МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ГРАЖДАНСКОЙ АВИАЦИИ

И. С. Красильщик, Г. Н. Радковский,
А. В. Самохин

МАТЕМАТИКА
Часть I

Алгебра
и
аналитическая геометрия

*Учебное пособие для студентов I курса
специальности 090106
дневного обучения*

Москва – 2006

МИНИСТЕРСТВО ТРАНСПОРТА РФ
ГОСУДАРСТВЕННАЯ СЛУЖБА
ГРАЖДАНСКОЙ АВИАЦИИ
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ГРАЖДАНСКОЙ АВИАЦИИ

Кафедра высшей математики

И. С. Красильщик, Г. Н. Радковский,
А. В. Самохин

МАТЕМАТИКА
Часть I

Алгебра
и
аналитическая геометрия

*Учебное пособие для студентов I курса
специальности 090106
дневного обучения*

Москва – 2006

Аннотация

Учебное пособие содержит изложение теории множеств, линейной алгебры и аналитической геометрии, а также основ теории важнейших алгебраических структур. Материал составлен в соответствии с требованиями, учитывающими особенности подготовки студентов МГТУ ГА по специальности 090106 и рекомендуется для использования в курсе «Математика» в 1-м семестре. Работа издаётся в соответствии с учебным планом для студентов I курса и может быть также использована при обучении студентов I курса специальности 230101.

Рассмотрено и одобрено на заседаниях кафедры 25.12.2005 и методического совета факультета 15.01.2006.

Оглавление

Введение

Учебное пособие состоит из четырёх глав, вариантов контрольных домашних заданий, приложения,списка литературы и предметного указателя. Каждая глава разбита на параграфы, содержащие изложения необходимого теоретического материала и многочисленные примеры. В конце глав разбираются решения типовых задач и приводятся списки вопросов для самопроверки усвоения материала.

В первой главе на элементарном уровне излагаются основы наивной теории множеств и описывается множество вещественных чисел по Дедекинду. Вторая глава посвящена теории линейных пространств и операторов и решению систем линейных уравнений с произвольным числом неизвестных. Третья глава посвящена аналитической геометрии плоских кривых второго порядка. В четвёртой главе обсуждаются элементы коммутативных колец и полей, включая кольца и поля вычетов, целых чисел, а также поле комплексных чисел и кольцо полиномов. Далее приводятся варианты контрольных домашних заданий.

Приложение содержит краткие биографические сведения о математиках, чьи имена упомянуты в пособии, а также греческий и готический алфавиты.

В конце пособия приведён перечень использованных источников и рекомендуемой учебной литературы и предметный указатель.

ГЛАВА I

Теория множеств

§1. Множества

Понятие *множества* относится к числу простейших и в то же время фундаментальных понятий математики. Это понятие является *неопределимым* — его нельзя свести к каким-то более простым математическим объектам, но можно пояснить с помощью наглядных примеров. Множества — это совокупности каких-то объектов произвольной природы, и эти объекты называются *элементами* того или иного множества. Тот факт, что какой-то объект e является элементом множества E, записывается в виде:

$$e \in E \text{ или } E \ni e$$

и выражается словами:

$$e \textit{ принадлежит } (\textit{множеству})\ E,$$

или

$$(\textit{множество})\ E \textit{ содержит } (\textit{элемент})\ e,$$

или

$$e \textit{ является элементом } (\textit{множества})\ E.$$

Если хотят сказать, что e *не* является элементом множества E, то пишут:

$$e \notin E, \text{ или } E \not\ni e$$

(иногда также используются обозначения $e \bar{\in} E$ и $E \bar{\ni} e$).

Простейший способ описания множества состоит в *перечислении* его элементов. Например, запись

$$S = \{\spadesuit, \clubsuit, \diamondsuit, \heartsuit\} \tag{1}$$

определяет множество карточных мастей, и тот факт, что символ пик $\spadesuit$ является мастью,мы можем записать в виде $\spadesuit \in S$, где S задано равенством (1).

Другой способ задания множеств — их словесное описание. Например, можно сказать: «Рассмотрим множество студентов, поступивших в МГТУ ГА в 2003 году», или: «Пусть X — множество всех камней, лежащих на обратной стороне Луны». Из этих двух примеров видно, что словесные описания не всегда позволяют точно понять, какое множество имеется в виду: если в первом случае можно перечислить все элементы (например, просмотрев списки поступивших студентов), то во втором случае это не так — что есть камень, что называть обратной стороной, да и как на эту сторону попасть?

Чтобы избежать подобных проблем, в математике обычно используют более *формальные* способы описания множеств. Например, запись

$$\mathbb{N}_2 = \{\, 2n \mid n \in \mathbb{N} \,\},$$

где $\mathbb{N}$ — множество натуральных чисел[1], определяет множество чётных чисел (конечно, если мы знаем, что такое натуральные числа). Ещё один пример: равенство

$$C = \{\, (x, y) \mid x^2 + y^2 = 1,\ x, y \in \mathbb{R} \,\}$$

определяет множество точек, лежащих на окружности единичного радиуса с центром в начале координат.

Среди всевозможных множеств, изучаемых в математике, есть одно особое. Оно называется *пустым* и не содержит ни одного элемента. Пустое множество можно описывать разными способами. Например, множество

$$\{\, x \in \mathbb{N} \mid n^2 + 1 = 0 \,\}$$

(то есть множество натуральных чисел, квадрат которых равен -1) является пустым. Пустое множество обозначается через $\varnothing$.

Пусть E и E' — множества. Множество E' называется *подмножеством* множества E, если любой элемент из E' является элементом множества E. В этом случае используются обозначения

$$E' \subset E \text{ или } E \supset E'.$$

Из определения следует что любое множество является своим подмножеством, а также пустое множество является подмножеством любого множества, то есть

$$E \subset E, \qquad \varnothing \subset E.$$

Говорят также, что E *содержит* E' в качестве подмножества, или E' *содержится* в E. Имеет место простой и очень важный факт.

Предложение 1. *Если $E \subset E'$ и $E' \subset E$, то $E = E'$.*

Замечание. Если множество E' является подмножеством множества E, причём $E' \neq E$ и $E' \neq \varnothing$, то его называют *собственным подмножеством.* Иногда (особенно в старой литературе) символы «$\subset$» и «$\supset$» используют для обозначения собственных подмножеств, а когда хотят подчеркнуть, что подмножество может совпадать со всем множеством, пользуются обозначениями «$\subseteq$» и «$\supseteq$».

[1] Что такое натуральные и другие числа нам ещё предстоит выяснить — см. §3 и §4. Пока же будем исходить из наивного, школьного представления о них.

Рассмотрим теперь основные понятия, связанные с множествами.

Множество подмножеств. Пусть E — некоторое множество. Тогда можно рассмотреть множество, элементами которого являются всевозможные подмножества множества E. Оно обозначается через 2^E. Например, для множества S, заданного равенством (1), множество 2^S состоит из[2]

$$
\begin{aligned}
&S_0^0 = \varnothing,\\
&S_1^1 = \{\spadesuit\},\ S_1^2 = \{\clubsuit\},\ S_1^3 = \{\diamondsuit\},\ S_1^4 = \{\heartsuit\},\\
&S_2^1 = \{\spadesuit, \clubsuit\},\ S_2^2 = \{\spadesuit, \diamondsuit\},\ S_2^3 = \{\spadesuit, \heartsuit\},\ S_2^4 = \{\clubsuit, \diamondsuit\},\ S_2^5 = \{\clubsuit, \heartsuit\},\\
&\quad S_2^6 = \{\diamondsuit, \heartsuit\},\\
&S_3^1 = \{\spadesuit, \clubsuit, \diamondsuit\},\ S_3^2 = \{\spadesuit, \clubsuit, \heartsuit\},\ S_3^3 = \{\spadesuit, \diamondsuit, \heartsuit\},\ S_3^4 = \{\clubsuit, \diamondsuit, \heartsuit\},\\
&S_4^1 = \{\spadesuit, \clubsuit, \diamondsuit, \heartsuit\}.
\end{aligned}
$$

Вообще, если множество E содержит n элементов, то множество 2^E содержит 2^n элементов.

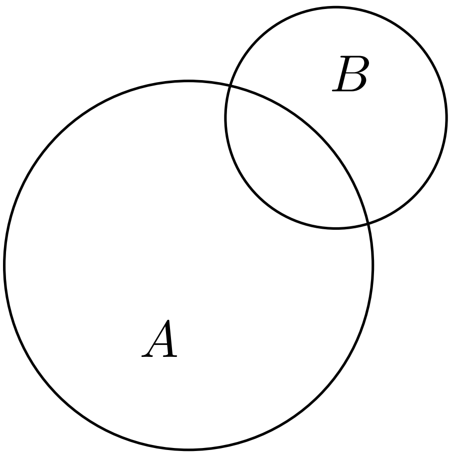

Рис. 1: Диаграмма Венна для двух множеств A и B

Прежде чем переходить к обсуждению теоретико-множественных операций, введём простой и наглядный графический способ их представления, называемый *диаграммами Венна*. При этом способе множества изображаются в виде фигур на плоскости (как, например, на рис. 1), а нужные их части отмечаются штриховкой, цветом и т.п. Ниже мы будем пользоваться диаграммами Венна для иллюстрации операций над множествами.

Операции над множествами. Основные операции, применяемые к множествам, это — объединение, пересечение, разность и симметрическая разность, а также дополнение.

Объединение: Пусть A и B — множества. Их *объединением* называется множество, содержащее все элементы, принадлежащие либо множеству A, либо B, либо им обоим. Объединение обозначается через $A \cup B$. Если есть произвольный набор множеств A_α, где буква α — элемент некоторого множества *индексов* I, то аналогичным образом можно

[2]Обратите внимание на то, что *порядок* перечисления элементов не имеет значения!

определить объединение $\cup_{\alpha\in I}A_\alpha$. Например, если S_i^j — введённые выше множества мастей, то

$$S_1^1\cup S_1^2=S_2^1,\ S_2^1\cup S_2^2=S_3^1,\ S_3^1\cup S_3^2=S_4^1$$

и т.д. Если $(0,2)$ интервал чисел от 0 до 2, а $(1,3)$ — интервал от 1 до 3, то

$$(0,2)\cup(1,3)=(0,3).$$

Диаграмма Венна объединения множеств A и B представлена на рис. 2.

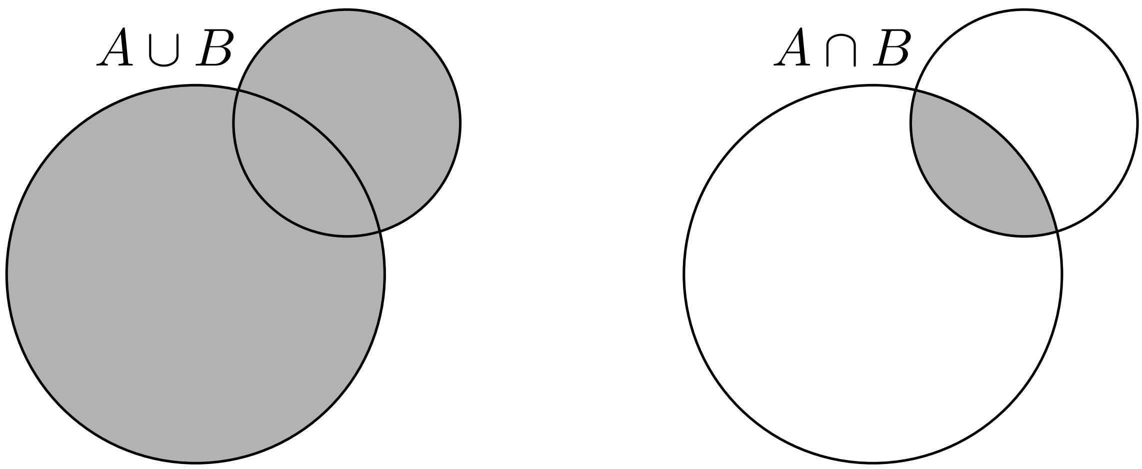

Рис. 2: Объединение (слева) и пересечение (справа) множеств

Пересечение: *Пересечением* множеств A и B называется множество, которое обозначается через $A\cap B$ и содержит элементы, одновременно принадлежащие и множеству A, и множеству B. Как и выше, можно определить и пересечение $\cap_{\alpha\in I}A_\alpha$ произвольного набора множеств A_α. Например,

$$S_3^1\cap S_3^2=S_1^2,\ S_2^1\cap S_2^3=S_1^1,\ S_2^1\cap S_2^6=\varnothing$$

и

$$(0,2)\cap(1,3)=(1,2).$$

Если пересечение двух множеств равно пустому множеству, то их называют *непересекающимися*. Диаграмма Венна пересечения множеств A и B представлена на рис. 2.

Разность: *Теоретико-множественная разность* между множеством A и множеством B состоит из тех элементов множества A, которые не принадлежат множеству B, и обозначается через $A\setminus B$. Например,

$$S_2^1\setminus S_2^2=S_1^2,\ S_2^2\setminus S_2^1=S_1^4,$$

а

$$(0,2)\setminus(1,3)=(0,1],\quad (1,3)\setminus(0,2)=[2,3).$$

Разность множеств иллюстрируется диаграммой Венна на рис. 3.

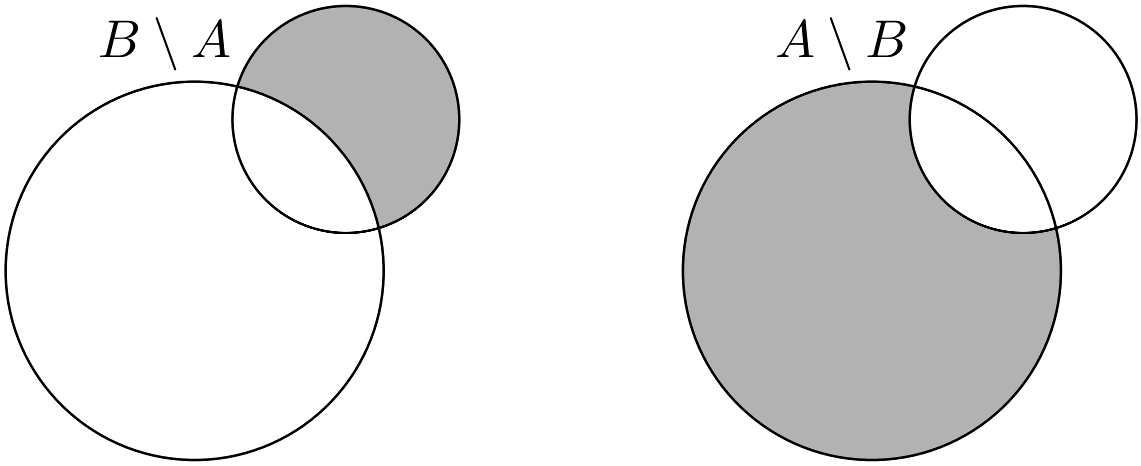

Рис. 3: Разность $B \setminus A$ (слева) $A \setminus B$ и (справа)

Ещё две важных операции определяются через предыдущие.

Дополнение: Если A и B — множества и $A \supset B$, то разность $A \setminus B$ называется *дополнением* множества B в A и обозначается через $\overline{B}$. Дополнение представлено левой диаграммой Венна на рис. 4.

Симметрическая разность: *Симметрической разностью* двух множеств A и B называется множество

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

(см. рис. 4 справа).

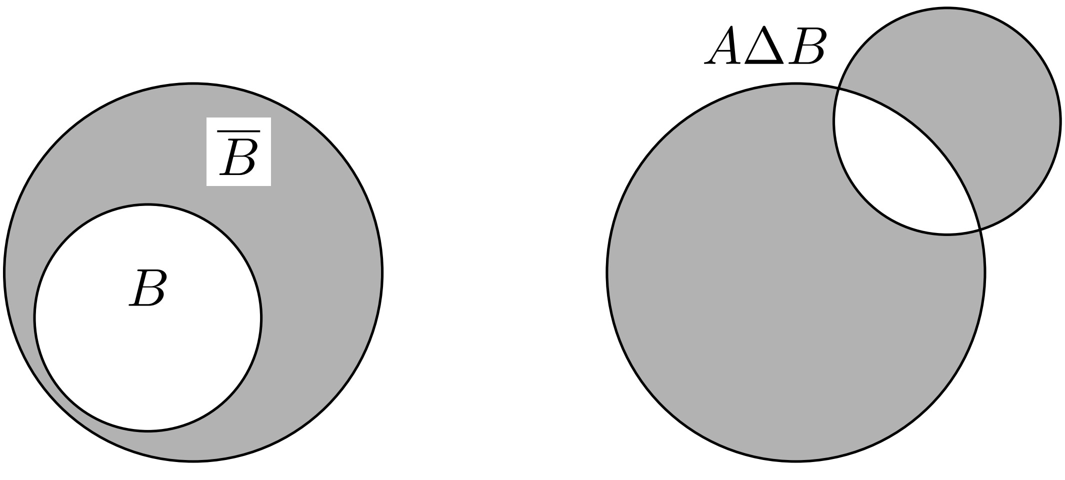

Рис. 4: Дополнение (слева) и симметрическая разность (справа)

Предложение 2 (свойства теоретико-множественных операций). *Предположим, что A, B и C — множества, и будем считать, что все они являются подмножествами некоторого множества $\mathfrak{U}$. Тогда справедливы равенства:*

$$A \cup B = B \cup A, \tag{2}$$

$$A \cup (B \cup A) = (A \cup B) \cup A, \tag{3}$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \tag{4}$$

$$A \cup \varnothing = A, \tag{5}$$

$$A \cup \overline{A} = \mathfrak{U}, \tag{6}$$

$$A \cap (B \cap C) = (A \cap B) \cap C, \tag{7}$$

$$A \cap B = B \cap A, \tag{8}$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \tag{9}$$

$$A \cap \mathfrak{U} = A, \tag{10}$$

$$A \cap \overline{A} = \varnothing, \tag{11}$$

$$A \cup \mathfrak{U} = \mathfrak{U}, \tag{12}$$

$$A \cap \varnothing = \varnothing, \tag{13}$$

а также

$$\overline{A \cup B} = \overline{A} \cap \overline{B}, \tag{14}$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \tag{15}$$

и

$$\overline{(\overline{A})} = A. \tag{16}$$

Равенства (14) и (15) называются *законами двойственности* (или *правилами де Моргана*).

Связь с логикой. Операции над множествами соответствуют тем логическим законам, которым, как правило, подчиняются разумные рассуждения, используемые в обыденной жизни[3]. Математические модели (схемы) этих рассуждений изучает *математическая логика* — специальный раздел математики, — для нас же в данном случае будут полезны обозначения, используемые в логике, их толкование и связь с теорией множеств. Операции, которые обсуждаются ниже, совершаются над *высказываниями*, то есть некоторыми утверждениями, которые могут быть либо *истинными*, либо *ложными*.

[3]Как правило, но не всегда, логика реальной жизни значительно богаче формальной!

Импликация: *Импликация* высказываний означает, что одно из них *следует* из другого. Импликация обозначается символом $\Rightarrow$ (используются также обозначения $\to$ и $\supset$), и ей соответствует вложение множеств: пусть $A \subset B$, тогда

$$a \in A \Rightarrow a \in B.$$

Например, если A — множество всех квадратов, а B — множество прямоугольников, то, конечно, $A \subset B$ и

$$(a \text{ — квадрат}) \Rightarrow (a \text{ — прямоугольник})$$

(если a является квадратом, то a является прямоугольником).

Дизъюнкция: *Дизъюнкция* — это связь высказываний через логическое «или». Она обозначается через $\vee$ и соответствует объединению множеств[4]:

$$(a \in A) \vee (a \in B) \Leftrightarrow (a \in A \cup B).$$

Заметим, что логическое «или» имеет *объединительный* смысл (в отличие от его каждодневного употребления, когда «или» понимается как «или–или», но не оба вместе). Например, высказывание

$$(x > 2) \vee (x < 3)$$

означает, что x — любое число.

Конъюнкция: *Конъюнкция* — логическое «и» обозначается через & и соответствует пересечению множеств

$$(a \in A) \,\&\, (a \in B) \Leftrightarrow (a \in A \cap B).$$

Для конъюнкции используются также обозначения $\wedge$ и «$\cdot$». Конъюнкция двух высказываний описывает объекты, обладающие и первым, и вторым свойством. Например, запись

$$(a \text{ — ромб}) \,\&\, (a \text{ — прямоугольник})$$

означает, что a является квадратом.

Отрицание: *Отрицание* высказывания обозначается символом $\neg$ и соответствует операции дополнения множеств:

$$\neg(a \in A) \Leftrightarrow a \in \overline{A}.$$

Например, если x — число, то

$$\neg(x > 0)$$

означает, что $x \leqslant 0$.

[4] Двойная стрелка $\Leftrightarrow$ означает, что высказывания *логически эквивалентны*, т.е. первое является следствием (импликацией) второго и наоборот. Такая двойная стрелка называется *эквиваленцией* высказываний.

Свойства теоретико-множественных операций (2)–(16) соответствующим образом находят отражение в свойствах высказываний. Например, законы двойственности (14) и (15) на языке высказываний имеют вид

$$\neg(x \vee y) \Leftrightarrow (\neg x)\,\&\,(\neg y)$$

и

$$\neg(x\,\&\,y) \Leftrightarrow (\neg x) \vee (\neg y).$$

Кванторы. При описании свойств математических объектов часто используют так называемые *кванторы*. Важнейшими из них являются *квантор общности*, обозначаемый символом $\forall$, и *квантор существования*, обозначаемый через $\exists$. При этом запись

$$\forall a \in A\ (\textit{высказывание})$$

означает, что *любой* элемент множества A обладает свойствами, описываемыми соответствующим высказыванием, а запись

$$\exists a \in A\ (\textit{высказывание})$$

означает, что *существует* хотя бы один элемент, обладающий этими свойствами.

Например, запись

$$\exists M \in \mathbb{R}\colon \forall a \in A \subset \mathbb{R},\ a \leqslant M \tag{17}$$

означает, что подмножество действительных чисел A обладает следующим свойством: существует такое действительное число M, что любое число a из этого подмножества не превосходит M (иными словами, множество A ограничено сверху).

Чтобы построить отрицание какой-то записи, содержащей кванторы, нужно $\forall$ заменить на $\exists$ и наоборот, а смысл высказываний поменять на противоположный. Например, отрицание записи (17) выглядит следующим образом:

$$\forall M \in \mathbb{R}\colon \exists a \in A \subset \mathbb{R},\ a > M$$

и выражает тот факт, что множество A нельзя ограничить сверху никаким числом.

Наряду с квантором $\exists$ используется квантор $\exists!$, означающий *единственность* существования чего-то. Например, запись

$$\forall a \in \mathbb{R}, a > 0, \exists! b \in \mathbb{R}, b > 0\colon b^2 = a$$

выражает существование единственного положительного квадратного корня из положительного действительного числа.

Необходимость и достаточность. Понятия *необходимости* и *достаточности* являются важнейшими составляющими многих математических рассуждений и доказательств.

Некоторое свойство X называется *достаточным*, для того чтобы объект обладал свойством Y, если наличие свойства X влечёт за собой наличие свойства Y. Например, для того чтобы четырёхугольник являлся прямоугольником, достаточно, чтобы он был квадратом. Или, для того чтобы число делилось на три, достаточно, чтобы сумма его цифр делилась на девять. Пусть B — множество объектов, обладающих свойством X, а A — множество объектов, обладающих свойством Y. Тогда X достаточно для Y означает, что $B \subset A$. Например, множество квадратов является подмножеством множества прямоугольников. На языке логики достаточность выражается записью $X \Rightarrow Y$: «если квадрат, то прямоугольник».

Если свойство X достаточно для Y, то, в свою очередь, Y *необходимо* для X. Так, для того чтобы четырёхугольник был квадратом, необходимо, чтобы он был прямоугольником. Чтобы число делилось на четыре, необходимо, чтобы оно было чётным.

Условие, являющееся одновременно и необходимым, и достаточным называется *необходимым и достаточным.* Например, для того чтобы ромб являлся квадратом, необходимо и достаточно, чтобы он был прямоугольником. Необходимость и достаточность в математических текстах часто выражают словами «тогда и только тогда»: натуральное число тогда и только тогда делится на три, когда сумма его цифр кратна трём. Ещё одно синонимичное выражение — «в том и только в том случае»: треугольник является равнобедренным в том и только в том случае, когда одна из его высот совпадает с соответствующей биссектрисой.

§2. Отображения и отношения

Понятие *отображения*, или *соответствия*, как и понятие множества, также принадлежит к числу основополагающих и неопределимых понятий математики. Говорят, что f — отображение из множества A в множество B, если задан *закон*, *правило*, позволяющие по каждому элементу $a \in A$ *однозначно* определить элемент $f(a) \in B$. При этом элемент $b = f(a)$ называется *образом* элемента a при отображении f, а элемент a — *прообразом* элемента b. Два отображения $f, g\colon A \to B$ считаются *равными*, если $f(a) = g(a)$ для всех элементов $a \in A$. Тогда пишут $f = g$. Множество всевозможных образов отображения f обозначается через $f(A)$:

$$f(A) = \{\, b \in B \mid \exists a \in A\colon b = f(a) \,\} \subset B.$$

Множество прообразов элемента b обозначается через $f^{-1}(b)$:

$$f^{-1}(b) = \{\, a \in A \mid b = f(a) \,\} \subset A.$$

Если f — отображение из A в B, то пишут $f\colon A \to B$. Множество всех отображений из A в B обозначается через B^A.

Отображение $f\colon A \to B$ называется *отображением на* (или *сюръекцией*), если $f(A) = B$, то есть если любой элемент множества A является образом некоторого элемента из B:

$$\forall b \in B\ \exists a \in A\colon b = f(a).$$

Отображение называется *вложением* (или *инъекцией*), если прообраз любого элемента из B содержит не более одного элемента из A:

$$\forall a, a' \in A\colon f(a) = f(a') \Rightarrow a = a'.$$

Наконец, отображение $f\colon A \to B$ называется *взаимно однозначным соответствием* (или *биекцией*), если оно одновременно является и инъекцией, и сюръекцией, то есть если любой элемент $b \in B$ является образом какого-то элемента $a \in A$, и всякий элемент $b \in B$ обладает ровно одним прообразом.

Пример 1. Пусть $\mathcal{K}$ — колода карт, то есть множество всевозможных карт различной масти и достоинства. Сопоставим каждой карте её масть. Тем самым мы определим отображение $f\colon \mathcal{K} \to S$ в множество S, заданное записью (1), поскольку всякая карта обладает единственной мастью. Это отображение является сюръекцией[5].

Пример 2. Пусть отображение $f\colon \mathbb{R} \to \mathbb{R}$ сопоставляет каждому действительному числу его квадрат. Тогда

$$f^{-1}(y) = \begin{cases} \{\sqrt{y}, -\sqrt{y}\}, & \text{если } y > 0,\\ \{0\}, & \text{если } y = 0,\\ \varnothing & \text{если } y < 0,\end{cases}$$

и $f(\mathbb{R})$ есть множество всех неотрицательных чисел.

Пример 3. Рассмотрим действительное число x и сопоставим ему такое число y, что

$$y^2 = x. \tag{18}$$

Эта конструкция *не* задаёт отображения, поскольку, во-первых, квадратный корень можно извлекать только их неотрицательных чисел и, во-вторых, при

[5]Если часть карт из колоды потеряна, то это отображение может и не быть сюръективным.

$x > 0$ существует *два* значения y, определяемых уравнением (18). Если, однако, рассматривать только неотрицательные x и выбрать какое-то одно значение корня (например, $y \geqslant 0$), то мы получим взаимно-однозначное соответствие из множества неотрицательных действительных чисел в себя. То же самое отображение, понимаемое как отображение во всё множество действительных чисел, является инъекцией.

Пусть A — произвольное множество. Тогда отображение $\mathrm{id}_A\colon A \to A$, сопоставляющее каждому элементу $a \in A$ его самого, то есть

$$\forall a \in A\colon\ \mathrm{id}_A(a) = a,$$

называется *тождественным*. Если понятно, какое множество имеется в виду, пишут просто id.

Если A, B и C — множества, а

$$f\colon A \to B, \qquad g\colon B \to C$$

— отображения, то можно определить отображение $g \circ f\colon A \to C$, полагая

$$(g \circ f)(a) = g(f(a)), \qquad a \in A.$$

Это отображение называется *композицией* отображений f и g.

Предложение 3. *Если $f\colon A \to B$, $g\colon B \to C$ и $h\colon C \to D$ — произвольные отображения множеств, то*

$$h \circ (g \circ f) = (h \circ g) \circ f \tag{19}$$

и

$$\mathrm{id}_B \circ f = f, \qquad f \circ \mathrm{id}_A = f. \tag{20}$$

Кроме того, композиция сюрьекций является сюръекцией, а композиция инъекций — инъекцией.

Отображение $g\colon B \to A$ называется *обратным* к отображению $f\colon A \to B$, если

$$g \circ f = \mathrm{id}_A, \qquad f \circ g = \mathrm{id}_B\,.$$

Очевидно, что и g обратно к f. В этом случае пишут $g = f^{-1}$ и $f = g^{-1}$ и отображения называют *взаимно обратными*.

Предложение 4. *Отображение $f\colon A \to B$ обладает обратным тогда и только тогда, когда оно является взаимно однозначным соответствием.*

Декартово произведение. Пусть A и B — множества.

Определение 1. *Декартовым* (или *прямым*) *произведением* множеств A и B называется множество

$$A \times B = \{\, (a, b) \mid a \in A,\ b \in B \,\},$$

состоящее из всевозможных *упорядоченных* пар элементов $a \in A$ и $b \in B$. Отображения $\mathrm{pr}_A\colon A \times B \to A$ и $\mathrm{pr}_B\colon A \times B \to B$, задаваемые условиями

$$\mathrm{pr}_A(a, b) = a, \qquad \mathrm{pr}_B(a, b) = b,$$

называются *проекциями* на левый и правый сомножители. Аналогичным образом определяется декартово произведение трёх и более множеств.

Пример 4. Если N — множество различных достоинств карт из колоды, то есть

$$N = \{2,\ 3, \ldots, 10,\ \text{В, Д, К, Т}\},$$

а S — множество мастей, то $N \times S$ — множество всех карт колоды. Например, пара $(\text{Т}, \spadesuit)$ — это туз пик, пара $(3, \clubsuit)$ обозначает тройку треф и т.п.

Пример 5. Всевозможные прямоугольные таблицы — это прямые произведения, в которых одним сомножителем является множество имён строк, а вторым — множество имён столбцов. При этом заполненная таблица является отображением из этого произведения в множество соответствующих значений.

Пример 6. Если $X = [x, x']$ и $Y = [y, y']$ — отрезки, то $X \times Y$ — прямоугольник со сторонами X и Y.

Пример 7. Декартово произведение $\mathbb{R} \times \mathbb{R}$ — это плоскость.

Предложение 5. *Пусть A и B — множества. Тогда отображение $f\colon A \times B \to B \times A$, определённое равенством*

$$f(a, b) = (b, a), \qquad a \in A, \quad b \in B,$$

является биекцией. Если C — третье множество, то отображение $g\colon (A \times B) \times C \to A \times (B \times C)$, определённое равенством

$$g((a, b), c) = (a, (b, c)), \qquad a \in A, \quad b \in B, \quad c \in C,$$

— также биекция.

Пусть A — множество. Рассмотрим множество $A^n = \underbrace{A \times \cdots \times A}_{n \text{ раз}}$.

Определение 2. Подмножество $\mathcal{R} \subset A^n$ называется *n-арным отношением* на множестве A. Говорят, что элементы $a_1, \ldots, a_n$ *связаны* отношением $\mathcal{R}$, если

$$A^n \ni (a_1, \ldots, a_n) \in \mathcal{R}.$$

В этом случае пишут

$$a_1\mathcal{R}\ldots\mathcal{R}a_n. \tag{21}$$

Иногда отношением называют запись (21), а само множество $\mathcal{R}$ называют *графиком* этого отношения.

Пример 8. Если $n = 1$, то отношение называется *унарным*. Таким образом, унарные отношения — это просто подмножества множества A. Например, свойство карты быть бубной является унарным отношением, определённым на колоде карт.

Пример 9. Если $n = 2$, то отношение называется *бинарным*. Например, свойство двух чисел не иметь общих делителей является бинарным отношением на множестве натуральных чисел. Свойство двух точек прямой находиться друг от друга на расстоянии не более заданного числа ε является бинарным отношением на множестве действительных чисел.

Пример 10. Пусть $f\colon A \to A$ — отображение множества A в себя. Ему соответствует бинарное отношение

$$\mathcal{G}_f = \{\, (a, f(a)) \mid a \in A \,\} \subset A \times A, \tag{22}$$

которое называется *графиком* отображения f.

Пример 11. Если $n = 3$, то отношение называется *тернарным*. Например, свойство трёх точек быть вершинами равностороннего треугольника — тернарное отношение на плоскости. Свойство трёх человек быть отцом, матерью и ребёнком является тернарным отношением на множестве всех людей.

Рассмотрим два важных типа бинарных отношений.

Отношения эквивалентности. Рассмотрим множество A.

Определение 3. Бинарное отношение $\mathcal{R} \subset A \times A$ называется *отношением эквивалентности*, если оно обладает следующими свойствами:

рефлексивность:	$a\mathcal{R}a$,	(23)
симметричность:	$a\mathcal{R}b \Rightarrow b\mathcal{R}a$,	(24)
транзитивность:	$a\mathcal{R}b \;\&\; b\mathcal{R}c \Rightarrow a\mathcal{R}c$	(25)

для любых элементов a, b, $c \in A$.

Очень часто отношения эквивалентности обозначают символом $\sim$. В этом случае свойства (23)—(25) перепишутся в виде:

рефлексивность:	$a \sim a$,
симметричность:	$a \sim b \Rightarrow b \sim a$,
транзитивность:	$a \sim b \;\&\; b \sim c \Rightarrow a \sim c$.

Пример 12. Свойство двух карт колоды быть одной масти является отношением эквивалентности.

Пример 13. Свойство двух точек плоскости, не совпадающих с началом координат O, лежать на одном луче, проходящем через O, — отношение эквивалентности.

Пример 14. Скажем, что два множества *равномощны* (или имеют *одинаковую мощность*), если между ними существует взаимно-однозначное соответствие. Равномощность — отношение эквивалентности.

Пусть $\sim$ — отношение эквивалентности на множестве A. Подмножество

$$[a] = \{\, b \in A \mid b \sim a \,\} \subset A$$

называется *классом эквивалентности* элемента a (построенным по отношению $\sim$).

Предложение 6. *Любые два класса эквивалентности либо не пересекаются, либо совпадают.*

Определение 4. Множество классов эквивалентности, построенных по некоторому отношению $\sim$, называется *фактормножеством* и обозначается через $A/\sim$. Сопоставление каждому элементу $a \in A$ его класса эквивалентности называется *факторотображением*, или *отображением факторизации*:

$$\pi\colon A \to A/\sim, \qquad \pi(a) = [a].$$

Пример 15. В примере 12 фактормножеством является множество мастей, а отображение факторизации сопоставляет каждой карте её масть.

Пример 16. В примере 13 каждому классу эквивалентности можно сопоставить угол между соответствующим лучом и положительным направлением оси OX, а фактормножество отождествить, например, с единичной окружностью с центром в начале координат.

Пример 17. В примере 14 множества объединяются в классы эквивалентности, содержащие равномощные множества. Такой класс эквивалентности называется *кардинальным числом*, хотя и не является числом в обычном понимании (см. ниже).

Отношения порядка. Пусть A — множество.

Определение 5. Отношение $\mathcal{R} \subset A \times A$ называется *отношением порядка*, если оно обладает следующими свойствами:

рефлексивность:	$a\mathcal{R}a,$	(26)
транзитивность:	$a\mathcal{R}b \;\&\; b\mathcal{R}c \Rightarrow a\mathcal{R}c,$	(27)

$$\text{антисимметричность:} \qquad a\mathcal{R}b \ \&\ b\mathcal{R}a \Rightarrow a = b. \tag{28}$$

Если множество снабжено отношением порядка, оно называется *упорядоченным.* Если отношение порядка обладает дополнительным свойством

$$\forall a, b \in A\colon a\mathcal{R}b \lor b\mathcal{R}a, \tag{29}$$

то множество называется *линейно упорядоченным.*

Отношение порядка часто обозначается символом $\leqslant$. В этом случае свойства (26)—(28) перепишутся в виде:

$$\begin{array}{ll} \text{рефлексивность:} & a \leqslant a, \\ \text{транзитивность:} & a \leqslant b \ \&\ b \leqslant c \Rightarrow a \leqslant c, \\ \text{антисимметричность:} & a \leqslant b \ \&\ b \leqslant a \Rightarrow a = b, \end{array}$$

а свойство (29) — в виде

$$\forall a, b \in A\colon a \leqslant b \lor b \leqslant a.$$

Пример 18. Отношение «меньше или равно» является отношением линейного порядка на множестве натуральных (а также целых, рациональных и действительных) чисел.

Пример 19. Свойство множества быть подмножеством другого определяет отношение порядка на множестве 2^A, где A — какое-то множество. Этот порядок не является линейным.

Пример 20 (лексикографический порядок). Пусть $\mathfrak{A}$ — какой-то алфавит (например, кириллический или латинский), то есть конечное и линейно упорядоченное множество букв. Тогда множество слов, записанных в этом алфавите тоже линейно упорядочено (как это сделано в словарях). Этот порядок слов называется *лексикографическим.*

Кардинальные числа. В примере 17 было введено понятие кардинального числа как класса эквивалентности равномощных множеств. Поскольку, по определению, все множества с данным кардинальным числом имеют одну и ту же мощность, понятие кардинального числа и понятие мощности — это одно и то же. Кардинальное число множества A (или его мощность) обозначается через $|A|$ (иногда через $\#(A)$).

Пример 21. Пусть T — множество, состоящее из двух элементов. Тогда множество подмножеств любого множества A равномощно множеству T^A, состоящему из всевозможных отображений из A в T.

Мощности множеств можно сравнивать.

Определение 6. Пусть A и B — множества. Скажем, что $|A| \leqslant |B|$ (то есть множество A *не мощнее* множества B), если A равномощно какому-нибудь подмножеству множества B. Скажем, что $|A| < |B|$, если $|A| \leqslant |B|$ и A не равномощно B.

Теорема 1. *Пусть A — произвольное множество. Тогда $|A| < |2^A|$.*

Определение 7. Множество называется *бесконечным*, если оно равномощно своему собственному подмножеству. В противном случае оно называется *конечным*.

Арифметика изучает кардинальные числа множеств, не являющихся бесконечными.

§3. Натуральные, целые и рациональные числа

Господь дал людям единицу, а остальное они придумали сами.

Широко известный факт, обнаруженный Леопольдом Кронекером.

На самом деле, как это ни парадоксально, построение всей математики можно начать с пустого множества. Положим $\#(\varnothing) = 0$ — это определение нуля! Единица — это кардинальное число множества $2^{\varnothing}$: $\#(2^{\varnothing}) = 1$, и множество $2^{\varnothing}$ содержит ровно один элемент. Располагая этим множеством, мы можем построить множества с произвольным *конечным* числом элементов. Так, множество мощности 2 получается объединением двух одноэлементных множеств, и, если построено множество мощности n, то множество мощности $n+1$ получается из предыдущего добавлением одноэлементного множества. Получаемые таким образом кардинальные числа называются *натуральными*. Множество натуральных чисел линейно упорядочено,

$$1 < 2 < \ldots < n < n+1 < \ldots,$$

обозначается через $\mathbb{N}$ и называется *натуральным рядом*.

Замечание. Натуральный ряд обладает более сильным свойством, чем линейный порядок: у каждого натурального числа есть *последующее* и у каждого, кроме единицы, — *предыдущее*.

Аксиома индукции. Заметим, что само определение натуральных чисел *индуктивно*: следующее натуральное число определяется добавлением единицы к предыдущему. Это отражает важнейшее свойство натурального ряда, которое называется *аксиомой* (или *принципом*) *математической индукции*: если какое-то утверждение верно для 1 и из предположения, что оно верно для n, следует, что оно верно для $n+1$, то это утверждение верно для всех натуральных чисел[6].

Принцип математической индукции является одним из основных при определении понятий и доказательстве различных утверждений, относящихся к натуральным числам. Например, сложение и умножение натуральных чисел *определяется по индукции следующим образом*:

Сложение:	Умножение:
$1+1=2,$	$1\cdot 1=1,$
$n+(m+1)=(n+m)+1,$	$n\cdot(m+1)=n\cdot m+n,$

а потом по индукции же *доказывается*, что эти операции обладают известными свойствами:

$n+m=m+n,$	коммутативность сложения,
$(n+m)+k=n+(m+k),$	ассоциативность сложения,
$1\cdot n=n,$	умножение на единицу тождественно,
$n\cdot m=m\cdot m,$	коммутативность умножения,
$n\cdot(m\cdot k)=(n\cdot m)\cdot k,$	ассоциативность умножения,
$n\cdot(m+k)=n\cdot m+n\cdot k,$	дистрибутивность умножения относительно сложения.

Докажем, например, что $1\cdot n=n$. Для $n=1$ это выполняется по определению. Предположим, что при n это верно. Тогда из определения умножения и сделанного предположения следует, что

$$1\cdot(n+1)=1\cdot n+1\cdot 1=n+1.$$

Значит, по принципу индукции это верно для всех n.

Множество натуральных чисел бесконечно. Его мощность обозначается через $\aleph_0$, и всякое множество, имеющее такую мощность, то есть равномощное натуральному ряду, называется *счётным*[7].

---

[6]Мы предполагаем, что натуральный ряд начинается с единицы. Можно считать, что он начинается с нуля, — это вопрос договорённости. Аксиому индукции можно также переформулировать следующим образом: если какое-то утверждение верно для некоторого натурального числа k и из предположения, что оно верно для $n>k$, следует, что оно верно для $n+1$, то это утверждение верно для всех натуральных чисел, бо́льших или равных k.

[7]$\aleph$ — первая буква древнееврейского алфавита; читается «а́леф».

Целые числа. *Целые* числа возникают как решения уравнений вида

$$x + n = 0, \qquad n \in \mathbb{N}, \tag{30}$$

которые нельзя решить, находясь внутри натурального ряда. А именно, мы «собственными руками» расширяем натуральный ряд нулём, а также «значками» вида «$-n$», где n — натуральное число (эти значки называются *отрицательными* целыми числами), и полагаем

$$n + (-1) = \{\text{число, предшествующее } n\},$$

если $n > 1$, и далее по индукции

$$n + (-(m+1)) = \begin{cases} n - m - 1, & \text{если } n > m+1, \\ 0, & \text{если } n = m+1, \\ -(m - n + 1), & \text{если } n < m+1. \end{cases}$$

Умножаются целые числа по правилам

$$(-n) \cdot m = -(nm), \qquad (-n) \cdot (-m) = nm.$$

Далее можно доказать, что сложение и умножение целых чисел коммутативно, ассоциативно и дистрибутивно. Полученное множество с операциями сложения и умножения обозначается через $\mathbb{Z}$. Оно счётно и тоже линейно упорядочено:

$$\ldots - (n+1) < -n < \ldots < -1 < 0 < 1 < \ldots$$

Кроме того, в отличие от натуральных чисел, все целые числа можно вычитать друг из друга:

$$n - m = n + (-m), \quad n - (-m) = n + m,$$
$$(-n) - m = -(n + m), \quad (-n) - (-m) = m - n.$$

Замечание. Пифагор, живший в VI в. до нашей эры, считал, что числа существуют в природе. С тех пор человечество шагнуло далеко вперёд, и, как мы убедились, даже такие «естественные» числа, как натуральные и целые, создаются «руками».

Рациональные числа. *Рациональные* числа возникают при решении уравнения

$$mx + n = 0, \qquad m, n \in \mathbb{Z}, \tag{31}$$

которое, вообще говоря, неразрешимо в целых числах. Чтобы сделать уравнение (31) разрешимым, вводят понятие *рациональной дроби*, и делают это следующим образом.

Рассмотрим прямое произведение $\mathbb{Z}\times\mathbb{Z}$ и подмножество

$$Q = \{\,(m,n)\mid m,n\in\mathbb{Z},\ n\neq 0\,\}\subset\mathbb{Z}\times\mathbb{Z}.$$

Введём на множестве пар $(m,n)\in Q$ отношение P, полагая

$$(m,n)P(m',n')\Leftrightarrow mn'=nm'. \tag{32}$$

Предложение 7. *P — отношение эквивалентности.*

Обозначим через $\frac{m}{n}$ класс эквивалентности пары (m,n) и назовём этот класс *рациональной дробью* с *числителем* m и *знаменателем* n. На множестве рациональных дробей можно ввести операции *сложения* и *умножения*, полагая

$$\frac{m}{n}+\frac{k}{l}=\frac{ml+kn}{nl},\qquad \frac{m}{n}\cdot\frac{k}{l}=\frac{mk}{nl}. \tag{33}$$

Ситуация оказывается, однако, не столь простой, как это кажется на первый взгляд. Дело в том, что по определению рациональная дробь — это класс эквивалентности, то есть множество, а определение операций, данное равенствами (33), фактически формулируется в терминах отдельных элементов, то есть *представителей* этих классов. Поэтому, вообще говоря, может случиться так, что выбрав два разных представителя, мы получим разные результаты. Чтобы этого не случилось, определение (33) должно быть, как говорят в математике, *корректным*. Это означает следующее.

Предложение 8. *Пусть (m,n) и (m',n'), а также (k,l) и (k',l') — пары, эквивалентные в смысле отношения эквивалентности* (32). *Тогда пары*

$$(ml+kn,nl),\qquad (m'l'+k'n',n'l')$$

и

$$(mk,nl),\qquad (m'k',n'l')$$

также эквивалентны.

Это и означает, что сложение и умножение рациональных дробей действительно определено на множестве этих дробей, а не на отдельных парах, из которых эти дроби строятся.

Замечание. Класс эквивалентности пары (m,n) состоит из всевозможных дробей, которые приводятся друг к другу «сокращением числителя и знаменателя на общий множитель». То есть вводя отношение эквивалентности (32), мы на самом деле говорим, что, скажем, $\frac{1}{2}$ и $\frac{2}{4}$ — это одно и то же. К сожалению, никак проще, чем это было сделано выше, этого сделать нельзя (если мы, конечно, хотим придерживаться математической строгости).

Полученное множество дробей обозначается через $\mathbb{Q}$ и называется *полем рациональных чисел*[8]. В этом поле можно складывать, вычитать, умножать

[8] О понятии поля см. ниже гл. IV.

и, в отличие от целых чисел, делить на любую ненулевую дробь. Существует инъекция множества целых чисел в поле $\mathbb{Q}$: каждому целому числу m можно сопоставить дробь $\frac{m}{1}$.

Может показаться, что рациональных чисел «гораздо больше», чем целых. На самом деле это не так.

Предложение 9. *Множество $\mathbb{Q}$ рациональных чисел счётно.*

Заметим также, что множество рациональных чисел линейно упорядочено: $\frac{m}{n} \leqslant \frac{k}{l}$ тогда и только тогда, когда

$$(ml - nk)nl \leqslant 0. \tag{34}$$

Этот порядок согласован с порядком, заданным на множестве целых чисел: если $m, n \in \mathbb{Z}$, то $m \leqslant n$ тогда и только тогда, когда $\frac{m}{1} \leqslant \frac{n}{1}$.

Замечание. Фактически, к понятию рационального числа пришли ещё древние греки (и, как ни странно, рациональные числа были «изобретены» гораздо раньше, чем целые отрицательные). Правда, они использовали не абстрактный алгебраический язык, а язык геометрии, рассматривая задачу о *соизмеримости отрезков*. Они же обнаружили существование *несоизмеримых* отрезков, то есть, говоря современным языком, *иррациональных чисел*. Чтó это такое, мы обсудим в §4.

§4. Действительные числа

Действительные числа проходят в школе.
Распространённое заблуждение.

Хотя по-настоящему строго действительные числа были определены только во второй половине XIX в. Р. Дедекиндом, представление об их существовании сформировалось, как уже отмечалось, ещё у древних греков.

Несоизмеримые отрезки. Два отрезка называются *соизмеримыми*, если они имеют *общую меру*, то есть если существует такой отрезок, который укладывается целое число раз и в первом, и во втором отрезке. Если такого отрезка нет, отрезки называются *несоизмеримыми*. Примером несоизмеримых отрезков являются сторона и диагональ квадрата. Действительно, если принять сторону квадрата за a, а длину диагонали за c, то из теоремы Пифагора будет следовать, что

$$c^2 = 2a^2. \tag{35}$$

Соизмеримость означает, что $c = ml$, $a = nl$, где l — общая мера. Поэтому уравнение (35) перепишется в виде

$$m^2 = 2n^2, \qquad m, n \in \mathbb{N}. \tag{36}$$

Можно считать, что числа m и n не имеют общего делителя (в противном случае на этот делитель можно было бы сократить). Из уравнения (36) следует, что число m делится на 2, то есть $m = 2k$, $k \in \mathbb{N}$. Значит, $2k^2 = n^2$ и, следовательно, n тоже делится на 2. Но это противоречит предположению о том, что m и n не имеют общего делителя. Следовательно, представление (36) невозможно.

Последовательные приближения. Несмотря на полученный выше отрицательный результат, мы можем сколь угодно точно найти выражение величины c через a. Именно, положим $c = ax$, и тогда равенство (35) примет вид

$$x^2 = 2. \tag{37}$$

Поскольку $1^2 < 2$, а $2^2 > 2$, искомое решение, если оно существует, должно лежать в интервале $(1, 2)$. Рассмотрим середину этого интервала — число $\frac{3}{2}$; оно отличается от решения не более, чем на $\frac{1}{2}$. Далее очевидно, что решение должно лежать в интервале $(1, \frac{3}{2})$, поскольку $(\frac{3}{2})^2 > 2$. Следовательно, число $\frac{5}{4}$ — середина интервала $(1, \frac{3}{2})$ — отличается от решения не более, чем на $\frac{1}{4}$. На следующем шаге мы замечаем, что решение лежит в интервале $(\frac{5}{4}, \frac{3}{2})$ и так далее, до бесконечности.

Рассмотренный пример показывает, что существует «нечто», являющееся решением уравнения (37), но это — не рациональное число, хотя и может быть как угодно точно приближено рациональными числами. Что это такое объясняется ниже.

Сечения Дедекинда. Итак, мы установили, что в множестве рациональных чисел имеются лакуны, «дыры». Оказывается, их можно «заклеить».

Определение 8. Пара подмножеств (A, A'), где $A, A' \subset \mathbb{Q}$, называется *сечением Дедекинда* (или просто сечением) множества рациональных чисел, если выполняются следующие условия:

1) $A, A' \neq \varnothing$;
2) $A \cup A' = \mathbb{Q}$;
3) $A \cap A' = \varnothing$;
4) $\forall p \in A,\ q \in A' \Rightarrow p < q$.

Множество A называется *нижним классом* сечения, а множество A' — его *верхним классом*.

Иными словами, сечение — это такое разбиение множества рациональных чисел на два подмножества, что любое рациональное число попадает в одно из этих подмножеств (но не в оба вместе) и всякое число из нижнего класса строго меньше всякого числа, принадлежащего верхнему классу.

Пример 22. Пусть

$$A = \{\, p \in \mathbb{Q} \mid p^2 > 2 \ \&\ p > 0 \,\}$$

и

$$A' = \{\, q \in \mathbb{Q} \mid (q \leqslant 0) \vee (q^2 \leqslant 2 \ \&\ q > 0) \,\}.$$

Пара (A,A') — сечение множества рациональных чисел.

Пример 23. Пара

$$A = \{\, p \in \mathbb{Q} \mid p < 0 \,\}, \quad A' = \{\, q \in \mathbb{Q} \mid q \geqslant 0 \,\}.$$

является сечением.

Пример 24. Пара

$$A = \{\, p \in \mathbb{Q} \mid p \leqslant 0 \,\}, \quad A' = \{\, q \in \mathbb{Q} \mid q > 0 \,\}$$

также является сечением.

Сечение, построенное в примере 22, принципиально отличается от сечений, построенных в двух других примерах. Именно, сечения из примеров 23 и 24 определяются рациональными числами, в то время как в примере 22 это не так — там построено новое число. Это, как нетрудно видеть, квадратный корень из 2.

Определение 9. Сечение множества рациональных чисел называется *рациональным*, если либо его верхний класс содержит минимальный элемент, либо его нижний класс содержит максимальный элемент. В противном случае сечение называется *иррациональным*.

Сечения из примеров 23 и 24 рациональны, а сечение, описанное в примере 22, иррационально.

Действительные числа. В определении 9 введены два типа рациональных сечений. Таким образом, все рациональные сечения разбиваются на пары, задаваемые одним и тем же рациональным числом. Мы всегда для определённости будем предполагать, что это число лежит в верхнем классе.

Определение 10. Множество $\mathbb{R}$, составленное из всех иррациональных сечений, а также таких рациональных сечений, что их верхний класс содержит минимальный элемент, называется *множеством действительных* (или *вещественных*) *чисел*.

Элементы множества $\mathbb{R}$ называются *действительными* (или *вещественными*) *числами*. Если действительному числу соответствует рациональное сечение, то оно называется *рациональным*; в противном случае оно называется *иррациональным*.

Два действительных числа считаются *равными*, если верхние классы (или, эквивалентно, нижние классы) соответствующих им сечений совпадают.

Свойства действительных чисел можно подразделить на два типа — теоретико-множественные и алгебраические. Изучению этих свойств посвящена оставшаяся часть настоящей главы.

Теоретико-множественные свойства. Первым замечательным свойством множества действительных чисел является следующее.

Теорема 2. *Множество $\mathbb{R}$ равномощно множеству подмножеств множества $\mathbb{N}$.*

Мощность множества действительных чисел обозначается буквой $\aleph$. Из теоремы 1 следует, что она больше $\aleph_0$. Можно также условно записать, что $\aleph = 2^{\aleph_0}$. Про множества, равномощные $\mathbb{R}$, говорят, что они имеют *мощность континуума*.

Второе важное свойство действительных чисел — их линейная упорядоченность. Пусть α и β — действительные числа и A и B — нижние классы соответствующих сечений.

Определение 11. Скажем, что $\alpha \leqslant \beta$, если $A \subset B$.

Предложение 10. *Введённое в определении* 11 *отношение является отношением линейного порядка на множестве действительных чисел. Более того, этот порядок согласован с линейным порядком* (34), *определённым на множестве $\mathbb{Q}$ рациональных чисел.*

Построенное отношение порядка обладает свойствами, описываемыми следующими тремя леммами.

Лемма 1. *Если α и β — действительные числа и $\alpha < \beta$, то всегда найдётся бесконечное множество таких рациональных чисел r, что $\alpha < r < \beta$.*

Лемма 2. *Если α и β — такие действительные числа, что для любого рационального числа $\varepsilon > 0$ найдутся такие рациональные числа r и r', что*

$$r \leqslant \alpha \leqslant r', \quad r \leqslant \beta \leqslant r', \quad r - r' \leqslant \varepsilon,$$

то $\alpha = \beta$.

Лемма 3. *Если α — действительное число, то всегда найдётся такое целое число n, что $n \leqslant \alpha < n + 1$.*

Число n, возникающее в лемме 3, называется *целой частью* действительного числа α и обозначается через $[\alpha]$. Разность $\alpha - [\alpha]$ называется *дробной частью* и обозначается через $\{\alpha\}$.

Поскольку множество действительных чисел упорядочено, в нём, точно так же, как это было сделано в определении 8 для рациональных чисел, можно ввести понятие сечения. Оказывается, ничего нового мы не получим:

Теорема 3 (теорема Дедекинда о непрерывности множества $\mathbb{R}$). *Если (A, A') — сечение множества действительных чисел, где A — нижний класс, а A' — верхний класс, то существует такое действительное число α, что либо*

$$A = \{\, \beta \in \mathbb{R} \mid \beta \leqslant \alpha \,\}, \quad A' = \{\, \beta \in \mathbb{R} \mid \beta > \alpha \,\},$$

либо

$$A = \{\, \beta \in \mathbb{R} \mid \beta < \alpha \,\}, \quad A' = \{\, \beta \in \mathbb{R} \mid \beta \geqslant \alpha \,\}.$$

Замечание. Теорема 3 говорит о том, что множество действительных чисел непрерывно, не имеет, в отличие от множества рациональных чисел, лакун. Поэтому множество $\mathbb{R}$ иногда называют *континуумом*[9], а равномощные ему, как уже отмечалось, множествами мощности континуума.

Обсудим теперь некоторые понятия, относящиеся к *ограниченным* подмножествам в $\mathbb{R}$.

Определение 12. Пусть $X \subset \mathbb{R}$ — подмножество.

1. Оно называется *ограниченным сверху*, если существует такое действительное число $M \in \mathbb{R}$, что $x \leqslant M$ для любого $x \in X$.
2. Оно называется *ограниченным снизу*, если существует такое число $m \in \in \mathbb{R}$, что $x \geqslant M$ для любого $x \in X$.
3. Наименьшее из чисел, ограничивающих X сверху, называется *точной верхней гранью* и обозначается через $\sup X$ (от латинского *supremum* — наивысший).
4. Наибольшее из чисел, ограничивающих X снизу, называется *точной нижней гранью* и обозначается через $\inf X$ (от латинского *infinum* — наинизший).

Если множество *не* ограничено сверху, то пишут $\sup X = +\infty$, а если оно *не* ограничено снизу, то $\inf X = -\infty$.

Теорема 4. *Всякое подмножество $X \subset \mathbb{R}$, ограниченное снизу (сверху), имеет точную нижнюю (верхнюю) грань.*

[9] От латинского *continuum* — непрерывное.

Замечание. Для подмножеств множества рациональных чисел это, вообще говоря, неверно. Например, множество

$$E = \left\{ \left(1 + \frac{1}{n}\right)^n \middle| \, n \in \mathbb{N} \right\}$$

ограничено сверху, но не имеет точной верхней грани среди рациональных чисел.

Прежде чем переходить ко второй группе свойств, установим связь между данным выше формальным определением действительного числа и привычным представлением о нём.

Приближение десятичными дробями. Действительные числа, с которыми люди сталкиваются в «обыденной жизни», являются, как правило, десятичными дробями. Это не случайно.

Предложение 11. *Пусть α — действительное число. Тогда для любого рационального числа $\varepsilon > 0$ найдутся такие конечные десятичные дроби d и d', что $d - d' \leqslant \varepsilon$ и $d \leqslant \alpha \leqslant d'$.*

Число d называется *приближением с недостатком*, число d' — *приближением с избытком*, а величина $\frac{\varepsilon}{2}$ — *точностью приближения.*

Предложение 11 означает, что произвольные действительные числа можно мыслить себе как *бесконечные десятичные дроби.* Рассмотрим такую дробь и обозначим k-ю десятичную цифру после запятой через c_k (если дробь конечна и имеет длину, меньшую k, то $c_k = 0$). Скажем, что дробь *периодическая*, если найдутся такие натуральные числа K и p, что $c_k = c_{k+p}$, для всех $k \geqslant K$.

Предложение 12. *Действительное число является рациональным тогда и только тогда, когда соответствующая ему десятичная дробь является периодической.*

Арифметические операции и их свойства.

Определение 13. Пусть α и β — действительные числа. Их *суммой* называется число γ, удовлетворяющее неравенствам

$$a + b \leqslant \gamma \leqslant a' + b',$$

где a, a', b, b' — произвольные рациональные числа, удовлетворяющие неравенствам

$$a \leqslant \alpha \leqslant a', \qquad b \leqslant \beta \leqslant b'.$$

Сумма обозначается через $\alpha + \beta$.

Предложение 13. *Для любых действительных чисел их сумма существует, единственна и обладает следующими свойствами:*

1. $\alpha + \beta = \beta + \alpha$.
2. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.
3. $\alpha + 0 = 0 + \alpha = \alpha$.
4. *Для любого числа* α *существует такое число* $-\alpha$ (*число, противоположное* α), *что* $\alpha + (-\alpha) = (-\alpha) + \alpha = 0$.
5. *Если* $\alpha < \beta$, *то и* $\alpha + \gamma < \beta + \gamma$ *для любого* $\gamma \in \mathbb{R}$.

Определим *модуль* (или *абсолютную величину*) числа α, полагая

$$|\alpha| = \begin{cases} \alpha, & \text{если } \alpha \geqslant 0, \\ -\alpha, & \text{если } \alpha < 0. \end{cases}$$

Определение 14. Пусть α и β — положительные действительные числа. Их *произведением* называется число γ, удовлетворяющее неравенствам

$$ab \leqslant \gamma \leqslant a'b',$$

где a, a', b, b' — произвольные рациональные числа, удовлетворяющие неравенствам

$$0 < a \leqslant \alpha \leqslant a', \qquad 0 < b \leqslant \beta \leqslant b'.$$

Произведение обозначается через $\alpha \cdot \beta$ (или $\alpha\beta$). Если $\beta = 0$, то мы полагаем

$$\alpha \cdot 0 = 0 \cdot \alpha = 0.$$

Для произвольных α и β их произведение определяется следующим образом:

$$\alpha \cdot \beta = \begin{cases} |\alpha| \cdot |\beta|, & \text{если } \alpha \text{ и } \beta \text{ одного знака}, \\ -(|\alpha| \cdot |\beta|), & \text{если } \alpha \text{ и } \beta \text{ разных знаков}. \end{cases}$$

Предложение 14. *Для любых действительных чисел их произведение существует, единственно и обладает следующими свойствами*:

1. $\alpha \cdot \beta = \beta \cdot \alpha$.
2. $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$.
3. $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$.
4. $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.
5. *Для любого числа* $\alpha \neq 0$ *существует такое число* α^{-1} (*число, обратное к* α), *что* $\alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1$.
6. *Если* $\alpha < \beta$ *и* $\gamma > 0$, *то и* $\alpha \cdot \gamma < \beta \cdot \gamma$.

Степени и логарифмы. Пусть α — действительное число и n — целое. Положим

$$\alpha^n = \begin{cases} \underbrace{\alpha \cdot \ldots \cdot \alpha}_{n \text{ раз}}, & \text{если } n > 0, \\ 1, & \text{если } n = 0 \text{ и } \alpha \neq 0, \\ \frac{1}{\alpha^{-n}}, & \text{если } n < 0 \text{ и } \alpha \neq 0. \end{cases}$$

При $\alpha = 0$ и $n \leqslant 0$ величина α^n не определена.

Предложение 15 (существование корней). *Пусть $\alpha > 0$ — действительное число. Тогда для любого целого числа n существует и единственно такое действительное число $\beta > 0$, что*

$$\beta^n = \alpha.$$

Число β называется *арифметическим корнем n-й степени из α* и обозначается либо через $\sqrt[n]{\alpha}$, либо через $\alpha^{-\frac{1}{n}}$. Если $\alpha < 0$ и n нечётно, то мы полагаем $\sqrt[n]{\alpha} = -\sqrt[n]{-\alpha}$. Для любого рационального числа r, представленного в виде несократимой дроби $\frac{m}{n}$, положим

$$\alpha^r = (\alpha^m)^{\frac{1}{n}}$$

во всех случаях, когда это выражение имеет смысл.

Определение 15. Пусть $\alpha > 1$ и β — действительные числа. *Степенью* числа α *с показателем* β называется такое число γ, что

$$\alpha^b \leqslant \gamma \leqslant \alpha^{b'},$$

где b и b' — любые рациональные числа, удовлетворяющие неравенствам

$$1 < b \leqslant \beta \leqslant b'.$$

Степень обозначается через α^β. Если $0 < \alpha < 1$, то мы полагаем

$$\alpha^\beta = \left(\frac{1}{\alpha}\right)^{-\beta}.$$

По определению $1^\beta = 1$.

Предложение 16. *Для любых действительных чисел $\alpha > 0$ и β их степень α^β существует, единственна и обладает следующими свойствами*:

1. $\alpha^\beta \alpha^\gamma = \alpha^{\beta+\gamma}$.
2. $\frac{1}{\alpha^\beta} = \alpha^{-\beta}$.
3. $(\alpha^\beta)^\gamma = \alpha^{\beta\gamma}$.
4. $\alpha^\gamma \beta^\gamma = (\alpha\beta)^\gamma$.

Предложение 17. *Для любых действительных чисел $\alpha > 0$, $\alpha \neq 1$, и $\beta > 0$ существует такое единственное число γ, что $\alpha^\gamma = \beta$. Это число называется* логарифмом *числа β* по основанию *α, обозначается через $\log_\alpha \beta$ и обладает следующими свойствами*:

1. $\log_\alpha \beta \cdot \log_\beta \gamma = \log_\alpha \gamma$ (*в частности*, $\log_\alpha \beta = \frac{1}{\log_\beta \alpha}$).
2. $\log_\alpha(\beta\gamma) = \log_\alpha \beta + \log_\alpha \gamma$.
3. $\log_\alpha(\beta^\gamma) = \gamma \log_\alpha \beta$.

Вопросы для самопроверки

1. Что такое множество, его элемент, подмножество? Приведите примеры.
2. Какие теоретико-множественные операции вам известны? Перечислите их, приведите примеры и проиллюстрируйте диаграммами Венна.
3. Перечислите основные свойства теоретико-множественных операций?
4. Что такое правила де Моргана? Проиллюстрируйте их с помощью диаграмм Венна.
5. Как теория множеств связана с математической логикой?
6. Какие кванторы вам известны?
7. Объясните понятия необходимости и достаточности, приведите примеры.
8. Что такое отображение, его образ и прообраз?
9. Какие виды отображений вам известны? Приведите примеры.
10. Что такое композиция отображений, обратное отображение? Опишите их свойства.
11. Что такое декартово произведение множеств? Приведите примеры.
12. Дайте определение отношения и приведите примеры.
13. Дайте определение отношения эквивалентности, приведите примеры и опишите его свойства. Объясните, что такое класс эквивалентности.
14. Что такое равномощные множества?
15. Дайте определение порядка эквивалентности, приведите примеры и опишите его свойства. Какие множества называются линейно упорядоченными.
16. Что такое кардинальное число? Какие множества называются конечными и бесконечными?
17. Что такое аксиома индукции?
18. Целые числа и операции над ними.
19. Рациональные числа и операции над ними.
20. В чём проявляется неполнота множества рациональных чисел?
21. Что такое сечения Дедекинда?
22. Действительные числа и операции над ними?
23. Непрерывность множества действительных чисел.
24. Что такое ограниченное множество? Что такое верхняя и нижняя грань множества?
25. Связь между действительными числами и десятичными дробями.

ГЛАВА II

Линейная алгебра

§6. Векторные пространства и линейные операторы

Определение 1. Множество V называется *векторным пространством* (над полем действительных чисел $\mathbb{R}$), если его элементы можно складывать между собой и умножать на действительные числа, причём эти операции обладают следующими свойствами (которые называются *аксиомами векторного пространства*):

1) сложение *коммутативно*: $u + v = v + u$ для любых u, $v \in V$;
2) сложение *ассоциативно*: $u + (v + w) = (u + v) + w$ для любых u, v и $w \in V$;
3) в множестве V существует *нулевой элемент* 0 (или *нуль*), обладающий тем свойством, что $0 + u = u + 0 = u$ для любого $u \in V$;
4) для каждого $u \in V$ существует *противоположный* ему элемент $-u$ такой, что $u + (-u) = (-u) + u = 0$;
5) умножение *ассоциативно*: $\lambda(\mu u) = (\lambda\mu)u$ для любых чисел λ, $\mu \in \mathbb{R}$ и элемента $u \in V$;
6) умножение *дистрибутивно* относительно сложения: $\lambda(u+v) = \lambda u+\lambda v$ для любого числа $\lambda \in \mathbb{R}$ и элементов u, $v \in V$;
7) умножение на единицу *тождественно*: $1 \cdot u = u$ для любого элемента $u \in V$.

Элементы векторного пространства называются *векторами*.

Пример 1. Само множество $\mathbb{R}$ действительных чисел является векторным пространством. Множество, состоящее из единственного элемента — нуля, — также является векторным пространством. Оно обозначается через 0 и называется *тривиальным*.

Пример 2. Рассмотрим множество

$$\mathbb{R}^n = \{ (\lambda_1, \ldots, \lambda_n) \mid \lambda_1, \ldots, \lambda_n \in \mathbb{R} \}$$

и положим

$$(\lambda_1, \ldots, \lambda_n) + (\lambda'_1, \ldots, \lambda'_n) = (\lambda_1 + \lambda'_1, \ldots, \lambda_n + \lambda'_n),$$
$$\lambda(\lambda_1, \ldots, \lambda_n) = (\lambda\lambda_1, \ldots, \lambda\lambda_n), \quad \lambda \in \mathbb{R}.$$

Тогда множество $\mathbb{R}^n$ превращается в векторное пространство, которое называется *n-мерным арифметическим пространством*.

Определение 2. Подмножество $V' \subset V$ векторного пространства V называется *подпространством*, если:

1. $u + v \in V'$ для любых u, $v \in V'$;
2. $\lambda u \in V'$ для любого числа $\lambda \in \mathbb{R}$ и вектора $u \in V'$,

то есть если V' *замкнуто* относительно операций сложения и умножения на числа.

Предложение 1. *Всякое подпространство векторного пространства само является векторным пространством.*

Пример 3. Пусть V — векторное пространство и $v \in V$. Тогда множество $\{\, \lambda v \mid \lambda \in \mathbb{R} \,\}$ является подпространством в V.

Определение 3. Отображение $A\colon V \to W$ двух векторных пространств V и W называется *линейным оператором* (*действующим* из V в W), если:

1) $A(u+v) = A(u) + A(v)$ для любых векторов u, $v \in V$;
2) $A(\lambda u) = \lambda A(u)$ для любого числа $\lambda \in \mathbb{R}$ и вектора $u \in V$.

Пример 4. Пусть $\lambda \in \mathbb{R}$. Тогда отображение $A_\lambda\colon V \to V$, действующее по правилу $A_\lambda(v) = \lambda v$, $v \in V$, является линейным оператором, который называется *оператором умножения* на число λ.

Определение 4. Пусть $A\colon V \to W$ — линейный оператор. Множество

$$\ker A = \{\, v \in V \mid A(v) = 0 \,\} \subset V$$

называется *ядром* оператора A. Множество

$$\operatorname{im} A = \{\, w \in W \mid \exists v \in V : w = A(v) \,\} \subset W$$

называется *образом* оператора A.

Предложение 2. *Ядро и образ любого линейного оператора являются подпространствами пространств V и W соответственно.*

Определение 5. Линейный оператор $A\colon V \to W$ называется *изоморфизмом*, если $\ker A = 0$, а $\operatorname{im} A = W$. Если A — изоморфизм, то пространства V и W называются *изоморфными*.

Пример 5. Пусть A_λ оператор умножения на λ (см. пример 4). Тогда

$$\ker A_\lambda = \begin{cases} 0, & \text{если } \lambda \neq 0, \\ V, & \text{если } \lambda = 0, \end{cases} \quad \text{и} \quad \operatorname{im} A_\lambda = \begin{cases} V, & \text{если } \lambda \neq 0, \\ 0, & \text{если } \lambda = 0. \end{cases}$$

Определение 6. Пусть U, V и W — векторные пространства, а $A\colon U \to V$, $B\colon V \to W$ — линейные операторы. Отображение $B \circ A\colon U \to W$, действующее по правилу

$$(B \circ A)(u) = B(A(u)), \quad u \in U,$$

называется *композицией* (или *произведением*) операторов A и B.

Предложение 3. *Композиция линейных операторов является линейным оператором.*

Определение 7. Пусть A, $B\colon V \to W$ — линейные операторы. Отображение $A+B\colon V \to W$, действующее по правилу

$$(A+B)(v) = A(v) + B(v), \quad v \in V,$$

называется *суммой* операторов A и B. Если λ — число, то отображение

$$(\lambda A)(v) = \lambda A(v), \quad v \in V,$$

называется *произведением* оператора на число.

Предложение 4. *Если A и B — линейные операторы, а λ — действительное число, то $A+B$ и λA — также линейные операторы.*

Пример 6. Если λ и μ — действительные числа, то выполняются равенства

$$A_\lambda + A_\mu = A_{\lambda+\mu}, \quad A_\lambda \circ A_\mu = A_{\lambda\mu}.$$

Предложение 5. *Операции над линейными операторами, введённые в определениях* 6 *и* 7, *обладают следующими свойствами*:

$$\begin{aligned}
&A + B = B + A,\\
&A + (B + C) = (A + B) + C,\\
&0 + A = A + 0 = A,\\
&-A = (-1)\cdot A,\\
&\lambda(\mu A) = (\lambda\mu)A,\\
&\lambda(A + B) = \lambda A + \lambda B,\\
&1 \cdot A = A.
\end{aligned}$$

Кроме того, имеют место следующие тождества:

$$\begin{aligned}
&A \circ (B \circ C) = (A \circ B) \circ C,\\
&A \circ (B + C) = A \circ B + A \circ C,\\
&(A + B) \circ C = A \circ C + B \circ C.
\end{aligned}$$

Следствие 1. *Множество линейных операторов, действующих из векторного пространства V в векторное пространство W, само образует векторное пространство, которое обозначается через* $\mathrm{Lin}(V, W)$.

Определение 8. Если A, $B \in \mathrm{Lin}(V, V)$, то оператор

$$[A, B] = A \circ B - B \circ A$$

называется *коммутатором* операторов A и B.

Определение 9. Оператор $E = E_V$, действующий из пространства V в себя по правилу

$$E(v) = v, \quad v \in V,$$

называется тождественным. Оператор $A \in \mathrm{Lin}(V, V)$ называется *обратимым*, если существует такой оператор $A^{-1} \in \mathrm{Lin}(V, V)$, что

$$A \circ A^{-1} = A^{-1} \circ A = E.$$

При этом оператор A^{-1} называется *обратным* к оператору A. Заметим, что справедливо тождество $(A^{-1})^{-1} = A$, т.е. оператор A обратен к A^{-1}.

Предложение 6. *Для любого линейного оператора $A\colon V \to W$ выполняются равенства*

$$E_W \circ A = A \circ E_V = A.$$

Определение 10. Пусть $A\colon V \to V$ — линейный оператор. Число $\lambda \in \mathbb{R}$ называется *собственным значением* этого оператора, если существует такой вектор $v \neq 0$, что

$$A(v) = \lambda v. \tag{1}$$

При этом v называется *собственным вектором*, отвечающим собственному значению λ.

Предложение 7. *Множество собственных векторов, отвечающих некоторому λ, образует линейное подпространство в V.*

Это подпространство называется *собственным подпространством* и, как правило, обозначается через V_λ. В частности, пространство V_0 совпадает с ядром оператора A.

§7. Базисы и размерность

Определение 11. Пусть V — векторное пространство.

1. *Линейной комбинацией* векторов $v_1, \ldots, v_r \in V$ называется вектор

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_r v_r, \quad \lambda_1, \lambda_2, \ldots, \lambda_r \in \mathbb{R}.$$

2. Векторы $v_1, \ldots, v_r$ называются *линейно зависимыми*, если существуют такие числа $\lambda_1, \lambda_2, \ldots, \lambda_r$, хотя бы одно из которых не равно нулю, что

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_r v_r = 0.$$

В противном случае векторы называются *линейно независимыми*.

3. Система векторов $e_1, \ldots, e_n$ называется (конечным) *базисом* пространства V, если любой вектор $v \in V$ является их линейной комбинацией, причём представление
$$v = \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n$$
единственно[1]. В этом случае пространство называется *конечномерным*. Числа λ_i называются *координатами* вектора в данном базисе.

Теорема 1. *Если $e_1, \ldots, e_n$ и $e'_1, \ldots, e'_{n'}$ — два базиса пространства V, то $n = n'$.*

Таким образом, если пространство конечномерно, то количество векторов во всех базисах этого пространства одинаково.

Определение 12. Количество векторов в базисе данного конечномерного пространства V называется *размерностью* этого пространства и обозначается через $\dim V$.

Пример 7. Векторы
$$\begin{aligned}
\varepsilon_1 &= (1, 0, \ldots, 0),\\
\varepsilon_2 &= (0, 1, \ldots, 0),\\
&\ldots\ldots\ldots\ldots\\
\varepsilon_n &= (0, 0, \ldots, 1)
\end{aligned}$$
образуют базис пространства $\mathbb{R}^n$. Значит, оно n-мерно.

Предложение 8. *Если $V' \subset V$ — подпространство, то $\dim V' \leqslant \dim V$ и равенство достигается в том и только том случае, когда $V' = V$.*

Предложение 9. *Пусть V и W — конечномерные векторные пространства и $e_1, \ldots, e_n$ — базис пространства V. Тогда для любого набора векторов $w_1, \ldots, w_n \in W$ существует и единственным образом определён такой линейный оператор $A\colon V \to W$, что*
$$A(e_i) = w_i, \quad i = 1, \ldots, n.$$

Следствие 2. *Если $\dim V = n$, $\dim W = m$, то $\dim \operatorname{Lin}(V, W) = mn$.*

Определение 13. Пусть $v_1, \ldots, v_r \in V$. Множество
$$\mathcal{L}(v_1, \ldots, v_r) = \{\, v = \sum_{i=1}^{r} \lambda_i v_i \mid \lambda_i \in \mathbb{R} \,\},$$
образованное всевозможными линейными комбинациями векторов $v_1, \ldots, v_r$, называется их *линейной оболочкой*.

[1]Единственность означает, что из равенства $\lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n = \lambda'_1 e_1 + \lambda'_2 e_2 + \ldots + \lambda'_n e_n$ следуют равенства $\lambda_1 = \lambda'_1, \ldots, \lambda_n = \lambda'_n$.

Предложение 10. *Линейная оболочка является подпространством.*

Определение 14. *Рангом* системы векторов $v_1, \ldots, v_r \in V$ называется размерность её линейной оболочки этой системы. Ранг системы обозначается через $\operatorname{rank}(v_1, \ldots, v_r)$.

Таким образом, $\operatorname{rank}(v_1, \ldots, v_r) = \dim \mathcal{L}(v_1, \ldots, v_r)$.

Следствие 3. *Если* $v_1, \ldots, v_r \in V$, *то* $\operatorname{rank}(v_1, \ldots, v_r) \leqslant \dim V$.

§8. Матрицы и определители

Пусть V — конечномерное векторное пространство и $e_1, \ldots, e_n$ — его базис. Рассмотрим вектор $v = \lambda_1 e_1 + \ldots + \lambda_n e_n \in V$ и сопоставим ему элемент $\varphi(v) = (\lambda_1, \ldots, \lambda_n) \in \mathbb{R}^n$ n-мерного арифметического пространства.

Предложение 11. *Построенное отображение* $\varphi(v)$ *является изоморфизмом между* V *и* $\mathbb{R}^n$.

Следствие 4. *Все векторные пространства размерности* n *попарно изоморфны между собой и изоморфны* n-*мерному арифметическому пространству.*

Пусть V и W — векторные пространства размерности n и m соответственно и $e_1, \ldots, e_n \in V$, $f_1, \ldots, f_n \in W$ — их базисы. Если $A\colon V \to W$ — линейный оператор, то каждый вектор $A(e_i)$ единственным образом представляется в виде

$$A(e_i) = a_{i1} f_1 + a_{i2} f_2 + \cdots + a_{in} f_n, \quad i = 1, \ldots, n, \quad a_{ij} \in \mathbb{R}, \quad j = 1, \ldots, m. \tag{2}$$

Определение 15. Таблица

$$M = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}, \tag{3}$$

состоящая из m строк и n столбцов, называется *матрицей* (размера $m \times n$) оператора A, записанной в базисах $e_1, \ldots, e_n$ и $f_1, \ldots, f_n$. Если $m = n$, то матрица называется *квадратной.*

Пример 8. Оператору A_λ из примера 4 соответствует матрица

$$\begin{pmatrix} \lambda & 0 & \ldots & 0 \\ 0 & \lambda & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \lambda \end{pmatrix},$$

называемая *скалярной*. Если $\lambda = 1$, то эта матрица называется *единичной* и обозначается через E. Заметим также, что матрицы вида

$$\begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

называются *диагональными*.

Предложение 12. *При выбранных базисах пространств V и W каждый линейный оператор однозначно определяется своей матрицей. При этом, если $v = \lambda_1 e_1 + \ldots + \lambda_n e_n$, то*

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_m \end{pmatrix},$$

где

$$\mu_i = a_{i1}\lambda_1 + a_{i2}\lambda_2 + \ldots + a_{in}\lambda_n = \sum_{j=1}^{n} a_{ij}\lambda_j, \quad i = 1, \ldots, m. \tag{4}$$

Вектор $(\mu_1, \ldots, \mu_m) \in \mathbb{R}^m$, вычисляемый по формуле (4), называется результатом *действия* матрицы M на вектор $(\lambda_1, \ldots, \lambda_n) \in \mathbb{R}^n$.

Предложение 13. *Пусть $A, B\colon V \to W$ — линейные операторы и $M = (a_{ij})$, $N = (b_{ij})$ — матрицы, соответствующие этим операторам в некоторых выбранных базисах. Тогда их сумме соответствует матрица*

$$M + N = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{pmatrix},$$

которая называется суммой *матриц M и N, а оператору λA — матрица*

$$\lambda M = \begin{pmatrix} \lambda a_{11} & \lambda a_{12} & \dots & \lambda a_{1n} \\ \lambda a_{21} & \lambda a_{22} & \dots & \lambda a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda a_{m1} & \lambda a_{m2} & \dots & a\lambda_{mn} \end{pmatrix}$$

— результат умножения *матрицы M на число λ.*

Таким образом, множество матриц образует векторное пространство, обычно обозначаемое через $\mathrm{Mat}(m, n)$. Его размерность равна nm.

Сопоставим каждой матрице вида (3) матрицу

$$M^* = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix}. \tag{5}$$

Матрица M^* называется *транспонированной* к матрице M и имеет размерность $m \times n$. Таким образом, операция транспонирования матриц является отображением из пространства $\mathrm{Mat}(m,n)$ в пространство $\mathrm{Mat}(n,m)$.

Предложение 14. *Отображение транспонирования*

$$*\colon \mathrm{Mat}(n,m) \to \mathrm{Mat}(m,n)$$

является линейным, причём $* \circ * = \mathrm{id}$, *т.е.*

$$(M^*)^* = M$$

для любой матрицы M.

Если M — квадратная матрица и $M^* = M$, то эта матрица называется *симметрической.* Таким образом, симметрические матрицы характеризуются свойством

$$a_{ij} = a_{ji}$$

для любых $i, j = 1, \dots, n$.

Предложение 15. *Пусть* $A\colon U \to V$, $B\colon V \to W$ *— линейные операторы, где* U, V *и* W *— векторные пространства размерностей* n, m *и* k *соответственно. Тогда, если этим операторам соответствуют матрицы* $M = (a_{il})$ *и* $N = (b_{lj})$, *то их композиции соответствует матрица* $M \cdot N = (c_{ij})$ *размерности* $n \times k$, *где*

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{im}b_{mj} = \sum_{s=1}^{m} a_{is}b_{sj}, \quad i = 1, \dots, n, \quad j = 1, \dots, k.$$

Матрица $M \cdot N$ называется *произведением* (или *композицией*) матриц M и N. Если M и N — квадратные матрицы, то разность $[M, N] = M \cdot N - N \cdot M$ называется их *коммутатором.*

Преобразование матриц при замене базисов. Пусть $A\colon V \to W$ — некоторый линейный оператор и $M = (a_{ij})$ — его матрица, записанная в базисах $e_1, \dots, e_n$ и $f_1, \dots, f_m$ пространств V и W соответственно. Пусть $e'_1, \dots, e'_n$ и $f'_1, \dots, f'_m$ — другие базисы этих пространств. Тогда в этих базисах оператор A будет представлен матрицей $M' = (a'_{ij})$. С другой стороны, векторы старых базисов выражаются через новые:

$$e_i = b_{i1}e'_1 + \ldots + b_{in}e'_n, \ i = 1, \dots, n, \quad f_j = c_{j1}f'_1 + \ldots + c_{jm}f'_m, \ j = 1, \dots, m.$$

Пусть $F = (b_{il})$ и $G = (c_{lj})$ — соответствующие матрицы (размерности $n \times n$ и $m \times m$). Тогда

$$F \cdot M' = M \cdot G. \tag{6}$$

Если оператор A обратим и ему соответствует матрица M, то матрица, соответствующая оператору A^{-1}, называется *обратной* к матрице M и обозначается через M^{-1}. Таким образом, $M \cdot M^{-1} = M^{-1} \cdot M = E$. Наша задача — научиться определять, когда матрица обратима и вычислять обратную матрицу, если она существует.

Замечание. Матрицы перехода от векторов одного базиса к другому всегда обратимы. Поэтому равенство (6) можно переписать в виде $M' = F^{-1} \cdot M \cdot G$. В частности, если линейный оператор действует из пространства V в то же самое пространство, то

$$M' = F^{-1} \cdot M \cdot F. \tag{7}$$

Подстановки и перестановки.

Определение 16. *Подстановкой* длины n называется взаимно-однозначное отображение множества первых n натуральных чисел в себя. Множество перестановок длины n обозначается через Σ_n. Композиция таких отображений называется *композицией* подстановок.

Подстановку $\sigma \in \Sigma_n$ принято представлять таблицей

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & k & \ldots & n \\ i_1 & i_2 & \ldots & i_k & \ldots & i_n \end{pmatrix}, \quad 1 \leqslant i_k \leqslant n, \quad i_\alpha \neq i_\beta,$$

которая означает, что $\sigma(1) = i_1$, $\sigma(2) = i_2, \ldots, \sigma(n) = i_n$. Нижняя строчка этой таблицы называется *перестановкой*. Количество подстановок (и перестановок) длины n равно $n!$.

Замечание. Напомним, что величина $n!$ (читается «эн факториа́л») определяется как произведение всех натуральных чисел от 1 до n: $n! = 1 \cdot 2 \cdot \cdot \ldots \cdot (n-1) \cdot n$.

Пример 9. Существует шесть разных подстановок длины три:

$$\begin{gathered} \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \\ \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}. \end{gathered} \tag{8}$$

Простейшими подстановками являются *транспозиции* — подстановки, которые переставляют между собой два элемента, а остальные оставляют на месте:

$$\begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ 1 & 2 & \dots & j & \dots & i & \dots & n \end{pmatrix}.$$

Например, среди подстановок (8) транспозициями являются σ_2, σ_4 и σ_5.

Предложение 16. *Любую подстановку можно представить в виде композиции транспозиций. При любом таком разложении количество участвующих в нём транспозиций либо всегда чётно, либо всегда нечётно.*

Определение 17. Подстановка (и соответствующая перестановка) называется *чётной*, если её можно разложить в композицию чётного числа транспозиций. В противном случае она называется *нечётной*. Чётность подстановки σ обозначается через $|\sigma|$.

Так, в примере 9 подстановки σ_1, σ_3 и σ_6 — чётные, а σ_2, σ_4 и σ_5 — нечётные.

Определители и их свойства.

Определение 18. Пусть $M = (a_{ij})$ — матрица, $i, j = 1, \dots, n$. Её *определителем* (или *детерминантом*) называется выражение

$$\Delta_M = \sum_{\sigma \in \Sigma_n} (-1)^{|\sigma|} a_{1i_1} a_{2i_2} \dots a_{a_n i_n}. \tag{9}$$

Матрица M называется *невырожденной*, если её определитель отличен от нуля.

Для определителя используются также обозначения $|a_{ij}|$, ΔM, $|M|$ и $\det M$.

Предложение 17 (основные свойства определителей). *Пусть M — матрица и $\Delta = \Delta_M$ — её определитель. Тогда:*

1. *Определитель не изменится, если матрицу M заменить на* транспонированную $M^* = (a_{ji})$,
$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{vmatrix}.$$
2. *Определитель меняет знак, если поменять местами любые две его строки (столбца).*
3. *Определитель матрицы равен нулю, если элементы каких-нибудь двух строк (столбцов) пропорциональны. В частности, он равен нулю, если одна из строк (один из столбцов) состоит целиком из нулей.*
4. *Общий множитель всех элементов какой-нибудь строки (столбца) можно вынести за знак определителя.*

5. *Если все элементы какой-либо строки (столбца) являются суммой двух слагаемых, то и определитель является суммой соответствующих определителей, например,*

$$\begin{vmatrix} a_{11}+a'_{11} & a_{12}+a'_{12} & \dots & a_{1n}+a'_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a'_{11} & a'_{12} & \dots & {}'a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

6. *Определитель не изменится, если к элементам одной строки прибавить линейную комбинацию других строк.*
7. *Определитель* треугольной *матрицы равен произведению её диагональных элементов,*

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{vmatrix} = a_{11}a_{22}\dots a_{nn}.$$

8. *Определитель произведения двух квадратных матриц равен произведению их определителей,* $\Delta_{M\cdot N} = \Delta_M \Delta_N$.

Из последнего равенства и равенства (7) вытекает ещё один важный результат.

Следствие 5. *Пусть* $A\colon V \to V$ *— линейный оператор и* M *— его матрица в каком-нибудь базисе пространства* V. *Тогда определитель* Δ_M *не зависит от выбора базиса, а определяется самим оператором* A.

Определение 19. Пусть M— квадратная матрица и a_{ij} — её элемент. *Минором*, дополнительным к этому элементу, называется определитель матрицы, полученной из M вычёркиванием i-й строки и j-го столбца. Этот определитель обозначается через M_{ij}. Величина $A_{ij} = (-1)^{i+j}M_{ij}$ называется *алгебраическим дополнением* элемента a_{ij}.

Теорема 2 (о разложении по строке или столбцу). *Пусть* $M = (a_{ij})$ *— матрица размера* $n \times n$. *Тогда для любых* i *и* j *имеют место тождества*

$$\Delta_M = (-1)^{i+1}a_{i1}M_{i1} + (-1)^{i+2}a_{i2}M_{i2} + \dots + (-1)^{i+n}a_{in}M_{in} \tag{10}$$

и

$$\Delta_M = (-1)^{j+1}a_{1j}M_{1j} + (-1)^{j+2}a_{2j}M_{2j} + \dots + (-1)^{j+n}a_{nj}M_{nj}. \tag{11}$$

Равенство (10) называется *разложением определителя по i-й строке*, а равенство (11) — *разложением по j-му столбцу*.

Вычисление обратных матриц. Следствием теоремы 2 является другая важная теорема.

Теорема 3. *Квадратная матрица $M = (a_{ij})$ обратима тогда и только тогда, когда её определитель не равен нулю. При этом обратная матрица имеет вид*

$$M^{-1} = \frac{1}{\Delta_M} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix}, \tag{12}$$

где A_{ji} — алгебраические дополнения элементов a_{ij}.

§9. Системы линейных уравнений

Определение 20. Пусть V и W — векторные пространства размерности n и m соответственно и $w \in W$ — вектор. *Системой из m уравнений с n неизвестными*, наложенной на неизвестный вектор x, называется уравнение

$$Ax = w. \tag{13}$$

Вектор $v \in V$ называется *решением* системы (13), если $Av = w$. Вектор w называется *правой частью* системы. Система называется *однородной*, если $w = 0$. Система называется *невырожденной*, если $V = W$ и A — обратимый оператор.

Предложение 18. *Множество S решений однородной системы $Ax = 0$ является векторным подпространством пространства V. Если $x = v_0$ — некоторое решение системы $Ax = w$, то $x = v_0 + v$, $v \in S$, — также решение этой системы и любое её решение имеет такой вид.*

Если в пространствах V и W выбрать базисы и представить оператор A матрицей $M = (a_{ij})$, а вектор w — набором его координат $b_1, \dots, b_m$, то система (13) перепишется в виде

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m. \end{cases} \tag{14}$$

Решение невырожденных систем. Если (13) — невырожденная система, то она имеет единственное решение

$$x = A^{-1}(w). \tag{15}$$

Как практически найти вектор x?

Замечание. Если в невырожденной системе (13) (такие системы называются *однородными*) вектор w равен нулю, то её единственным решением является $x = 0$.

Метод обратной матрицы. В силу (15), решение имеет вид

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = M^{-1} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

Пользуясь теоремой 3, получаем

$$\begin{cases} x_1 = \frac{1}{\Delta}(M_{11}b_1 - M_{21}b_2 + \ldots + (-1)^{n+1}M_{n1}x_n), \\ x_2 = \frac{1}{\Delta}(-M_{12}b_1 + M_{22}b_2 - \ldots + (-1)^{n+2}M_{n2}x_n), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_i = \frac{1}{\Delta}((-1)^{i+1}M_{1i}b_1 + (-1)^{i+2}M_{2i}b_2 + \ldots + (-1)^{i+n}M_{ni}x_n), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = \frac{1}{\Delta}((-1)^{n+1}M_{1n}b_1 + (-1)^{n+2}M_{2n}b_2 - \ldots + M_{nn}x_n), \end{cases} \tag{16}$$

или

$$x_i = \sum_{j=1}^{n} (-1)^{i+j} M_{ji} b_j, \qquad j = 1, \ldots, n, \tag{17}$$

где M_{ji} — минор, дополнительный к элементу a_{ji}.

Правило Крамера. Рассмотрим определители

$$\Delta_i = \begin{vmatrix} a_{11} & \ldots & a_{1,i-1} & b_1 & a_{1,i+1} & \ldots & a_{1n} \\ a_{21} & \ldots & a_{2,i-1} & b_2 & a_{2,i+1} & \ldots & a_{2n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{n,i-1} & b_1 & a_{n,i+1} & \ldots & a_{nn} \end{vmatrix}, \quad i = 1, \ldots, n. \tag{18}$$

Тогда формулу (16) для решений системы можно переписать в виде

$$x_1 = \frac{\Delta_1}{\Delta}, \quad x_2 = \frac{\Delta_2}{\Delta}, \ldots, x_n = \frac{\Delta_n}{\Delta}. \tag{19}$$

Нахождение решений по формуле (19) называется *правилом Крамера*. Правилом Крамера можно пользоваться, если определитель решаемой системы отличен от нуля.

Метод Гаусса. Поскольку M — невырожденная матрица, хотя бы одно из чисел $a_{11}, \ldots, a_{n1}$ отлично от нуля. Без ограничения общности можно считать, что $a_{11} \neq 0$ (если это не так, строки системы переставить так, чтобы отличный от нуля коэффициент a_{ni} стал первым). Разделив первую строку на a_{11} и вычитая из i-й строки первую, умноженную на a_{i1}, мы придём к системе

$$\begin{cases} x_1 + a'_{12}x_2 + a'_{13}x_3 + \ldots + a'_{1n}x_n = b'_1, \\ \qquad a'_{22}x_2 + a'_{23}x_3 + \ldots + a'_{2n}x_n = b'_2, \\ \qquad a'_{32}x_2 + a'_{33}x_3 + \ldots + a'_{3n}x_n = b'_3, \\ \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \qquad a'_{n2}x_2 + a'_{n3}x_3 + \ldots + a'_{nn}x_n = b'_n. \end{cases}$$

Система уравнений

$$\begin{cases} a'_{22}x_2 + a'_{23}x_3 + \ldots + a'_{2n}x_n = b'_2, \\ a'_{32}x_2 + a'_{33}x_3 + \ldots + a'_{3n}x_n = b'_3, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a'_{n2}x_2 + a'_{n3}x_3 + \ldots + a'_{nn}x_n = b'_n \end{cases}$$

также является невырожденной, и с ней можно проделать ту же процедуру, что и с исходной, и т.д. В итоге мы придём к системе уравнений

$$\begin{cases} x_1 + a'_{12}x_2 + a'_{13}x_3 + \ldots + a'_{1n}x_n = b'_1, \\ \qquad\quad x_2 + a'_{23}x_3 + \ldots + a'_{2n}x_n = b'_2, \\ \qquad\qquad\qquad x_3 + \ldots + a'_{3n}x_n = b'_3, \\ \qquad\qquad\qquad \ldots\ldots\ldots\ldots \\ \qquad\qquad\qquad\qquad\qquad x_n = b'_n. \end{cases} \tag{20}$$

Это завершает *первый этап* решения по методу Гаусса.

Второй этап состоит из следующих шагов. Последнее уравнение системы (20) даёт значение неизвестной x_n. Подставляя x_n в предпоследнее уравнение, находим x_{n-1} и т.д. В итоге мы найдём значения всех неизвестных $x_1, \ldots, x_n$.

Метод Гаусса называется также *методом последовательного исключения неизвестных.*

Решение произвольных систем. Пусть $N = (c_{ij})$ — произвольная матрица, $i = 1, \ldots, k$, $j = 1, \ldots, l$.

Предложение 19. *Ранг системы векторов*

$$c_1 = (c_{11}, c_{12}, \ldots, c_{1l}),$$

$$\begin{aligned} c_2 &= (c_{21}, c_{22}, \ldots, c_{2l}),\\ &\ldots\ldots\ldots\ldots\\ c_k &= (c_{k1}, c_{k2}, \ldots, c_{kl}) \end{aligned}$$

совпадает с рангом системы векторов

$$\begin{aligned} c_1^* &= (c_{11}, c_{21}, \ldots, c_{k1}),\\ c_2^* &= (c_{12}, c_{22}, \ldots, c_{k2}),\\ &\ldots\ldots\ldots\ldots\\ c_l^* &= (c_{1l}, c_{2l}, \ldots, c_{kl}). \end{aligned}$$

Определение 21. *Рангом* матрицы N называется ранг системы векторов, составленной из её строк или столбцов. Ранг матрицы обозначается через $\operatorname{rank} N$.

Определение 22. Пусть

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

— система линейных уравнений. Матрица

$$\tilde{M} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} & b_1\\ a_{21} & a_{22} & \ldots & a_{2n} & b_2\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{pmatrix}$$

называется *расширенной матрицей* этой системы.

Теорема 4 (теорема Кронекера–Капелли). *Система* (21) *имеет решение тогда и только тогда, когда ранг r её матрицы $M = (a_{ij})$ совпадает с рангом её расширенной матрицы $\tilde{M}$. При этом решение системы зависит от произвольных $n-r$ параметров. В частности, система имеет единственное решение, если $n = r$.*

Собственные значения и собственные векторы. Пусть $A\colon V \to V$ — линейный оператор и M — его матричная запись в некотором базисе пространства V. Как, пользуясь матрицей M, найти собственные значения и собственные векторы оператора A?

Пусть $v \neq 0$ — собственный вектор, соответствующий собственному значению λ, и $x_1, \ldots, x_n$ — его координаты, а a_{ij} — элементы матрицы M. Тогда из определения 10 следует, что должны выполняться равенства

$$\begin{aligned} &a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = \lambda x_1, \\ &a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = \lambda x_2, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = \lambda x_n, \end{aligned}$$

или

$$\begin{aligned} &(a_{11} - \lambda)x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0, \\ &a_{21}x_1 + (a_{22} - \lambda)x_2 + \ldots + a_{2n}x_n = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &a_{n1}x_1 + a_{n2}x_2 + \ldots + (a_{nn} - \lambda)x_n = 0. \end{aligned}$$

Иными словами, однородная система линейных уравнений

$$(M - \lambda E)v = 0 \tag{22}$$

должна иметь ненулевое решение. В силу замечания на с. 46 это возможно тогда и только тогда, когда определитель матрицы системы (22) равен нулю:

$$|M - \lambda E| = 0. \tag{23}$$

Очевидно, выражение, стоящее в левой части уравнения (23), является полиномом степени n относительно λ, т.е. имеет вид

$$|M - \lambda E| = d_0 + d_1\lambda + d_2\lambda^2 + \cdots + d_n\lambda^n.$$

При этом, очевидно, $d_n = (-1)^n$, а коэффициент d_0 совпадает с определителем матрицы M.

Определение 23. Полином $\chi_M(\lambda) = |M - \lambda E|$ называется *характеристическим полиномом* (или *многочленом*) матрицы M.

Таким образом, действительное число λ является собственным значением матрицы M тогда и только тогда, когда оно есть корень её характеристического полинома $\chi_M(\lambda)$. Чтобы найти соответствующий собственный вектор, нужно решить систему уравнений (22) относительно v при данном значении λ.

Пример 10. Характеристический полином матрицы

$$M = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

имеет вид

$$\chi_M(\lambda) = \begin{vmatrix} a_{11}-\lambda & a_{12} \\ a_{21} & a_{22}-\lambda \end{vmatrix} = (a_{11}-\lambda)(a_{22}-\lambda) - a_{12}a_{21} =$$
$$= \lambda^2 - (a_{11}+a_{22}) + a_{11}a_{22} - a_{12}a_{21}.$$

Таким образом, чтобы найти собственные значения этой матрицы, нужно решить квадратное уравнение

$$\lambda^2 - (a_{11}+a_{22})\lambda + a_{11}a_{22} - a_{12}a_{21} = 0. \tag{24}$$

Дискриминант этого уравнения равен $(a_{11}-a_{22})^2 + 4a_{12}a_{21}$, и поэтому матрица M имеет собственные решения тогда и только тогда, когда

$$(a_{11}-a_{22})^2 + 4a_{12}a_{21} \geqslant 0. \tag{25}$$

Пример 11. В случае матрицы размера 3×3 характеристический полином имеет вид

$$\chi_M(\lambda) = d_0 - d_1\lambda + d_2\lambda^2 - \lambda^3,$$

где $d_0 = \Delta_M$ (как и для любой матрицы),

$$d_1 = \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix},$$

т.е. совпадает с суммой миноров, дополнительных к диагональным элементам, и, наконец,

$$d_2 = \operatorname{tr} M = a_{11} + a_{22} + a_{33}.$$

Пример 12. Важным для дальнейшего частным случаем примера 10 являются собственные значения *симметрических* 2×2-матриц, т.е. матриц вида

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}.$$

В этом случае неравенство (25) имеет вид

$$(a_{11}-a_{22})^2 + 4a_{12}^2 \geqslant 0$$

и, значит, выполняется всегда. Заметим, что равенство возможно тогда и только тогда, когда

$$a_{11} = a_{22}, \quad a_{12} = 0,$$

т.е. когда M — скалярная матрица, а если неравенство строгое, то существуют два различных собственных значения. Обозначим их через λ_1 и λ_2, и пусть v_1, v_2 — соответствующие им собственные векторы. Рассмотрим такие числа μ_1 и μ_2, что

$$\mu_1 v_1 + \mu_2 v_2 = 0. \tag{26}$$

Применяя к этому равенству матрицу M, получаем

$$\mu_1\lambda_2 v_1 + \mu_2\lambda_2 v_2 = 0. \tag{27}$$

Умножая равенство (26) на λ_1 и вычитая из (27), получаем

$$(\lambda_2 - \lambda_1)\mu_2 v_2 = 0.$$

Аналогично, умножая на λ_2, получим

$$(\lambda_1 - \lambda_2)\mu_1 v_1 = 0.$$

Поскольку $\lambda_1 \neq \lambda_2$, а векторы v_1 и v_2 — ненулевые, из этого следует, что $\mu_1 = \mu_2 = 0$, т.е. v_1 и v_2 — линейно независимы. Значит, их можно выбрать в качестве нового базиса. В этом базисе рассматриваемая матрица будет иметь вид

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}.$$

Итак, мы доказали следующий результат:

Теорема 5. *Для любой симметрической матрицы 2×2 существует базис, состоящий из собственных векторов. В этом базисе матрица принимает диагональный вид, причём на диагонали стоят её собственные значения.*

§10. Плоскость и трёхмерное пространство

Точкой n-мерного арифметического пространства $\mathbb{R}^n$ называется набор чисел $A = (a_1, \ldots, a_n)$, которые называются *координатами* этой точки. Упорядоченная пара точек $\overline{AB}$ называется *направленным отрезком*, соединяющим точки A и B. При этом A называется *началом* этого отрезка, а B его *концом*. Говорят также, что отрезок $\overline{AB}$ *приложен* к точке A. Отрезок $\overline{OA}$, где $O = (0, \ldots, 0)$ — начало координат, называется *радиус-вектором* точки A.

Каждому направленному отрезку $\overline{AB}$ соответствует вектор $v_{AB} = (b_1 - a_1, \ldots, b_n - a_n)$. Точки $A_0, \ldots, A_k$ (или их радиус-векторы) называются *коллинеарными*, если ранг системы векторов $v_{A_0A_1}, \ldots, v_{A_0A_k}$ равен 1, и *компланарными*, если её ранг равен 2.

Скалярным произведением векторов $v = (v_1, \ldots, v_n)$ и $w = (w_1, \ldots, w_n)$ называется величина

$$(v, w) = v_1 w_1 + v_2 w_2 + \ldots + v_n w_n. \tag{28}$$

Величина

$$\|v\| = \sqrt{(v, v)} = \sqrt{v_1^2 + v_2^2 + \ldots + v_n^2} \tag{29}$$

называется *длиной* вектора v.

Базис $e_1, \ldots, e_n$ пространства $\mathbb{R}^n$ называется *ортонормированным*, если

$$(e_i, e_j) = \begin{cases} 1, & \text{при } i = j, \\ 0, & \text{при } i \neq j. \end{cases}$$

В частности, стандартный базис, описанный в примере 7, является ортонормированным. Ортонормированные базисы называют также реперами, а их элементы — ортами.

Случай $n = 2$ (плоскость). На плоскости $\mathbb{R}^2$ координаты точек и векторов иногда принято обозначать через x (абсцисса) и y (ордината). Если $A_0(x_0, y_0)$ и $A_1(x_1, y_1)$ — точки, то величина

$$\|v_{A_0A_1}\| = \sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2} \tag{30}$$

совпадает с *длиной отрезка* A_0A_1. Если $A_2(x_2, y_2)$ — третья точка, то скалярное произведение между векторами $v_{A_0A_1}$ и $v_{A_0A_2}$ вычисляется по формуле

$$(v_{A_0A_1}, v_{A_0A_2}) = (x_1 - x_0)(x_2 - x_0) + (y_1 - y_0)(y_2 - y_0). \tag{31}$$

С помощью скалярного произведения можно вычислить *угол* между векторами:

$$\begin{aligned} \cos\alpha = \frac{(v_{A_0A_1}, v_{A_0A_2})}{\|v_{A_0A_1}\| \cdot \|v_{A_0A_2}\|} &= \\ &= \frac{(x_1 - x_0)(x_2 - x_0) + (y_1 - y_0)(y_2 - y_0)}{\sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2} \cdot \sqrt{(x_2 - x_0)^2 + (y_2 - y_0)^2}}, \end{aligned} \tag{32}$$

где α — угол $A_1A_0A_2$. Если через $S_{A_0A_1A_2}$ обозначить *площадь треугольника* $A_0A_1A_2$, то имеет место равенство

$$S_{A_0A_1A_2} = \frac{1}{2}\big|(x_1 - x_0)(y_2 - y_0) - (x_2 - x_0)(y_1 - y_0)\big|. \tag{33}$$

Пусть заданы две несовпадающие точки $A_1(x_1, y_1)$ и $A_2(x_2, y_2)$ и $A(x, y)$ — произвольная точка плоскости. Эта точка лежит на прямой A_1A_2 тогда и только тогда, когда точки A, A_1 и A_2 коллинеарны. Условие коллинеарности записывается в виде

$$\begin{vmatrix} x - x_1 & y - y_1 \\ x_2 - x_1 & y_2 - y_1 \end{vmatrix} = 0,$$

или

$$\frac{x - x_1}{x_2 - x_1} = \frac{y - y_1}{y_2 - y_1}. \tag{34}$$

Таким образом, уравнение (34) — это *уравнение прямой, проходящей через точки* $A_1(x_1, y_1)$ и $A_2(x_2, y_2)$.

Замечание. Если $x_1 = x_2$, то уравнением прямой, проходящей через точки A_1 и A_2, является $x = x_1$, а если $y_1 = y_2$, то $y = y_1$. Равенства $x_1 = x_2$ и $y_1 = y_2$ не могут выполняться одновременно, поскольку A_1 и A_2 — разные точки.

Уравнение прямой на плоскости можно также задать в виде

$$ax + by + c = 0, \tag{35}$$

где числа a и b одновременно не обращаются в нуль. При этом вектор $v = (a, b)$ *ортогонален* этой прямой, и поэтому уравнение прямой, *перпендикулярной* прямой (35) и проходящей через точку $A_1(x_1, y_1)$, имеет вид

$$\frac{x - x_1}{a} = \frac{y - y_1}{b}. \tag{36}$$

Вводя новую переменную $t \in \mathbb{R}$, уравнение (36) можно переписать в виде

$$x = at + x_1, \quad y = bt + y_1, \quad t \in \mathbb{R}. \tag{37}$$

Эти уравнения называются *параметрическими уравнениями прямой*, а переменная t — *параметром*. Вектор $v = (a, b)$ называется *направляющим вектором* прямой, задаваемой уравнением (37).

Случай $n = 3$ (трёхмерное пространство). В трёхмерном пространстве координаты точек и векторов иногда принято обозначать через x (абсцисса), y (ордината) и z (аппликата). Если $A_0(x_0, y_0, z_0)$ и $A_1(x_1, y_1, z_1)$ — точки, то величина

$$\|v_{A_0A_1}\| = \sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2 + (z_1 - z_0)^2} \tag{38}$$

совпадает с *длиной отрезка* A_0A_1. Если $A_2(x_2, y_2, z_2)$ — третья точка, то скалярное произведение между векторами $v_{A_0A_1}$ и $v_{A_0A_2}$ вычисляется по формуле

$$(v_{A_0A_1}, v_{A_0A_2}) = (x_1 - x_0)(x_2 - x_0) + (y_1 - y_0)(y_2 - y_0) + (z_1 - z_0)(z_2 - z_0). \tag{39}$$

Как и в случае плоскости, имеет место равенство

$$\cos\alpha = \frac{(v_{A_0A_1}, v_{A_0A_2})}{\|v_{A_0A_1}\| \cdot \|v_{A_0A_2}\|} =$$
$$= \frac{(x_1 - x_0)(x_2 - x_0) + (y_1 - y_0)(y_2 - y_0) + (z_1 - z_0)(z_2 - z_0)}{\sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2 + (z_1 - z_0)^2} \cdot \sqrt{(x_2 - x_0)^2 + (y_2 - y_0)^2 + (z_2 - z_0)^2}}, \tag{40}$$

где α — угол $A_1A_0A_2$.

Обозначим через $\mathbf{i} = (1,0,0)$, $\mathbf{j} = (0,1,0)$ и $\mathbf{k} = (0,0,1)$ стандартные базисные векторы трёхмерного пространства. Вектор

$$v_{A_0A_1} \times v_{A_0A_2} = \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ x_1 - x_0 & y_1 - y_0 & z_1 - z_0 \\ x_2 - x_0 & y_2 - y_0 & z_2 - z_0 \end{vmatrix} \tag{41}$$

называется *векторным произведением*[2]. Длина этого вектора есть *удвоенная площадь треугольника* $A_0A_1A_2$. Таким образом,

$$S_{A_0A_1A_2} = \frac{1}{2}\sqrt{\begin{vmatrix} y_1 - y_0 & z_1 - z_0 \\ y_2 - y_0 & z_2 - z_0 \end{vmatrix}^2 + \begin{vmatrix} x_1 - x_0 & z_1 - z_0 \\ x_2 - x_0 & z_2 - z_0 \end{vmatrix}^2 + \begin{vmatrix} x_1 - x_0 & y_1 - y_0 \\ x_2 - x_0 & y_2 - y_0 \end{vmatrix}^2}. \tag{42}$$

Пусть $A_3(x_3, y_3, z_3)$ — ещё одна точка пространства. Величина

$$(v_{A_0A_1} \times v_{A_0A_2}, v_{A_0A_2}) \tag{43}$$

называется *смешанным произведением* векторов $v_{A_0A_1}$, $v_{A_0A_2}$ и $v_{A_0A_3}$. Оно следующим образом связано с объёмом пирамиды $A_0A_1A_2A_3$:

$$V_{A_0A_1A_2A_3} = \frac{1}{6}\left|(v_{A_0A_1} \times v_{A_0A_2}, v_{A_0A_2})\right| = \frac{1}{6}\left|\det\begin{pmatrix} x_1 - x_0 & y_1 - y_0 & z_1 - z_0 \\ x_2 - x_0 & y_2 - y_0 & z_2 - z_0 \\ x_3 - x_0 & y_3 - y_0 & z_3 - z_0 \end{pmatrix}\right|. \tag{44}$$

Пусть $A(x, y, z)$ — произвольная точка плоскости. Эта точка лежит на прямой A_1A_2 тогда и только тогда, когда точки A, A_1 и A_2 коллинеарны. Условие коллинеарности записывается в виде

$$\operatorname{rank}\begin{pmatrix} x - x_1 & y - y_1 & z - z_1 \\ x_2 - x_1 & y_2 - y_1 & z_2 - z_1 \end{pmatrix} = 1. \tag{45}$$

Значит,

$$\frac{x - x_1}{x_2 - x_1} = \frac{y - y_1}{y_2 - y_1} = \frac{z - z_1}{z_2 - z_1} \tag{46}$$

— уравнение прямой, проходящей через точки A_1 и A_2 (см. также замечание на с. 53).

Точка A лежит в плоскости $A_1A_2A_3$ тогда и только тогда, когда точки A, A_1, A_2 и A_3 компланарны. Условие компланарности записывается в виде

$$\operatorname{rank}\begin{pmatrix} x - x_1 & y - y_1 & z - z_1 \\ x_2 - x_1 & y_2 - y_1 & z_2 - z_1 \\ x_3 - x_1 & y_3 - y_1 & z_3 - z_1 \end{pmatrix} = 2 \Leftrightarrow \begin{vmatrix} x - x_1 & y - y_1 & z - z_1 \\ x_2 - x_1 & y_2 - y_1 & z_2 - z_1 \\ x_3 - x_1 & y_3 - y_1 & z_3 - z_1 \end{vmatrix} = 0. \tag{47}$$

[2] Определитель в правой части равенства (41) является сокращённым обозначением вектора, получаемого разложением по первой строке: $\begin{vmatrix} y_1-y_0 & z_1-z_0 \\ y_2-y_0 & z_2-z_0 \end{vmatrix} \cdot \mathbf{i} - \begin{vmatrix} x_1-x_0 & z_1-z_0 \\ x_2-x_0 & z_2-z_0 \end{vmatrix} \cdot \mathbf{j} + \begin{vmatrix} x_1-x_0 & y_1-y_0 \\ x_2-x_0 & y_2-y_0 \end{vmatrix} \cdot \mathbf{k}$. Такие обозначения часто используются в математике и, в особенности, в физике.

Значит, уравнение плоскости, проходящей через точки A_1, A_2 и A_3, имеет вид

$$\begin{vmatrix} y_2 - y_1 & z_2 - z_1 \\ y_3 - y_1 & z_3 - z_1 \end{vmatrix} (x - x_1) - \begin{vmatrix} x_2 - x_1 & z_2 - z_1 \\ x_3 - x_1 & z_3 - z_1 \end{vmatrix} (y - y_1) + \\ + \begin{vmatrix} x_2 - x_1 & y_2 - y_1 \\ x_3 - x_1 & y_3 - y_1 \end{vmatrix} (z - z_1) = 0. \quad (48)$$

Уравнения произвольной прямой в пространстве можно также записать в виде

$$\frac{x - \alpha_1}{\alpha} = \frac{y - \beta_1}{\beta} = \frac{z - \gamma_1}{\gamma}, \tag{49}$$

а плоскости — в виде

$$ax + by + cz + d = 0, \tag{50}$$

где $v = (\alpha, \beta, \gamma) \neq 0$ —*направляющий вектор прямой*, а $n = (a, b, c) \neq 0$ — *вектор нормали к плоскости.* Поэтому уравнение плоскости, проходящей через точку (x_1, y_1, z_1) и перпендикулярной к прямой (49), имеет вид

$$\alpha(x - x_1) + \beta(y - y_1) + \gamma(z - z_1) = 0, \tag{51}$$

а прямой, проходящей через эту точку и перпендикулярной плоскости (50) — вид

$$\frac{x - x_1}{a} = \frac{y - y_1}{b} = \frac{z - z_1}{c}. \tag{52}$$

Как и в случае прямой на плоскости, уравнения (52) можно переписать в *параметрической форме*:

$$x = at + x_1, \quad y = bt + y_1, \quad z = ct + z_1, \qquad t \in \mathbb{R}, \tag{53}$$

где t — параметр.

§11. Образцы решения задач

Задача 1. Вычислить результат действия матрицы $A = \begin{pmatrix} 1 & 2 & 1 & 0 & 1 \\ 2 & 1 & 3 & 1 & 0 \\ 2 & 2 & 1 & 1 & 3 \end{pmatrix}$ на вектор $v = (3, -1, 2, 1, 0)$.

Решение. Пусть $w = Av$ и $w = (w_1, w_2, w_3)$. Тогда

$$w_1 = \sum_{i=1}^{5} a_{1i} v_i = 1 \cdot 3 + 2 \cdot (-1) + 1 \cdot 2 + 0 \cdot 1 + 1 \cdot 0 = \\ = 3 - 2 + 2 + 0 + 0 = 3,$$

$$w_2 = \sum_{i=1}^{5} a_{2i} v_i = 2 \cdot 3 + 1 \cdot (-1) + 3 \cdot 2 + 1 \cdot 1 + 0 \cdot 0 =$$

$$= 6 - 1 + 6 + 1 + 0 = 12,$$

$$w_3 = \sum_{i=1}^{5} a_{3i}v_i = 2 \cdot 3 + 2 \cdot (-1) + 1 \cdot 2 + 1 \cdot 1 + 3 \cdot 0 =$$

$$= 6 - 2 + 2 + 1 + 0 = 7.$$

■

Ответ: $w = (3, 12, 7)$.

Задача 2. Вычислить произведение и коммутатор матриц $A = \left(\begin{smallmatrix} 2 & 2 & 1 \\ 2 & 3 & 0 \\ 1 & 3 & 1 \end{smallmatrix}\right)$ и $B = \left(\begin{smallmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 3 \end{smallmatrix}\right)$.

Решение. Имеем

$$A \circ B = \begin{pmatrix} 2 & 2 & 1 \\ 2 & 3 & 0 \\ 1 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 3 \end{pmatrix} =$$

$$= \begin{pmatrix} 2 \cdot 1 + 2 \cdot 0 + 1 \cdot 1 & 2 \cdot 2 + 2 \cdot 1 + 1 \cdot 1 & 2 \cdot 1 + 2 \cdot 1 + 1 \cdot 3 \\ 2 \cdot 1 + 3 \cdot 0 + 0 \cdot 1 & 2 \cdot 2 + 3 \cdot 1 + 0 \cdot 1 & 2 \cdot 1 + 3 \cdot 1 + 0 \cdot 3 \\ 1 \cdot 1 + 3 \cdot 0 + 1 \cdot 1 & 1 \cdot 2 + 3 \cdot 1 + 1 \cdot 1 & 1 \cdot 1 + 3 \cdot 1 + 1 \cdot 3 \end{pmatrix} =$$

$$= \begin{pmatrix} 2+0+1 & 4+2+1 & 2+2+3 \\ 2+3+0 & 4+3+0 & 2+3+0 \\ 1+0+1 & 2+3+1 & 1+3+3 \end{pmatrix} = \begin{pmatrix} 3 & 7 & 7 \\ 5 & 7 & 5 \\ 2 & 6 & 7 \end{pmatrix}.$$

Аналогично,

$$B \circ A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 2 & 2 & 1 \\ 2 & 3 & 0 \\ 1 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 11 & 2 \\ 3 & 6 & 1 \\ 7 & 14 & 4 \end{pmatrix}.$$

Поэтому

$$[A, B] = A \circ B - B \circ A = \begin{pmatrix} 3 & 7 & 7 \\ 5 & 7 & 5 \\ 2 & 6 & 7 \end{pmatrix} - \begin{pmatrix} 7 & 11 & 2 \\ 3 & 6 & 1 \\ 7 & 14 & 4 \end{pmatrix} =$$

$$= \begin{pmatrix} 3-7 & 7-11 & 7-2 \\ 5-3 & 7-6 & 5-1 \\ 2-7 & 6-14 & 7-4 \end{pmatrix} = \begin{pmatrix} -4 & -4 & 5 \\ 2 & 1 & 4 \\ -5 & -8 & 3 \end{pmatrix}.$$

■

Ответ: $A \circ B = \left(\begin{smallmatrix} 3 & 7 & 7 \\ 5 & 7 & 5 \\ 2 & 6 & 7 \end{smallmatrix}\right)$, $[A, B] = \left(\begin{smallmatrix} -4 & -4 & 5 \\ 2 & 1 & 4 \\ -5 & -8 & 3 \end{smallmatrix}\right)$.

Задача 3. Вычислить определители матриц $A = \left(\begin{smallmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 0 & 1 & 1 \end{smallmatrix}\right)$ и $B = \left(\begin{smallmatrix} 1 & 2 & 3 & 1 \\ 2 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 2 & 2 & 1 & 1 \end{smallmatrix}\right)$.

Решение. Разложим первый определитель по первому столбцу:

$$|A| = \begin{vmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 0 & 1 & 1 \end{vmatrix} = 1 \cdot \begin{vmatrix} 1 & 3 \\ 1 & 1 \end{vmatrix} - 1 \cdot \begin{vmatrix} 2 & 1 \\ 1 & 1 \end{vmatrix} + 0 \cdot \begin{vmatrix} 2 & 1 \\ 1 & 3 \end{vmatrix} =$$

$$= (1 \cdot 1 - 3 \cdot 1) - (2 \cdot 1 - 1 \cdot 1) = -3.$$

Второй определитель удобно разложить по третьей строке:

$$|B| = \begin{vmatrix} 1 & 2 & 3 & 1 \\ 2 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 2 & 2 & 1 & 1 \end{vmatrix} = 1 \cdot \begin{vmatrix} 2 & 3 & 1 \\ 0 & 1 & 1 \\ 2 & 1 & 1 \end{vmatrix} - 0 \cdot \begin{vmatrix} 1 & 3 & 1 \\ 2 & 1 & 1 \\ 2 & 1 & 1 \end{vmatrix} + 0 \cdot \begin{vmatrix} 1 & 2 & 1 \\ 2 & 0 & 1 \\ 2 & 2 & 1 \end{vmatrix} - 1 \cdot \begin{vmatrix} 1 & 2 & 3 \\ 2 & 0 & 1 \\ 2 & 2 & 1 \end{vmatrix} =$$

$$= \left(2 \cdot \begin{vmatrix} 1 & 1 \\ 1 & 1 \end{vmatrix} + 2 \cdot \begin{vmatrix} 3 & 1 \\ 2 & 1 \end{vmatrix} \right) - \left(-2 \cdot \begin{vmatrix} 2 & 3 \\ 2 & 1 \end{vmatrix} - 1 \cdot \begin{vmatrix} 1 & 2 \\ 2 & 2 \end{vmatrix} \right) = -8.$$

■

Ответ: $|A| = -3$, $|B| = -8$.

ЗАДАЧА 4. Найти матрицу, обратную к матрице $A = \left(\begin{smallmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 0 & 1 & 1 \end{smallmatrix}\right)$.

Решение. Матрица, составленная из миноров, дополнительных к элементам матрицы A, имеет вид

$$M = \begin{pmatrix} \begin{vmatrix} 1 & 3 \\ 1 & 1 \end{vmatrix} & \begin{vmatrix} 1 & 3 \\ 0 & 1 \end{vmatrix} & \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} \\ \begin{vmatrix} 2 & 1 \\ 1 & 1 \end{vmatrix} & \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} & \begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix} \\ \begin{vmatrix} 2 & 1 \\ 1 & 3 \end{vmatrix} & \begin{vmatrix} 1 & 1 \\ 1 & 3 \end{vmatrix} & \begin{vmatrix} 1 & 2 \\ 1 & 1 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} -2 & 1 & 1 \\ 1 & 1 & 1 \\ 5 & 2 & -1 \end{pmatrix}.$$

Тогда

$$\bar{M} = \begin{pmatrix} -2 \cdot (-1)^{1+1} & 1 \cdot (-1)^{1+2} & 1 \cdot (-1)^{1+3} \\ 1 \cdot (-1)^{2+1} & 1 \cdot (-1)^{2+2} & 1 \cdot (-1)^{2+3} \\ 5 \cdot (-1)^{3+1} & 2 \cdot (-1)^{3+2} & -1 \cdot (-1)^{3+3} \end{pmatrix} = \begin{pmatrix} -2 & -1 & 1 \\ -1 & 1 & -1 \\ 5 & -2 & -1 \end{pmatrix}$$

— матрица, составленная из алгебраических дополнений, а

$$\bar{M}^* = \begin{pmatrix} -2 & -1 & 5 \\ -1 & 1 & -2 \\ 1 & -1 & -1 \end{pmatrix}$$

— транспонированная к ней. Поскольку определитель матрицы A равен -3 (задача 3), обратная матрица имеет вид

$$A^{-1} = \frac{1}{|A|}\bar{M}^* = \begin{pmatrix} \frac{2}{3} & \frac{1}{3} & -\frac{5}{3} \\ \frac{1}{3} & -\frac{1}{3} & \frac{2}{3} \\ -\frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}.$$

Сделаем проверку:

$$A \circ A^{-1} = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 0 & 1 & 1 \end{pmatrix} \circ \begin{pmatrix} \frac{2}{3} & \frac{1}{3} & -\frac{5}{3} \\ \frac{1}{3} & -\frac{1}{3} & \frac{2}{3} \\ -\frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

и

$$A^{-1} \circ A = \begin{pmatrix} \frac{2}{3} & \frac{1}{3} & -\frac{5}{3} \\ \frac{1}{3} & -\frac{1}{3} & \frac{2}{3} \\ -\frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Значит, обратная матрица вычислена правильно. ■

Ответ: $A^{-1} = \begin{pmatrix} \frac{2}{3} & \frac{1}{3} & -\frac{5}{3} \\ \frac{1}{3} & -\frac{1}{3} & \frac{2}{3} \\ -\frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$.

Задача 5. Решить систему уравнений

$$\begin{cases} x_1 + 2x_2 + x_3 = 8, \\ x_1 + x_2 + 3x_3 = 12, \\ x_2 + x_3 = 5 \end{cases}$$

методом Крамера.

Решение. Имеем

$$\Delta_1 = \begin{vmatrix} 8 & 2 & 1 \\ 12 & 1 & 3 \\ 5 & 1 & 1 \end{vmatrix} = -3, \quad \Delta_2 = \begin{vmatrix} 1 & 8 & 1 \\ 1 & 12 & 3 \\ 0 & 5 & 1 \end{vmatrix} = -6, \quad \Delta_3 = \begin{vmatrix} 1 & 2 & 8 \\ 1 & 1 & 12 \\ 0 & 1 & 15 \end{vmatrix} = -9.$$

Матрица рассматриваемой системы совпадает с матрицей A из задачи 3. Поэтому $\Delta = 3$ и

$$x_1 = \frac{\Delta_1}{\Delta} = 1, \quad x_2 = \frac{\Delta_2}{\Delta} = 2, \quad x_3 = \frac{\Delta_3}{\Delta} = 3.$$

■

Ответ: $x_1 = 1$, $x_2 = 2$, $x_3 = 3$.

Задача 6. Решить систему уравнений

$$\begin{cases} x_1 + 2x_2 + 3x_3 + x_4 = 18, \\ 2x_1 + x_3 + x_4 = 9, \\ x_1 + x_4 = 5, \\ 2x_1 + 2x_2 + x_3 + x_4 = 13 \end{cases}$$

методом Гаусса.

Решение. Составим расширенную матрицу этой системы:

$$\left(\begin{array}{cccc|c} 1 & 2 & 3 & 1 & 18 \\ 2 & 0 & 1 & 1 & 9 \\ 1 & 0 & 0 & 1 & 5 \\ 2 & 2 & 1 & 1 & 13 \end{array}\right).$$

Вычтем из третьей строки первую, а также, умножив первую строку на 2, вычтем её из второй и четвёртой:

$$\left(\begin{array}{cccc|c} 1 & 2 & 3 & 1 & 18 \\ 0 & -4 & -5 & -1 & -27 \\ 0 & -2 & -3 & 0 & -13 \\ 0 & -2 & -5 & -1 & -23 \end{array}\right).$$

Вычтем теперь первую строку из четвёртой и её же, умноженную на 2, из второй:

$$\left(\begin{array}{cccc|c} 1 & 2 & 3 & 1 & 18 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & -2 & -3 & 0 & -13 \\ 0 & 0 & -2 & -1 & -10 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 2 & 3 & 1 & 18 \\ 0 & -2 & -3 & 0 & -13 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & -2 & -1 & -10 \end{array}\right)$$

(правая матрица получена из левой перестановкой второй и третьей строк). Наконец, прибавим к последней строке третью, умноженную на 2:

$$\left(\begin{array}{cccc|c} 1 & 2 & 3 & 1 & 18 \\ 0 & -2 & -3 & 0 & -13 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & -3 & -12. \end{array}\right). \tag{54}$$

Это завершает *первый этап* решения системы.

Второй этап. Последняя строка матрицы (54) означает, что $-3x_4 = -12$, т.е. $x_4 = 4$. Тогда из предпоследней строки следует, что

$$x_3 - x_4 = x_3 - 4 = -1,$$

т.е. $x_3 = 3$. Вторая строка влечёт за собой равенство

$$-2x_2 - 3x_3 + 0 \cdot x_4 = -2x_2 - 9 = -13.$$

Значит, $x_2 = 2$. Наконец, из первой строки получаем

$$x_1 + 2x_2 + 3x_3 + x_4 = x_1 + 4 + 9 + 4 = 18,$$

т.е. $x_1 = 1$. ■

Ответ: $x_1 = 1$, $x_2 = 2$, $x_3 = 3$, $x_4 = 4$.

Задача 7. Найти характеристический многочлен матрицы $A = \left(\begin{smallmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 0 & 1 & 1 \end{smallmatrix}\right)$.

Решение. По определению характеристического многочлена матрицы A имеем

$$\chi_A(\lambda) = \begin{vmatrix} 1-\lambda & 2 & 1 \\ 1 & 1-\lambda & 3 \\ 0 & 1 & 1-\lambda \end{vmatrix} =$$
$$= (1-\lambda)[(1-\lambda)(1-\lambda) - 1 \cdot 3] - 1 \cdot [2(1-\lambda) - 1 \cdot 1] = -3 - 3\lambda + 3\lambda^2 - \lambda^3.$$

■

Ответ: $\chi_A(\lambda) = -3 - 3\lambda + 3\lambda^2 - \lambda^3$.

Задача 8. Найти собственные значения и собственные векторы матрицы $A = \left(\begin{smallmatrix} 10 & 4 \\ 4 & 7 \end{smallmatrix}\right)$ и представить матрицу A в базисе из собственных векторов.

Решение. Характеристический многочлен имеет вид

$$\chi_A(\lambda) = \begin{vmatrix} 10-\lambda & 2 \\ 2 & 7-\lambda \end{vmatrix} = \lambda^2 - 17\lambda + 64.$$

Чтобы найти собственные значения, решим уравнение

$$\chi_A(\lambda) = \lambda^2 - 17\lambda + 64 = 0.$$

Имеем

$$\lambda_{1,2} = \frac{17 \pm \sqrt{17^2 - 4 \cdot 64}}{2} = \frac{17 \pm 5}{2}, \quad \lambda_1 = 11,\ \lambda_2 = 6.$$

Чтобы найти собственные векторы $v_1 = (x_1, y_1)$ и $v_2 = (x_2, y_2)$, соответствующие этим собственным значениям, необходимо решить две системы уравнений

$$\begin{cases} 10x_1 + 2y_1 = 11x_1, \\ 2x_1 + 7y_1 = 11y_1, \end{cases} \qquad \begin{cases} 10x_2 + 2y_2 = 6x_2, \\ 2x_2 + 7y_2 = 6y_2. \end{cases}$$

Из первой следует, что $x_1 = 2y_1$, а из второй —$y_2 = -2x_2$. Таким образом, в качестве собственных векторов можно выбрать $v_1 = (2, 1)$ и $v_2 = (1, -2)$. Поскольку $Av_1 = 11v_1$, $Av_2 = 6v_2$, в базисе (v_1, v_2) матрица A записывается в виде $\left(\begin{smallmatrix} 11 & 0 \\ 0 & 6 \end{smallmatrix}\right)$. ■

Ответ: $\lambda_1 = 11$, $\lambda_2 = 6$, $v_1 = (2, 1)$, $v_2 = (1, -2)$, $\left(\begin{smallmatrix} 11 & 0 \\ 0 & 6 \end{smallmatrix}\right)$.

В оставшихся задачах рассматриваются четыре точки

$$A_0(1,3,1),\ A_1(2,5,2),\ A_2(3,5,7),\ A_3(1,5,3) \tag{55}$$

трёхмерного пространства $\mathbb{R}^3$.

Задача 9. Доказать, что система точек (55) не компланарна и вычислить объём пирамиды с вершинами A_0, A_1, A_2, A_3.

Решение. Рассмотрим направленные отрезки $\overline{A_0A_1}$, $\overline{A_0A_2}$, $\overline{A_0A_3}$ и соответствующие векторы $v_1 = (2,5,2) - (1,3,1) = (1,3,1)$, $v_2 = (3,5,7) - (1,3,1) = (2,2,6)$, $v_3 = (1,5,3) - (1,3,1) = (0,2,2)$. Компланарность точек эквивалентна равенству нулю определителя Δ, составленного из координат этих векторов. Имеем

$$\Delta = \begin{vmatrix} 1 & 3 & 1 \\ 2 & 2 & 6 \\ 0 & 2 & 2 \end{vmatrix} = -12 \neq 0.$$

Следовательно, точки не являются компланарными.

Объём V рассматриваемой пирамиды равен $\frac{1}{6}|(v_1 \times v_2, v_3)|$, т.е. $V = \frac{1}{6}|\Delta|$. Таким образом, $V = 2$ (кубических единиц). ■

Ответ: точки не компланарны, $V = 2$.

Задача 10. Найти уравнение и длину l ребра A_0A_1.

Решение. Эти вершины соединены вектором v_1 из задачи 9. Поэтому искомая длина есть

$$|v_1| = \sqrt{1^2 + 3^2 + 1^2} = \sqrt{11}.$$

Этот же вектор является направляющим вектором прямой, содержащей рассматриваемое ребро, и поэтому её параметрическое уравнение имеет вид

$$\begin{cases} x = 1 + t, \\ y = 3 + 3t, \\ z = 1 + t. \end{cases}$$

Исключая параметр t, получаем уравнение той же прямой в другой форме

$$\frac{x-1}{1} = \frac{y-1}{1} = \frac{y-3}{3}.$$

■

Ответ: $l = \sqrt{11}$ (линейных единиц), $\frac{x-1}{1} = \frac{y-1}{1} = \frac{y-3}{3}$.

Задача 11. Найти уравнение и площадь S грани $A_0A_1A_2$.

Решение. Начнём с вычисления векторного произведения векторов v_1 и v_2, соединяющих точку A_0 с точками A_1 и A_2 соответственно. Имеем

$$v_1 \times v_2 = \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ 2 & 2 & 6 \\ 0 & 2 & 2 \end{vmatrix} = \left(\begin{vmatrix} 2 & 6 \\ 2 & 2 \end{vmatrix}, -\begin{vmatrix} 2 & 6 \\ 0 & 2 \end{vmatrix}, \begin{vmatrix} 2 & 2 \\ 0 & 2 \end{vmatrix} \right) = (-8, -4, 4).$$

Тогда площадь грани вычисляется по формуле

$$S = \frac{1}{2}|v_1 \times v_2| = \frac{1}{2}\sqrt{(-8)^2 + (-4)^2 + 4^2} = 4\sqrt{6}.$$

Уравнение грани находится из условия $(v, v_1 \times v_2) = 0$, где $v = (x - 1, y - 3, z - 1)$, т.е. имеет вид

$$2x + y - z = 4.$$

■

Ответ: $S = 4\sqrt{6}$ (квадратных единиц), $2x + y - z = 4$.

Задача 12. Вычислить угол α между рёбрами A_0A_1 и A_0A_3.

Решение. Поскольку $(v_1, v_3) = |v_1| \cdot |v_3| \cos\alpha$, получаем

$$\cos\alpha = \frac{(v_1, v_3)}{|v_1| \cdot |v_3|} = \frac{1 \cdot 0 + 3 \cdot 2 + 1 \cdot 2}{\sqrt{1^2 + 3^2 + 1^2} \cdot \sqrt{0^2 + 2^2 + 2^2}} = \sqrt{\frac{8}{11}} \approx 0,85.$$

Поэтому $\alpha = \arccos 0,85 \approx 35°$. ■

Ответ: $\alpha \approx 35°$.

Задача 13. Определить длину высоты h пирамиды, опущенной из вершины A_3 на грань $A_0A_1A_2$.

Решение. Поскольку $V = \frac{1}{3}S_{A_0A_1A_2}h$, из задач 9 и 11 получаем

$$h = \frac{3V}{S} = \frac{3 \cdot 2}{4\sqrt{6}} = \frac{\sqrt{6}}{4}.$$

■

Ответ: $h = \frac{\sqrt{6}}{4}$ (линейных единиц).

Вопросы для самопроверки

1. Дайте определение векторного пространства.
2. Что такое арифметическое пространство?
3. Дайте определение линейного оператора.
4. Что такое ядро и образ линейного оператора?
5. Какой линейный оператор называется изоморфизмом?

6. Какие операции определены над линейными операторами и каковы их свойства?
7. Что такое коммутатор линейных операторов?
8. Дайте определение линейной комбинации векторов.
9. Что такое линейно зависимые и линейно независимые векторы?
10. Дайте определение базиса и размерности векторного пространства.
11. Что такое линейная оболочка системы векторов?
12. Дайте определение матрицы.
13. Какова связь между матрицами и линейными операторами?
14. Что такое транспонированная матрица?
15. Какая матрица называется обратной к данной?
16. Что такое определитель квадратной матрицы?
17. Перечислите основные свойства определителей.
18. Какая матрица называется невырожденной?
19. Опишите способ вычисления обратной матрицы.
20. Как решаются системы линейных уравнений методом обратной матрицы?
21. Опишите правило Крамера.
22. Опишите, как решать системы линейных уравнений методом Гаусса.
23. Сформулируйте теорему Кронекера–Капелли.
24. Что такое собственный вектор?
25. Что такое характеристический многочлен матрицы?
26. Что такое собственные значения матрицы и как их находить?
27. Как вычислить длину вектора в координатах?
28. Что такое скалярное произведение векторов?
29. Какие векторы называются коллинеарными и компланарными?
30. Как вычисляется угол между векторами?
31. Что такое векторное произведение?
32. Как вычисляется площадь треугольника?
33. Что такое смешанное произведение?
34. Как вычисляется объём пирамиды?
35. Выпишите уравнение прямой, проходящей через две заданные точки.
36. Выпишите уравнение плоскости, проходящей через три заданные точки.
37. Выпишите уравнение нормали к плоскости, если задана точка, через которую эта нормаль проходит.

ГЛАВА III

Кривые второго порядка

Понятие *кривой* на (или *линии*) плоскости является обобщением понятия графика функции, а кривые в пространстве — это объекты, обобщающие кривые на плоскости. Например, множество точек на плоскости с координатами x и y, удовлетворяющих уравнению

$$y^2 - x = 0,$$

«ничем не хуже» хорошо известной из школьного курса математики параболы, но не является графиком никакой функции (оно «склеено» из двух графиков — $y = \sqrt{x}$ и $y = -\sqrt{x}$). Ниже мы изучим один важный класс кривых, играющих чрезвычайно важную роль в геометрии, алгебре, астрономии и в других областях знаний.

§13. Определения и классификация

Гипербола — это единица на икс.
Из ответа на экзамене.

Определение 1. Пусть на плоскости задана прямая d и точка F, не лежащая на этой прямой. Множество точек плоскости, равноудалённых от d и F, называется *параболой*. При этом прямая d называется *директрисой* параболы, а точка F — её *фокусом*. Прямая, перпендикулярная директрисе и проходящая через фокус, называется *фокальной осью*. Точка пересечения параболы с фокальной осью называется *вершиной* этой параболы.

Расстояние p от фокуса до директрисы называется фокальным параметром параболы, а число $\frac{p}{2}$ — фокусным расстоянием.

Пример 1. Подмножество точек плоскости, задаваемое уравнением

$$y^2 = 2px, \qquad p > 0, \tag{1}$$

является параболой с фокусом в точке $F = (\frac{p}{2}, 0)$. Директриса этой параболы — вертикальная прямая, заданная уравнением $x = -\frac{p}{2}$, а фокальная ось — прямая $y = 0$.

Уравнение (1) называется *каноническим уравнением параболы.* Пример параболы представлен на рис. 1.

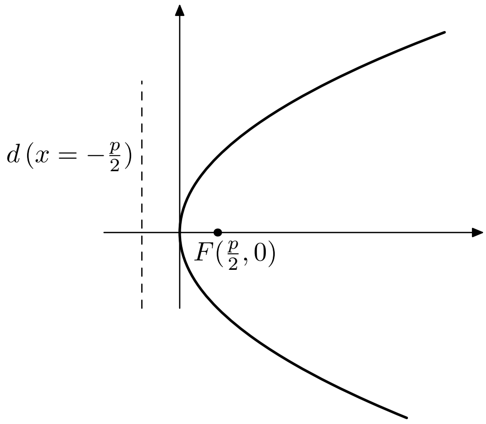

Рис. 1: Парабола, её директриса (d) и фокус (F)

Замечание. Если допустить, что фокус лежит на директрисе, то множество, описываемое определением 1, превратится в прямую, перпендикулярную директрисе и проходящую через фокус.

Определение 2. Пусть F_1 и F_2 — точки плоскости. Множество точек, сумма расстояний от которых до точек F_1 и F_2 постоянна и равна некоторому числу $2a$, $a>0$, называется *эллипсом.* Точки F_1 и F_2 называются *фокусами* эллипса. Прямая, проходящая через фокусы, а также перпендикулярная ей прямая, проходящая через середину отрезка, соединяющего фокусы, называются *фокальными осями* эллипса.

Если $2c$ — расстояние между фокусами, то число c называется *эксцентриситетом*[1] эллипса, а числа a и $b=\sqrt{a^2-c^2}$ — его *полуосями.*

Пример 2. Подмножество точек плоскости, задаваемое уравнением

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}=1, \qquad a\geqslant b>0, \tag{2}$$

является эллипсом. Его полуоси — это a и b, а эксцентриситет равен $c = \sqrt{a^2-b^2}$. Если $a\neq b$, то фокальными осями являются оси координат, а при $a=b$ — любые пары взаимно перпендикулярных прямых, проходящих через начало координат.

Уравнение (2) называется *каноническим уравнением эллипса.* Пример эллипса приведён на рис. 2.

Замечание. Если фокусы эллипса совпадают, то он превращается в окружность радиуса a и тогда его фокальные оси не определены однозначно (см. пример 2). В случае, когда $a=c$, эллипс вырождается в отрезок, соединяющий фокусы[2], а если $a<c$, то множество точек эллипса пусто.

[1]Эксцентриси́те́т — ударение на последнем слоге.

[2]Точнее было бы сказать, что он вырождается в две копии этого отрезка.

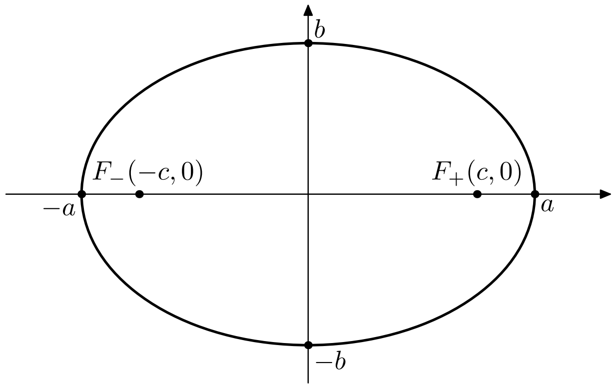

Рис. 2: Эллипс и его фокусы

Определение 3. Пусть F_1 и F_2 — две не совпадающие между собой точки плоскости. Множество точек, абсолютная величина разности расстояний от которых до точек F_1 и F_2 постоянна и равна некоторому числу $2a$, $a > 0$, называется *гиперболой*. Точки F_1 и F_2 называются *фокусами* гиперболы. Прямая, проходящая через фокусы, называется *фокальной осью*, а перпендикулярная ей прямая, проходящая через середину отрезка (эта середина называется *центром* гиперболы), соединяющего фокусы, *мнимой осью* гиперболы. Точки пересечения гиперболы с фокальной осью называются *вершинами* этой гиперболы.

Если $2c$ — расстояние между фокусами, то число c называется *эксцентриситетом* гиперболы, а числа a и $b = \sqrt{c^2 - a^2}$ — её *действительной* и *мнимой полуосями* соответственно.

Прямые, проходящие через центр гиперболы и образующие с фокальной осью углы, для которых $\operatorname{tg}\alpha = \pm\frac{b}{a}$, называются *асимптотами*[3] этой гиперболы.

Пример 3. Подмножество точек плоскости, задаваемое уравнением

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1, \qquad a > 0, \quad b > 0, \tag{3}$$

является гиперболой. Её фокальная ось совпадает с осью абсцисс, а мнимая — с осью ординат. Действительная полуось этой гиперболы равна a, а мнимая — b. Фокусы гиперболы находятся в точках $(\pm c, 0)$, где $c = \sqrt{a^2 + b^2}$, а вершины — в точках $(\pm a, 0)$. Уравнениями асимптот являются $y = \pm\frac{b}{a}x$.

Уравнение (3) называется *каноническим уравнением гиперболы*. Пример гиперболы приведён на рис. 3.

[3] Аси́мптота — ударение на втором слоге.

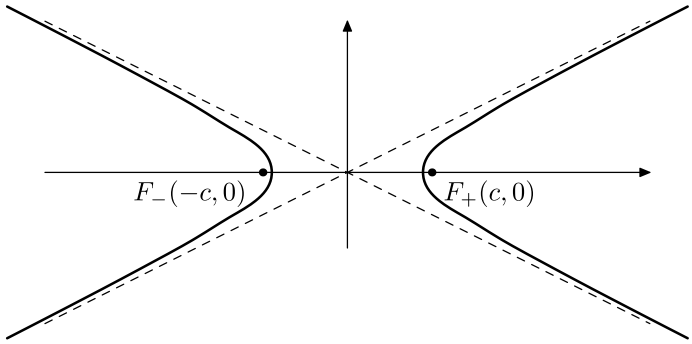

Рис. 3: Гипербола, её фокусы и асимптоты

Замечание. При стремлении a к нулю гипербола вырождается в два экземпляра прямой, проходящей через середину отрезка, соединяющего фокусы, и перпендикулярной этому отрезку. Если же b стремится к бесконечности, она вырождается в пару прямых $x = \pm a$.

Оказывается, все перечисленные фигуры (парабола, эллипс и гипербола) можно задать в общем и единообразном виде.

Определение 4. Множество точек плоскости, координаты которых удовлетворяют уравнению

$$a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + 2b_1x + 2b_2y + c = 0, \tag{4}$$

где a_{ij}, b_i и c — действительные числа и хотя бы одно из чисел a_{ij} отлично от нуля, называется *кривой второго порядка.*

Как мы убедимся, перечисленными в определениях 1—3 множествами исчерпываются все «интересные» кривые второго порядка.

Инварианты кривых второго порядка. О том, какую кривую задаёт уравнение (4), можно судить по коэффициентам, находящимся в правой части этого уравнения.

Определение 5. Матрица

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix} \tag{5}$$

называется *характеристической матрицей* кривой, заданной уравнением (4). Матрица

$$B = \begin{pmatrix} a_{11} & a_{12} & b_1 \\ a_{12} & a_{22} & b_2 \\ b_1 & b_2 & c \end{pmatrix} \tag{6}$$

называется расширенной характеристической матрицей.

Рассмотрим матрицу $A-\lambda E$, $\lambda\in\mathbb{R}$, и её определитель

$$|A-\lambda E| = \begin{vmatrix} a_{11}-\lambda & a_{12} \\ a_{12} & a_{22}-\lambda \end{vmatrix} = \lambda^2-(a_{11}+a_{22})\lambda+a_{11}a_{22}-a_{12}^2. \qquad (7)$$

Таким образом, рассматриваемый определитель является многочленом[4] второй степени от переменной λ.

Определение 6. Многочлен $P(\lambda)=\lambda^2-(a_{11}+a_{22})\lambda+a_{11}a_{22}-a_{12}^2$ называется *характеристическим многочленом* кривой, описываемой уравнением (4). Числа

$$\operatorname{tr} A = a_{11}+a_{22}, \quad \Delta_A, \quad \Delta_B, \qquad (8)$$

где Δ_A и Δ_B — определители матриц A и B соответственно, называются *инвариантами* этой кривой. Заметим попутно, что величина $\operatorname{tr} A$ называется *следом* матрицы A.

Инварианты почти полностью определяют форму любой кривой второго порядка. Если же ввести в рассмотрение ещё одну величину

$$K_A = \begin{vmatrix} a_{11} & b_1 \\ b_1 & c \end{vmatrix} + \begin{vmatrix} a_{22} & b_2 \\ b_2 & c \end{vmatrix}, \qquad (9)$$

называемую *полуинвариантом* (или *относительным инвариантом*), то четыре числа Δ_A, $\operatorname{tr} A$, Δ_B и K_A определят тип кривой полностью.

Лемма 1. *Пусть $P(\lambda)=\lambda^2-(a_{11}+a_{22})\lambda+a_{11}a_{22}-a_{12}^2$ — характеристический многочлен кривой второго порядка. Тогда:*

1) *его дискриминант неотрицателен;*
2) *хотя бы один из его корней отличен от нуля.*

Действительно, дискриминант характеристического многочлена равен

$$D=(a_{11}+a_{22})^2-4(a_{11}a_{22}-a_{12}^2)=(a_{11}-a_{22})^2+4a_{12}^2 \geqslant 0.$$

Значит, характеристический многочлен имеет два действительных корня λ_1 и λ_2.

Если оба корня равны нулю, то по теореме Виета

$$\Delta_A = a_{11}a_{22}-a_{12}^2=\lambda_1\lambda_2=0$$

и

$$\operatorname{tr} A = a_{11}+a_{22}=\lambda_1+\lambda_2=0,$$

откуда следует, что все коэффициенты a_{ij} равны нулю. Но по определению 4 этого не может быть.

[4] Напомним, что этот многочлен называется характеристическим многочленом матрицы A (см. определение 23 на с. 49).

Теорема 1. *Пусть задана кривая второго порядка, описываемая уравнением* (4). *Тогда*:

1. *Если* $\Delta_A > 0$, *то*
   а) *при* $\operatorname{tr} A \cdot \Delta_B < 0$ *эта кривая является эллипсом* (*в частности, при* $\lambda_1 = \lambda_2$ *этот эллипс является окружностью*);
   б) *при* $\operatorname{tr} A \cdot \Delta_B > 0$ *эта кривая является пустым множеством* (*называемым в данном случае мнимым эллипсом*);
   в) *при* $\Delta_B = 0$ *эта кривая состоит из одной точки* (*называемой в данном случае вырожденным эллипсом*).
2. *Если* $\Delta_A < 0$, *то*
   а) *при* $\Delta_B \neq 0$ *эта кривая является гиперболой*;
   б) *при* $\Delta_B = 0$ *рассматриваемая кривая является парой пересекающихся прямых.*
3. *Если* $\Delta_A = 0$, *то*
   а) *при* $\Delta_B \neq 0$ *эта кривая является параболой*;
   б) *при* $\Delta_B = 0$ *и* $K_A < 0$ *эта кривая является парой параллельных прямых*;
   в) *при* $\Delta_B = 0$ *и* $K_A > 0$ *эта кривая является пустым множеством* (*называемым в данном случае парой мнимых*);
   г) *при* $\Delta_B = 0$ *и* $K_A = 0$ *эта кривая является парой совпадающих прямых.*

Поясним термины «инвариант» и «полуинвариант», введённые выше. Обозначим через e и f векторы длины 1, направленные вдоль осей x и y вправо и вверх соответственно и приложенные к началу координат O. Пусть O_1 другая точка плоскости и v_1 и w_1 — приложенные к ней векторы, имеющие единичную длину и взаимно перпендикулярные. Тогда точка O_1 вместе с векторами v_1 и w_1 образуют новую декартову систему координат на плоскости.

Пусть теперь на плоскости задана кривая второго порядка, определяемая уравнением (4). Обозначим через x_1, y_1 новые координаты. Они связаны со старыми соотношениями

$$\begin{cases} x = \alpha_{11}x_1 + \alpha_{12}y_1 + \beta_1, \\ y = \alpha_{21}x_1 + \alpha_{22}y_1 + \beta_2, \end{cases}$$

и в новых координатах уравнение кривой примет вид

$$a_{11}^1 x_1^2 + 2a_{12}^1 x_1 y_1 + a_{22}^1 y_1^2 + 2b_1^1 x_1 + 2b_2^1 y_1 + c^1 = 0.$$

Пусть

$$A^1 = \begin{pmatrix} a^1_{11} & a^1_{12} \\ a^1_{12} & a^1_{22} \end{pmatrix}, \qquad B^1 = \begin{pmatrix} a^1_{11} & a^1_{12} & b^1_1 \\ a^1_{12} & a^1_{22} & b^1_2 \\ b^1_1 & b^1_2 & c^1 \end{pmatrix}$$

— характеристическая и расширенная характеристическая матрицы кривой в новых координатах. Тогда справедлива

Теорема 2. *Имеют место равенства*

$$\Delta_A = \Delta_{A^1}, \quad \operatorname{tr} A = \operatorname{tr} A^1, \quad \Delta_B = \Delta_{B^1}.$$

Если $\Delta_A = 0$, *то и*

$$K_A = K_{A^1}.$$

Таким образом, инварианты кривой не меняются при заменах координат указанного вида.

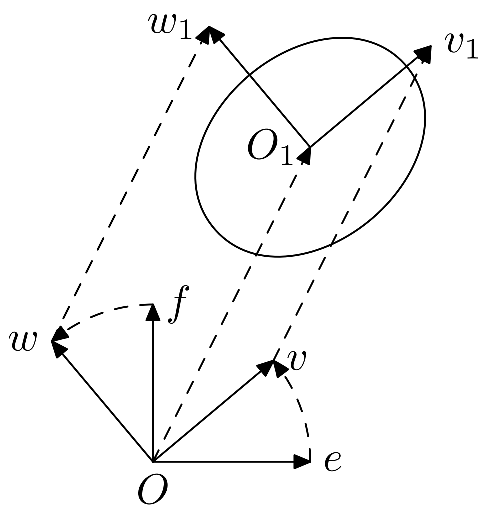

Рис. 4: Выбор канонических координат для эллипса

Рассмотрим кривую, заданную уравнением (4). Её характеристическая матрица симметрична, и поэтому (см. пример 12 из §8) обладает двумя вещественными собственными значениями λ и μ. Если $\lambda \neq \mu$, то соответствующие собственные векторы v и w ортогональны, если же $\lambda = \mu$, то любую пару ортогональных векторов можно выбрать в качестве базиса собственных векторов матрицы A. Поскольку собственные векторы определены с точностью до пропорциональности, можно считать, что они имеют единичную длину.

Возьмём векторы v и w в качестве базисных. В новом базисе матрица A примет вид

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix},$$

и, значит, кривая будет задаваться уравнением

$$\lambda x^2 + \mu y^2 + 2b_1x + 2b_2y + c = 0.$$

Если оба собственных значения отличны от нуля, то последнее уравнение можно переписать следующим образом

$$\lambda\left(x + \frac{b_1}{\lambda}\right)^2 + \mu\left(y + \frac{b_2}{\mu}\right)^2 = \frac{b_1^2}{\lambda} + \frac{b_2^2}{\mu} - c.$$

Сделаем замену

$$x_1 = x + \frac{b_1}{\lambda}, \qquad y_1 = y + \frac{b_2}{\mu}$$

и приложим базисные векторы v и w к точке $O_1(\frac{b_1}{\lambda}, \frac{b_2}{\mu})$ (см. рис. 4). Теперь новое уравнение кривой — это

$$\lambda x_1^2 + \mu y_1^2 = d,$$

где $d = \frac{b_1^2}{\lambda} + \frac{b_2^2}{\mu} - c$. Если $d \neq 0$, то деля на это число обе части уравнения и полагая

$$a^2 = \frac{|d|}{|\lambda|}, \qquad b^2 = \frac{|d|}{|\mu|},$$

мы, в зависимости от знаков, придём к каноническому уравнению эллипса (возможно, мнимого) или гиперболы. Аналогичным образом рассматриваются остальные случаи. Полученные таким образом координаты называются *каноническими*.

§14. Другие способы задания кривых

Задание кривой с помощью уравнения (4) — не единственный и далеко не всегда самый удобный способ её описания. Ниже мы опишем ещё два способа, используемые и в гораздо более общих ситуациях.

14.1. Параметрическое задание

Рассмотрим эллипс, заданный каноническим уравнением (2) и введём новую переменную t таким образом, чтобы выполнялись равенства

$$x = a\cos t, \qquad y = b\sin t. \tag{10}$$

Тогда, при любом значении $t \in \mathbb{R}$ точка с координатами (x, y), задаваемыми равенствами (10), будет лежать на рассматриваемом эллипсе. Величина t называется *параметром*, а уравнение (10) — *параметрическим уравнением эллипса*. Часто роль параметра выполняет время, если мы, например, описываем *траекторию движения* материальной точки. Заметим, что уравнения вида (10) несут больше информации о движении, чем уравнение (2). Действительно, рассмотрим, например, уравнение

$$x = a\cos 2t, \qquad y = b\sin 2t. \tag{11}$$

Множество точек плоскости, задаваемых этим уравнением, то же что и множество, задаваемое уравнением (10), т.е. эллипс

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

Однако движение точки в этом случае другое — если в силу уравнения (10) точка проходит эллипс за время 2π, то во втором случае тот же эллипс проходится за время π, т.е. движение, описываемое уравнением (11) в два раза быстрее первого.

Нетрудно выписать параметрическое уравнение параболы:

$$y = t, \qquad x = \frac{t^2}{2p}. \tag{12}$$

Нахождение же удобной параметризации для гиперболы не столь тривиально и приводит к понятию *гиперболических функций.*

Гиперболические функции. Функция

$$\operatorname{sh} x = \frac{\mathrm{e}^x - \mathrm{e}^{-x}}{2} \tag{13}$$

называется *гиперболическим синусом.* Функция

$$\operatorname{ch} x = \frac{\mathrm{e}^x + \mathrm{e}^{-x}}{2} \tag{14}$$

называется *гиперболическим косинусом.* Непосредственно из определений этих функций вытекает тождество

$$\operatorname{ch}^2 x - \operatorname{sh}^2 x = 1, \tag{15}$$

являющееся аналогом тригонометрического тождества $\cos^2 x + \sin^2 x = 1$ и позволяющее ввести параметризацию гиперболы следующим образом

$$x = a \operatorname{ch} t, \quad y = b \operatorname{sh} t, \quad t \in \mathbb{R}. \tag{16}$$

Таким образом, гиперболические функции играют ту же роль для гиперболы, что и обычные тригонометрические функции для эллипса. Отсюда и название этих функций. Параллель между «гиперболической» и «эллиптической» тригонометрией этим не ограничивается, и об этой параллели будет сказано в §21.

Определим *гиперболический тангенс*, полагая

$$\operatorname{th} x = \frac{\operatorname{sh} x}{\operatorname{ch} x} = \frac{\mathrm{e}^x - \mathrm{e}^{-x}}{\mathrm{e}^x + \mathrm{e}^{-x}}, \tag{17}$$

и *гиперболический котангенс* —

$$\operatorname{cth} x = \frac{\operatorname{ch} x}{\operatorname{sh} x} = \frac{e^x + e^{-x}}{e^x - e^{-x}}. \tag{18}$$

Обратные гиперболические функции[5] имеют вид

$$\operatorname{Arsh} x = \ln(x + \sqrt{x^2+1}), \quad x \in \mathbb{R}, \text{ гиперболический арксинус,} \tag{19}$$

$$\operatorname{Arch} x = \pm\ln(x + \sqrt{x^2-1}), \quad 1 \leqslant x, \text{ гиперболический арккосинус,} \tag{20}$$

$$\operatorname{Arth} x = \frac{1}{2}\ln\frac{1+x}{1-x}, \quad |x| < 1, \text{ гиперболический арктангенс,} \tag{21}$$

$$\operatorname{Arcth} x = \frac{1}{2}\ln\frac{x+1}{x-1}, \quad |x| > 1, \text{ гиперболический арккотангенс.} \tag{22}$$

Отметим в заключение основные свойства гиперболических функций, которые также напоминают аналогичные свойства тригонометрических:

$$\operatorname{th} x \cdot \operatorname{cth} x = 1, \tag{23}$$

$$\operatorname{sh}(x \pm y) = \operatorname{sh} x \operatorname{ch} y \pm \operatorname{ch} x \operatorname{sh} y, \tag{24}$$

$$\operatorname{ch}(x \pm y) = \operatorname{ch} x \operatorname{ch} y \pm \operatorname{sh} x \operatorname{sh} y, \tag{25}$$

$$\operatorname{th}(x \pm y) = \frac{\operatorname{th} x \pm \operatorname{th} y}{1 \pm \operatorname{th} x \operatorname{th} y}, \tag{26}$$

$$\operatorname{cth}(x \pm y) = \frac{1 \pm \operatorname{cth} x \operatorname{cth} y}{\operatorname{cth} x \pm \operatorname{cth} y}, \tag{27}$$

$$\operatorname{sh} x \pm \operatorname{sh} y = 2\operatorname{sh}\frac{x \pm y}{2}\operatorname{ch}\frac{x \mp y}{2}, \tag{28}$$

$$\operatorname{ch} x + \operatorname{ch} y = 2\operatorname{ch}\frac{x + y}{2}\operatorname{ch}\frac{x - y}{2}, \tag{29}$$

$$\operatorname{ch} x - \operatorname{ch} y = 2\operatorname{sh}\frac{x + y}{2}\operatorname{sh}\frac{x - y}{2}, \tag{30}$$

а также ещё одно замечательное свойство —

$$(\operatorname{ch} x \pm \operatorname{sh} x)^n = \operatorname{ch} nx \pm \operatorname{sh} nx. \tag{31}$$

Замечание. В последней формуле читаются либо два верхних плюса, либо два нижних минуса. Аналогичным образом понимаются ниже и все остальные равенства подобного вида. Например, $a^2 - b^2 = (a \pm b)(a \mp b)$.

[5] Обратные гиперболические функции называются иногда *ареа-функциями*.

14.2. Полярные координаты

До сих пор мы задавали координаты точки на плоскости, указывая её проекции на оси абсцисс и ординат, т.е. пользовались декартовой системой координат. Такой способ координирования позиции точки не единственный. Другой, часто используемый, состоит в указании расстояния и направления от некоторой фиксированной точки (начала отсчёта) до данной.

Точнее, пусть точка A имеет прямоугольные координаты (x, y). Рассмотрим величины

$$r = \sqrt{x^2 + y^2} \tag{32}$$

и

$$\varphi = \begin{cases} \operatorname{arctg} \frac{y}{x}, & \text{если } x > 0, \\ \operatorname{arctg} \frac{y}{x} + \pi, & \text{если } x < 0, y \geqslant 0, \\ \operatorname{arctg} \frac{y}{x} - \pi, & \text{если } x < 0, y < 0, \\ \frac{\pi}{2}, & \text{если } x = 0, y > 0, \\ -\frac{\pi}{2}, & \text{если } x = 0, y < 0, \end{cases} \tag{33}$$

называемые *полярным радиусом* и *полярным углом* соответственно. Они однозначно определяют положение точки и называются её *полярными координатами.* Заметим, что в начале координат полярный угол не определён и эта точка определяется нулевым полярным радиусом. Обратно, если известны полярные координаты точки, то её прямоугольные координаты определяются по формулам

$$x = r\cos\varphi, \qquad y = r\sin\varphi. \tag{34}$$

Замечание. Очевидно, в качестве начала полярных координат можно выбрать любую точку плоскости — скажем $A(x_0, y_0)$. В этом случае замена координат (34) будет иметь вид

$$x = x_0 + r\cos\varphi, \qquad y = y_0 + r\sin\varphi. \tag{35}$$

Пример 4. В качестве примера использования полярных координат выведем уравнения кривых второго порядка в этих координатах, используя их канонические уравнения.

Парабола. Рассмотрим каноническое уравнение параболы (1) и выберем начало полярных координат в фокусе параболы, т.е. положим

$$x = \frac{p}{2} + r\cos\varphi, \qquad y = r\sin\varphi.$$

Подставляя эти выражения в каноническое уравнение параболы

$$y^2 = 2px,$$

получаем

$$\sin^2\varphi \cdot r^2 - 2p\cos\varphi \cdot r - p^2.$$

Это — квадратное уравнение относительно r. Решая его и принимая во внимание, что полярный радиус не может быть отрицательным, получаем

$$r = \frac{p}{1-\cos\varphi}. \tag{36}$$

Это и есть уравнение параболы в полярных координатах.

Эллипс. В случае эллипса поместим начало полярных координат в одном из фокусов — скажем, в левом, т.е. положим

$$x = -c + r\cos\varphi, \qquad y = r\sin\varphi,$$

где $c = \sqrt{a^2 - b^2}$— эксцентриситет. Подставляя эти выражения в каноническое уравнение эллипса (2)

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1, \qquad a \geqslant b > 0,$$

получим

$$r = \frac{p}{1 - e\cos\varphi}, \tag{37}$$

где $p = \frac{b^2}{a}$, $e = \frac{c}{a} < 1$.

Гипербола. Точно такие же вычисления приводят к уравнению гиперболы: если поместить начало координат в её правый фокус, то мы получим уравнение правой ветви в виде

$$r = \frac{p}{1 - e\cos\varphi}, \tag{38}$$

где $p = \frac{b^2}{a}$, $e = \frac{c}{a} > 1$.

Итак, имеет место следующий результат:

Теорема 3. *Любая невырожденная кривая второго порядка (т.е. парабола, гипербола или эллипс) в полярных координатах описывается уравнением*

$$r = \frac{p}{1 - e\cos\varphi}, \quad e > 0, \tag{39}$$

где $e < 1$ для эллипса, $e = 1$ для параболы и $e > 1$ для гиперболы.

§15. Оптические свойства кривых второго порядка

Кривые второго порядка обладают замечательными оптическими свойствами. Чтобы эти свойства описать, обсудим вначале, как свет отражается от «кривых зеркал». Если зеркало плоское, то закон отражения известен — угол падения равен углу отражения. В случае же кривого зеркала этот закон формулируется так: угол падения света на касательную к зеркалу равен углу отражения от неё. Значит, чтобы заниматься «криволинейной геометрической оптикой», нужно знать, чтó такое касательная.

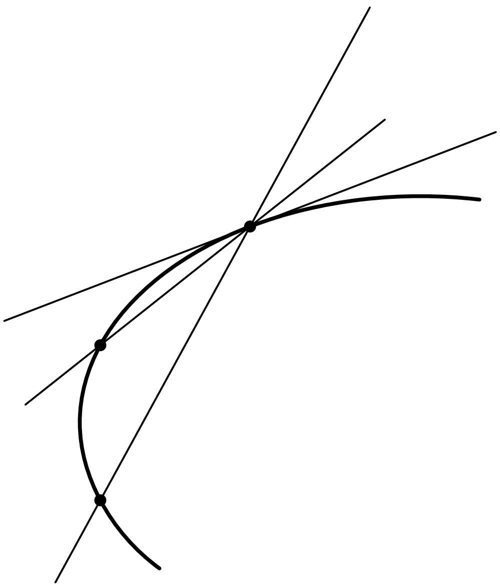

Рис. 5: Приближение касательной секущими

Школьное определение («касательной к окружности называется прямая, пересекающая эту окружность в единственной точке») не является удовлетворительным: легко понять, что для других кривых (например, для параболы) это определение будет приводить к результатам, противоречащим нашему интуитивному представлению о касательных.

Гораздо более правильным было бы определить касательную так: рассмотрим точку на кривой, проведём через эту точку произвольную секущую и будем приближать вторую точку пересечения к исходной — тогда «в пределе» мы получим касательную (см. рис. 5). Такое определение, надлежащим образом уточнённое, применимо к любой кривой, но чтобы его можно было использовать с полной математической строгостью, необходим язык математического анализа, знакомство с которым пока не предполагается. Поскольку мы имеем дело не с произвольными кривыми, а с кривыми второго порядка, нужное нам определение можно сформулировать.

Именно, рассмотрим точку на кривой и скажем, что прямая, проходящая через эту точку, является касательной, если пересечение является «двукратным». Точное определение таково.

Определение 7. Рассмотрим кривую второго порядка

$$a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + 2b_1x + 1b_2y + c = 0$$

и точку (x_0, y_0) на этой кривой. Прямая, проходящая через эту точку и задаваемая параметрическими уравнениями

$$x = v_1t + x_0, \qquad y = v_2t + y_0,$$

называется *касательной* к этой кривой в рассматриваемой точке, если уравнение

$$a_{11}(v_1t+x_0)^2+2a_{12}(v_1t+x_0)(v_2t+y_0)+a_{22}(v_2t+y_0)^2+\\ +2b_1(v_1t+x_0)+1b_2(v_2t+y_0)+c=0, \quad (40)$$

рассматриваемое как уравнение относительно неизвестной t, имеет корень кратности два.

Пользуясь этим определением, мы можем вывести уравнение касательной. Действительно, раскрывая скобки в уравнении (40), получаем

$$(a_{11}v_1^2+2a_{12}v_1v_2+a_{22}v_2^2)t^2+\\ +2(a_{11}v_1x_0+a_{12}(v_1y_0+v_2x_0)+a_{22}v_2y_0+b_1v_1+b_2v_2)t+\\ +a_{11}x_0^2+2a_{12}x_0y_0+a_{22}y_0^2+2b_1x_0+2b_2y_0+c=\\ =(a_{11}v_1^2+2a_{12}v_1v_2+a_{22}v_2^2)t^2+2((a_{11}x_0+a_{12}y_0)v_1+(a_{12}x_0+a_{22}y_0)v_2)t=0,$$

поскольку точка (x_0,y_0) лежит на кривой и, значит, её координаты удовлетворяют уравнению этой кривой. Это уравнение имеет корень $t=0$, и, следовательно, чтобы этот корень был кратности 2, необходимо равенство

$$(a_{11}x_0+a_{12}y_0+b_1)v_1+(a_{12}x_0+a_{22}y_0+b_2)v_2=0.$$

Для выполнения этого равенства достаточно положить

$$v_1=a_{12}x_0+a_{22}y_0+b_2, \quad v_2=-(a_{11}x_0+a_{12}y_0+b_1).$$

Таким образом,

$$\begin{cases} x=(a_{12}x_0+a_{22}y_0+b_2)t+x_0,\\ y=-(a_{11}x_0+a_{12}y_0+b_1)t+y_0 \end{cases} \quad (41)$$

— параметрическое уравнение касательной к кривой второго порядка. Если из системы (41) исключить переменную t, то мы получим другую форму уравнения касательной:

$$(x-x_0)(a_{11}x_0+a_{12}y_0+b_1)+(y-y_0)(a_{12}x_0+a_{22}y_0+b_2)=0, \quad (42)$$

или, учитывая, что точка (x_0,y_0) лежит на кривой,

$$(a_{11}x_0+a_{12}y_0+b_1)x+(a_{12}x_0+a_{22}y_0+b_2)y+b_1x_0+b_2y_0+c=0. \quad (43)$$

В частности, для параболы, задаваемой каноническим уравнением $y^2=2px$, параметрическое уравнение касательной, проходящей через точку (x_0,y_0), где $y_0^2=2px_0$, приобретает вид $x=y_0t+x_0$, $y=pt+y_0$.

Рассмотрим прямую $y=c$, параллельную оси параболы. Она пересекается с параболой в точке $(\frac{c^2}{2p},c)$. Рассмотрим также прямую, соединяющую фокус параболы $(\frac{p}{2}, 0)$ с точкой пересечения. Тогда, пользуясь свойствами скалярного произведения (формула (32) из §10), можно убедиться, что углы между этими прямыми и касательной к параболе в рассматриваемой точке, равны между собой. Это означает, что пучок параллельных оси лучей, падающих на параболическое зеркало, концентрируется в его фокусе, — отсюда и название. Обратно, если в фокусе помещён источник света, то отражённый от параболы свет распространяется параллельным оси пучком (см. рис. 6).

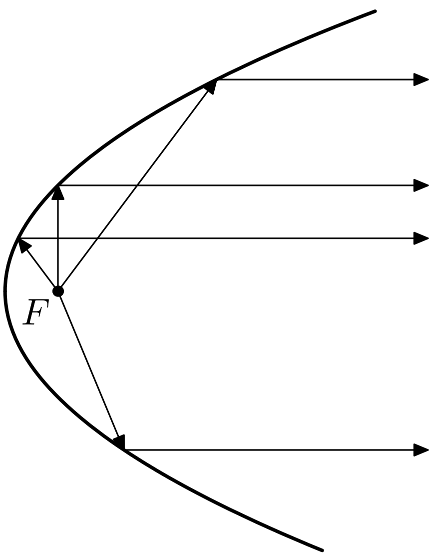

Рис. 6: Параболическое зеркало

Перейдём к рассмотрению оптических свойств эллипса. Уравнение касательной, проходящей через точку (x_0, y_0), имеет вид

$$\frac{x_0 x}{a^2} + \frac{y_0 y}{b^2} = 1,$$

если эллипс задан своим каноническим уравнением

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

Соединим рассматриваемую точку прямыми с фокусами эллипса. Тогда, воспользовавшись уже упомянутой формулой (32) для косинуса, мы можем убедиться, что эти прямые образуют одинаковые углы с касательной к эллипсу. Значит, если внутренняя поверхность эллипса является зеркалом, то пучок света, выпущенный из одного фокуса, будет собираться в другом (см. рис. 7).

Наконец, рассмотрим гиперболу

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1.$$

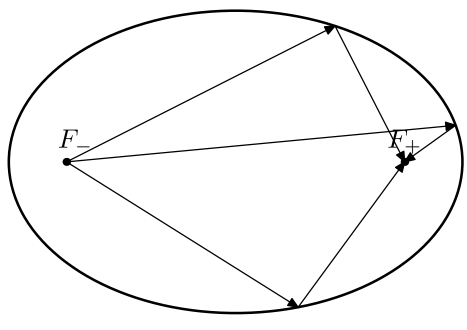

Рис. 7: Эллиптическое зеркало

Уравнение касательной плоскости для неё имеет вид
$$\frac{xx_0}{a^2} - \frac{yy_0}{b^2} = 1.$$

Пусть (x_0, y_0) — точка на правой ветви гиперболы. Соединим эту точку с фокусами. Тогда, как и выше, можно проверить, что полученные прямые будут пересекаться с касательной к гиперболе в рассматриваемой точке под одинаковыми углами. Это означает, что если в левом фокусе помещён источник света, то отражённые от правой ветви лучи будут распространяться так же как если бы источник находился в правом фокусе (см. рис. 8).

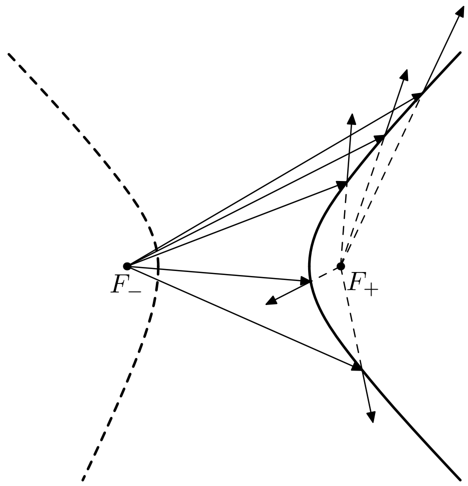

Рис. 8: Гиперболическое зеркало

§16. Образцы решения задач

Задача 1. Кривая второго порядка задана уравнением
$$2x^2 + 4xy - y^2 + 2x + 6y + 7 = 0. \tag{44}$$
Выписать уравнения касательной и нормали к этой кривой, проходящих через точку $A(1, -1)$.

Решение. Очевидно, точка A лежит на кривой (44). Рассмотрим параметрическое уравнение произвольной прямой, проходящей через эту точку:
$$x = at + 1, \qquad y = bt - 1.$$
Подставляя выражения для x и y в уравнение (44), получаем
$$2(at+1)^2 + 4(at+1)(bt-1) - (bt-1)^2 + 2(at+1) + 6(bt-1) + 7 =$$
$$= 2(a^2t^2 + 2at + 1) + 4(abt^2 + (b-a)t - 1) - (b^2t^2 - 2bt + 1)+$$

$$+2(at+1)+6(bt-1)+7=(2a^2+4ab-b^2)t^2+(2a+12b)t=0.$$

Условием касания является то, что $t=0$ есть корень кратности 2 полученного уравнения, т.е. $2a+12b=0$. Значит,

$$x=-6t+1, \qquad y=t-1$$

— уравнение касательной, а

$$x=t+1, \qquad y=6t-1$$

— уравнение нормали. ■

Ответ: $x=-6t+1$, $y=t-1$ — уравнение касательной, $x=t+1$, $y=6t-1$— уравнение нормали.

ЗАДАЧА 2. Определить тип кривой, заданной уравнением (44).

Решение. Рассмотрим характеристическую и расширенную характеристическую матрицы кривой

$$A=\begin{pmatrix}2 & 2\\ 2 & -1\end{pmatrix}, \qquad B=\begin{pmatrix}2 & 2 & 1\\ 2 & -1 & 3\\ 1 & 3 & 7\end{pmatrix}.$$

Поскольку $\Delta_A=-6<0$ и $\Delta_B=-47\neq 0$, кривая является гиперболой. ■

Ответ: кривая, заданная уравнением (44), является гиперболой.

ЗАДАЧА 3. Найти каноническое уравнение и канонические координаты кривой, заданной уравнением (44).

Решение. Рассмотрим характеристическое уравнение

$$|A-\lambda E|=\begin{vmatrix}2-\lambda & 2\\ 2 & -1-\lambda\end{vmatrix}=\lambda^2-\lambda-6=0.$$

Его корни $\lambda_1=3$ и $\lambda_2=-2$ суть собственные значения характеристической матрицы A. Этим собственным значениям соответствуют собственные векторы $e_1=(v_1,w_1)$ и $e_2=(v_2,w_2)$, определяемые из условий

$$\begin{pmatrix}2 & 2\\ 2 & -1\end{pmatrix}\begin{pmatrix}v_1\\ w_1\end{pmatrix}=3\begin{pmatrix}v_1\\ w_1\end{pmatrix}, \qquad \begin{pmatrix}2 & 2\\ 2 & -1\end{pmatrix}\begin{pmatrix}v_2\\ w_2\end{pmatrix}=-2\begin{pmatrix}v_2\\ w_2\end{pmatrix},$$

откуда следует, что в качестве решений можно выбрать векторы $e_1=(2,1)$ и $e_2=(1,-2)$. Соответствующие единичные векторы имеют вид

$$f_1=\Big(\frac{2\sqrt{5}}{5},\frac{\sqrt{5}}{5}\Big), \qquad f_2=\Big(\frac{\sqrt{5}}{5},-\frac{2\sqrt{5}}{5}\Big). \tag{45}$$

Отсюда следует, что старые координаты (x, y) выражаются через новые (x_1, y_1) посредством равенств

$$x = \frac{2\sqrt{5}}{5}x_1 + \frac{\sqrt{5}}{5}y_1, \qquad y = \frac{\sqrt{5}}{5}x_1 - \frac{2\sqrt{5}}{5}y_1.$$

Подставляя эти выражения в исходное уравнение кривой (44), получим её уравнение в новом базисе в виде

$$3x_1^2 - 2y_1^2 + 2\sqrt{5}\,x_1 - 2\sqrt{5}\,y_1 + 7 = 0.$$

Преобразуем последнее равенство, выделяя полные квадраты:

$$3\Big(x_1^2 + 2\frac{\sqrt{5}}{3}\,x_1 + \frac{5}{9}\Big) - 2\Big(y_1^2 + 2\frac{\sqrt{5}}{2}\,y_1 + \frac{5}{4}\Big) - \frac{5}{3} + \frac{5}{2} + 7 = 0,$$

или

$$3\Big(x_1 + \frac{\sqrt{5}}{3}\Big)^2 - 2\Big(y_1 + \frac{\sqrt{5}}{2}\Big)^2 + \frac{26}{3} = 0.$$

Полагая

$$x_2 = y_1 + \frac{\sqrt{5}}{2}, \qquad y_2 = x_1 + \frac{\sqrt{5}}{3},$$

мы приходим к каноническому уравнению

$$\frac{x_2^2}{\left(\sqrt{\frac{13}{3}}\right)^2} - \frac{y_2^2}{\left(\sqrt{\frac{26}{9}}\right)^2} = 1.$$

Это — уравнение кривой (44) в базисе из векторов (45), приложенных к точке $(-\frac{\sqrt{5}}{2}, -\frac{\sqrt{5}}{3})$. ■

Ответ: каноническое уравнение — $\frac{x_2^2}{\left(\sqrt{\frac{13}{3}}\right)^2} - \frac{y_2^2}{\left(\sqrt{\frac{26}{9}}\right)^2} = 1$, канонический базис — $f_1 = (\frac{2\sqrt{5}}{5}, \frac{\sqrt{5}}{5})$, $f_2 = (\frac{\sqrt{5}}{5}, -\frac{2\sqrt{5}}{5})$, приложенный к точке $(-\frac{\sqrt{5}}{2}, -\frac{\sqrt{5}}{3})$.

Задача 4. Определить значения параметра α, при которых кривая, задаваемая уравнением

$$2x^2 - \alpha xy + 3y^2 + 4y + 2 = 0,$$

является эллипсом.

Решение. Рассмотрим инварианты этой кривой:

$$\Delta_A = \begin{vmatrix} 2 & -\frac{\alpha}{2} \\ -\frac{\alpha}{2} & 3 \end{vmatrix} = 6 - \frac{\alpha^2}{4},\ \Delta_B = \begin{vmatrix} 2 & -\frac{\alpha}{2} & 0 \\ -\frac{\alpha}{2} & 3 & 2 \\ 0 & 2 & 2 \end{vmatrix} = 4 - \frac{\alpha^2}{2}, \quad \operatorname{tr} A = 2 + 3 = 6.$$

Поскольку эллипс определяется условиями

$$\Delta_A > 0, \quad \operatorname{tr} A \cdot \Delta_B < 0,$$

мы получаем следующие неравенства:
$$6 - \frac{\alpha^2}{4} > 0, \qquad 6 \cdot \Big(4 - \frac{\alpha^2}{2}\Big) < 0,$$
т.е. $|\alpha| < 2\sqrt{6}$, $|\alpha| > 2\sqrt{2}$. ■

Ответ: $\alpha \in (-2\sqrt{6}, -2\sqrt{2}) \cup (2\sqrt{2}, 2\sqrt{6})$.

Задача 5. В зависимости от значения параметра α определить тип кривой, задаваемой уравнением
$$x^2 + 4xy + 4y^2 + 2\alpha x + 4y + 3 = 0.$$

Решение. Поскольку $\Delta_A = \left|\begin{smallmatrix} 1 & 2 \\ 2 & 4 \end{smallmatrix}\right| = 0$, тип кривой определяется значениями инварианта Δ_B и полуинварианта K_A. Имеем
$$\Delta_B = \begin{vmatrix} 1 & 2 & \alpha \\ 2 & 4 & 2 \\ \alpha & 2 & 3 \end{vmatrix} = -4(\alpha - 1)^2, \qquad K_A = \begin{vmatrix} 1 & \alpha \\ \alpha & 3 \end{vmatrix} + \begin{vmatrix} 4 & 2 \\ 2 & 3 \end{vmatrix} = 11 - \alpha^2.$$
Значит, при $\alpha \neq 1$ кривая является параболой. При $\alpha = 1$ выполнены равенства $\Delta_B = 0$ и $K_A = 10 > 0$, т.е. рассматриваемая кривая является парой мнимых прямых. ■

Ответ: парабола при $\alpha \neq 1$ и пара мнимых прямых при $\alpha = 1$.

Вопросы для самопроверки

1. Дайте определение параболы. Каково её каноническое уравнение?
2. Дайте определение эллипса. Каково его каноническое уравнение?
3. Дайте определение гиперболы. Каково её каноническое уравнение?
4. Уравнением какого вида задаются кривые второго порядка на плоскости?
5. Что такое характеристическая матрица и расширенная характеристическая матрица кривой второго порядка?
6. Дайте определение инвариантов и полуинварианта кривой второго порядка.
7. Как определить тип кривой второго порядка по её инвариантам и полуинварианту?
8. Как найти канонический базис для кривой второго порядка?
9. Выпишите параметрические уравнения эллипса и параболы.
10. Дайте определение гиперболических функций и перечислите их свойства.
11. Какова связь между гиперболическими и тригонометрическими функциями?

12. Выпишите параметрическое уравнение гиперболы.
13. Что такое полярный радиус и полярный угол точки на плоскости?
14. Выпишите формулы, связывающие полярные и декартовы координаты точки.
15. Выпишите канонические уравнения кривых второго порядка в полярных координатах.
16. Дайте определения касательной и нормали к кривой второго порядка.
17. Выпишите уравнения касательной и нормали к эллипсу, заданному своим каноническим уравнением.
18. Выпишите уравнения касательной и нормали к гиперболе, заданной своим каноническим уравнением.
19. Выпишите уравнения касательной и нормали к параболе, заданной своим каноническим уравнением.
20. Опишите оптические свойства кривых второго порядка и проиллюстрируйте их на чертеже.

ГЛАВА IV

Группы, кольца и поля

Понятия абстрактных алгебраических объектов (групп, полей, колец, а также и других, которые здесь не рассматриваются) возникли в математике при исследовании общих свойств операций сложения и умножения.

§18. Основные определения и примеры

Определение 1. Множество G, снабжённое операцией «$\cdot$», условно называемой умножением[1], называется *группой*, если эта операция обладает следующими свойствами:

1) для любых трёх элементов выполняется равенство $f \cdot (g \cdot h) = (f \cdot g) \cdot h$ (*ассоциативность*);
2) существует такой элемент $e \in G$, что $e \cdot g = g \cdot e = g$ для любого $g \in G$ (существование *единицы*)[2];
3) для любого элемента g из множества G существует такой элемент $g^{-1} \in$ $\in G$, что $g \cdot g^{-1} = g^{-1} \cdot g = e$ (существование *обратного элемента*).

Группа называется *коммутативной* (или *абелевой*[3]), если $f \cdot g = g \cdot f$ для всех $f, g \in G$.

Подмножество $H \subset G$ называется *подгруппой* в G, если из $f, g \in H$ следует, что $f \cdot g \in H$.

Очевидно, если множество H — подгруппа, то оно само является группой.

Пример 1. В любой группе, содержащей более одного элемента, есть по крайней мере одна подгруппа, не совпадающая с самой группой, — это подгруппа состоящая из единичного элемента. Она же является самой простой из существующих групп. Ниже мы, конечно, рассмотрим более сложные и интересные примеры.

Пример 2. Множество рациональных чисел, отличных от нуля, образует группу относительно операции умножения, а подмножество положительных

[1]Это название действительно условно: в конкретных примерах в качестве группового умножения может выступать и умножение, и сложение, и операции иного характера.

[2]Как будет видно из примеров, этот элемент, в зависимости от операции в группе, может действительно быть единицей, может совпадать с нулём, а может быть ни тем и не другим.

[3]Название происходит от фамилии норвежского математика Н. Х. Абеля.

рациональных чисел является подгруппой. Точно так же группу по умножению образует множество всех действительных чисел, а подмножество положительных чисел — её подгруппа.

Пример 3. Множество $\mathbb{Z}$ всех целых чисел является группой относительно сложения, а все чётные числа образуют подгруппу (в отличие от нечётных). Заметим, что пока все рассмотренные нами группы были коммутативными.

Определение 2. Отображение $\varphi\colon G \to H$ группы G в группу H называется *гомоморфизмом*, если $\varphi(f \cdot g) = \varphi(f) \cdot \varphi(g)$ для всех $f, g \in G$. Гомоморфизм называется *эпиморфизмом*, если он является сюръекцией, и *мономорфизмом*, если он — инъекция. Если гомоморфизм является одновременно и эпиморфизмом, и мономорфизмом, то он называется *изоморфизмом*. Группы, между которыми существует изоморфизм, называются *изоморфными*, и с алгебраической точки зрения они неразличимы.

Пример 4. Сопоставим каждому целому числу n число $2n$. Это сопоставление — гомоморфизм группы целых чисел в группу чётных чисел, являющееся изоморфизмом.

Пример 5. Множество $\mathbb{R}$ всех действительных чисел является коммутативной группой относительно сложения, а множество $\mathbb{R}^+$ всех положительных чисел — коммутативной группой относительно умножения. Отображение

$$\exp\colon \mathbb{R} \to \mathbb{R}^+, \quad x \mapsto \mathrm{e}^x$$

— изоморфизм этих групп. Обратным к нему является отображение

$$\ln\colon \mathbb{R}^+ \to \mathbb{R}, \quad x \mapsto \ln x.$$

Рассмотрим ещё несколько примеров.

Пример 6 (группы подстановок). Пусть $\mathbb{N}_2 = \{1, 2\}$ — множество, состоящее из первых двух натуральных чисел. Существуют два отображения $\mathbb{N}_2 \to \mathbb{N}_2$, являющиеся взаимно однозначными соответствиями:

$$\sigma_{12}\colon \begin{cases} 1 \to 1, \\ 2 \to 2 \end{cases} \quad \text{и} \quad \sigma_{21}\colon \begin{cases} 1 \to 2, \\ 2 \to 1. \end{cases}$$

Обозначим множество, состоящее из этих двух отображений, через Σ_2 и в качестве групповой операции рассмотрим композицию отображений. Тогда «произведение» элементов будет задаваться следующей таблицей

$\circ$	σ_{12}	σ_{21}
σ_{12}	σ_{12}	σ_{21}
σ_{21}	σ_{21}	σ_{12}

Легко проверить, что относительно введённой операции Σ_2 является группой, единицей которой служит отображение σ_{12}, и $\sigma_{21}^{-1} = \sigma_{21}$.

Точно так же можно рассмотреть множество $\mathbb{N}_3 = \{1, 2, 3\}$ и всевозможные взаимно однозначные отображения этого множества в себя. Их будет шесть:

$$\sigma_{123}\colon \begin{cases} 1 \to 1, \\ 2 \to 2, \\ 3 \to 3, \end{cases} \quad \sigma_{132}\colon \begin{cases} 1 \to 1, \\ 2 \to 3, \\ 3 \to 2, \end{cases} \quad \sigma_{213}\colon \begin{cases} 1 \to 2, \\ 2 \to 1, \\ 3 \to 3, \end{cases}$$

$$\sigma_{231}\colon \begin{cases} 1 \to 2, \\ 2 \to 3, \\ 3 \to 1, \end{cases} \quad \sigma_{312}\colon \begin{cases} 1 \to 3, \\ 2 \to 1, \\ 3 \to 2, \end{cases} \quad \sigma_{321}\colon \begin{cases} 1 \to 3, \\ 2 \to 2, \\ 3 \to 1. \end{cases}$$

Вновь взяв за групповую операцию композицию отображений, мы получим следующую таблицу «умножения»:

$\circ$	σ_{123}	σ_{132}	σ_{213}	σ_{231}	σ_{312}	σ_{321}
σ_{123}	σ_{123}	σ_{132}	σ_{213}	σ_{231}	σ_{312}	σ_{321}
σ_{132}	σ_{132}	σ_{123}	σ_{231}	σ_{213}	σ_{321}	σ_{312}
σ_{213}	σ_{213}	σ_{312}	σ_{123}	σ_{321}	σ_{132}	σ_{231}
σ_{231}	σ_{231}	σ_{321}	σ_{132}	σ_{312}	σ_{123}	σ_{213}
σ_{312}	σ_{312}	σ_{213}	σ_{321}	σ_{123}	σ_{231}	σ_{132}
σ_{321}	σ_{321}	σ_{231}	σ_{312}	σ_{132}	σ_{213}	σ_{123}

Эта таблица тоже задаёт группу, обозначаемую через Σ_3. Эта группа не коммутативна.

Вообще, рассмотрев множество $\mathbb{N}_k = \{1, 2, \ldots, k\}$ и все его взаимно однозначные отображения в себя, мы получим группу Σ_k, называемую *группой подстановок* порядка k; она содержит $k!$ элементов. Если в Σ_k рассмотреть такие подстановки σ, что $\sigma(k) = k$, то они образуют подгруппу, изоморфную Σ_{k-1}.

Пример 7. Множество $\mathrm{GL}(n)$ всех невырожденных (т.е. обратимых) матриц размера $n \times n$ является группой по отношению к произведению матриц, называемой *полной линейной группой* (обратите внимание на то, что в $\mathrm{GL}(n)$ матрицы можно перемножать, но нельзя складывать). Отображение $\Delta\colon \mathrm{GL}(n) \to \mathbb{R} \setminus \{0\}$, сопоставляющее каждой матрице её определитель, является эпиморфизмом полной линейной группы в группу ненулевых действительных чисел.

Матрицы с положительным определителем образуют подгруппу полной линейной группы. Матрицы, чей определитель равен 1, также образуют подгруппу в $\mathrm{GL}(n)$, обозначаемую через $\mathrm{SL}(n)$.

Пример 8. Рассмотрим в группе $\mathrm{GL}(2)$ матрицы $A_{12} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ и $A_{21} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Они образуют подгруппу, изоморфную группе Σ_2. Аналогичным образом, в $\mathrm{GL}(3)$ можно рассмотреть матрицы

$$A_{123} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_{132} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad A_{213} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$
$$A_{231} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad A_{312} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad A_{321} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Они образуют подгруппу, изоморфную Σ_3.

Вообще, если в $\mathrm{GL}(n)$ рассмотреть все матрицы, в каждой строке и каждом столбце которых будет стоять ровно по одной единице, а остальные элементы будут нулевыми, то множество этих матриц (их будет ровно $n!$) будет являться подгруппой, изоморфной Σ_n. Матрицы этого вида, определитель которых равен единице (таких матриц $\frac{n!}{2}$), также образует группу, называемую *группой чётных подстановок* и обозначаемую через Σ_n^+. Например, группа Σ_3^+ состоит из матриц A_{123}, A_{231} и A_{312} (или, что то же самое, из подстановок σ_{123}, σ_{231} и σ_{312}).

Рассмотрим последний пример группы.

Пример 9. Пусть $\mathrm{SO}(2)$ — множество поворотов плоскости вокруг некоторой выбранной точки. Композиция двух поворотов является поворотом и, поскольку поворот — отображение плоскости в себя, композиция является ассоциативной. Поворот на 0 градусов выполняет роль единичного элемента. Таким образом, $\mathrm{SO}(2)$ — группа.

Сопоставим повороту на угол φ матрицу $A_\varphi = \left(\begin{smallmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{smallmatrix}\right)$. Очевидно, $A_\varphi \circ A_\psi = A_{\varphi+\psi}$. Это означает, что композиции поворотов соответствует композиция матриц, т.е. мы построили гомоморфизм группы $\mathrm{SO}(2)$ в группу $\mathrm{GL}(2)$. Этот гомоморфизм является мономорфизмом.

Изучим теперь абстрактные алгебраические объекты, снабжённые двумя операциями.

Определение 3. Множество R, наделённое операциями *сложения* «$+$» и *умножения* «$\cdot$», называется *кольцом*, если эти операции обладают следующими свойствами:

1) для любых элементов a и $b \in R$ имеет место равенство $a + b = b + a$ (сложение *коммутативно*);
2) если $c \in R$, то $(a + b) + c = a + (b + c)$ (сложение *ассоциативно*);

3) существует такой элемент $0 \in R$, что $0+a = a+0 = a$ для любого $a \in R$ (существование *нуля*);
4) для любого $a \in R$ существует такой элемент $-a \in R$, что $(-a) + a = a + (-a) = 0$ (существование *противоположного элемента*);
5) для любых элементов a, b и $c \in R$ выполняются равенства $a(b+c) = ab + ac$, $(a + b)c = ac + bc$ (*дистрибутивность* умножения относительно сложения).

Замечание. Из определения 3 следует, что всякое кольцо является коммутативной (абелевой) группой относительно сложения.

Определение 4. Кольцо R называется *кольцом с единицей*, если существует такой элемент $1 \in R$ (*единица* кольца), что $1 \cdot a = a \cdot 1$ для всех $a \in R$.

Определение 5. Кольцо R называется *ассоциативным*, если $a(bc) = (ab)c$ для любых элементов a, b и $c \in R$ (то есть если определённое в нём *умножение ассоциативно*).

Определение 6. Кольцо R называется *коммутативным*, если $ab = ba$ для любых элементов a и $b \in R$ (то есть если определённое в нём *умножение коммутативно*).

Определение 7. Коммутативное и ассоциативное кольцо R с единицей называется *полем*, если каждый ненулевой элемент $a \in R$ обладает *обратным*, то есть существует такой элемент a^{-1}, что $a^{-1}a = aa^{-1} = 1$.

Замечание. Для всякого поля R множество $R \setminus \{0\}$ его ненулевых элементов является коммутативной группой относительно умножения.

Рассмотрим примеры колец и полей.

Пример 10. Множество $\mathbb{Z}$ *целых чисел* является кольцом относительно обычных операций сложения и умножения. Это кольцо коммутативно, ассоциативно и обладает единицей.

Пример 11. Подмножество $2\mathbb{Z} \subset \mathbb{Z}$, состоящее из всех *чётных* целых чисел, то есть чисел вида $2k$, $k \in \mathbb{Z}$, также является коммутативным и ассоциативным кольцом, но в этом кольце нет единицы.

Пример 12. Множество *нечётных* чисел не образует кольца, поскольку оно не замкнуто относительно сложения — сумма двух нечётных чисел чётна.

Пример 13. Множество $\mathbb{N} \subset \mathbb{Z}$ *натуральных чисел* также не является кольцом, поскольку число, противоположное натуральному, уже не является натуральным числом.

Пример 14. Множество $\mathrm{Mat}(n, n)$ *квадратных матриц* размера $n \times n$ является ассоциативным кольцом с единицей относительно сложения и композиции матриц. Однако это кольцо не коммутативно.

Пример 15. То же самое множество можно наделить другим умножением, взяв в качестве такового *коммутатор матриц*. Это тоже будет кольцом, но ни ассоциативным, ни коммутативным и без единицы.

Пример 16. Если V — векторное пространство размерности n, то можно рассмотреть множество $\mathrm{Lin}(V, V)$ *линейных операторов*, действующих в этом пространстве. Оно является ассоциативным кольцом с единицей относительно сложения и композиции операторов. Аналогично примеру 15 в этом множестве можно ввести другое умножение, рассмотрев коммутатор линейных операторов.

Пример 17. Множества $\mathbb{Q}$ рациональных чисел и $\mathbb{R}$ действительных чисел являются полями относительно обычных операций сложения и умножения чисел.

Пример 18. Множество $C(\mathbb{R})$, состоящее из функций, непрерывных на прямой, является кольцом, если сложение и умножение определить следующим образом:

$$(f+g)(x) = f(x) + g(x),\ (f \cdot g)(x) = f(x)g(x), \quad f, g \in C'(\mathbb{R}),\ x \in \mathbb{R}. \quad (1)$$

Определение 8. Элементы a и b кольца R называются *делителями нуля*, если

1) сами они отличны от нуля, $a \neq 0$, $b \neq 0$;
2) их произведение равно нулю, $ab = 0$.

Пример 19. Функции $f(x) = |x| + x$, $g(x) = |x| - x$ являются делителями нуля в кольце непрерывных функций на прямой.

Пример 20. Матрицы $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ и $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ являются делителями нуля в кольце $\mathrm{Mat}(2, 2)$.

Определение 9. Пусть R и R' — кольца. Отображение $f\colon R \to R'$ называется *гомоморфизмом* колец, если

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b)$$

для любых элементов a, $b \in R$.

Определение 10. Пусть $f\colon R \to R'$ — гомоморфизм колец. Множество

$$\ker f = \{\, a \in R \mid f(a) = 0 \,\}$$

называется *ядром* гомоморфизма f. Множество

$$\mathrm{im}\, f = \{\, a' \in R' \mid a' = f(a), a \in R \,\}$$

называется *образом* гомоморфизма f.

Определение 11. Пусть $f\colon R \to R'$ гомоморфизм колец. Тогда:

1) f называется *мономорфизмом*, если $\ker f = 0$;
2) f называется *эпиморфизмом*, если $\operatorname{im} f = R'$;
3) f называется *изоморфизмом*, если f одновременно и эпиморфизм, и мономорфизм.

Пример 21. Сопоставим каждому действительному числу $r \in \mathbb{R}$ скалярную матрицу $r \cdot E$, где E — единичная матрица размера $n \times n$. Это определяет мономорфизм $\mathbb{R} \to \mathrm{Mat}(n, n)$.

Пример 22. Зафиксируем точку $x_0 \in \mathbb{R}$ и сопоставим каждой непрерывной функции $f \in C(\mathbb{R})$ её значение в точке x_0. Это — эпиморфизм $C(\mathbb{R}) \to \mathbb{R}$. Его ядро состоит из функций, обращающихся в нуль в точке x_0.

Пример 23. Рассмотрим n-мерное векторное пространство V и некоторый его базис $e_1, \ldots, e_n \in V$. Сопоставим каждому линейному оператору $A\colon V \to V$ его матрицу в этом базисе. Это сопоставление определяет изоморфизм колец $\mathrm{Lin}(V, V) \to \mathrm{Mat}(n, n)$. Заметим, что этот изоморфизм зависит от выбора базиса!

Предложение 1. *Пусть $f\colon R \to R'$ — гомоморфизм колец. Тогда:*

1) *если $a', b' \in \operatorname{im} f$, то $a' + b' \in \operatorname{im} f$ и $a'b' \in \operatorname{im} f$;*
2) *если $a, b \in \ker f$, то $a + b \in \ker f$, а также $ac \in \ker f$ и $ca \in \ker f$ для любого $c \in R$.*

Определение 12. Подмножество $S \subset R$ называется *подкольцом*, если оно обладает свойствами, описанными в п. 1 предложения 1. Оно называется *идеалом*, если обладает свойствами, описанными в п. 2 этого предложения.

Пример 24. Множество скалярных матриц является подкольцом кольца диагональных матриц, а диагональные матрицы, в свою очередь, образуют подкольцо кольца *верхних треугольных матриц*[4].

Пример 25. Множество $2\mathbb{Z} \subset \mathbb{Z}$ чётных целых чисел является идеалом кольца целых чисел.

Пример 26. Множество $\mu(x_0) \subset C(\mathbb{R})$, состоящее из функций, обращающихся в нуль в точке $x_0 \in \mathbb{R}$, является идеалом кольца непрерывных функций.

§19. Кольцо целых чисел

Главное свойство целых чисел — это свойство *делимости*.

[4]Квадратная матрица (a_{ij}) называется *верхней треугольной*, если $a_{ij} = 0$ при $i > j$.

Предложение 2. *Пусть m и n — целые числа и $n \neq 0$. Тогда существует единственная пара таких целых чисел q и r, что*

$$m = qn + r, \qquad 0 \leqslant r < |n|. \tag{2}$$

Число q называется (*неполным*) *частным* от деления m на n, а r — *остатком.*

Если в равенстве (2) $r = 0$, то говорят, что m *делится* на n (или *кратно* n). В этом случае n называется *делителем* числа m. В этом случае неполное частное называется просто *частным.*

Определение 13. Целое число $p > 1$ называется *простым*, если оно делится только на себя и на единицу.

Пример 27 (первые 10 простых чисел). Вот первые 10 простых чисел: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

Теорема 1 (теорема Евклида). *Множество простых чисел бесконечно.*

Теорема 2 (основная теорема арифметики). *Любое натуральное число $n > 1$ единственным образом разлагается на простые множители. Точнее, существует единственный набор таких простых чисел $p_1 < p_2 < \cdots < p_k$, что*

$$n = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}, \quad 0 < i_1, \ldots, i_k \in \mathbb{N}. \tag{3}$$

Замечание. Числа вида pq, где p и q — различные простые числа, используются для создания так называемых RSA-кодов (см. ниже пример 28), широко применяющихся в практике защиты данных. Чем больше p и q, тем сложнее расшифровать код. В свою очередь, «инструментом» получения больших простых чисел служит одна из самых известных теорем арифметики.

Теорема 3 (малая теорема Ферма). *Пусть p — простое число и a — натуральное число, не делящееся на p. Тогда $a^{p-1} - 1$ делится на p.*

Малая теорема Ферма важна для теории чисел. Например, с её помощью можно найти признаки делимости на все простые числа, кроме 2 и 5.

Пример 28 (RSA-коды). Криптографическая система RSA (название составлено из первых букв фамилий её создателей — **R**ivest+**S**hamir+**A**dleman) является классическим примером так называемых систем *с открытыми ключами* и основана на следующей схеме.

Каждый абонент строит свою пару *открытых* и *секретных* ключей. Для этого берутся два больших простых числа p и q и вычисляются произведение $n = pq$ и $\varphi(n) = (p-1)(q-1)$. Затем наугад выбирается число e, не имеющее общих делителей с $\varphi(n)$, и строится число d, обладающее свойством

остаток от деления ed на $\varphi(n)$ равен 1.

Пара чисел (n, e) объявляется открытым ключом и помещается в открытый каталог, а число d является секретным.

Если абонент A хочет послать сообщение t (натуральное число) абоненту B, то он выбирает из открытого каталога абонента B пару (n, e) и вычисляет шифрованное сообщение

$$s = \text{ остаток от деления } t^e \text{ на } n,$$

а абонент B, получив это сообщение, вычисляет t по формуле

$$t = \text{ остаток от деления } s^d \text{ на } n.$$

Чем больше числа p и q, тем сложнее расшифровать код (т.е. найти число d).

Определение 14. Пусть m и n — целые числа.

1. *Наибольшим общим делителем* (НОД) чисел m и n называется такой общий положительный делитель[5] этих чисел, на который делится любой другой их общий делитель.
2. Числа m и n называются *взаимно простыми*, если их НОД равен единице.
3. *Наименьшим общим кратным* (НОК) чисел m и n называется такое общее положительное кратное этих чисел, которое делит любое другое общее кратное этих чисел.

Предложение 3. *У любых двух ненулевых целых чисел существуют и единственны НОД и НОК.*

Нахождение НОД и НОК. Чтобы найти НОД и НОК чисел m и n, нужно:

1) найти разложение (3) для чисел m и n.
2) записать числа m и n в виде $m = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$, $n = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$. Если какое-нибудь из чисел p_α не является делителем m или n, то соответствующий показатель степени равен нулю;
3) взять числа $l_\alpha = \min(i_\alpha, j_\alpha)$. Тогда НОД $= p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$;
4) взять числа $s_\alpha = \max(i_\alpha, j_\alpha)$. Тогда НОК $= p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$.

Пример 29. Пусть $m = 72$, $n = 75$. Тогда $72 = 2^3 \cdot 3^2$, $75 = 3 \cdot 5^2$. Значит, $72 = 2^3 \cdot 3^2 \cdot 5^0$, $75 = 2^0 \cdot 3^1 \cdot 5^2$. Поэтому $l_1 = \min(3, 0) = 0$, $l_2 = \min(2, 1) = 1$, $l_3 = \min(0, 2) = 0$, а $s_1 = \max(3, 0) = 3$, $s_2 = \max(2, 1) = 2$, $l_3 = \max(0, 2) = 2$. Значит,

$$\text{НОД}(72, 75) = 2^0 \cdot 3^1 \cdot 5^0 = 3, \qquad \text{НОК}(72, 75) = 2^3 \cdot 3^2 \cdot 5^2 = 1800.$$

[5]То есть число, которое является делителем и m, и n.

Алгоритм Евклида. Ещё один способ находить НОД двух чисел основан на следующем результате (который вытекает из равенства (2)).

Теорема 4 (алгоритм Евклида). *Пусть m_0 и m_1 — натуральные числа, $m_0 > m_1$ и m_1 не является делителем числа m_0. Тогда существуют такие целые числа q_0, $q_1, \dots, q_{k-1}$, q_k и m_2, $m_3, \dots, m_k$, что $m_0 > m_1 > \dots > m_k$, $q_k > 1$ и*

$$\begin{cases} m_0 = m_1 q_0 + m_2, \\ m_1 = m_2 q_1 + m_3, \\ \dots\dots\dots\dots \\ m_{k-2} = m_{k-1} q_{k-1} + m_k, \\ m_{k-1} = m_k q_k. \end{cases}$$

При этом m_k является наибольшим общим делителем чисел m_0 и m_1.

Пример 30. Для чисел из примера 29 имеем

$$\begin{cases} 75 = 72 \cdot 1 + 3, \\ 72 = \boxed{3} \cdot 24. \end{cases}$$

Ещё один пример: пусть $m_0 = 165$, $m_1 = 35$. Тогда

$$\begin{cases} 165 = 35 \cdot 4 + 25, \\ 35 = 25 \cdot 1 + 10, \\ 25 = 10 \cdot 2 + 5, \\ 10 = \boxed{5} \cdot 2. \end{cases}$$

Позиционные системы счисления. Зафиксируем натуральное число $n \neq \neq 1$ и рассмотрим произвольное целое число m. Тогда, в силу равенства (2), m можно представить в виде $m = q_1 n + r_0$. Если $q_1 \geqslant n$, то $q_1 = q_2 n + r_1$ и, следовательно, $m = q_2 n^2 + r_1 n + r_0$. Продолжая этот процесс, мы придём к представлению

$$m = q_k n^k + q_{k-1} n^{k-1} + \ldots + q_1 n + q_0, \tag{4}$$

где все числа q_i удовлетворяют неравенствам $0 \leqslant q_i < n$. Представление (4) называется записью числа m в *n-ичной системе счисления*, а числа q_i *n-ичными цифрами*. В этом случае пишут

$$m = (q_k q_{k-1} \ldots q_1 q_0)_n.$$

Например, в двоичной системе имеются всего две цифры — 0 и 1 — и всякое число записывается в этой системе в виде

$$m = q_k \cdot 2^k + q_{k-1} \cdot 2^{k-1} + \ldots + q_1 \cdot 2 + q_0, \qquad q_0, q_1, \ldots, q_k = 0, 1,$$

или $m = (q_k q_{k-1} \ldots q_1 q_0)_2$.

Пример 31. Имеем,

$$1 = 1_2,\ 2 = 10_2,\ 3 = 11_2,\ 4 = 100_2,\ 5 = 101_2,\ 6 = 110_2, \ldots$$

и

$$1 = 1_3,\ 2 = 2_3,\ 3 = 10_3,\ 4 = 11_3,\ 5 = 12_3,\ 6 = 200_2, \ldots$$

Замечание. Если требуется перевести из десятичной в иную систему счисления дробное число, то его представляют в виде суммы целой и дробной частей, целую часть переводят так, как было описано выше, а для перевода дробной части используют алгоритм, который мы проиллюстрируем на примерах. Он состоит в последовательном умножении исходного числа на основание новой системы счисления и выписывании получающихся целых частей результатов.

Пример 32. Перевести число 0,125 в двоичную систему. Имеем

$$\begin{array}{r} 0{,}125 \\ 2 \\ \hline \boxed{0}{,}250 \\ 2 \\ \hline \boxed{0}{,}500 \\ 2 \\ \hline \boxed{1}{,}000 \\ \hline\hline \end{array}$$

Значит, $(0{,}125)_{10} = (0{,}001)_2$.

Пример 33. Перевести число 0,3 в двоичную систему. Имеем

$$\begin{array}{r} 0{,}3 \\ 2 \\ \hline \boxed{0}{,}6 \\ 2 \\ \hline \boxed{1}{,}2 \\ 2 \\ \hline \boxed{0}{,}4 \\ 2 \\ \hline \boxed{0}{,}8 \\ 2 \\ \hline \boxed{1}{,}6 \\ 2 \\ \hline \boxed{1}{,}2 \\ \ldots \\ \hline\hline \end{array}$$

Значит, $(0{,}3)_{10} = (0{,}0100110011001...)_2$. В правой части этого равенства стоит периодическая дробь с периодом 1001.

Пример 34. Перевести число 0,2 в троичную систему. Имеем

$$\begin{array}{r}
0{,}2\\
3\\ \hline
\boxed{0}{,}6\\
3\\ \hline
\boxed{1}{,}8\\
3\\ \hline
\boxed{2}{,}4\\
3\\ \hline
\boxed{1}{,}2\\
3\\ \hline
\boxed{0}{,}6\\
3\\ \hline
\boxed{1}{,}8\\
\dots\\ \hline\hline
\end{array}$$

Значит, $(0{,}3)_{10} = (0{,}012101210121...)_3$. В правой части этого равенства стоит периодическая дробь с периодом 0121.

Позиционные системы нашли широкое применение в современных компьютерах, где внутреннее представление чисел основано на двоичной системе. Приведём два примера совсем другого рода.

Пример 35 (игра «Ним»). По всей видимости, эта игра впервые появилась в древнем Китае, и состоит она в следующем: на стол кладут несколько кучек одинаковых предметов — например, спичек, и два игрока по очереди выбирают одну из кучек и вынимают из неё любое количество спичек (в частности, можно взять все, но не менее одной). Выигрывает тот, кто забирает последнюю (есть вариант игры, в котором *проигрывает* тот, кто взял последнюю спичку).

Если кучек две, то довольно легко показать, что игрок, сумевший после своего хода сделать количество спичек в обеих кучках одинаковым, всегда (если играет правильно!) выигрывает. Таким образом, если в исходной позиции кучки были одинаковыми, то выигрывает второй игрок, в противном же случае — первый.

Если же кучек несколько (больше двух), то ситуация осложняется. В этом случае выигрышная позиция определяется следующим образом. Предположим, например, что имеется четыре кучки и в них 3, 7, 12 и 17 спичек. Представим каждое из чисел в двоичной системе:

$$3_{10} = 11_2,\ 7_{10} = 111_2,\ 12_{10} = 1100_2, 17_{10} = 10001_2.$$

После этого сложим поразрядно (в десятичной системе) полученные числа

$$\begin{array}{r} 11\\ 111\\ 1100\\ 10001\\ \hline 11223 \end{array}$$

и заменим каждую из поразрядных сумм остатком от её деления на 2:

$$11223 \mapsto 11001.$$

Если полученная последовательность состоит из нулей, то игрок, оказавшийся в этой позиции проигрывает, в противном случае — выигрывает. Таким образом, следует стремиться к тому, чтобы после вашего хода возникла позиция, которой соответствует нулевая последовательность. Этого всегда можно добиться, если вы в непроигрышной позиции.

Пример 36 (фокус Жергона). Этот карточный фокус объясняется с помощью троичной системы счисления и состоит в следующем. Зритель запоминает одну из 27 карт и выкладывает их в три стопки по девять карт картинками вверх (при этом первая карта идёт в первую стопку, вторая — во вторую, третья — в третью, четвёртая — в первую и т.д.). Фокуснику сообщается, в какой из стопок находится задуманная карта, потом стопки складываются в любом из шести возможных порядков (но карты *внутри* стопок не перетасовываются) и вновь раскладываются в три стопки, начиная с верхней карты. Потом карты складываются вновь и процедура повторяется ещё раз (при этом зритель каждый раз сообщает, в какую из стопок попала задуманная карта).

Всякий раз фокусник замечает, куда легла стопка с задуманной картой и запоминает троичную цифру: 0, если карта в верхней стопке, 1, если она в средней стопке и 2, если карта оказалась в нижней стопке. В результате получается трёхзначное число в троичной системе. К нему прибавляется единица и отсчитывается соответствующее число карт, начиная с верхней. Последняя из них — та, которая была задумана.

Попробуйте объяснить этот фокус.

§20. Кольца и поля вычетов

Зафиксируем натуральное число $k \neq 1$ и рассмотрим множество

$$\mathbb{Z}_k = \{\, 0, 1, \ldots, k-1 \,\} \tag{5}$$

всевозможных остатков от деления на k. Определим на множестве $\mathbb{Z}_k$ операции *сложения* и *умножения* следующим образом

$$a + b = \text{остаток от деления суммы } a \text{ и } b \text{ на } k \tag{6}$$

и

$$ab = \text{остаток от деления произведения } a \text{ и } b \text{ на } k. \tag{7}$$

Теорема 5. *Относительно операций* (6) *и* (7) *множество* $\mathbb{Z}_k$ *является коммутативным и ассоциативным кольцом с единицей. Это кольцо является полем тогда и только тогда, когда k — простое число.*

Определение 15. Множество $\mathbb{Z}_k$, снабжённое операцией сложения (6) и умножения (7) называется *кольцом вычетов по модулю k*. Если k — простое число, то оно называется *полем вычетов*.

Пример 37. Структура кольца (поля) в $\mathbb{Z}_k$ задаётся *таблицами сложения и умножения*. Например, для поля $\mathbb{Z}_2$ эти таблицы имеют вид

+	0	1
0	0	1
1	1	0

,

·	0	1
0	0	0
1	0	1

,

в поле $\mathbb{Z}_3$ —

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

,

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

,

а в кольце $\mathbb{Z}_6$ таблицы таковы:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	1	4

,

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

.

Кольца и поля вычетов широко используются в криптографии и являются частными случаями очень важной для алгебры конструкции. Пусть $S \subset R$ — идеал кольца R. Рассмотрим элемент $a \in R$ и подмножество $[a] \subset R$ всех таких элементов $a' \in R$, что $a' - a \in S$. Можно показать, что любые два таких подмножества либо совпадают, либо не пересекаются[6]. Обозначим через R/S

[6]Причина состоит в том, что отношение $a \sim a' \Leftrightarrow a' - a \in S$ является отношением эквивалентности.

множество таких подмножеств и положим

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [a \cdot b], \quad a, b \in R. \tag{8}$$

Предложение 4. *Относительно операций (8) множество R/S является кольцом, а отображение $S \to R/S$, сопоставляющее каждому элементу $a \in S$ подмножество $[a] \subset S$, — эпиморфизмом колец. Ядром этого эпиморфизма является идеал S.*

Определение 16. Кольцо R/S называется *факторкольцом* кольца R по идеалу S.

Пример 38. Пусть $R = \mathbb{Z}$ и $S = k \cdot \mathbb{Z} = \{\, kn \mid n \in \mathbb{Z}\}$. Тогда $S = k \cdot \mathbb{Z}$ — идеал кольца целых чисел, а факторкольцо $\mathbb{Z}/S$ изоморфно кольцу вычетов $\mathbb{Z}_k$.

§21. Поле комплексных чисел

Мнимые числа — это прекрасное и чудесное убежище божественного духа, почти что амфибия бытия с небытием.
Готфрид Вильгельм Лейбниц

Комплексные числа возникли как обобщение чисел вещественных при попытках решать произвольные квадратные (и более общие) уравнения.

Матричное представление. Рассмотрим матрицы вида

$$M(x, y) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = x \cdot E + y \cdot I, \text{ где } E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad x, y \in \mathbb{R}.$$

Имеют место равенства

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix} + \begin{pmatrix} x' & -y' \\ y' & x' \end{pmatrix} = \begin{pmatrix} x + x' & -y - y' \\ y + y' & x + x' \end{pmatrix},$$
$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix} \cdot \begin{pmatrix} x' & -y' \\ y' & x' \end{pmatrix} = \begin{pmatrix} xx' - yy' & -xy' - x'y \\ xy' + x'y & xx' - yy' \end{pmatrix},$$

то есть

$$M(x, y) + M(x', y') = M(x + x', y + y'),$$
$$M(x, y) \cdot M(x', y') = M(xx' - yy', xy' + x'y).$$

В частности, $I^2 = I \cdot I = -E$. При этом

$$\begin{vmatrix} x & -y \\ y & x \end{vmatrix} = x^2 + y^2$$

и

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix} \cdot \begin{pmatrix} \frac{x}{x^2+y^2} & \frac{y}{x^2+y^2} \\ \frac{-y}{x^2+y^2} & \frac{x}{x^2+y^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad x^2+y^2 \neq 0,$$

то есть $M(x,y) \cdot M\left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right) = E$.

Изучим, как действует матрица I в пространстве $\mathbb{R}^2$. Рассмотрим произвольный вектор $\bar{v} = (x,y) \in \mathbb{R}^2$. Тогда $I \cdot \bar{v} = (-y, x)$ и поэтому[7]

$$\|I \cdot \bar{v}\| = \|\bar{v}\|, \quad (\bar{v}, I \cdot \bar{v}) = 0.$$

Значит, вектор $I \cdot \bar{v}$ имеет ту же длину что и $\bar{v}$ и перпендикулярен ему. *Действие матрицы I — это поворот плоскости на 90° против часовой стрелки.*

Поле комплексных чисел. Сопоставим матрице $M(x,y)$ точку $(x,y) \in \mathbb{R}^2$ и обозначим эту точку через $z = x + iy$. Операции сложения и умножения матриц перейдут в следующие:

$$z + z' = (x + x') + i(y + y'), \qquad zz' = (xx' - yy') + i(xy' + x'y).$$

Свойства:

$$z + z' = z' + z, \qquad z + (z' + z'') = (z + z') + z'',$$
$$z + 0 = z, \qquad z + (-z) = 0,$$

где

$$0 = 0 + i \cdot 0, \qquad -z = -x + i(-y),$$
$$zz' = z'z, \qquad z(z'z'') = (zz')z'',$$

и

$$z \cdot 1 = z, \qquad zz^{-1} = 1,$$

где

$$1 = 1 + i \cdot 0, \qquad z^{-1} = \frac{x}{x^2+y^2} - i\frac{y}{x^2+y^2}, z \neq 0.$$

Величи́ны $z = x + iy$, которые складывают и умножают по указанным правилам, называются *компле́ксными числами*, а такая запись — *алгебраической формой записи* комплексного числа. Множество всех комплексных чисел образует поле, которое обозначается через $\mathbb{C}$ и называется *полем комплексных чисел*. Частным от деления двух комплексных чисел z и z', $z' \neq 0$, называется комплексное число $\frac{z}{z'} = zz^{-1}$.

[7] Напомним, что $\|v\|$ обозначает длину вектора v, а (v,w) — скалярное произведение векторов v и w (см. §10).

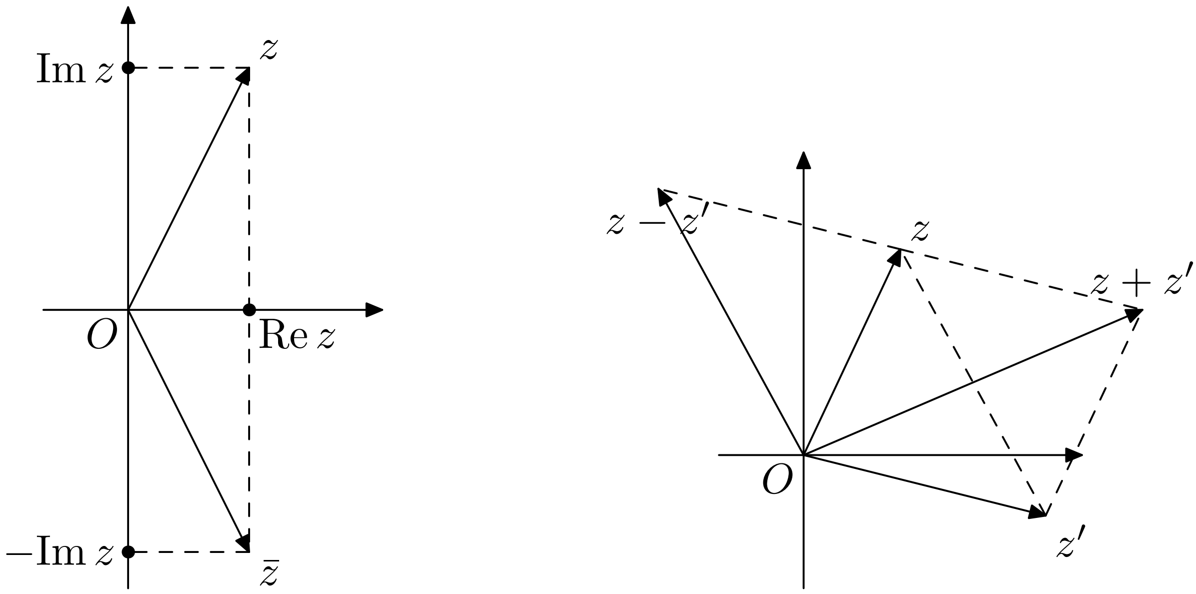

Рис. 1: Геометрическое представление комплексного числа, сумма и разность комплексных чисел

Если $z = x + iy$, то действительное число x называется *вещественной частью* комплексного числа z и обозначается через $\operatorname{Re} z$; число y называется *мнимой частью* комплексного числа z и обозначается через $\operatorname{Im} z$. Если $\operatorname{Im} z = 0$, то есть $z = x$, то это действительное число. Числа, у которых $\operatorname{Re} z = 0$, называются *чисто мнимыми*. Комплексное число $i = 0 + i \cdot 1$ называется *мнимой единицей*. При этом $i^2 = -1$.

Для всякого комплексного числа $z = x + iy$ число $\bar{z} = x - iy$ называется *комплексно-сопряжённым* данному. Операция комплексного сопряжения $z \mapsto \bar{z}$ обладает следующими свойствами:

$$\overline{z + z'} = \bar{z} + \bar{z}', \quad \overline{zz'} = \bar{z}\bar{z}', \quad \bar{\bar{z}} = z, \quad z + \bar{z} = 2 \operatorname{Re} z, \quad z - \bar{z} = 2i \operatorname{Im} z.$$

Комплексное число является действительным тогда и только тогда, когда $z = \bar{z}$, и чисто мнимым тогда и только тогда, когда $z = -\bar{z}$.

Замечание. Операция комплексного сопряжения $z \mapsto \bar{z}$ является изоморфизмом поля комплексных чисел в себя.

Модуль и аргумент. Для любого комплексного числа z произведение $z\bar{z} = x^2 + y^2$ является действительным числом. Число

$$\rho = |z| = \sqrt{x^2 + y^2}$$

называется *модулем* числа z. Угол φ, для которого справедливы равенства

$$\sin \varphi = \frac{\operatorname{Im} z}{\rho}, \quad \cos \varphi = \frac{\operatorname{Re} z}{\rho},$$

называется *аргументом* комплексного числа z. Аргумент определён с точностью до 2π и обозначается через $\operatorname{Arg} z$. Значение аргумента, выбранное в интервале $(-\pi, \pi]$, называется *главным* и обозначается через $\arg z$.

Главное значение аргумента вычисляется по следующей формуле:

$$\arg z = \begin{cases} \operatorname{arctg}\frac{y}{x}, & \text{если } x > 0, \\ \operatorname{arctg}\frac{y}{x} + \pi, & \text{если } x < 0,\ y \geqslant 0, \\ \operatorname{arctg}\frac{y}{x} - \pi, & \text{если } x < 0,\ y < 0, \\ \frac{\pi}{2}, & \text{если } x = 0,\ y > 0, \\ -\frac{\pi}{2}, & \text{если } x = 0,\ y < 0. \end{cases}$$

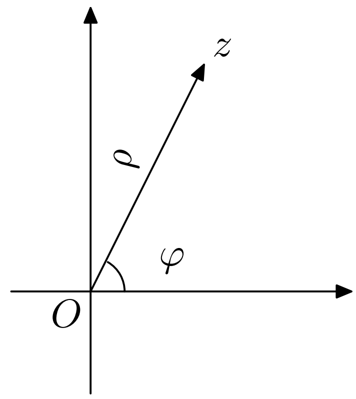

Рис. 2: Модуль и аргумент комплексного числа

При $z = 0$ значение аргумента не определено.

Таким образом, любое комплексное число можно записать в виде

$$z = \rho(\cos\varphi + i\sin\varphi).$$

Эта форма записи называется *тригонометрической*. Она удобна для умножения и деления комплексных чисел:

$$zz' = \rho\rho'(\cos(\varphi + \varphi') + i\sin(\varphi + \varphi'))$$

и

$$\frac{z}{z'} = \frac{\rho}{\rho'}(\sin(\varphi - \varphi') + i\cos(\varphi - \varphi')),$$

а также

$$z^n = \rho^n(\sin(n\varphi) + i\cos(n\varphi)), \quad n \in \mathbb{N}.$$

Последняя формула называется *формулой Муавра*.

Числа $\cos\varphi + i\sin\varphi$ записывают также в виде $\mathrm{e}^{i\varphi}$, или $\exp(i\varphi)$. Таким образом, каждое комплексное число можно представить как

$$z = \rho\mathrm{e}^{i\varphi} \equiv \rho\exp(i\varphi). \tag{9}$$

Это называется *экспоненциальной*, или *показательной* формой записи. Имеют место равенства

$$\rho\mathrm{e}^{i\varphi}\rho'\mathrm{e}^{i\varphi'} = \rho\rho'\mathrm{e}^{i(\varphi+\varphi')}, \quad \frac{\rho\mathrm{e}^{i\varphi}}{\rho'\mathrm{e}^{i\varphi'}} = \frac{\rho}{\rho'}\mathrm{e}^{i(\varphi-\varphi')}$$

(в последнем случае $\rho' \neq 0$).

Замечание. Из экспоненциальной формы записи комплексных чисел вытекают следующие связи между гиперболическими (см. §14) и тригонометрическими функциями, называемые *формулами Эйлера*:

$$\operatorname{sh} ix = i\sin x, \qquad \operatorname{ch} ix = \cos x,$$

$$\operatorname{th} ix = i \operatorname{tg} x, \qquad \operatorname{cth} ix = -i \operatorname{ctg} x.$$

Кроме того, гиперболические функции в следующем смысле периодичны:

$$\operatorname{sh}(x + 2\pi i) = \operatorname{sh} x, \qquad \operatorname{ch}(x + 2\pi i) = \operatorname{ch} x,$$
$$\operatorname{th}(x + \pi i) = \operatorname{th} x, \qquad \operatorname{ctg}(x + \pi i) = \operatorname{cth} x.$$

Решение уравнений в комплексных числах. В 1799 году Карл Фридрих Гаусс доказал следующий фундаментальный результат:

Теорема 6 (основная теорема алгебры). *Любое уравнение вида*

$$a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0 = 0, \quad a_n \neq 0, \tag{10}$$

где $a_0, \ldots, a_n$ — комплексные числа, имеет ровно n комплексных корней, если каждый корень считать с учётом его кратности.

Например, квадратные уравнения *всегда* имеют два корня (возможно, совпадающие), кубические — три и т.д.

Вычисление корней. Рассмотрим уравнение

$$z^n = x + iy.$$

Его решения — корни n-й степени из числа, стоящего в правой части. Представляя это число в тригонометрической форме и используя формулу Муавра, получаем n различных корней

$$z_k = \sqrt[n]{\rho}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right), \quad k = 0, 1, \ldots, n-1,$$

где $\sqrt[n]{\rho}$ — арифметическое значение корня. Таким образом, каждое комплексное (и, в частности, действительное!) число имеет, не равное нулю, n различных корней степени n. Например, корнями 4-й степени из единицы являются числа

$$1, i, -1, -i.$$

Выпишем выражение для квадратного корня из комплексного числа $p+iq$, не используя формулу Муавра. Пусть $z = x+iy$ — такое число, что $z^2 = p+iq$. Тогда

$$x^2 - y^2 = p, \qquad 2xy = q. \tag{11}$$

Следовательно, $y = \frac{q}{2p}$ и, значит,

$$x^2 - \frac{q^2}{4x^2} = p,$$

то есть

$$4x^4 - 4px^2 - q^2 = 0.$$

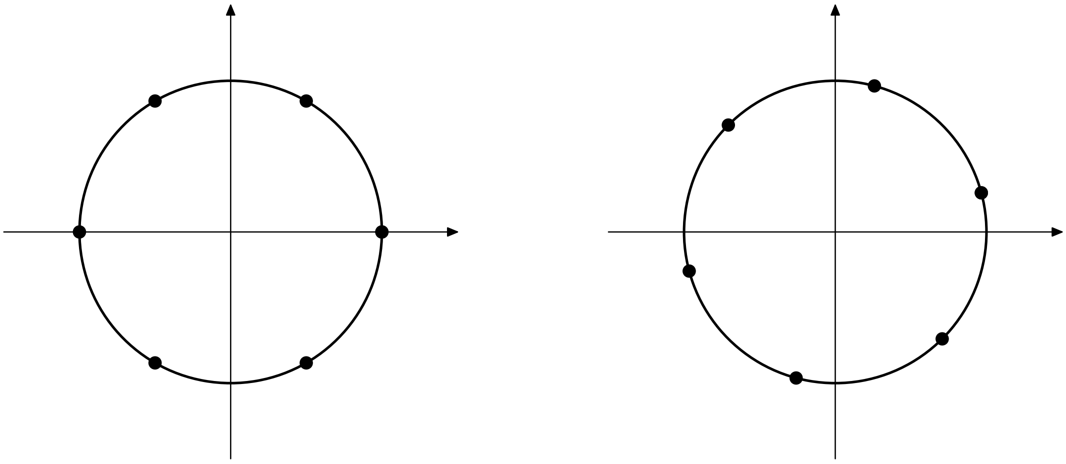

Рис. 3: Корни 6-й степени из 1 (слева) и -1 (справа)

Это — биквадратное уравнение, и его вещественными корнями являются

$$x_{1,2} = \pm\sqrt{\frac{\sqrt{p^2+q^2}+p}{2}}, \qquad x_{3,4} = \pm\sqrt{\frac{\sqrt{p^2+q^2}-p}{2}}.$$

Из четырёх возможных комбинаций только две при возведении в квадрат дают исходное число:

$$\begin{array}{ll} \pm\sqrt{\frac{\sqrt{p^2+q^2}+p}{2}} \pm i\sqrt{\frac{\sqrt{p^2+q^2}-p}{2}}, & \text{если } p \geqslant 0, \\ \pm\sqrt{\frac{\sqrt{p^2+q^2}+p}{2}} \mp i\sqrt{\frac{\sqrt{p^2+q^2}-p}{2}}, & \text{если } p < 0, \end{array} \tag{12}$$

и именно они являются квадратными корнями из комплексного числа $p+iq$.
Решение квадратных уравнений. Рассмотрим уравнение

$$az^2+bz+c=0, \qquad a,b,c\in\mathbb{R}, \quad a\neq 0.$$

Его решениями являются

$$z_{1,2} = \begin{cases} \dfrac{-b\pm\sqrt{D}}{2a}, & D\geqslant 0, \\ \dfrac{-b\pm i\sqrt{-D}}{2a}, & D<0, \end{cases}$$

где $D=b^2-4ac$. Заметим, что если корни комплексные (случай $D<0$), то они комплексно сопряжены. Таким же свойством обладают решения любого уравнения (10) с действительными коэффициентами: если число z — его решение, то $\bar{z}$ также является решением.

Если уравнение имеет комплексные коэффициенты, то его решения имеют вид

$$z_{1,2} = \frac{-b + \sqrt{D}}{2a},$$

где $\sqrt{D}$ вычисляется по формулам (12).

Как и для уравнений с действительными коэффициентами, для произвольных квадратных уравнений справедлива

Теорема 7 (теорема Виета). *Пусть*

$$az^2 + bz + c = 0, \qquad a, b, c \in \mathbb{C}, \quad a \neq 0,$$

и z_1, z_2 — его корни. Тогда выполняются равенства

$$z_1 z_2 = \frac{c}{a}, \qquad z_1 + z_2 = -\frac{b}{a}. \tag{13}$$

§22. Кольцо полиномов

Определение 17. Выражение вида

$$P(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n, \quad a_0, a_1, a_2, \ldots, a_n \in \mathbb{R}, \quad n \in \mathbb{N},$$

называется *многочленом* (или *полиномом*) от переменной x. Числа $a_0, \ldots, a_n$ называются *коэффициентами* многочлена, а число n — его *степенью*, если $a_n \neq 0$. Многочлены нулевой степени — это числа.

Степень многочлена $P(x)$ обозначается через $\deg P(x)$. Многочлены можно складывать и перемножать, причём

$$\begin{gathered} \deg(P(x) + Q(x)) \leqslant \deg P(x) + \deg Q(x), \\ \deg(P(x)Q(x)) = \deg P(x) + \deg Q(x). \end{gathered} \tag{14}$$

Предложение 5. *Множество многочленов является ассоциативным и коммутативным кольцом с единицей.*

Кольцо многочленов обозначается через $\mathbb{R}[x]$.

Замечание. Вместо поля $\mathbb{R}$ в качестве коэффициентов можно взять поле комплексных чисел $\mathbb{C}$. Мы тоже получим кольцо, которое обозначается через $\mathbb{C}[x]$.

Замечание. Точно так же как и из кольца целых чисел было получено поле рациональных чисел, из кольца многочленов можно получить *поле рациональных дробей.* Оно состоит из отношений $\frac{P(x)}{Q(x)}$, где $P(x)$ и $Q(x)$ — многочлены и $Q(x) \not\equiv 0$.

Благодаря соотношениям (14) кольцо многочленов «похоже» на кольцо целых чисел и обладает многими его свойствами

Предложение 6. *Пусть $M(x)$ и $N(x)$ — многочлены и $N(x) \not\equiv 0$. Тогда существует единственная пара таких многочленов $Q(x)$ и $R(x)$, что*

$$M(x) = Q(x)N(x) + R(x), \qquad 0 \leqslant \deg R(x) < \deg N(x). \tag{15}$$

Многочлен $Q(x)$ называется (*неполным*) *частным* от деления многочлена $M(x)$ на многочлен $N(x)$, а $R(x)$ — *остатком*. Если $R(x) \equiv 0$, то говорят, что $M(x)$ *делится* на $N(x)$ (или *кратен* $N(x)$). В этом случае $N(x)$ называется *делителем* многочлена $M(x)$, а неполное частное — просто *частным.*

Теорема 8 (теорема Безу). *Остаток от деления любого многочлена $M(x)$ на многочлен $N(x) = x - c$, $c \in \mathbb{R}$, равен значению $M(x)$ при $x = c$. В частности, $M(x)$ делится на $x - c$ тогда и только тогда, когда $M(c) = 0$.*

Мы будем говорить, что c — *корень многочлена* $M(x)$, если $M(c) = 0$.

Замечание. Как и в кольце целых чисел, в кольце многочленов выполняется *алгоритм Евклида* (ср. с теоремой 4). Для них также можно определить понятия *наибольшего общего делителя* и *наименьшего общего кратного* (см. определение 14).

Роль простых чисел в кольце многочленов играют *неразложимые многочлены.*

Определение 18. Многочлен $P(x)$ называется *неразложимым*, если его степень положительна ($\deg P(x) > 0$) и его нельзя представить в виде

$$P(x) = S(x)Q(x), \quad \deg S(x) > 0, \quad \deg Q(x) > 0.$$

Из основной теоремы алгебры (теорема 6) и теоремы Безу (теорема 8) следует, что любой многочлен степени n однозначно представляется в виде

$$P(x) = a_n(x - c_1)^{n_1}(x - c_2)^{n_2} \ldots (x - c_k)^{n_k}, \tag{16}$$

где $c_1 < \ldots < c_k$ — различные комплексные корни уравнения $P(x) = 0$, а $n_1, \ldots, n_k$, $n_i \neq 0$, — натуральные числа, называемые *кратностями* этих корней. При этом представление (16) единственно. Таким образом, справедлив следующий результат.

Предложение 7. *Над полем комплексных чисел неразложимыми являются многочлены первой степени и только они.*

Если же мы хотим оставаться внутри поля действительных чисел, то есть не рассматривать комплексные корни, то в этом случае предложение 7 становится неверным и результат более сложен. Действительно, заметим следующее. Пусть $P(x) \in \mathbb{R}[x]$ — многочлен с действительными коэффициентами и c — его (комплексный) корень. Тогда число $\bar{c}$, комплексно-сопряжённое с c, также является его корнем. Отсюда следует описание неразложимых многочленов над полем действительных чисел.

Теорема 9. *В кольце $\mathbb{R}[x]$ неразложимыми являются многочлены первой степени, а также квадратные трёхчлены $\alpha x^2 + \beta x + \gamma$, для которых $D = \beta^2 - 4\alpha\gamma < 0$. При этом любой многочлен разлагается в произведение неприводимых*:

$$P(x) = a_n(x - c_1)^{n_1} \dots (x - c_k)^{n_k}(x^2 + p_1x + q_1)^{m_1} \dots (x^2 + p_sx + q_s)^{m_s}, \quad (17)$$

где все сомножители попарно различны, $p_i^2 - 4q_i < 0$, c_j — различные действительные корни многочлена $P(x)$ и

$$\deg P(x) = n_1 + \ldots + n_k + 2(m_1 + \ldots + m_s).$$

Факторкольца. Пусть $P(x) \in \mathbb{R}[x]$. Рассмотрим множество

$$(P) = \{\, Q(x)P(x) \mid Q(x) \in \mathbb{R}[x] \,\} \subset \mathbb{R}[x].$$

Предложение 8. *Множество (P) является идеалом кольца $\mathbb{R}[x]$. Более того, любой идеал этого кольца имеет вид (P) для некоторого многочлена $P(x) \in \mathbb{R}[x]$.*

Следовательно, для любого $P(x) \in \mathbb{R}[x]$ можно рассмотреть факторкольцо $\mathbb{R}[x]/(P)$.

Предложение 9. *Пусть $P(x) \in \mathbb{R}[x]$. Тогда:*

1) *если $P(x) = \alpha x + \beta$, $\alpha \neq 0$, то факторкольцо $\mathbb{R}[x]/(P)$ изоморфно полю действительных чисел $\mathbb{R}$;*
2) *если $P(x) = \alpha x^2 + \beta x + \gamma$, $\alpha \neq 0$ и $D = \beta^2 - 4\alpha\gamma < 0$, то факторкольцо $\mathbb{R}[x]/(P)$ изоморфно полю комплексных чисел $\mathbb{C}$;*
3) *если $P(x) = \alpha x^2 + \beta x + \gamma$, $\alpha \neq 0$ и $D = \beta^2 - 4\alpha\gamma \geqslant 0$, то факторкольцо $\mathbb{R}[x]/(P)$ является некоторым кольцом с делителями нуля.*

Чтобы описать умножение в кольце $\mathbb{R}[x]/(P)$, где $P(x) = \alpha x^2 + \beta x + \gamma$, заметим, что любой элемент $L \in \mathbb{R}[x]/(P)$ однозначно представляется в виде

$$L = ax + b, \quad a, b \in \mathbb{R}.$$

Чтобы перемножить два элемента L_1 и L_2, нужно перемножить их как многочлены, а потом вычислить остаток от деления результата на $P(x) = \alpha x^2 + \beta x + \gamma$. Поэтому

$$(a_1x + b_1)(a_2x + b_2) = \Big(a_1b_2 + a_2b_1 - \frac{\beta}{\alpha}a_1a_2\Big)x + \Big(b_1b_2 - \frac{\gamma}{\alpha}a_1a_2\Big) \quad (18)$$

в факторкольце $\mathbb{R}[x]/(P)$.

§23. Образцы решения задач

Задача 1. Разложить числа 504 и 1188 на простые множители и найти их НОД и НОК.

Решение. Поскольку

$$504 = 2 \cdot 252 = 2 \cdot 2 \cdot 126 = 2 \cdot 2 \cdot 2 \cdot 63 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 21 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7$$

и

$$1188 = 2 \cdot 594 = 2 \cdot 2 \cdot 297 = 2 \cdot 2 \cdot 3 \cdot 99 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 332 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 11,$$

т.е.

$$504 = 2^3 \cdot 3^2 \cdot 7^1 \cdot 11^0, \quad 1188 = 2^2 \cdot 3^3 \cdot 7^0 \cdot 11^1$$

и, значит, НОД$(504, 1188) = 2^2 \cdot 3^2 \cdot 7^0 \cdot 11^0 = 36$, а НОК$(504, 1188) = 2^3 \cdot 3^3 \cdot 7^1 \cdot 11^1 = 16632$. ■

Ответ: $504 = 2^3 \cdot 3^2 \cdot 7$, $1188 = 2^2 \cdot 3^3 \cdot 11$, НОД$(504, 1188) = 36$, НОК$(504, 1188) = 16632$.

Задача 2. Перевести число 37 из десятичной в двоичную и троичную системы счисления.

Решение. Имеем

$$37 = 2 \cdot 18 + 1 = 2^2 \cdot 9 + 1 = 2^2(2^3+1)+1 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0,$$

т.е. $37_{10} = 100101_2$. Аналогично,

$$37 = 3 \cdot 12 + 1 = 3^2(3+1) + 1 = 1 \cdot 3^3 + 1 \cdot 3^2 + 0 \cdot 3^1 + 1 \cdot 3^0,$$

т.е. $37_{10} = 1001_3$. ■

Ответ: $37_{10} = 100101_2$, $37_{10} = 1001_3$.

Задача 3. Даны числа 10010 и 11 в двоичной системе счисления. Вычислить их сумму, разность, произведение и частное и перевести результат в десятичную систему.

Решение. Арифметические операции во всех системах счисления выполняются по общей схеме — «в столбик». Различаются только таблицы умножения и сложения. В двоичной системы эти таблицы таковы:

+	0	1
0	0	1
1	1	10

,

×	0	1
0	0	0
1	0	1

.

Поэтому $10010 + 11 = 10101 = 21_{10}$, $10010 - 11 = 1111 = 15_{10}$, $10010 \cdot 11 = 110110 = 54_{10}$, $10010 : 11 = 110 = 6_{10}$. ■

Ответ: $10010_2 + 11_2 = 10101_2 = 21_{10}$, $10010_2 - 11_2 = 1111_2 = 15_{10}$, $10010_2 \cdot 11_2 = 110110_2 = 54_{10}$, $10010_2 : 11_2 = 110_2 = 6_{10}$.

Задача 4. Даны числа 121 и 11 в двоичной системе счисления. Вычислить их сумму, разность, произведение и частное и перевести результат в десятичную систему.

Решение. В троичной системе таблицы сложения и умножения выглядят следующим образом:

+	0	1	2
0	0	1	2
1	1	2	10
2	2	10	11

,

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	11

.

Поэтому $121 + 11 = 202 = 20_{10}$, $121 - 11 = 110 = 12_{10}$, $121 \cdot 11 = 2101 = 64_{10}$, $121 : 11 = 11 = 4_{10}$. ■

Ответ: $121_3 + 11_3 = 202_3 = 20_{10}$, $121_3 - 11_3 = 110_3 = 12_{10}$, $121_3 \cdot 11_3 = 2101_3 = 64_{10}$, $121_3 : 11_3 = 11_3 = 4_{10}$.

Задача 5. Выписать таблицы сложения и умножения в кольце вычетов $\mathbb{Z}_6$ и указать пары делителей нуля в этом кольце.

Решение. Поскольку кольцо $\mathbb{Z}_8$ образовано остатками от деления на 6, имеем

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

,

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	**0**	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	**0**	4	**0**	4	**0**	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	**0**	6	4	2
7	0	7	6	5	4	3	2	1

.

Из второй таблицы следует, что числа $(2, 4)$, $(4, 4)$ и $(4, 6)$ образуют пары делителей нуля. ■

Ответ: $(2, 4)$, $(4, 4)$ и $(4, 6)$.

Задача 6. Указать элементы, обратные к ненулевым в поле $\mathbb{Z}_5$.

Решение. Поле $\mathbb{Z}_5$ образовано остатками от деления на 5. Поэтому элементом, обратным к некоторому элементу $a \in \mathbb{Z}_5$, является такое число b, $1 \leqslant b \leqslant 4$, что $a \cdot b = 5k + 1$, $k \in \mathbb{Z}$. Имеем

$$1 \cdot 1 = 5 \cdot 0 + 1, \quad 2 \cdot 3 = 5 \cdot 1 + 1, \quad 4 \cdot 4 = 5 \cdot 3 + 1,$$

что исчерпывает все элементы рассматриваемого поля. ■

Ответ: $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$.

Задача 7. Даны комплексные числа $z_1 = 1 + i$, $z_2 = 2 - 3i$. Вычислить величины $\bar{z}_1$, $\bar{z}_2$, $z_1 \pm z_2$, $z_1 z_2$, $\frac{z_1}{z_2}$.

Решение. По определению

$$\bar{z}_1 = \overline{1+i} = 1 - i, \quad \bar{z}_1 = \overline{2-3i} = 2 + 3i.$$

Имеем

$$z_1 + z_2 = (1+i) + (2-3i) = 1 + 2 + (1-3)i = 3 - 2i,$$
$$z_1 - z_2 = (1+i) - (2-3i) = 1 - 2 + (1+3)i = -1 + 4i.$$

Далее,

$$z_1 z_2 = (1+i)(2-3i) = 1 \cdot 2 - 1 \cdot 3i + 2i - 3i^2 = 2 + 3 + (2-1)i = 5 + i.$$

Наконец,

$$\frac{z_1}{z_2} = \frac{z_1 \bar{z}_2}{z_2 \bar{z}_2} = \frac{(1+i)(2+3i)}{(2-3i)(2+3i)} = \frac{1 - 3 + (2+3)i}{2^2 + 3^2} = -\frac{2}{13} + \frac{5}{13}i.$$

■

Ответ: $\bar{z}_1 = 1 - i$, $\bar{z}_1 = 2 + 3i$, $z_1 + z_2 = 3 - 2i$, $z_1 - z_2 = -1 + 4i$, $z_1 z_2 = 5 + i$, $\frac{z_1}{z_2} = -\frac{2}{13} + \frac{5}{13}i$.

Задача 8. Решить квадратное уравнение

$$x^2 + 2x + 2 = 0$$

и представить его решения в алгебраической, тригонометрической и показательной формах.

Решение. Имеем

$$x_{1,2} = \frac{-2 \pm \sqrt{(-2)^2 - 4 \cdot 2}}{2} = \frac{-2 \pm \sqrt{-4}}{2} = -1 \pm i.$$

По определению модуля комплексного числа получаем

$$|x_1| = |x_2| = \sqrt{(-1)^2 + (\pm 1)^2} = \sqrt{2}.$$

Таким образом,

$$x_{1,2} = \sqrt{2}\left(\frac{-\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2}i\right).$$

Главное значение аргумента полученных решений находится из условий

$$\cos\varphi_{1,2} = -\frac{\sqrt{2}}{2}, \quad \sin\varphi_{1,2} = \pm\frac{\sqrt{2}}{2}, \qquad -\pi < \varphi \leqslant \pi,$$

откуда следует, что $\varphi_{1,2} = \pm\frac{3\pi}{4}$. Итак,

$$x_{1,2} = \sqrt{2}\left((\cos\left(\frac{3\pi}{4}\right) + \sin\left(\pm\frac{3\pi}{4}\right)\right)\Bigg) = \sqrt{2}\mathrm{e}^{\pm\frac{3\pi}{4}}.$$

■

Ответ: $x_{1,2} = -1 \pm i = \sqrt{2}\left((\cos\left(\frac{3\pi}{4}\right) + \sin\left(\pm\frac{3\pi}{4}\right)\right)\big) = \sqrt{2}\mathrm{e}^{\pm\frac{3\pi}{4}}$.

Задача 9. Разделить с остатком многочлен $P(x) = x^2 + 2x - 12$ на многочлен $Q(x) = x + 5$.

Решение. Алгоритм деления многочленов такой же как и алгоритм деления десятичных дробей — «в столбик». Поэтому имеем

$$\begin{array}{rrr|l}
x^2 & +\,2x & -\,12 & x+5 \\ \cline{4-4}
x^2 & +\,5x & & x-3 \\ \cline{1-2}
 & -\,3x & -\,12 & \\
 & -\,3x & -\,15 & \\ \cline{2-3}
 & & 3, &
\end{array}$$

т.е. $x^2 + 2x - 12 = (x+5)(x-3) + 3$. ■

Ответ: $x^2 + 2x - 12 = (x+5)(x-3) + 3$, где $x - 3$ — неполное частное, а 3 — остаток.

Задача 10. Перемножить элементы $2x + 3$ и $3x + 2$ в факторкольце $\mathbb{R}[x]/(x^2+1)$.

Решение. По определению умножения в факторкольце произведение двух многочленов есть остаток от деления их «настоящего» произведения на x^2+1. Значит,

$$(2x+3)(3x+2) = 6x^2 + 13x + 6 = (x^2+1)(6x+7) - 1$$

и $(2x+3)\cdot(3x+2) = -1$. ■

Ответ: $(2x+3)\cdot(3x+2) = -1$ в факторкольце $\mathbb{R}[x]/(x^2+1)$.

Вопросы для самопроверки

1. Дайте определение группы. Какие группы называются абелевыми?
2. Приведите известные вам примеры групп.
3. Что такое гомоморфизм групп? Приведите примеры.
4. Что такое изоморфные группы?
5. Дайте определение кольца. Приведите примеры.
6. Какие кольца называются ассоциативными и коммутативными?
7. Что такое гомоморфизм колец?
8. Дайте определение ядра и образа гомоморфизма.

9. Что такое мономорфизм, эпиморфизм и изоморфизм колец?
10. Что такое идеал кольца? Приведите примеры.
11. Что такое поле? Приведите примеры.
12. Дайте определение делимости целых чисел. Какие числа называются простыми?
13. В чём состоит теорема Евклида о простых числах?
14. Сформулируйте основную теорему арифметики.
15. Сформулируйте малую теорему Ферма.
16. Что такое наибольший общий делитель и наименьшее общее кратное? Каков способ их нахождения?
17. Опишите алгоритм Евклида.
18. Опишите алгоритм перевода десятичной дроби в двоичную систему счисления.
19. Что такое кольцо вычетов? Как в этом кольце определяются операции сложения и умножения?
20. В каких случаях кольцо вычетов является полем?
21. Опишите геометрическое представление комплексных чисел. Как в поле комплексных чисел определяются операции сложения и умножения?
22. Что такое число, комплексно сопряжённое данному? Как вычислить число, обратное данному комплексному числу?
23. Опишите матричное представление комплексных чисел.
24. Что такое модуль и аргумент комплексного числа? Как вычисляется главное значение аргумента?
25. Опишите тригонометрическое и экспоненциальное представление комплексных чисел.
26. Что такое формула Муавра и как с её помощью вычисляются корни из комплексных чисел?
27. Сформулируйте основные свойства кольца многочленов.
28. Сформулируйте основную теорему алгебры.
29. Опишите факторкольца кольца многочленов по идеалам, порождённым многочленами степени $\leqslant 2$.

Варианты контрольных домашних заданий

Ниже приводятся варианты контрольных домашних заданий по курсу алгебры и аналитической геометрии. Домашнее задание № 1 включает в себя задачи по линейной алгебре, аналитической геометрии в трёхмерном пространстве и геометрии плоских кривых второго порядка. В домашнее задание № 2 входят задачи, относящиеся к полю комплексных чисел, арифметике целых чисел и колец вычетов, а также к алгебре многочленов.

Домашнее задание № 1

Задание 1.1: Линейная алгебра.

Заданы матрицы A, B, C и векторы $\bar{v}$, $\bar{w}$.

1. Вычислить определители матриц A, B и C.
2. Найти коммутатор матриц A и B.
3. Найти матрицу B^{-1}.
4. Решить систему уравнений $B\bar{x} = \bar{v}$ методом Крамера.
5. Решить систему уравнений $C\bar{x} = \bar{w}$ методом Гаусса.
6. Найти характеристический полином матрицы A.
7. Вычислить собственные значения и собственные векторы матрицы D и записать эту матрицу в базисе из собственных векторов.

Варианты заданий[8].

***Вариант 0*:** $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 5 & 7 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 & 3 \\ 2 & -3 & 2 \\ 5 & 8 & -1 \end{pmatrix}$, $C = \begin{pmatrix} 2 & 1 & -5 & 1 \\ 1 & 3 & 0 & -6 \\ 0 & 2 & -1 & 2 \\ 1 & 4 & -7 & 6 \end{pmatrix}$,
$\bar{v} = (14, 2, 18)$, $\bar{w} = (10, 1, 3, -6)$, $D = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.

***Вариант 1*:** $A = \begin{pmatrix} 2 & 3 & 4 \\ 3 & 4 & 5 \\ 5 & 7 & 9 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 & 3 \\ 2 & -1 & -1 \\ 1 & 3 & 4 \end{pmatrix}$, $C = \begin{pmatrix} 3 & 8 & 3 & -1 \\ 2 & 3 & 4 & 1 \\ 1 & -1 & -2 & -2 \\ 5 & -3 & 4 & 2 \end{pmatrix}$,
$\bar{v} = (13, -3, 18)$, $\bar{w} = (19, 5, -9, 9)$, $D = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$.

***Вариант 2*:** $A = \begin{pmatrix} 2 & 3 & 1 \\ 3 & 4 & 2 \\ 5 & 7 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 & -1 \\ 3 & 2 & 1 \\ 4 & -1 & 5 \end{pmatrix}$, $C = \begin{pmatrix} 1 & 1 & -8 & -4 \\ 3 & -1 & -6 & -4 \\ 2 & 3 & 9 & 2 \\ 3 & 2 & 3 & 6 \end{pmatrix}$,
$\bar{v} = (0, 11, 22)$, $\bar{w} = (12, -14, 24, 24)$, $D = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}$.

***Вариант 3*:** $A = \begin{pmatrix} 3 & 4 & 2 \\ 4 & 5 & 3 \\ 7 & 9 & 5 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 & 3 \\ 5 & -1 & -1 \\ 4 & 3 & 2 \end{pmatrix}$, $C = \begin{pmatrix} 2 & 1 & -5 & 1 \\ 1 & -3 & 0 & -6 \\ 0 & 2 & -1 & 2 \\ 1 & 4 & -7 & 6 \end{pmatrix}$,

[8] Здесь и далее номер варианта определяется по последней цифре номера студенческого билета.

$\bar{v} = (11, 6, 19)$, $\bar{w} = (-4, -14, 6, 5)$, $D = \left(\begin{smallmatrix} 1 & 4 \\ 4 & 1 \end{smallmatrix}\right)$.

Вариант 4: $A = \begin{pmatrix} 3 & 1 & 2 \\ 4 & 2 & 3 \\ 7 & 3 & 5 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, $C = \begin{pmatrix} 1 & -2 & 3 & -1 \\ 2 & 3 & -4 & 4 \\ 3 & 1 & 2 & -2 \\ 1 & -3 & 7 & 6 \end{pmatrix}$,

$\bar{v} = (13, 13, 6)$, $\bar{w} = (2, 9, 2, 30)$, $D = \left(\begin{smallmatrix} 4 & 1 \\ 1 & 4 \end{smallmatrix}\right)$.

Вариант 5: $A = \begin{pmatrix} 4 & 2 & 3 \\ 5 & 3 & 4 \\ 9 & 5 & 7 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 1 & -1 \\ 3 & 2 & 2 \\ 1 & 1 & -2 \end{pmatrix}$, $C = \begin{pmatrix} 2 & 2 & -1 & 1 \\ 4 & 3 & -1 & 2 \\ 8 & 5 & -3 & 4 \\ 3 & 3 & -2 & 2 \end{pmatrix}$,

$\bar{v} = (7, 15, 3)$, $\bar{w} = (3, 8, 12, 4)$, $D = \left(\begin{smallmatrix} 2 & 5 \\ 5 & 2 \end{smallmatrix}\right)$.

Вариант 6: $A = \begin{pmatrix} 2 & 3 & 4 \\ 1 & 4 & 7 \\ -1 & 1 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 & -1 \\ 2 & -3 & 2 \\ 3 & 1 & 1 \end{pmatrix}$, $C = \begin{pmatrix} 2 & -1 & -6 & 3 \\ 7 & -4 & 2 & -15 \\ 1 & -2 & -4 & 9 \\ 1 & -1 & 2 & 6 \end{pmatrix}$,

$\bar{v} = (3, 0, 7)$, $\bar{w} = (6, -33, 23, 21)$, $D = \left(\begin{smallmatrix} 5 & 2 \\ 2 & 5 \end{smallmatrix}\right)$.

Вариант 7: $A = \begin{pmatrix} 3 & 4 & 2 \\ 4 & 7 & 1 \\ 1 & 3 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 & -1 \\ 4 & -3 & 1 \\ 2 & 1 & -1 \end{pmatrix}$, $C = \begin{pmatrix} 1 & 1 & 2 & 3 \\ 3 & -1 & -1 & -2 \\ 2 & 3 & -1 & -1 \\ 1 & 2 & 3 & -1 \end{pmatrix}$,

$\bar{v} = (1, 7, 3)$, $\bar{w} = (12, 0, 3, 12)$, $D = \left(\begin{smallmatrix} 3 & 5 \\ 5 & 3 \end{smallmatrix}\right)$.

Вариант 8: $A = \begin{pmatrix} 4 & 2 & 3 \\ 7 & 1 & 4 \\ 3 & -1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 & 2 \\ 2 & -1 & 2 \\ 4 & 1 & 4 \end{pmatrix}$, $C = \begin{pmatrix} 1 & 2 & 3 & -2 \\ 2 & -1 & -2 & -3 \\ 3 & 2 & -1 & 2 \\ 2 & -3 & 2 & 1 \end{pmatrix}$,

$\bar{v} = (6, 4, 14)$, $\bar{w} = (9, -4, 13, -2)$, $D = \left(\begin{smallmatrix} 5 & 3 \\ 3 & 5 \end{smallmatrix}\right)$.

Вариант 9: $A = \begin{pmatrix} 4 & 6 & 3 \\ 3 & 1 & 4 \\ 1 & 5 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 & -1 \\ 8 & 3 & -6 \\ 4 & 1 & -3 \end{pmatrix}$, $C = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 3 \\ 3 & 2 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}$,

$\bar{v} = (-1, -7, -4)$, $\bar{w} = (14, 10, 16, 21)$, $D = \left(\begin{smallmatrix} 1 & 5 \\ 5 & 1 \end{smallmatrix}\right)$.

Задание 1.2: Аналитическая геометрия в $\mathbb{R}^3$.

В трёхмерном пространстве заданы координаты четырёх точек a, b, c и d. Доказать, что эти точки не компланарны и, приняв их за вершины пирамиды, найти:

1) уравнение и длину ребра ab;
2) уравнение и площадь грани abc;
3) угол между рёбрами ad и db;
4) длину высоты, опущенной из вершины a на грань bcd;
5) объём пирамиды.

Варианты заданий.

Вариант 0: $a(5, 1, 4)$, $b(-7, 6, 5)$, $c(3, -4, 3)$, $d(0, 2, 9)$.
Вариант 1: $a(5, 2, 0)$, $b(2, 5, 0)$, $c(1, 2, 4)$, $d(-1, 1, 1)$.
Вариант 2: $a(-2, 0, -4)$, $b(-1, 7, 1)$, $c(4, -8, -4)$, $d(1, -4, 6)$.
Вариант 3: $a(2, -1, 2)$, $b(1, 2, -1)$, $c(3, 2, 1)$, $d(-4, 2, 5)$.
Вариант 4: $a(-1, 2, -3)$, $b(4, -1, 0$, $c(2, 1, -2)$, $d(3, 4, 5)$.
Вариант 5: $a(1, -1, 1)$, $b(-2, 0, 3)$, $c(2, 1, -1)$, $d(2, -2, -4)$.
Вариант 6: $a(1, 2, 0)$, $b(1, -1, 2)$, $c(0, 1, -1)$, $d(-3, 0, 1)$.
Вариант 7: $a(1, 0, 2)$, $b(1, 2, -1)$, $c(2, -2, 1)$, $d(2, 1, 0)$.
Вариант 8: $a(1, 3, 0)$, $b(4, -1, 2)$, $c(3, 0, 1)$, $d(-4, 3, 5)$.
Вариант 9: $a(0, 3, 2)$, $b(-1, 3, 6)$, $c(-2, 4, 2)$, $d(0, 5, 4)$.

Задание 1.3: Геометрия плоских кривых второго порядка.

1. Заданы кривая $\mathcal{L}$ и точка A на этой кривой. Выписать уравнения касательной и нормали, проходящих через эту точку.
2. Определить тип кривой $\mathcal{L}$.
3. Определить тип кривой $\mathcal{Q}_\alpha$ в зависимости от значения параметра α.

Варианты заданий.

Вариант 0: $A(-1,-1)$, $\mathcal{L}\colon 4x^2+4xy+y^2=4x+13$;
$\mathcal{Q}_\alpha\colon 9x^2+\alpha xy+9y^2+2=\alpha x+6y$.

Вариант 1: $A(1,-1)$, $\mathcal{L}\colon 7x^2+6xy+1=14x+12y$;
$\mathcal{Q}_\alpha\colon 4x^2+\alpha xy+y^2=4x+\alpha y+13$.

Вариант 2: $A(-1,1)$, $\mathcal{L}\colon 74x^2+38xy+5y^2+120x+30y+49=0$;
$\mathcal{Q}_\alpha\colon \alpha x^2+6xy+1=\alpha x+12y$.

Вариант 3: $A(1,1)$, $\mathcal{L}\colon 9x^2+12xy+4y^2+47=42x+30y$;
$\mathcal{Q}_\alpha\colon \alpha x^2+38xy+5y^2+120x+30y=\alpha$.

Вариант 4: $A(-1,-1)$, $\mathcal{L}\colon 15x^2+11xy+2y^2+41x+15y+28=0$;
$\mathcal{Q}_\alpha\colon 9x^2+12xy+\alpha y^2+47=42x+\alpha y$.

Вариант 5: $A(1,-1)$, $\mathcal{L}\colon 13x^2+42xy+18y^2+1=2x+12y$;
$\mathcal{Q}_\alpha\colon 15x^2+\alpha xy+2y^2+\alpha x+15y+28=0$.

Вариант 6: $A(-1,1)$, $\mathcal{L}\colon 25x^2+10xy+y^2+26x+4y+6=0$;
$\mathcal{Q}_\alpha\colon 13x^2+\alpha xy+18y^2+1=2x+\alpha y$.

Вариант 7: $A(1,1)$, $\mathcal{L}\colon 27x^2+48xy+21y^2+106=108x+94y$;
$\mathcal{Q}\colon \alpha x^2+10xy+y^2+\alpha x+4y+6=0$.

Вариант 8: $A(-1,-1)$, $\mathcal{L}\colon \alpha x^2+4xy+5y^2+96x+37y+68=0$;
$\mathcal{Q}_\alpha\colon 27x^2+\alpha xy+21y^2+\alpha=108x+94y$.

Вариант 9: $A(1,-1)$, $\mathcal{L}\colon 9x^2+18xy+9y^2+2=8x+6y$;
$\mathcal{Q}_\alpha\colon 34x^2+26xy+\alpha y^2+96x+\alpha y+68=0$.

Домашнее задание № 2

Задание 2.1: Поле комплексных чисел.

1. Даны комплексные числа z_1 и z_2. Вычислить $z_1\pm z_2$, z_1z_2, $\dfrac{z_1}{z_2}$, $\bar{z}_1$ и $\bar{z}_2$. Указать расположение чисел z_1 и z_2 на комплексной плоскости.
2. Решить квадратное уравнение $z^2+pz+q=0$ и представить его решения в алгебраической, тригонометрической и показательной формах.

Варианты заданий.

Вариант 0: $z_1=2+3i$, $z_2=1+i$; $p=-\sqrt{2}$, $q=1$.

Вариант 1: $z_1=-1+i$, $z_2=-2-3i$; $p=\sqrt{3}$, $q=1$.

Вариант 2: $z_1=-1-i$, $z_2=2-3i$; $p=\sqrt{2}$, $q=1$.

Вариант 3: $z_1 = 1 - i$, $z_2 = 2 + 3i$; $p = -\sqrt{3}$, $q = 1$.
Вариант 4: $z_1 = 2 + i$, $z_2 = 3 + i$; $p = 1$, $q = 1$.
Вариант 5: $z_1 = -3 + i$, $z_2 = 2 - i$; $p = \sqrt{2}$, $q = 2$.
Вариант 6: $z_1 = -3 - i$, $z_2 = 2 - i$; $p = -1$, $q = 1$.
Вариант 7: $z_1 = 3 - i$, $z_2 = 2 + i$; $p = 2\sqrt{3}$, $q = 4$.
Вариант 8: $z_1 = 3 + 2i$, $z_2 = 1 + 3i$; $p = -\sqrt{2}$, $q = 2$.
Вариант 9: $z_1 = 3 - 2i$, $z_2 = 1 - 3i$; $p = -2\sqrt{3}$, $q = 4$.

Задание 2.2: Системы счисления.

1. Перевести указанные числа a_{10}, b_{10} и c_{10} из десятичной в двоичную и троичную системы.
2. Даны числа a_2 и b_2 в двоичной системе. Вычислить $a_2 \pm b_2$, $a_2 b_2$, $\dfrac{a_2}{b_2}$ и перевести результат в десятичную систему.
3. Даны числа a_3 и b_3 в троичной системе. Вычислить $a_3 \pm b_3$, $a_3 b_3$, $\dfrac{a_3}{b_3}$ и перевести результат в десятичную систему.

Варианты заданий.

Вариант 0: $a_{10} = 21$, $b_{10} = 22$, $c_{10} = 0{,}21$; $a_2 = 1100$, $b_2 = 100$; $a_3 = 112$, $b_3 = 21$.
Вариант 1: $a_{10} = 23$, $b_{10} = 24$ $c_{10} = 0{,}22$; $a_2 = 1110$, $b_2 = 111$; $a_3 = 120$, $b_3 = 12$.
Вариант 2: $a_{10} = 25$, $b_{10} = 26$ $c_{10} = 0{,}23$; $a_2 = 1111$, $b_2 = 101$; $a_3 = 110$, $b_3 = 11$.
Вариант 3: $a_{10} = 27$, $b_{10} = 28$ $c_{10} = 0{,}24$; $a_2 = 10010$, $b_2 = 1001$; $a_3 = 200$, $b_3 = 100$.
Вариант 4: $a_{10} = 29$, $b_{10} = 30$ $c_{10} = 0{,}26$; $a_2 = 10101$, $b_2 = 111$; $a_3 = 210$, $b_3 = 21$.
Вариант 5: $a_{10} = 13$, $b_{10} = 31$ $c_{10} = 0{,}27$; $a_2 = 11000$, $b_2 = 110$; $a_3 = 220$, $b_3 = 20$.
Вариант 6: $a_{10} = 14$, $b_{10} = 32$ $c_{10} = 0{,}28$; $a_2 = 10000$, $b_2 = 100$; $a_3 = 121$, $b_3 = 11$.
Вариант 7: $a_{10} = 15$, $b_{10} = 33$ $c_{10} = 0{,}29$; $a_2 = 11100$, $b_2 = 111$; $a_3 = 1001$, $b_3 = 21$.
Вариант 8: $a_{10} = 16$, $b_{10} = 34$ $c_{10} = 0{,}31$; $a_2 = 11011$, $b_2 = 1001$; $a_3 = 1000$, $b_3 = 100$.
Вариант 9: $a_{10} = 17$, $b_{10} = 35$ $c_{10} = 0{,}32$; $a_2 = 11110$, $b_2 = 101$; $a_3 = 1010$, $b_3 = 12$.

Задание 2.3: Арифметика целых чисел. Кольца и поля вычетов.

1. Разложить числа n и m на простые множители и найти для них НОК и НОД.
2. Выписать таблицы сложения и умножения для кольца вычетов $\mathbb{Z}_k$.

Перечислить пары делителей нуля.

3. Указать элементы, обратные к ненулевым в поле $\mathbb{Z}_p$.

Варианты заданий.

Вариант 0: $m = 8580$, $n = 19890$; $k = 6$; $p = 13$.
Вариант 1: $m = 41140$, $n = 6630$; $k = 9$; $p = 5$.
Вариант 2: $m = 17160$, $n = 28050$; $k = 12$; $p = 13$.
Вариант 3: $m = 12012$, $n = 37128$; $k = 14$; $p = 11$.
Вариант 4: $m = 23562$, $n = 18564$; $k = 8$; $p = 7$.
Вариант 5: $m = 47124$, $n = 14014$; $k = 16$; $p = 5$.
Вариант 6: $m = 39780$, $n = 6006$; $k = 10$; $p = 13$.
Вариант 7: $m = 36652$, $n = 9945$; $k = 16$; $p = 11$.
Вариант 8: $m = 56628$, $n = 9282$; $k = 18$; $p = 7$.
Вариант 9: $m = 43316$, $n = 6732$; $k = 20$; $p = 5$.

Задание 2.4: Кольца многочленов.

1. Разделить с остатком многочлен $P(x)$ на $Q(x)$.
2. Перемножить элементы $5x + 6$ и $7x + 1$ в факторкольце $\mathbb{R}[x]/(\alpha x^2 + \beta x + \gamma)$.

Варианты заданий.

Вариант 0: $P(x) = 2x^5 + 3x^4 + 4x^3 + 5x^2 + 7x + 7$, $Q(x) = x^2 + 2x + 3$; $\alpha = 2$, $\beta = 0$, $\gamma = \frac{1}{8}$.

Вариант 1: $P(x) = 3x^5 + 4x^4 + 5x^3 + 6x^2 + 7x + 8$, $Q(x) = x^2 + 3x + 4$; $\alpha = -2$, $\beta = 1$, $\gamma = -\frac{1}{4}$.

Вариант 2: $P(x) = 4x^5 + 5x^4 + 6x^3 + 7x^2 + 8x + 9$, $Q(x) = x^2 + 4x + 5$; $\alpha = 2$, $\beta = 2$, $\gamma = \frac{5}{8}$.

Вариант 3: $P(x) = 5x^5 + 6x^4 + 7x^3 + 8x^2 + 9x + 10$, $Q(x) = x^2 + 5x + 6$; $\alpha = -2$, $\beta = 3$, $\gamma = -\frac{5}{8}$.

Вариант 4: $P(x) = 6x^5 + 7x^4 + 8x^3 + 8x^2 + 10x + 11$, $Q(x) = x^2 + 6x + 7$; $\alpha = 2$, $\beta = 4$, $\gamma = \frac{17}{8}$.

Вариант 5: $P(x) = 2x^5 + x^4 - x^3 - 2x^2 - 4x - 4$, $Q(x) = x^2 + 2x + 3$; $\alpha = -2$, $\beta = 0$, $\gamma = -\frac{1}{8}$.

Вариант 6: $P(x) = 3x^5 + 2x^4 + x^3 - x^2 - 2x - 3$, $Q(x) = x^2 + 3x + 4$; $\alpha = 2$, $\beta = 1$, $\gamma = \frac{1}{4}$.

Вариант 7: $P(x) = 4x^5 + 3x^4 + 2x^3 + x^2 - 1x - 2$, $Q(x) = x^2 + 4x + 5$; $\alpha = -2$, $\beta = 2$, $\gamma = -\frac{5}{8}$.

***Вариант 8*:** $P(x) = 5x^5 + 4x^4 + 3x^3 + 2x^2 + x - 1$, $Q(x) = x^2 + 5x + 6$; $\alpha = 2$, $\beta = 3$, $\gamma = \dfrac{5}{8}$.

***Вариант 9*:** $P(x) = 6x^5 + 5x^4 + 4x^3 + 3x^2 + 2x + 8$, $Q(x) = x^2 + 6x + 7$; $\alpha = -2$, $\beta = 4$, $\gamma = \dfrac{-17}{8}$.

Приложения

Краткие биографические сведения

А́бель (Abel) Нильс Хенрик (1802–1829).
Норвежский математик. С 16 лет проявил исключительные математические способности. Окончил университет в Осло (1825). В 1825–1827 гг. был в Берлине, Париже, где встречался со многими известными математиками. Доказал, что алгебраические уравнения степени выше 4-й неразрешимы в радикалах (1824). Развил теорию сходимости степенных рядов, впервые полностью исследовал проблему сходимости биномиального ряда для комплексных значений переменных (1826). Изучал интегралы от алгебраических функций — абелевы интегралы (1827). Заложил основы теории интегральных уравнений (1823). За создание теории эллиптических функций ему (посмертно), совместно с Якоби, присуждена, премия Парижской академии наук (1830). Работы Абеля оказали большое влияние на развитие математики, привели к возникновению новых математических дисциплин. На родине при жизни Абель не был признан, жил в нужде. В 1908 г. в Осло ему воздвигли памятник.

Безу́ (Bezout) Этьенн (1730–1783).
Французский математик, член Парижской академии наук (1758). Преподавал математику в Училище гардемаринов (1763) и Королевском артиллерийском корпусе (1768). Основные его работы относятся к алгебре (исследование систем алгебраических уравнений высших степеней, исключение неизвестных в таких системах и др.). Автор шеститомного «Курса математики» (1764–1769), неоднократно переиздававшегося.

Венн (Venn) Джон (1834–1923).
Английский логик, разработал графический аппарат диаграмм. Работы в области вероятностной и индуктивной логики.

Вие́т (Viète) Франсуа (1540–1603).
Французский математик, юрист по профессии. Заинтересовавшись астрономией, начал изучать тригонометрию и алгебру. Алгебра в его трудах стала общей наукой об алгебраических уравнениях, основанной на буквенном исчислении. Впервые ввёл буквенные обозначения для коэффициентов уравнений (1591). Предложил новые методы решения алгебраических уравнений

(до четвёртой степени включительно). Установил связь между корнями и коэффициентами уравнений (формулы Виета). Дал полное решение задачи об определении всех элементов плоского или сферического треугольника по трём данным, нашёл разложения $\sin nx$, $\cos nx$ по степеням $\sin x$, $\cos x$. Впервые рассмотрел бесконечное произведение употребил фигурные скобки.

Га́усс (Gauss) Карл Фридрих (1777–1855).
Немецкий математик, астроном, физик и геодезист, член Лондонского королевского общества (1804), Парижской академии (1820), Петербургской академии наук (1824). Родился в Брауншвейге в семье водопроводчика. В раннем детстве обнаружил выдающиеся математические способности. Учился в Гёттингенском университете (1795–1798). С 1807 г. — профессор математики и астрономии в Гёттингенском университете, директор астрономической обсерватории. Работы Гаусса оказали большое влияние на развитие алгебры, теории чисел, дифференциальной геометрии, теории вероятностей, геодезии, небесной механики, астрономии, теории электричества и магнетизма. Гаусс предложил несколько вариантов доказательства основной теоремы алгебры, построил теорию комплексных чисел. Он исследовал уравнения $x^n - 1 = 0$, установил связь между методами решения этих уравнений и построением правильных многоугольников. Нашёл все значения n, для которых правильный n-угольник можно построить циркулем и линейкой. В частности, Гаусс дал построение правильного 17-угольника с помощью циркуля и линейки. В 1818 г. Гаусс пришёл к мысли о возможности построения неевклидовой геометрии. Опасаясь, что его идеи не будут поняты, он далее не разрабатывал их и не публиковал.

Деки́нд (Dedekind) Рихард Юлиус Вильгельм (1831–1916).
Немецкий математик, член Берлинской академии наук (1880). Учился у Гаусса и Дирихле в Гёттингенском университете. Основные работы относятся к теории алгебраических чисел. Создал ряд общих концепций, лежащих в основе современной алгебры, в частности ему принадлежит современное определение идеала. Дедекинд известен также как автор одной из первых систем строгого обоснования теории действительных чисел.

Декарт (Descartes) Рене (1596–1650).
Французский математик, философ, физик, физиолог. Образование получил в иезуитском колледже Ла-Флеш в Анжу (1604–1612), затем самостоятельно изучал математику и другие науки. В 1617–1621 гг. служил в армии и несколько лет путешествовал по Европе. В 1629 г. переехал в Нидерланды,

где провёл двадцать лет в уединении, занимаясь наукой. В 1649 г. по приглашению шведской королевы переехал в Стокгольм, где вскоре и умер. В сочинении «Геометрия» (1637) Декарт заложил основы аналитической геометрии. Ввёл общепринятые теперь обозначения переменных и искомых величин (x, y, $z, \ldots$), буквенных коэффициентов (a, b, $c, \ldots$), а также степеней (a^3, $x^5, \ldots$). Декарт положил начало исследованиям свойств алгебраических уравнений, сформулировал положение о том, что число действительных и комплексных корней уравнения равно его степени, привёл правило знаков для определения числа положительных и отрицательных корней уравнения, поставил вопрос о границах действительных корней.

Евкли́д ($E\upsilon\varkappa\lambda\varepsilon\iota\delta\eta\zeta$) (3 в. до н. э.).
Древнегреческий математик, автор первого из дошедших до нас теоретических трактатов по математике. Биография и сведения нём крайне скудны. Достоверным можно считать лишь то, что его научная деятельность протекала в Александрии в 3 веке до н. э. Его главная работа «Начала» (в латинском переводе — «Элементы») содержит изложение планиметрии, стереометрии и ряда вопросов теории чисел. В ней он подвёл итог предшествующему развитию греческой математики и создал фундамент дальнейшего развития математики. Из других сочинений по математике надо отметить «О делении фигур», сохранившееся в арабском переводе, четыре книги «Конические сечения». Евклид — автор работ по астрономии, оптике, музыке и др.

Капе́лли (Capelli) Альфредо (1855–1910).
Итальянский математик, член Национальной академии деи Линчей в Риме (1901). Родился в Милане, учился в университетах Рима и Павии. В Берлинском университете слушал лекции Вейерштрасса и Кронекера. Был профессором математики университета в Палермо (1881) и Неаполитанского университета (1886). Его лекции по алгебре (1895) при жизни автора выдержали четыре издания.

Краме́р (Cramér) Габриель (1704–1752).
Швейцарский математик. Родился и получил образование в Женеве. С 1724 г. преподавал математику в Женевской кальвинистской академии (с 1734 г. — профессор). Основные направления исследований — высшая алгебра и аналитическая геометрия. Заложил основы теории определителей, установил правило решения систем n линейных уравнений с n неизвестными, исследовал алгебраические линии высших порядков (особые точки, кривизну и т.п.).

Кро́некер (Kronecker) Леопольд (1823–1891).
Немецкий математик, член Берлинской (1861), член-корреспондент Петербургской Академий (1872). Окончил Берлинский университет (1845), там же преподавал. Основные работы относятся к алгебре, теории чисел. Был сторонником «арифметизации» математики, которая (математика), по его мнению, должна быть сведена к арифметике целых чисел.

Ле́йбниц (Leibniz) Готфрид Вильгельм (1646–1716).
Немецкий философ, математик, физик, юрист, теолог, языковед. В 1672–1676 гг. — в Париже. С 1676 г. — на службе у ганноверских герцогов. Основатель и президент (с 1700 г.) Бранденбургского научного общества (Берлинская академия наук). По просьбе Петра I разработал проекты развития образования и государственного управления в России. Один из создателей дифференциального и интегрального исчислений, автор учения о прирождённой способности ума к познанию высших категорий бытия и всеобщих и необходимых истин логики и математики.

Де Мо́рган (De Morgan) Огастес (1806–1871).
Шотландский математик и логик. Профессор математики Университетского колледжа в Лондоне; первый президент (1866) Лондонского математического общества. Известны его работы по теории рядов, а также историко-математические и историко-физические исследования. Основные результаты сформулированы в сочинении «Формальная логика» (1847), где он изложил элементы логики высказываний и логики классов, дал первую развитую систему алгебры отношений.

Де Муавр (Moivre) Абрахам (1667–1754).
Английский математик, по происхождению француз. Член Лондонского королевского общества (1697), а также член Парижской и Берлинской академий наук. Нашёл правила возведения в n-ю степень и извлечения корня n-й степени для комплексных чисел. Исследовал степенные ряды, названные им возвратными; первый пользовался возведением в степень бесконечных рядов. Муавру и Дж. Стирлингу принадлежит асимптотическое представление $n!$, носящее название формулы Стирлинга. В теории вероятностей доказал частный случай так называемой теоремы Лапласа.

Пифаго́р ($P\upsilon\theta\alpha\gamma o\rho\alpha\zeta$) Самосский (ок. 570 –ок. 500 до н. э.).
Древнегреческий мыслитель, религиозный и политический деятель, основатель пифагореизма. Скудные сведения о его жизни и учении трудно отделить от легенд, представляющих Пифагора как полубога, совершенного мудреца,

наследника всей античной и ближневосточной науки, чудотворца и мага. Покинул родной остров Самос в знак протеста против тирании Поликрата. В зрелом возрасте (по преданию, на 40-м году жизни) поселился в южноиталийском г. Кротоне, где основал закрытое сообщество своих последователей, уже при жизни почитавших его как высшее существо. В области математики Пифагору приписывается систематическое введение доказательств в геометрию, построение планиметрии прямолинейных фигур, создание учения о подобии, доказательство теоремы, носящей его имя, построение некоторых правильных многоугольников и многогранников. С именем Пифагора связывают также учение о чётных и нечётных, простых и составных, о фигурных и совершенных числах, об арифметических, геометрических и гармонических пропорциях и средних.

Ферма́ (Fermat) Пьер (1601–1665).
Французский математик. По профессии юрист, с 1631 г. работал советником Кассационной палаты парламента в Тулузе. Математикой занимался в свободное время, при жизни почти ничего не опубликовал. Полученные им математические результаты становились известными учёным благодаря переписке и личному общению. Ферма — один из создателей теории чисел, в которой с его именем связаны две теоремы: великая теорема Ферма (для любого натурального $n > 2$ уравнение $x^n + y^n = z^n$ не имеет решений в целых положительных числах x, y, z) и малая теорема Ферма (если p — простое число и a — целое число, не делящееся на p, то $a^{p-1} - 1$ делится на p). Ферма наряду с Декартом является основоположником аналитической геометрии. Предложил правило нахождения экстремумов, а также общие правила дифференцирования и интегрирования степенной функции, которые затем распространил на случаи дробных и отрицательных показателей. Также занимался вопросами физики.

Эйлер (Euler) Леонард (1707–1783).
Выдающийся математик, внёсший значительный вклад в развитие математики, а также механики, физики, астрономии и ряда прикладных наук. Эйлер — автор свыше 800 работ по математическому анализу, дифференциальной геометрии, теории чисел, приближенным вычислениям, небесной механике, математической физике, оптике, баллистике, кораблестроению, теории музыки и др., оказавших значительное влияние на развитие науки. В 1726 г. был приглашён работать в Санкт-Петербург, в 1727 г. переехал жить в Россию. В 1731–1741 гг. и, начиная с 1766 г., был академиком Петербургской академии наук (в 1741–1766 гг. работал в Берлине, оставаясь почётным членом Петербургской академии).

Греческий алфавит

Буква	Название
A, α	альфа
B, β	бета
Γ, γ	гамма
Δ, δ	дельта
E, ε	эпсилон
Z, ζ	дзета
H, η	эта
θ, θ	тета
I, ι	иота
K, κ	каппа
Λ, λ	ламбда
M, μ	ми (мю)
N, ν	ни (ню)
Ξ, ξ	кси
O, o	омикрон
Π, π	пи
P, ρ	ро
Σ, σ	сигма
T, τ	тау
Υ, υ	ипсилон
Φ, φ	фи
X, χ	хи
Ψ, ψ	пси
Ω, ω	омега

Готические алфавит

Готическая буква	Латинская буква
$\mathfrak{A}, \mathfrak{a}$	A,a
$\mathfrak{B}, \mathfrak{b}$	B,b
$\mathfrak{C}, \mathfrak{c}$	C,c
$\mathfrak{D}, \mathfrak{d}$	D,d
$\mathfrak{E}, \mathfrak{e}$	E,e
$\mathfrak{F}, \mathfrak{f}$	F,f
$\mathfrak{G}, \mathfrak{g}$	G,g
$\mathfrak{H}, \mathfrak{h}$	H,h
$\mathfrak{I}, \mathfrak{i}$	I,i
$\mathfrak{J}, \mathfrak{j}$	J,j
$\mathfrak{K}, \mathfrak{k}$	K,k
$\mathfrak{L}, \mathfrak{l}$	L,l
$\mathfrak{M}, \mathfrak{m}$	M,m
$\mathfrak{N}, \mathfrak{n}$	N,n
$\mathfrak{O}, \mathfrak{o}$	O,o
$\mathfrak{P}, \mathfrak{p}$	P,p
$\mathfrak{Q}, \mathfrak{q}$	Q,q
$\mathfrak{R}, \mathfrak{r}$	R,r
$\mathfrak{S}, \mathfrak{s}$	S,s
$\mathfrak{T}, \mathfrak{t}$	T,t
$\mathfrak{U}, \mathfrak{u}$	U,u
$\mathfrak{V}, \mathfrak{v}$	V,v
$\mathfrak{W}, \mathfrak{v}$	W,w
$\mathfrak{X}, \mathfrak{x}$	X,x
$\mathfrak{Y}, \mathfrak{y}$	Y,y
$\mathfrak{Z}, \mathfrak{z}$	Z,z

Литература

1. Ван дер Варден Б.Л. Алгебра. / Пер. с нем. Ю.И. Мерзлякова.—М.:Наука, 1976.
2. Веселов А.П., Троицкий Е.В. Лекции по аналитической геометрии.—СПб.: Лань, 2003.
3. Википедия. Электронная энциклопедия. `http://ru.wikipedia.org`
4. Гашков С.Б. Системы счисления и их применение.—М.: МЦНМО, 2004.
5. Клиот-Дашинский М.И. Алгебра матриц и векторов.—СПб.: Лань, 2001.
6. Письменный Д. Конспект лекций по высшей математике.—М.: Айрис-пресс, 2005.
7. Черемушкин А.В. Лекции по арифметическим алгоритмам и криптографии.—М.: МЦНМО, 2002.

Предметный указатель