m} \qquad (a_{(i)}\in K),$$

где M — конечное подмножество множества $\mathbf{N}^m$. В этой сумме нет подобных членов, и поскольку f — ненулевой многочлен, то в сумме (4) есть ненулевые коэффициенты. Так как множество M конечно, существует натуральное число n, удовлетворяющее условиям

$$a_{i_1\dots i_m}\neq 0, \quad i_1+\dots+i_n=n$$

и

если $a_{k_1\dots k_m}\neq 0$, то $k_1+\dots+k_m\leqslant n$ для всякого $(k_1, \dots, k_m)\in M$.

Пусть $M^*=\bigcup\limits_{k=0}^{n} S_k$. Положим

$$a_{(i)}=0 \quad \text{для} \quad (i)\in M^*\setminus M.$$

На основании (4) заключаем, что

$$(5)\quad f=\sum_{(i)\in M^*} a_{(i)}x_1^{i_1}\dots x_m^{i_m}.$$

Поскольку $M^*=\bigcup\limits_{k=0}^{n} S_k$ и $S_l\cap S_k=\emptyset$ при $l\neq k$, из (5) следует представление (2).

Допустим, что кроме представления (2) существует представление (3). Если $m<n$, то, вычитая из равенства (2) равенство (3), получаем

$$(6)\quad \sum_{(i)\in S_n} a_{(i)}x_1^{i_1}\dots x_m^{i_m}+\dots$$

$$\dots+\sum_{k=0}^{m}\Bigl(\sum_{(j)\in S_k}\bigl(a_{(j)}-b_{(j)}\bigr)x_1^{j_1}\dots x_m^{j_m}\Bigr)=0.$$

В силу алгебраической независимости элементов $x_1, \dots, x_m$ все коэффициенты в (6) равны нулю, в частности

$$a_{(i)}=0 \quad \text{для всех} \quad (i)\in S_n,$$

что противоречит условию теоремы. Аналогично убеждаемся в невозможности неравенства $n<m$, поэтому $m=n$.

Таким образом, равенство (6) можно записать в виде

$$(7)\quad \sum_{k=0}^{n}\Big(\sum_{(j)\in S_k}(a_{(j)}-b_{(j)})x_1^{j_1}\ldots x_m^{j_m}=0.$$

В силу алгебраической независимости $x_1, \ldots, x_m$ из (7) следует, что $a_{(j)}=b_{(j)}$ для всех $(j)\in S_k$, где $k=\{0, 1, \ldots, n\}$. □

Представление (2) теоремы 1.6 называется *нормальным представлением полинома.*

ОПРЕДЕЛЕНИЕ. *Степенью одночлена* $a_{(i)}x_1^{i_1}\ldots x_m^{i_m}$ с ненулевым коэффициентом $a_{(i)}$ называется сумма $i_1+\ldots+i_m$.

ОПРЕДЕЛЕНИЕ. *Степенью ненулевого полинома* f, $f\in K[x_1, \ldots, x_m]$, называется наибольшая из степеней ненулевых одночленов, входящих в нормальное представление полинома f.

Степень нулевого полинома не определяется. Степень полинома f обозначается символом $\deg f$.

ОПРЕДЕЛЕНИЕ. Полином f степени n называется *однородным*, если

$$f=\sum_{i_1+\ldots+i_m=n}a_{(i)}x_1^{i_1}\ldots x_m^{i_m}.$$

Однородный полином первой степени называется *линейным полиномом.*

Отметим простейшие свойства степени полинома.

ТЕОРЕМА 1.7. *Пусть f и g — любые ненулевые полиномы кольца полиномов $\mathscr{K}[x_1, \ldots, x_m]$. Тогда:*

(1) *если* $f+g\neq 0$, *то* $\deg(f+g)\leqslant \max\{\deg f, \deg g\}$;

(2) *если* $f\cdot g$ *— ненулевой полином, то* $\deg(fg)\leqslant \deg f+\deg g$;

(3) *если* $\mathscr{K}$ *— область целостности, то* $\deg(fg)=\deg f+\deg g$.

Доказательство теоремы 1.7 предоставляется читателю.

Факториальность кольца полиномов. Докажем теорему, аналогичную теореме 14.3.7.

ТЕОРЕМА 1.8. *Пусть $\mathscr{K}$ — факториальное кольцо. Тогда кольцо полиномов $\mathscr{K}[x_1, \ldots, x_n]$ от $x_1, \ldots, x_n$ над $\mathscr{K}$ также является факториальным.*

Доказательство. Теорема доказывается индукцией по n. Для $n=1$ утверждение верно по теореме 14.3.7. Предположим, что кольцо полиномов $\mathscr{K}[x_1, \ldots, x_{n-1}]$ от

$x_1, \ldots, x_{n-1}$ над $\mathscr{K}$ факториально. Докажем, что тогда факториально также кольцо $\mathscr{K}[x_1, \ldots, x_n]$. По теореме 1.1,

$$\mathscr{K}[x_1, \ldots, x_n] = \mathscr{K}[x_1] \ldots [x_n] = (\mathscr{K}[x_1] \ldots [x_{n-1}])[x_n] = \\ = (\mathscr{K}[x_1, \ldots, x_{n-1}])[x_n].$$

По индуктивному предположению, кольцо $\mathscr{K}[x_1, \ldots, x_{n-1}]$ факториально. Следовательно, в силу теоремы 14.3.7 факториально его расширение $(\mathscr{K}[x_1, \ldots, x_{n-1}])[x_n]$ с помощью элемента x_n, трансцендентного над кольцом $\mathscr{K}[x_1, \ldots, x_{n-1}]$. Таким образом, кольцо полиномов $\mathscr{K}[x_1, \ldots, x_n]$ факториально для любого натурального n. □

СЛЕДСТВИЕ 1.9. *Кольцо полиномов $\mathscr{F}[x_1, \ldots, x_n]$ над полем $\mathscr{F}$ факториально.*

Упражнения

1. Покажите, что неприводимы над полем рациональных чисел следующие полиномы от двух переменных: (a) $3x^2 - y$; (b) $x^2 + y^2 - 1$. Приводимы ли эти полиномы над полем комплексных чисел?

2. Докажите, что кольцо полиномов $\mathscr{F}[x, y]$ над полем $\mathscr{F}$ от двух переменных не является кольцом главных идеалов.

3. Пусть $\mathscr{F}[x, y]$ — кольцо полиномов над полем $\mathscr{F}$ от двух переменных. Докажите, что фактор-кольцо $\mathscr{F}[x, y]/(x - y)$ изоморфно кольцу $\mathscr{F}[x]$.

§ 2. СИММЕТРИЧЕСКИЕ ПОЛИНОМЫ

Лексикографическое упорядочение членов полинома. Пусть $\mathbf{N}$ — множество всех натуральных чисел и m — фиксированное натуральное число, отличное от нуля. Элементы множества $\mathbf{N}^m$ суть m-мерные векторы с натуральными координатами. Пусть

$$\boldsymbol{i} = (i_1, \ldots, i_m), \quad \boldsymbol{k} = (k_1, \ldots, k_m).$$

На множестве $\mathbf{N}^m$ введем лексикографическое упорядочение, считая, по определению,

$$(1)\ (i_1, \ldots, i_m) < (k_1, \ldots, k_m),$$

если положительна первая ненулевая координата вектора $(k_1 - i_1, \ldots, k_m - i_m)$. При этом будем говорить, что вектор $\boldsymbol{i}$ ниже вектора $\boldsymbol{k}$, а вектор $\boldsymbol{k}$ выше вектора $\boldsymbol{i}$.

ТЕОРЕМА 2.1. *Лексикографическое упорядочение на множестве $\mathbf{N}^m$ является отношением строгого линейного порядка.*

Доказательство. Из определения лексикографического упорядочения следует, что для любых двух векто-

ров i, k из $\mathbf{N}^m$ выполняется одно и только одно из трех условий: $i<k$, $i=k$, $k<i$.

Отношение $<$ на множестве $\mathbf{N}^m$ транзитивно. В самом деле, если $i<k$ и $k<l$, то $k-i>0$, $l-k>0$, где $0=(0, \ldots, 0)$. Отсюда следует, что $(k-i)+(l-k)>0$ и $l-i>0$, т. е. $i<l$. □

СЛЕДСТВИЕ 2.2. *Пусть M — непустое конечное подмножество множества $\mathbf{N}^m$. Тогда лексикографическое упорядочение (порядок) на $\mathbf{N}^m$ индуцирует строгий линейный порядок на M.*

Доказательство. Пусть f — ненулевой полином кольца полиномов $\mathscr{K}[x_1, \ldots, x_m]$ и

$$(2)\quad f=\sum_{(i)\in M} a_{(i)}x_1^{i_1}\ldots x_m^{i_m}$$

— его представление, не имеющее нулевых коэффициентов, т. е.

$$a_{(i)}\neq 0 \text{ для каждого } (i)\in M.$$

Пусть S — множество одночленов, входящих в f (в сумму (2)). На множестве S введем отношение порядка, считая, что

$$(3)\quad a_{i_1\ldots i_m}x_1^{i_1}\ldots x_m^{i_m}<a_{k_1\ldots k_m}x_1^{k_1}\ldots x_m^{k_m}$$

в том и только в том случае, когда $(i_1, \ldots, i_m)<(k_1, \ldots, k_m)$. Действительно, это бинарное отношение транзитивно, антирефлексивно и, кроме того, линейно. Следовательно, отношение лексикографического порядка на S является также строгим линейным порядком. □

ОПРЕДЕЛЕНИЕ. Наибольший элемент упорядоченного множества $\langle S, <\rangle$ называется *высшим членом полинома f*.

Если выполняется неравенство (3), то говорят, что член $a_{i_1\ldots i_m}x_1^{i_1}\ldots x_m^{i_m}$ ниже, чем член $a_{k_1\ldots k_m}x_1^{k_1}\ldots x_m^{k_m}$. Высший член, очевидно, выше любого другого одночлена полинома f.

Лемма о высшем члене произведения двух полиномов. При изучении свойств симметрических полиномов необходима следующая лемма.

ЛЕММА 2.3. *Пусть $\mathscr{K}[x_1, \ldots, x_m]$ — кольцо полиномов от $x_1, \ldots, x_m$ над областью целостности $\mathscr{K}$. Высший член произведения двух ненулевых полиномов кольца $\mathscr{K}[x_1, \ldots, x_m]$ равен произведению высших членов сомножителей.*

Доказательство. Пусть f и g — ненулевые полиномы рассматриваемого кольца, $ax_1^{i_1}\ldots x_m^{i_m}$ и $bx_1^{k_1}\ldots x_m^{k_m}$ —

высшие члены соответственно полиномов f и g. Надо доказать, что высшим членом полинома fg является одночлен

(I) $abx_1^{i_1+k_1} \dots x_m^{i_m+k_m}$.

Заметим, что $ab \neq 0$, так как $\mathscr{K}$ — область целостности. Пусть

(1) $cx_1^{j_1} \dots x_m^{j_m}$ и $dx_1^{s_1} \dots x_m^{s_m}$

— любые ненулевые слагаемые в нормальных представлениях полиномов f и g соответственно. Тогда выполняются неравенства

(2) $(j_1, \dots, j_m) \leqslant (i_1, \dots, i_m)$

(3) $(s_1, \dots, s_m) \leqslant (k_1, \dots, k_m)$.

Нам достаточно показать, что если хотя бы одно из этих неравенств является строгим, то

(4) $cdx_1^{j_1+s_1} \dots x_m^{j_m+s_m} < abx_1^{i_1+k_1} \dots x_m^{i_m+k_m}$.

В самом деле, если хотя бы одно из неравенств (2) и (3) является строгим, то

(5) $(i_1-j_1, \dots, i_m-j_m) > 0$ или $(k_1-s_1, \dots, k_m-s_m) > 0$

и в силу (2), (3), (5)

(6) $(i_1+k_1, \dots, i_m+k_m)-(j_1+s_1, \dots, j_m+s_m) > 0$.

Из (6) следует (4). Неравенство (4) выполняется для любых ненулевых слагаемых (1) в нормальных представлениях полиномов f и g, по крайней мере одно из которых не является высшим членом соответствующего полинома. На основании этого заключаем, что одночлен (I) является высшим членом произведения fg. □

Симметрические полиномы. Пусть $\mathscr{K}[x_1, \dots, x_m]$ — кольцо полиномов от $x_1, \dots, x_m$ над коммутативным кольцом $\mathscr{K}$. Пусть S_m — множество подстановок степени m.

ОПРЕДЕЛЕНИЕ. Полином f из $\mathscr{K}[x_1, \dots, x_m]$ называется *симметрическим полиномом от* $x_1, \dots, x_m$, если для любой подстановки $\tau \in S_m$ выполняется равенство

$$f(x_1, \dots, x_m) = f(x_{\tau(1)}, \dots, x_{\tau(m)}).$$

Пример. Полином $x_1^2 + \dots + x_m^2 + x_1 + x_2 + \dots + x_m$ переходит в себя при любой подстановке элементов $x_1, \dots, x_m$.

ОПРЕДЕЛЕНИЕ. *Элементарными симметрическими полиномами от* $x_1, \ldots, x_m$ называются полиномы

$$\sigma_1 = x_1 + x_2 + \ldots + x_m;$$
$$\sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_{m-1}x_m;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\sigma_m = x_1x_2 \ldots x_m.$$

Они возникают естественным образом при рассмотрении полинома $\varphi = (z - x_1)(z - x_2) \ldots (z - x_m)$, который равен полиному

$$z^m - (x_1 + x_2 + \ldots + x_m)z^{m-1} + (x_1x_2 + \ldots + x_{m-1}x_m)z^{m-2} + \\ + \ldots + (-1)^m x_1 \ldots x_m.$$

Таким образом, $\varphi = z^m - \sigma_1 z^{m-1} + \sigma_2 z^{m-2} - \ldots + (-1)^m \sigma_m$.

Легко проверить, что множество всех симметрических полиномов кольца $\mathscr{K}[x_1, \ldots, x_m]$ является подкольцом этого кольца; обозначим его через $S\mathscr{K}[x_1, \ldots, x_m]$. С другой стороны, элементарные симметрические полиномы от $x_1, \ldots, x_m$ порождают некоторое подкольцо $\mathscr{K}[x_1, \ldots, x_m]$; обозначим его через $\mathscr{K}[\sigma_1, \ldots, \sigma_m]$. Легко видеть, что

$$\mathscr{K}[\sigma_1, \ldots, \sigma_m] \supset S\mathscr{K}[x_1, \ldots, x_m].$$

Совпадают ли эти два кольца? Можно ли любой симметрический полином от $x_1, \ldots, x_m$ представить в виде полинома от элементарных симметрических полиномов $\sigma_1, \ldots, \sigma_m$? Ниже будет дан положительный ответ на этот вопрос.

Леммы о симметрических полиномах. Пусть $\mathscr{K}[x_1, \ldots, x_m]$ — кольцо полиномов от $x_1, \ldots, x_m$.

ЛЕММА 2.4. *Если* $ax_1^{k_1}x_2^{k_2} \ldots x_m^{k_m}$ — *высший член симметрического полинома, то* $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_m$.

Доказательство. Пусть f — полином из $K[x_1, \ldots, x_m]$, симметрический относительно $x_1, \ldots, x_m$, и

$$(1)\quad ax_1^{k_1}x_2^{k_2} \ldots x_m^{k_m} \qquad (a \in K)$$

— высший член полинома f. В нормальное представление симметрического полинома f входят также одночлены

$$(2)\quad ax_1^{k_2}x_2^{k_1}x_3^{k_3} \ldots x_m^{k_m},$$

$$(3)\quad ax_1^{k_1}x_2^{k_3}x_3^{k_2} \ldots x_m^{k_m}.$$

Так как одночлен (1) выше одночлена (2), то $k_1 \geqslant k_2$.

Поскольку одночлен (1) выше одночлена (3), то $k_2 \geqslant k_3$ и т. д. Следовательно, $k_1 \geqslant k_2 \geqslant k_3 \geqslant \ldots \geqslant k_m$. □

ЛЕММА 2.5. *Пусть* $ax_1^{k_1}x_2^{k_2}\ldots x_m^{k_m}$ — *высший член ненулевого симметрического полинома* $f \in K[x_1, \ldots, x_m]$. Тогда *высшие члены полиномов* f и $a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\ldots\sigma_m^{k_m}$ *совпадают*.

Доказательство. Нетрудно видеть, что элементарные симметрические полиномы $\sigma_1, \sigma_2, \ldots, \sigma_{m-1}, \sigma_m$ имеют соответственно следующие высшие члены:

$$x_1,\ x_1x_2,\ \ldots,\ x_1x_2\ldots x_{m-1},\ x_1x_2\ldots x_m.$$

По лемме о высшем члене произведения полиномов, высшими членами полиномов

(1) $a\sigma_1^{k_1-k_2},\ \sigma_2^{k_2-k_3},\ \ldots,\ \sigma_{m-1}^{k_{m-1}-k_m},\ \sigma_m^{k_m}$

являются соответственно одночлены

$$ax_1^{k_1-k_2},\ (x_1x_2)^{k_2-k_3},\ \ldots,\ (x_1x_2\ldots x_{m-1})^{k_{m-1}-k_m},\ (x_1\ldots x_m)^{k_m}.$$

В силу той же леммы произведение этих одночленов, т. е. одночлен $ax_1^{k_1}x_2^{k_2}\ldots x_m^{k_m}$, является высшим членом произведения полиномов (1). Таким образом, высшие члены полиномов f и $a\sigma_1^{k_1-k_2}, \ldots, \sigma_m^{k_m}$ совпадают. □

Пусть $\mathscr{K}[x_1, \ldots, x_m]$ — кольцо полиномов от $x_1, \ldots, x_m$. На множестве ненулевых полиномов этого кольца введем бинарное отношение $>$: $f > g$ *тогда и только тогда, когда высший член* f *выше, чем высший член* g. Нетрудно видеть, что это отношение есть отношение линейного порядка.

ОПРЕДЕЛЕНИЕ. Последовательность $\varphi_1, \varphi_2, \varphi_3, \ldots$ полиномов из $K[x_1, \ldots, x_n]$ называется *убывающей цепочкой*, если

(1) $\varphi_1 > \varphi_2 > \varphi_3 > \ldots$

ЛЕММА 2.6. *Убывающая цепочка ненулевых симметрических полиномов кольца полиномов* $\mathscr{K}[x_1, \ldots, x_m]$ *не может быть бесконечной*.

Доказательство. Пусть (1) есть убывающая цепочка симметрических полиномов. Тогда высший член φ_i выше, чем высший член φ_{i+1} для $i = 1, 2, 3, \ldots$. Пусть $ax_1^{k_1}x_2^{k_2}\ldots x_m^{k_m}$ — высший член полинома φ_1. Из симметричности φ_1, по лемме 2.4, следует, что $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_m$.

Пусть $(l_1, l_2, \ldots, l_m)$ — вектор показателей высшего члена любого симметрического полинома φ_i цепочки (1), отличного от φ_1. В силу (1)

$$(k_1, k_2, \ldots, k_m) > (l_1, l_2, \ldots, l_m),$$

поэтому

(2) $k_1 \geqslant l_1 \geqslant l_2 \geqslant \ldots \geqslant l_m$.

Заменим эти условия следующими, более слабыми условиями

(3) $0 \leqslant l_1 \leqslant k_1, \ldots, 0 \leqslant l_m \leqslant k_1$.

Число векторов $(l_1, \ldots, l_m)$ из $\mathbf{N}^m$, удовлетворяющих условиям (3), при фиксированном k_1 конечно и равно $(k_1+1)^m$. Поэтому число векторов $(l_1, \ldots, l_m)$, удовлетворяющих условиям (2), также конечно, так как из условий (2) следуют условия (3). Следовательно, цепочка (3) не может быть бесконечной. □

Основная теорема о симметрических полиномах. Пусть $\mathscr{K}[x_1, \ldots, x_m]$ — кольцо полиномов от $x_1, \ldots, x_m$ над областью целостности $\mathscr{K}$. Пусть $\sigma_1, \ldots, \sigma_m$ — симметрические полиномы от $x_1, \ldots, x_m$. Любой полином $g(\sigma_1, \ldots, \sigma_m)$ над $\mathscr{K}$ будем рассматривать как симметрический полином

$$g(\sigma_1(x_1, \ldots, x_m), \ldots, \sigma_m(x_1, \ldots, x_m)) \text{ от } x_1, \ldots, x_m \text{ над } \mathscr{K}.$$

ТЕОРЕМА 2.7. *Всякий симметрический полином из кольца полиномов $\mathscr{K}[x_1, \ldots, x_m]$ можно представить в виде полинома над $\mathscr{K}$ от элементарных симметрических полиномов $\sigma_1, \ldots, \sigma_m$, т. е. для любого $f(x_1, \ldots, x_m) \in K[x_1, \ldots, x_m]$ существует такой полином $g(x_1, \ldots, x_m) \in \mathscr{K}[x_1, \ldots, x_m]$, что*

$$f(x_1, \ldots, x_m) = g(\sigma_1(x_1, \ldots, x_m), \ldots, \sigma_m(x_1, \ldots, x_m)).$$

Доказательство. Пусть f — ненулевой симметрический полином над $\mathscr{K}$ и $a_0 x_1^{k_1} \ldots x_m^{k_m}$ — его высший член. Полином

(1) $f_1 = f - a_0 \sigma^{k_1 - k_2} \ldots \sigma_m^{k_m}$

— симметрический, как разность симметрических полиномов, причем, по лемме 2.5, $f > f_1$. Пусть $a_1 x_1^{l_1} \ldots x_m^{l_m}$ — высший член полинома f_1. Аналогично, полином

(2) $f_2 = f_1 - a_1 \sigma^{l_1 - l_2} \ldots \sigma_m^{l_m}$

является симметрическим, причем $f_1 > f_2$ и т. д. В результате получается убывающая цепочка симметрических полиномов $f_0 > f_1 > f_2 > \ldots$. По лемме 2.6, эта цепочка не может быть бесконечной. Предположим, что она обрывается на $(s+1)$-м шаге, т. е.

$$(s+1)\ f_{s+1} = f_s - a_s \sigma_1^{n_1 - n_2} \ldots \sigma_m^{n_m} = 0.$$

Складывая почленно равенства (1), (2), ..., $(s+1)$, получим

$$f = a_0 \sigma^{k_1 - k_2} \ldots \sigma_m^{k_m} + a_1 \sigma_1^{l_1 - l_2} \ldots \sigma_m^{l_m} + \ldots + a_s \sigma_1^{n_1 - n_m} \ldots \sigma_m^{n_m}.$$

Это равенство дает искомое представление симметрического полинома f в виде полинома над $\mathscr{K}$ от элементарных симметрических полиномов $\sigma_1, \ldots, \sigma_m$. □

Пример: $x_1^2 + x_2^2 + \ldots + x_m^2 =$
$= (x_1 + \ldots + x_m)^2 - 2(x_1 x_2 + \ldots + x_{m-1} x_m) = \sigma_1^2 - 2\sigma_2$.

СЛЕДСТВИЕ 2.8. *Пусть* $\varphi = z^m + a_1 z^{m-1} + \ldots + a_m$ — *полином над числовым кольцом* $\mathscr{K}$ *и* $\varphi = (z - c_1)(z - c_2) \ldots$ $\ldots (z - c_m)$, *где* $c_1, \ldots, c_m \in \mathbb{C}$. *Если* $f(x_1, \ldots, x_m)$ — *симметрический полином от* $x_1, \ldots, x_m$ *с коэффициентами* из K, то $f(c_1, \ldots, c_m) \in K$.

Доказательство. Из равенства

$$(z - c_1)(z - c_2) \ldots (z - c_m) = z^m + a_1 z^{m-1} + a_2 z^{m-2} + \ldots + a_m$$

вытекают следующие формулы (*Виета*), выражающие связь между корнями и коэффициентами полинома:

$$\begin{aligned} &c_1 + \ldots + c_m = -a_1; \\ &c_1 c_2 + \ldots + c_{m-1} c_m = a_2; \\ &\ldots\ldots\ldots\ldots \\ &c_1 c_2 \ldots c_m = (-1)^m a_m. \end{aligned}$$

Эти равенства можно записать в виде

$$(1)\quad \begin{aligned} &\sigma_1(c_1, \ldots, c_m) = -a_1, \\ &\sigma_2(c_1, \ldots, c_m) = a_2; \\ &\ldots\ldots\ldots\ldots\ldots \\ &\sigma_m(c_1, \ldots, c_m) = (-1)^m a_m. \end{aligned}$$

В силу основной теоремы о симметрических полиномах симметрический полином f из $K[x_1, \ldots, x_m]$ можно пред-

ставить в виде полинома g от элементарных симметрических полиномов $\sigma_1, \ldots, \sigma_m$ с коэффициентами из K, т. е.

(2) $f(x_1, \ldots, x_m) = g(\sigma_1(x_1, \ldots, x_m), \ldots, \sigma_m(x_1, \ldots, x_m))$.

Полагая в равенстве (2) $x_1 = c_1, \ldots, x_m = c_m$ и учитывая равенства (1), получим

(3) $f(c_1, \ldots, c_m) = g(-a_1, a_2, \ldots, (-1)^m a_m)$.

Кроме того, $g \in K[x_1, \ldots, x_m]$ и $a_1, \ldots, a_m \in K$, следовательно,

$$f(c_1, \ldots, c_m) \in K. \ \square$$

Упражнения

1. Является ли симметрическим полином $(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$?
2. Найдите высший член полинома $2\sigma_1^4\sigma_2^3\sigma_3^2$, где $\sigma_1 = x_1 + x_2 + x_3$, $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$, $\sigma_3 = x_1x_2x_3$.
3. Покажите, что множество всех симметрических полиномов из $K[x_1, \ldots, x_n]$, где K — основное множество области целостности $\mathscr{K}$, замкнуто в кольце полиномов $\mathscr{K}[x_1, \ldots, x_n]$.
4. Найдите сумму кубов комплексных корней полинома $2z^4 - 4z^3 + 2z^2 - 6z + 1$.
5. Найдите сумму квадратов комплексных корней полинома $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ над полем комплексных чисел.

3. РЕЗУЛЬТАНТ ПОЛИНОМОВ И ИСКЛЮЧЕНИЕ ПЕРЕМЕННЫХ

Результант двух полиномов. Пусть f и g — полиномы из кольца полиномов $\mathscr{F}[x]$ над полем $\mathscr{F}$. Найдем условия, при которых эти полиномы обладают общим делителем положительной степени.

ТЕОРЕМА 3.1. *Пусть f и g — полиномы от x над полем $\mathscr{F}$ такие, что*

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_n, \ g = b_0x^m + b_1x^{m-1} + \ldots + b_m,$$

и по крайней мере один из коэффициентов a_0, b_0 отличен от нуля. Полиномы f и g имеют общий делитель положительной степени в $\mathscr{F}[x]$ тогда и только тогда, когда в $F[x]$ существуют полиномы c и d, удовлетворяющие условиям:

(α) $fc = gd$,

(β) $c = c_0x^{m-1} + \ldots + c_{m-1}$, $d = d_0x^{n-1} + \ldots + d_{n-1}$,

(γ) *хотя бы один из полиномов c и d отличен от нуля.*

Доказательство. Предположим, что полиномы f и g имеют в $F[x]$ общий делитель u положительной степени. Тогда существуют полиномы c и d такие, что $f=du$, $g=cu$. Легко проверить, что полиномы c и d удовлетворяют условиям $(\alpha)-(\gamma)$.

Предположим теперь, что существуют полиномы c, d, удовлетворяющие условиям (α), (β) и (γ). Предположим, что степень полинома f равна n, т. е. $a_0\neq 0$ (в противном случае можно было бы поменять ролями f и g). Пусть φ — наибольший общий делитель c и d. Тогда в $F[x]$ существуют такие полиномы c_1 и d_1, что

(1) $c=c_1\varphi$, $d=d_1\varphi$, НОД $(c_1, d_1)=1$.

Отметим, что $d_1\neq 0$, так как в противном случае $d=0$ и ввиду (α) $c=0$, что противоречит условию (γ). В силу (1) и условия (α) $fc_1\varphi=gd_1\varphi$ и, значит,

(2) $fc_1=gd_1$.

Поскольку полином d_1 делит fc_1 и является взаимно простым с c_1, то d_1 делит f; так что

(3) $f=d_1t$,

где t — полином положительной степени, так как степень d_1 не выше степени d, а степень d ниже степени f в силу условия (β). Из (3) и (2) получаем $d_1th=gd_1$ и $g=ht$. Таким образом, f и g имеют общий делитель t положительной степени. □

Запишем условия (α) и (β) более подробно:

$$(1)\quad (a_0x^n+\ldots+a_n)(c_0x^{m-1}+\ldots+c_{m-1})=$$
$$=(b_0x^m+\ldots+b_m)(d_0x^{n-1}+\ldots+d_{n-1}).$$

Произведя умножение в обеих частях равенства и приравнивая коэффициенты при одинаковых степенях x, получаем следующую систему линейных уравнений:

$$\begin{aligned}
a_0c_0 &= b_0d_0;\\
a_1c_0+a_0c_1 &= b_1d_0+b_0d_1;\\
a_2c_0+a_1c_1+a_0c_2 &= b_2d_0+b_1d_1+b_0d_2;\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
a_nc_{m-2}+a_{n-1}c_{m-1} &= b_md_{n-2}+b_{m-1}d_{n-1};\\
a_nc_{m-1} &= b_md_{n-1}.
\end{aligned}$$

Это есть система $n+m$ однородных линейных уравнений с $n+m$ переменными $c_0, c_1, \ldots, c_{m-1}, d_0, d_1, \ldots, d_{n-1}$. Она имеет ненулевые решения тогда и только тогда, когда определитель этой системы равен нулю. Для того чтобы избежать появления минусов перед элементами матрицы определителя, можно, перенеся правые части уравнений влево, считать переменными $c_0, c_1, \ldots, c_{m-1}, -d_0, -d_1, \ldots, -d_{n-1}$. Если, кроме того, транспонировать матрицу определителя, то определитель системы примет вид

$$R = \begin{vmatrix} a_0 & a_1 & \ldots & a_n & & & \\ & a_0 & a_1 & \ldots & a_n & & \\ & & \ldots & \ldots & \ldots & \ldots & \\ & & & a_0 & a_1 & \ldots & a_n \\ b_0 & b_1 & \ldots & b_m & & & \\ & b_0 & b_1 & \ldots & b_m & & \\ & & \ldots & \ldots & \ldots & \ldots & \\ & & & b_0 & b_1 & \ldots & b_m \end{vmatrix} \begin{matrix} \Big\} m \\ \\ \\ \\ \Big\} n \\ \\ \\ \\ \end{matrix}$$

ОПРЕДЕЛЕНИЕ. Результантом полиномов $f=a_0x^n+\ldots+a_n$ и $g=b_0x^m+\ldots+b_m$ называется *определитель* R.

Из теоремы 3.1 следует, что полиномы f и g (у которых $a_0 \neq 0$ или $b_0 \neq 0$) имеют общий делитель положительной степени тогда и только тогда, когда система линейных уравнений имеет ненулевые решения, т. е. когда определитель R равен нулю. Итак, доказана следующая теорема.

ТЕОРЕМА 3.2. *Пусть* $f=a_0x^n+\ldots+a_n$, $g=b_0x^m+\ldots+b_m$ — *полиномы над полем* $\mathcal{F}$ *и хотя бы один из коэффициентов* a_0 *и* b_0 *отличен от нуля. Полиномы* f *и* g *имеют общий делитель положительной степени тогда и только тогда, когда результант этих полиномов равен нулю.*

СЛЕДСТВИЕ 3.3. *Если результант полиномов* f *и* g *равен нулю, то либо полиномы имеют общий делитель положительной степени, либо коэффициенты* a_0 *и* b_0 *равны нулю, и обратно.*

Исключение переменных. Результант можно применить к исключению переменных из системы двух алгебраических уравнений, хотя бы одно из которых нелинейно, с двумя переменными. Пусть дана система уравнений

(1) $f(x, y)=0$, $g(x, y)=0$,

где f и g — полиномы от x и y над полем $\mathscr{F}$. Запишем эти полиномы по убывающим степеням x:

$$f(x, y) = a_0(y)\,x^n + a_1(y)\,x^{n-1} + \ldots + a_n(y);$$
$$g(x, y) = b_0(y)\,x^m + b_1(y)\,x^{m-1} + \ldots + b_n(y),$$

где $a_i(y)$ и $b_k(y)$ — полиномы из кольца $\mathscr{F}[y]$. Найдем результант полиномов f и g, рассматривая их как полиномы от x. Этот результант есть полином из кольца $\mathscr{F}[y]$, обозначим его через $R(y)$.

Предположим, что система (1) имеет в поле $\mathscr{F}$ (или в его расширении) решение (α, β). Тогда полиномы

$$f(x, \beta) = a_0(\beta)\,x^n + a_1(\beta)\,x^{n-1} + \ldots + a_n(\beta);$$
$$g(x, \beta) = b_0(\beta)\,x^m + b_1(\beta)\,x^{m-1} + \ldots + b_m(\beta)$$

имеют общий корень α. Поэтому они имеют общий множитель положительной степени (над $F(\beta)$). Следовательно, в силу теоремы 3.2 их результант, равный $R(\beta)$, должен быть равен нулю. Обратно: если β — корень результанта $R(y)$, т. е. $R(\beta) = 0$, то, по следствию 3.3, полиномы $f(x, \beta)$ и $g(x, \beta)$ либо имеют общий корень, либо их коэффициенты $a_0(\beta)$ и $b_0(\beta)$ оба равны нулю.

Таким образом, решение системы уравнений (1) с двумя переменными сведено к решению уравнения

(2) $R(y) = 0$

с одной переменной y. Говорят, что уравнение (2) представляет собой результант исключения x из системы уравнений (1).

Пример. Найдем решения системы уравнений

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

Исключим x из системы (1). Для этого запишем левые части уравнений по убывающим степеням x:

$$(2')\quad \begin{cases} (y^2 + y)\,x^2 + x + y = 0, \\ (y^2 + 2y)\,x + 1 = 0 \end{cases}$$

и составим определитель:

$$R(y) = \begin{vmatrix} y^2 + y & 1 & y \\ y^2 + 2y & 1 & 0 \\ 0 & y^2 + 2y & 1 \end{vmatrix}.$$

Вычисляя определитель, получаем

$$R(y) = y^2 + y + y(y^2+2y)^2 - y^2 - 2y = y[(y^2+2y)^2 - 1].$$

Уравнение $R(y) = y[(y^2+2y)^2 - 1] = y(y+1)^2(y^2+2y-1)$ имеет корни $0, -1, -1+\sqrt{2}, -1-\sqrt{2}$.

При $y=0$ система (1) переходит в систему $x=0, 1=0$, которая несовместна.

При $y=-1$ система (1) переходит в систему $x-1=0$, $-x+1=0$. Таким образом, получается решение системы (1): $(1, -1)$.

При $y=-1\pm\sqrt{2}$ система (1) превращается в систему

$$(2\mp\sqrt{2})x^2 + x + (-1\pm\sqrt{2}) = 0,$$
$$x+1=0,$$

которая имеет решение $x=-1$. Следовательно, мы получаем еще два решения системы (1): $(-1, -1+\sqrt{2})$, $(-1, -1-\sqrt{2})$.

Упражнения

1. Вычислить результант полиномов:

(a) $2x^3 - 3x^2 + 2x + 1$ и $x^2 + x + 3$;

(b) $x^3 + 2x^2 + 2x - 2$ и $x^2 - 2x + 4$;

(c) $x^3 - 3x + 6$ и $x^3 + x^2 - x - 1$.

2. При каком значении λ полиномы имеют общий корень:

(a) $x^3 - 2\lambda x + \lambda^3$ и $x^2 + \lambda^2 - 2$;

(b) $x^3 + \lambda x^2 - 9$ и $x^2 + \lambda x - 3$?

3. Исключите x из системы уравнений

$$x^2 - 3xy + y^2 - 2 = 0, \quad 2x^2 - xy + 3y^2 - 1 = 0.$$

4. Решите с помощью результанта систему уравнений

$$y^2 + x^2 - y - 3x = 0, \quad y^2 - 6xy - x^2 + 11y + 7x - 12 = 0.$$

Глава шестнадцатая

ПОЛИНОМЫ НАД ПОЛЕМ КОМПЛЕКСНЫХ ЧИСЕЛ И НАД ПОЛЕМ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ

§ 1. АЛГЕБРАИЧЕСКАЯ ЗАМКНУТОСТЬ ПОЛЯ КОМПЛЕКСНЫХ ЧИСЕЛ

Теорема о возрастании модуля полинома. Пусть $\mathscr{C}[z]$ — кольцо полиномов над полем комплексных чисел $\mathscr{C}$ и $\mathbf{C}[z]$ — его основное множество.

ТЕОРЕМА 1.1. *Пусть f — полином положительной степени из $\mathbf{C}[z]$. Для всякого действительного числа $M>0$ существует такое действительное число $r>0$, что для любого комплексного числа z $|f(z)|\geqslant M$, как только $|z|\geqslant r$.*

Доказательство. Пусть

$$f(z)=a_0+a_1z+\ldots+a_nz^n\in\mathbf{C}[z],\ a_n\neq 0,\ n\geqslant 1.$$

В силу свойств модуля (теорема 4.7.8)

$$|a_nz^n+a_{n-1}z^{n-1}+\ldots+a_0|\geqslant|a_nz^n|-|a_0+a_1z+\ldots+a_{n-1}z^{n-1}|,$$
$$|a_0+a_1z+\ldots+a_{n-1}z^{n-1}|\leqslant|a_0|+|a_1||z|+\ldots+|a_{n-1}||z|^{n-1}.$$

Следовательно, при $z\neq 0$

$$(1)\quad |f(z)|\geqslant|a_n||z|^n\left[1-\left(\frac{|a_0|}{|a_n||z|^n}+\ldots+\frac{|a_{n-1}|}{|a_n||z|}\right)\right].$$

Положим

$$(2)\quad b=\max\left\{\frac{|a_0|}{|a_n|},\ \ldots,\ \frac{|a_{n-1}|}{|a_n|}\right\}.$$

Отметим, что при $k\geqslant 1$ и $|z|\geqslant 1$ выполняются неравенства $|z|^k\geqslant|z|$ и

$$(3)\quad \frac{1}{|z|^k}\leqslant\frac{1}{|z|}.$$

На основании (1) — (3) получаем

$$(4)\quad |f(z)|\geqslant|a_n||z|^n\left(1-\frac{nb}{|z|}\right).$$

Легко видеть, что

(5) $\left(1-\frac{nb}{|z|}\right)\geqslant\frac{1}{2}$, если $|z|\geqslant 2nb$.

Далее, имеем

(6) $\frac{|a_n||z|^n}{2}\geqslant M$, если $|z|\geqslant\left(\frac{2M}{|a_n|}\right)^{1/n}$.

На основании (4)—(6) заключаем, что

$$|f(z)|\geqslant M, \text{ если } |z|\geqslant r,$$

где $r=\max\left\{1,\ 2nb,\ \left(\frac{2M}{|a_n|}\right)^{1/n}\right\}$. □

Непрерывность модуля полинома. Пусть f — полином от z над полем комплексных чисел. Отображение $z\longmapsto|f(z)|$, определенное на множестве $\mathbf{C}$ всех комплексных чисел, есть действительная функция комплексной переменной. Ее мы будем называть *модулем полинома* f и обозначать символом $|f|$.

ТЕОРЕМА 1.2. *Пусть f — любой полином из $\mathbf{C}[z]$. Модуль полинома f является непрерывной функцией на множестве* $\mathbf{C}$.

Доказательство. Покажем, что для всякого положительного ε найдется такое положительное δ, что для всякого комплексного числа z, если $|z-a|<\delta$, то $||f(z)|-|f(a)||<\varepsilon$.

Теорема, очевидно, верна, если полином f нулевой или имеет нулевую степень. Предположим, что полином f имеет положительную степень n.

Разложим f по степеням разности $z-a$:

$$f(z)=c_0+c_1(z-a)+\ldots+c_n(z-a)^n \quad (c_n\neq 0).$$

Поскольку $f(a)=c_0$, то

$$f(z)-f(a)=c_1(z-a)+\ldots+c_n(z-a)^n$$

и по теореме 4.7.8 получаем неравенство

(1) $|f(z)-f(a)|\leqslant|c_1||z-a|+\ldots+|c_n||z-a|^n$.

Положим

$$b=\max\{|c_1|,\ \ldots,\ |c_n|\};$$

так как $c_n\neq 0$, то $b\neq 0$. Легко видеть, что при $k\geqslant 1$

(2) $|z-a|^k\leqslant|z-a|$, если $|z-a|\leqslant 1$.

В силу (1) и (2) имеем

$$|f(z)-f(a)|\leqslant nb\,|z-a|.$$

Кроме того, для любого $\varepsilon>0$

$$nb\,|z-a|<\varepsilon, \text{ если } |z-a|<\varepsilon/nb.$$

Каждому числу ε поставим в соответствие положительное число $\delta=\min\left\{\frac{\varepsilon}{nb}, 1\right\}$; тогда $|f(z)-f(a)|<\varepsilon$, если $|z-a|<\delta$. Кроме того, для любого комплексного числа z

$$||f(z)|-|f(a)||\leqslant|f(z)-f(a)|.$$

Следовательно, для любого $\varepsilon>0$ можно найти такое $\delta>0$, что для всякого z из $\mathbf{C}$

$$||f(z)|-|f(a)||<\varepsilon, \text{ если } |z-a|<\delta. \ \square$$

ТЕОРЕМА 1.3. *Пусть f — полином из $\mathbf{C}[z]$. Если последовательность $\langle z_n\rangle$ сходится к комплексному числу a, то последовательность $\langle|f(z_n)|\rangle$ сходится к числу $|f(a)|$.*

Доказательство. По теореме 1.2,

$$(1)\quad (\forall\varepsilon>0)(\exists\delta>0)(\forall z\in\mathbf{C})(|z-a|<\delta\rightarrow \\ \rightarrow||f(z)|-|f(a)||<\varepsilon).$$

По условию, последовательность $\langle z_n\rangle$ сходится к числу a. Следовательно, для любого $\delta>0$ существует такое натуральное число n_0, что $|z_n-a|<\delta$ для всякого $n>n_0$. Отсюда в силу (1) следует

$$(\forall\varepsilon>0)(\exists n_0\in\mathbf{N})(\forall n\in\mathbf{N})(n>n_0\rightarrow||f(z_n)|-|f(a)||<\varepsilon).$$

Таким образом, последовательность $\langle|f(z_n)|\rangle$ сходится к числу $|f(a)|$. $\square$

Наименьшее значение модуля полинома. Ниже будет нужна следующая известная из анализа теорема Больцано—Вейерштрасса: всякая бесконечная последовательность $\langle z_n\rangle$ точек круга $|z|\leqslant r$ (r — фиксированное положительное действительное число) обладает подпоследовательностью, сходящейся к некоторой точке этого круга.

ТЕОРЕМА 1.4. *Пусть f — полином из $\mathbf{C}[z]$, r — положительное действительное число и $m=\inf|f(z)|$. Тогда существует такое комплексное число a, что $|f(a)|=m$ и $|a|\leqslant r$.*

Доказательство. Пусть $\langle\varepsilon_n\rangle$ — последовательность положительных действительных чисел, сходящаяся к нулю.

Так как $m = \inf\limits_{|z|\leqslant r} |f(z)|$, то для каждого члена ε_n последовательности существует такое z_n, что

(1) $m \leqslant |f(z_n)| \leqslant m + \varepsilon_n,\ |z_n| \leqslant r.$

Поэтому последовательность $\langle |f(z_n)| \rangle$ сходится к m:

(2) $\lim\limits_{n\to\infty} |f(z_n)| = m.$

В силу (1) все элементы последовательности $\langle z_n \rangle$ принадлежат кругу $|z| \leqslant r$. По теореме Больцано — Вейерштрасса, эта последовательность обладает подпоследовательностью $\langle x_n \rangle$, сходящейся к некоторой точке a круга $|z| \leqslant r$, т. е.

(3) $\lim\limits_{n\to\infty} x_n = a,\ |a| \leqslant r.$

По теореме 1.3, из (3) следует, что

(4) $\lim\limits_{n\to\infty} |f(x_n)| = |f(a)|.$

Так как $\langle |f(x_n)| \rangle$ есть подпоследовательность последовательности $\langle f(z_n) \rangle$, которая сходится к m, то

(5) $\lim\limits_{n\to\infty} |f(x_n)| = m.$

На основании (3), (4) и (5) заключаем, что $|f(a)| = m$ и $|a| \leqslant r$. □

ТЕОРЕМА 1.5. *Модуль любого полинома f из* $\mathbf{C}[z]$ *достигает своего наименьшего значения на множестве* $\mathbf{C}$.

Доказательство. Теорема, очевидно, верна, если $\deg f = 0$ или $f(0) = 0$. Поэтому предположим, что $\deg f \geqslant 1$ и $f(0) \neq 0$. Положим $M = |f(0)|$. По теореме 1.1,

(1) $(\exists r > 0)(\forall z \in \mathbf{C})(|z| \geqslant r \to |f(z)| \geqslant M).$

Пусть $K = \{z \in \mathbf{C} \mid |z| \leqslant r\}$. По теореме 1.4, $|f|$ достигает наименьшего значения в круге K, т. е. существует число a такое, что

(2) $|f(a)| \leqslant |f(z)|$, если $|z| \leqslant r$, в частности

(3) $|f(a)| \leqslant |f(0)| = M.$

На основании (1) и (3) заключаем, что

(4) $|f(a)| \leqslant |f(z)|$, если $|z| \geqslant r$.

В силу (2) и (4) имеем $(\forall z \in \mathbf{C})(|f(a)| \leqslant |f(z)|)$. Таким образом, $|f|$ достигает на множестве $\mathbf{C}$ наименьшего значения в точке a. □

Лемма Даламбера. Доказательство теоремы 1.7 в значительной мере основано на следующей лемме, называемой леммой Даламбера.

ЛЕММА 1.6. *Пусть* $f(x)$ — *полином положительной степени над полем комплексных чисел и* $a \in \mathbf{C}$. *Если* $f(a) \neq 0$, *то существует такое комплексное число* c, *что* $|f(c)| < |f(a)|$.

Доказательство. Пусть $f(x) = a_0 + \ldots + a_n x^n$ — полином степени $n > 0$ и $f(a) \neq 0$. Разложим f по степеням разности $x - a$:

(1) $f(x) = c_0 + c_1(x-a) + \ldots + c_n(x-a)^n$, где $c_i \in \mathbf{C}$, $c_0 = f(a) \neq 0$, $c_n \neq 0$.

Положим $z = x - a$ и

(2) $g(z) = c_0 + c_1 z + \ldots + c_n z^n$.

Пусть c_m — ненулевой коэффициент полинома g с наименьшим положительным индексом $(0 < m \leqslant n)$; тогда

(3) $f(a+z) = g(z) = c_0 + c_m z^m + c_{m+1} z^{m+1} + \ldots + c_n z^n$.

Определим $h(z)$:

$$(4)\quad h(z) = \begin{cases} c_{m+1} + \ldots + c_n z^{n-m-1}, & \text{если } m < n, \\ 0, & \text{если } m = n. \end{cases}$$

Тогда равенство (3) можно записать в виде

(5) $g(z) = c_0 + c_m z^m + z^{m+1} h(z)$.

В силу (1) $\frac{c_0}{c_m} \neq 0$. Обозначим через d какой-либо корень m-й степени из числа $(-c_0/c_m)$:

(6) $d^m = -c_0/c_m$.

Рассмотрим в (5) значения z вида

(7) $z = \lambda d$, где $0 < \lambda < 1$, $\lambda \in \mathbf{R}$.

В силу (5) и (6) получаем равенства

$$(8)\quad \begin{aligned} g(\lambda d) &= c_0 - c_0\lambda^m + \lambda^{m+1} d^{m+1} h(\lambda d), \\ g(\lambda d) &= c_0 [1 - \lambda^m + \lambda^{m+1} c_0^{-1} d^{m+1} h(\lambda d)]. \end{aligned}$$

На основании (4) заключаем, что

$$d^{m+1} h(\lambda d) = c_{m+1} d^{m+1} + \ldots + c_n d^n \lambda^{n-m-1} \quad (m < n);$$

и

$$|c_0^{-1}d^{m+1}h(\lambda d)| \leqslant |c_0|^{-1}[|c_{m+1}d^{m+1}|+\ldots+|c_nd^n|]\ (m<n).$$

Положим теперь

$$(9)\quad B=\begin{cases} |c_0|^{-1}[|c_{m+1}d^{m+1}|+\ldots+|c_nd^n|], & \text{если } m<n, \\ 0, & \text{если } m=n. \end{cases}$$

Отметим, что при $m<n$ $B>0$, поскольку c_n и d отличны от нуля.

Из (8) и (9) вытекает неравенство

$$|g(\lambda d)| \leqslant |c_0|[1-\lambda^m+\lambda^{m+1}B] = |c_0|[1-\lambda^m(1-\lambda B)].$$

Если λ удовлетворяет условиям $0<\lambda<1$, $\lambda B<1$, то $|g(\lambda d)|<|c_0|$. А так как $c_0=f(a)$ и в силу (3) $g(\lambda d)=f(a+\lambda d)$, то

$$|f(a+\lambda d)|<|f(a)|, \text{ если } \begin{cases} 0<\lambda<\min\{1,\ B^{-1}\} \\ \qquad\qquad\qquad \text{при } m<n, \\ 0<\lambda<1 \text{ при } m=n. \end{cases} \square$$

Алгебраическая замкнутость поля комплексных чисел. Пусть $\mathscr{F}[x]$ — кольцо полиномов от x над полем $\mathscr{F}$.

ОПРЕДЕЛЕНИЕ. Поле $\mathscr{F}$ называется *алгебраически замкнутым*, если любой полином положительной степени из $\mathscr{F}[x]$ имеет в поле $\mathscr{F}$ хотя бы один корень.

ТЕОРЕМА 1.7. *Поле комплексных чисел алгебраически замкнуто.*

Доказательство. Пусть f — произвольный полином положительной степени из $F[x]$. Если $f(0)=0$, то нуль есть корень полинома f. Допустим, что $f(0)\neq 0$, и положим $M=|f(0)|$. Пусть r — такое положительное число, что

$$(1)\quad (\forall z\in \mathbf{C})(|z|\leqslant r \rightarrow M\leqslant |f(z)|).$$

Такое r существует в силу теоремы 1.1.

Пусть $K=\{z\in\mathbf{C}\,||z|\leqslant r\}$. В силу теоремы 1.5 функция $|f|$ достигает наименьшего значения на множестве K, т. е. существует такое число $a\in K$, что

$$(2)\ |f(a)|\leqslant |f(z)| \text{ для всякого } z\in K\ (|z|\leqslant r_0),$$

в частности

$$(3)\ |f(a)|\leqslant |f(0)|=M.$$

Из (1) и (3) получаем

(4) $(\forall z \in \mathbf{C})(|z| \leqslant r_0 \rightarrow |f(a)| \leqslant |f(z)|)$.

На основании (2) и (4) заключаем, что

(5) $(\forall z \in \mathbf{C})(|f(a)| \leqslant |f(z)|)$.

Если $f(a) \neq 0$, то, по лемме Даламбера, существует такое комплексное число c, что

$$|f(c)| < |f(a)| \quad (c \in \mathbf{C}).$$

Однако последнее неравенство противоречит (5), поэтому случай, когда $f(a) \neq 0$, невозможен. Следовательно, $f(a) = 0$, т. е. комплексное число a является корнем полинома f. □

СЛЕДСТВИЕ 1.8. *Всякий полином из кольца* $\mathscr{C}[x]$, *степень которого больше единицы, приводим в кольце* $\mathscr{C}[x]$.

Доказательство. Пусть $f \in \mathscr{C}[x]$ и $\deg f > 1$. По теореме 1.7, существует $a \in \mathbf{C}$ такое, что $f(a) = 0$. Тогда, по теореме 14.1.11, $(x-a)$ делит f, т. е. существует такой полином g в $\mathscr{C}[x]$, что $f = (x-a) \cdot g$. При этом $\deg g > 0$, поскольку $\deg f > 1$. Таким образом, полином f приводим в кольце $\mathscr{C}[x]$.

СЛЕДСТВИЕ 1.9. *Любой полином* f *положительной степени из кольца* $\mathscr{C}[x]$ *можно единственным образом представить в виде произведения комплексного числа и нормированных линейных множителей, т. е. в виде*

(1) $f = c(x-\alpha_1)\ldots(x-\alpha_n)$,

где $\alpha_1, \ldots, \alpha_n$ — *корни полинома* f (в $\mathbf{C}$) *и* c — *старший коэффициент полинома.*

Это утверждение вытекает из следствия 1.8 и теоремы 14.2.11 о разложимости полинома над полем в произведение нормированных неприводимых множителей.

Если в разложении (1) $\alpha_1, \ldots, \alpha_m$ суть все различные корни полинома f в $\mathbf{C}$, то это разложение можно представить в виде

(2) $f = c(x-\alpha_1)^{k_1} \ldots (x-\alpha_m)^{k_m}$, $k_1 + \ldots + k_m = n$.

Разложение (2) называется *каноническим разложением полинома* f *на неприводимые множители.* Число k_s называется *показателем кратности корня* α_s.

СЛЕДСТВИЕ 1.10. *Всякий полином* f *положительной степени* n *из* $\mathscr{C}[x]$ *имеет точно* n *комплексных корней,*

если каждый его корень считать столько раз, какова его кратность.

Формулы Виета. Установим зависимость между корнями и коэффициентами полинома.

ТЕОРЕМА 1.11 (Виета). *Пусть* $f = z^n + c_1 z^{n-1} + \ldots + c_{n-1} z + c_n$ *— полином над полем комплексных чисел и* $\alpha_1, \ldots, \alpha_n$ *— его корни; тогда*

$$
\begin{aligned}
&c_1 = -(\alpha_1 + \alpha_2 + \ldots + \alpha_n);\\
&c_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n;\\
&c_3 = -(\alpha_1\alpha_2\alpha_3 + \ldots + \alpha_{n-2}\alpha_{n-1}\alpha_n);\\
&\qquad\ldots\ldots\ldots\ldots\ldots\ldots\\
&c_n = (-1)^n \alpha_1\alpha_2 \ldots \alpha_n.
\end{aligned}
\tag{1}
$$

Доказательство. Так как $\alpha_1, \ldots, \alpha_n$ — корни полинома f, то, по следствию 1.9,

$$z^n + c_1 z^{n-1} + \ldots + c_{n-1} z + c_n = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_n).$$

Перемножив линейные множители в правой части равенства, получим

$$z^n + c_1 z^{n-1} + \ldots + c_{n-1} z + c_n = z^n - (\alpha_1 + \ldots + \alpha_n) z^{n-1} + \ldots + (-1)^n \alpha_1\alpha_2 \ldots \alpha_n.$$

Из равенства двух полиномов от z следует равенство коэффициентов при одинаковых степенях z; приравнивая коэффициенты при одинаковых степенях z, получаем формулы (1). □

Формулы (1) называются *формулами Виета.*

СЛЕДСТВИЕ 1.12. *Если* $\alpha_1, \ldots, \alpha_n$ *— корни полинома* $c_0 z^n + c_1 z^{n-1} + \ldots + c_{n-1} z + c_n$ *степени* n *из* $C[z]$, *то*

$$
\begin{aligned}
&\frac{c_1}{c_0} = -(\alpha_1 + \ldots + \alpha_n);\\
&\frac{c_2}{c_0} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n;\\
&\qquad\ldots\ldots\ldots\ldots\ldots\ldots\\
&\frac{c_n}{c_0} = (-1)^n \alpha_1\alpha_2 \ldots \alpha_n.
\end{aligned}
$$

Упражнения

1. Разложите на линейные множители в кольце $\mathscr{C}[z]$ полиномы: (a) $z^2 + z + 1 + i$; (b) $z^4 + z^3 - z - 1$.

2. Разложите на неприводимые множители полином $z^4 + 3z^3 + 4z^2 + 3z + 1$ в $\mathscr{C}[z]$ и в $\mathscr{R}[z]$.

3. Разложите полином $z^n - 1$, где n — натуральное число, отличное от 0 и 1, на линейные множители в $\mathscr{C}[z]$.

4. Сумма двух корней уравнения $2x^3-x^2-7x+\lambda=0$ равна 1. Найдите λ.

5. Определите λ так, чтобы один из корней уравнения $x^3-7x+\lambda=0$ равнялся удвоенному другому.

6. Зная, что полином $z^n+a_{n-1}z^{n-1}+\ldots+a_1z+a_0$, где $a_{n-1}, \ldots, a_0$ — комплексные числа, имеет корни $\alpha_1, \ldots, \alpha_n$, вычислите произведение $(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_n+1)$.

7. Пусть $b^2<4ac$, где a, b, c — действительные числа. Докажите, что фактор-кольцо $\mathscr{R}[z]/(az^2+bz+c)$ изоморфно полю комплексных чисел.

8. Докажите утверждение, обратное теореме Виета (теорема 1.11): если имеют место формулы Виета (формулы (1)), то комплексные числа $\alpha_1, \ldots, \alpha_n$ являются корнями полинома $f=z^n+c_1z^{n-1}+\ldots+c_n$ над полем $\mathscr{C}$.

§ 2. ПОЛИНОМЫ НАД ПОЛЕМ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ

Сопряженность мнимых корней полинома с действительными коэффициентами. Пусть $\mathscr{R}[x]$ — кольцо полиномов над полем действительных чисел $\mathscr{R}$.

Напомним, что комплексное число $a+bi$, где $a, b\in\mathbf{R}$, называется мнимым, если $b\neq 0$. Если $\alpha=a+bi$, то через $\overline{\alpha}$ будем обозначать сопряженное комплексное число $a-bi$.

ЛЕММА 2.1. *Если f — полином из кольца $\mathscr{R}[x]$ и α — произвольное комплексное число, то $f(\overline{\alpha})=\overline{f(\alpha)}$.*

Доказательство непосредственно вытекает из теоремы 4.7.6.

ТЕОРЕМА 2.2. *Пусть f — произвольный полином из кольца $\mathscr{R}[x]$. Если $a+bi$ — мнимый корень полинома f, то $a-bi$ также является корнем этого полинома.*

Доказательство. Пусть $a+bi$ — корень полинома, т. е. $f(a+bi)=0$. Тогда, по лемме 2.1,

$$f(a-bi)=f\overline{(a+bi)}=\overline{f(a+bi)}=\overline{0}=0,$$

т. е. $f(a-bi)=0$. □

Неприводимые над полем действительных чисел полиномы.

ТЕОРЕМА 2.3. *Пусть f — полином, степень которого больше единицы, неприводимый над полем действительных чисел $\mathscr{R}$. Тогда существуют такие $a, b\in\mathbf{R}$, что $b\neq 0$ и полином f ассоциирован с полиномом $(x-a)^2+b^2$.*

Доказательство. По теореме 1.7, полином f имеет хотя бы один комплексный корень. Пусть $a+bi$ — корень полинома f, где $a, b\in\mathbf{R}$. Если $b=0$, то $x-a$ делит f, что противоречит условию неприводимости f над $\mathscr{R}$. Следовательно, $b\neq 0$. Применим к полиномам f и $(x-a)^2+b$ теорему

о делении с остатком. Согласно этой теореме, в кольце $\mathscr{R}[x]$ существуют полиномы $q(x)$ и $cx+d$ такие, что

$$f(x)=q(x)[(x-a)^2+b^2]+(cx+d),\ c,\ d\in\mathbf{R}.$$

Полагая в этом равенстве $x=a+bi$, получаем

$$f(a+bi)=c(a+bi)+d=0,\quad (ca+d)+bci=0.$$

Отсюда вытекает, что $ca+d=0$, $bc=0$. Так как $b\neq 0$, то $c=0$ и $d=0$. Таким образом,

$$f(x)=q(x)[(x-a)^2+b^2].$$

Поскольку, по условию, полином f неприводим над $\mathscr{R}$, то степень полинома $q(x)$ равна нулю. Следовательно, полином f ассоциирован с полиномом $(x-a)^2+b^2$. □

СЛЕДСТВИЕ 2.4. *В кольце $\mathscr{R}[x]$ неприводимы только полиномы первой степени и полиномы второй степени, ассоциированные с полиномами вида $(x-a)^2+b^2$, где a, b — любые действительные числа и $b\neq 0$.*

Из следствия 2.4 и теоремы 14.2.11 вытекает следующая теорема.

ТЕОРЕМА 2.5. *Любой полином f положительной степени из кольца $\mathscr{R}[x]$ можно единственным образом представить в виде произведения действительного числа и неприводимых над $\mathscr{R}$ полиномов не выше чем второй степени:*

$$f=d\prod_k[(x-a_k)^2+b_k^2]\prod_s(x-c_s),\quad \text{где}\quad b_k\neq 0.$$

СЛЕДСТВИЕ 2.6. *Любой полином с действительными коэффициентами имеет четное число мнимых корней.*

СЛЕДСТВИЕ 2.7. *Полином нечетной степени с действительными коэффициентами имеет хотя бы один действительный корень.*

СЛЕДСТВИЕ 2.8. *Пусть f — полином степени n из $\mathscr{R}[x]$. Четность числа действительных корней полинома f совпадает с четностью числа n.*

Упражнения

1. Найдите полином наименьшей степени с действительными коэффициентами, имеющий корни $i-1$, π, $-1+i\sqrt{3}$.

2. Разложите на неприводимые множители над полем действительных чисел полиномы:

(a) x^3+x+2; (b) x^4+2x^2+4; (c) x^5-1; (d) x^4-x^2+1.

3. Разложите полином x^4+4 на неприводимые множители: (a) над полем $\mathscr{Z}$; (b) над полем $\mathscr{R}$; (c) над полем $\mathscr{Q}$.

4. Разложите на неприводимые множители над полем действительных чисел полином x^4-ax^2+1, где $-2<a<2$.

5. Докажите, что полином $x^{3m}+x^{3n+1}+x^{3p+2}$ делится на полином x^2+x+1.

6. Пусть f—полином над полем действительных чисел, у которого старший коэффициент и свободный член имеют разные знаки. Докажите, что полином f имеет хотя бы один действительный корень.

§ 3. УРАВНЕНИЯ ТРЕТЬЕЙ И ЧЕТВЕРТОЙ СТЕПЕНИ

Уравнения третьей степени. Уравнение

(1) $x^3+px+q=0 \quad (p,\ q\in\mathbf{C})$

называется *неполным кубическим уравнением*. В уравнении (1) положим $x=u+v$, т. е. вместо одной переменной введем две. Получим

$$(u+v)^3+p(u+v)+q=0,$$

или

(2) $u^3+v^3+q+(3uv+p)(u+v)=0.$

Потребуем, чтобы выполнялось условие $3uv+p=0$, т. е. условие $uv=-p/3$. При выполнении этого условия u и v удовлетворяют системе

(3) $u^3+v^3=-q, \quad uv=-p/3.$

На основании (3), (2) и (1) заключаем: если $(u,\ v)$ есть решение системы (3), то сумма $u+v$ является решением уравнения (1).

Покажем, что верно также обратное утверждение: если x есть корень уравнения (1), то существует такое решение $(u,\ v)$ системы (3), что $x=u+v$. В самом деле, пусть x — корень уравнения (1). Рассмотрим уравнение

$$y^2-xy-p/3=0.$$

Пусть $u,\ v$ — его комплексные корни. Тогда, по формулам Виета,

$$x=u+v, \quad uv=-p/3.$$

Так как x — корень уравнения (1), то $(u,\ v)$ есть решение (2) и, следовательно, решение системы (3). Таким образом, зная решения системы (3), можно найти все корни уравнения (1).

Система уравнений

(4) $u^3+v^3=-q, \quad u^3v^3=-p^3/27,$

очевидно, есть следствие системы (3). Числа u, v удовлетворяют (4) тогда и только тогда, когда числа u^3, v^3 являются корнями квадратного уравнения

(5) $z^2+qz-p^3/27=0.$

Это уравнение называется *разрешающим для уравнения* (1). Его дискриминант обозначим через Δ:

$$\Delta=\frac{q^2}{4}+\frac{p^3}{27}.$$

Корни z_1, z_2 уравнения (5) выражаются формулами

(6) $z_1=u^3=-q/2+\sqrt{\Delta}, \quad z_2=v^3=-q/2-\sqrt{\Delta}.$

Отсюда находим девять решений системы (4). Отбирая из них только такие решения (u, v) системы (4), которые удовлетворяют условию $uv=-p/3$, получаем все решения системы (3).

Система (3) имеет хотя бы одно решение. В самом деле, пусть (u_1, v_1) есть какое-нибудь решение системы (4), тогда $u_1^3v_1^3=-p^3/27$. Значит,

$$u_1v_1=-\frac{p}{3}, \quad \text{или} \quad u_1v_1=-\frac{p}{3}\cdot\varepsilon, \quad \text{или} \quad u_1v_1=-\frac{p}{3}\cdot\varepsilon^2,$$

где $\varepsilon^3=1$;

поэтому

$$u_1v_1=-\frac{p}{3}, \quad \text{или} \quad u_1(v_1\varepsilon^2)=-\frac{p}{3}, \quad \text{или} \quad u_1(v_1\varepsilon)=-\frac{p}{3}.$$

Следовательно, для любого значения u корня третьей степени из z_1 существует такое значение v корня третьей степени из z_2, что $uv=-p/3$, т. е. пара (u, v) будет решением системы (3).

Если u, $u\varepsilon$, $u\varepsilon^2$ — значения корня третьей степени из z_1, то им соответствуют v, $v\varepsilon^2$, $v\varepsilon$ — значения корня третьей степени из z_2. Таким образом, если (u, v) — какое-нибудь решение системы (3), то (u, v), $(u\varepsilon, v\varepsilon^2)$, $(u\varepsilon^2, v\varepsilon)$ есть совокупность всех решений системы (3) — система (3) имеет три различных решения. Заключаем, что уравнение (1) имеет следующие решения:

(7) $x_1=u+v, \quad x_2=u\varepsilon+v\varepsilon^2, \quad x_3=u\varepsilon^2+v\varepsilon.$

ТЕОРЕМА 3.1. *Пусть дано уравнение*

(1) $x^3+px+q=0.$

Пусть z_1 и z_2 — *корни разрешающего уравнения* $z^2+qz-p^3/27=0$. *Корни уравнения* (1) *выражаются формулами*

(I) $x_1=u+v, \quad x_2=u\varepsilon+v\varepsilon^2, \quad x_3=u\varepsilon^2+v\varepsilon,$

где u и v — *числа, удовлетворяющие условиям*

(*) $u^3=z_1, \quad v^3=z_2, \quad uv=-p/3,$

и ε — *мнимый корень третьей степени из единицы.*

Доказательство. Непосредственная проверка показывает, что x^3+px+q делится на $x-x_1$, причем частное равно $x^2+x_1x+x_1^2+p$; следовательно,

(2) $x^3+px+q=(x-x_1)(x^2+x_1x+x_1^2+p).$

Далее, имеем

(3) $(x-x_2)(x-x_3)=x^2-(x_2+x_3)x+x_2x_3.$

В силу формул Виета

(4) $1+\varepsilon+\varepsilon^2=0 \quad$ и $\quad \varepsilon+\varepsilon^2=-1.$

Отсюда и из формул (I) следует, что

(5) $x_1+x_2+x_3=0, \quad -(x_2+x_3)=x_1.$

В силу формул (I), (*) и (4) получаем

$$x_2x_3=(u\varepsilon+v\varepsilon^2)(u\varepsilon^2+v\varepsilon)=u^2+v^2+uv(\varepsilon^2+\varepsilon)=$$
$$=u^2+v^2-uv=(u+v)^2-3uv=x_1^2+p,$$

т. е.

(6) $x_2x_3=x_1^2+p.$

В силу (5) и (6) формулу (3) можно записать в виде

(7) $(x-x_2)(x-x_3)=x^2+x_1x+x_1^2+p.$

На основании (2) и (7) заключаем, что

$$x^3+px+q=(x-x_1)(x-x_2)(x-x_3). \quad \square$$

СЛЕДСТВИЕ 3.2. *Корни уравнения* (1) *выражаются формулами*

(II) $x_1=u+v; \quad x_2=-\frac{1}{2}(u+v)+i\frac{\sqrt{3}}{2}(u-v);$

$$x_3=-\frac{1}{2}(u+v)-i\frac{\sqrt{3}}{2}(u-v),$$

где u и v — *числа, удовлетворяющие условиям* (*).

Доказательство. Формулы (II) получаются из формул (I), если положить $\varepsilon = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$. □

Исследование корней уравнения третьей степени с действительными коэффициентами. Следующая теорема дает возможность определять число действительных и мнимых корней уравнения третьей степени.

ТЕОРЕМА 3.3. *Пусть*

(1) $x^3 + px + q = 0$

— уравнение с действительными коэффициентами и $\Delta = \frac{q^2}{4} + \frac{p^3}{27}$. *Тогда*:

(a) *если* $\Delta > 0$, *то уравнение* (1) *имеет один действительный корень и два мнимых сопряженных*;

(b) *если* $\Delta = 0$, *то корни уравнения* (1) *действительны и хотя бы один из них кратный*;

(c) *если* $\Delta < 0$, *то все корни уравнения* (1) *действительны и различны.*

Доказательство. Первый случай: $\Delta > 0$. В этом случае корни z_1 и z_2 разрешающего уравнения действительны и различны. Следовательно, хотя бы один из них, например z_1, отличен от нуля. Пусть $u = (z_1)^{1/3}$ — арифметический корень из z_1. Число v также является действительным числом, поскольку $uv = -p/3$. Так как $z_1 \neq z_2$ и, значит, $u^3 \neq v^3$, то $u \neq v$. По следствию 3.2,

$$\text{(II)} \quad x_1 = u + v, \quad x_2 = -\frac{1}{2}(u+v) + i\frac{\sqrt{3}}{2}(u-v),$$

$$x_3 = -\frac{1}{2}(u+v) - i\frac{\sqrt{3}}{2}(u-v).$$

Поскольку u и v — действительные различные числа, из формул (II) следует, что x_1 — действительный корень, а x_2 и x_3 — мнимые сопряженные.

Второй случай: $\Delta = 0$. Если $\Delta = 0$ и $q \neq 0$, то $z_1 = z_2 = -q/2 \neq 0$. Пусть $u = (-q/2)^{1/3}$ — арифметический корень из числа $-q/2$. Поскольку $uv = p/3$ есть действительное число, то $v = (-q/2)^{1/3}$, т. е. $u = v \neq 0$. В силу формул (II) отсюда следует, что

$$x_1 = 2u \neq 0, \quad x_2 = x_3 = -u.$$

Таким образом, при $q \neq 0$ уравнение (I) имеет три действительных корня, причем один из них двукратный.

Если же $\Delta=0$ и $q=0$, то и $p=0$. В этом случае уравнение (1) имеет вид $x^3=0$. Следовательно, $x_1=x_2=x_3=0$.

Третий случай: $\Delta<0$. В этом случае $z_1=-q/2+\sqrt{\Delta}$, $z_2=-q/2-\sqrt{\Delta}$.

Следовательно, z_1 и z_2 — мнимые сопряженные числа, поэтому

(1) $|z_1|=|z_2|\neq 0$

и

(2) $z_1\neq z_2$.

В силу теоремы 3.1 существуют числа u и v такие, что

(3) $u^3=z_1$, $uv=-p/3$, $v^3=z_2$.

Из (1) и (3) следует, что $|u|^3=|v|^3\neq 0$ и, значит.

(4) $|u|=|v|\neq 0$.

Далее, в силу (2)

(5) $u\neq v$.

На основании (3) и (4) заключаем, что

(6) $-\frac{p}{3|u|^2}=1$.

На основании (3) и (6) получаем

(7) $v=-\frac{p}{3u}=-\frac{p}{3u\bar{u}}\cdot\bar{u}=-\frac{p}{3|u|^2}\cdot\bar{u}=\bar{u}$.

Из (5) и (7) следует, что u и v — мнимые сопряженные числа. По следствию 3.2 имеем:

(II)
$$x_1=u+v;$$
$$x_2=-\frac{1}{2}(u+v)+i\frac{\sqrt{3}}{2}(u-v);$$
$$x_3=-\frac{1}{2}(u+v)-i\frac{\sqrt{3}}{2}(u-v).$$

Поскольку $\bar{u}=v$ и $u\neq v$, из этих формул следует, что все корни x_1, x_2 и x_3 действительны. Кроме того, они попарно различны. Действительно, в силу формул (II) $x_2\neq x_3$. Допустим, что $x_1=x_2$. Тогда в силу формул (I) $u+v=u\varepsilon+v\varepsilon^2$, откуда $u(1-\varepsilon)=v(\varepsilon^2-1)$; поэтому $u=v\varepsilon^2$. Отсюда вытекают равенства $z_1=z_2$ и $\Delta=0$; однако последнее равенство противоречит условию $\Delta<0$.

Аналогично убеждаемся, что $x_1 \neq x_3$. □

Уравнения четвертой степени. По методу Феррари решение уравнения четвертой степени сводится к решению некоторого вспомогательного уравнения третьей степени. Метод Феррари состоит в следующем. Данное уравнение четвертой степени с комплексными коэффициентами

$$(1)\quad x^4+ax^3+bx^2+cx+d=0$$

запишем в виде $x^4+ax^3=-bx^2-cx-d$. Прибавив к обеим частям уравнения $a^2x^2/4$, получим

$$\left(x^2+\frac{ax}{2}\right)^2=\left(\frac{a^2}{4}-b\right)x^2-cx-d.$$

Далее, прибавив к обеим частям уравнения сумму

$$\left(x^2+\frac{ax}{2}\right)y+\frac{y^2}{4},$$

в левой части уравнения получим полный квадрат:

$$(2)\quad \left(x^2+\frac{ax}{2}+\frac{y}{2}\right)^2=\left(\frac{a^2}{4}-b+y\right)x^2+\left(\frac{ay}{2}-c\right)x+\frac{y^2}{4}-d.$$

Трехчлен справа зависит от параметра y. Подберем параметр y так, чтобы этот трехчлен был квадратом двучлена первой степени от x. Для того чтобы трехчлен Ax^2+Bx+C был квадратом линейного двучлена от x, достаточно, чтобы $B^2-4AC=0$. В самом деле, при выполнении этого условия получаем

$$Ax^2+Bx+C=Ax^2+2\sqrt{AC}\,x+C=(\sqrt{A}x+\sqrt{C})^2.$$

Следовательно, в правой части (2) надо подобрать y так, чтобы выполнялось условие

$$\left(\frac{ay}{2}-c\right)^2-4\left(\frac{a^2}{4}-b+y\right)\left(\frac{y^2}{4}-d\right)=0,$$

которое можно записать в виде

$$(3)\quad y^3-by^2+(ac-4d)\,y-[c^2+d\,(a^2-4b)]=0.$$

При выполнении этого условия правая часть уравнения (2) будет квадратом линейного двучлена от x.

Решая вспомогательное уравнение (3), найдем один из его корней y_0. Затем найдем числа m и n такие, чтобы квадрат двучлена $mx+n$ был равен правой части равенства (2), тогда

$$(4)\quad \left(x^2+\frac{ax}{2}+\frac{y_0}{2}\right)^2=(mx+n)^2,$$

где $m=\sqrt{\frac{a^2}{4}-b+y_0}$, $n=\sqrt{\frac{y_0^2}{4}-d}$. Решение уравнения (4) сводится к решению совокупности следующих двух квадратных уравнений:

$$x^2+\frac{ax}{2}+\frac{y_0}{2}=mx+n,\quad x^2+\frac{ax}{2}+\frac{y_0}{2}=-mx-n.$$

Решив эти два уравнения, найдем все четыре корня исходного уравнения (1).

Упражнения

1. Решите следующие уравнения третьей степени:

(a) $x^3-3x+2=0$; (b) $x^3-6x+4=0$;

(c) $x^3+3x-x+4=0$; (d) $x^3+3x-2i=0$.

2. Решите следующие уравнения четвертой степени:

(a) $x^4+2x^3+2x^2+x-7=0$;

(b) $x^4-x^3-x^2+2x-2=0$;

(c) $x^4+12x+3=0$.

3. Докажите, что $(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2=-4p^3-27q^2$, где x_1, x_2, x_3 — корни уравнения $x^3+px+q=0$.

§ 4. ОТДЕЛЕНИЕ ДЕЙСТВИТЕЛЬНЫХ КОРНЕЙ ПОЛИНОМА

Система полиномов Штурма. Пусть f — полином с действительными коэффициентами, a и b, $a<b$ — произвольные действительные числа, не являющиеся корнями полинома.

Ниже методом Штурма решается задача о нахождении точного числа различных действительных корней полинома f в интервале $a<x<b$.

Пусть дана конечная последовательность действительных чисел, например 2, 5, —3, 4, —5, —2, 7. Знаки чисел этой последовательности чередуются следующим образом: +, +, —, +, —, —, + и меняются четыре раза. Таким образом, в данной последовательности имеется четыре перемены знаков.

Пусть f — полином положительной степени с действительными коэффициентами, не имеющий кратных действительных корней. Определим конечную последовательность полиномов $f_0, f_1, f_2, \ldots, f_m$, исходя из данного полинома

$f_0 = f$, следующим образом:

$f_1 = f'$, где f' — производная от f;

$f_0 = q_1 f_1 - f_2$;

$f_1 = q_2 f_2 - f_3$;

. . . . . .

$f_{m-1} = q_m f_m$.

Таким образом, мы применяем к полиномам f и f' алгоритм Евклида (способ последовательного деления), изменяя при этом всякий раз знак остатка на противоположный.

ОПРЕДЕЛЕНИЕ. Последовательность полиномов f_0, $f_1, f_2, \ldots, f_m$ называется *системой полиномов Штурма для* f.

Отметим некоторые свойства полиномов системы Штурма.

СВОЙСТВО 4.1. *Любые два соседних полинома системы Штурма не имеют общих действительных корней.*

Доказательство. Это утверждение верно для полиномов f_0 и f_1 ($f_0 = f$, $f_1 = f'$), так как f не имеет кратных действительных корней. Три рядом стоящие полинома связаны равенством

$$(*) \quad f_{k-1} = q_k f_k - f_{k+1}.$$

В силу этого равенства одновременное обращение в нуль соседних полиномов f_k и f_{k+1} повлекло бы за собой одновременное обращение в нуль f_{k-1} и f_k, затем то же для полиномов f_{k-2} и f_{k-1} и т. д., наконец, для полиномов f_0 и f_1, что невозможно. □

СВОЙСТВО 4.2. *Если γ — действительный корень промежуточного полинома f_k, $1 \leqslant k < m$, то числа $f_{k-1}(\gamma)$ и $f_{k+1}(\gamma)$ имеют разные знаки.*

Доказательство. В самом деле, если $f_k(\gamma) = 0$, то, полагая в равенстве (*) $x = \gamma$, получаем $f_{k-1}(\gamma) = -f_{k+1}(\gamma)$. □

Теорема Штурма. При доказательстве теоремы Штурма будет использована следующая теорема Вейерштрасса: если действительная функция f непрерывна на отрезке $[a, b]$ и числа $f(a)$, $f(b)$ имеют разные знаки, то f имеет корень между a и b.

Пусть f — полином с действительными коэффициентами. Пусть для каждого действительного числа c $w(c)$ обозначает число перемен знака в числовом ряде $f_0(c), f_1(c), \ldots, f_m(c)$, в котором опущены все нули.

ТЕОРЕМА (Штурма). *Пусть f — полином с действительными коэффициентами, не имеющий кратных действительных корней, и*

(1) $f_0, f_1, \ldots, f_m$

— система полиномов Штурма для f. Пусть a и b $(a<b)$ — произвольные действительные числа, не являющиеся корнями полинома f. Число различных действительных корней полинома f в интервале (a, b) равно разности $w(a)-w(b)$.

Доказательство. Пусть M — множество всех действительных корней полиномов (1). Элементы множества M разбивают интервал (a, b) на подынтервалы. Внутри каждого такого подынтервала ни один из полиномов (1) не обращается в нуль. В силу теоремы Вейерштрасса отсюда следует, что внутри каждого подынтервала все полиномы (1) сохраняют свои знаки и, значит, число $w(c)$ не изменяется. Нам остается исследовать, как изменится число $w(c)$ при переходе через действительное значение γ, в котором хотя бы один из полиномов (1) обращается в нуль, т. е. $\gamma \in M$.

Пусть α и β $(\alpha<\beta)$ — внутренние точки двух соседних подынтервалов, примыкающих к точке γ. Докажем, что разность $w(\alpha)-w(\beta)$ выражается формулами

$$(2)\quad w(\alpha)-w(\beta)=\begin{cases}1, & \text{если } f(\gamma)=0,\\ 0, & \text{если } f(\gamma)\neq 0.\end{cases}$$

Предположим, что γ — корень полинома f_k, где $1\leqslant k<m$. По свойству 4.2, числа $f_{k-1}(\gamma)$ и $f_{k+1}(\gamma)$ имеют противоположные знаки. Поэтому в двух подынтервалах, примыкающих к γ, значения полиномов f_{k-1} и f_{k+1} имеют противоположные знаки. Следовательно, число перемен знаков в последовательностях

$$f_{k-1}(\alpha),\ f_k(\alpha),\ f_{k+1}(\alpha) \text{ и } f_{k-1}(\beta),\ f_k(\beta),\ f_{k+1}(\beta)$$

одно и то же, а именно равно единице. В остальных частях системы полиномов (1) число перемен знаков не меняется. Следовательно, в рассматриваемом случае $w(\alpha)-w(\beta)=0$.

Предположим теперь, что γ — корень полинома f $(f=f_0,\ f_1=f')$. Так как, по условию, полином f не имеет кратных действительных корней, то существует такой

полином g с действительными коэффициентами, что

(3) $f_0(x) = (x-\gamma)g(x),\ g(\gamma) \neq 0;$

следовательно,

(4) $f_1(x) = g(x) + (x-\gamma)g'(x).$

В силу (4) знак полинома f_1 в точке γ, а следовательно, и в обоих примыкающих к γ подынтервалах совпадает со знаком числа $g(\gamma)$. В то же время в силу (3) знак f_0 для каждого значения x совпадает со знаком $(x-\gamma)g(\gamma)$. Следовательно, между $f_0(\alpha)$ и $f_1(\alpha)$ есть одна перемена знака, а числа $f_0(\beta)$ и $f_1(\beta)$ имеют один и тот же знак. При этом все остальные возможные перемены знака в ряде (1), как уже показано, сохраняются при переходе через точку γ. Таким образом, в рассматриваемом случае $w(\alpha) - w(\beta) = 1$.

Итак, доказано, что только при переходе через значение корня полинома f число $w(c)$ уменьшается на единицу. Следовательно, число различных действительных корней полинома f равно разности $w(a) - w(b)$. □

Теорема Штурма верна также и в том случае, когда полином имеет кратные действительные корни. Доказательство теоремы в этом случае несущественным образом отличается от доказательства, приведенного выше.

Для определения числа всех различных корней полинома f с помощью теоремы Штурма удобно выбрать a и b такими, чтобы ни один полином системы Штурма не имел корней вне интервала $a \leqslant x \leqslant b$. Тогда знаки полиномов системы Штурма будут определяться знаками их старших коэффициентов. Действительно, для очень больших значений x знак полинома $a_0x^n + a_1x^{n-1} + \ldots + a_n$ совпадает со знаком a_0, а для очень больших по абсолютной величине отрицательных значений x знак полинома совпадает со знаком $(-1)^n a_0$. Следовательно, при таком способе нет необходимости думать о том, как велики должны быть a и b, так как достаточно знать только знаки старших коэффициентов полиномов системы Штурма для f и степени этих полиномов.

Используя теорему Штурма, можно действительные корни полинома f отделить — найти интервалы, в каждом из которых лежит только один корень полинома f.

Пример. Найдем число положительных и отрицательных корней полинома $f = x^4 - 4x^2 + x + 1$.

Применив метод последовательного деления, находим для f следующую систему полиномов Штурма:

$$f_0 = f = x^4 - 4x^2 + x + 1;$$
$$f_1 = 4x^3 - 8x + 1;$$
$$f_2 = 8x^2 - 3x - 4;$$
$$f_3 = 87x - 28;$$
$$f_4 = 1.$$

Для отрицательного и достаточно большого по абсолютной величине значения x ряд знаков будет $+$, $-$, $+$, $-$, $+$ (четыре перемены знака). При $x = 0$ знаки совпадают со знаками свободных членов, т. е. $+$, $+$, $-$, $-$, $+$ (две перемены знака).

Таким образом, потеряны две перемены знака, следовательно, полином f имеет два отрицательных корня. Для положительного достаточно большого значения x имеем знаки старших членов $+$, $+$, $+$, $+$, $+$ (нуль перемен знака). Следовательно, полином имеет два положительных корня.

Упражнения

1. Составьте полиномы Штурма и отделите корни полиномов: (a) $x^3 - 3x - 3$; (b) $x^4 - x - 1$; (c) $x^4 - 4x^3 + 4x^2 - 4$; (d) $x^4 - 4x^2 - 1$.

2. Определите с помощью теоремы Штурма число действительных корней полинома $x^5 + px + q$ с действительными коэффициентами p и q.

3. Определите с помощью теоремы Штурма число действительных корней полинома $x^n + px + q$ при действительных p и q.

4. Докажите, что если система Штурма для полинома f степени n с действительными коэффициентами состоит из $n + 1$ полиномов, то число перемен знака в ряду старших коэффициентов полиномов Штурма равно числу пар сопряженных комплексных корней полинома f.

5. Найдите число действительных корней полинома $x^4 - 2x^2 + 4x - 1$. Между какими последовательными целыми числами лежат эти корни?

Глава семнадцатая

ПОЛИНОМЫ НАД ПОЛЕМ РАЦИОНАЛЬНЫХ ЧИСЕЛ И АЛГЕБРАИЧЕСКИЕ ЧИСЛА

§ 1. ЦЕЛЫЕ И РАЦИОНАЛЬНЫЕ КОРНИ ПОЛИНОМА. КРИТЕРИЙ НЕПРИВОДИМОСТИ

Целые и рациональные корни полинома. Следующая теорема дает возможность найти рациональные корни полинома с целыми коэффициентами.

ТЕОРЕМА 1.1. *Пусть m и q — целые взаимно простые числа и $q \neq 0$. Если m/q — корень полинома $a_0+a_1x+\ldots+a_nx^n$ с целыми коэффициентами, то m делит a_0 и q делит a_n.*

Доказательство. По условию,

$$a_0+a_1\frac{m}{q}+\ldots+a_{n-1}\left(\frac{m}{q}\right)^{n-1}+a_n\left(\frac{m}{q}\right)^n=0.$$

Умножив обе части равенства на q^n, получим

$$(1)\quad a_0q^n+a_1mq^{n-1}+\ldots+a_{n-1}m^{n-1}q+a_nm^n=0.$$

На основании равенства (1) заключаем, что m делит a_0q^n. А так как числа m и q — взаимно простые, то взаимно простыми будут числа m и q^n. Следовательно, m делит a_0.

В силу (1) q делит a_nm^n. Кроме того, числа q и m^n — взаимно простые, так как, по условию, числа q и m — взаимно простые. Следовательно, q делит a_n. □

СЛЕДСТВИЕ 1.2. *Если целое число m есть корень полинома $a_0+a_1x+\ldots+a_nx^n$ с целыми коэффициентами, то m делит свободный член a_0.*

СЛЕДСТВИЕ 1.3. *Рациональный корень нормированного полинома $a_0+a_1x+\ldots+x^n$ с целыми коэффициентами является целым числом.*

Критерий неприводимости Эйзенштейна. Вопрос о приводимости полинома в кольце $\mathbb{Q}[x]$ сводится к вопросу о приводимости в кольце $\mathbb{Z}[x]$.

ПРЕДЛОЖЕНИЕ 1.4. *Пусть f — полином из кольца полиномов $\mathbb{Z}[x]$. Если полином f приводим в кольце $\mathbb{Q}[x]$, то он приводим в кольце $\mathbb{Z}[x]$.*

Поскольку поле $\mathbb{Q}$ является полем частных кольца $\mathbb{Z}$ целых чисел, то предложение 1.4 непосредственно следует из леммы 14.3.5.

ТЕОРЕМА 1.5 (критерий Эйзенштейна). *Пусть* $f = c_0 + c_1 x + \ldots + c_n x^n$ *— полином с целыми коэффициентами. Пусть все коэффициенты полинома* f, *кроме старшего, делятся на какое-нибудь простое число* p *и свободный член* c_0 *не делится на* p^2. *Тогда полином* f *неприводим в кольце* $\mathbb{Q}[x]$.

Доказательство. Допустим, что полином f приводим в кольце $\mathbb{Q}[x]$. Тогда в силу предложения 1.4 он приводим в кольце $\mathbb{Z}[x]$, т. е. в $\mathbf{Z}[x]$ существуют такие полиномы g и h положительной степени, что $f = gh$. Пусть

$$g = a_0 + \ldots + a_k x^k, \quad h = b_0 + \ldots + b_m x^m \quad (a_k \neq 0, \ b_m \neq 0);$$

тогда

(1) $f = (a_0 + \ldots + a_k x^k)(b_0 + \ldots + b_m x^m) = c_0 + c_1 x + \ldots + c_n x^n$,

причем $1 \leqslant k, \ m < n$,

(2) $c_0 = a_0 b_0$,

(3) $c_n = a_k b_m$.

По условию,

(4) $p \mid c_0, \quad p^2 \nmid c_0$.

В силу (2) и (4) только одно из чисел a_0 и b_0 делится на p; пусть

(5) $p \mid a_0, \ p \nmid b_0$.

По условию, $p \nmid c_n$. Отсюда в силу (3) следует, что

(6) $p \nmid a_k$.

Пусть a_s — не делящийся на p коэффициент полинома g с наименьшим индексом, т. е.

(7) $p \mid a_0, \ \ldots, \ p \mid a_{s-1}, \ p \nmid a_s \qquad (1 \leqslant s \leqslant k < n)$.

В силу (1) коэффициент c_s можно представить в виде

$$c_s = a_s b_0 + (a_{s-1} b_1 + \ldots + a_0 b_s) \qquad (s < n).$$

Из (7) следует, что p делит $a_{s-1} b_1 + \ldots + a_0 b_s$, а так как p не делит b_0 и a_s, то p не делит c_s, причем $s \leqslant k < n$. Это противоречит условию теоремы, поскольку, по условию, p делит коэффициенты $c_0, \ c_1, \ \ldots, \ c_{n-1}$. □

СЛЕДСТВИЕ 1.6. *Если p — простое число и n — любое целое положительное число, то полином $x^n - p$ неприводим в кольце $\mathbb{Q}[x]$.*

Упражнения.

1. Докажите, что полином f с целыми коэффициентами не имеет целых корней, если $f(0)$ и $f(1)$ — нечетные числа.

2. Установите, какие из следующих полиномов неприводимы над полем рациональных чисел:
(a) $2x^5+6x^4-9x^2+12$; (b) x^2+x+1; (c) x^2+3x-4; (d) x^3-12; (e) x^3+x-2; (f) x^3-3x+5; (g) x^4-2x+3.

3. Докажите, что полином $\frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\ldots+x+1$, где p — простое число, неприводим над полем рациональных чисел.

4. Докажите, что полином x^3-p, где p — простое число, неприводим над полем рациональных чисел.

5. Для каких целых чисел n полином x^3+n приводим над полем рациональных чисел?

6. Для каких целых чисел m и n полином mx^3+n приводим над полем рациональных чисел?

7. Разложите полиномы x^6-1 и x^8-1 на неприводимые над полем рациональных чисел множители.

8. Найдите условия приводимости полинома $x^4+\alpha x^2+\beta$, где α, β — рациональные числа, над полем рациональных чисел.

9. Докажите, что если полином f неприводим над полем $\mathbb{Q}$ рациональных чисел, то полином $f(\alpha x+\beta)$, где α, β — рациональные числа и $\alpha \neq 0$, также неприводим над полем $\mathbb{Q}$.

§ 2. ПРОСТОЕ АЛГЕБРАИЧЕСКОЕ РАСШИРЕНИЕ ПОЛЯ

Простое расширение поля. Пусть $\mathcal{P}[x]$ — кольцо полиномов от x над полем $\mathcal{P}$, где $\mathcal{P}$ — подполе поля $\mathcal{F}$. Напомним, что элемент α поля $\mathcal{F}$ называется *алгебраическим над полем* $\mathcal{P}$, если α является корнем какого-нибудь полинома положительной степени из $\mathcal{P}[x]$.

ОПРЕДЕЛЕНИЕ. Пусть $\mathcal{P} \subset \mathcal{F}$ и $\alpha \in F$. *Простым расширением поля $\mathcal{P}$ с помощью элемента α* называется наименьшее подполе поля $\mathcal{F}$, содержащее множество P и элемент α. Простое расширение $\mathcal{P}$ с помощью α обозначается через $\mathcal{P}(\alpha)$, основное множество поля $\mathcal{P}(\alpha)$ обозначается через $P(\alpha)$.

Пусть $\alpha \in F$, $\mathcal{P}[x]$ — кольцо полиномов от x и

$$P[\alpha] = \{f(\alpha) \mid f \in P[x]\},$$

т. е. $P[\alpha]$ есть множество всех выражений вида $a_0+a_1\alpha+\ldots+a_n\alpha^n$, где $a_0, a_1, \ldots, a_n \in P$ и n — любое натуральное число.

Легко видеть, что алгебра $\langle P[\alpha], +, -, \cdot, 1\rangle$ — подкольцо поля $\mathscr{P}(\alpha)$ — является кольцом; это кольцо обозначается символом $\mathscr{P}[\alpha]$.

ТЕОРЕМА 2.1. *Пусть $\mathscr{P}[x]$ — кольцо полиномов от x над $\mathscr{P}$ и $\mathscr{P}(\alpha)$ — простое расширение поля $\mathscr{P}$. Пусть ψ — отображение $P[x]$ на $P[\alpha]$ такое, что $\psi(f) = f(\alpha)$ для любого f из $P[x]$. Тогда:*

(a) *для любого a из P $\psi(a) = a$;*

(b) $\psi(x) = \alpha$;

(c) ψ является гомоморфизмом кольца $\mathscr{P}[x]$ на кольцо $\mathscr{P}[\alpha]$;

(d) $\operatorname{Ker}\psi = \{f \in P[x] \mid f(\alpha) = 0\}$;

(e) фактор-кольцо $\mathscr{P}[x]/\operatorname{Ker}\psi$ изоморфно кольцу $\mathscr{P}[\alpha]$.

Доказательство. Утверждения (a) и (b) непосредственно следуют из определения ψ. Отображение ψ сохраняет главные операции кольца $\mathscr{P}[x]$, так как для любых f и g из $P[x]$

$$\psi(f+g) = f(\alpha) + g(\alpha),\ \psi(fg) = f(\alpha)\,g(\alpha),\ \psi(1) = 1.$$

Далее, по условию, ψ есть отображение $P[x]$ на $P[\alpha]$. Следовательно, ψ является гомоморфизмом кольца $\mathscr{P}[x]$ на кольцо $\mathscr{P}[\alpha]$.

Утверждение (d) непосредственно следует из определения отображения ψ.

Поскольку ψ — гомоморфизм кольца $\mathscr{P}[x]$ на $\mathscr{P}[\alpha]$, то, по теореме 13.1.6, фактор-кольцо $\mathscr{P}[x]/\operatorname{Ker}\psi$ изоморфно кольцу $\mathscr{P}[\alpha]$. □

СЛЕДСТВИЕ 2.2. *Пусть α — трансцендентный элемент над полем $\mathscr{P}$. Тогда кольцо полиномов $\mathscr{P}[x]$ изоморфно кольцу $\mathscr{P}[\alpha]$.*

Доказательство. В силу трансцендентности α над $\mathscr{P}$ $\operatorname{Ker}\psi = \{0\}$. Поэтому, согласно теореме 13.1.6, $\mathscr{P}[x]/\{0\} \cong \mathscr{P}[\alpha]$. Кроме того, фактор-кольцо кольца $\mathscr{P}[x]$ по нулевому идеалу изоморфно $\mathscr{P}[x]$. Следовательно, $\mathscr{P}[x] \cong \mathscr{P}[\alpha]$. □

Минимальный полином алгебраического элемента. Пусть $\mathscr{P}[x]$ — кольцо полиномов над полем $\mathscr{P}$.

ОПРЕДЕЛЕНИЕ. Пусть α — алгебраический элемент над полем $\mathscr{P}$. *Минимальным полиномом элемента α* над $\mathscr{P}$ называется нормированный полином из $\mathscr{P}[x]$ наименьшей степени, корнем которого является α. Степень минимального полинома называется *степенью элемента α над $\mathscr{P}$.*

Легко видеть, что для всякого элемента α, алгебраического над $\mathcal{F}$, существует минимальный полином.

ПРЕДЛОЖЕНИЕ 2.3. *Если α — алгебраический элемент над полем $\mathcal{F}$, а g и φ — его минимальные полиномы над $\mathcal{F}$, то $g = \varphi$.*

Доказательство. Степени минимальных полиномов g и φ совпадают. Если $g \neq \varphi$, то элемент α (степени n над $\mathcal{F}$) будет корнем полинома $g - \varphi$, степень которого меньше степени полинома φ (меньше n), что невозможно. Следовательно, $g = \varphi$. □

ТЕОРЕМА 2.4. *Пусть α — алгебраический элемент степени n над полем $\mathcal{F}$ ($\alpha \notin P$) и g — его минимальный полином над $\mathcal{F}$. Тогда:*

(a) *полином g неприводим в кольце $\mathcal{F}[x]$;*

(b) *если $f(\alpha) = 0$, где $f \in P[x]$, то g делит f;*

(c) *фактор-кольцо $\mathcal{F}[x]/(g)$ изоморфно кольцу $\mathcal{F}[\alpha]$;*

(d) *$\mathcal{F}[x]/(g)$ является полем;*

(e) *кольцо $\mathcal{F}[\alpha]$ совпадает с полем $\mathcal{F}(\alpha)$.*

Доказательство. Допустим, что полином g приводим в кольце $\mathcal{F}[x]$, т. е. существуют в $P[x]$ такие полиномы φ и h, что

$$g = \varphi h, \quad 1 \leqslant \deg \varphi, \quad \deg h < \deg g = n.$$

Тогда $g(\alpha) = \varphi(\alpha)\, h(\alpha) = 0$. Так как $\mathcal{F}(\alpha)$ — поле, то $\varphi(\alpha) = 0$ или $h(\alpha) = 0$, что невозможно, поскольку, по условию, степень элемента α над $\mathcal{F}$ равна n.

Предположим, что $f \in P[x]$ и $f(\alpha) = 0$. По условию, $g(\alpha) = 0$. Следовательно, f и g не могут быть взаимно простыми. Поскольку полином g неприводим, то g делит f.

Пусть ψ — гомоморфизм кольца $\mathcal{F}[x]$ на кольцо $\mathcal{F}[\alpha]$ ($\psi(f) = f(\alpha)$ для всякого f из $P[x]$), рассмотренный в теореме 2.1. В силу (b) ядро гомоморфизма ψ состоит из кратных полинома g, т. е. $\operatorname{Ker} \psi = (g)$. Следовательно, по теореме 13.1.6, фактор-кольцо $\overline{\mathcal{F}} = \mathcal{F}[x]/(g)$ изоморфно кольцу $\mathcal{F}[\alpha]$.

Поскольку $P[\alpha] \subset P(\alpha)$, то $\mathcal{F}[\alpha]$ есть область целостности. Так как $\overline{\mathcal{F}} \cong \mathcal{F}[\alpha]$, то фактор-кольцо $\overline{\mathcal{F}}$ также есть область целостности. Нам надо показать, что любой ненулевой элемент $\bar{f}$ из $\overline{\mathcal{F}}$ обратим в $\overline{\mathcal{F}}$. Пусть f — элемент смежного класса $\bar{f}$. Так как $\bar{f} \neq \bar{0}$, то $f(\alpha) \neq 0$; поэтому

полином g не делит полином f. Поскольку полином g неприводим, отсюда следует, что полиномы f и g — взаимно простые. Следовательно, в $P[x]$ существуют такие полиномы u и v, что $uf+vg=1$. Отсюда вытекает равенство $\bar{u}\bar{f}=\bar{1}$, показывающее, что элемент $\bar{f}$ обратим в кольце $\overline{\mathscr{P}}$. Итак, установлено, что фактор-кольцо $\overline{\mathscr{P}}$ является полем.

В силу (c) и (d) $\mathscr{P}[\alpha]$ является полем и поэтому $P(\alpha)\subset P[\alpha]$. Кроме того, очевидно, $P[\alpha]\subset P(\alpha)$. Значит, $P[\alpha]=P(\alpha)$. Следовательно, кольцо $\mathscr{P}[\alpha]$ совпадает с полем $\mathscr{P}(\alpha)$. □

Строение простого алгебраического расширения поля.

ТЕОРЕМА 2.5. *Пусть α — алгебраический над полем $\mathscr{P}$ элемент положительной степени n. Тогда любой элемент поля $\mathscr{P}(\alpha)$ однозначно представим в виде линейной комбинации n элементов $1, \alpha, \ldots, \alpha^{n-1}$ с коэффициентами из P.*

Доказательство. Пусть β — любой элемент поля $\mathscr{P}(\alpha)$. По теореме 2.4, $P(\alpha)=P[\alpha]$; следовательно, существует в $P[x]$ полином f такой, что

$$(1)\quad \beta=f(\alpha).$$

Пусть g — минимальный полином для α над $\mathscr{P}$; в силу условия теоремы его степень равна n. По теореме о делении с остатком, существуют в $P[x]$ полиномы h и r такие, что

$$(2)\quad f=gh+r, \text{ где } r=0 \text{ или } \deg r<\deg g=n, \text{ т. е.}$$
$$r=c_0+c_1x+\ldots+c_{n-1}x^{n-1} \qquad (c_i\in P).$$

Полагая в (2) $x=\alpha$ и учитывая равенство (1), имеем

$$(3)\quad \beta=c_0+c_1\alpha+\ldots+c_{n-1}\alpha^{n-1}.$$

Покажем, что элемент β однозначно представим в виде линейной комбинации элементов $1, \alpha, \ldots, \alpha^{n-1}$. Пусть

$$(4)\quad \beta=d_0+d_1\alpha+\ldots+d_{n-1}\alpha^{n-1} \qquad (d_i\in P)$$

— любое такое представление. Рассмотрим полином φ

$$\varphi=(c_0-d_0)+(c_1-d_1)x+\ldots+(c_{n-1}-d_{n-1})x^{n-1}.$$

Случай, когда степень φ меньше n, невозможен, так как в силу (3) и (4) $\varphi(\alpha)=0$ и степень φ меньше степени g. Возможен лишь случай, когда $\varphi=0$, т. е. $c_0=d_0, \ldots, c_{n-1}=d_{n-1}$. Следовательно, элемент β однозначно представим в виде линейной комбинации элементов $1, \alpha, \ldots, \alpha^{n-1}$. □

Освобождение от алгебраической иррациональности в знаменателе дроби. Задача об освобождении от алгебраической иррациональности в знаменателе дроби состоит в следующем. Пусть α — алгебраический элемент степени $n>1$ над полем $\mathscr{P}$; f и h — полиномы из кольца полиномов $\mathscr{P}[x]$ и $h(\alpha)\neq 0$. Требуется представить элемент $\frac{f(\alpha)}{h(\alpha)}\in P(\alpha)$ в виде линейной комбинации степеней элемента α, т. е. в виде $\varphi(\alpha)$, где $\varphi\in P[x]$.

Эта задача решается следующим образом. Пусть g — минимальный полином для α над $\mathscr{P}$. Так как, по теореме 2.4, полином неприводим над $\mathscr{P}$ и $h(\alpha)\neq 0$, то g не делит h и, значит, полиномы h и g — взаимно простые. Поэтому существуют в $P[x]$ такие полиномы u и v, что

(1) $uh+vg=1$.

Поскольку $g(\alpha)=0$, из (1) следует, что

$$u(\alpha)h(\alpha)=1,\quad \frac{1}{h(\alpha)}=u(\alpha).$$

Следовательно, $f(\alpha)/h(\alpha)=f(\alpha)u(\alpha)$, причем $f,\ u\in P[x]$ и $f(\alpha)u(\alpha)\in P[\alpha]$. Итак, мы освободились от иррациональности в знаменателе дроби $\frac{f(\alpha)}{h(\alpha)}$.

Упражнения

1. Найдите минимальный полином для α над полем $\mathscr{P}$, если:

(a) $\alpha=-i$, $\mathscr{P}=\mathscr{R}$; (b) $\alpha=i\sqrt{2}$, $\mathscr{P}=\mathscr{C}$;

(c) $\alpha=i\sqrt{2}$; $\mathscr{P}=\mathscr{Q}$; (d) $\alpha=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$, $\mathscr{P}=\mathscr{Q}$;

(e) $\alpha=\sqrt[4]{2}$, $\mathscr{P}=\mathscr{Q}$.

2. Освободитесь от алгебраической иррациональности в знаменателе дроби $\frac{1}{\sqrt[3]{4}-2\sqrt[3]{2}-1}$.

3. Освободитесь от иррациональности в знаменателе дроби $\frac{1}{\sqrt{2}+2\sqrt[4]{2}-1}$.

§ 3. СОСТАВНОЕ АЛГЕБРАИЧЕСКОЕ РАСШИРЕНИЕ ПОЛЯ

Конечное расширение поля. Пусть $\mathscr{P}$ — подполе поля $\mathscr{F}$. Тогда мы можем рассматривать $\mathscr{F}$ как векторное пространство над $\mathscr{P}$, т. е. рассматривать векторное пространство

$$\langle F,\ +,\ \{\omega_\lambda\,|\,\lambda\in P\}\rangle,$$

где ω_λ — операция умножения элементов из F на скаляр $\lambda \in P$.

ОПРЕДЕЛЕНИЕ. Расширение $\mathscr{F}$ поля $\mathscr{P}$ называется *конечным*, если $\mathscr{F}$, как векторное пространство над $\mathscr{P}$, имеет конечную размерность. Эта размерность обозначается через $[\mathscr{F} : \mathscr{P}]$.

ПРЕДЛОЖЕНИЕ 3.1. *Если α — алгебраический элемент степени n над $\mathscr{P}$, то* $[\mathscr{P}(\alpha) : \mathscr{P}] = n$.

Это предложение непосредственно следует из теоремы 2.5.

ОПРЕДЕЛЕНИЕ. Расширение $\mathscr{F}$ поля $\mathscr{P}$ называется *алгебраическим*, если каждый элемент из F является алгебраическим над $\mathscr{P}$.

ТЕОРЕМА 3.2. *Любое конечное расширение $\mathscr{F}$ поля $\mathscr{P}$ является алгебраическим над $\mathscr{P}$.*

Доказательство. Пусть n-размерность $\mathscr{F}$ над $\mathscr{P}$. Теорема, очевидно, верна, если $n = 0$. Предположим, что $n > 0$. Любые $n+1$ элементов из F линейно зависимы над $\mathscr{P}$. В частности, линейно зависима система элементов $1, \alpha, \ldots, \alpha^n$, т. е. существуют в P такие элементы $c_0, c_1, \ldots, c_n$, не все равные нулю, что

$$c_0 \cdot 1 + c_1\alpha + \ldots + c_n\alpha^n = 0.$$

Следовательно, элемент α является алгебраическим над $\mathscr{P}$. □

Отметим, что существуют алгебраические расширения поля, не являющиеся конечными расширениями.

Составное алгебраическое расширение поля. Расширение $\mathscr{F}$ поля $\mathscr{P}$ называется *составным*, если существует возрастающая цепочка подполей $\mathscr{L}_i$ поля $\mathscr{F}$ такая, что

$$\mathscr{P} = \mathscr{L}_0 \subset \mathscr{L}_1 \subset \ldots \subset \mathscr{L}_k = \mathscr{F} \text{ и } k \geqslant 1.$$

ТЕОРЕМА 3.3. *Пусть $\mathscr{F}$ — конечное расширение поля $\mathscr{L}$ и $\mathscr{L}$ — конечное расширение поля $\mathscr{P}$. Тогда $\mathscr{F}$ является конечным расширением поля $\mathscr{P}$ и*

(I) $[\mathscr{F} : \mathscr{P}] = [\mathscr{F} : \mathscr{L}] \cdot [\mathscr{L} : \mathscr{P}]$.

Доказательство. Пусть

(1) $\alpha_1, \ldots, \alpha_m$

— базис поля $\mathscr{L}$ над $\mathscr{P}$ (как векторного пространства) и

(2) $\beta_1, \ldots, \beta_n$

— базис поля $\mathscr{F}$ над $\mathscr{L}$. Любой элемент d из F можно линейно выразить через базис:

(3) $d = l_1\beta_1 + \ldots + l_n\beta_n$ $(l_k \in L)$.

Коэффициенты l_k можно линейно выразить через базис (1):

(4) $l_k = p_{1k}\alpha_1 + \ldots + p_{mk}\alpha_m \ (p_{ik} \in P)$.

Подставляя выражения для коэффициентов l_k в (3), получаем

$$d = \sum_{\substack{i \in \{1, \ldots, m\} \\ k \in \{1, \ldots, n\}}} p_{ik}\alpha_i\beta_k.$$

Таким образом, каждый элемент поля $\mathscr{F}$ представим в виде линейной комбинации элементов множества B, где

$$B = \{\alpha_i\beta_k \mid i \in \{1, \ldots, m\}, \ k \in \{i, \ldots, n\}\}.$$

Отметим, что множество B состоит из nm элементов.

Покажем, что B есть базис $\mathscr{F}$ над полем $\mathscr{P}$. Нам надо показать, что система элементов множества B линейно независима. Пусть

(5) $\sum\limits_{i,\ k} c_{ik}\alpha_i\beta_k = 0,$

где $c_{ik} \in P$. Так как система (2) линейно независима над $\mathscr{L}$, то из (5) следуют равенства

(6) $c_{1k}\alpha_1 + \ldots + c_{mk}\alpha_m = 0 \ (k = 1, \ldots, n)$.

Поскольку элементы $\alpha_1, \ldots, \alpha_m$ линейно независимы над $\mathscr{P}$, то из (6) следуют равенства

$$c_{1k} = 0, \ \ldots, \ c_{mk} = 0 \ (k = 1, \ldots, n),$$

показывающие, что все коэффициенты в (5) равны нулю. Таким образом, система элементов B линейно независима и является базисом $\mathscr{F}$ над $\mathscr{P}$.

Итак установлено, что $[\mathscr{F}, \mathscr{P}] = nm = [\mathscr{F} : \mathscr{L}] \cdot [\mathscr{L} : \mathscr{P}]$. Следовательно, $\mathscr{F}$ является конечным расширением поля $\mathscr{P}$ и имеет место формула (I). □

ОПРЕДЕЛЕНИЕ. Расширение $\mathscr{F}$ поля $\mathscr{P}$ называется *составным алгебраическим*, если существует возрастающая цепочка подполей поля $\mathscr{P}$

(1) $\mathscr{P} = \mathscr{L}_0 \subset \mathscr{L}_1 \subset \ldots \subset \mathscr{L}_k = \mathscr{F} \ (k > 1)$

такая, что при $i = 1, \ldots, k$ поле $\mathscr{L}_i$ является простым алгебраическим расширением поля $\mathscr{L}_{i-1}$. Число k называется *длиной цепочки* (1).

СЛЕДСТВИЕ 3.4. *Составное алгебраическое расширение $\mathscr{F}$ поля $\mathscr{P}$ является конечным расширением поля $\mathscr{P}$.*

Доказательство легко проводится индукцией по длине цепочки (1) на основании теоремы 3.3.

ТЕОРЕМА 3.5. *Пусть* $\alpha_1, \ldots, \alpha_k$ — *алгебраические над полем* $\mathcal{P}$ *элементы поля* $\mathcal{F}$. *Тогда поле* $\mathcal{P}(\alpha_1, \ldots, \alpha_k)$ *является конечным расширением поля* $\mathcal{P}$.

Доказательство. Пусть

$$\mathcal{L}_0 = \mathcal{P},\ \mathcal{L}_1 = \mathcal{P}[\alpha_1],\ \mathcal{L}_2 = \mathcal{P}[\alpha_1, \alpha_2],\ \ldots,\ \mathcal{L}_k = \mathcal{P}[\alpha_1, \ldots, \alpha_k].$$

Тогда $\mathcal{L}_1 = \mathcal{P}[\alpha_1]$ есть простое алгебраическое расширение поля $\mathcal{L}_0$; $\mathcal{L}_2$ есть простое алгебраическое расширение поля $\mathcal{L}_1$, так как

$$\mathcal{L}_2 = \mathcal{P}[\alpha_1, \alpha_2] = (\mathcal{P}[\alpha_1])[\alpha_2] = \mathcal{L}_1[\alpha_2] = \mathcal{L}_1(\alpha_2) \text{ и т. д.}$$

Таким образом,

$$\mathcal{P} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \ldots \subset \mathcal{L}_k = \mathcal{F},$$

где $\mathcal{L}_i = \mathcal{L}_{i-1}(\alpha_i)$ при $i = 1, \ldots, k$, т. е. каждый член цепочки (2) является простым алгебраическим расширением предшествующего члена цепочки. Итак, поле $\mathcal{F}$ является составным алгебраическим расширением поля $\mathcal{P}$. Следовательно, в силу следствия 3.4 поле $\mathcal{F}$ является конечным расширением поля $\mathcal{P}$. □

СЛЕДСТВИЕ 3.6. *Составное алгебраическое расширение поля является алгебраическим расширением этого поля.*

Простота составного алгебраического расширения поля.

ТЕОРЕМА 3.7. *Пусть числовое поле* $\mathcal{F}$ *есть составное алгебраическое расширение поля* $\mathcal{P}$. *Тогда* $\mathcal{F}$ *является простым алгебраическим расширением поля* $\mathcal{P}$.

Доказательство. Пусть $\mathcal{P} \subset \mathcal{L} \subset \mathcal{F}$, причем $L = P(\alpha)$, $F = L(\beta)$ и, следовательно,

$$F = P(\alpha, \beta).$$

Пусть f и g — минимальные полиномы над $\mathcal{P}$ соответственно для чисел α и β и $\deg f = m$, $\deg g = n$. Полиномы f и g неприводимы над $\mathcal{P}$ и, следовательно, не имеют в поле $\mathcal{C}$ комплексных чисел кратных корней. Пусть

$\alpha = \alpha_1, \ldots, \alpha_m$ — корни полинома f в $\mathbf{C}$ и

$\beta = \beta_1, \ldots, \beta_n$ — корни полинома g в $\mathbf{C}$.

Рассмотрим конечное множество M:

$$M = \left\{ \frac{\alpha_i - \alpha}{\beta - \beta_k} \,\middle|\, i \in \{1, \ldots, m\},\ k \in \{2, \ldots, n\} \right\}.$$

Поскольку $\mathscr{P}$ — числовое множество (и, значит, бесконечное), то в P существует число c, отличное от элементов множества M, $c \in P \setminus M$, $c \notin M$. Пусть

(1) $\gamma = \alpha + c\beta$.

Тогда выполняются соотношения

(2) $\gamma \neq \alpha_i + c\beta_k$ $(i \in \{1, \ldots, m\}, k \in \{2, \ldots, n\})$.

В самом деле, в случае равенства $\alpha + c\beta = \alpha_i + c\beta_k$ было бы

$$c = \frac{\alpha_i - \alpha}{\beta - \beta_k} \in M,$$

что противоречило бы выбору числа c.

Пусть $\mathscr{F}_1 = \mathscr{P}(\gamma)$ и $\mathscr{F}_1[x]$ — кольцо полиномов от x. Пусть $h = f(\gamma - cx)$ — полином из $F_1[x]$ $(\gamma,\ c \in P(\gamma) = F_1)$. Покажем, что $x - \beta$ есть наибольший общий делитель полиномов h и g в кольце $\mathscr{F}_1[x]$. Так как $g(\beta) = 0$, то $x - \beta$ делит g в $\mathscr{C}[x]$. Далее, в силу (1)

$$h(\beta) = f(\gamma - c\beta) = f(\alpha) = 0.$$

Поэтому $x - \beta$ делит полином h в $\mathscr{C}[x]$. Таким образом, $x - \beta$ есть общий делитель h и g в кольце $\mathscr{C}[x]$.

Докажем, что g и h в $\mathbf{C}$ не имеет корней, отличных от β. В самом деле, допустим, что β_k, $k \in \{2, \ldots, n\}$, есть их общий корень. Тогда $h(\beta_k) = f(\gamma - c\beta_k) = 0$. Следовательно, найдется такой индекс $i \in \{1, \ldots, m\}$, что $\gamma = \alpha_i + c\beta_k$ $(k > 1)$, а это противоречит (2). На основании этого заключаем, что $x - \beta$ есть наибольший общий делитель g и h в $\mathscr{C}[x]$. Поскольку $x - \beta$ — нормированный полином, то отсюда следует, что $x - \beta$ является наибольшим общим делителем g и h в кольце $\mathscr{F}_1[x]$. Поэтому

$$(x - \beta) \in F_1[x] \text{ и } \beta \in F_1 = P(\gamma).$$

Кроме того, $\alpha = \gamma - c\beta \in F_1$. Таким образом,

$$F = P(\alpha,\ \beta) \subset F_1,\ F_1 \subset F.$$

Следовательно, $F = P(\gamma)$. Далее, так как γ (как и всякий элемент из F) есть алгебраический элемент над $\mathscr{P}$ и $\mathscr{F} = \mathscr{P}(\gamma)$, то поле $\mathscr{F} = \mathscr{P}(\gamma)$ является искомым простым алгебраическим расширением поля $\mathscr{P}$. □

Поле алгебраических чисел. В классе подполей поля комплексных чисел одним из наиболее важных является поле алгебраических чисел.

ОПРЕДЕЛЕНИЕ. *Алгебраическим числом* называется комплексное число, являющееся корнем полинома положительной степени с рациональными коэффициентами.

Отметим, что алгебраическое число есть любое комплексное число, алгебраическое над полем $\mathcal{Q}$. В частности, любое рациональное число является алгебраическим.

ТЕОРЕМА 3.8. *Множество A всех алгебраических чисел замкнуто в кольце $\mathcal{C}=\langle \mathbf{C}, +, -, \cdot, 1\rangle$ комплексных чисел. Алгебра $\mathcal{A}=\langle A, +, -, \cdot, 1\rangle$* является полем, подполем поля $\mathcal{C}$.

Доказательство. Пусть a и b — любые элементы из A. По следствию 3.6, поле $\mathcal{Q}(a, b)$ является алгебраическим над $\mathcal{Q}$. Поэтому числа $a+b$, $-a$, ab, 1 являются алгебраическими, т. е. принадлежат множеству A. Таким образом, множество A замкнуто относительно главных операций кольца $\mathcal{C}$. Поэтому алгебра $\mathcal{A}$ — подкольцо кольца $\mathcal{C}$ — является кольцом.

Кроме того, если a — ненулевой элемент из A, то $a^{-1} \in \mathbf{Q}(a, b)$ и поэтому a^{-1} принадлежит A. Следовательно, алгебра $\mathcal{A}$ есть поле, подполе поля $\mathcal{C}$. □

ОПРЕДЕЛЕНИЕ. *Поле $\mathcal{A}=\langle A, +, -, \cdot, 1\rangle$ называется полем алгебраических чисел.*

Алгебраическая замкнутость поля алгебраических чисел.

ТЕОРЕМА 3.9. *Поле алгебраических чисел алгебраически замкнуто.*

Доказательство. Пусть $\mathcal{A}[x]$ — кольцо полиномов от x над полем $\mathcal{A}$ алгебраических чисел. Пусть

$$f=a_0+a_1x+\ldots+a_nx^n \quad (a_0, \ldots, a_n \in A)$$

— любой полином положительной степени из $A[x]$. Нам надо доказать, что f имеет корень в A. Так как $f \in \mathbf{C}[x]$ и поле $\mathcal{C}$ алгебраически замкнуто, то f имеет корень в $\mathcal{C}$, т. е. существует такое комплексное число c, что $f(c)=0$. Пусть $\mathcal{L}=\mathcal{Q}(a_0, \ldots, a_n)$ и $\mathcal{L}(c)$ — простое алгебраическое расширение поля $\mathcal{L}$ с помощью c. Тогда $\mathcal{Q} \prec \mathcal{L} \prec \mathcal{L}(c)$, $\mathcal{L}(c)$ есть конечное алгебраическое расширение поля $\mathcal{L}$. По теореме 3.2, $\mathcal{L}$ есть конечное расширение поля $\mathcal{Q}$. В силу теоремы 3.3 $\mathcal{L}(c)$ является конечным расширением поля $\mathcal{Q}$. Отсюда, по теореме 3.2, следует, что поле $\mathcal{L}(c)$ является алгебраическим расширением поля $\mathcal{Q}$ и, значит, $c \in A$. Таким образом, любой полином из $A[x]$ положительной степени имеет в A корень, т. е. поле $\mathcal{A}$ алгебраически замкнуто. □

Упражнения

1. Найдите степень поля $\mathcal{F}$ над полем $\mathcal{P}$, если:

(a) $\mathcal{F}=\mathcal{Q}(\sqrt{2}, \sqrt{3})$, $\mathcal{P}=\mathcal{Q}$; (b) $\mathcal{F}=\mathcal{Q}(\sqrt{2}, \sqrt[3]{5})$, $\mathcal{P}=\mathcal{Q}(\sqrt{2})$; (c) $\mathcal{F}=\mathcal{R}$, $\mathcal{P}=\mathcal{R}$.

2. Найдите базис и степень поля $\mathcal{F}$ над полем $\mathcal{P}$, если:

(a) $\mathcal{F}=\mathcal{Q}(i, \sqrt[3]{2})$, $\mathcal{P}=\mathcal{Q}$; (b) $\mathcal{F}=\mathcal{R}(-i)$, $\mathcal{P}=\mathcal{R}$; (c) $\mathcal{F}=\mathcal{C}$, $\mathcal{P}=\mathcal{C}$.

3. Пусть f и g — полиномы над полем рациональных чисел, имеющие общий действительный корень. Докажите, что f и g имеют общий делитель положительной степени с рациональными коэффициентами.

4. Докажите, что неприводимый над числовым полем полином не имеет кратных корней в поле комплексных чисел.

5. Докажите, что комплексное число есть алгебраическое число тогда и только тогда, когда оно является корнем полинома положительной степени с целыми коэффициентами.

§ 4. УСЛОВИЯ РАЗРЕШИМОСТИ УРАВНЕНИЯ ТРЕТЬЕЙ СТЕПЕНИ В КВАДРАТНЫХ РАДИКАЛАХ

Понятие разрешимости уравнения в квадратных радикалах.

ОПРЕДЕЛЕНИЕ. Поле $\mathcal{F}$ называется *квадратичным расширением поля* $\mathcal{P}$, если существует такой элемент α, что $F=P(\alpha)$, $\alpha \notin P$, $\alpha^2 \in P$.

Примеры. 1. Поле $\mathcal{Q}(2^{1/2})$ есть квадратичное расширение поля $\mathcal{Q}$.

2. Поле $\mathcal{R}(i)$ является квадратичным расширением поля $\mathcal{R}$.

3. Поле $\mathcal{Q}(2^{1/3})$ не является квадратичным расширением поля $\mathcal{Q}$.

Говорят, что уравнение

$$(1)\quad x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n=0 \quad (a_i \in \mathbf{Q})$$

разрешимо в квадратных радикалах, если его корни можно выразить рационально (т. е. с помощью операций сложения, вычитания, умножения и деления) через корни цепочки двучленных квадратных уравнений:

$$x^2-\alpha_0=0, \quad \alpha_0 \in \mathbf{Q}=F_0;$$
$$x^2-\alpha_1=0, \quad \alpha_1 \in F_1=F_0(\sqrt{\alpha_0});$$
$$x^2-\alpha_2=0, \quad \alpha_2 \in F_2=F_1(\sqrt{\alpha_1});$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x^2-\alpha_{k-1}=0, \quad \alpha_{k-1} \in F_{k-1}=F_{k-2}(\sqrt{\alpha_{k-2}}).$$

Таким образом, все корни уравнения (1) рационально выражаются через числа $\sqrt{\alpha_0}$, $\sqrt{\alpha_1}$, $\dots$, $\sqrt{\alpha_{k-1}}$ и принадлежат полю $\mathcal{F}_k = \mathcal{F}_{k-1}\left(\sqrt{\alpha_{k-1}}\right)$.

Другими словами, уравнение (1) разрешимо в квадратных радикалах, если существует возрастающая цепочка числовых полей

$$\mathcal{Q} = \mathcal{F}_0 \subset \mathcal{F}_1 \subset \dots \subset \mathcal{F}_{k-1} \subset \mathcal{F}_k$$

такая, что каждое поле $\mathcal{F}_i$ цепочки является квадратичным расширением предыдущего поля $\mathcal{F}_{i-1}$ и поле $\mathcal{F}_k$ содержит все корни уравнения (1).

ОПРЕДЕЛЕНИЕ. Говорят, что *уравнение* (1) *разрешимо в радикалах*, если его корни можно выразить рационально через корни цепочки двучленных уравнений:

$$x^{n_0} - \alpha_0 = 0, \quad \alpha \in \mathbf{Q} = F_0;$$
$$x^{n_1} - \alpha_1 = 0, \quad \alpha_1 \in F_1 = F_0\left(\sqrt[n_0]{\alpha_0}\right);$$
$$x^{n_2} - \alpha_2 = 0, \quad \alpha_2 \in F_2 = F_1\left(\sqrt[n_1]{\alpha_1}\right);$$
$$\dots\dots\dots\dots\dots\dots\dots$$
$$x^{n_{k-1}} - \alpha_{k-1} = 0, \quad \alpha_{k-1} \in F_{k-1} = F_{k-2}\left(\sqrt[n_{k-2}]{\alpha_{k-2}}\right).$$

Таким образом, все корни уравнения (1) рационально выражаются через числа $\sqrt[n_0]{\alpha_0}$, $\dots$, $\sqrt[n_{k-1}]{\alpha_{k-1}}$ и принадлежат полю $\mathcal{F}_k = \mathcal{F}_{k-1}\left(\sqrt[n_{k-1}]{\alpha_{k-1}}\right)$.

Условия разрешимости уравнения третьей степени в квадратных радикалах.

ТЕОРЕМА 4.1. *Уравнение третьей степени*

(1) $x^3 + ax^2 + bx + c = 0$

с рациональными коэффициентами разрешимо в квадратных радикалах тогда и только тогда, когда оно имеет хотя бы один рациональный корень.

Доказательство. Если полином $f = x^3 + ax^2 + bx + c$ имеет хотя бы один рациональный корень, например d, то полином можно представить в виде

$$f = (x - d)(x^2 + ex + g),$$

где $e, g \in \mathbf{Q}$. Поэтому уравнение (1) разрешимо в квадратных радикалах.

Предположим, что уравнение (1) разрешимо в квадратных радикалах и не имеет рациональных корней. Тогда

существует такая цепочка квадратичных расширений

(2) $\mathbf{Q} = F_0 \subset F_1 \subset \ldots \subset F_{k-1} \subset F_k$,

что хотя бы один из корней x_1, x_2, x_3 уравнения (1) содержится в $F_k \setminus F_{k-1}$, например

(3) $x_1 \in F_k \setminus F_{k-1}$,

и ни один из корней x_1, x_2, x_3 уравнения (1) не содержится в F_{k-1},

(4) $\{x_1, x_2, x_3\} \cap F_{k-1} = \emptyset$.

Поле $\mathscr{F}_k$ есть квадратичное расширение поля F_{k-1}, т. е. существует элемент $\alpha \in F_k \setminus F_{k-1}$ такой, что

(5) $F_k = F_{k-1}(\alpha)$, $\alpha \notin F_{k-1}$, $\alpha^2 \in F_{k-1}$.

На основании (3) и (5) заключаем, что

(6) $x_1 = p + q\alpha$, где p, $q \in F_{k-1}$, $q \neq 0$.

Непосредственная проверка показывает, что $p - q\alpha$ также является корнем полинома f. В самом деле,

(7) $f(p+q\alpha) = (p+q\alpha)^3 + a(p+q\alpha)^2 + b(p+q\alpha) + c = A + B\alpha$,

где

(8) $\begin{aligned} A &= f(p) + 3pq^2\alpha^2 + aq^2\alpha^2, \\ B &= 3p^2q + q^3\alpha^2 + 2apq + bq. \end{aligned}$

Так как A, $B \in F_{k-1}$ и $\alpha \notin F_{k-1}$, то из

(9) $f(p+q\alpha) = A + B\alpha = 0$

следует, что

(10) $A = B = 0$.

На основании (7), (8), (9) и (10) заключаем, что

$f(p - q\alpha) = A - B\alpha = 0$.

Таким образом, $p - q\alpha$ есть также корень полинома f. Пусть $x_2 = p - q\alpha$. Тогда в силу (6) $x_1 - x_2 = 2q\alpha \neq 0$ и, значит, $x_1 \neq x_2$.

По формулам Виета, $x_1 + x_2 + x_3 = -a$. Кроме того, в силу (6) $x_1 + x_2 = 2p \in F_{k-1}$. Поэтому $x_3 = -a - 2p \in F_{k-1}$, что противоречит предположению (4). □

СЛЕДСТВИЕ 4.2. *Уравнение* (1) *с рациональными коэффициентами разрешимо в квадратных радикалах тогда и*

только тогда, когда полином x^3+ax^2+bx+c *неприводим в кольце* $\mathbb{Q}[x]$.

Примеры задач, неразрешимых в квадратных радикалах. В геометрии доказывается, что корни уравнения $x^3+ax^2+bx+c=0$ с рациональными коэффициентами могут быть построены циркулем и линейкой тогда и только тогда, когда это уравнение разрешимо в квадратных радикалах, т. е. когда решение этого уравнения сводится к решению цепочки квадратных уравнений.

Задача об удвоении куба. *Построить ребро куба, объем которого вдвое больше объема данного куба.*

Нам дан только отрезок — ребро данного куба; примем этот отрезок за единичный. Тогда длина x ребра искомого куба удовлетворяет уравнению

(1) $x^3-2=0$.

Это уравнение неразрешимо в квадратных радикалах, так как не имеет рациональных корней. Следовательно, корни уравнения (1) *не могут быть построены циркулем и линейкой.*

Задача о трисекции угла. *Разделить данный угол на три равные части.*

Мы можем считать, что даны два луча, исходящие из точки O и образующие угол φ. Проведем дугу круга единичного радиуса. Построим точку A такую, что отрезок OA имеет длину $a=\cos\varphi$. Обратно: зная отрезок OA длины $\cos\varphi$, легко построить угол циркулем и линейкой. Поэтому мы можем считать, что искомым является угол $x=\cos\frac{\varphi}{3}$. Так как

$$\cos\varphi+i\sin\varphi=\left(\cos\frac{\varphi}{3}+i\sin\frac{\varphi}{3}\right)^3=$$
$$=\cos^3\frac{\varphi}{3}-3\cos\frac{\varphi}{3}\sin^2\frac{\varphi}{3}+i\left(3\cos^2\frac{\varphi}{3}\sin\frac{\varphi}{3}-\sin^3\frac{\varphi}{3}\right),$$

то

$$\cos\varphi=\cos^3\frac{\varphi}{3}-3\cos\frac{\varphi}{3}\sin^2\frac{\varphi}{3}=$$
$$=\cos^3\frac{\varphi}{3}-3\cos\frac{\varphi}{3}\left(1-\cos^2\frac{\varphi}{3}\right)$$

и

$$4\cos^3\frac{\varphi}{3}-3\cos\frac{\varphi}{3}-\cos\varphi=0.$$

Поскольку $x=\cos\frac{\varphi}{3}$, то

(1) $4x^3-3x-a=0$.

При $\varphi=\frac{\pi}{2}$ $a=0$ и поэтому уравнение (1) разрешимо в квадратных радикалах.

Если же $\varphi=\frac{\pi}{3}$, то $a=\cos\frac{\pi}{3}=\frac{1}{2}$ и мы получим уравнение

(2) $8x^3-6x-1=0$.

Полагая в нем $y=2x$, получим

(3) $y^3-3y-1=0$.

Уравнение (3) и, значит, (2) неразрешимо в квадратных радикалах, так как не имеет рациональных корней. Следовательно, корни этих уравнений невозможно построить циркулем и линейкой. Таким образом, угол $\pi/3$ *невозможно разделить на три равные части циркулем и линейкой.*

Задача о построении правильного семиугольника. *Построить правильный семиугольник, вписанный в единичный круг.*

Корни уравнения $z^7-1=0$ изображаются на плоскости вершинами правильного семиугольника, вписанного в единичный круг. Один из корней этого уравнения равен единице, а остальные удовлетворяют уравнению

(1) $z^6+z^5+z^4+z^3+z^2+z+1=0$.

Докажем, что уравнение (1) неразрешимо в квадратных радикалах. Разделив обе части уравнения (1) на z^3 и сгруппировав слагаемые, получим

$$\left(z+\frac{1}{z}\right)^3-3\left(z+\frac{1}{z}\right)+\left(z+\frac{1}{z}\right)^2+\left(z+\frac{1}{z}\right)-1=0.$$

Полагая

(2) $t=z+\frac{1}{z}$,

получим

(3) $t^3+t^2-2t-1=0$.

Уравнение (3) неразрешимо в квадратных радикалах, так как не имеет рациональных корней. Уравнение (1) неразрешимо в квадратных радикалах. В самом деле, если бы

уравнение (1) было разрешимо в квадратных радикалах, то в силу (2) уравнение (3) также было бы разрешимо в квадратных радикалах. Следовательно, корни уравнения (1) невозможно построить циркулем и линейкой. Отсюда следует, что *правильный семиугольник невозможно построить циркулем и линейкой.*

Для каких натуральных n ($n>2$) можно построить правильный n-угольник при помощи циркуля и линейки?

Вопрос этот был решен полностью Гауссом в 1796 г. Гаусс доказал, что построение возможно в том и только в том случае, когда n можно представить в виде

$$n=2^k p_1 p_2 \dots p_m,$$

где k — натуральное число, а $p_1, \dots, p_m$ — различные простые числа вида 2^m+1 ($m \in \mathbf{N} \setminus \{0\}$).

Упражнения

1. Покажите, что полином x^6+x^3+1 неприводим над полем рациональных чисел.
2. Покажите, что полином третьей степени над полем либо неприводим, либо имеет корень в этом поле. Является ли полином x^5-5x^2+1 неприводимым над полем рациональных чисел?
3. Покажите, что полином от двух переменных x^2+y^2-1 неприводим над полем рациональных чисел. Приводим ли он над полем комплексных чисел?
4. Докажите, что уравнение $x^5-1=0$ разрешимо в квадратных радикалах.
5. Докажите, что правильный пятиугольник можно построить циркулем и линейкой.
6. Докажите, что правильный девятиугольник невозможно построить циркулем и линейкой.

ЛИТЕРАТУРА

1. И. В. Арнольд. Теория чисел. М., 1939.
2. А. А. Бухштаб. Теория чисел. М., 1966.
3. И. М. Виноградов. Основы теории чисел. М., 1976.
4. Б. Л. Ван-дер-Варден. Алгебра. М., 1976.
5. Д. Гейл. Теория линейных экономических моделей. М., 1963.
6. Ж. Дьедонне. Линейная алгебра и элементарная геометрия. М., 1972.
7. И. М. Гельфанд. Лекции по линейной алгебре. М. 1966.
8. Л. А. Калужнин. Введение в общую алгебру. М., 1973.
9. М. И. Каргаполов, Ю. И. Мерзляков. Основы теории групп. М., 1972.
10. А. И. Кострикин. Введение в алгебру. М., 1977.
11. А. Г. Курош. Курс высшей алгебры. М., 1971.
12. А. Г. Курош. Лекции по общей алгебре. М., 1962.
13. И. А. Лавров, Л. Л. Максимова. Задачи по теории множеств, математической логике и теории алгоритмов. М., 1975.
14. А. И. Мальцев. Основы линейной алгебры. М., 1970.
15. А. И. Мальцев. Алгебраические системы. М., 1970.
16. А. А. Марков. Теория алгоритмов. — Труды Математического института АН СССР 42, 1954.
17. Э. Мендельсон. Введение в математическую логику. М., 1971.
18. П. С. Новиков. Элементы математической логики. М., 1973.
19. М. М. Постников. Теория Галуа. М., 1963.
20. И. В. Проскуряков. Сборник задач по линейной алгебре. М., 1967.
21. Е. Слупецкий, Л. Борковский. Элементы математической логики и теории множеств. М., 1965.
22. Р. Р. Столл. Множества, логика, аксиоматические теории. М., 1968.
23. Д. К. Фаддеев, И. С. Соминский. Сборник задач по высшей алгебре. М., 1977.
24. С. Феферман. Числовые системы. М., 1971.
25. Р. Фор, А. Кофман, М. Дени-Папен. Современная математика. М., 1966.
26. Г. Хассе. Лекции по теории чисел. М., 1953.
27. П. Халмош. Конечномерные векторные пространства. М., 1963.
28. М. Холл. Комбинаторика. М., 1970.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Абсолютное значение элемента 151
Абелева группа 94
Автоморфизм алгебры 84
— группы 99
— кольца 107
Аддитивная группа 95, 96, 135
— — векторного пространства 246
— — классов вычетов 356, 400
— — кольца 104
— — поля 146
Аддитивный моноид натуральных чисел 123
Аксиома математической индукции 119, 120
Алгебра 82
— кватернионов 299
— линейная 298
— линейных операторов 300
— матриц 299
Алгебраическая замкнутость поля 510
— независимость элементов 487
— система 112, 113
Алгебраический элемент 528
Алгебраическое расширение поля 531, 533
— число 537
Алгоритм Евклида 379
Алфавит 117
Арифметический корень n-й степени 154
Арифметическое векторное пространство 175
Ассоциативность 76, 347
Ассоциированные элементы 445, 446

Базис векторного пространства 256
— — — ортогональный 271
— — — ортонормированный 278
— системы векторов 182
Бинарная операция 75
Бинарное отношение 48, 49

Вектор нормированный 277
— собственный 307, 309
Векторное пространство 245, 246
— — арифметическое 175
— — действительное 276
— — евклидово 276
— — конечномерное 256
— — со скалярным умножением 270
Взаимно-простые числа 372, 375
Включения знак 40
Вполне упорядоченное множество 73

Выпуклый конус пространства 318
Высказывания 5—8

Геометрическое представление комплексных чисел 164
Главные операции алгебры 82
— элементы алгебры 83
Гомоморфизм 84
— алгебраической системы 114
— алгебры 84
— векторного пространства 283
— группы 99
— кольца 107
Граф 52
— бинарного отношения 53
График предиката 52
Группа 94
— абелева 94
— симметрическая 96, 350
— циклическая 102, 355

Двучленные сравнения 418
Делимость элементов 445
Делитель 445
— нуля 104, 105
— общий наибольший 372, 453, 454
— собственный 447
Дефект оператора 286
Диагональная матрица 227, 313, 314
Диаграммы Эйлера—Венна 45
Дизъюнкция 6
Дистрибутивность 76, 128, 129
Доказательство косвенное 19, 20
— от противного 19, 20
— по индукции 121
Дополнение множества 45
Дополнение ортогональное 273

Евклидово пространство 276
Единица группы 95
— кольца 104
Единичный идеал 430
Естественное отображение 70
Естественный гомоморфизм 92

Зависимость линейная 176
Закон двойного отрицания 12
— де Моргана 45
— исключенного третьего 10
— контрапозиции 12
— сокращения 98, 125
Замкнутое подмножество 80, 87
Знак включения 40
— подстановки 224
— принадлежности 39
— числа 224

Идеал 430
— главный 431, 448
— единичный 430
— нулевой 430
Изоморфизм алгебры 84
— — линейных операторов 301
— алгебраической системы 114
— векторного пространства 266, 283
— группы 99
— евклидова пространства 280
— кольца 364, 430
Изоморфные алгебры 84
— алгебраические системы 114
— векторные пространства 266
— группы 99
— евклидовы пространства 280
— кольца 107
Импликация 7
Индекс числа по модулю 417
Исключение переменных 502, 503
Истинностная таблица 6, 7, 13

Канонические задачи линейного программирования 328, 335

Каноническое разложение на простые множители 367, 474
Квантор общности 28
— существования 28, 29
Класс вычетов 397, 432
— смежный 352
— эквивалентности 68
Кольцо 104
— главных идеалов 448
— евклидово 451
— классов вычетов 401
— коммутативное 104
— нулевое 104
— полиномов 489
— факториальное 450, 478
— целых чисел 139—141
— числовое 163
Коммутативная группа 94
Коммутативность 76, 124, 129
Комплексные числа 161
Композиция отображений 50, 56—58
Конгруэнция 81
Конечное расширение поля 533
Конъюнкция 6
Координатная строка вектора 265
Корень из единицы 159
— полинома 467
— — кратный 483
— — простой 483
Кратность корня 483
Критерий неприводимости Эйзенштейна 527
— несовместности системы неравенств 323
— совместности системы линейных уравнений 191

Лексикографическое упорядочение 72, 493
Лемма Гаусса 476
— Даламбера 509
Линейная зависимость системы векторов 176, 247
— независимость системы векторов 176, 247
— оболочка 176, 251
Линейно упорядоченное множество 72
Линейное многообразие 253
— отображение векторного пространства 283
Линейный оператор обратимый 303, 304
— — пространства 283
— — с простым спектром 312
— порядок 72
Логика высказываний 8
Логическое следствие 14, 26

Математическая индукция 121
Матрица 210
— квадратная 210
— линейного оператора 289, 290
— обратимая 215, 240
— транспонированная 213
Многообразие линейное 253
Множество 39
— вполне упорядоченное 73
— замкнутое относительно операции 80
— линейно упорядоченное 72, 150
— упорядоченное 72
— частично упорядоченное 72
Модуль комплексного числа 163
Моноид 83, 346
— натуральных чисел (мультипликативный) 130
Мономорфизм алгебры 84

Наибольший общий делитель 327, 453, 454
Наименьшее общее кратное 376, 455
— подкольцо кольца 437

Натуральные числа 119, 120
Независимость линейная 247, 248
Неприводимый полином 472
— элемент кольца 447
Неравенство треугольника 277
— Чебышева 392
Нейтральный элемент 77
НОД 372, 453
НОК 376, 455
Норма вектора 277
Нормальный делитель группы 358
Нулевое кольцо 104
Нулевой идеал 430
— элемент 80
Нуль 120, 146

Область целостности 104
— значений 50, 55
— определения 50, 55
Образ линейного оператора 286
Обратимый элемент 81, 98
Обратимая матрица 215
Объединение множеств 41
Однотипные алгебры 83
Операция бинарная 75
— n-местная 75
— сложения 80
— умножения 81
— унарная 75
Определитель матрицы 227
Ортонормированная система векторов 278
Отношение 49, 52
— антирефлексивное 66
— антисимметричное 66
— бинарное 49
— делимости 143
— изоморфизма 86, 99
— конгруэнтности 81, 91
— линейного порядка 72
— n-местное 52
— порядка 71, 131, 148
— рефлексивное 65
Отношение симметричное 66
— строгого порядка 71
— транзитивное 66
— эквивалентности 65, 67, 68
Отображение 54, 55
— инъективное 59
— линейное 283
Отрицание высказывания 6

Пара упорядоченная 48
Первообразный корень 415, 416
Переменная свободная 22
— связанная 28, 29
— предметная 33
Пересечение множеств 42
Период систематической дроби 421
Подалгебра 87
Подгруппа 100, 350
Подкольцо 109
— наименьшее 437
Подмножество 40
— замкнутое в алгебре 87, 89
Подобные матрицы 297, 313
Подполе 146
— простое 146
Подпространство векторного пространства 250
Подстановка 221
— нечетная 223
— обратная 222
— четная 223
Подсистема алгебраической системы 115
Поле 146
— алгебраически замкнутое 510, 537
— алгебраических чисел 537
— действительных чисел 153
— классов вычетов 404
— комплексных чисел 157, 161
— простое 146
— рациональных чисел 148
— скаляров 245

Поле упорядоченное 150
— частных 148, 439
— числовое 162
Полином минимальный 529
— неприводимый 472
— нормированный 466
— от нескольких переменных 486
— приводимый 472
— примитивный 475
— симметрический 459, 498
Полная линейная группа 305
— система вычетов 399
Полугруппа 346
Порядок 71, 72
— группы 94
— классов вычетов 413
— нестрогий 71
— строгий 71
— числа по модулю 413
— элемента группы 354
Правила введения и удаления 18
Правило Крамера 241
— отделения 19
Предикат 23, 25, 26, 27
Предикатные формулы 34
Предметные переменные 33
Приведенная система вычетов 402, 403
Принадлежности знак 39
Принцип математической индукции 121
Произведение матриц 211
Производная полинома формальная 480
Простое алгебраическое расширение поля 528, 531
— поле 146
— расширение поля 459
— трансцендентное расширение кольца 459, 461
— число 365
Простой корень полинома 483
Простой элемент области целостности 446
Противоположный элемент 80, 95
Противоречие 10
Процесс ортогонализации 272
Прямая сумма подпространств 252
Прямое произведение множеств 48, 49
Пустое множество 41

Равенство полиномов алгебраическое 468
— — функциональное 468
— множеств 39
Равносильные формулы 15
— предикаты 26
— системы уравнений 186
Разбиение множества 68
Разложение на простые множители 366, 450, 473, 478
— определителя 235
Размерность векторного пространства 260
Разность множеств 42
Ранг линейного оператора 294
— матрицы 189, 199, 200
— операции 75
— системы векторов 183
Распределение простых чисел 389
Расширение поля алгебраическое 533
— — конечное 533
— — простое 528
— — составное 533, 534
— — трансцендентное 459
Рациональные числа 148
Результант 502
Рефлексивное отношение 65
Решение системы линейных неравенств 335
— — — уравнений 185, 206—208, 220

Решение уравнений 515, 520
Решето Эратосфена 370

Свободная переменная 22
Свойства группы 97
— кольца 106
— поля 146
Связанная переменная 28, 29
Симметрическая группа 96, 350
Симметрический полином 495
Симплекс-метод 335
Система действительных чисел 150, 153
— алгебраическая 112
— векторов ортогональная 271
— линейных неравенств 317
— — уравнений 185
— — — однородная 192, 203
Скалярное произведение 270
Следствие систем линейных уравнений 180, 195, 196
— — — неравенств 318
Смежный класс 352, 433
— — левый 353
— — правый 352
Собственное значение 307, 309
Собственный вектор 307, 309
— делитель элемента 447
Сравнение по идеалу 432
— по модулю 397
Стандартные задачи линейного программирования 327, 328, 335
Старший коэффициент полинома 466
Степенные вычеты 419
Степень полинома 466, 492
— элемента 529
Строгий порядок 71
Ступенчатая матрица 198
— — приведенная 201
Сужение функции 63
Сумма подпространств 251, 252

Таблица истинности 6, 7
Тавтология 10
Теорема двойственности 330, 333
— Кронекера—Капелли 193
— Кэли 351
— Лагранжа 353
— Минковского 321
— о гомоморфизмах 362
— о делении с остатком 141, 142, 469
— Ферма 408
— Штурма 523
— Эйлера 408
Тернарное отношение 52
Тождественно истинная формула 10
— ложная формула 10
Транзитивное отношение 66
Трансцендентное расширение кольца 459, 488
Тригонометрическая форма комплексного числа 166, 168
Трисекция угла 541

Удвоение куба 541
Универсальное множество 44
Упорядочение лексикографическое 493
Упорядоченное множество 72
— поле 150
Уравнения третьей степени 515
— четвертой степени 520
Условие с одной свободной переменной 23
— с несколькими свободными переменными 23

Фактор-алгебра 91
Фактор-группа 359, 360
Фактор-кольцо 433, 434
Фактор-множество 68
Формула логики высказываний 8
Формулы Крамера 242

Фундаментальная система решений 204
Функция 54, 55
— инъективная 59
— обратная 60—62
— Эйлера 406

Характеристика кольца 436
Характеристическое уравнение 310, 311

Целые числа 135, 139
Циклическая группа 102, 355

Числа алгебраические 537
— действительные 153
— комплексные 161
— — сопряженные 163
— натуральные 119, 120
— простые 365
— рациональные 148
— целые 135, 139

Эквивалентности отношение 65, 67, 68
Эквивалентность 67
— логическая 15
Эквивалентные системы векторов 180
Эквиваленция 8
Элемент алгебраический 528
— множества 39
— нейтральный 77
— обратный по умножению 81
— противоположный по сложению 80
— симметрический 78, 79
Элементарные преобразования системы векторов 181
— симметрические полиномы 496
Эндоморфизм алгебры 84
Эпиморфизм 84

Ядро гомоморфизма 361
— линейного оператора 286

ОГЛАВЛЕНИЕ

Предисловие 3

Глава первая

Элементы логики

§ 1. Логика высказываний 5

Высказывания (5). Логические операции над высказываниями (5). Формулы логики высказываний (8). Законы логики (10). Упражнения (14).

§ 2. Логическое следствие 14

Основные определения (14). Схемы доказательств (18). Косвенное доказательство (19). Упражнения (21).

§ 3. Предикаты 22

Свободные переменные (22). Предикаты (22). Операции над предикатами (24). Логическое следствие. Равносильные предикаты (25). Упражнения (27).

§ 4. Кванторы 28

Квантор общности (28). Квантор существования (28). Запись высказываний на языке логики предикатов (31). Упражнения (32).

§ 5. Предикатные формулы. Законы логики 33

Элементарные формулы (33). Предикатные формулы (34). Законы логики предикатов (35). Упражнения (37).

Глава вторая

Множества и отношения

§ 1. Множества 39

Понятие множества (39). Подмножества (40). Пустое множество (41). Операции над множествами (41). Основные свойства операций над множествами (43). Универсальное множество. Дополнение множества (44). Диаграммы Эйлера — Венна (45). Упражнения (47).

§ 2. Бинарные отношения 48

Прямое произведение множества (48). Бинарные отношения (49). n-местные отношения (52). Представление бинарных отношений графами (52). Упражнения (53)

§ 3. Функции 54

Понятие функции (отображения) (54). Композиция функций (56). Инъективные функции (59). Обратимые функции (60). Ограничение функции (63). Упражнения (64).

§ 4. Отношение эквивалентности 65
Некоторые виды бинарных отношений (65). Отношение эквивалентности (67). Фактор-множество (68). Отношение равнообразности отображения (69). Упражнения (70).
§ 5. Отношения порядка 71
Отношения порядка (71). Линейный порядок (72). Упорядоченное множество (72). Упражнения (73).

Глава третья

Алгебры и алгебраические системы

§ 1. Бинарные операции 75
Бинарные и n-местные операции (75). Виды бинарных операций (76). Нейтральные элементы (77). Регулярные элементы (77). Симметричные элементы (78). Подмножества, замкнутые относительно операций (80). Аддитивная и мультипликативная формы записи (80). Конгруэнция (81). Упражнения (82).
§ 2. Алгебры 82
Понятие алгебры (82). Гомоморфизмы алгебры (84). Подалгебры (87). Фактор-алгебра (91). Упражнения (93).
§ 3. Группы 94
Понятие группы (94). Примеры групп (95). Простейшие свойства группы (97). Гомоморфизмы групп (98). Подгруппы (100). Упражнения (103).
§ 4. Кольца 104
Понятие кольца (104). Простейшие свойства кольца (106). Гомоморфизм колец (107). Подкольца (109). Упражнения (112).
§ 5. Алгебраические системы 112
Понятие алгебраической системы (112). Изоморфизмы алгебраических систем (114). Подсистемы (114). Упражнения (116).

Глава четвертая

Основные числовые системы

§ 1. Система натуральных чисел 117
Алфавит и слова (117). Слова в однобуквенном алфавите (118). Система натуральных чисел (119). Принцип математической индукции (121). Упражнения (122).
§ 2. Свойства сложения и умножения натуральных чисел 122
Свойства сложения (122). Свойства умножения (128). Упражнения (131).
§ 3. Отношение порядка на множестве натуральных чисел . . . 131
Отношение порядка (131). Полная упорядоченность множества натуральных чисел (133). Упражнения (134).
§ 4. Кольцо целых чисел 135
Аддитивная группа целых чисел (135). Естественное умножение в аддитивной группе целых чисел (138). Кольцо целых чисел (139). Теорема о делении с остатком (141). Отношение делимости в кольце целых чисел (143). Упражнения (144).
§ 5. Поля. Поле рациональных чисел 146
Понятие поля (146). Простейшие свойства поля (146). Поле рациональных чисел (148). Упражнения (149)
§ 6. Система действительных чисел 150
Упорядоченные поля (150). Система действительных чисел (152). Построение системы действительных чисел (154). Упражнения (156).

§ 7. Поле комплексных чисел 157
Комплексное расширение поля (157). Поле комплексных чисел (161). Сопряженные комплексные числа (163). Модуль комплексного числа (163). Геометрическое представление комплексных чисел (164). Упражнения (165).
§ 8. Тригонометрическая форма комплексного числа. Извлечение корней из комплексных чисел 166
Тригонометрическая форма комплексного числа (166). Корни n-й степени из единицы (169). Корни n-й степени из произвольного комплексного числа (171). Упражнения (172).

Глава пятая

Арифметические векторные пространства и системы линейных упражнений

§ 1. Арифметические векторные пространства 174
Арифметическое n-мерное векторное пространство (174). Линейная зависимость и независимость системы векторов (176). Эквивалентные системы векторов (180). Базис конечной системы векторов (182). Ранг конечной системы векторов (183). Упражнения (184).
§ 2. Системы линейных уравнений 185
Следствия системы линейных уравнений (185). Равносильные системы линейных уравнений и элементарные преобразования системы (186). Равенство строчечного и столбцового рангов матрицы (188). Критерий совместности системы линейных уравнений (191). Связь между решениями неоднородной линейной системы и решениями ассоциированной с ней однородной системы (193). Теоремы о следствиях системы линейных уравнений (195). Упражнения (197).
§ 3. Ступенчатые матрицы и системы линейных уравнений . . . 198
Ступенчатые матрицы (198). Приведенные ступенчатые матрицы (201). Однородные системы линейных уравнений (203). Фундаментальная система решений (204). Решение системы линейных уравнений методом последовательного исключения переменных (206). Упражнения (209).

Глава шестая

Матрицы и определители

§ 1. Операции над матрицами и их свойства 210
Операции над матрицами (210). Транспонирование произведения матриц (213). Упражнения (214).
§ 2. Обратимые матрицы 215
Обратимые матрицы (215). Элементарные матрицы (216). Условия обратимости матрицы (218). Вычисление обратной матрицы (219). Запись и решение системы n линейных уравнений с n переменными в матричной форме (220). Упражнения (221).
§ 3. Подстановки 221
Подстановки. Группа подстановок (221). Четные и нечетные подстановки (223). Знак подстановки (224). Упражнения (225).
§ 4. Определители 226
Определитель квадратной матрицы (226). Основные свойства определителей (227). Упражнения (231).
§ 5. Миноры и алгебраические дополнения, Теоремы об определителях 232
Миноры и алгебраические дополнения (232). Разложение определителя по строке или столбцу (235). Определитель произведения матриц (237). Необходимые и достаточные условия равенства нулю определителя (238). Упражнения (239).

§ 6. Теоремы о матрицах. Правило Крамера 239
Теорема о ранге матрицы (239). Обратная матрица (240). Правило Крамера (241). Условия, при которых система n линейных однородных уравнений с n переменными имеет ненулевые решения (242). Упражнения (243.)

Глава седьмая

Векторные пространства

§ 1. Векторные пространства 245
Понятие векторного пространства (245). Простейшие свойства векторных пространств (247). Линейная зависимость и независимость системы векторов (247). Упражнения (248).

§ 2. Подпространства векторного пространства 250
Подпространство (250). Линейная оболочка множества векторов (250). Сумма подпространств (251). Линейные многообразия (253). Упражнения (255).

§ 3. Базис и размерность векторного пространства 256
Базис векторного пространства (256). Дополнение независимой системы векторов до базиса (258). Размерность векторного пространства (260). Упражнения (263).

§ 4. Изоморфизмы векторных пространств 265
Координатная строка вектора относительно данного базиса (265). Изоморфизм векторных пространств (266). Упражнения (269).

§ 5. Векторные пространства со скалярным умножением 270
Скалярное умножение в векторном пространстве (270). Ортогональная система векторов (271). Процесс ортогонализации (272). Ортогональное дополнение к подпространству (273). Упражнения (275).

§ 6. Евклидовы векторные пространства 276
Евклидово векторное пространство (276). Норма вектора (277). Ортонормированный базис евклидова пространства (278). Изоморфизмы евклидовых пространств (280). Упражнения (282).

Глава восьмая

Линейные операторы

§ 1. Линейные отображения 283
Линейные отображения и операторы (283). Ядро и образ линейного оператора (286). Операции над линейными отображениями (287). Упражнения (288).

§ 2. Представление линейных операторов матрицами 289
Матрица линейного оператора (289). Связь между координатными столбцами векторов x и $\varphi(x)$ (291). Ранг линейного оператора (294). Связь между координатными столбцами вектора относительно различных базисов (295). Связь между матрицами линейного оператора относительно различных базисов (296). Упражнения (297).

§ 3. Линейные алгебры 298
Линейная алгебра (298). Алгебра линейных операторов векторного пространства (300). Изоморфизм алгебры линейных операторов и полной матричной алгебры (301). Упражнения (302).

§ 4. Обратимые операторы 303
Обратимые операторы (303). Полная линейная группа (305). Упражнения (306).

§ 5. Собственные векторы и собственные значения. Характеристические уравнения 307
Собственные векторы и собственные значения (307). Нахождение собственных векторов линейного оператора (308). Характеристическое уравнение (309). Линейные операторы с простым спектром (311). Условия, при которых матрица подобна диагональной матрице (313). Упражнения (315).

Глава девятая

Системы линейных неравенств

§ 1. Системы линейных неравенств 317
Основные понятия (317). Однородные системы линейных неравенств и выпуклые конусы (318). Следствия однородной системы линейных неравенств (319). Теорема Минковского (321). Критерий несовместимости системы линейных неравенств (323). Неотрицательные решения системы линейных уравнений и системы линейных неравенств (325). Упражнения (326).
§ 2. Стандартные и канонические задачи линейного программирования. Теоремы двойственности 327
Стандартные и канонические задачи (327). Допустимые и оптимальные векторы (328). Теоремы двойственности для стандартных задач (330). Теорема двойственности для канонических задач (333). Теорема равновесия (334). Упражнения (335).
§ 3. Симплекс-метод 335
Симплекс-метод (335). Упражнения (344).

Глава десятая

Группы

§ 1. Полугруппы и моноиды 346
Полугруппы (346). Моноиды (346). Обобщенный закон ассоциативности (347). Упражнения (349).
§ 2. Подгруппы и смежные классы 350
Подгруппы (350). Смежные классы (351). Теорема Лагранжа (353). Упражнения (353)
§ 3. Циклические группы 354
Порядок элемента группы (354). Циклические группы (355). Подгруппы циклической группы (357). Упражнения (358).
§ 4. Нормальные делители и фактор-группы 358
Нормальные делители группы (358). Фактор-группа (359). Ядро гомоморфизма (361). Теорема о гомоморфизмах (362). Упражнения (362).

Глава одиннадцатая

Теория делимости в кольце целых чисел

§ 1. Разложение целых чисел на простые множители 364
Идеалы кольца целых чисел (364). Простые числа (365). Разложение целых чисел на простые множители (365). Делители целого числа (367). Число и сумма натуральных делителей числа (368). Бесконечность множества простых чисел (369). Решето Эратосфена (370). Упражнения (371).
§ 2. Наибольший общий делитель и наименьшее общее кратное 372
Наибольший общий делитель (372). Взаимно простые числа (375). Наименьшее общее кратное (376). Упражнения (379).

§ 3. Алгоритм Евклида и конечные цепные дроби 379
Алгоритм Евклида (379). Конечные цепные дроби (380). Подходящие дроби (382). Упражнения (385).
§ 4. Целые систематические числа 385
Целые систематические числа (385). Арифметические операции над целыми систематическими числами (387). Перевод чисел из одной системы счисления в другую (388). Упражнения (389).
§ 5. Распределение простых чисел 389
Распределение простых чисел (389). Функции $T(x)$ и $A(x)$ (390). Неравенства для функции $T(x)$ (391). Неравенства Чебышева (392). Простые числа в арифметических прогрессиях (394). Упражнения (396).

Глава двенадцатая

Теория сравнений с арифметическими положениями

§ 1. Сравнения и их свойства 397
Сравнения в кольце целых чисел (397). Простейшие свойства сравнений (398). Упражнения (399).
§ 2. Полная система вычетов 399
Полная система вычетов (399). Аддитивная группа классов вычетов (400). Кольцо классов вычетов (401). Упражнения (402).
§ 3. Приведенная система вычетов 402
Приведенная система вычетов (402). Мультипликативная группа классов вычетов, взаимно простых с модулем (404). Функция Эйлера (406). Теоремы Эйлера и Ферма (408). Упражнения (408).
§ 4. Сравнения первой степени. Сравнения высших степеней по простому модулю 409
Степень и число решений сравнения (409). Сравнения первой степени (409). Сравнения высших степеней по простому модулю (411). Упражнения (413).
§ 5. Первообразные корни и индексы 413
Порядок числа и класса вычетов по модулю (413). Первообразные корни по простому модулю (415). Индексы по простому модулю (416). Двучленные сравнения (418). Упражнения (420).
§ 6. Обращение обыкновенной дроби в систематическую и определение длины периода систематической дроби 421
Упражнения (428).

Глава тринадцатая

Кольца

§ 1. Идеалы кольца. Фактор-кольцо 430
Идеалы кольца (430). Сравнения и классы вычетов по идеалу (432). Фактор-кольцо (433). Теорема об эпиморфизмах колец (434). Характеристика кольца (436). Наименьшее подкольцо кольца (437). Упражнения (438).
§ 2. Поле частных области целостности 439
Поле частных области целостности (439). Изоморфизм полей частных (443). Упражнения (445).
§ 3. Кольца главных идеалов 445
Простейшие свойства делимости в коммутативном кольце (445). Простые и составные элементы области целостности (446). Кольца главных идеалов (448). Факториальность кольца главных идеалов (449). Евклидовы кольца (451). Упражнения (452).

§ 4. Наибольший общий делитель. Наименьшее общее кратное 453
Наибольший общий делитель (453). Наименьшее общее кратное (455). Упражнения (458).

Глава четырнадцатая

Полиномы от одной переменной

§ 1. Кольцо полиномов 459
Простое трансцендентное расширение кольца (459). Теорема о существовании простого трансцендентного расширения коммутативного кольца (461). Степень полинома (465). Деление полинома на двучлен и корни полинома (466). Теорема о наибольшем возможном числе корней полинома в области целостности (467). Алгебраическое и функциональное равенства полиномов (468). Упражнения (469).

§ 2. Полиномы над полем 469
Теорема о делении с остатком (469). Алгоритм Евклида (470). Неприводимые над данным полем полиномы (471). Разложение полинома в произведение нормированных неприводимых множителей (473). Упражнения (474).

§ 3. Факториальность кольца полиномов над факториальным кольцом 475
Примитивные полиномы (475). Факториальность кольца полиномов (478). Упражнения (479).

§ 4. Формальная производная полинома. Неприводимые кратные множители 479
Формальная производная полинома (479). Разложение полинома по степеням разности $x-c$ (481). Неприводимые кратные множители полинома (482). Кратные корни полинома (483). Упражнения (484).

Глава пятнадцатая

Полиномы от нескольких переменных

§ 1. Кольцо полиномов от нескольких переменных 485
Кратное расширение кольца (485). Кольцо полиномов от нескольких переменных (486). Изоморфизм колец полиномов (489). Нормальное представление полинома и степень полинома (490). Факториальность кольца полиномов (492). Упражнения (493).

§ 2. Симметрические полиномы 493
Лексикографическое упорядочение членов полинома (493). Лемма о высшем члене произведения двух полиномов (494). Симметрические полиномы (495). Леммы о симметрических полиномах (496). Основная теорема о симметрических полиномах (498). Упражнения (500).

§ 3. Результант полиномов и исключение переменных 500
Результант двух полиномов (500). Исключение переменных (502). Упражнения (504).

Глава шестнадцатая

Полиномы над полем комплексных чисел и над полем действительных чисел

§ 1. Алгебраическая замкнутость поля комплексных чисел . . . 505
Теорема о возрастании модуля полинома (505). Непрерывность модуля полинома (506). Наименьшее значение модуля полинома (507). Лемма Даламбера (509). Алгебраическая замкнутость поля комплексных чисел (510). Формулы Виета (512). Упражнения (512).

§ 2. Полиномы над полем действительных чисел 513
Сопряженность мнимых корней полинома с действительными коэффициентами (513). Неприводимые над полем действительных чисел полиномы (513). Упражнения (514).
§ 3. Уравнения третьей и четвертой степени 515
Уравнения третьей степени (515). Исследование корней уравнения третьей степени с действительными коэффициентами (518). Уравнения четвертой степени (520). Упражнения (521).
§ 4. Отделение действительных корней полинома 521
Система полиномов Штурма (521). Теорема Штурма (522). Упражнения (525).

Глава семнадцатая

Полиномы над полем рациональных чисел и алгебраические числа

§ 1. Целые и рациональные корни полинома. Критерий неприводимости 526
Целые и рациональные корни полинома (526). Критерий неприводимости Эйзенштейна (526). Упражнения (528).
§ 2. Простое алгебраическое расширение поля 528
Простое расширение поля (528). Минимальный полином алгебраического элемента (529). Строение простого алгебраического расширения поля (531). Освобождение от алгебраической иррациональности в знаменателе дроби (532). Упражнения (532).
§ 3. Составное алгебраическое расширение поля 532
Конечное расширение поля (532). Составное алгебраическое расширение поля (533). Простота составного алгебраического расширения поля (535). Поле алгебраических чисел (536). Алгебраическая замкнутость поля алгебраических чисел (537). Упражнения (538).
§ 4. Условия разрешимости уравнения третьей степени в квадратных радикалах 538
Понятие разрешимости уравнения в квадратных радикалах (538). Условия разрешимости уравнения третьей степени в квадратных радикалах (539). Примеры задач, неразрешимых в квадратных радикалах (541). Упражнения (543).
Литература 544
Предметный указатель 545

ЛЕОНИД ЯКОВЛЕВИЧ КУЛИКОВ

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Редактор А. И. Селиверстова. Художник Ю. Д. Федичкин. Художественный редактор В. И. Пономаренко. Технический редактор Н. В. Яшукова. Корректор Г. И. Кострикова.

ИБ № 1647

Изд. № ФМ-607. Сдано в набор 25.01.79. Подп. в печать 19.06.79. Формат 84×108$^{1}/_{32}$. Бум. тип. № 2. Гарнитура литературная. Печать высокая. Объем 29,40 усл. печ. л. 26,99 уч.-изд. л. Тираж 40 000 экз. Зак. 452. Цена 1 руб. 10 коп.

Издательство «Высшая школа»,
Москва, К-51, Неглинная ул., д. 29/14

Ордена Октябрьской Революции, ордена Трудового Красного Знамени Ленинградское производственно-техническое объединение «Печатный Двор» имени А. М. Горького «Союзполиграфпрома» при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. 197136, Ленинград, П-136, Гатчинская, 26.

1р. 10к.