Л. Я. ОКУНЕВ

ВЫСШАЯ АЛГЕБРА

ИЗДАНИЕ ТРЕТЬЕ, ПЕРЕРАБОТАННОЕ

Допущено Всесоюзным комитетом по делам высшей школы при СНК СССР в качестве учебника для физико-математических факультетов университетов и педвузов

ОГИЗ
ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1944 ЛЕНИНГРАД


ИЗДАНИЯ ВОЕННЫХ ЛЕТ
1941-1945

ПРЕДИСЛОВИЕ К ТРЕТЬЕМУ ИЗДАНИЮ

Изменения, сделанные в третьем издании, вызваны, в основном, стремлением приблизить содержание книги к программам педагогических институтов при сохранении основного назначения книги как университетского учебника.

Наиболее существенные изменения состоят в следующем:

Глава I. Упрощено доказательство теоремы в § 11 и выброшен § 12 (II изд.).

Глава II. Дано более простое доказательство теоремы в § 17 (II изд. § 18) и добавлен § 19, посвящённый теории линейных уравнений в векторной форме.

Глава V. Исключена теория рациональных чисел.

Глава VI. Опущены интерполяционные формулы Лагранжа и Ньютона (II изд. § 36) и метод Кронекера (часть § 37 во II изд.).

Глава VIII. Добавлен § 46. Теорема Фробениуса. Этот параграф не требуется университетской программой. Его следует рассматривать как хороший пример к теории гиперкомплексных чисел. Теорема Фробениуса является логическим завершением теории комплексных чисел.

Глава IX. В § 48 (во II изд. § 51) исключено изложение идей доказательства Руффини и доказательства Абеля о невозможности алгебраического решения уравнений выше 4-й степени.

Глава X. Добавлен новый § 52. Преобразование Чирнгаузена.

Сохранена глава XI, несмотря на то, что её содержание выходит за пределы университетской программы. Эта глава, во-первых, содержит хороший иллюстративный материал к изложенному курсу алгебры. Во-вторых, она представляет интерес для преподавателей средней школы, которым приходится делать построения только циркулем и линейкой, так как она определяет круг задач, решение которых возможно геометрическим путём с применением только циркуля и линейки.

Л. Я. Окунев

ОГЛАВЛЕНИЕ

ГЛАВА ЧЕТВЁРТАЯ

Квадратичные формы

ГЛАВА ПЯТАЯ

Числа и общая теория многочленов

ГЛАВА ШЕСТАЯ

Кольцо многочленов в поле рациональных чисел

ГЛАВА СЕДЬМАЯ

Кольцо многочленов в поле действительных чисел

ГЛАВА ВОСЬМАЯ

Комплексные числа и основная теорема алгебры

ГЛАВА ДЕВЯТАЯ

Алгебраическое решение уравнений

ГЛАВА ДЕСЯТАЯ

Теория исключения

ГЛАВА ОДИННАДЦАТАЯ

Построения с помощью циркуля и линейки

ГЛАВА ПЕРВАЯ

ТЕОРИЯ ОПРЕДЕЛИТЕЛЕЙ

§ 1. Определители второго порядка

Мы начинаем курс высшей алгебры с теории определителей, потому что эта теория имеет важное значение как в алгебре, так и в других математических дисциплинах, например, в аналитической геометрии. Как мы увидим ниже, понятие определителя тесно связано с общей теорией уравнений первой степени со многими неизвестными.

Простейшим случаем уравнений первой степени, или, как мы будем постоянно выражаться, линейных уравнений, является уравнение с одним неизвестным. Из элементарной алгебры мы знаем, что всякое уравнение первой степени с одним неизвестным можно привести к виду

$$ax = b. \tag{1}$$

Если $a \neq 0$, то, разделив обе части уравнения (1) на a, получим единственное решение, или, как иногда говорят, корень уравнения: $x = \frac{b}{a}$. В случае $a = 0$ и $b \neq 0$ уравнение (1) не может иметь решений, так как, очевидно, всякое число x, умноженное на нуль, должно было бы дать нуль. Наконец, если $a = 0$ и $b = 0$, то любое число будет удовлетворять уравнению (1); таким образом в этом случае рассматриваемое уравнение будет иметь бесконечное множество корней.

Несколько сложнее случай двух уравнений с двумя неизвестными:

$$\left.\begin{aligned} a_1x + b_1y &= c_1, \\ a_2x + b_2y &= c_2. \end{aligned}\right\} \tag{2}$$

Умножим первое уравнение системы (2) на b_2, а второе на b_1 и затем вычтем из первого уравнения второе. Получим тогда:

$$(a_1b_2 - a_2b_1)\,x = c_1b_2 - c_2b_1. \tag{3}$$

Подобным же образом исключая x, получим

$$(a_1b_2 - a_2b_1)\,y = a_1c_2 - a_2c_1. \tag{4}$$

Если выражение $a_1b_2 - a_2b_1$ не равно нулю, то, разделив обе части уравнений (3) и (4) на $a_1b_2 - a_2b_1$, получим единственное решение системы (2):

$$x = \frac{c_1b_2 - c_2b_1}{a_1b_2 - a_2b_1}; \quad y = \frac{a_1c_2 - a_2c_1}{a_1b_2 - a_2b_1}. \tag{5}$$

Формулы (5) полезны в том отношении, что с их помощью можно сразу решить линейную систему двух уравнений с двумя неизвестными.

Пример. В качестве примера возьмём систему уравнений:

$$2x - 5y = 1,$$
$$3x + y = 4.$$

По формулам (5) сразу получаем корни:

$$x = \frac{1 \cdot 1 - 4 \cdot (-5)}{2 \cdot 1 - 3 \cdot (-5)} = \frac{1 + 20}{2 + 15} = \frac{21}{17},$$
$$y = \frac{2 \cdot 4 - 3 \cdot 1}{2 \cdot 1 - 3 \cdot (-5)} = \frac{8 - 3}{2 + 15} = \frac{5}{17}.$$

До сих пор мы ограничивались случаем $a_1b_2 - a_2b_1 \neq 0$; но при некоторых значениях коэффициентов системы (2) может оказаться, что $a_1b_2 - a_2b_1 = 0$. Тогда формулы (5) применять нельзя, так как деление на нуль невозможно. Легко убедиться на примерах, что в случае $a_1b_2 - a_2b_1 = 0$ система (2) либо противоречива, либо имеет бесчисленное множество решений.

Например, система уравнений:

$$\begin{aligned} x + y &= 1, \\ 2x + 2y &= 1 \end{aligned} \qquad (a_1b_2 - a_2b_1 = 1 \cdot 2 - 2 \cdot 1 = 0)$$

противоречива; так как левая часть второго уравнения вдвое больше левой части первого уравнения, а правые части одинаковы.

Система уравнений:

$$\begin{aligned} 2x + y &= 2, \\ 4x + 2y &= 4 \end{aligned} \qquad (a_1b_2 - a_2b_1 = 2 \cdot 2 - 4 \cdot 1 = 0)$$

допускает бесчисленное множество решений, так как второе уравнение есть следствие первого.

Вернёмся теперь к дробям (5) и установим, по какому закону они составлены.

Напишем следующую табличку коэффициентов при неизвестных системы (2):

$$\begin{matrix} a_1 & b_1 \\ a_2 & b_2 \end{matrix} \tag{A}$$

Мы эту табличку будем называть *матрицей*, а коэффициенты a_1, b_1, a_2, b_2 — её *элементами*. В первой строке этой матрицы идут коэффициенты первого уравнения, а во второй — коэффициенты второго уравнения. Составим два произведения «крест-накрест»:

a_1b_2 и a_2b_1. Если из первого произведения вычесть второе, то как раз и получится общий знаменатель дробей (5):

$$D = a_1b_2 - a_2b_1.$$

Это выражение называется *определителем* (или *детерминантом*) второго порядка, составленным из чисел матрицы (A); числа a_1, a_2, b_1, b_2 называются *элементами* определителя. Определитель D принято обозначать следующим символом:

$$D = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = a_1b_2 - a_2b_1.$$

Теперь нетрудно подметить общий закон составления числителей дробей (5). Числитель икса получается из знаменателя заменой коэффициентов a_1 и a_2 свободными членами уравнения: c_1 и c_2. Точно так же числитель игрека получается из знаменателя путём замены коэффициентов b_1 и b_2 свободными членами c_1 и c_2. Так как, согласно введённому обозначению

$$c_1b_2 - c_2b_1 = \begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix},$$

$$a_1c_2 - a_2c_1 = \begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix},$$

то формулы (5) принимают следующий окончательный вид:

$$x = \frac{\begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}}; \quad y = \frac{\begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}}. \tag{5'}$$

Пример. Рассмотрим систему уравнений:

$$5x - 3y = 7,$$
$$2x - 5y = 1.$$

Прежде всего составляем определитель системы:

$$D = \begin{vmatrix} 5 & -3 \\ 2 & -5 \end{vmatrix} = 5 \cdot (-5) - 2 \cdot (-3) = -19.$$

Далее составляем числитель для x, для чего первый столбец определителя D надо заменить свободными членами 7 и 1. Имеем после такой замены:

$$D_1 = \begin{vmatrix} 7 & -3 \\ 1 & -5 \end{vmatrix} = 7 \cdot (-5) - 1 \cdot (-3) = -32.$$

Подобным же образом, заменяя в D второй столбец свободными членами, получим определитель

$$D_2 = \begin{vmatrix} 5 & 7 \\ 2 & 1 \end{vmatrix} = 5 \cdot 1 - 2 \cdot 7 = -9.$$

Так как $D \neq 0$, то по формулам (5) получаем:

$$x = \frac{D_1}{D} = \frac{-32}{-19} = \frac{32}{19}, \quad y = \frac{D_2}{D} = \frac{-9}{-19} = \frac{9}{19}.$$

§ 2. Определители третьего порядка

Попробуем теперь решить систему уравнений

$$\left.\begin{aligned} a_1x + b_1y + c_1z &= d_1, \\ a_2x + b_2y + c_2z &= d_2, \\ a_3x + b_3y + c_3z &= d_3 \end{aligned}\right\} \qquad (1)$$

с тремя неизвестными, для чего воспользуемся хотя и искусственным, но зато быстро приводящим к цели способом.

Умножим первое уравнение на $b_2c_3 - b_3c_2$, второе на $b_3c_1 - b_1c_3$ и третье на $b_1c_2 - b_2c_1$; затем все три уравнения сложим почленно. Будем иметь:

$$\begin{aligned} &(a_1b_2c_3 - a_1b_3c_2 + a_2b_3c_1 - a_2b_1c_3 + a_3b_1c_2 - a_3b_2c_1)\,x + \\ &+ (b_1b_2c_3 - b_1b_3c_2 + b_2b_3c_1 - b_2b_1c_3 + b_3b_1c_2 - b_3b_2c_1)\,y + \\ &+ (c_1b_2c_3 - c_1b_3c_2 + c_2b_3c_1 - c_2b_1c_3 + c_3b_1c_2 - c_3b_2c_1)\,z = \\ &= d_1b_2c_3 - d_1b_3c_2 + d_2b_3c_1 - d_2b_1c_3 + d_3b_1c_2 - d_3b_2c_1. \end{aligned}$$

Легко заметить, что члены, стоящие в скобках при y и z; взаимно уничтожаются; таким образом неизвестные y и z пропадают, и мы получаем:

$$\begin{aligned} &(a_1b_2c_3 - a_1b_3c_2 + a_2b_3c_1 - a_2b_1c_3 + a_3b_1c_2 - a_3b_2c_1)\,x = \\ &= (d_1b_2c_3 - d_1b_3c_2 + d_2b_3c_1 - d_2b_1c_3 + d_3b_1c_2 - d_3b_2c_1). \end{aligned} \qquad (2)$$

В левой части уравнения (2) коэффициентом при x служит несколько громоздкое выражение

$$D = a_1b_2c_3 - a_1b_3c_2 + a_2b_3c_1 - a_2b_1c_3 + a_3b_1c_2 - a_3b_2c_1, \qquad (3)$$

которое мы будем называть *определителем* (или *детерминантом*) *третьего порядка*; числа a_1, a_2, a_3; b_1; ...; c_1;...; входящие в D, будем называть *элементами* этого определителя. Определитель третьего порядка принято обозначать так:

$$D = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

Постараемся теперь разобраться в структуре этого определителя. Существует следующая закономерность, называемая *правилом Саррюса*.

Проведём по схеме 1 «левую» главную диагональ $a_1b_2c_3$; идущую слева вниз; и «правую» главную диагональ $c_1b_2a_3$; идущую

справа вниз. Кроме двух главных диагоналей можно провести ещё четыре «неполные» диагонали b_1c_2; a_2b_3; b_1a_2 и c_2b_3. Условимся называть неполную диагональ «левой»; если она параллельна левой главной диагонали; и «правой»; если она параллельна правой главной диагонали. Легко видеть; что произведение $a_1b_2c_3$ элементов левой главной диагонали входит в определитель D со знаком плюс, а произведение $a_3b_2c_1$ элементов правой главной диагонали — со знаком минус. Каждое из остальных четырёх слагаемых определителя D представляет собою

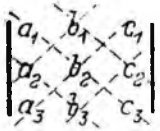


Схема 1.

произведение из трёх элементов, причём два элемента находятся на неполной диагонали, а третий элемент — в противоположном углу. Это произведение берётся со знаком плюс в случае левой неполной диагонали и со знаком минус в случае правой неполной диагонали. Например, одна из неполных диагоналей проходит через a_2 и b_1; в противоположном углу находится элемент c_3; поэтому получаем произведение $a_2b_1c_3$, которое следует взять со знаком минус, так как элементы a_2; b_1 лежат на правой диагонали.

Пример. Вычислим определитель

$$D=\begin{vmatrix}1&2&3\\2&2&1\\3&1&2\end{vmatrix}.$$

Воспользуемся правилом Саррюса; тогда

$$D=1\cdot2\cdot2+2\cdot1\cdot3+3\cdot2\cdot1-3\cdot2\cdot3-2\cdot2\cdot2-1\cdot1\cdot1=-11.$$

Посмотрим теперь, что представляет собой выражение, стоящее в правой части уравнения (2). Оказывается, что оно есть также определитель третьего порядка, а именно:

$$D_1=\begin{vmatrix}d_1&b_1&c_1\\d_2&b_2&c_2\\d_3&b_3&c_3\end{vmatrix}.$$

Поэтому уравнение (2) принимает следующий вид:

$$\begin{vmatrix}a_1&b_1&c_1\\a_2&b_2&c_2\\a_3&b_3&c_3\end{vmatrix}\cdot x=\begin{vmatrix}d_1&b_1&c_1\\d_2&b_2&c_2\\d_3&b_3&c_3\end{vmatrix}. \qquad (4)$$

Можно показать, что неизвестные y и z удовлетворяют уравнениям:

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} \cdot y = \begin{vmatrix} a_1 & d_1 & c_1 \\ a_2 & d_2 & c_2 \\ a_3 & d_3 & c_3 \end{vmatrix}. \tag{5}$$

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} \cdot z = \begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix}. \tag{6}$$

В самом деле, если первое уравнение системы (1) умножить на $a_3c_2 - a_2c_3$, второе на $a_1c_3 - a_3c_1$, третье на $a_2c_1 - a_1c_2$ и затем почленно сложить эти уравнения, то мы придём к уравнению (5).

Если же, наконец, первое уравнение системы (1) умножить на $a_2b_3 - a_3b_2$, второе на $a_3b_1 - a_1b_3$, третье на $a_1b_2 - a_2b_1$ и затем почленно сложить эти уравнения, то получится уравнение (6).

Пусть определитель D отличен от нуля; тогда уравнения (4); (5) и (6) можно решить относительно x, y, z:

$$x = \frac{\begin{vmatrix} d_1 & b_1 & c_1 \\ d_2 & b_2 & c_2 \\ d_3 & b_3 & c_3 \end{vmatrix}}{D}, \quad y = \frac{\begin{vmatrix} a_1 & d_1 & c_1 \\ a_2 & d_2 & c_2 \\ a_3 & d_3 & c_3 \end{vmatrix}}{D}, \quad z = \frac{\begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix}}{D}.$$

Мы приходим к следующей теореме:

Если определитель D, составленный из коэффициентов системы (1), отличен от нуля, то система допускает единственное решение; каждое из неизвестных равно при этом дроби, знаменатель которой есть D, а числитель есть определитель, получающийся из D путём замены столбца из коэффициентов рассматриваемого неизвестного столбцом из свободных членов d_1, d_2, d_3.

Пример. Решим с помощью определителей систему

$$\begin{aligned} 2x_1 - 4x_2 + x_3 &= 1, \\ x_1 - 5x_2 + 3x_3 &= 2, \\ x_1 - x_2 + x_3 &= -1. \end{aligned}$$

Прежде всего вычислим D:

$$D = \begin{vmatrix} 2 & -4 & 1 \\ 1 & -5 & 3 \\ 1 & -1 & 1 \end{vmatrix} = 2 \cdot (-5) \cdot 1 + (-4) \cdot 3 \cdot 1 + 1 \cdot (-1) \cdot 1 - 1 \cdot (-5) \cdot 1 - (-4) \cdot 1 \cdot 1 - (-1) \cdot 3 \cdot 2 = -8.$$

$D \neq 0$, следовательно, система допускает решение и притом единственное. Вычисляем теперь остальные три определителя:

$$D_1 = \begin{vmatrix} 1 & -4 & 1 \\ 2 & -5 & 3 \\ -1 & -1 & 1 \end{vmatrix} = 1 \cdot (-5) \cdot 1 + (-4) \cdot 3 \cdot (-1) + 2 \cdot (-1) \cdot 1 - (-1) \cdot (-5) \cdot 1 - (-1) \cdot 3 \cdot 1 - 2 \cdot (-4) \cdot 1 = 11.$$

$$D_2=\begin{vmatrix}2 & 1 & 1\\ 1 & 2 & 3\\ 1 & -1 & 1\end{vmatrix}=2\cdot 2\cdot 1+1\cdot 3\cdot 1+1\cdot(-1)\cdot 1-1\cdot 2\cdot 1-$$
$$-(-1)\cdot 3\cdot 2-1\cdot 1\cdot 1=9.$$

$$D_3=\begin{vmatrix}2 & -4 & 1\\ 1 & -5 & 2\\ 1 & -1 & -1\end{vmatrix}=2\cdot(-5)\cdot(-1)+(-4)\cdot 2\cdot 1+1\cdot(-1)\cdot 1-$$
$$-1\cdot(-5)\cdot 1-(-1)\cdot 2\cdot 2-1\cdot(-4)\cdot(-1)=6.$$

Итак:

$$x_1=\frac{D_1}{D}=-\frac{11}{8},\quad x_2=\frac{D_2}{D}=-\frac{9}{8},\quad x_3=\frac{D_3}{D}=-\frac{6}{8}=-\frac{3}{4}.$$

В качестве контроля можно найденные значения неизвестных подставить в уравнения, легко убедиться, что система решена правильно.

Задачи. 1. Вычислить значения следующих определителей второго порядка:

$$\begin{vmatrix}1 & 1\\ 2 & 3\end{vmatrix},\quad \begin{vmatrix}3 & 5\\ 6 & 8\end{vmatrix},\quad \begin{vmatrix}5 & 10\\ 2 & 4\end{vmatrix}.$$

2. Вычислить значения определителей:

$$\begin{vmatrix}a^2 & ab\\ ab & b^2\end{vmatrix},\quad \begin{vmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{vmatrix},\quad \begin{vmatrix}1+t^2 & 2t\\ 1-t^2 & 1-t^2\\ \hline 2t & 1+t^2\\ t^2-1 & t^2-1\end{vmatrix}.$$

3. Проверить справедливость следующих тождеств:

a) $\begin{vmatrix}a+a_1 & b+b_1\\ c & d\end{vmatrix}=\begin{vmatrix}a & b\\ c & d\end{vmatrix}+\begin{vmatrix}a_1 & b_1\\ c & d\end{vmatrix}$,

b) $\begin{vmatrix}a+a_1 & b\\ c+c_1 & d\end{vmatrix}=\begin{vmatrix}a & b\\ c & d\end{vmatrix}+\begin{vmatrix}a_1 & b\\ c_1 & d\end{vmatrix}$,

c) $\begin{vmatrix}aa_1+bc_1 & ab_1+bd_1\\ a_1c+c_1d & b_1c+dd_1\end{vmatrix}=\begin{vmatrix}a & b\\ c & d\end{vmatrix}\cdot\begin{vmatrix}a_1 & b_1\\ c_1 & d_1\end{vmatrix}$,

d) $a_1\begin{vmatrix}b_1 & c_1\\ b_2 & c_2\end{vmatrix}-b_1\begin{vmatrix}a_1 & c_1\\ a_2 & c_2\end{vmatrix}+c_1\begin{vmatrix}a_1 & b_1\\ a_2 & b_2\end{vmatrix}=0$,

e) $a_1\begin{vmatrix}b_2 & c_2\\ b_3 & c_3\end{vmatrix}-b_1\begin{vmatrix}a_2 & c_2\\ a_3 & c_3\end{vmatrix}+c_1\begin{vmatrix}a_2 & b_2\\ a_3 & b_3\end{vmatrix}=\begin{vmatrix}a_1 & b_1 & c_1\\ a_2 & b_2 & c_2\\ a_3 & b_3 & c_3\end{vmatrix}$.

4. **С помощью определителей второго порядка решить следующие системы уравнений:**

a) $5u+2v=3,$
$11u-7v=1.$

b) $x\cos\alpha-y\sin\alpha=a,$
$x\sin\alpha+y\cos\alpha=b,$

c) $5x-y=0,$
$x-2y=0.$

5. С помощью правила Саррюса вычислить следующие определители третьего порядка:

$$\begin{vmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & 1 & 1 \\ 3 & 1 & 4 \\ 8 & 9 & 5 \end{vmatrix}, \quad \begin{vmatrix} 0 & a & 0 \\ b & 0 & c \\ 0 & d & 0 \end{vmatrix}, \quad \begin{vmatrix} 0 & -a & -b \\ a & 0 & -c \\ b & c & 0 \end{vmatrix}.$$

6. Показать, что

$$\begin{vmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{vmatrix} = (b-a)(c-a)(c-b).$$

7. Распространить тождества *a*), *b*), *d*) задачи 3 на определители третьего порядка.

8. С помощью определителей третьего порядка решить следующие системы уравнений.

a) $\begin{aligned} x+y-2z &= -3, \\ 5x-2y+7z &= 22, \\ 2x-5y+4z &= 4. \end{aligned}$ b) $\begin{aligned} bx-ay &= -2ab, \\ -2cy+3bz &= bc, \\ cx+az &= 0. \end{aligned}$

§ 3. Определители высших порядков

Изучение структуры определителей второго и третьего порядка даёт возможность ввести понятие об определителе любого порядка и решать с помощью этих определителей системы линейных уравнений, содержащих любое число неизвестных.

Для обозначения элементов определителя введём так называемую *систему двойных индексов*: каждый из элементов определителя обозначим одной и той же буквой a с двумя индексами внизу; первый индекс будет указывать номер строки, а второй—номер столбца, занимаемого элементом. Например, в определителе

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

элемент c_2 занимает вторую строку и третий столбец, поэтому мы его обозначим через a_{23}.

Определители второго и третьего порядка в новом обозначении будут выглядеть так:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}, \tag{1}$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}. \tag{2}$$

Ниже мы увидим, насколько плодотворна подобная система обозначений.

Отвлечёмся несколько в сторону и займёмся на первый взгляд посторонними вещами.

Пусть дано n цифр $1, 2, \ldots, n$. Из элементарной алгебры известно, что из этих n цифр можно составить $1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ перестановок. Произведение $1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ принято сокращённо обозначать через $n!$ и называть «n факториал».

Например из трёх цифр 1, 2, 3 можно составить всего $3! = 1 \cdot 2 \cdot 3 = 6$ перестановок: 123, 132, 312, 321, 231, 213.

Среди написанных шести перестановок выделяется первая, 123, — в ней цифры идут в натуральном порядке; в остальных перестановках порядок нарушен. Возьмём, например, расположение 132; мы видим, что цифра 3 стоит впереди цифры 2. Такое явление, когда бо́льшая цифра находится впереди меньшей, называется *беспорядком*, или *инверсией*. Итак, в расположении 132 наблюдается лишь одна инверсия. Рассматривая далее 312, находим, что 312 имеет уже две инверсии: 3 стоит впереди 2 и 3 — впереди 1. Перестановка 321 содержит три инверсии и т. д. Таким образом получается следующая табличка:

Перестановка	Число инверсий
123	инверсий нет
132	одна инверсия
312	две инверсии
321	три инверсии
231	две инверсии
213	одна инверсия

Подсчёт числа инверсий удобнее всего выполнять следующим образом: прежде всего находим, сколько цифр стоит впереди 1; затем 1 вычёркиваем и подсчитываем, сколько цифр стоит впереди 2 (не считая зачёркнутой единицы); после этого вычёркиваем 2 и подсчитываем, сколько цифр стоит впереди 3 (зачёркнутые цифры не считаются), и т. д. Пусть впереди 1 было m_1 цифр, впереди 2 было m_2 цифр и т. д., наконец, впереди n было m_n цифр. Тогда общее число инверсий равно $m_1 + m_2 + \ldots + m_n$.

Пример. Подсчитаем, сколько инверсий имеется в перестановке 531246.

Впереди 1 стоят две цифры (5 и 3). Зачёркиваем 1: 531246.

Впереди 2 стоят две цифры (5 и 3). Зачёркиваем 2: 531246.

Впереди 3 стоит одна цифра (5). Зачёркиваем 3: 531246.

Впереди 4 стоит одна цифра (5). Зачёркиваем 4: 531246.

Впереди 5 ничего не стоит. Зачёркиваем 5: 531246. Наконец впереди 6 также ничего не стоит (всё вычеркнуто). Следовательно, искомое число инверсий равно шести: $2 + 2 + 1 + 1 + 0 + 0 = 6$.

Вернёмся к определителю (1) второго порядка. Члены разложения в правой части (1) нарочно написаны так, что первые индексы букв идут в натуральном порядке. Что касается вторых индексов, то они образуют всевозможные перестановки из двух цифр 1 и 2, а именно 12 и 21. Первому расположению цифр отвечает член $a_{11}a_{22}$, взятый со знаком плюс, а второму — член $a_{12}a_{21}$, взятый со знаком минус. Мы видим, что член берётся со знаком плюс, когда среди его вторых индексов букв наблюдается чётное число инверсий, и со знаком минус при нечётном числе инверсий (нуль считается числом чётным). Заметим ещё, что каждый член содержит один и

только один элемент из каждой строки и каждого столбца определителя.

По отношению к определителю (2) третьего порядка подмеченная закономерность остаётся в силе: первые индексы букв в каждом члене расположены в натуральном порядке; вторые индексы образуют $3! = 6$ всевозможных перестановок из трёх цифр 1, 2, 3 (123, 231, 312, 321, 213, 132); члены с чётным числом инверсий во вторых индексах букв имеют знак плюс; с нечётным числом инверсий знак минус. Наконец, каждый член содержит один и только один элемент из каждой строки и каждого столбца определителя.

Оказывается, что подмеченную закономерность можно положить в основу обобщения понятия определителя.

Пусть n^2 величин a_{ij} расположены в виде следующей квадратной таблицы:

$$\begin{matrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \dots & a_{nn}. \end{matrix} \qquad (A)$$

Назовём таблицу (A) *матрицей*; а входящие в неё величины *элементами* матрицы и введём следующее определение.

Определение. *Определителем* (или *детерминантом*) *n-го порядка из n^2 элементов матрицы* (A) *называется алгебраическая сумма n членов; каждый член есть произведение n элементов, взятых по одному и только по одному из каждой строки и каждого столбца матрицы. Знак члена равен $(-1)^t$, где t—число инверсий во вторых индексах, когда элементы члена расположены в порядке возрастания первых индексов.*

Таким образом член имеет знак плюс при чётном t и минус при нечётном t.

Определитель n-го порядка принято обозначать символом:

$$D = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}\ ^{1}).$$

Этот символ введён известным английским математиком XIX столетия—Кэли (A. Cayley, 1821—1895).

Пример 1. Найдём, чему равен определитель четвёртого порядка у которого все элементы, кроме $a_{11}, a_{14}, a_{22}, a_{23}, a_{32}, a_{33}, a_{41}$ и a_{44}, равны нулю. Такой определитель имеет вид:

$$D = \begin{vmatrix} a_{11} & 0 & 0 & a_{14} \\ 0 & a_{22} & a_{23} & 0 \\ 0 & a_{32} & a_{33} & 0 \\ a_{41} & 0 & 0 & a_{44} \end{vmatrix}.$$

[1]) В тех случаях, когда это не может вызвать недоразумений употребляется краткий символ $|a_{ik}|$ для обозначения того же определителя.

Согласно определению D есть алгебраическая сумма $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$ членов, но здесь значительная часть членов равна нулю, и только четыре члена

$$a_{14}a_{22}a_{33}a_{41}, \quad a_{14}a_{23}a_{32}a_{41}, \quad a_{11}a_{22}a_{33}a_{44}, \quad a_{11}a_{23}a_{32}a_{44}$$

отличны от нуля.

Первые индексы написанных членов идут в порядке возрастания; что касается вторых индексов, то они образуют перестановки:

$$4\ 2\ 3\ 1, \quad 4\ 3\ 2\ 1, \quad 1\ 2\ 3\ 4, \quad 1\ 3\ 2\ 4,$$

которые имеют соответственно 5, 6, 0 и 1 инверсий. Следовательно, первый и четвёртый члены надо взять со знаком минус, второй и третий со знаком плюс. Получаем:

$$D = -a_{14}a_{22}a_{33}a_{41} + a_{14}a_{23}a_{32}a_{41} + a_{11}a_{22}a_{33}a_{44} - a_{11}a_{23}a_{32}a_{44}. \quad (3)$$

Если в частности

$$D = \begin{vmatrix} 1 & 0 & 0 & 2 \\ 0 & 3 & 1 & 0 \\ 0 & 1 & 3 & 0 \\ 4 & 0 & 0 & 5 \end{vmatrix},$$

то, подставляя в выражение (3) числовые значения элементов, получим:

$$D = -2 \cdot 3 \cdot 3 \cdot 4 + 2 \cdot 1 \cdot 1 \cdot 4 + 1 \cdot 3 \cdot 3 \cdot 5 - 1 \cdot 1 \cdot 1 \cdot 5 = -24.$$

Пример 2. Найти, при каких значениях i и j член $a_{21}a_{1i}a_{5j}a_{43}a_{32}$ определителя пятого порядка имеет знак минус.

Индексы i и j могут принимать только следующие значения: а) $i=4, j=5$ или б) $i=5, j=4$; так как при других значениях i и j произведение $a_{21}a_{1i}a_{5j}a_{43}a_{32}$ будет содержать по меньшей мере два элемента из одного столбца. Чтобы определить знак члена; надо расположить элементы члена в натуральном порядке первых индексов и затем подсчитать число инверсий во вторых индексах. Перемещая надлежащим образом элементы, получим:

$$a_{1i}a_{21}a_{32}a_{43}a_{5j};$$

первые индексы расположены теперь в порядке возрастания.

Пусть а) $i=4, j=5$. Тогда получим расположение вторых индексов: 4 1 2 3 5; содержащее три беспорядка. Таким образом при $i=4$, $j=5$ член имеет знак минус.

Пусть затем б) $i=5, j=4$. Вторые индексы образуют расположение: 5 1 2 3 4, содержащее четыре беспорядка; следовательно, в этом случае получается знак плюс.

Итак, заданный член имеет знак минус только при $i=4$; $j=5$.

§ 4. Транспозиции

В настоящем и следующем параграфах мы займёмся рассмотрением свойств перестановок, играющих основную роль во всей теории определителей.

В некоторой перестановке

$$a, b, c, \ldots, l$$

из n элементов поменяем местами какие-нибудь два элемента, например, a и c; тогда, очевидно, получится новая перестановка

$$c, b, a, \ldots, l.$$

Подобная операция перемещения двух элементов называется *транспозицией*; мы её обозначим символом (a, c).

В этом параграфе и в следующих за элементы $a, b, c, \ldots, l$ мы будем принимать первые n цифр натурального ряда $1, 2, 3, \ldots, n$.

Легко сообразить, что с помощью транспозиций всегда можно перейти от одной перестановки к любой другой престановке тех же цифр. Возьмём для наглядности конкретный пример: покажем, как с помощью транспозиций перейти от перестановки

$$3, 4, 5, 6, 8, 7, 1, 2 \qquad (A)$$

к перестановке

$$8, 1, 7, 2, 5, 4, 3, 6. \qquad (B)$$

В перестановке (A) на первом месте стоит 3, а в перестановке (B) на первом месте стоит 8; чтобы получить 8 на первом месте, выполним в перестановке (A) транспозицию (3, 8); имеем в результате:

$$8, 4, 5, 6, 3, 7, 1, 2. \qquad (A_1)$$

Теперь сравниваем (A_1) с (B). В (A_1) на втором месте стоит 4, а в (B)—1. После транспозиции (4, 1) перестановка (A_1) перейдёт в перестановку

$$8, 1, 5, 6, 3, 7, 4, 2 \qquad (A_2)$$

с цифрой 1 на втором месте. Дальнейший ход преобразования таков (слева в скобках указаны выполняемые транспозиции):

$$\begin{array}{lll} (5,7) & 8,1, 7, 6, 3, 5, 4, 2 & (A_3) \\ (6,2) & 8,1, 7, 2, 3, 5, 4, 6 & (A_4) \\ (3,5) & 8,1, 7, 2, 5, 3, 4, 6 & (A_5) \\ (3,4) & 8,1, 7, 2, 5, 4, 3, 6. & (B) \end{array}$$

Но роль транспозиций этим не исчерпывается.

Все перестановки из n цифр $1, 2, \ldots, n$ можно разбить на два класса. А именно, назовём перестановку *чётной* (или *чётного класса*), если число её инверсий чётное, и *нечётной* (*нечётного класса*) в противном случае. Например, перестановка 2 3 1 является чётной, так как она имеет две инверсии.

Но если мы выполним в перестановке 2 3 1 транспозицию (2, 3) то получим перестановку 3 2 1 с тремя инверсиями, т. е. нечётную перестановку. Мы видим, что от транспозиции чётность перестановки изменилась. Подмеченное свойство не случайно, так как справедлив следующая теорема:

Теорема I. *От одной транспозиции чётность перестановки меняется.*

Доказательство. Рассмотрим прежде всего тот частный случай, когда транспонируемые цифры i и k находятся рядом, т. е. перестановка имеет вид $AikB$. Буквой A здесь обозначена группа цифр, находящихся влево от i, а буквой B—группа цифр, находящихся вправо от k. После транспозиции (i, k) получится перестановка $AkiB$. Очевидно, что до и после транспозиции число инверсий, образуемых цифрой i с группой A или B, остаётся неизменным. То же самое можно сказать и относительно цифры k. Допустим теперь, что в перестановке $AikB$ цифры ik расположены в порядке; тогда в перестановке $AkiB$ цифры ki будут давать инверсию. Мы видим, что в этом случае после транспозиции число инверсий увеличивается на единицу. Если же допустить, что в перестановке $AikB$ цифры ik находятся в инверсии, то после транспозиции инверсия между ними исчезает. В том и другом случае происходит изменение числа инверсий на ± 1, т. е. на нечётное число.

Переходим к разбору второго случая. Пусть между транспонируемыми цифрами i и k находится m цифр, т. е. перестановка имеет вид

$$Aii_1i_2 \dots i_mkB. \tag{1}$$

Будем i постепенно перемещать вправо, транспонируя i с рядом стоящими цифрами $i_1, i_2, \dots, i_m$. Тогда после m транспозиций получится перестановка

$$Ai_1i_2 \dots i_mikB.$$

Затем станем k постепенно передвигать влево, транспонируя k с рядом стоящими цифрами $i, i_m, \dots, i_2, i_1$. После $m+1$ таких транспозиций получится перестановка

$$Aki_1i_2 \dots i_miB. \tag{2}$$

Всего, следовательно, понадобится $m+(m+1)=2m+1$ транспозиций для того, чтобы k очутилось на месте i, а i на месте k. При каждой транспозиции чётность перестановки будет меняться, и так как $2m+1$ число нечётное, то класс перестановки будет меняться нечётное число раз, и потому класс перестановки (2) должен быть противоположен классу перестановки (1).

Из доказанной теоремы вытекают следующие следствия:

1. Чтобы перейти от одной перестановки к другой того же класса, надо выполнить чётное число транспозиций. Напротив, чтобы перейти от одной перестановки к другой противоположного класса, надо выполнить нечётное число транспозиций.

2. Из n цифр можно составить $\frac{n!}{2}$ чётных перестановок и столько же нечётных.

Это следствие не столь очевидно и поэтому нуждается в доказательстве.

Доказательство. Мы знаем, что из n цифр $1, 2, \dots, n$ можно составить всего $n!$ перестановок. Пусть среди них имеется p чётных и q нечётных перестановок.

Совершим над каждой чётной перестановкой одну и ту же транспозицию, например (1, 2). Тогда они, в силу доказанной выше теоремы, превратятся в нечётные и притом различные перестановки; значит $p \leqslant q$.

Точно так же, подвергая нечётные перестановки транспозиции (1, 2), получим q различных чётных перестановок; значит $q \leqslant p$.

Сопоставляя неравенства $p \leqslant q$ и $q \leqslant p$, приходим к выводу, что $q = p$. Таким образом определитель n-го порядка имеет одинаковое число положительных и отрицательных членов, а именно $\frac{n!}{2}$.

Всё изложенное тотчас же находит применение в теории определителей. Пусть член определителя n-го порядка $a_{i_1 j_1} a_{i_2 j_2} \dots a_{i_n j_n}$ записан таким образом, что его первые индексы не идут в порядке возрастания. Как установить знак этого члена? Очевидно, что, переставляя элементы надлежащим образом, всегда можно первые индексы расположить в натуральном порядке, после чего знак найдётся без труда.

Например, для установления знака члена $a_{21} a_{34} a_{43} a_{12}$ определителя четвёртого порядка располагаем его элементы в натуральном порядке первых индексов: $a_{12} a_{21} a_{34} a_{43}$. Подсчитываем затем число инверсий в расположении 2143 вторых индексов. Оно оказывается равным двум; значит член имеет знак плюс.

Однако, как мы сейчас увидим, знак члена можно определить иначе, совершенно не переставляя его элементов.

Теорема II. *Знак члена*

$$a_{i_1 j_1} a_{i_2 j_2} \dots a_{i_n j_n} \tag{3}$$

определителя n-го порядка равен знаку числа $(-1)^{s+t}$, где s—*число инверсий среди первых индексов* $i_1, i_2, \dots, i_n$, а t—*число инверсий среди вторых индексов* $j_1, j_2, \dots, j_n$.

Доказательство. Прежде всего покажем, что от транспозиции элементов члена (3) чётность числа $s+t$ не меняется.

В самом деле, после транспозиции, например, элементов $a_{i_1 j_1}$ и $a_{i_2 j_2}$ первые индексы составят перестановку

$$i_2 i_1 \dots i_n, \tag{A}$$

а вторые — перестановку

$$j_2 j_1 \dots j_n. \tag{B}$$

Мы видим, что произошла транспозиция индексов i_1, i_2 и j_1, j_2. Поэтому, обозначив через s' и t' число инверсий в расположениях (A) и (B), получим согласно теореме I, что разности $s'-s$ и $t'-t$ суть нечётные числа. Отсюда следует, что число

$$(s'+t')-(s+t)=(s'-s)+(t'-t),$$

как сумма двух нечётных чисел, чётно, т. е. числа $s'+t'$ и $s+t$ одинаковой чётности. Тем самым наше утверждение доказано.

Переходим к доказательству самой теоремы.

Расположим с помощью транспозиций элементы члена (3) в порядке возрастания первых индексов; тогда член примет следующий вид:

$$a_{1\alpha_1}a_{2\alpha_2}\dots a_{n\alpha_n}.$$

Знак члена равен $(-1)^{t'}$, где t' — число инверсий во вторых индексах $\alpha_1, \alpha_2, \dots, \alpha_n$. Так как первые индексы расположены в порядке возрастания, то $s'=0$; значит $s+t$ и t' должны быть одинаковой чётности. Тем самым теорема доказана.

Пример. Найдём знак члена $a_{23}a_{32}a_{41}a_{14}$, не перемещая его элементов.

Имеем $s=3$, $t=3$; отсюда $(-1)^{s+t}=(-1)^6=+1$. Член имеет знак плюс, как и следовало ожидать (ср. пример 1 на стр. 17).

Задачи. 1. Подсчитать число инверсий в следующих перестановках: a) 5, 2, 3, 1, 4, b) 10, 9, 5, 1, 2, 6, 3, 7, 8, 4, c) 5, 2, 3, 1, 4, 6, 7, 8, 9, d) n, $n-1$, $n-2$, ... , 3, 2, 1, e) $2k$, 1, $2k-1$, 2, $2k-2$, 3, ... , $k+1$, k.

2. Привести с помощью транспозиций перестановку 6, 3, 1, 4, 5, 2 к перестановке 6, 5, 4, 3, 2, 1.

3. Определить знак члена $a_{81}a_{35}a_{42}a_{63}a_{14}a_{28}a_{57}a_{76}$ детерминанта восьмого порядка, не перемещая элементов.

4. Какой знак имеет член $a_{n,1}a_{n-1,2}a_{n-2,3}\dots a_{1,n}$ детерминанта n-го порядка?

§ 5. Подстановки, циклы и транспозиции

Введём теперь более широкую операцию, чем транспозиция,— подстановку.

Подстановкой из n элементов

$$a, b, c, \dots, l$$

называют такую замену каждого из этих n элементов каким-либо другим из их числа, что в результате замены сохраняются всё те же n элементов. Легко видеть, что транспозиция есть частный случай подстановки.

В дальнейшем элементами подстановки у нас будут n цифр: 1, 2, ..., n.

Подстановку мы будем записывать так: заменяющие цифры записывают под первоначальными и всё выражение заключают в круглые скобки. Например

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

есть подстановка четырёх цифр 1, 2, 3, 4, которая заменяет 1 на 2, 2 на 3, 3 на 4 и 4 на 1. Отметим ещё, что порядок записи цифр первой строчки несущественен. Так, подстановку (1) можно записать также в таком виде:

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

отчего характер замены, конечно, не изменится, потому что попрежнему цифра 1 заменяется цифрой 2, 2—3; 3—4 и 4—1.

Применяя подстановку к некоторому расположению из n цифр, мы, очевидно, получим новое расположение тех же цифр. Например, если применить подстановку (1) к расположению 4 3 2 1, то получится новое расположение: 1 4 3 2.

Возьмём теперь две подстановки цифр 1, 2, 3, 4:

$$S_1=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},\quad S_2=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$

и посмотрим, что произойдёт, если сперва выполнить подстановку S_1, затем подстановку S_2. Подстановка S_1 заменяет 1 на 4, а S_2—4 на 1. Таким образом цифра 1 под влиянием двух подстановок S_1 и S_2 заменяется цифрой 1; записываем: $\begin{matrix}1\\1\end{matrix}$. Затем подстановка S_1 заменяет 2 на 1, а S_2—1 на 4, значит 2 под совместным влиянием S_1 и S_2 переходит в 4; записываем: $\begin{matrix}1&2\\1&4\end{matrix}$. Легко далее видеть, что цифра 3 при совместном действии подстановок S_1 и S_2 переходит в 3 (т. е. не меняется); записываем: $\begin{matrix}1&2&3\\1&4&3\end{matrix}$. Наконец, видим, что 4 при совместном действии S_1 и S_2 переходит в 2; записываем $\begin{matrix}1&2&3&4\\1&4&3&2\end{matrix}$. Итак, в результате получилась подстановка

$$S_3=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix},$$

которая одна производит то же действие, что обе подстановки S_1 и S_2, произведённые последовательно одна за другой.

Подстановку S_3 обычно называют *произведением* подстановок S_1 и S_2 и пишут:

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

Конечно, термины «произведение» и «умножение» подстановок имеют здесь особый, отнюдь не арифметический смысл. Мы «умножили» S_1 на S_2, в результате чего получилась подстановка S_3. Но, если «умножить» S_2 на S_1, то, как легко убедиться, получится совсем иное произведение:

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

Таким образом порядок перемножения подстановок весьма существенен; *умножение подстановок, в отличие от обычного арифметического умножения, вообще говоря, не коммутативно*: не всегда S_1S_2 равно S_2S_1.

Задачи. 1. Какое получится расположение цифр, если к расположению 6 5 1 2 3 4 применить подстановку $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 6 & 5 \end{pmatrix}$?

2. Перемножить подстановки:

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

b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix}$ и $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$,

c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 3 & 2 & 1 & 8 & 7 & 9 & 10 & 6 & 5 \end{pmatrix}$ и $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 3 & 1 & 8 & 5 & 7 & 6 & 10 & 2 & 9 \end{pmatrix}$.

3. Сколько различных подстановок можно составить из n цифр 1, 2, 3, ..., n?

Среди всевозможных подстановок n цифр выделяется одна, так называемая тождественная или единичная подстановка

$$I = \begin{pmatrix} 1 & 2 & 3 & 4 \dots n \\ 1 & 2 & 3 & 4 \dots n \end{pmatrix},$$

которая при умножении подстановок ведёт себя так же, как число 1 при арифметическом умножении. Именно, для любой подстановки

$$S = \begin{pmatrix} 1 & 2 & 3 & \dots n \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots \alpha_n \end{pmatrix}$$

имеет место равенство

$$SI = IS = S.$$

Аналогия подстановок с числами простирается и дальше. Во-первых, *для каждой подстановки S всегда можно подыскать так называемую обратную подстановку S^{-1}*, характеризующуюся равенством

$$SS^{-1} = S^{-1}S = I.$$

Эта обратная подстановка имеет вид:

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

И в самом деле, если S переводит 1 в α_1, то S^{-1} переводит α_1 в 1; следовательно, произведение SS^{-1} переводит 1 в 1. Точно так же SS^{-1} переводит 2 в 2, 3 в 3, ..., n в n, а это и значит, что $SS^{-1} = I$. Подобным же образом можно убедиться, что $S^{-1}S = I$.

Во-вторых, *перемножение подстановок подчиняется сочетательному закону*:

$$(S_1S_2)S_3 = S_1(S_2S_3).$$

Докажем это соотношение. Пусть подстановка S_1 переводит некоторую цифру α в β, подстановка S_2 переводит β в γ и подстановка S_3 переводит γ в δ. Тогда S_1S_2 переведёт α в γ, после чего S_3 переведёт γ в δ. Таким образом мы видим, что $(S_1S_2)S_3$ цифру α переводит в δ.

Посмотрим, как ведёт себя $S_1(S_2S_3)$. S_1 переводит α в β, а S_2S_3 переводит β в δ, значит $S_1(S_2S_3)$ переводит α в δ, т. е. производит такое же действие, что и $(S_1S_2)S_3$. Поэтому мы вправе написать: $(S_1S_2)S_3 = S_1(S_2S_3)$.

Введённое выше несколько громоздкое обозначение подстановок мы намерены теперь заменить другим, более кратким. Для наглядности обратимся к конкретным примерам. Рассмотрим подстановку:

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

Она цифру 1 переводит в 3; записываем это так: 1, 3 (читают: 1 переводится в 3). Цифра 3 переводится в 5; записываем: 1, 3, 5 (читают: 1 переводится в 3, 3 в 5). Затем видим, что 5 переводится в 7; записываем: 1, 3, 5, 7 (читают: 1 переводится в 3, 3 в 5, 5 в 7). Наконец, видим, что 7 переходит в 1, т. е. 7 переходит в цифру, с которой начинался ряд; в этом случае говорят, что «цикл замкнулся» и пишут: (1 3 5 7). Читается этот символ так: 1 переходит в 3, 3 в 5, 5 в 7 и 7 в 1.

Однако в цикл (1 3 5 7) вошли не все цифры, например не вошла цифра 2. Поэтому начнём новый цикл с этой цифры (или с какой-нибудь другой цифры, не вошедшей в первый цикл). Подстановка S цифру 2 переводит в 4, 4 в 6, 6 в 8, 8 в 2; цикл замкнулся, и мы можем написать: (2 4 6 8).

Итак, подстановка S выражается через два цикла:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 6 & 7 & 8 & 1 & 2 \end{pmatrix} = (1\ 3\ 5\ 7)\ (2\ 4\ 6\ 8),$$

или, как принято говорить, *разлагается на два независимых*[1]) цикла. Ясно, что порядок, в котором записаны в разложении независимые циклы, не имеет значения.

Возьмём ещё один пример: разложим на циклы подстановку $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$. Цифра 1 переводится в 4, 4 в 2 и 2 в 1; цикл замкнулся: (1 4 2). Но в этот цикл не вошла тройка. Цифра 3 переводится в 3 (т. е. не меняется); записываем это так: (3). Получился так называемый одночленный цикл—цикл, состоящий только из одной цифры.

Итак:

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

Эти два примера показывают, что *подстановку любого числа цифр можно разложить на независимые циклы.*

Задачи. 1. Разложить $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 4 & 3 & 2 \end{pmatrix}$ на циклы.

2. Следующие подстановки: a) (5 6) (1 2) (3 4), b) (1 8 9) (5 6) (2 3 4) (7), c) (1 10 3 4 5) (2) (6) (7 8 9), записанные в циклах, представить в обычном виде.

[1]) Независимых в том смысле, что никакие два цикла разложения не имеют общих цифр.

Заметим, что цикл можно начинать с любой цифры, входящей в его состав. Например, цикл (3 5 1 2) можно записать так: (5 1 2 3) или так: (1 2 3 5) и т. д.

Отметим ещё, что транспозиция есть не что иное, как цикл $(i\ j)$, состоящий из двух цифр. Легко сообразить, что всякий цикл можно свести к транспозициям. Такое «разложение» на транспозиции уже не будет разложением на независимые циклы. Так, цикл (2 3 5 6) можно разложить следующим образом на транспозиции:

$$(2\ 3\ 5\ 6) = (2\ 3)\ (2\ 5)\ (2\ 6).$$

Действительно, написанные транспозиции производят тот же эффект, что и рассматриваемый цикл. Мы видим, что первая транспозиция (23) переводит 2 в 3, а 3 в 2; затем транспозиция (25) переводит 2 в 5, а 5 в 2, т. е. обе транспозиции (23) и (25) совместно переводят 2 в 3, 3 в 5 и 5 в 2, иначе говоря, они производят то же действие, что и цикл (2 3 5). Рассуждая таким же образом далее, легко заключить, что (2 3) (2 5) (2 6) равносильны циклу (2 3 5 6), т. е. указанные транспозиции 2 переводят в 3, 3 в 5, 5 в 6 и, наконец, 6 в 2.

Из этого примера видно, что порядок следования зависимых циклов имеет существенное значение.

Вообще цикл $(a_1\ a_2 \dots a_k)$ можно следующим образом разложить на $(k-1)$ транспозиций:

$$(a_1\ a_2 \dots a_k) = (a_1\ a_2)\ (a_1\ a_3) \dots (a_1\ a_k).$$

Теорема I. *Всякую подстановку из n цифр можно разложить на $n-s$ транспозиций, где s—число независимых циклов, на которые распадается данная подстановка.*

Доказательство. Пусть подстановка

$$S = \begin{pmatrix} 1 & 2 & 3 \dots n \\ \alpha_1 & \alpha_2 & \alpha_3 \dots \alpha_n \end{pmatrix}$$

распадается на s независимых циклов:

$$S = (i_1 i_2 \dots i_{k_1})\ (j_1 j_2 \dots j_{k_2}) \dots (t_1 t_2 \dots t_{k_s}).$$

Но мы уже знаем, что цикл из k цифр разлагается на $k-1$ транспозиций; поэтому рассматриваемая подстановка S разлагается на

$$(k_1 - 1) + (k_2 - 1) + \dots + (k_s - 1) =$$
$$= (k_1 + k_2 + \dots + k_s) - \underbrace{(1 + 1 + \dots + 1)}_{s \text{ раз}} = n - s$$

транспозиций, что и требовалось доказать.

Разность $n-s$, называемая *декрементом* подстановки, позволяет разбить подстановки на два класса. Подстановки с чётным декрементом мы будем называть *подстановками чётного класса* или, проще, *чётными подстановками*; остальные подстановки мы отнесём к *нечётному классу*.

Можно, впрочем, подстановки классифицировать и по другому принципу. Подстановку $S = \begin{pmatrix} 1 & 2 \dots n \\ \alpha_1 \alpha_2 \dots \alpha_n \end{pmatrix}$ мы отнесём к чётному классу, если расположение $\alpha_1 \alpha_2 \dots \alpha_n$ имеет чётное число инверсий, и к нечётному классу, если расположение $\alpha_1 \alpha_2 \dots \alpha_n$ имеет нечётное число инверсий. Оказывается, что оба принципа классификации равносильны, как это видно из следующей теоремы.

Теорема II. *Если p—число инверсий в расположении $\alpha_1 \alpha_2 \dots \alpha_n$, то декремент подстановки*

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

имеет ту же чётность, что и число p.

Доказательство. Пусть подстановка S разлагается на s независимых циклов; тогда её декремент равен $n - s$. Применим теперь подстановку S к натуральному расположению 1 2 3 ... n; мы, очевидно, получим расположение $\alpha_1 \alpha_2 \dots \alpha_n$. Так как S, согласно теореме I, разлагается на $n - s$ транспозиций, то выходит, что расположение $\alpha_1 \alpha_2 \dots \alpha_n$ можно получить из натурального расположения 1 2 3...n с помощью $n - s$ транспозиций. На основании теоремы I § 4 заключаем, что число $n - s$ транспозиций должно иметь ту же чётность, что и число p инверсий в расположении $\alpha_1 \alpha_2 \dots \alpha_n$.

Теорема II приводит к одному довольно удобному способу для установления знаков членов определителя. Возьмём, например, член

$$a_{31} a_{73} a_{26} a_{54} a_{15} a_{37} a_{48} a_{62}$$

определителя восьмого порядка и составим подстановку

$$S = \begin{pmatrix} 8 & 7 & 2 & 5 & 1 & 3 & 4 & 6 \\ 1 & 3 & 6 & 4 & 5 & 7 & 8 & 2 \end{pmatrix};$$

в первой строке мы написали расположение первых индексов, а во второй строке—расположение вторых индексов. Найдём декремент подстановки S, для чего разложим S на независимые циклы:

$$S = (8\ 1\ 5\ 4)\ (7\ 3)\ (2\ 6).$$

Здесь $s = 3$; декремент $n - s = 8 - 3 = 5$ есть нечётное число. Значит рассматриваемый член имеет знак минус.

Задача. Установить с помощью декремента класс следующих расположений: а) 7, 6, 1, 3, 5, 4, 2, 8; б) 8, 7, 1, 3, 6, 2, 5, 4; в) 10, 1, 9, 2, 8, 3, 7, 4, 6, 5.

§ 6. Свойства определителей

Определители имеют широкое применение в различных областях математики. Причина этого заключена в том, что они обладают рядом замечательных свойств, которые, как мы увидим впоследствии, сильно облегчают вычисление определителей.

Свойство I. *Значение определителя не изменится от замены его строк столбцами, и обратно.*

Доказательство. Нам надо показать, что определитель

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

равен определителю

$$\Delta_1 = \begin{vmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{vmatrix}.$$

Легко видеть, что члены определителя Δ ничем не отличаются от членов определителя Δ_1, и обратно. В самом деле, каждый член определителя Δ имеет вид:

$$(-1)^{s+t} a_{i_1 j_1} a_{i_2 j_2} \dots a_{i_n j_n},$$

где $i_1 i_2 \dots i_n$ и $j_1 j_2 \dots j_n$ суть некоторые перестановки n цифр $1, 2, 3, \dots, n$, а $s+t$ — сумма чисел инверсий по первым и вторым индексам (см. § 4, теорема II). Но точно такие же члены имеет и определитель Δ_1, откуда $\Delta = \Delta_1$, и свойство I доказано.

Свойство II. *Если поменять местами два столбца (строки), то определитель изменит знак.*

Доказательство. Поменяем местами, например, μ-й и ν-й столбцы. Что произойдёт с членами определителя? Если до перестановки столбцов член определителя имел вид:

$$(-1)^s a_{1\alpha} a_{2\beta} \dots a_{k\mu} \dots a_{l\nu} \dots a_{n\rho},$$

где s — число инверсий в расположении $\alpha\beta \dots \mu \dots \nu \dots \rho$, то после перестановки расположение его вторых индексов будет:

$$\alpha\beta \dots \nu \dots \mu \dots \rho,$$

и он будет иметь знак $(-1)^{s'}$, где s' — число инверсий в расположении $\alpha\beta \dots \nu \dots \mu \dots \rho$. Но мы знаем (см. § 4, теорема I), что от транспозиции (μ, ν) чётность расположения меняется. Следовательно, $(-1)^{s'}$ имеет знак, противоположный знаку $(-1)^s$. Таким образом от перестановки двух столбцов знак каждого члена определителя меняется на обратный, откуда и следует справедливость свойства II для столбцов.

Справедливость свойства II для строк следует из того, что мы можем строки сделать столбцами (см. свойство I).

Следствие. *Определитель, у которого два столбца (строки) одинаковы, равен нулю.*

Доказательство. Поменяем местами эти столбцы (строки). С одной стороны, определитель должен изменить свой знак на обратный (см. свойство II): если он раньше был равен D, то после перестановки двух столбцов он станет равен $-D$.

С другой стороны, так как перемещаемые столбцы (строки) одинаковы, определитель не может измениться. Таким образом $D = -D$ или $2D = 0$, откуда $D = 0$.

Свойство III. *Если все элементы какого-нибудь столбца (строки) определителя умножить на одно и то же число m, то значение определителя от этого увеличится в m раз.*

Доказательство. Помножим, например, элементы μ-го столбца на m. Тогда элементы $a_{1\mu}, a_{2\mu}, \ldots, a_{n\mu}$ этого столбца превратятся в $ma_{1\mu}, ma_{2\mu}, \ldots, ma_{n\mu}$. Если до умножения каждый член определителя имел вид

$$(-1)^s a_{1\alpha} a_{2\beta} \ldots a_{k\mu} \ldots a_{n\nu},$$

то после умножения он примет вид

$$(-1)^s a_{1\alpha} a_{2\beta} \ldots (ma_{k\mu}) \ldots a_{n\nu} = m \cdot (-1)^s a_{1\alpha} a_{2\beta} \ldots a_{k\mu} \ldots a_{n\nu},$$

т. е. возрастёт в m раз.

Справедливость свойства III для строк следует из того, что мы можем согласно свойству I сделать строки столбцами.

Следствие 1. *Если все элементы какого-нибудь столбца (строки) определителя обладают общим множителем, то его можно вынести за знак определителя.*

Например

$$\begin{vmatrix} 1 & 5 & 10 \\ 2 & 6 & 2 \\ 3 & 7 & 4 \end{vmatrix} = 2 \begin{vmatrix} 1 & 5 & 5 \\ 2 & 6 & 1 \\ 3 & 7 & 2 \end{vmatrix}.$$

Следствие 2. *Определитель, у которого элементы двух строк (столбцов) соответственно пропорциональны, равен нулю.*

Доказательство. Пусть, например, пропорциональны μ-й и ν-й столбцы определителя. Это значит, что каждый элемент μ-го столбца отличается от соответствующего элемента ν-го столбца на один и тот же множитель m. Иными словами:

$$a_{1\mu} = ma_{1\nu}, \; a_{2\mu} = ma_{2\nu}, \ldots, a_{n\mu} = ma_{n\nu},$$

и определитель D выглядит так:

$$D = \begin{vmatrix} a_{11} & a_{12} \ldots ma_{1\nu} \ldots a_{1\nu} \ldots a_{1n} \\ a_{21} & a_{22} \ldots ma_{2\nu} \ldots a_{2\nu} \ldots a_{2n} \\ \ldots & \ldots \ldots \ldots \ldots \ldots \\ a_{n1} & a_{n2} \ldots ma_{n\nu} \ldots a_{n\nu} \ldots a_{nn} \end{vmatrix}.$$

Но, вынеся общий множитель m за знак определителя, получим определитель с двумя одинаковыми столбцами. Такой определитель (см. свойство II, следствие) равен нулю.

Свойство IV. *Пусть каждый элемент какого-нибудь столбца (строки) определителя D есть сумма двух слагаемых. Тогда определитель D равен сумме двух определителей, причём в одном определителе соответствующий столбец (строка) состоит из первых слагаемых, а в другом—из вторых слагаемых.*

Иными словами, имеет место равенство

$$D=\begin{vmatrix} a_{11} & a_{12} \dots (a_{1\mu}+b_{1\mu}) \dots a_{1n} \\ a_{21} & a_{22} \dots (a_{2\mu}+b_{2\mu}) \dots a_{2n} \\ \dots & \dots \\ a_{n1} & a_{n2} \dots (a_{n\mu}+b_{n\mu}) \dots a_{nn} \end{vmatrix}=\begin{vmatrix} a_{11} & a_{12} \dots a_{1\mu} \dots a_{1n} \\ a_{21} & a_{22} \dots a_{2\mu} \dots a_{2n} \\ \dots & \dots \\ a_{n1} & a_{n2} \dots a_{n\mu} \dots a_{nn} \end{vmatrix}+$$
$$+\begin{vmatrix} a_{11} & a_{12} \dots b_{1\mu} \dots a_{1n} \\ a_{21} & a_{22} \dots b_{2\mu} \dots a_{2n} \\ \dots & \dots \\ a_{n1} & a_{n2} \dots b_{n\mu} \dots a_{nn} \end{vmatrix}.$$

Доказательство. Каждый член определителя D имеет вид:

$$(-1)^s a_{1\alpha}\, a_{2\beta} \dots (a_{k\mu}+b_{k\mu}) \dots a_{n\rho},$$

где s—число инверсий во вторых индексах $\alpha\beta \dots \mu \dots \rho$. Раскроем скобки; тогда член распадётся на два члена:

$$(-1)^s a_{1\alpha}\, a_{2\beta} \dots (a_{k\mu}+b_{k\mu}) \dots a_{n\rho}=(-1)^s a_{1\alpha}\, a_{2\beta} \dots a_{k\mu} \dots a_{n\rho}+$$
$$+(-1)^s a_{1\alpha}\, a_{2\beta} \dots b_{k\mu} \dots a_{n\rho}.$$

Но члены вида $(-1)^s a_{1\alpha}\, a_{2\beta} \dots a_{k\mu} \dots a_{n\rho}$ образуют определитель

$$D_1=\begin{vmatrix} a_{11} & a_{12} \dots a_{1\mu} \dots a_{1n} \\ a_{21} & a_{22} \dots a_{2\mu} \dots a_{2n} \\ \dots & \dots \\ a_{n1} & a_{n2} \dots a_{n\mu} \dots a_{nn} \end{vmatrix},$$

а члены вида $(-1)^s a_{1\alpha}\, a_{2\beta} \dots b_{k\mu} \dots a_{n\rho}$—определитель

$$D_2=\begin{vmatrix} a_{11} & a_{12} \dots b_{1\mu} \dots a_{1n} \\ a_{21} & a_{22} \dots b_{2\mu} \dots a_{2n} \\ \dots & \dots \\ a_{n1} & a_{n2} \dots b_{n\mu} \dots a_{nn} \end{vmatrix},$$

откуда и следует свойство IV.

Очевидно, что свойство IV справедливо не только для случая двух, но и для большего числа слагаемых. Например

$$\begin{vmatrix} 1+2+3 & 7 & 1 \\ 0-1+5 & 3-1 & 2 \\ 2-1+3 & -1 & 2 \end{vmatrix}=\begin{vmatrix} 1 & 7 & 1 \\ 0 & 3-1 & 2 \\ 2-1 & & 2 \end{vmatrix}+\begin{vmatrix} 2 & 7 & 1 \\ -1 & 3-1 & 2 \\ -1 & -1 & 2 \end{vmatrix}+$$
$$+\begin{vmatrix} 3 & 7 & 1 \\ 5 & 3-1 & 2 \\ 3-1 & & 2 \end{vmatrix}.$$

Следствие. *Определитель D не меняет своего значения от прибавления ко всем элементам какого-нибудь столбца (строки) соответствующих элементов другого столбца (строки), умноженных на одно и то же число.*

Доказательство. Прибавим, например, к элементам μ-го столбца соответствующие элементы ν-го столбца, умноженные на некоторое число k. Тогда получится такой определитель:

$$D' = \begin{vmatrix} a_{11} & a_{12} \dots (a_{1\mu} + ka_{1\nu}) & \dots a_{1\nu} \dots a_{1n} \\ a_{21} & a_{22} \dots (a_{2\mu} + ka_{2\nu}) & \dots a_{2\nu} \dots a_{2n} \\ \dots & \dots & \dots \\ a_{n1} & a_{n2} \dots (a_{n\mu} + ka_{n\nu}) & \dots a_{n\nu} \dots a_{nn} \end{vmatrix}.$$

Мы видим, что элементы μ-го столбца определителя D' являются суммами двух слагаемых. Отсюда по свойству IV:

$$D' = \begin{vmatrix} a_{11} & a_{12} \dots a_{1\mu} \dots a_{1\nu} \dots a_{1n} \\ a_{21} & a_{22} \dots a_{2\mu} \dots a_{2\nu} \dots a_{2n} \\ \dots & \dots & \dots \\ a_{n1} & a_{n2} \dots a_{n\mu} \dots a_{n\nu} \dots a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} \dots ka_{1\nu} \dots a_{1\nu} \dots a_{1n} \\ a_{21} & a_{22} \dots ka_{2\nu} \dots a_{2\nu} \dots a_{2n} \\ \dots & \dots & \dots \\ a_{n1} & a_{n2} \dots ka_{n\nu} \dots a_{n\nu} \dots a_{nn} \end{vmatrix}.$$

Но первый определитель суммы есть D, а второй равен нулю, так как у него два столбца пропорциональны (см. свойство III, следствие 2); таким образом $D' = D$, что и требовалось показать. Для строк доказательство повторяется дословно.

Свойство IV, как мы увидим впоследствии, значительно упрощает вычисление определителей. Впрочем и сейчас до некоторой степени можно видеть, насколько применение свойства IV может ускорить и упростить вычисление. Мы ограничимся следующим примером.

Пример. Вычислить определитель

$$D = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 3 & 7 & 0 & 1 \\ 2 & 5 & 6 & 7 \\ 2 & 0 & 1 & -1 \end{vmatrix}.$$

Постараемся определитель D преобразовать так, чтобы все элементы первой строки, кроме одного, стали равными нулю. Этого можно достигнуть, пользуясь следствием свойства IV. Вычтем из элементов второго столбца элементы первого. Получим:

$$D = \begin{vmatrix} 1 & 0 & 1 & 1 \\ 3 & 4 & 0 & 1 \\ 2 & 3 & 6 & 7 \\ 2 & -2 & 1 & -1 \end{vmatrix}.$$

В этом определителе вычтем из элементов третьего столбца элементы первого, в результате чего получим:

$$D = \begin{vmatrix} 1 & 0 & 0 & 1 \\ 3 & 4 & -3 & 1 \\ 2 & 3 & 4 & 7 \\ 2 & -2 & -1 & -1 \end{vmatrix}.$$

Наконец, вычтем из элементов четвёртого столбца элементы первого. Получим:

$$D=\begin{vmatrix}1&0&0&0\\3&4&-3&-2\\2&3&4&5\\2&-2&-1&-3\end{vmatrix}.$$

Этот определитель вычислить гораздо легче, чем первоначальный. Так как все элементы первой строки, кроме $a_{11}=1$, равны нулю, то значительная часть членов определителя равна нулю. Выпишем все члены, не равные нулю. Это будут:

$$+a_{11}a_{22}a_{33}a_{44},\quad -a_{11}a_{22}a_{34}a_{43},\quad +a_{11}a_{24}a_{32}a_{43},$$
$$-a_{11}a_{24}a_{33}a_{42},\quad +a_{11}a_{23}a_{34}a_{42},\quad -a_{11}a_{23}a_{32}a_{44},$$

откуда

$$D=a_{11}a_{22}a_{33}a_{44}-a_{11}a_{22}a_{34}a_{43}+a_{11}a_{24}a_{32}a_{43}-$$
$$-a_{11}a_{24}a_{32}a_{42}+a_{11}a_{23}a_{34}a_{42}-a_{11}a_{23}a_{32}a_{44},$$

или, после вынесения общего множителя a_{11} за скобку:

$$D=a_{11}(a_{22}a_{33}a_{44}-a_{22}a_{34}a_{43}+a_{24}a_{32}a_{43}-a_{24}a_{33}a_{42}+$$
$$+a_{23}a_{34}a_{42}-a_{23}a_{32}a_{44}).$$

Но в скобке стоит определитель третьего порядка:

$$\begin{vmatrix}a_{22}&a_{23}&a_{24}\\a_{32}&a_{33}&a_{34}\\a_{42}&a_{43}&a_{44}\end{vmatrix},$$

откуда

$$D=a_{11}\begin{vmatrix}a_{22}&a_{23}&a_{24}\\a_{32}&a_{33}&a_{34}\\a_{42}&a_{43}&a_{44}\end{vmatrix}.$$

Подставляя теперь вместо элементов a_{ij} их числовые значения, получим окончательно:

$$D=1\begin{vmatrix}4&-3&-2\\3&4&5\\-2&-1&-3\end{vmatrix}=-48+30+6-16-27+20=-35.$$

Получился такой эффект, как если бы мы в определителе

$$\begin{vmatrix}1&0&0&0\\3&4&-3&-2\\2&3&4&5\\2&-2&-1&-3\end{vmatrix}$$

вычеркнули первый столбец и первую строку. Мы увидим в следующем параграфе, что подмеченный факт далеко не случаен.

З а [illegible] Проверить на определителях второго и третьего порядка все четыре свойства и их [illegible]

§ 7. Миноры, алгебраические дополнения и простейший мет вычисления определителей

В конце предыдущего параграфа мы показали, что определите четвёртого порядка, у которого все элементы первой строки, кро одного, равны нулю, можно привести к определителю трет порядка. Мы увидим, что такое сведение к определителям низш порядка возможно всегда.

Введём прежде всего следующие определения.

Определение 1. *Минором* M_{ij} *элемента* a_{ij} *определителя*

$$D=\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nj} & \dots & a_{nn} \end{vmatrix}$$

называется такой новый определитель, который получается из вычёркиванием строки и столбца, проходящих через данный элемен

Пример. Найдём минор M_{23} элемента a_{23} определителя

$$D=\begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{vmatrix}.$$

Согласно определению надо вычеркнуть вторую строку и третий столбец, так как элемент a_{23} стоит на пересечении этих строк и столбца. Таким образом

$$M_{23}=\begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{vmatrix}=\begin{vmatrix} a_{11} & a_{12} & a_{14} \\ a_{31} & a_{32} & a_{34} \\ a_{41} & a_{42} & a_{44} \end{vmatrix}.$$

Определение 2. *Алгебраическим дополнением элемента* a_{ij} *назы вается его минор* M_{ij}, *взятый со знаком* $(-1)^{i+j}$.

Алгебраическое дополнение элемента a_{ij} мы будем обозначать через A_{ij}. Таким образом $A_{ij}=(-1)^{i+j}M_{ij}$.

Пример. Найдём алгебраическое дополнение элемента a_{23} определителя предыдущего примера. Выше было обнаружено, что

$$M_{23}=\begin{vmatrix} a_{11} & a_{12} & a_{14} \\ a_{31} & a_{32} & a_{34} \\ a_{41} & a_{42} & a_{44} \end{vmatrix};$$

отсюда

$$A_{23}=(-1)^{2+3}M_{23}=-M_{23}=-\begin{vmatrix} a_{11} & a_{12} & a_{14} \\ a_{31} & a_{32} & a_{34} \\ a_{41} & a_{42} & a_{44} \end{vmatrix}.$$

Теперь мы в состоянии сформулировать следующую теорему.

Теорема. *Если в определителе n-го порядка все элементы i-й строки (j-го столбца), кроме a_{ij}, равны нулю, то такой определитель равен произведению элемента a_{ij} на его алгебраическое дополнение A_{ij}:* $D = a_{ij}A_{ij}$.

Доказательство. 1) Рассмотрим сперва тот случай, когда все элементы первой строки (первого столбца), кроме a_{11}, равны нулю, т. е.

$$D = \begin{vmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{vmatrix}, \tag{1}$$

или

$$D = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ 0 & a_{32} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots \\ 0 & a_{n2} & \dots & a_{nn} \end{vmatrix}, \tag{2}$$

покажем, что

$$D = a_{11}A_{11} = a_{11}(-1)^{1+1}M_{11} = a_{11}M_{11},$$

или, что то же самое:

$$D = a_{11}\begin{vmatrix} a_{22} & a_{23} & \dots & a_{2n} \\ a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots \\ a_{n2} & a_{n3} & \dots & a_{nn} \end{vmatrix}.$$

Так как в каждый член определителя входит один из элементов первой строки, которые все, за исключением одного, равны нулю, то значительная часть членов определителя (1) будет равна нулю. Какие члены не равны нулю? Это, очевидно, будут члены вида

$$(-1)^s a_{11}a_{2\alpha}a_{3\beta}\dots a_{n\rho}$$

(здесь s—число инверсий в расположении $1\alpha\beta\dots\rho$, или, что то же, в расположении $\alpha\beta\dots\rho$, так как индекс 1 стоит на своем месте). Мы видим, что члены определителя имеют общий множитель a_{11}; вынося a_{11}, как общий множитель, за скобку, получим в скобке сумму членов вида

$$(-1)^s a_{2\alpha}a_{3\beta}\dots a_{n\rho},$$

т. е. определитель $(n-1)$-го порядка:

$$M_{11} = \begin{vmatrix} a_{22} & a_{23} & \dots & a_{2n} \\ a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots \\ a_{n2} & a_{n3} & \dots & a_{nn} \end{vmatrix}.$$

Значит $D = a_{11}M_{11}$. Таким образом для определителя (1) теорема доказана.

Что касается определителя (2), то для него теорему также можно считать доказанной, так как, заменяя в нём по свойству I строки столбцами, получим определитель того же типа, что и (1).

2) Переходим к разбору второго случая. Пусть, например,

$$D = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{ij} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nj} & \dots & a_{nn} \end{vmatrix}.$$

Преобразуем определитель D так, чтобы элемент a_{ij} оказался на месте элемента a_{11}. Для этого сначала передвинем i-ю строку на место первой, переставляя её последовательно с $(i-1)$-й, $(i-2)$-й, ..., 3-й, 2-й и, наконец, с 1-й строками. Очевидно, что придётся совершить всего $i-1$ транспозиций строк. По свойству II (см. § 6) определитель при каждой транспозиции строк будет менять знак на обратный; таким образом, когда i-я строка окажется на первом месте, определитель приобретёт знак $(-1)^{i-1}$.

Затем передвинем j-й столбец на место первого, переставляя его последовательно с $(j-1)$-м, $(j-2)$-м, ..., 3-м, 2-м и 1-м столбцами: всего придётся совершить ещё $j-1$ транспозиций столбцов, откуда по свойству II определитель приобретёт знак $(-1)^{i-1}\cdot(-1)^{j-1} = (-1)^{i+j-2} = (-1)^{i+j}$ и будет выглядеть так:

$$D = (-1)^{i+j} D' = (-1)^{i+j} \begin{vmatrix} a_{ij} & 0 & \dots 0 & 0 & \dots 0 \\ a_{1j} & a_{11} & \dots a_{1\,j-1} & a_{1\,j+1} & \dots a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i-1\,j} & a_{i-11} & \dots a_{i-1\,j-1} & a_{i-1\,j+1} & \dots a_{i-1\,n} \\ a_{i+1\,j} & a_{i+11} & \dots a_{i+1\,j-1} & a_{i+1\,j+1} & \dots a_{i+1\,n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{nj} & a_{n1} & \dots a_{n\,j-1} & a_{n\,j+1} & \dots a_{nn} \end{vmatrix}.$$

Мы видим, что в определителе D' элемент a_{ij} занимает положение элемента a_{11}. Поэтому согласно 1) имеем:

$$D' = a_{ij} \begin{vmatrix} a_{11} & a_{12} & \dots a_{1j-1} & a_{1j+1} & \dots a_{1n} \\ a_{21} & a_{22} & \dots a_{2j-1} & a_{2j+1} & \dots a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i-11} & a_{i-12} & \dots a_{i-1\,j-1} & a_{i-1\,j+1} & \dots a_{i-1n} \\ a_{i+11} & a_{i+12} & \dots a_{i+1\,j-1} & a_{i+1\,j+1} & \dots a_{i+1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots a_{nj-1} & a_{nj+1} & \dots a_{nn} \end{vmatrix} = a_{ij}M_{ij},$$

откуда

$$D=(-1)^{i+j}a_{ij}M_{ij}=a_{ij}(-1)^{i+j}M_{ij}=a_{ij}A_{ij},$$

что и требовалось показать.

Только что доказанная теорема имеет весьма большое теоретическое и практическое значение. Её практическое значение заключается в том, что, делая нули в какой-либо строке или столбце определителя n-го порядка и применяя затем эту теорему, получаем определитель низшего, $(n-1)$-го порядка. В свою очередь определитель $(n-1)$-го порядка можно свести к определителю $(n-2)$-го порядка и т. д., пока не придём к определителю второго порядка.

Поясним сказанное на примерах.

Пример 1. Вычислить определитель

$$D=\begin{vmatrix}1&2&3&4\\1&0&1&2\\3&-1&-1&0\\1&2&0&-5\end{vmatrix}.$$

С помощью следствия свойства IV (см. § 6) преобразуем D так, чтобы все элементы какой-нибудь строки (или столбца) оказались нулями, кроме одного. Лучше всего делать нули во второй строке, так как числа, стоящие в этой строке, невелики и к тому же один нуль уже есть. Вычтем из элементов третьего столбца элементы первого. Тогда по свойству IV получим:

$$D=\begin{vmatrix}1&2&2&4\\1&0&0&2\\3&-1&-4&0\\1&2&-1&-5\end{vmatrix}.$$

Затем вычтем из элементов четвёртого столбца удвоенные элементы первого. Получим:

$$D=\begin{vmatrix}1&2&2&2\\1&0&0&0\\3&-1&-4&-6\\1&2&-1&-7\end{vmatrix}.$$

Наша цель достигнута: все элементы второй строки, кроме первого, обратились в нули. А теперь согласно доказанной выше теореме имеем:

$$a_{21}=1,\quad A_{21}=(-1)^{2+1}\begin{vmatrix}2&2&2\\-1&-4&-6\\2&-1&-7\end{vmatrix}=-\begin{vmatrix}2&2&2\\-1&-4&-6\\2&-1&-7\end{vmatrix},$$

$$D=a_{21}A_{21}=-\begin{vmatrix}2&2&2\\-1&-4&-6\\2&-1&-7\end{vmatrix}.$$

Вторая строка полученного определителя имеет общим множителем -1, а первая 2. Вынося эти множители за знак определителя (см. § 6, свойство III, следствие 1), получим:

$$D=2\begin{vmatrix}1 & 1 & 1\\ 1 & 4 & 6\\ 2 & -1 & -7\end{vmatrix}.$$

В этом определителе целесообразнее делать нули в первой строке. Вычтем из второго столбца первый. Определитель примет вид:

$$D=2\begin{vmatrix}1 & 0 & 1\\ 1 & 3 & 6\\ 2 & -3 & -7\end{vmatrix}.$$

Затем вычтем из третьего столбца первый. Получим:

$$D=2\begin{vmatrix}1 & 0 & 0\\ 1 & 3 & 5\\ 2 & -3 & -9\end{vmatrix},$$

откуда

$$D=2\cdot 1\cdot(-1)^{1+1}\begin{vmatrix}3 & 5\\ -3 & -9\end{vmatrix}=2\begin{vmatrix}3 & 5\\ -3 & -9\end{vmatrix}.$$

Вынося из второй строки общий множитель -3, получим окончательно:

$$D=-6\begin{vmatrix}3 & 5\\ 1 & 3\end{vmatrix}=-6(9-5)=-24.$$

Итак, оказалось, что $D=-24$.

Пример 2. Вычислить определитель

$$V_n=\begin{vmatrix}1 & a_1 & a_1^2 & \dots & a_1^{n-1}\\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1}\\ \dots & \dots & \dots & \dots & \dots\\ 1 & a_n & a_n^2 & \dots & a_n^{n-1}\end{vmatrix},$$

называемый *определителем Вандермонда.*

Вычтем из каждого столбца предыдущий, увеличенный в a_1 раз. Получим:

$$V_n=\begin{vmatrix}1 & 0 & 0 & \dots & 0\\ 1 & a_2-a_1 & a_2(a_2-a_1) & \dots & a_2^{n-2}(a_2-a_1)\\ 1 & a_3-a_1 & a_3(a_3-a_1) & \dots & a_3^{n-2}(a_3-a_1)\\ \dots & \dots & \dots & \dots & \dots\\ 1 & a_n-a_1 & a_n(a_n-a_1) & \dots & a_n^{n-2}(a_n-a_1)\end{vmatrix}=$$

$$=\begin{vmatrix}a_2-a_1 & a_3(a_2-a_1) & \dots & a_2^{n-2}(a_2-a_1)\\ a_3-a_1 & a_3(a_3-a_1) & \dots & a_3^{n-2}(a_3-a_1)\\ \dots & \dots & \dots & \dots\\ a_n-a_1 & a_n(a_n-a_1) & \dots & a_n^{n-2}\end{vmatrix},$$

или, вынося за знак определителя общие множители каждой строки,

$$V_n=(a_2-a_1)(a_3-a_1)\dots(a_n-a_1)\begin{vmatrix} 1 & a_2 & a_2^2 \dots a_2^{n-2} \\ 1 & a_3 & a_3^2 \dots a_3^{n-2} \\ \dots & \dots & \dots \\ 1 & a_n & a_n^2 \dots a_n^{n-2} \end{vmatrix}.$$

Мы видим, что в правую часть равенства вошёл определитель Вандермонда от $n-1$ букв $a_2, a_3, \dots, a_n$. Обозначим его через V_{n-1}.

Подвергая V_{n-1} аналогичным преобразованиям, получим:

$$V_{n-1}=(a_3-a_2)(a_4-a_2)\dots(a_n-a_2)\,V_{n-2},$$

где V_{n-2} — определитель Вандермонда от $n-2$ букв $a_3, a_4, \dots, a_n$. Точно так же получим, что

$$V_{n-2}=(a_4-a_3)(a_5-a_3)\dots(a_n-a_3)\,V_{n-3},$$

где V_{n-3} — определитель Вандермонда от $n-3$ букв $a_4, a_5, \dots, a_n$, и т. д. Так, понижая постепенно порядок определителя, мы в конечном счёте получим, что

$$V_n=(a_2-a_1)(a_3-a_1)\dots(a_n-a_1)(a_3-a_2)(a_4-a_2)\dots(a_n-a_{n-1}).$$

Пример 3. Покажем, что определитель

$$D=\begin{vmatrix} a_{11} & a_{12} \dots a_{1n} \\ 0 & a_{22} \dots a_{2n} \\ \dots & \dots \\ 0 & 0 \dots a_{nn} \end{vmatrix},$$

у которого все элементы ниже главной диагонали равны нулю, равен произведению диагональных элементов:

$$D=a_{11}a_{22}\dots a_{nn}.$$

Так как в определителе D все элементы первого столбца, кроме a_{11}, равны нулю, то

$$D=a_{11}\begin{vmatrix} a_{22} & a_{23} \dots a_{2n} \\ 0 & a_{33} \dots a_{3n} \\ \dots & \dots \\ 0 & 0 \dots a_{nn} \end{vmatrix}.$$

Точно так же

$$D_1=\begin{vmatrix} a_{22} & a_{23} \dots a_{2n} \\ 0 & a_{33} \dots a_{3n} \\ \dots & \dots \\ 0 & 0 \dots a_{nn} \end{vmatrix}=a_{22}\begin{vmatrix} a_{33} & a_{34} \dots a_{3n} \\ 0 & a_{44} \dots a_{4n} \\ \dots & \dots \\ 0 & 0 \dots a_{nn} \end{vmatrix} \text{ и т. д.}$$

В конце концов мы получим, что

$$D=a_{11}a_{22}\dots a_{nn}\ ^{1}).$$

---

[1]) Подобным же образом можно показать также, что определитель, у которого все элементы выше главной диагонали равны нулю, равен произведению диагональных элементов.

На этом мы пока закончим разбор примеров на вычисление определителей. В дальнейшем мы ещё вернёмся к этому вопросу.

Задачи. 1. Вычислить определители

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 5 & 0 & 0 & -1 \\ -1 & 2 & 3 & 6 \\ 5 & -1 & 1 & 2 \end{vmatrix}, \quad \begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \\ 2 & 3 & 4 & 5 & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & 0 & 0 & 2 & 3 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 3 & 5 \\ 2 & 8 & 7 & 1 & 4 \\ -1 & 0 & 5 & 7 & -2 \end{vmatrix}.$$

2. Пользуясь полученным выше значением определителя Вандермонда, вычислить определитель:

$$\begin{vmatrix} \alpha_1^n & \alpha_1^{n-1}\beta_1 & \alpha_1^{n-2}\beta_1^2 & \dots & \alpha_1\beta_1^{n-1} & \beta_1^n \\ \alpha_2^n & \alpha_2^{n-1}\beta_2 & \alpha_2^{n-2}\beta_2^2 & \dots & \alpha_2\beta_2^{n-1} & \beta_2^n \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha_{n+1}^n & \alpha_{n+1}^{n-1}\beta_{n+1} & \alpha_{n+1}^{n-2}\beta_{n+1}^2 & \dots & \alpha_{n+1}\beta_{n+1}^{n-1} & \beta_{n+1}^n \end{vmatrix}.$$

§ 8. Разложение определителей по элементам строки и столбца. Формулы Крамера

В § 3 мы ввели понятие определителя n-го порядка, изучили его свойства (§ 6) и на конкретных примерах указали практический метод вычисления определителей любого порядка.

Теперь мы покажем, как с помощью определителей n-го порядка можно решать системы линейных уравнений со многими неизвестными.

Докажем прежде всего следующие две теоремы.

Теорема I. *Какую бы строку (столбец) определителя мы ни взяли, определитель D всегда равен сумме произведений элементов этой строки (столбца) на их алгебраические дополнения.* Иными словами, имеет место такое разложение D по элементам строки или столбца:

$$D = a_{i1}A_{i1} + a_{i2}A_{i2} + \dots + a_{in}A_{in} \quad (i = 1, 2, \dots, n) \tag{1}$$

или

$$D = a_{1i}A_{1i} + a_{2i}A_{2i} + \dots + a_{ni}A_{ni}. \tag{2}$$

Доказательство. Мы ограничимся доказательством формулы (1), так как формула (2) доказывается дословно так же.

Напишем определитель D в таком виде:

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{i1}+0+\dots+0 & 0+a_{i2}+0+\dots+0 & \dots & 0+0+\dots+a_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

Мы представили элементы i-й строки в виде суммы n слагаемых для того, чтобы воспользоваться свойством IV (§ 6). По этому свойству предыдущий определитель равен сумме

$$\begin{vmatrix} a_{11} & a_{12} \dots a_{1n} \\ a_{21} & a_{22} \dots a_{2n} \\ \dots & \dots \\ a_{i1} & 0 \dots 0 \\ \dots & \dots \\ a_{n1} & a_{n2} \dots a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} \dots a_{1n} \\ a_{21} & a_{22} \dots a_{2n} \\ \dots & \dots \\ 0 & a_{i2} \dots 0 \\ \dots & \dots \\ a_{n1} & a_{n2} \dots a_{nn} \end{vmatrix} + \dots + \begin{vmatrix} a_{11} & a_{12} \dots a_{1n} \\ a_{21} & a_{22} \dots a_{2n} \\ \dots & \dots \\ 0 & 0 \dots a_{in} \\ \dots & \dots \\ a_{n1} & a_{n2} \dots a_{nn} \end{vmatrix},$$

откуда в силу теоремы § 7

$$D = a_{i1}A_{i1} + a_{i2}A_{i2} + \dots + a_{in}A_{in},$$

что и требовалось доказать.

Теорема I является непосредственным обобщением теоремы предыдущего параграфа и может быть также использована для вычисления определителей.

Пример. Вычислим определитель

$$D = \begin{vmatrix} 1 & 2 & 3 & 4 \\ 1 & 0 & 1 & 2 \\ 3 & -1 & -1 & 0 \\ 1 & 2 & 0 & -5 \end{vmatrix},$$

не делая нулей. Разложим D по элементам второй строки:

$$D = a_{21}A_{21} + a_{22}A_{22} + a_{23}A_{23} + a_{24}A_{24}.$$

Так как

$$a_{21} = 1, \quad a_{22} = 0, \quad a_{23} = 1, \quad a_{24} = 2$$

и

$$A_{21} = -\begin{vmatrix} 2 & 3 & 4 \\ -1 & -1 & 0 \\ 2 & 0 & -5 \end{vmatrix}, \quad A_{22} = \begin{vmatrix} 1 & 3 & 4 \\ 3 & -1 & 0 \\ 1 & 0 & -5 \end{vmatrix},$$

$$A_{23} = -\begin{vmatrix} 1 & 2 & 4 \\ 3 & -1 & 0 \\ 1 & 2 & -5 \end{vmatrix}, \quad A_{24} = \begin{vmatrix} 1 & 2 & 3 \\ 3 & -1 & -1 \\ 1 & 2 & 0 \end{vmatrix},$$

то

$$D = -\begin{vmatrix} 2 & 3 & 4 \\ -1 & -1 & 0 \\ 2 & 0 & -5 \end{vmatrix} + 0 \begin{vmatrix} 1 & 3 & 4 \\ 3 & & 0 \\ 1 & & -5 \end{vmatrix} -$$

$$- \begin{vmatrix} 1 & 2 & 4 \\ 3 & -1 & 0 \\ 1 & 2 & -5 \end{vmatrix} + 2 \begin{vmatrix} 1 & 2 & \\ 3 & -1 & \\ 1 & 2 & 0 \end{vmatrix} =$$

$$= -\begin{vmatrix} 2 & 3 & 4 \\ -1 & -1 & 0 \\ 2 & 0 & -5 \end{vmatrix} - \begin{vmatrix} 1 & 2 & 4 \\ 3 & -1 & 0 \\ 1 & 2 & -5 \end{vmatrix} + 2 \begin{vmatrix} 1 & 2 & 3 \\ 3 & -1 & -1 \\ 1 & 2 & 0 \end{vmatrix}.$$

Находим значение каждого из определителей третьего порядка по правилу Саррюса. Получим:

$$D = -3 - 63 + 2 \cdot 21 = -24.$$

Необходимо, впрочем, отметить, что такое вычисление не всегда оказывается удобным; в большинстве случаев метод вычисления, данный в § 7, скорее приводит к цели.

Теорема II. *Сумма произведений элементов какой-нибудь строки (столбца) на алгебраические дополнения соответственных элементов другой строки (столбца) равна нулю.*

Иными словами:

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \ldots + a_{in}A_{jn} = 0 \quad (i \neq j), \tag{3}$$

$$a_{1s}A_{1t} + a_{2s}A_{2t} + \ldots + a_{ns}A_{nt} = 0 \quad (s \neq t). \tag{4}$$

Доказательство. Кроме данного определителя

$$D = \begin{vmatrix} a_{11} & a_{12} \ldots a_{1n} \\ a_{21} & a_{22} \ldots a_{2n} \\ \cdots & \cdots \\ a_{i1} & a_{i2} \ldots a_{in} \\ \cdots & \cdots \\ a_{j1} & a_{j2} \ldots a_{jn} \\ \cdots & \cdots \\ a_{n1} & a_{n2} \ldots a_{nn} \end{vmatrix}$$

рассмотрим ещё вспомогательный определитель

$$D_1 = \begin{vmatrix} a_{11} & a_{12} \ldots a_{1n} \\ a_{21} & a_{22} \ldots a_{2n} \\ \cdots & \cdots \\ a_{i1} & a_{i2} \ldots a_{in} \\ \cdots & \cdots \\ a_{i1} & a_{i2} \ldots a_{in} \\ \cdots & \cdots \\ a_{n1} & a_{n2} \ldots a_{nn} \end{vmatrix},$$

у которого i-я и j-я строки одинаковы. Он, очевидно, равен нулю (см. § 6, свойство II, следствие). С другой стороны, разлагая D_1 по элементам j-й строки, получим в силу формулы (1):

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \ldots + a_{in}A_{jn} = D_1 = 0,$$

т. е. мы придём к равенству (3).

Аналогичным образом выводится и равенство (4).

После введения этих теорем можно уже сразу перейти к решению системы n линейных уравнений с n неизвестными.

Пусть дана система n уравнений с n неизвестными:

$$a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1,$$
$$a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$a_{n1}x_1 + a_{n2}x_2 + \ldots$$

Составим определитель

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

из коэффициентов при неизвестных системы; его называют определителем системы. Покажем теперь, как с помощью формул (2) и (4) можно решить предложенную систему уравнений.

Помножим первое уравнение системы (5) на A_{1s} [1]), второе уравнение на A_{2s}, третье на A_{3s}, ..., n-е на A_{ns} и затем сложим почленно уравнения. Тогда у нас получится:

$$\begin{aligned} &(a_{11}A_{1s}+a_{21}A_{2s}+\dots+a_{n1}A_{ns})\,x_1+\\ &+\dots\dots\dots\dots\dots\dots+\\ &+(a_{1s}A_{1s}+a_{2s}A_{2s}+\dots+a_{ns}A_{ns})\,x_s+\\ &+\dots\dots\dots\dots\dots\dots+\\ &+(a_{1n}A_{1s}+a_{2n}A_{2s}+\dots+a_{nn}A_{ns})\,x_n=\\ &=b_1A_{1s}+b_2A_{2s}+\dots+b_nA_{ns}. \end{aligned}$$

Но согласно формуле (4) все суммы вида:

$$a_{1k}A_{1s}+a_{2k}A_{2s}+\dots+a_{nk}A_{ns}\quad (k\neq s)$$

равны нулю. Поэтому все скобки, кроме

$$a_{1s}A_{1s}+a_{2s}A_{2s}+\dots+a_{ns}A_{ns}=D$$

[см. формулу (2)], пропадут, и мы получим:

$$Dx_s=b_1A_{1s}+b_2A_{2s}+\dots+b_nA_{ns}. \tag{6}$$

Займёмся правой частью уравнения (6). Возьмём определитель

$$D_s=\begin{vmatrix} a_{11} & a_{12} \dots b_1 \dots a_{1n} \\ a_{21} & a_{22} \dots b_2 \dots a_{2n} \\ \dots & \dots \dots \dots \\ a_{n1} & a_{n2} \dots b_n \dots a_{nn} \end{vmatrix},$$

отличающийся от D только s-м столбцом, в котором коэффициенты a_{1s}, a_{2s}, ..., a_{ns} заменены свободными членами b_1, b_2, ..., b_n, и разложим его по элементам s-го столбца. Тогда как раз получится правая часть уравнения (6). Следовательно, (6) можно переписать так:

$$Dx_s=D_s.$$

Если $D\neq 0$, то

$$x_s=\frac{D_s}{D}\qquad (s=1, 2, \dots, n).$$

---

[1]) s равным одному из чисел 1, 2, ..., n.

Однако надо дополнительно проверить, будут ли найденные значения неизвестных действительно корнями системы (5).

Для проверки подставим

$$x_1=\frac{D_1}{D},\quad x_2=\frac{D_2}{D},\ \ldots,\ x_n=\frac{D_n}{D}$$

в левые части уравнений (5). Возьмём, например, первое уравнение. После подстановки мы получим:

$$a_{11}D_1+a_{12}D_2+\ldots+a_{1n}D_n=b_1D,$$

или, заменяя D_s их выражениями $D_s=b_1A_{1s}+b_2A_{2s}+\ldots+b_nA_{ns}$,

$$a_{11}(b_1A_{11}+b_2A_{21}+\ldots+b_nA_{n1})+a_{12}(b_1A_{12}+b_2A_{22}+\ldots+b_nA_{n2})+\\+\ldots+a_{1n}(b_1A_{1n}+b_2A_{2n}+\ldots+b_nA_{nn})=b_1D.$$

Раскроем скобки и соберём вместе члены с одинаковыми b_i. Получим:

$$b_1(a_{11}A_{11}+a_{12}A_{12}+\ldots+a_{1n}A_{1n})+b_2(a_{11}A_{21}+a_{12}A_{22}+\ldots+a_{1n}A_{2n})+\\+\ldots+b_n(a_{11}A_{n1}+a_{12}A_{n2}+\ldots+a_{1n}A_{nn})=b_1D. \qquad (7)$$

По формуле (3) все скобки левой части равенства (7), кроме первой, должны равняться нулю. Что касается первой скобки, то она по формуле (1) равна D, поэтому равенство (7) превращается в тождество:

$$b_1D=b_1D.$$

Подобным же образом проверяются и остальные уравнения системы (5).

Итак, *если* $D\neq 0$, *то система имеет единственное решение, которое находится по формулам*:

$$x_1=\frac{D_1}{D},\quad x_2=\frac{D_2}{D},\ \ldots,\ x_n=\frac{D_n}{D}. \qquad (8)$$

Формулы (8) известны под названием *формул Крамера*.

Пример. С помощью формул Крамера решить систему:

$$\begin{aligned}x_1+x_2+x_3+x_4&=5,\\ x_1+2x_2-x_3+4x_4&=-2,\\ 2x_1-3x_2-x_3-5x_4&=-2,\\ 3x_1+x_2+2x_3+11x_4&=0.\end{aligned}$$

Сперва составляем и вычисляем определитель системы

$$D=\begin{vmatrix}1&1&1&1\\1&2&-1&4\\2&-3&-1&-5\\3&1&2&11\end{vmatrix}=-142.$$

Итак, $D\neq 0$, и потому формулы Крамера применимы. Составляем

определители:

$$D_1=\begin{vmatrix} 5 & 1 & 1 & 1\\ -2 & 2 & -1 & 4\\ -2 & -3 & -1 & -5\\ 0 & 1 & 2 & 11 \end{vmatrix}=-142,$$

$$D_2=\begin{vmatrix} 1 & 5 & 1 & 1\\ 1 & -2 & -1 & 4\\ 2 & -2 & -1 & -5\\ 3 & 0 & 2 & 11 \end{vmatrix}=-284,$$

$$D_3=\begin{vmatrix} 1 & 1 & 5 & 1\\ 1 & 2 & -2 & 4\\ 2 & -3 & -2 & -5\\ 3 & 1 & 0 & 11 \end{vmatrix}=-426,$$

$$D_4=\begin{vmatrix} 1 & 1 & 1 & 5\\ 1 & 2 & -1 & -2\\ 2 & -3 & -1 & -2\\ 3 & 1 & 2 & 0 \end{vmatrix}=142,$$

откуда

$$x_1=\frac{D_1}{D}=1,\ x_2=\frac{D_2}{D}=2,\ x_3=\frac{D_3}{D}=3,\ x_4=\frac{D_4}{D}=-1.$$

Подстановкой в уравнения убеждаемся в правильности найденного решения.

Формулы Крамера пригодны лишь в случае $D\neq 0$. Однако можно привести многочисленные примеры систем уравнений с определителем $D=0$. Имеют ли подобные системы решения, а если имеют, то как эти решения найти? На этот вопрос мы ответим со всей подробностью во второй главе, а пока заметим; что при $D=0$ рассматриваемая система уравнений либо противоречива, либо допускает бесчисленное множество решений.

В заключение этого параграфа рассмотрим несколько детальнее один особый случай n линейных уравнений с n неизвестными. Мы имеем в виду однородные уравнения.

Система n линейных уравнений с n неизвестными называется *однородной*, если все свободные члены b_i равны нулю, т. е.

$$\left.\begin{aligned} a_{11}x_1+a_{12}x_2+\ \dots\ +a_{1n}x_n&=0,\\ a_{21}x_1+a_{22}x_2+\ \dots\ +a_{2n}x_n&=0,\\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ &\\ a_{n1}x_1+a_{n2}x_2+\ \dots\ +a_{nn}x_n&=0. \end{aligned}\right\} \qquad (9)$$

Пусть по крайней мере одно из неизвестных, например x_s, отлично от нуля. Для этого неизвестного можно написать уравнение

$$x_sD=D_s,$$

или, так как $D_s = 0$,

$$x_s D = 0.$$

Но один из сомножителей, а именно x_s, не равен нулю. Следовательно, должен быть равен нулю второй из сомножителей:

$$D = 0.$$

Итак, мы показали, что *ненулевые решения системы* (9) *могут быть только в случае* $D = 0$[1]). Во второй главе нашего курса будет показано, что и, обратно, когда $D = 0$, система обязательно имеет ненулевые решения.

Пример. При каких значениях k система уравнений

$$\begin{aligned} kx + y + z &= 0, \\ x + ky - z &= 0, \\ 2x - y + z &= 0 \end{aligned}$$

имеет ненулевые решения?

Необходимым условием является равенство нулю определителя D системы:

$$D = \begin{vmatrix} k & 1 & 1 \\ 1 & k & -1 \\ 2 & -1 & 1 \end{vmatrix} = 0.$$

Раскрывая определитель, будем иметь: $(k+1)(k-4) = 0$, откуда получаем два значения для k: $k_1 = -1$ и $k_2 = 4$.

Проверим, имеет ли система при этих значениях k ненулевые решения. При $k_1 = -1$ система такова:

$$\begin{aligned} -x + y + z &= 0, \\ x - y - z &= 0, \\ 2x - y + z &= 0. \end{aligned}$$

Мы видим, что второе уравнение является следствием первого, так как отличается от него лишь знаками всех членов. Таким образом мы в действительности имеем не три, а два уравнения с тремя неизвестными, т. е. неопределённую систему. Чтобы её решить, перенесём z в первом и третьем уравнениях в правую часть:

$$\begin{aligned} -x + y &= -z, \\ 2x - y &= -z, \end{aligned}$$

откуда найдём, что $x = -2z$, $y = -3z$. Если положить z, например,

---

[1]) К этому же выводу можно притти на основании следующих соображений. Пусть определитель D из коэффициентов системы (9) отличен от нуля; тогда по формулам Крамера получаем:

$$x_1 = \frac{D_1}{D} = \frac{0}{D} = 0, \quad x_2 = \frac{D_2}{D} = \frac{0}{D} = 0, \quad \ldots, \quad x_n = \frac{D_n}{D} = \frac{0}{D} = 0.$$

Здесь все определители $D_i = 0$, так как в каждом из них имеется столбец, состоящий из нулей. Таким образом в случае $D \neq 0$ однородная система (9) допускает лишь нулевое решение $x_1 = x_2 = \ldots = x_n = 0$.

равным 1, то получим как раз ненулевое решение

$$x=-2,\quad y=-3,\quad z=1.$$

При $k_2=4$ система имеет вид:

$$\begin{aligned}4x+y+z&=0,\\ x+4y-z&=0,\\ 2x-y+z&=0.\end{aligned}$$

И здесь одно уравнение является лишним. В самом деле, если из утроенного первого уравнения вычесть удвоенное второе и затем получившееся уравнение сократить на 5, то мы будем иметь как раз третье уравнение. Предоставляем читателю самостоятельно найти ненулевое решение.

§ 9. Теорема Лапласа. Правило умножения определителей

Как мы уже знаем, всякий определитель можно разложить по элементам строки или столбца (см. § 8), т. е. выразить через определители низшего порядка. Знаменитым французским математиком Лапласом была найдена гораздо более общая формула разложения, основанная на обобщении понятия минора и алгебраического дополнения.

Выделим в определителе D n-го порядка какие-нибудь k строк и k столбцов. Элементы, стоящие на пересечении этих строк и столбцов, образуют определитель M k-го порядка, который мы назовём *минором k-го порядка*. Вычеркнем затем в определителе D рассматриваемые строки и столбцы и сдвинем оставшиеся элементы. Мы получим второй минор M $(n-k)$-го порядка. *Миноры M и $\overline{M}$ называются взаимно дополнительными.*

Пример. Выделим в определителе пятого порядка

$$D=\begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15}\\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25}\\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35}\\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45}\\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55}\end{vmatrix}$$

первую и пятую строки, третий и четвёртый столбцы. Мы получим следующие два взаимно дополнительных минора:

$$M=\begin{vmatrix} a_{13} & a_{14}\\ a_{53} & a_{54}\end{vmatrix},\qquad M=\begin{vmatrix} a_{21} & a_{22} & a_{25}\\ a_{31} & a_{32} & a_{35}\\ a_{41} & a_{42} & a_{45}\end{vmatrix}.$$

Так обобщается понятие минора, данное в § 7. Теперь остаётся обобщить понятие алгебраического дополнения. Введём такое определение.

Определение. *Алгебраическим дополнением минора M k-го порядка называется дополнительный минор $\overline{M}$, умноженный на* $(-1)^{(\alpha_1+\alpha_2+\ldots+\alpha_k)+(\beta_1+\beta_2+\ldots+\beta_k)}$, где $\alpha_1, \alpha_2, \ldots, \alpha_k$ и $\beta_1, \beta_2, \ldots, \beta_k$ *соответственно номера строк и столбцов, входящих в минор M.*

Например алгебраическим дополнением минора

$$M = \begin{vmatrix} a_{12} & a_{14} \\ a_{53} & a_{54} \end{vmatrix}$$

определителя пятого порядка является

$$(-1)^{(1+5)+(3+4)} \begin{vmatrix} a_{21} & a_{22} & a_{25} \\ a_{31} & a_{32} & a_{35} \\ a_{41} & a_{42} & a_{45} \end{vmatrix} = - \begin{vmatrix} a_{21} & a_{22} & a_{25} \\ a_{31} & a_{32} & a_{35} \\ a_{41} & a_{42} & a_{45} \end{vmatrix}.$$

После этих предварительных приготовлений мы можем уже легко сформулировать теорему Лапласа.

Теорема Лапласа. *Выделим в определителе D произвольно k строк (столбцов). Тогда определитель D равен сумме произведений всех миноров k-го порядка, составленных из элементов этих строк (столбцов), на их алгебраические дополнения.*

Пример. В определителе

$$D = \begin{vmatrix} 3 & 2 & 0 & 1 \\ -1 & 0 & 5 & 3 \\ 3 & -1 & 2 & 5 \\ 1 & -1 & 1 & -1 \end{vmatrix}$$

выделим первые две строки и составим всевозможные миноры второго порядка, содержащиеся в этих строках. Это будут миноры

$$M_1 = \begin{vmatrix} 3 & 2 \\ -1 & 0 \end{vmatrix}, \quad M_2 = \begin{vmatrix} 3 & 0 \\ -1 & 5 \end{vmatrix}, \quad M_3 = \begin{vmatrix} 3 & 1 \\ -1 & 3 \end{vmatrix},$$

$$M_4 = \begin{vmatrix} 2 & 0 \\ 0 & 5 \end{vmatrix}, \quad M_5 = \begin{vmatrix} 2 & 1 \\ 0 & 3 \end{vmatrix}, \quad M_6 = \begin{vmatrix} 0 & 1 \\ 5 & 3 \end{vmatrix}.$$

А теперь напишем соответствующие алгебраические дополнения:

$$A_1 = (-1)^{(1+2)+(1+2)} \begin{vmatrix} 2 & 5 \\ 1 & -1 \end{vmatrix}, \quad A_2 = (-1)^{(1+2)+(1+3)} \begin{vmatrix} -1 & 5 \\ -1 & -1 \end{vmatrix},$$

$$A_3 = (-1)^{(1+2)+(1+4)} \begin{vmatrix} -1 & 2 \\ -1 & 1 \end{vmatrix}, \quad A_4 = (-1)^{(1+2)+(2+3)} \begin{vmatrix} 3 & 5 \\ 1 & -1 \end{vmatrix},$$

$$A_5 = (-1)^{(1+2)+(2+4)} \begin{vmatrix} 3 & 2 \\ 1 & 1 \end{vmatrix}, \quad A_6 = (-1)^{(1+2)+(3+4)} \begin{vmatrix} 3 & -1 \\ 1 & -1 \end{vmatrix}.$$

Таким образом согласно теореме Лапласа:

$$D = \begin{vmatrix} 3 & 2 \\ -1 & 0 \end{vmatrix} \cdot \begin{vmatrix} 2 & 5 \\ 1 & -1 \end{vmatrix} - \begin{vmatrix} 3 & 0 \\ -1 & 5 \end{vmatrix} \cdot \begin{vmatrix} -1 & 5 \\ -1 & -1 \end{vmatrix} +$$

$$+ \begin{vmatrix} 3 & 1 \\ -1 & 3 \end{vmatrix} \cdot \begin{vmatrix} -1 & 2 \\ -1 & 1 \end{vmatrix} + \begin{vmatrix} 2 & 0 \\ 0 & 5 \end{vmatrix} \cdot \begin{vmatrix} 3 & 5 \\ 1 & -1 \end{vmatrix} -$$

$$- \begin{vmatrix} 2 & 1 \\ 0 & 3 \end{vmatrix} \cdot \begin{vmatrix} 3 & 2 \\ 1 & 1 \end{vmatrix} + \begin{vmatrix} 0 & 1 \\ 5 & 3 \end{vmatrix} \cdot \begin{vmatrix} 3 & -1 \\ 1 & -1 \end{vmatrix} =$$

$$= 2 \cdot (-7) - 15 \cdot 6 + 10 \cdot 1 + 10 \cdot (-8) - 6 \cdot 1 + (-5) \cdot (-2) = -170.$$

Тот же результат получается с помощью обычного метода вычисления определителя.

Переходим к доказательству теоремы Лапласа, для чего рассмотрим следующую лемму.

Лемма. *Каждый член произведения минора на его алгебраическое дополнение является вместе с тем членом определителя.*

Доказательство. Надо различать два случая.

Первый случай: минор M находится в левом верхнем углу определителя, т. е. занимает такое положение:

$$\left|\begin{array}{ccc|ccc} a_{11} & \dots & a_{1k} & a_{1k+1} & \dots & a_{1n} \\ \cdot & & \cdot & \cdot & & \cdot \\ \cdot & M & \cdot & \cdot & & \cdot \\ \cdot & & \cdot & \cdot & & \cdot \\ a_{k1} & \dots & a_{kk} & a_{kk+1} & \dots & a_{kn} \\ \hline a_{k+1\,1} & \dots & a_{k+1\,k} & a_{k+1\,k+1} & \dots & a_{k+1\,n} \\ \cdot & & \cdot & \cdot & & \cdot \\ \cdot & & \cdot & \cdot & \overline{M} & \cdot \\ \cdot & & \cdot & \cdot & & \cdot \\ a_{n1} & \dots & a_{nk} & a_{nk+1} & \dots & a_{nn} \end{array}\right|.$$

Дополнительный минор $\overline{M}$ находится в правом нижнем углу. Легко видеть, что алгебраическое дополнение минора M равно $(-1)^{(1+2+\dots+k)+(1+2+\dots+k)}\overline{M} = (-1)^{2(1+2+\dots+k)}\overline{M} = \overline{M}$. Любой член минора M имеет вид:

$$(-1)^p a_{1i_1} a_{2i_2} \dots a_{ki_k},$$

где p—число инверсий во вторых индексах $i_1, i_2, \dots, i_k$. Любой член дополнительного минора $\overline{M}$ выглядит так:

$$(-1)^q a_{k+1j_1} a_{k+2j_2} \dots a_{nj_{n-k}},$$

где q—число инверсий во вторых индексах $j_1, j_2, \dots, j_{n-k}$. Следовательно, любой член произведения $M\overline{M}$ имеет вид:

$$(-1)^{p+q} a_{1i_1} a_{2i_2} \dots a_{ki_k} a_{k+1j_1} \dots a_{nj_{n-k}}. \qquad (1)$$

Подсчитаем число s инверсий в расположении $i_1 i_2 \dots i_k j_1 j_2 \dots j_{n-k}$ вторых индексов члена (1). Мы уже знаем, что между индексами $i_1, i_2, \dots, i_k$ имеется p инверсий и между индексами $j_1, j_2, \dots, j_{n-k}$ q инверсий. Этим исчерпываются все инверсии в расположении $i_1 i_2 \dots i_k j_1 j_2 \dots j_{n-k}$, так как любое i меньше всякого j. Таким образом видим, что общее число инверсий $s = p + q$, откуда ясно, что выражение (1) есть член определителя D. Итак, лемма для первого случая доказана.

Второй случай: минор M не находится в левом верхнем углу. Этот случай легко приводится к первому.

Пусть минор состоит из строк с номерами $\alpha_1, \alpha_2, \dots, \alpha_k$ и столбцов с номерами $\beta_1, \beta_2, \dots, \beta_k$. Передвинем α_1-ю строку на первое

место, для чего будем её переставлять последовательно с лежащи выше неё строками; очевидно, что при этом придётся совершi $\alpha_1 - 1$ транспозиций. Подобным же образом передвинем и α_2-ю ст ку на второе место, для чего придётся совершить $\alpha_2 - 2$ транс зиций, и так поступим со всеми строками с номерами $\alpha_3, \alpha_4, \ldots$, пока после

$$(\alpha_1 - 1) + (\alpha_2 - 2) + \ldots + (\alpha_k - k) = \\ = (\alpha_1 + \alpha_2 + \ldots + \alpha_k) - (1 + 2 + \ldots + k)$$

транспозиций минор M не окажется в верхней половине оп делителя.

Затем, чтобы переместить минор M в левый верхний угол; пе двигаем β_1-й столбец на первое место, β_2-й столбец на второе ме и т. д., наконец, β_k-й столбец на k-е место, для чего придё совершить ещё

$$(\beta_1 - 1) + (\beta_2 - 2) + \ldots + (\beta_k - k) = \\ = (\beta_1 + \beta_2 + \ldots + \beta_k) - (1 + 2 + \ldots + k)$$

транспозиций; при этом дополнительный минор M перейдёт правый нижний угол.

В общей сложности придётся произвести всего

$$(\alpha_1 + \alpha_2 + \ldots + \alpha_k) + (\beta_1 + \beta_2 + \ldots + \beta_k) - 2(1 + 2 + \ldots +$$

транспозиций строк и столбцов, откуда по свойству II (см. § 6) нов определитель D_1, содержащий минор M в левом верхнем углу, д жен отличаться от D множителем

$$(-1)^{(\alpha_1+\alpha_2+\ldots+\alpha_k)+(\beta_1+\beta_2+\ldots+\beta_k)-2(1+2+\ldots+k)} = \\ = (-1)^{(\alpha_1+\alpha_2+\ldots+\alpha_k)+(\beta_1+\beta_2+\ldots+\beta_k)}.$$

Члены произведения $M\overline{M}$ должны быть также членами опре лителя D_1 (см. первый случай); поэтому члены произведения

$$(-1)^{(\alpha_1+\alpha_2+\ldots+\alpha_k)+(\beta_1+\beta_2+\ldots+\beta_k)} MM = MA$$

(здесь A—алгебраическое дополнение минора M) являются вме с тем членами определителя D. Итак, лемма доказана и для втор случая.

Теперь теорема Лапласа доказывается без всякого труда.

Доказательство теоремы Лапласа. Пу в определителе D выделено k строк (столбцов). Обозначим всевозм ные миноры k-го порядка, содержащиеся в этих строках (столбц через $M_1, M_2, \ldots, M_t$, а их алгебраические дополнения соотве венно через $A_1, A_2, \ldots, A_t$. Нам надо показать, что

$$M_1A_1 + M_2A_2 + \ldots + M_tA_t = D.$$

Согласно лемме каждое из произведений M_iA_i состоит из чле определителя D; при этом никакие два произведения M_iA_i M_jA_j не могут иметь подобных членов, так как миноры M_i и M_j

чаются друг от друга по меньшей мере одним столбцом. Таким азом сумма

$$M_1A_1 + M_2A_2 + \ldots + M_tA_t \qquad (2)$$

тоит из различных членов определителя D. Для окончательго доказательства теоремы остаётся, следовательно, показать, о в состав суммы (2) входят все $n!$ членов определителя D. Подитаем для этого число членов суммы (2). Каждый минор M_i, как ределитель k-го порядка, состоит из $k!$ членов; его алгебраическое дополнение A_i состоит из $(n-k)!$ членов. Следовательно, ходит, что каждое произведение M_iA_i состоит из $k!\,(n-k)!$ членов, куда сумма (2) содержит $tk!\,(n-k)!$ членов. Найдём, чему равно t, з k выделенных строк можно составить столько миноров M_i, колько существует сочетаний из n элементов по k. Следовательно,

$$t = C_n^k = \frac{n!}{k!\,(n-k)!}.$$

одставляя в $tk!\,(n-k)!$ это значение t, получим

$$\frac{n!}{k!\,(n-k)!}\,k!\,(n-k)! = n!,$$

е. число всех членов определителя D.

Среди приложений теоремы Лапласа наиболее замечательно дно: с помощью теоремы Лапласа произведение двух определителей сегда можно представить в виде одного определителя. Покажем это а конкретном примере. Перемножим, например, определители

$$D_1 = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}, \qquad D_2 = \begin{vmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{vmatrix}.$$

Легко видеть, что определитель пятого порядка

$$\Delta = \begin{vmatrix} a_1 & b_1 & 0 & 0 & 0 \\ a_2 & b_2 & 0 & 0 & 0 \\ u_1 & v_1 & \alpha_1 & \beta_1 & \gamma_1 \\ u_2 & v_2 & \alpha_2 & \beta_2 & \gamma_2 \\ u_3 & v_3 & \alpha_3 & \beta_3 & \gamma_3 \end{vmatrix},$$

где u и v—произвольные величины, как раз равен произведению D_1D_2. Действительно, разлагая Δ по минорам первых двух строк, получим:

$$\Delta = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \cdot \begin{vmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{vmatrix}.$$

Но особенно замечателен тот случай, когда перемножаются определители одинакового порядка. Мы собираемся доказать следующее правило.

Правило перемножения определителей. *Чтобы перемножить два определителя n-го порядка*

$$D_1=\begin{vmatrix} a_{11}\dots a_{1n} \\ \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \\ a_{n1}\dots a_{nn} \end{vmatrix},\qquad D_2=\begin{vmatrix} b_{11}\dots b_{1n} \\ \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \\ b_{n1}\dots b_{nn} \end{vmatrix},$$

надо элементы i-й строки определителя D_1 умножить на соответствующие элементы j-го столбца определителя D_2 и все эти произведения сложить:

$$c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\dots+a_{in}b_{nj}.$$

Определитель

$$\Delta=\begin{vmatrix} c_{11}\dots c_{1n} \\ \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \\ c_{n1}\dots c_{nn} \end{vmatrix}$$

как раз и является произведением определителей D_1 и D_2.

Пример. Перемножим

$$D_1=\begin{vmatrix} 1 & 0 & 2 \\ -1 & 1 & 0 \\ 3 & 2 & 1 \end{vmatrix} \text{ и } \quad D_2=\begin{vmatrix} 2 & 0 & 5 \\ 7 & 1 & 0 \\ -1 & 1 & -1 \end{vmatrix}.$$

Для этого вычисляем c_{ij}. Элемент c_{11} равен сумме произведений элементов первой строки определителя D_1 на соответствующие элементы первого столбца определителя D_2:

$$c_{11}=1\cdot 2+0\cdot 7+2\cdot(-1)=0.$$

Точно так же имеем:

$c_{12}=1\cdot 0+0\cdot 1+2\cdot 1=2,$ $\quad c_{13}=1\cdot 5+0\cdot 0+2\cdot(-1)=3,$

$c_{21}=(-1)\cdot 2+1\cdot 7+0\cdot(-1)=5,$ $\quad c_{22}=(-1)\cdot 0+1\cdot 1+0\cdot 1=1,$

$c_{23}=(-1)\cdot 5+1\cdot 0+0\cdot(-1)=-5,$ $\quad c_{21}=3\cdot 2+2\cdot 7+1\cdot(-1)=19,$

$c_{32}=3\cdot 0+2\cdot 1+1\cdot 1=3,$ $\quad c_{33}=3\cdot 5+2\cdot 0+1\cdot(-1)=14,$

откуда

$$\begin{vmatrix} 1 & 0 & 2 \\ -1 & 1 & 0 \\ 3 & 2 & 1 \end{vmatrix}\cdot\begin{vmatrix} 2 & 0 & 5 \\ 7 & 1 & 0 \\ -1 & 1 & -1 \end{vmatrix}=\begin{vmatrix} 0 & 2 & 3 \\ 5 & 1 & -5 \\ 19 & 3 & 14 \end{vmatrix}.$$

И в самом деле

$$\begin{vmatrix} 1 & 0 & 2 \\ -1 & 1 & 0 \\ 3 & 2 & 1 \end{vmatrix}=-9,\qquad \begin{vmatrix} 2 & 0 & 5 \\ 7 & 1 & 0 \\ -1 & 1 & -1 \end{vmatrix}=38,$$

$$\begin{vmatrix} 0 & 2 & 3 \\ 5 & 1 & -5 \\ 19 & 3 & 14 \end{vmatrix}=-342,\qquad -9\cdot 38=-342.$$

Доказательство правила умножения. По теореме Лапласа определитель $2n$-го порядка

$$\Delta = \begin{vmatrix} a_{11} & a_{12}\cdots & a_{1n} & 0 & 0 & \cdots 0 \\ a_{21} & a_{22}\cdots & a_{2n} & 0 & 0 & \cdots 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2}\cdots & a_{nn} & 0 & 0 & \cdots 0 \\ -1 & 0 \cdots & 0 & b_{11} & b_{12} & \cdots b_{1n} \\ 0 & -1 \cdots & 0 & b_{21} & b_{22} & \cdots b_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 \cdots & -1 & b_{n1} & b_{n2} & \cdots b_{nn} \end{vmatrix}$$

равен произведению $D_1 D_2$. Преобразуем определитель Δ так, чтобы элементы b_{ij} превратились в нули. Для этого умножим первый столбец на b_{11}, второй на b_{21} и т. д., n-й на b_{n1} и прибавим к $(n+1)$-му столбцу. Затем умножим первый столбец на b_{12}, второй на b_{22} и т. д., n-й на b_{n2} и прибавим к $(n+2)$-му столбцу. Вообще, умножим первый столбец на b_{1k}, второй на b_{2k} и т. д., n-й на b_{nk} и прибавим к $(n+k)$-му столбцу.

После таких преобразований определитель Δ примет следующий вид:

$$\Delta = \begin{vmatrix} a_{11} & a_{12}\cdots & a_{1n} & c_{11} & c_{12}\cdots c_{1n} \\ a_{21} & a_{22}\cdots & a_{2n} & c_{21} & c_{22}\cdots c_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2}\cdots & a_{nn} & c_{n1} & c_{n2}\cdots c_{nn} \\ -1 & 0 \cdots & 0 & 0 & 0 \cdots 0 \\ 0 & -1 \cdots & 0 & 0 & 0 \cdots 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 \cdots & -1 & 0 & 0 \cdots 0 \end{vmatrix}.$$

Этот определитель разложим по минорам последних n строк. Мы видим, что минор

$$M = \begin{vmatrix} -1 & 0\cdots & 0 \\ 0 & -1\cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & 0\cdots & -1 \end{vmatrix} = (-1)^n$$

есть единственный минор, отличный от нуля. Его алгебраическое дополнение A равно

$$A = (-1)^{[(n+1)+\ldots+2n]+[1+2+\ldots+n]} \begin{vmatrix} c_{11}\cdots c_{1n} \\ \cdots \\ c_{n1}\cdots c_{nn} \end{vmatrix} =$$

$$= (-1)^{n(2n+1)} \begin{vmatrix} c_{11}\cdots c_{1n} \\ \cdots \\ c_{n1}\cdots c_{nn} \end{vmatrix},$$

откуда

$$\Delta = MA = (-1)^{2n(n+1)} \begin{vmatrix} c_{11} \dots c_{1n} \\ \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \\ c_{n1} \dots c_{nn} \end{vmatrix}$$

или, так как $2n(n+1)$ — чётное число:

$$\Delta = \begin{vmatrix} c_{11} \dots c_{1n} \\ \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \\ c_{n1} \dots c_{nn} \end{vmatrix},$$

что и требовалось показать.

Задачи. 1. Перемножить определители

а) $\begin{vmatrix} a & b \\ a_1 & b_1 \end{vmatrix}$ и $\begin{vmatrix} c & d \\ c_1 & d_1 \end{vmatrix}$;

b) $\begin{vmatrix} 5 & 1 & 2 \\ 3 & 1 & 6 \\ 2 & 3 & -1 \end{vmatrix}$ и $\begin{vmatrix} 1 & 2 & 3 \\ 3 & -1 & 0 \\ 1 & 5 & 8 \end{vmatrix}$;

c) $\begin{vmatrix} 1 & 2 & 0 & 8 \\ 1 & 3 & -1 & 7 \\ 1 & -1 & 2 & 4 \\ 1 & 5 & 3 & 11 \end{vmatrix}$ и $\begin{vmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \\ 3 & 4 & 1 & 2 \\ 2 & 3 & 4 & 1 \end{vmatrix}$.

2. С помощью правила умножения определителей вывести тождества

а) $(ab_1 - a_1b)^2 = (a^2 + b^2)(a_1^2 + b_1^2) - (aa_1 + bb_1)^2$;

b) $(a^2 + b^2)(a_1^2 + b_1^2) = (aa_1 - bb_1)^2 + (ab_1 + a_1b)^2$.

Указание. Для вывода первого тождества следует перемножить

$$\begin{vmatrix} a & b \\ a_1 & b_1 \end{vmatrix} \text{ и } \begin{vmatrix} a & a_1 \\ b & b_1 \end{vmatrix},$$

а для вывода второго тождества

$$\begin{vmatrix} a & b \\ -b & a \end{vmatrix} \text{ и } \begin{vmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{vmatrix}.$$

3. Показать, что помимо указанного выше правила перемножения существуют следующие три различных способа умножения определителей D_1 и D_2:
1) можно строки D_1 комбинировать со строками D_2;
2) можно столбцы D_1 комбинировать со строками D_2;
3) можно столбцы D_1 комбинировать со столбцами D_2.

§ 10. Методы вычисления определителей

Существует целый ряд различных приёмов вычисления определителей; с несколькими из них мы уже познакомились в § 7, некоторые другие мы покажем на ряде примеров.

Пример 1. Вычислим

$$D=\begin{vmatrix} a+x_1 & a & \dots & a \\ a & a+x_2 & \dots & a \\ \dots & \dots & \dots & \dots \\ a & a & \dots & a+x_{n-1} \\ a & a & \dots & a \end{vmatrix} \quad \begin{matrix} a \\ a \\ \dots \\ a \\ a \end{matrix}.$$

Вычтем из первых $n-1$ столбцов последний, в результате чего получится

$$D=\begin{vmatrix} x_1 & 0 & \dots & a \\ 0 & x_2 & \dots & a \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a \\ 0 & 0 & \dots & a \end{vmatrix} \quad \begin{matrix} a \\ a \\ \dots \\ a \\ a \end{matrix}.$$

Все элементы ниже главной диагонали обратились в нуль; поэтому D равно произведению диагональных элементов:

$$D=ax_1x_2\dots x_{n-1}.$$

Пример 2. В некоторых случаях оказывается выгоднее не делать нули, а сразу разлагать определитель по элементам строки или столбца. Возьмём в качестве примера хотя бы такой определитель:

$$\Delta=\begin{vmatrix} a & b & 0 & \dots & 0 & 0 \\ 0 & a & b & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a & b \\ b & 0 & 0 & \dots & 0 & a \end{vmatrix}.$$

Разлагаем Δ по элементам первого столбца:

$$a\begin{vmatrix} a & b & 0 & \dots & 0 & 0 \\ 0 & a & b & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a & b \\ 0 & 0 & 0 & \dots & 0 & a \end{vmatrix} + b\cdot(-1)^{n+1}\begin{vmatrix} b & 0 & 0 & \dots & 0 & 0 \\ a & b & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & b & 0 \\ 0 & 0 & 0 & \dots & a & b \end{vmatrix}=$$

$$=a\cdot a^{n-1}+b\cdot(-1)^{n+1}b^{n-1}=a^n+(-1)^{n+1}b^n,$$

так как в первом миноре все элементы ниже главной диагонали равны нулю, а во втором—выше главной диагонали равны нулю.

Пример 3. В других случаях целесообразнее делать частично нули и затем разлагать по элементам строки или столбца. Так, определитель

$$\Delta_n=\begin{vmatrix} a+x_1 & a & \dots & a \\ a & a+x_2 & \dots & a \\ \dots & \dots & \dots & \dots \\ a & a & \dots & a+x_{n-1} \\ a & a & \dots & a+x_n \end{vmatrix} \quad (1)$$

сравнительно быстро вычисляется следующим способом. Вычтем из последнего столбца первый. Получим:

$$A_n=\begin{vmatrix} a+x_1 & a & a & \dots a & -x_1 \\ a & a+x_2 & a & \dots a & 0 \\ a & a & a+x_3 & \dots a & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a & a & a & \dots a+x_{n-1} & 0 \\ a & a & a & \dots a & x_n \end{vmatrix}.$$

Теперь, разлагая по элементам последнего столбца, будем иметь:

$$A_n=(-x_1)\cdot(-1)^{1+n}\begin{vmatrix} a & a+x_2 & a & \dots a \\ a & a & a+x_3 & \dots a \\ \dots & \dots & \dots & \dots \\ a & a & a & \dots a+x_{n-1} \\ a & a & a & \dots a \end{vmatrix}+$$

$$+x_n\begin{vmatrix} a+x_1 & a & a\dots a \\ a & a+x_2 & a\dots a \\ \dots & \dots & \dots \\ a & a & a\dots a \\ a & a & a\dots a+x_{n-1} \end{vmatrix}. \qquad (2)$$

Первый минор несколько преобразуем. А именно, переставим последовательно первый столбец со вторым, третьим, ..., (n—1)-м столбцом. Всего придётся совершить n—2 перестановок, при каждой перестановке столбцов минор будет менять свой знак (см. § 6, свойство II) и в результате превратится в

$$(-1)^{n-2}\begin{vmatrix} a+x_2 & a & \dots a & a \\ a & a+x_3 & \dots a & a \\ \dots & \dots & \dots & \dots \\ a & a & \dots a+x_{n-1} & a \\ a & a & \dots a & a \end{vmatrix}=(-1)^{n-2}ax_2x_3\dots x_{n-1}$$

(см. пример 1).

Что касается второго минора разложения (2), то он того же типа, что и определитель A_n, но его порядок на единицу ниже. Поэтому мы этот минор обозначим через A_{n-1}. Таким образом разложение (2) принимает следующий вид:

$$A_n=ax_1x_2\dots x_{n-1}+A_{n-1}x_n. \qquad (3)$$

Если значение определителя A_{n-1} известно, то из формулы (3) значение A_n находится без всякого труда. Предлагаем читателю показать с помощью равенства (3), что

$$A_n=x_1x_2\dots x_n\left(\frac{a}{x_1}+\frac{a}{x_2}+\dots+\frac{a}{x_n}+1\right).$$

Пример 4. Некоторые определители удобно вычислять с помощью теоремы Лапласа. Вычислим определитель:

$$\delta = \begin{vmatrix} a & b & 0 & 0 & c & 0 \\ a_1 & b_1 & 0 & 0 & 0 & c_1 \\ 0 & 0 & a & b & d & 0 \\ 0 & 0 & a_1 & b_1 & 0 & d_1 \\ a_2 & b_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & a_2 & b_2 & 0 & 0 \end{vmatrix}.$$

Разложим этот определитель по минорам третьего, четвёртого и пятого столбцов. Легко видеть, что отличными от нуля будут только четыре минора:

$$M_1 = \begin{vmatrix} 0 & 0 & c \\ a & b & d \\ a_1 & b_1 & 0 \end{vmatrix}, \quad M_2 = \begin{vmatrix} 0 & 0 & c \\ a & b & d \\ a_2 & b_2 & 0 \end{vmatrix},$$

$$M_3 = \begin{vmatrix} 0 & 0 & c \\ a_1 & b_1 & 0 \\ a_2 & b_2 & 0 \end{vmatrix}, \quad M_4 = \begin{vmatrix} a & b & d \\ a_1 & b_1 & 0 \\ a_2 & b_2 & 0 \end{vmatrix}.$$

Выписываем соответствующие алгебраические дополнения:

$$A_1 = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & 0 \\ 0 & 0 & 0 \end{vmatrix} = 0, \quad A_2 = \begin{vmatrix} a_1 & b_1 & c_1 \\ 0 & 0 & d_1 \\ a_2 & b_2 & 0 \end{vmatrix},$$

$$A_3 = -\begin{vmatrix} a_1 & b_1 & c_1 \\ 0 & 0 & 0 \\ a_2 & b_2 & 0 \end{vmatrix} = 0, \quad A_4 = -\begin{vmatrix} a & b & 0 \\ a_1 & b_1 & c_1 \\ a_2 & b_2 & 0 \end{vmatrix}.$$

Таким образом:

$$\delta = \begin{vmatrix} 0 & 0 & c \\ a & b & d \\ a_1 & b_1 & 0 \end{vmatrix} \cdot 0 + \begin{vmatrix} 0 & 0 & c \\ a & b & d \\ a_2 & b_2 & 0 \end{vmatrix} \cdot \begin{vmatrix} a_1 & b_1 & c_1 \\ 0 & 0 & d_1 \\ a_2 & b_2 & 0 \end{vmatrix} +$$

$$+ \begin{vmatrix} 0 & 0 & c \\ a_1 & b_1 & 0 \\ a_2 & b_2 & 0 \end{vmatrix} \cdot 0 - \begin{vmatrix} a & b & d \\ a_1 & b_1 & 0 \\ a_2 & b_2 & 0 \end{vmatrix} \cdot \begin{vmatrix} a & b & 0 \\ a_1 & b_1 & c_1 \\ a_2 & b_2 & 0 \end{vmatrix} =$$

$$= \begin{vmatrix} 0 & 0 & c \\ a & b & d \\ a_2 & b_2 & 0 \end{vmatrix} \cdot \begin{vmatrix} a_1 & b_1 & c_1 \\ 0 & 0 & d_1 \\ a_2 & b_2 & 0 \end{vmatrix} - \begin{vmatrix} a & b & d \\ a_1 & b_1 & 0 \\ a_2 & b_2 & 0 \end{vmatrix} \cdot \begin{vmatrix} a & b & 0 \\ a_1 & b_1 & c_1 \\ a_2 & b_2 & 0 \end{vmatrix}$$

или

$$\delta = c \begin{vmatrix} a & b \\ a_2 & b_2 \end{vmatrix} \cdot (-d_1) \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} - d \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \cdot (-c_1) \begin{vmatrix} a & b \\ a_2 & b_2 \end{vmatrix} =$$

$$= \begin{vmatrix} a & b \\ a_2 & b_2 \end{vmatrix} \cdot \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} (c_1 d - c d_1),$$

откуда окончательно:

$$\delta = (ab_2 - a_2b)(a_1b_2 - a_2b_1)(c_1d - cd_1).$$

В заключение разберём пример на вычисление определителя путём умножения его на другой определитель.

Пример 5. Найдём значение определителя

$$D = \begin{vmatrix} -a & b & c & d \\ b & -a & d & c \\ c & d & -a & b \\ d & c & b & -a \end{vmatrix}.$$

Применим следующий приём: умножим D на

$$H = \begin{vmatrix} 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{vmatrix} \neq 0.$$

Тогда по правилу умножения определителей получим:

$$DH = \begin{vmatrix} -a+b+c+d & a-b+c+d & a+b-c+d & a+b+c-d \\ b-a+d+c & -b+a+d+c & -b-a-d+c & -b-a+d-c \\ c+d-a+b & -c-d-a+b & -c+d+a+b & -c+d-a-b \\ d+c+b-a & -d-c+b-a & -d+c-b-a & -d+c+b+a \end{vmatrix}$$

или, вынося из первого столбца множитель $(b+c+d-a)$, из второго столбца множитель $-(a+c+d-b)$, из третьего столбца множитель $-(a+b+d-c)$ и из четвёртого множитель $-(a+b+c-d)$ получим:

$$DH = -(b+c+d-a)(a+c+d-b) \times \\ \times (a+b+d-c)(a+b+c-d) \begin{vmatrix} 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{vmatrix}. \quad (4$$

Мы видим, что в правой части равенства (4) появился определитель H и потому (4) можно переписать следующим образом:

$$DH = -(b+c+d-a)(a+c+d-b)(a+b+d-c)(a+b+c-d)H,$$

откуда, сокращая на H, получим:

$$D = -(b+c+d-a)(a+c+d-b)(a+b+d-c)(a+b+c-d).$$

Впрочем, определитель D можно было вычислить более естественным способом; не прибегая к умножению на H.

В самом деле, прибавим к первой строке сумму остальных строк:

$$\begin{vmatrix} b+c+d-a & b+c+d-a & b+c+d-a & b+c+d-a \\ b & -a & d & c \\ c & d & -a & b \\ d & c & b & -a \end{vmatrix} =$$

$$= (b+c+d-a) \begin{vmatrix} 1 & 1 & 1 & 1 \\ b & -a & d & c \\ c & d & -a & b \\ d & c & b & -a \end{vmatrix}.$$

В первой строке появились единицы, и мы легко можем все элементы этой строки, кроме первого, превратить в нули. Вычтем хотя бы первый столбец из всех остальных столбцов. Получим:

$$(b+c+d-a) \begin{vmatrix} 1 & 0 & 0 & 0 \\ b & -a-b & d & -b & c-b \\ c & d-c & -a & -c & b-c \\ d & c-d & b & -d & -a-d \end{vmatrix} =$$

$$= (b+c+d-a) \begin{vmatrix} -a-b & d & -b & c-b \\ d-c & -a & -c & b-c \\ c-d & b & -d & -a-d \end{vmatrix}.$$

Теперь прибавим к первой строке вторую; тогда D примет следующий вид:

$$D = (b+c+d-a) \begin{vmatrix} -a-b-c+d & -a-b-c+d & 0 \\ d-c & -a-c & b-c \\ c-d & b-d & -a-d \end{vmatrix} =$$

$$= -(b+c+d-a)(a+b+c-d) \begin{vmatrix} 1 & 1 & 0 \\ d-c & -a-c & b-c \\ c-d & b-d & -a-d \end{vmatrix}.$$

Сделаем нули в первой строке, вычитая из второго столбца первый; получим

$$D = -(b+c+d-a)(a+b+c-d) \begin{vmatrix} 1 & 0 & 0 \\ d-c & -a-d & b-c \\ c-d & b-c & -a-d \end{vmatrix} =$$

$$= -(b+c+d-a)(a+b+c-d) \begin{vmatrix} -a-d & b-c \\ b-c & -a-d \end{vmatrix}.$$

Наконец прибавим к первой строке вторую:

$$-(b+c+d-a)(a+b+c-d)\times$$
$$\times\begin{vmatrix} -a-c-d+b & -a-c-d+b \\ b-c & -a-d \end{vmatrix} =$$
$$=(b+c+d-a)(a+b+c-d)(a+c+d-b)\begin{vmatrix} 1 & 1 \\ b-c & -a-d \end{vmatrix},$$

или, раскрывая определитель второго порядка:

$$D=-(b+c+d-a)\,(a+b+c-d)\,(a+c+d-b)\,(a+b+d-c).$$

Задачи. 1. Вычислить определители

а) $\begin{vmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & a & b \\ 1 & a & 0 & c \\ 1 & b & c & 0 \end{vmatrix}$, b) $\begin{vmatrix} 1+a & 1 & 1 & 1 \\ 1 & 1+b & 1 & 1 \\ 1 & 1 & 1+c & 1 \\ 1 & 1 & 1 & 1+d \end{vmatrix}$, c) $\begin{vmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{vmatrix}$,

d) $\begin{vmatrix} 1 & 2 & 3 & \dots & n \\ n & 1 & 2 & \dots & n-1 \\ n-1 & n & 1 & \dots & n-2 \\ \dots & \dots & \dots & \dots & \dots \\ 2 & 3 & 4 & \dots & 1 \end{vmatrix}$.

Указание к d): преобразовать так, чтобы все элементы выше главной диагонали обратились в нули.

2. Вычислить определитель

$$\begin{vmatrix} 1 & 5 & -1 & 7 & 3 \\ -1 & 0 & 1 & 4 & 0 \\ 1 & 1 & 2 & 3 & -1 \\ 5 & 0 & 1 & 1 & 0 \\ -1 & 1 & 3 & 2 & -2 \end{vmatrix}$$

разлагая его по минорам, составленным из второй и четвёртой строк.

3. С помощью теоремы Лапласа показать, что

$$\begin{vmatrix} a & b & c & d \\ a_1 & b_1 & c_1 & d_1 \\ d & c & b & a \\ d_1 & c_1 & b_1 & a_1 \end{vmatrix} = (ac_1-a_1c)^2+(bd_1-b_1d)^2-(ab_1-a_1b)^2-(cd_1-c_1d)^2-$$
$$-2(ad_1-a_1d)(bc_1-b_1c).$$

4. С помощью теоремы Лапласа вычислить следующие определители:

а) $\begin{vmatrix} 0 & a & b & c \\ 1 & d & 0 & 0 \\ 1 & 0 & e & 0 \\ 1 & 0 & 0 & f \end{vmatrix}$, b) $\begin{vmatrix} 0 & a_1 & b_1 & c_1 \\ a & 1 & 0 & 0 \\ b & 0 & 1 & 0 \\ c & 0 & 0 & 1 \end{vmatrix}$, c) $\begin{vmatrix} 1 & a & a & a \\ 1 & a & 0 & 0 \\ 1 & 0 & b & 0 \\ 1 & 0 & 0 & c \end{vmatrix}$.

5. Вычислить определитель

$$D=\begin{vmatrix} a & b & c & d \\ -b & a & d & -c \\ -c & -d & a & b \\ -d & c & -b & a \end{vmatrix}$$

путём возвышения его в квадрат.

Указание: в определителе D заменяем строки столбцами, в результате чего получится

$$D=\begin{vmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{vmatrix}.$$

Затем производим перемножение:

$$\begin{vmatrix} a & b & c & d \\ -b & a & d & -c \\ -c & -d & a & b \\ -d & c & -b & a \end{vmatrix} \cdot \begin{vmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{vmatrix}.$$

§ 11. Взаимный определитель

Заменим в определителе

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

элементы их алгебраическими дополнениями. Мы получим тогда новый определитель

$$\overline{D}=\begin{vmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \dots & \dots & \dots & \dots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{vmatrix}$$

(A_{ij}—алгебраическое дополнение элемента a_{ij}), который называется *взаимным относительно* D. Как мы сейчас увидим, между D и $\overline{D}$ имеется довольно простая зависимость.

Заменим в $\overline{D}$ строки столбцами и составим произведение

$$D\overline{D}=\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \cdot \begin{vmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{vmatrix}.$$

Согласно правилу умножения определителей это произведение равно определителю, у которого элементы c_{ij} составлены по следующему закону:

$$c_{ij}=a_{i1}A_{j1}+a_{i2}A_{j2}+\dots+a_{in}A_{jn}.$$

Но c_{ij} $(i\neq j)$ есть не что иное, как сумма произведений элементов одной строки на алгебраические дополнения соответствующих элементов другой строки; мы знаем, что такая сумма равна нулю (см. § 8, формулу (3)). Что касается элемента c_{ii}, то он, как сумма произведений элементов i-й строки на их алгебраиче-

ские дополнения, равен D [см. § 8, формулу (1)]. Итак, $c_{ij} = 0$ $(i \neq j)$ и $c_{ii} = D$, откуда

$$D\bar{D} = \begin{vmatrix} D & 0 & 0 & \dots & 0 \\ 0 & D & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & D \end{vmatrix} = D^n.$$

Если $D \neq 0$, то обе части равенства можно сократить на D:

$$D = D^{n-1}. \tag{1}$$

Остаётся показать, что соотношение (1) имеет место и при $D = 0$.

Если все элементы определителя D равны нулю, то все элементы A_{ik} взаимного определителя $\bar{D}$ будут, очевидно, также равны нулю, вследствие чего $\bar{D} = 0$. Поэтому остаётся разобрать тот случай, когда при $D = 0$ существует по меньшей мере один элемент определителя D, отличный от нуля. Без ограничения общности рассуждений предположим, что $a_{11} \neq 0$.

Легко видеть, что

$$a_{11}A_{i1} + a_{12}A_{i2} + \dots + a_{1n}A_{in} = 0 \tag{2}$$

при $i = 1, 2, \dots, n$. Действительно, при $i \neq 1$ левая часть равенства (2) равна нулю по формуле (3) § 8, а при $i = 1$ равна $D = 0$ по формуле (1) § 8. Так как $a_{11} \neq 0$, то из равенства (2) следует, что

$$A_{i1} = b_2A_{i2} + b_3A_{i3} + \dots + b_nA_{in}, \tag{3}$$

где $b_2 = -\dfrac{a_{12}}{a_{11}}$, $b_3 = -\dfrac{a_{13}}{a_{11}}$, $\dots$, $b_n = -\dfrac{a_{1n}}{a_{11}}$.

Вычтем теперь из первого столбца взаимного определителя $\bar{D}$ второй, третий, $\dots$, n-й столбцы, умноженные соответственно на $b_2, b_3, \dots, b_n$. Тогда в силу равенства (3) элементы первого столбца обратятся в нуль. Мы видим отсюда, что взаимный определитель $\bar{D}$ при $D = 0$ также равен нулю.

§ 12. Краткие исторические сведения

Зарождение теории определителей следует отнести к концу XVII века. В 1693 г. Лейбниц, изучая линейные уравнения со многими неизвестными, впервые подметил общий закон составления определителя. В письме к Лопиталю от 28 апреля 1693 г. Лейбниц сообщает, что своему открытию он обязан особому способу обозначения коэффициентов уравнения. Этот способ обозначения состоит в том, что каждый коэффициент обозначается двумя числами (система двойных индексов). Свои результаты Лейбниц, однако, не опубликовал, и потому они остались неизвестными его современникам.

В 1750 г. женевским профессором Крамером была опубликована работа, посвящённая теории алгебраических кривых. В приложении, помещённом в конце своего сочинения, Крамер указывает общий закон составления определителей и приводит общую формулу решения n линейных уравнений с n неизвестными — как раз ту формулу, которую мы вывели в § 8.

Однако ни Лейбниц, ни Крамер не дали более или менее законченной теории определителей. Первые шаги в этом направлении были сделаны французским математиком Вандермондом в мемуаре [1]), доложенном Парижской академии наук в 1771 г.

Дальнейшее и притом значительное развитие теория определителей получила в 1812 г., когда появились работы двух выдающихся французских мате-

[1]) A. Vandermonde, Mémoire sur l'élimination, Histoire de l'Académie Royale des Sciences, 1772.

матиков: Бине (J. Binet) и Коши (A. L. Cauchy) [1]): особенно важное значение имеет мемуар Коши, в котором дано настолько исчерпывающее изложение теории, что содержание современных учебников теории определителей не намного превосходит материал мемуара Коши. Отметим, что правило умножения определителей, которое мы разобрали в § 9, было установлено Бине и Коши.

С этого момента определители становятся одним из важных орудий математического исследования. В настоящее время нет почти ни одной отрасли математики, в которой определители не имели бы приложения. Мы их встречаем в алгебре, в аналитической геометрии, в механике, в теории чисел, в теории функций, в теории дифференциальных уравнений и т. д.[2]).

ГЛАВА ВТОРАЯ

ЛИНЕЙНЫЕ УРАВНЕНИЯ

§ 13. Линейные уравнения и линейные формы. Линейная зависимость

До сих пор мы имели дело только с такой системой n линейных уравнений с n неизвестными, определитель из коэффициентов которой не равен нулю. Однако на практике часто приходится сталкиваться с системами, у которых определитель равен нулю, и даже с такими системами, у которых число неизвестных не равно числу уравнений. Начнём с конкретных примеров; они помогут нам наметить общие методы исследования и решения подобных систем.

Пример 1. Рассмотрим следующую систему трёх уравнений с тремя неизвестными:

$$\left.\begin{aligned} x+2y-z&=2,\\ 2x-y+z&=3,\\ x+7y-4z&=3. \end{aligned}\right\} \qquad (1)$$

мы видим, что формулы Крамера неприменимы, так как

$$D=\begin{vmatrix} 1 & 2 & -1\\ 2 & -1 & 1\\ 1 & 7 & -4 \end{vmatrix}=0.$$

И всё же рассматриваемая система имеет не только одно, но даже бесчисленное множество решений. Присмотримся внимательнее к левым частям уравнений. Если мы их обозначим соответственно через f_1, f_2, f_3, то легко заметить, что они связаны следующей зависимостью:

---

[1]) J. Binet, Mémoire sur un Système des formules analytiques et leur applications à des considérations géométriques, *Journal de l'École Polytechnique*, тетрадь 16.

A. Cauchy, Mémoire sur les fonctions que ne peuvent obtenir que deux valeurs égales et de signes contraires par suite des transpositions opérés entre les variables qu' elles renferment, *Journal de l'École Polytechnique*, тетрадь 17.

[2]) Обстоятельные исторические сведения по теории определителей можно найти в книге T. Muir. The theory of determinants in the historical order of development, т. I—IV, 1906—1923.

$f_3 = 3f_1 - f_2$, которую мы назовём линейной. Мы видим, что эта линейная зависимость распространяется и на правые части: $3 = 3 \cdot 2 - 3$. Таким образом третье уравнение является следствием первых двух, и мы фактически имеем два уравнения с тремя неизвестными:

$$x + 2y - z = 2,$$
$$2x - y + z = 3.$$

Переносим z в правую часть и решаем относительно x и y:

$$x + 2y = 2 + z, \qquad 2x - y = 3 - z,$$
$$x = \frac{8 - z}{5}, \qquad y = \frac{3z + 1}{5}.$$

Итак, мы выразили x и y через z; но неизвестному z можно придавать произвольные числовые значения, при этом мы будем каждый раз получать решение системы (1). Например, полагая $z = 3$, получим решение

$$x = 1, \quad y = 2, \quad z = 3.$$

Пример 2. Рассмотрим теперь несколько иную систему:

$$x - y + z = 1,$$
$$x + y - z = 2,$$
$$3x - y + z = 3.$$

Здесь также $D = 0$, но система несовместна. В самом деле, обозначив левые части уравнений снова через f_1, f_2, f_3, получим такую линейную зависимость: $f_3 = 2f_1 + f_2$, которая, однако, не распространяется на правые части: $3 \neq 2 \cdot 1 + 2$. Таким образом, вычитая почленно из третьего уравнения удвоенное первое уравнение и второе уравнение, получим нелепость:

$$0 = -1.$$

Уже из этих примеров видно, какое важное значение имеет понятие линейной зависимости в общей теории линейных уравнений. Сформулируем это понятие точнее.

Назовём всякое выражение вида

$$f = a_1x_1 + a_2x_2 + \ldots + a_nx_n,$$

где $a_1, a_2, \ldots, a_n$—постоянные, *линейной формой* n неизвестных $x_1, x_2, \ldots, x_n$ и введём следующее определение.

Определение. *Линейные формы $f_1, f_2, \ldots, f_m$ называются линейно зависимыми, если можно подобрать такие постоянные числа $c_1, c_2, \ldots, c_m$, не все равные нулю, что имеет место тождество*

$$c_1f_1 + c_2f_2 + \ldots + c_mf_m \equiv 0.$$

Если же это тождество возможно только в том случае, когда все числа $c_1, c_2, \ldots, c_m$ равны нулю, то формы $f_1, f_2, \ldots, f_m$ называются линейно независимыми.

Пример 1. Возьмём следующие формы:

$$f_1 = x_1 + 2x_2 + 2x_3,$$
$$f_2 = -2x_1 + x_2 - x_3,$$
$$f_3 = x_1 - 3x_2 - x_3.$$

При некоторой наблюдательности можно заметить, что их сумма тождественно равна нулю. Таким образом рассматриваемые формы линейно зависимы:

$$f_1 + f_2 + f_3 \equiv 0.$$

Однако любые две формы будут уже линейно независимы. В самом деле; если бы, например, формы f_1 и f_2 были линейно зависимы, то их соответственные коэффициенты были бы пропорциональны, чего в действительности нет.

Из определения линейной зависимости можно сделать следующий вывод: если линейные формы $f_1, f_2, \ldots, f_m$ линейно зависимы, то хотя бы одну из них можно представить, как линейную комбинацию остальных форм. В самом деле, если линейные формы $f_1, f_2, \ldots, f_m$ линейно зависимы, то в тождестве

$$c_1 f_1 + c_2 f_2 + \ldots + c_m f_m \equiv 0$$

не все коэффициенты c_i равны нулю. Пусть, например, $c_i \neq 0$. Тогда форму f_i можно выразить через остальные формы:

$$f_i = \lambda_1 f_1 + \ldots + \lambda_{i-1} f_{i-1} + \lambda_{i+1} f_{i+1} + \ldots + \lambda_m f_m, \qquad \lambda_s = -\frac{c_s}{c_i}.$$

Пример 2. Рассмотрим следующую систему четырёх форм с пятью неизвестными:

$$f_1 = x_1 - x_2 + x_3 - x_4 + x_5, \qquad f_2 = x_1 + 2x_3 + x_5,$$
$$f_3 = x_1 - 5x_2 - x_3 + 2x_4 - x_5, \qquad f_4 = 3x_1 - 6x_2 + 2x_3 + x_4 + x_5.$$

Легко убедиться, что имеет место тождество

$$f_1 + f_2 + f_3 - f_4 \equiv 0,$$

откуда и следует, что четыре формы f_1, f_2, f_3, f_4 линейно зависимы. Из полученного тождества можно, в соответствии со сказанным выше, любую из этих форм выразить через остальные. Например,

$$f_4 = f_1 + f_2 + f_3.$$

Пример 3. Покажем, что формы

$$f_1 = x_1 + x_2 + x_3, \qquad f_2 = x_1 + 2x_2 + 3x_3, \qquad f_3 = x_1 + 3x_2 + 6x_3$$

линейно независимы.

Если в тождестве

$$c_1 f_1 + c_2 f_2 + c_3 f_3 \equiv 0$$

подставить значения форм f_1, f_2, f_3 и сгруппировать члены с одинаковыми неизвестными, то получится

$$(c_1 + c_2 + c_3) x_1 + (c_1 + 2c_2 + 3c_3) x_2 + (c_1 + 3c_2 + 6c_3) x_3 \equiv 0.$$

Полагая в этом тождестве $x_1 = 1$, $x_2 = 0$, $x_3 = 0$, затем $x_1 = 0$, $x_2 = 1$, $x_3 = 0$ и, наконец, $x_1 = 0$, $x_2 = 0$, $x_3 = 1$, получим три однородных уравнения относительно c_1, c_2, c_3:

$$\begin{aligned} c_1 + c_2 + c_3 &= 0, \\ c_1 + 2c_2 + 3c_3 &= 0, \\ c_1 + 3c_2 + 6c_3 &= 0. \end{aligned}$$

Легко видеть, что определитель этой системы отличен от нуля; следовательно,

$$c_1 = 0, \quad c_2 = 0, \quad c_3 = 0.$$

Итак, действительно, формы f_1, f_2, f_3 линейно независимы, так как нельзя подобрать c_1, c_2, c_3, не все равные нулю.

Вообще понятие линейной зависимости можно применить только к линейным формам, а и к другим величинам, например функциям, системам постоянных, векторам и т. д. Формулиров определения останется без изменения, нужно только вместо сл «линейные формы» поставить название соответствующих велич

§ 14. Матрица, ранг матрицы. Связь между рангом матри и числом линейно независимых форм

Пусть дано m линейных форм с n неизвестными:

$$\begin{aligned} f_1 &= a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n, \\ f_2 &= a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ f_m &= a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n. \end{aligned}$$

Назовём прямоугольную табличку из m строк и n столбцов

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

матрицей, а коэффициенты a_{ij}, из которых составлена матрица, элементами [1]). В написанной матрице коэффициенты расположе в том же порядке, что и в линейных формах. Обычно матрицу о значают двойными чёрточками; мы этого обозначения и будем время придерживаться.

Отметим ещё раз, что матрица есть только таблица и сменив её с определителем нельзя.

Очевидно, что матрица вполне определяет ту систему линей форм, коэффициенты которых служат её элементами. Но этого ма матрица позволяет также судить о характере линейной зависимо между формами. Приведём примеры.

[1]) В тех случаях, когда это не может вызвать недоразумений, употребл краткий символ $\| a_{ik} \|$ для обозначения этой матрицы.

Пример 1. Рассмотрим матрицу

$$A=\begin{Vmatrix} 1 & -2 & 1 \\ 2 & -4 & 2 \end{Vmatrix}.$$

Из неё можно составить следующие определители второго порядка:

$$\Delta_1=\begin{vmatrix} 1 & -2 \\ 2 & -4 \end{vmatrix}, \qquad \Delta_2=\begin{vmatrix} 1 & 1 \\ 2 & 2 \end{vmatrix}, \qquad \Delta_3=\begin{vmatrix} -2 & 1 \\ -4 & 2 \end{vmatrix},$$

они все равны нулю. Условимся называть каждый элемент матрицы *определителем первого порядка*. Все определители первого порядка, содержащиеся в матрице A, отличны от нуля. Мы будем говорить в таких случаях, что ранг матрицы равен 1.

Легко видеть, что в матрице A строки пропорциональны[1]): вторая строка равна удвоенной первой. Отсюда следует, что между формами

$$f_1=x_1-2x_2+x_3,$$
$$f_2=2x_1-4x_2+2x_3$$

существует линейная зависимость: $2f_1-f_2\equiv 0$.

Пример 2. Теперь возьмём несколько более сложную матрицу:

$$B=\begin{Vmatrix} 1 & 2 & 3 & 4 \\ 1 & -2 & 4 & 5 \\ 1 & 10 & 1 & 2 \end{Vmatrix}.$$

Легко видеть, что все определители третьего порядка, содержащиеся в этой матрице, равны нулю, но зато существуют определители второго порядка, не равные нулю, например:

$$\begin{vmatrix} 1 & 2 \\ 1 & -2 \end{vmatrix}\neq 0.$$

По аналогии с предыдущим примером можем сказать, что ранг матрицы равен уже не 1, а 2.

При некоторой наблюдательности можно заметить, что между всеми строками матрицы B существует линейная зависимость: третья строка равна разности между утроенной первой и удвоенной второй строками. Что касается двух каких-либо строк, например, второй и третьей, то они между собой линейно независимы, так как в противном случае одна строка была бы пропорциональна другой, и все определители второго порядка были бы равны нулю. Отсюда следует, что среди форм

$$f_1=x_1+2x_2+3x_3+4x_4,$$
$$f_2=x_1-2x_2+4x_3+5x_4,$$
$$f_3=x_1+10x_2+x_3+2x_4$$

любая пара форм между собой линейно независима; а три формы f_1, f_2, f_3 линейно зависимы: $3f_1-2f_2-f_3\equiv 0$.

[1]) Точнее: соответственные элементы строк пропорциональны. Однако более точное выражение общеупотребительно, так как оно удобнее и не вызывает недоразумений.

Из этих примеров видно, какая тесная связь имеется между рангом матрицы и линейной зависимостью форм. В первом примере ранг матрицы A равен *единице*, *одна* форма линейно независима, а *две*—линейно зависимы. Во втором примере ранг *матрицы* B равен *двум*, *две* формы линейно независимы, а три линейно зависимы между собой; наибольшее число линейно независимых форм (от которых зависят остальные формы в том и другом примере) равно рангу матрицы. Подмеченную закономерность надо ещё доказать, но сначала дадим строгое определение ранга.

Определение 1. *Выделим в матрице M произвольно t строк и t столбцов. Определитель t-го порядка, составленный из элементов, лежащих на пересечении выделенных строк и столбцов, называется определителем, порождаемым матрицей M или просто определителем матрицы. Как строки, так и столбцы этого определителя должны быть расположены в том же порядке, что и в матрице M.*

Определение 2. *Говорят, что матрица M имеет ранг r, если среди определителей r-го порядка, порождаемых матрицей, есть хотя бы один, отличный от нуля, а все определители более высокого порядка равны нулю.*

Пример. Найдём ранг матрицы

$$M=\begin{Vmatrix} 3 & 2 & 1 & 3 & -1 \\ 2 & 3 & 5 & 1 & 0 \\ 8 & 5 & 6 & 4 & -1 \\ 13 & 10 & 12 & 8 & -2 \end{Vmatrix}.$$

Сначала выпишем все определители 4-го (наивысшего!) порядка, порождаемые матрицей M:

$$\Delta_1=\begin{vmatrix} 3 & 2 & 1 & 3 \\ 2 & 3 & 5 & 1 \\ 8 & 5 & 6 & 4 \\ 13 & 10 & 12 & 8 \end{vmatrix}=0, \qquad \Delta_2=\begin{vmatrix} 3 & 2 & 1 & -1 \\ 2 & 3 & 5 & 0 \\ 8 & 5 & 6 & -1 \\ 13 & 10 & 12 & -2 \end{vmatrix}=0,$$

$$\Delta_3=\begin{vmatrix} 3 & 2 & 3 & -1 \\ 2 & 3 & 1 & 0 \\ 8 & 5 & 4 & -1 \\ 13 & 10 & 8 & -2 \end{vmatrix}=0, \qquad \Delta_4=\begin{vmatrix} 3 & 1 & 3 & -1 \\ 2 & 5 & 1 & 0 \\ 8 & 6 & 4 & -1 \\ 13 & 12 & 8 & -2 \end{vmatrix}=0,$$

$$\Delta_5=\begin{vmatrix} 2 & 1 & 3 & -1 \\ 3 & 5 & 1 & 0 \\ 5 & 6 & 4 & -1 \\ 10 & 12 & 8 & -2 \end{vmatrix}=0.$$

Все они равны нулю и потому ранг матрицы не равен четырём. Н легко видеть, что ранг матрицы равен 3, так как определитель треть его порядка

$$\begin{vmatrix} 3 & 2 & 1 \\ 2 & 3 & 5 \\ 8 & 5 & 6 \end{vmatrix}\neq 0.$$

Теперь можно приступить к доказательству подмеченной закономерности.

Теорема. *Если ранг матрицы системы линейных форм равен r, то существует r линейно независимых форм, от которых линейно зависят все остальные формы.*

Доказательство. Пусть мы имеем систему m линейных форм

$$\left.\begin{aligned} f_1 &= a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n, \\ f_2 &= a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ f_m &= a_{m1}x_1 + x_{m2}x_2 + \ldots + a_{mn}x_n; \end{aligned}\right\} \quad (A$$

матрица

$$M = \left\| \begin{array}{ccc|ccc} a_{11} & \ldots & a_{1r} & a_{1r+1} & \ldots & a_{1n} \\ \cdot & & \cdot & \cdot & & \cdot \\ \cdot & D & \cdot & \cdot & & \cdot \\ \cdot & & \cdot & \cdot & & \cdot \\ a_{r1} & \ldots & a_{rr} & a_{rr+1} & \ldots & a_{rn} \\ \hline \cdot & \ldots & \cdot & \cdot & \ldots & \cdot \\ a_{m1} & \ldots & a_{mr} & a_{mr+1} & \ldots & a_{mn} \end{array} \right\|$$

из коэффициентов этой системы пусть имеет ранг r. Тогда среди определителей, порождаемых матрицей M, есть хотя бы один определитель r-го порядка, отличный от нуля. Мы можем предположить, что один из таких определителей находится в левом верхнем углу матрицы M (он обозначен через D и ограничен пунктиром). Это предположение не уменьшает общности наших рассуждений, так как если бы этого не было, то мы соответственным образом изменили бы нумерацию форм и неизвестных.

Легко видеть, что первые r форм $f_1, f_2, \ldots, f_r$ линейно независимы. И в самом деле, если бы эти формы были зависимы, то одна из строк определителя D была бы линейной комбинацией других строк и поэтому было бы $D = 0$, что невозможно, так как по условию $D \neq 0$.

Остаётся показать, что всякая форма $f_k\,(k > r)$ линейно зависит от $f_1, f_2, \ldots, f_r$. Очевидно, что для этого достаточно показать, что k-я строка матрицы M есть линейная комбинация её r первых строк. Возьмём определитель $(r+1)$-го порядка

$$\Delta_i = \left| \begin{array}{ccc|c} a_{11} & a_{12} \ldots & a_{1r} & a_{1i} \\ a_{21} & a_{22} \ldots & a_{2r} & a_{2i} \\ \ldots\ldots & D \ldots & & \ldots \\ a_{r1} & a_{r2} \ldots & a_{rr} & a_{ri} \\ \hline a_{k1} & a_{k2} \ldots & a_{kr} & a_{ki} \end{array} \right| \quad (i = 1, 2, \ldots, n).$$

Этот определитель равен нулю. Действительно, если $i \leqslant r$, то будет иметь два одинаковых столбца и потому $\Delta_i = 0$; если же $i >$ то Δ_i будет определителем $(r+1)$-го порядка, порождённым матрицей ранга r, и потому и здесь $\Delta_i = 0$.

Разложим определитель Δ_i по элементам последнего столбца, обозначив их алгебраические дополнения через $A_1, A_2, \ldots, A_{r+1}$:

$$a_{1i}A_1 + a_{2i}A_2 + \ldots + a_{ki}A_{r+1} = \Delta_i = 0.$$

Так как $A_{r+1} = D \neq 0$, то полученную зависимость можно разрешить относительно a_{ki}:

$$a_{ki} = c_1 a_{1i} + c_2 a_{2i} + \ldots + c_r a_{ri}, \qquad (1)$$

где

$$c_1 = -\frac{A_1}{D}, \quad c_2 = -\frac{A_2}{D}, \quad \ldots, \quad c_r = -\frac{A_r}{D}.$$

Наша цель достигнута: соотношение (1) говорит как раз о том, что k-я строка матрицы M есть линейная комбинация её первых r строк.

Насколько доказанная теорема помогает обнаружить линейную зависимость, видно из следующего примера.

Пример. Найти линейную зависимость между формами:

$$f_1 = x_1 + 4x_2 + x_3, \qquad f_2 = 2x_1 + x_2 - x_3 - 3x_4,$$
$$f_3 = x_1 - 3x_2 - x_4, \qquad f_4 = 2x_2 - 6x_3 + 3x_4.$$

Нетрудно убедиться, что ранг матрицы

$$M = \left\| \begin{array}{cccc} 1 & 4 & 1 & 0 \\ 2 & 1 & -1 & -3 \\ 1 & 0 & -3 & -1 \\ \hdashline 0 & 2 & -6 & 3 \end{array} \right\|$$

из коэффициентов форм равен 3, причём определитель третьего порядка, не равный нулю, находится в левом верхнем углу. Отсюда следует согласно только что доказанной теореме, что формы f_1, f_2, f_3 линейно независимы, а f_4 линейно зависит от f_1, f_2, f_3. Найдём эту линейную зависимость. Составляем, следуя теореме, определитель

$$\Delta = \begin{vmatrix} 1 & 4 & 1 & 0 \\ 2 & 1 & -1 & -3 \\ 1 & 0 & -3 & -1 \\ 0 & 2 & -6 & 3 \end{vmatrix} = 0$$

и находим c_1, c_2, c_3.

$$D = \begin{vmatrix} 1 & 4 & 1 \\ 2 & 1 & -1 \\ 1 & 0 & -3 \end{vmatrix} = 16;$$

$$A_1 = -\begin{vmatrix} 2 & 1 & -1 \\ 1 & 0 & -3 \\ 0 & 2 & -6 \end{vmatrix} = -16; \quad A_2 = \begin{vmatrix} 1 & 4 & 1 \\ 1 & 0 & -3 \\ 0 & 2 & -6 \end{vmatrix} = 32;$$

$$A_3 = -\begin{vmatrix} 1 & 4 & 1 \\ 1 & 1 & -1 \\ 0 & 2 & -6 \end{vmatrix} = -48,$$

откуда

$$c_1 = -\frac{A_1}{D} = 1, \qquad c_2 = -\frac{A_2}{D} = -2; \quad c_3 = -\frac{A_3}{D} = 3$$

и

$$f_4 = f_1 - 2f_2 + 3f_3.$$

Легко проверить, что найденная зависимость действительно имеет место.

Задачи. 1. Если матрица состоит из m строк и n столбцов, то она порождает всего $C_m^k C_n^k$ определителей k-го порядка. Доказать это.

2. Найти линейную зависимость между формами:

$$f_1 = x_1 + x_3 - x_4, \quad f_2 = 2x_1 - x_2 + x_3 - 5x_4,$$
$$f_3 = 3x_1 + 3x_2 + 3x_3 - 8x_4, \quad f_4 = 14x_1 + 7x_2 + 12x_3 - 35x_4.$$

3. Зависимы ли формы:

$$f_1 = 2x_1 - x_2 + 5x_3, \quad f_2 = x_1 - 2x_2 - 3x_3, \quad f_3 = 6x_1 + 7x_2 - 8x_3?$$

4. Пусть $f_1, f_2, \ldots, f_m$ некоторая система линейных форм. Показать, что максимальное число линейно независимых форм равно рангу матрицы данной системы форм.

§ 15. Вычисление ранга матрицы

Во многих случаях вычисление ранга матрицы сопряжено с выпи сыванием довольно большого количества детерминантов, отчего вс вычисление становится непомерно громоздким. Однако существую особые приёмы, сильно облегчающие определение ранга; эти приём мы сейчас укажем.

Один из методов основан на следующей теореме.

Теорема 1. *Ранг матрицы не меняется, если* a) *все строки заме нить столбцами*; b) *поменять местами две строки* (*столбца*) c) *умножить каждый элемент строки* (*столбца*) *на один и тот ж множитель, отличный от нуля*; d) *сложить одну строку* (*столбец с другой строкой* (*столбцом*), *увеличенной в т раз.*

Замечание. Преобразования a), b), c) и d) называются *элементарными.*

Доказательство. Первые три преобразования, очевидно не меняют ранга матрицы; если определитель до преобразовани был равен нулю, то он и после преобразования останется равны нулю; то же самое можно сказать и относительно определителя отличного от нуля.

Таким образом остаётся разобрать преобразование d). Покаже прежде всего, что операция d) не может повысить ранг нашей ма рицы M.

Подвергнем матрицу M преобразованию d): прибавим, наприме к p-й строке q-ю, умноженную на m. Получится новая матрица, м её обозначим через N. Пусть r — ранг матрицы M, а r_1 — ранг N. В определители k-го порядка ($k > r$) матрицы M равны нулю, причё если определитель не содержит p-й строки или содержит p-ю и q-

строки, то он и после преобразования будет равен нулю. Несколько сложнее тот случай, когда определитель Δ k-го порядка ($k > r$) содержит p-ую строку, но не содержит q-й строки. После преобразования определитель Δ превратится в некоторый другой определитель Δ', а каждый элемент p-й строки станет равным сумме двух слагаемых; отсюда следует, что определитель Δ' распадается на сумму двух определителей: $\Delta' = \Delta_1 + m\Delta_2$. Но Δ_1 и Δ_2 суть определители k-го порядка ($k > r$) матрицы M, поэтому $\Delta_1 = 0$, $\Delta_2 = 0$ и Δ' также равен нулю. Итак, мы видим, что в матрице N все определители выше r-го порядка равны нулю, а это как раз и означает, что ранг матрицы N не выше ранга матрицы M; т. е. $r_1 \leqslant r$.

В свою очередь можно показать, что $r \leqslant r_1$. В самом деле, подвергнем N преобразованию d): к p-й строке прибавим q-ю, увеличенную в $-m$ раз. Мы тогда, очевидно, получим матрицу M. Но от преобразования d) ранг не может повыситься; поэтому $r \leqslant r_1$. Таким образом мы получим, с одной стороны, что $r_1 = r$, а с другой $r \leqslant r_1$, откуда и следует; что $r = r_1$.

Теперь рассмотрим следующие примеры.

Пример 1. Определить ранг матрицы

$$M = \begin{Vmatrix} 14 & 12 & 6 & 8 & 2 \\ 6 & 104 & 21 & 9 & 17 \\ 7 & 6 & 3 & 4 & 1 \\ 35 & 30 & 15 & 20 & 5 \end{Vmatrix}.$$

Прежде всего целесообразно сократить общие множители в первой четвёртой строках; от этого наша матрица станет проще. Имеем после такого преобразования:

$$\begin{Vmatrix} 7 & 6 & 3 & 4 & 1 \\ 6 & 104 & 21 & 9 & 17 \\ 7 & 6 & 3 & 4 & 1 \\ 7 & 6 & 3 & 4 & 1 \end{Vmatrix}.$$

Далее вычтем первую строку из третьей и четвёртой, получим:

$$\begin{Vmatrix} 7 & 6 & 3 & 4 & 1 \\ 6 & 104 & 21 & 9 & 17 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{Vmatrix}.$$

о последняя матрица, как это видно сразу, имеет ранг 2. Поэтому анг матрицы M также равен 2.

Пример 2. Определить ранг матрицы

$$\begin{Vmatrix} 3 & 2 & -1 & -3 & -2 \\ 2 & -1 & 3 & 1 & -3 \\ 4 & 5 & -5 & -6 & 1 \end{Vmatrix}.$$

Делаем нули в последнем столбце, для чего прибавляем к первой строке удвоенную третью, а ко второй — утроенную третью. Получим:

$$\begin{Vmatrix} 11 & 12 & -11 & -15 & 0 \\ 14 & 14 & -12 & -17 & 0 \\ 4 & 5 & -5 & -6 & 1 \end{Vmatrix}.$$

Затем делаем нули в последней строке, пользуясь последним столбцом:

$$\begin{Vmatrix} 11 & 12 & -11 & -15 & 0 \\ 14 & 14 & -12 & -17 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{Vmatrix}.$$

Легко видеть, что ранг последней матрицы равен трём:

$$\begin{vmatrix} 11 & 12 & 0 \\ 14 & 14 & 0 \\ 0 & 0 & 1 \end{vmatrix} = -14 \neq 0.$$

Следовательно, и ранг M равен трём.

Другой приём вычисления ранга базируется на нижеследующей теореме.

Теорема II. *Если некоторый определитель r-го порядка матрицы M отличен от нуля, а все определители $(r+1)$-го порядка, заключающие его в качестве минора, равны нулю, то ранг матрицы M равен r.*

Доказательство. Без ограничения общности можно предположить, что этот отличный от нуля определитель r-го порядка находится в левом верхнем углу матрицы:

$$M = \left\| \begin{array}{ccc|ccc} a_{11} & \dots & a_{1r} & a_{1r+1} & \dots & a_{1n} \\ \cdot & & \cdot & \cdot & & \cdot \\ \cdot & D & \cdot & \cdot & & \cdot \\ \cdot & & \cdot & \cdot & & \cdot \\ a_{r1} & \dots & a_{rr} & a_{rr+1} & \dots & a_{rn} \\ \hline \cdot & & \cdot & \cdot & & \cdot \\ a_{i1} & \dots & a_{ir} & a_{ir+1} & \dots & a_{in} \\ \cdot & & \cdot & \cdot & & \cdot \\ a_{m1} & \dots & a_{mr} & a_{mr+1} & \dots & a_{mn} \end{array} \right\|.$$

Рассмотрим определитель

$$\Delta_i = \left| \begin{array}{ccc|c} a_{11} & a_{12} \dots & a_{1r} & a_{1i} \\ a_{21} & a_{22} \dots & a_{2r} & a_{2i} \\ \cdots & D & \cdots & \cdots \\ a_{r1} & a_{r2} \dots & a_{rr} & a_{ri} \\ \hline a_{k1} & a_{k2} \dots & a_{kr} & a_{ki} \end{array} \right| \quad (k > r).$$

Если $i \leqslant r$, то Δ_i будет иметь два одинаковых столбца и потому $\Delta_i = 0$, если же $i > r$, то Δ_i будет определителем $(r+1)$-го порядка, содержащим D в качестве минора; поэтому, вследствие условия теоремы, и здесь $\Delta_i = 0$. Отсюда следует, что k-я строка матрицы M должна *линейно зависеть* от r первых строк (см. стр. 68). Воспользуемся теперь теоремой I, вычтем из $(r+1)$-й, $(r+2)$-й, ..., m-й строки матрицы M соответствующие линейные комбинации r первых строк; тогда наша матрица превратится в

$$M' = \begin{Vmatrix} a_{11} \dots a_{1r} \dots a_{1n} \\ \cdot \quad\quad \cdot \quad \dots \\ \cdot \quad D \quad \cdot \quad \dots \\ \cdot \quad\quad \cdot \quad \dots \\ a_{r1} \dots a_{rr} \dots a_{rn} \\ 0 \quad \dots 0 \quad \dots 0 \\ \cdot \quad \dots \cdot \quad \dots \cdot \\ 0 \quad \dots 0 \quad \dots 0 \end{Vmatrix}.$$

Ранг M', очевидно, равен r, откуда и ранг M также равен r. Теорема доказана.

Пример. Найдём с помощью теоремы II ранг матрицы

$$M = \begin{Vmatrix} 2 & -3 & 8 & 2 \\ 2 & 12 & -2 & 12 \\ 1 & 3 & 1 & 4 \end{Vmatrix}.$$

Легко видеть, что не все определители второго порядка равны нулю, например, $\begin{vmatrix} -3 & 8 \\ 12 & -2 \end{vmatrix} \neq 0$. Этот определитель входит минором в следующие определители третьего порядка:

$$\Delta_1 = \begin{vmatrix} 2 & -3 & 8 \\ 2 & 12 & -2 \\ 1 & 3 & 1 \end{vmatrix} = 0, \quad \Delta_2 = \begin{vmatrix} -3 & 8 & 2 \\ 12 & -2 & 12 \\ 3 & 1 & 4 \end{vmatrix} = 0,$$

откуда следует, что ранг матрицы M равен двум.

Задачи. 1. Определить ранг матриц:

$$\begin{Vmatrix} 1 & 0 & -1 & 5 & 12 \\ 6 & 7 & 8 & 0 & -9 \\ 26 & 21 & 26 & -10 & -51 \\ 15 & 14 & 13 & -15 & -54 \end{Vmatrix}, \quad \begin{Vmatrix} 8 & 5 & 3 & 7 & 1 & 2 \\ 4 & 6 & 7 & 9 & 11 & 12 \\ 3 & 0 & -1 & 2 & 7 & 1 \\ 15 & 11 & 9 & 18 & 19 & 15 \\ 17 & 10 & 2 & -5 & 6 & 3 \end{Vmatrix}.$$

2. Показать, что с помощью элементарных преобразований всякую матрицу ранга r можно преобразовать так, чтобы первые r элементов главной диагонали (элементы a_{ii}, $i \leqslant r$) превратились в единицу, а все остальные элементы матрицы — в нули.

§ 16. Линейные уравнения и теорема Кронекера-Капелли

Теперь можно без особого труда перейти к изучению систем линейных уравнений. Пусть

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

— система m уравнений с n неизвестными (m может быть и не равно n).

Система уравнений (1) называется *совместной*, если можно найти такие значения:

$$x_1 = \beta_1, \quad x_2 = \beta_2, \ldots, \quad x_n = \beta_n$$

для неизвестных, которые удовлетворяют всем уравнениям системы; совокупность этих значений $\beta_1, \beta_2, \ldots, \beta_n$ называется *решением* системы.

Обозначим через A матрицу из коэффициентов системы (1), а через B — матрицу, полученную из A присоединением столбца свободных членов:

$$A = \begin{Vmatrix} a_{11} & a_{12} \ldots a_{1n}\\ a_{21} & a_{22} \ldots a_{2n}\\ \ldots\ldots\ldots\\ a_{m1} & a_{m2} \ldots a_{mn} \end{Vmatrix}, \quad B = \begin{Vmatrix} a_{11} & a_{12} \ldots a_{1n} & b_1\\ a_{21} & a_{22} \ldots a_{2n} & b_2\\ \ldots\ldots\ldots\ldots\\ a_{m1} & a_{m2} \ldots a_{mn} & b_m \end{Vmatrix}.$$

Мы сейчас докажем теорему, играющую основную роль во всей теории линейных уравнений.

Теорема Кронекера-Капелли. *Система уравнений (1) совместна тогда и только тогда, когда ранг матрицы A равен рангу расширенной матрицы B.*

Доказательство. Пусть система (1) совместна, покажем, что тогда матрицы A и B должны быть одинакового ранга.

Раз уравнения (1) совместны, то они имеют решение, т. е. можно для неизвестных подыскать такие числовые значения $x_1 = \beta_1$, $x_2 = \beta_2$, ..., $x_n = \beta_n$, что

$$\left.\begin{aligned} a_{11}\beta_1 + a_{12}\beta_2 + \ldots + a_{1n}\beta_n &= b_1,\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ a_{m1}\beta_1 + a_{m2}\beta_2 + \ldots + a_{mn}\beta_n &= b_m. \end{aligned}\right\} \qquad (2)$$

Найдём, чему равен ранг матрицы B, для чего из её последнего столбца вычтем первый, умноженный на β_1, второй, умноженный на β_2, ..., n-й, умноженный на β_n. Тогда в силу равенств (2) матрица B, не меняя своего ранга (см. § 15, теорему I), превратится в матрицу

$$B^* = \begin{Vmatrix} a_{11} & \ldots & a_{1n} & 0\\ \cdot & & \cdot & \cdot\\ \cdot & & \cdot & \cdot\\ \cdot & & \cdot & \cdot\\ a_{m1} & \ldots & a_{mn} & 0 \end{Vmatrix}.$$

Но последний столбец матрицы B^* состоит из нулей, откуда, очевидно, ранг B^*, или, что то же, ранг B равен рангу матрицы A.

Обратно, пусть матрицы A и B имеют одинаковый ранг r. Покажем, что в таком случае система (1) совместна.

Без ограничения общности доказательства можно допустить, что отличный от нуля определитель D r-го порядка находится в левом верхнем углу как матрицы A, так и матрицы B; в противном случае мы изменили бы соответствующим образом нумерацию уравнений и неизвестных. Тогда первые r строк матриц A и B должны быть линейно независимы, а остальные строки должны от них зависеть (см. теорему § 14). Иными словами, первые r уравнений системы будут линейно независимы, а прочие уравнения будут от них линейно зависеть. Но зависимые уравнения мы смело можем отбросить, так как всякое решение первых r уравнений, очевидно, удовлетворяет и зависимому уравнению.

Теперь могут представиться только две возможности: а) $r = n$ или b) $r < n$. Разберём эти два случая отдельно.

Если $r = n$, то у нас будет n независимых уравнений с n неизвестными, причём определитель D из коэффициентов отличен от нуля. Мы хорошо знаем (см. § 8), что такая система имеет *единственное* решение, получаемое по формулам Крамера.

Если $r < n$, то число независимых уравнений будет уже меньше числа неизвестных. Перенесём лишние неизвестные $x_{r+1}, x_{r+2}, \ldots, x_n$, которые принято называть *свободными*, в правые части; наша система независимых уравнений примет при этом такой вид:

$$\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \ldots + a_{1r}x_r &= b_1 - a_{1r+1}x_{r+1} - \ldots - a_{1n}x_n,\\
a_{21}x_1 + a_{22}x_2 + \ldots + a_{2r}x_r &= b_2 - a_{2r+1}x_{r+1} - \ldots - a_{2n}x_n,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
a_{r1}x_1 + a_{r2}x_2 + \ldots + a_{rr}x_r &= b_r - a_{rr+1}x_{r+1} - \ldots - a_{rn}x_n.
\end{aligned}$$

Мы видим, что её можно решить относительно $x_1, x_2, \ldots, x_n$, так как определитель D r-го порядка из коэффициентов отличен от нуля. Придавая свободным неизвестным произвольные числовые значения, получим по формулам Крамера соответствующие числовые значения для $x_1, x_2, \ldots, x_r$. Таким образом при $r < n$ получается даже не одно, а *бесчисленное множество решений*.

Итак, разбирая случаи $r = n$ и $r < n$, мы не только убедились, что система (1) совместна, но и указали практический способ её решения.

Пример 1. Рассмотрим систему уравнений:

$$\begin{aligned}
x_1 - 2x_2 + 3x_3 - x_4 + 2x_5 &= 2,\\
3x_1 - x_2 + 5x_3 - 3x_4 - x_5 &= 6,\\
2x_1 + x_2 + 2x_3 - 2x_4 - 3x_5 &= 8.
\end{aligned}$$

Легко видеть, что ранг матрицы из коэффициентов:

$$A = \begin{Vmatrix} 1 & -2 & 3 & -1 & 2 \\ 3 & -1 & 5 & -3 & -1 \\ 2 & 1 & 2 & -2 & -3 \end{Vmatrix}$$

равен двум, а ранг расширенной матрицы

$$B=\begin{Vmatrix} 1 & -1 & -1 & 2 & 2 \\ 3 & -1 & 5 & -3 & -1 & 6 \\ 2 & 1 & 2 & -2 & -3 & 8 \end{Vmatrix}$$

равен трём, откуда следует, что рассматриваемая система несовместна, т. е. не имеет решений.

Пример 2. Разберём теперь другую систему:

$$\begin{aligned} x_1 - x_2 + 2x_3 &= 1, \\ x_1 - 2x_2 - x_3 &= 2, \\ 3x_1 - x_2 + 5x_3 &= 3, \\ -2x_1 + 2x_2 + 3x_3 &= -4. \end{aligned}$$

Ранг r матрицы из коэффициентов равен трём и тому же числу равен ранг расширенной матрицы. Таким образом система уравнений совместна и допускает единственное решение; так как ранг r равен числу неизвестных. Отбрасывая четвёртое уравнение, как линейно зависимое от первых трёх, будем иметь три уравнения с тремя неизвестными:

$$\begin{aligned} x_1 - x_2 + 2x_3 &= 1, \\ x_1 - 2x_2 - x_3 &= 2, \\ 3x_1 - x_2 + 5x_3 &= 3; \end{aligned}$$

решая их по формулам Крамера, получим:

$$x_1=\frac{10}{7}, \quad x_2=-\frac{1}{7}, \quad x_3=-\frac{2}{7}.$$

Для контроля подставляем эти значения неизвестных во все четыре уравнения; легко видеть, что система решена правильно.

Пример 3. Рассмотрим систему $n+1$ уравнений с n неизвестными:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n+11}x_1 + a_{n+12}x_2 + \ldots + a_{n+1n}x_n &= b_{n+1}. \end{aligned}$$

Легко заметить, что

$$D=\begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n+11} & a_{n+12} & \ldots & a_{n+1n} & b_{n+1} \end{vmatrix}$$

есть единственный определитель $(n+1)$-го порядка матрицы B.

Матрица A состоит из $n+1$ строк и n столбцов; отсюда ясно, что её ранг не может превосходить n. Таким образом, если ранг A равен рангу B, то определитель D должен равняться нулю. Итак, мы доказали следующее предложение: если система $n+1$ уравнений сов-

местна, то определитель D, составленный из коэффициентов и свободных членов, равен нулю.

Обратное неверно. D может равняться нулю и тогда, когда система несовместна.

Пример 4. Наконец, рассмотрим систему

$$\begin{aligned} x_1 - x_2 + x_3 - x_4 &= 1, \\ x_1 - x_2 - x_3 + x_4 &= 0, \\ x_1 - x_2 - 2x_3 + 2x_4 &= -\frac{1}{2}. \end{aligned}$$

Она совместна, так как матрицы A и B имеют одинаковый ранг $r = 2$. но здесь число независимых уравнений меньше числа неизвестных: $r < n$; поэтому данная система имеет бесчисленное множество решений. Определитель второго порядка

$$D = \begin{vmatrix} -1 & 1 \\ -1 & -1 \end{vmatrix} = 2$$

отличен от нуля, откуда следует, что первые два уравнения линейно независимы, а третье от них зависит. Отбрасываем третье уравнение и переносим свободные неизвестные x_1 и x_4 в правую часть:

$$\begin{aligned} -x_2 + x_3 &= 1 - x_1 + x_4, \\ -x_2 - x_3 &= -x_1 - x_4, \end{aligned}$$

откуда

$$x_2 = \frac{\begin{vmatrix} 1 - x_1 + x_4 & 1 \\ -x_1 - x_4 & -1 \end{vmatrix}}{D} = x_1 - \frac{1}{2},$$

$$x_3 = \frac{\begin{vmatrix} -1 & 1 - x_1 + x_4 \\ -1 & -x_1 - x_4 \end{vmatrix}}{D} = x_4 + \frac{1}{2}.$$

Для контроля подставляем это решение во все три уравнения; легко убедиться, что система решена правильно. Свободным неизвестным x_1 и x_4 можно давать любые значения. Например, полагая $x_1 = 1$, $x_4 = 2$, получим

$$x_1 = 1, \quad x_2 = \frac{1}{2}, \quad x_3 = \frac{5}{2}, \quad x_4 = 2.$$

Задача. Исследовать на совместность и решить следующие системы уравнений:

a) $\begin{aligned} 2x - y + 3z - u &= 1, \\ 3x - 2y - 2z + 3u &= 3, \\ x - y - 5z + 4u &= 2, \\ 7x - 5y - 9z + 10u &= 8. \end{aligned}$

b) $\begin{aligned} 2x_1 - x_2 + x_4 &= -1, \\ x_1 + 3x_2 - 7x_3 + 4x_4 &= 3, \\ 3x_1 - 2x_2 + x_3 + x_4 &= -2. \end{aligned}$

c) $\begin{aligned} x - y + z &= 1, \\ x + y - z &= 1, \\ x - y + z &= -1, \\ x + y + z &= 2. \end{aligned}$

В заключение этого параграфа рассмотрим несколько ближе случай однородных уравнений:

$$\left.\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= 0, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots & \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= 0. \end{aligned}\right\} \qquad (3)$$

Уже с первого взгляда видно, что $x_1 = 0$, $x_2 = 0$, ..., $x_n = 0$ есть одно из решений системы (3); таким образом однородная система уравнений всегда совместна. К тому же выводу можно притти, сравнивая ранг матрицы A с рангом расширенной матрицы B. А именно, последний столбец матрицы B состоит из нулей, поэтому ранг матрицы B равен рангу матрицы A, и система (3) должна быть совместной.

Но помимо очевидного решения $x_1 = 0$, $x_2 = 0$, ..., $x_n = 0$ могут быть другие, ненулевые решения. Можно высказать следующее предложение:

Если ранг матрицы A из коэффициентов равен числу неизвестных ($r = n$), то $x_1 = 0$, $x_2 = 0$, ..., $x_n = 0$ будет единственным решением. Если же ранг матрицы A меньше числа неизвестных ($r < n$), то помимо нулевого должно существовать бесчисленное множество ненулевых решений.

В самом деле, если $r = n$, то система (3) имеет единственное, а именно нулевое решение $x_1 = 0$, ..., $x_n = 0$. Если же $r < n$, то $n - r$ неизвестных будут свободными и система будет иметь помимо нулевого бесчисленное множество других решений (см. доказательство теоремы Кронекера-Капелли).

Задача. Решить следующие системы однородных уравнений:

а) $\begin{aligned} 11x_1 + 8x_2 - 2x_3 + 3x_4 &= 0, \\ 2x_1 + 3x_2 - x_3 + 2x_4 &= 0, \\ 7x_1 - x_2 + x_3 - 3x_4 &= 0, \\ 4x_1 - 11x_2 + 5x_3 - 12x_4 &= 0. \end{aligned}$ б) $\begin{aligned} 2x_1 - 3x_2 + 5x_3 + 3x_4 &= 0, \\ 4x_1 - x_2 + x_3 + x_4 &= 0, \\ 3x_1 - 2x_2 + 3x_3 + 4x_4 &= 0. \end{aligned}$

§ 17. Фундаментальная система решений

Продолжаем изучение системы однородных уравнений. Пусть $x_1 = \alpha_1$, $x_2 = \alpha_2$, ..., $x_n = \alpha_n$ одно из ненулевых решений системы:

$$\left.\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= 0, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots & \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= 0. \end{aligned}\right\} \qquad (1)$$

Легко видеть, что значения $x_1 = c\alpha_1$, $x_2 = c\alpha_2$, ..., $x_n = c\alpha_n$ также удовлетворяют уравнениям (1). В самом деле, подставляя эти числа в уравнения (1) и вынося за скобку общий множитель c, получим в скобках выражение, равное нулю.

Вообще легко убедиться, что [illegible]; $\beta_1, \ldots, \beta_n$; $\ldots$; $\omega_1, \ldots, \omega_n$ — какая-нибудь система, то [illegible]нием будет также и их линейная комбинация

$$c_1\alpha_1 + c_2\beta_1 + \ldots + c_k\omega_1, \ldots, c_1\alpha_n + c_2\beta_n + \ldots + c_k\omega_n. \qquad (2)$$

Возникает следующий естественный вопрос: можно ли с помощью линейных комбинаций (2) получить все решения системы (1)? Чтобы ответить на этот вопрос, вводим прежде всего такое определение.

Определение. *Система решений*

$$\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{in} \quad (i = 1, 2, \ldots, k)$$

уравнений (1) *называется фундаментальной, если эти решения между собой линейно независимы и любое решение* (1) *является их линейной комбинацией.*

Теперь мы можем дать исчерпывающий ответ, сформулировав его в виде теоремы.

Теорема. *Если ранг r матрицы из коэффициентов уравнений* (1) *меньше числа n неизвестных, то уравнения* (1) *обладают фундаментальными системами решений. Число решений, входящих в фундаментальную систему, равно* $n - r$, *т. е числу свободных неизвестных.*

Доказательство. Без ограничения общности можно предположить, что отличный от нуля определитель D r-го порядка находится в левом верхнем углу матрицы коэффициентов. Тогда $x_{r+1}, x_{r+2}, \ldots, x_n$ будут свободными неизвестными. Перенося в первых r уравнениях свободные неизвестные в правые части и решая эти уравнения по формулам Крамера относительно $x_1, x_2, \ldots, x_r$, мы каждое из неизвестных $x_1, x_2, \ldots, x_r$ выразим линейно через свободные неизвестные. Придавая свободным неизвестным $x_{r+1}, \ldots, x_n$ произвольные числовые значения, получим соответствующие значения для $x_1, x_2, \ldots, x_r$. Так действуя, мы будем иметь бесчисленное множество решений. Из этих решений возьмём такие k решений ($k = n - r$):

$$\left.\begin{array}{l} \alpha_{11}, \ldots, \alpha_{1r}, \alpha_{1r+1}, \ldots, \alpha_{1n}, \\ \alpha_{21}, \ldots, \alpha_{2r}, \alpha_{2r+1}, \ldots, \alpha_{2n}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_{k1}, \ldots, \alpha_{kr}, \alpha_{kr+1}, \ldots, \alpha_{kn}, \end{array}\right\} \qquad (3)$$

чтобы определитель k-го порядка

$$\Delta = \begin{vmatrix} \alpha_{1r+1} & \ldots & \alpha_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \alpha_{kr+1} & \ldots & \alpha_{kn} \end{vmatrix}$$

был отличен от нуля [1]). Покажем, что эти решения образуют фундаментальную систему

Рассмотрим матрицу

$$M = \left\| \begin{array}{ccc|ccc} \alpha_{11} & \dots & \alpha_{1r} & \alpha_{1r+1} & \dots & \alpha_{1n} \\ \alpha_{21} & \dots & \alpha_{2r} & \alpha_{2r+1} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots & \Delta & \dots \\ \alpha_{k1} & \dots & \alpha_{kr} & \alpha_{kr+1} & \dots & \alpha_{kn} \\ \hline \beta_1 & \dots & \beta_r & \beta_{r+1} & \dots & \beta_n \end{array} \right\|,$$

образованную из системы решений (3) с добавлением ещё одной строки, состоящей из произвольного решения $\beta_1, \beta_2, \dots, \beta_n$ однородных уравнений (1).

В правом верхнем углу этой матрицы M находится определитель Δ k-го порядка, не равный нулю. Каждый из r первых столбцов матрицы M линейно зависит от её последних $n-r=k$ столбцов, так как каждое неизвестное $x_1, x_2, \dots, x_r$ линейно выражается через свободные неизвестные. Отсюда следует, что ранг матрицы M равен k. В самом деле, благодаря линейной зависимости мы можем элементы первых r столбцов матрицы превратить в нули, вычитая из этих столбцов соответствующие линейные комбинации последних k столбцов. После такого вычитания любой определитель $k+1$-го порядка матрицы M будет иметь по меньшей мере один столбец из нулей и потому будет равен нулю.

Итак, мы установили, что ранг матрицы M равен k, причём в правом верхнем углу матрицы находится определитель k-го порядка, отличный от нуля. Вспомним теперь связь между рангом матрицы и числом её линейно независимых строк (см. § 14). Согласно этой связи первые k строк матрицы M должны быть линейно независимыми, а последняя строка должна линейно зависеть от этих k строк:

$$\beta_i = c_1\alpha_{1i} + c_2\alpha_{2i} + \dots + c_n\alpha_{ni}.$$

Иными словами, решения (3) между собой независимы и любое решение $\beta_1, \beta_2, \dots, \beta_n$ является их линейной комбинацией.

Поясним доказанную теорему на конкретном примере.

Пример. Найдём фундаментальную систему решений однородных уравнений:

$$\begin{aligned} x_1 - x_2 + 5x_3 - x_4 &= 0, \\ x_1 + x_2 - 2x_3 + 3x_4 &= 0, \\ 3x_1 - x_2 + 8x_3 + x_4 &= 0, \\ x_1 + 3x_2 - 9x_3 + 7x_4 &= 0. \end{aligned}$$

[1]) Так как $x_{r+1}, x_{r+2}, \dots, x_n$ — свободные неизвестные, то всегда можно положить, например, $x_{ir+1} = 0, \dots, \alpha_{ir+i} = 1, \dots, \alpha_{in} = 0$, и тогда

$$\Delta = \begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{vmatrix} = 1 \neq 0.$$

Ранг матрицы из коэффициентов равен здесь двум, причём

$$D=\begin{vmatrix}1 & -1\\ 1 & 1\end{vmatrix}=2\neq 0.$$

Таким образом x_3 и x_4 являются свободными неизвестными; переносим их в правую часть и первые два уравнения:

$$x_1-x_2=-5x_3+x_4,$$
$$x_1+x_2=2x_3-3x_4$$

решаем сперва при $x_3=1$, $x_4=0$, а затем при $x_3=0$, $x_4=1$. Получим такие два решения:

$$-\frac{3}{2},\ \frac{7}{2},\ 1,\ 0,$$
$$-1,\ -2,\ 0,\ 1,$$

которые образуют фундаментальную систему, так как $\begin{vmatrix}1 & 0\\ 0 & 1\end{vmatrix}=$

Следовательно, любое решение рассматриваемой системы однородных уравнений имеет вид:

$$x_1=-\frac{3}{2}c_1-c_2,\quad x_2=\frac{7}{2}c_1-2c_2,\quad x_3=c_1,\quad x_4=c_2,$$

где c_1 и c_2 могут принимать произвольные значения.

Задача. Найти фундаментальную систему решений следующих уравнений:

а) $\begin{aligned}x-y+2z&=0,\\ 3x-5y-z&=0,\\ 3x-7y-8z&=0.\end{aligned}$ b) $\begin{aligned}x-7y+5z-3u&=0,\\ 2x-3y+7z-u&=0,\\ x-y+z-2u&=0,\\ 5y+z+4u&=0.\end{aligned}$

c) $\begin{aligned}x_1+x_2+2x_3+2x_4+7x_5&=0,\\ 2x_1+3x_2+4x_3+5x_4&=0,\\ 3x_1+5x_2+6x_3+8x_4&=0.\end{aligned}$

§ 18. Модуль линейных форм

Определители, как мы уже неоднократно видели, играют чрезвычайно важную роль в исследовании и решении систем линейных уравнений. Тем не менее, можно изложить теорию линейных уравнений, совершенно не пользуясь понятием определителя. Этой задачей мы сейчас и займёмся.

Пусть $f_1, f_2, \ldots, f_m$ линейные формы от n переменных $x_1, x_2, \ldots, x_n$. Из этих форм можно составить новую форму φ, являющуюся их линейной комбинацией:

$$\varphi=c_1f_1+c_2f_2+\ldots+c_mf_m.$$

Давая коэффициентам $c_1, c_2, \ldots, c_m$ произвольные значения (в том числе и нулевые), мы, очевидно, получим бесконечное множество всевозможных форм вида. Это множество называется *линейным модулем*, или просто *модулем*; мы будем обозначать символом $(f_1, f_2, \ldots, f_m)$, а систему форм $f_1, f_2, \ldots, f_m$ называем *базисом* модуля. Очевидно, что базисом может быть названа всякая система форм $\varphi_1, \varphi_2, \ldots, \varphi_s$, от которых линейно зависит любая форма модуля. Если $f_1, f_2, \ldots, f_m$ линейно зависимы, то зависимые формы можно отбросить и вместо базиса $f_1, f_2, \ldots, f_m$ рассматривать линейно независимый базис $f_1, f_2, \ldots, f_r$. Ма...

ьное число r линейно независимых форм, входящих в состав системы $f_1, \ldots, f_m$, принято называть рангом модуля. Теории линейных уравнений, орую мы собираемся развить, основана на следующей теореме, принадлежей Штейницу.

Теорема. *Если $\varphi_1, \varphi_2, \ldots, \varphi_s$ линейно независимые формы модуля, то $s \leqslant m$ зис $f_1, f_2, \ldots, f_m$ при $s < m$ может быть заменён новым базисом $\varphi_1, \varphi_2, \ldots, \varphi_s, f_{s+1}, \ldots, f_m$, а при $s = m$ — новым базисом $\varphi_1, \varphi_2, \ldots, \varphi_m$*[1]).

Доказательство. Будем производить замену постепенно. Сначала ём форму

$$\varphi_1 = a_1 f_1 + a_2 f_2 + \ldots + a_m f_m,$$

торой по крайней мере один из коэффициентов a_i не равен нулю. Мы вправе ложить, что $a_1 \neq 0$, так как в противном случае мы могли бы изменить мерацию форм. Но если $a_1 \neq 0$, то

$$f_1 = b_1 \varphi_1 + b_2 f_2 + \ldots + b_m f_m, \tag{2}$$

$$b_1 = \frac{1}{a_1}, \quad b_2 = -\frac{a_2}{a_1}, \ldots, b_m = -\frac{a_m}{a_1}.$$

Пусть Ψ — произвольная форма модуля; она должна линейно выражаться ез базис

$$\Psi = c_1 f_1 + c_2 f_2 + \ldots + c_m f_m.$$

дставляя сюда вместо f_1 его значение (2), получим:

$$\Psi = c_1' \varphi_1 + c_2' f_2 + \ldots + c_m' f_m.$$

следнее равенство свидетельствует как раз о том, что система $\varphi_1, f_2, \ldots, f_m$ же образует базис.

Теперь введём φ_2:

$$\varphi_2 = a_1' \varphi_1 + a_2' f_2 + \ldots + a_m' f_m. \tag{3}$$

По крайней мере один из коэффициентов $a_2', a_3', \ldots, a_m'$ должен быть отличен нуля. В самом деле, если бы $a_2' = a_3' = \ldots = a_m' = 0$, то мы имели бы $\varphi_2 = a_1' \varphi_1$, это противоречит линейной независимости форм $\varphi_1, \ldots, \varphi_s$. Мы вправе предложить, что $a_2' \neq 0$, так как в противном случае мы изменили бы нумерацию рм $f_2, \ldots, f_m$. Но если $a_2' \neq 0$, то равенство (3) можно решить относительно в результате чего получится:

$$f_2 = b_1' \varphi_1 + b_2' \varphi_2 + b_3' f_3 + \ldots + b_m' f_m.$$

Затем снова берём произвольную форму Ψ, которая выражается через зис $\varphi_1, f_2, \ldots, f_m$ так:

$$\Psi = d_1 \varphi_1 + d_2 f_2 + d_3 f_3 + \ldots + d_m f_m$$

подставляем в это равенство значение f_2. Получим после подстановки

$$\Psi = d_1' \varphi_1 + d_2' \varphi_2 + d_3' f_3 + \ldots + d_m' f_m,$$

куда ясно, что система форм $\varphi_1, \varphi_2, f_3, \ldots, f_m$ также образует базис, и так продолжаем далее.

Относительно s можно высказать только три предположения: либо $s < m$, либо $s = m$, либо $s > m$. Если $s < m$, то после указанного процесса замены форм f_i рез φ_i мы получим базис $\varphi_1, \varphi_2, \ldots, \varphi_s, f_{s+1}, \ldots, f_m$. Если $s = m$, то мы, очевидно, получим базис $\varphi_1, \ldots, \varphi_m$. Наконец, если $s > m$, то мы будем иметь базис $\varphi_1, \varphi_2, \ldots, \varphi_m$ и, кроме того, останутся лишние формы $\varphi_{m+1}, \ldots, \varphi_s$; при этом каждая из этих форм, как и любая форма модуля, будет выражаться через базис $\varphi_1, \varphi_2, \ldots, \varphi_m$. Например,

$$\varphi_{m+1} = c_1 \varphi_1 + c_2 \varphi_2 + \ldots + c_m \varphi_m.$$

Но последнее равенство противоречит линейной независимости форм $\varphi_1, \varphi_2, \ldots, \varphi_s$; следовательно, третье предположение исключается: s не может превосходить m.

[1]) В частности, индекс s можно взять равным единице.

Из этой теоремы вытекает целый ряд следствий.

Следствие 1. *Число s линейно независимых форм $\varphi_1, \ldots, \varphi_s$ не может быть больше ранга r.*

В самом деле, базис $f_1, \ldots, f_m$ можно заменить линейно независимым базисом $f_1, f_2, \ldots, f_r$. В свою очередь базис $f_1, \ldots, f_r$ можно заменить базисом $\varphi_1, \varphi_2, \ldots, \varphi_s, f_{s+1}, \ldots, f_r$ или $\varphi_1, \ldots, \varphi_r$, откуда и следует, что $s \leqslant r$.

Следствие 2. *Ранг модуля не зависит от выбора базиса.*

Действительно, пусть кроме базиса $f_1, f_2, \ldots, f_m$ существует ещё другой базис $\varphi_1, \varphi_2, \ldots, \varphi_s$, относительно которого ранг модуля равен r'. Тогда, в силу следствия 1, с одной стороны, число линейно независимых форм не может быть больше первоначального ранга r, $r' \leqslant r$, а с другой стороны, оно не может быть больше ранга r', $r \leqslant r'$. Сопоставление этих неравенств показывает, что $r' = r$.

Только что доказанная теорема имеет чрезвычайно важное значение: из неё как простое следствие вытекает вся теория линейных уравнений. Кроме того, эта теорема приводит к новому способу определения ранга, к так называемому *способу исключения*.

Рассмотрим модуль $(x_1, \ldots, x_n)$; он состоит из всевозможных линейных форм от переменных $x_1, x_2, \ldots, x_n$ и потому содержит как часть модуль $(f_1, f_2, \ldots, f_m)$. Пусть

$$\left.\begin{aligned} f_1 &= a_{11}x_1 + \ldots + a_{1n}x_n, \\ f_2 &= a_{21}x_1 + \ldots + a_{2n}x_n, \\ &\cdots\cdots\cdots\cdots \\ f_m &= a_{m1}x_1 + \ldots + a_{mn}x_n. \end{aligned}\right\} \qquad (4)$$

По крайней мере один из коэффициентов формы f_1 не должен быть равен нулю. Без ограничения общности можно предположить, что $a_{11} \neq 0$; если бы это не имело места, то мы изменили бы нумерацию переменных. А теперь из первого уравнения системы (4) находим x_1 и подставляем его значение во все остальные уравнения. Получим:

$$\begin{aligned} f_2 &= b_{21}f_1 + b_{22}x_2 + \ldots + b_{2n}x_n, \\ &\cdots\cdots\cdots\cdots\cdots \\ f_m &= b_{m1}f_1 + b_{m2}x_2 + \ldots + b_{mn}x_n. \end{aligned}$$

Может случиться, что одна из форм f_i будет выражаться только через f_1; такую форму, как линейно зависимую, мы отбросим. Далее, подобно тому, как мы исключали x_1, исключаем x_2 и т. д. Действуя так, мы в конце концов переменные $x_1, \ldots, x_r$ заменим формами $f_1, f_2, \ldots, f_r$ и вместо базиса $x_1, \ldots, x_n$ получим базис $f_1, f_2, \ldots, f_r, x_{r+1}, \ldots, x_n$[1]). Легко видеть, что r и есть ранг модуля $(f_1, f_2, \ldots, f_m)$. В самом деле, ранг модуля $(x_1, x_2, \ldots, x_n)$ равен n; поэтому его новый базис $f_1, f_2, \ldots, f_r, x_{r+1}, \ldots, x_n$ линейно независим (см. следствие 2); в частности линейно независима и система форм $f_1, f_2, \ldots, f_r$, образующая базис модуля $(f_1, f_2, \ldots, f_m)$.

Пример. Определить ранг модуля, имеющего базисом

$$\begin{aligned} f_1 &= x_1 - x_2 + x_3, \\ f_2 &= x_1 + x_2 - x_3, \\ f_3 &= x_1 - 5x_2 + 5x_3. \end{aligned}$$

Сначала исключаем x_1, для чего

$$x_1 = f_1 + x_2 - x_3$$

подставляем в выражения f_2 и f_3:

$$\begin{aligned} f_2 &= f_1 + 2x_2 - 2x_3, \\ f_3 &= f_1 - 4x_2 + 4x_3. \end{aligned}$$

---

[1]) Здесь и в дальнейшем мы для краткости будем писать $f_1, f_2, \ldots, f_r, x_{r+1}, \ldots, x_n$, имея в виду оба случая $r < n$ и $r = n$. Если $r = n$, то надо в записи $f_1, f_2, \ldots, f_r, x_{r+1}, \ldots, x_n$ переменные $x_{r+1}, \ldots, x_n$ просто отбросить.

Затем исключаем x_2, для чего пишем:

$$2x_2 = f_2 - f_1 + 2x_3$$

и подставляем в выражение f_3. Имеем:

$$f_3 = 3f_1 - 2f_2,$$

т. е. форму f_3, как линейно зависимую, можно отбросить. Итак, мы x_1 и x_2 заменили через f_1 и f_2, следовательно, ранг модуля (f_1, f_2, f_3) равен двум.

Переходим к непосредственному изложению теории линейных уравнений. Пусть

$$f_i = a_{i1}x_1 + \ldots + a_{in}x_n = b_i \quad (i = 1, 2, \ldots, m) \tag{5}$$

— система m уравнений с n неизвестными. Левые части этих уравнений суть линейные формы от n переменных; мы их обозначили через $f_1, f_2, \ldots, f_m$. Введём, кроме того, следующую вспомогательную систему форм от $n+1$ переменных $x_1, \ldots, x_n, x_{n+1}$:

$$F_1 = f_1 - b_1x_{n+1}, \quad F_2 = f_2 - b_2x_{n+1}, \quad \ldots, \quad F_m = f_m - b_mx_{n+1}.$$

Мы собираемся вновь доказать хорошо знакомую нам теорему:

Теорема Кронекера-Капелли. *Система линейных уравнений* (5) *совместна тогда и только тогда, когда ранг модуля* $(f_1, \ldots, f_m)$ *равен рангу модуля* $(F_1, \ldots, F_m)$.

Доказательство. Покажем сперва, что система не может быть совместной, когда ранг r_1 модуля $(F_1, \ldots, F_m)$ выше ранга r модуля $(f_1, \ldots, f_m)$ [1]).

В самом деле, если $r < r_1$, то формы $f_1, \ldots, f_{r1}$ будут линейно зависимы: $c_1f_1 + \ldots + c_{r1}f_{r1} \equiv 0$, а формы $F_1, \ldots, F_{r1}$ линейно независимы: $c_1F_1 + \ldots + c_{r1}F_{r1} \not\equiv 0$. Отсюда следует, что

$$c_1F_1 + \ldots + c_{r1}F_{r1} \equiv -(b_1c_1 + \ldots + b_{r1}c_{r1})\, x_{n+1} \not\equiv 0,$$

т. е. $b_1c_1 + \ldots + b_{r1}c_{r1} \neq 0$.

Допустим теперь, что система (5) совместна, например, имеет решение $x_1 = \alpha_1, \ldots, x_n = \alpha_n$. Тогда при $x_1 = \alpha_1, \ldots, x_n = \alpha_n, x_{n+1} = 1$ формы $F_1, F_2, \ldots, F_{r1}$ обращаются в нуль, а потому обращается в нуль и их линейная комбинация $c_1F_1 + \ldots + c_{r1}F_{r1}$. Но последнее невозможно, так как $b_1c_1 + \ldots + b_{r1}c_{r1} \neq 0$.

Переходим ко второму случаю: $r = r_1$. Если $r = r_1$, то $f_1, \ldots, f_r$, а также и $F_1, \ldots, F_r$ должны быть линейно независимыми. Иными словами, первые r уравнений системы (5) будут линейно независимыми, а остальные будут от них линейно зависеть. Эти зависимые уравнения можно смело отбросить и ограничиться первыми r уравнениями. Так как $f_1, f_2, \ldots, f_r$ линейно независимы, то по теореме Штейница базис модуля $(x_1, x_2, \ldots, x_n)$ можно заменить новым базисом $f_1, f_2, \ldots, f_r, x_{r+1}, \ldots, x_n$, откуда

$$x_i \equiv (\delta_{i1}f_1 + \ldots + \delta_{ir}f_r) + (\beta_{i1}x_{r+1} + \ldots + \beta_{i\,n-r}x_n) \quad (i = 1, 2, 3, \ldots, r). \tag{6}$$

Мы покажем сейчас, что

$$x_i = (\delta_{i1}b_1 + \ldots + \delta_{ir}b_r) + (\beta_{i1}x_{r+1} + \ldots + \beta_{i\,n-r}x_n) \tag{7}$$

и есть *общее* решение системы (5). Подставим значения $x_1, \ldots, x_r$ из (6) в первые r линейных форм f_i. Получим тогда равенства вида

$$f_i = c_{i1}f_1 + \ldots + c_{ii}f_i + \ldots + c_{ir}f_r + c_{ir+1}x_{r+1} + \ldots + c_{in}x_n \quad (i = 1, 2, \ldots, r). \tag{8}$$

[1]) Очевидно, r_1 не может быть меньше r, так как тогда формы $F_1, \ldots, F_r$ будут линейно зависимы:

$$c_1F_1 + \ldots + c_rF_r \equiv 0.$$

Полагая в этом тождестве $x_{n+1} = 0$, получим $c_1f_1 + \ldots + c_rf_r \equiv 0$, что противоречит независимости $f_1, \ldots, f_r$.

Так как $f_1, \ldots, f_r, x_{r+1}, \ldots, x_n$ есть *линейно независимый* базис модуля $(x_1, x_2, \ldots, x_n)$, то $c_{ii}=1$, а все остальные коэффициенты c_{ij} равны нулю. Но тогда равенства (8) будут выполняться при любых значениях $f_1, \ldots, f_r, x_{r+1}, \ldots, x_n$. В частности (8) будут удовлетворяться при $f_1=b_1$, $f_2=b_2$, ..., $f_r=b_r$ и произвольных значениях свободных неизвестных $x_{r+1}, \ldots, x_n$. Таким образом (7) есть решение системы (5).

Обратно, пусть $x_1=\alpha_1, \ldots, x_n=\alpha_n$ какое-нибудь решение системы (5). Подставляя эти значения неизвестных в тождества (6), получим, очевидно:

$$\alpha_i=(\delta_{i1}b_1+\ldots+\delta_{ir}b_r)+(\beta_{i1}\alpha_{r+1}+\ldots+\beta_{in}\alpha_n).$$

Мы видим, что решение $x_1=\alpha_1, \ldots, x_n=\alpha_n$ удовлетворяет равенствам (7).

Итак, равенства (7) дают все корни нашей системы, т. е. (7) есть общее решение.

Пример. Рассмотрим систему уравнений:

$$\begin{aligned} f_1&= x_1-x_2+2x_3=1,\\ f_2&= x_1-2x_2-x_3=2,\\ f_3&=3x_1-x_2+5x_3=3,\\ f_4&=-2x_1+2x_2+3x_3=-4. \end{aligned}$$

Легко видеть, что ранг модуля (f_1, f_2, f_3, f_4) равен рангу модуля (F_1, F_2, F_3, F_4); именно, $r=r_1=3$. Следовательно, данная система совместна и допускает единственное решение, так как число свободных неизвестных равно нулю: $n-r=3-3=0$. Предлагаем читателю самостоятельно решить эту систему, пользуясь способом подстановки неизвестных.

§ 19. Теория линейных уравнений в векторной форме

В заключение познакомимся в основных чертах с так называемым векторным изложением теории линейных уравнений.

Поскольку линейная форма $f=a_1x_1+\ldots+a_nx_n$ вполне определяется своими коэффициентами, мы можем вместо линейной формы рассматривать систему n чисел $a_1, \ldots, a_n$, взятых в определённом порядке [1]). Обозначим эту систему через

$$\bar{a}=(a_1, \ldots, a_n)$$

и назовём её *n-мерным вектором* или, короче, вектором, а числа a_i — *компонентами* или *координатами* вектора. В частности вектор $(0, 0, \ldots, 0)$ с компонентами, равными нулю, мы будем называть *нулевым вектором* и для краткости обозначать через 0. Совокупность всех n-мерных векторов принято называть *n-мерным векторным пространством*.

Два вектора, отличающиеся друг от друга порядком следования компонентов или самими компонентами, мы будем считать различными. Иными словами:

I. Два вектора $\bar{a}=(a_1, \ldots, a_n)$ и $\bar{b}=(b_1, \ldots, b_n)$ равны тогда и только тогда, когда $a_1=b_1, \ldots, a_n=b_n$.

Для дальнейшего нам придётся ввести ещё два понятия — понятие суммы векторов и понятие умножения числа на вектор.

Сложение мы определяем так:

II. $\bar{a}+\bar{b}=(a_1, \ldots, a_n)+(b_1, \ldots, b_n)=(a_1+b_1, \ldots, a_n+b_n)$.

Это понятие суммы можно распространить и на любое число слагаемых.

Умножение числа c на вектор $\bar{a}=(a_1, \ldots, a_n)$ мы определяем следующим образом:

III. $\bar{a}\cdot c=c\cdot\bar{a}=(a_1c, \ldots, a_nc)$.

Нетрудно убедиться, что сложение векторов и умножение числа на вектор обладают следующими свойствами:

---

[1]) Числа a_i могут быть не только действительными, но и комплексными.

1. Переместительный (коммутативный) закон сложения:

$$\bar{a}+\bar{b}=\bar{b}+\bar{a}.$$

2. Сочетательный (ассоциативный) закон сложения:

$$(\bar{a}+\bar{b})+\bar{c}=\bar{a}+(\bar{b}+\bar{c}).$$

3. Переместительный (коммутативный) закон для умножения числа на вектор:

$$\bar{a}\cdot c=c\cdot\bar{a}.$$

4. Распределительный (дистрибутивный) закон для умножения числа на вектор:

$$c\cdot(\bar{a}+\bar{b})=c\cdot\bar{a}+c\cdot\bar{b},$$
$$(c+d)\,\bar{a}=c\cdot\bar{a}+d\cdot\bar{a}.$$

5. $\bar{a}+\bar{0}=\bar{a}$, т. е. нулевой вектор ведёт себя при сложении как обычное число нуль.

6. Уравнение $\bar{a}+\bar{z}=\bar{b}$ всегда имеет единственное решение, а именно если $\bar{a}=(a_1, \ldots, a_n)$ и $\bar{b}=(b_1, \ldots, b_n)$, то $\bar{z}=(b_1-a_1, \ldots, b_n-a_n)$.

Это решение называется разностью векторов $\bar{b}$ и $\bar{a}$ и обозначается через $\bar{b}-\bar{a}$. В частности, разность $\bar{0}-\bar{a}$ обозначается просто через $-\bar{a}$ и называется вектором, противоположным вектору $\bar{a}$.

Мы опускаем выводы этих свойств; в § 42, посвящённом гиперкомплексным числам, читатель найдёт аналогичные определения и свойства с подробными выводами.

Заменим теперь обозначение $(a_1, \ldots, a_n)$ вектора другим выражением. Именно, по определению сложения векторов и умножения числа на вектор

$$\bar{a}=(a_1, \ldots, a_n)=(a_1, 0, \ldots, 0)+\ldots+(0, 0, \ldots, 0, a_n)=$$
$$=a_1(1, 0, \ldots, 0)+\ldots+a_n(0, 0, \ldots, 0, 1)=a_1\cdot\bar{c}_1+\ldots+a_n\bar{c}_n,$$

где

$$\bar{c}_1=(1, 0, \ldots, 0), \ldots, \bar{c}_n=(0, \ldots, 0, 1).$$

Таким образом, мы выразили вектор $\bar{a}$ в виде линейной комбинации векторов $\bar{c}_i$. Система этих векторов $\bar{c}_i$ называется *базисом* n-мерного векторного пространства, а сами $\bar{c}_i$ — *элементами* базиса.

Мы видим, что получается некоторая аналогия с линейным модулем. Но эта аналогия проявится ещё отчётливее, если мы обратимся к так называемым векторным подпространствам.

Понятие линейной зависимости можно без изменений распространить и на n-мерные векторы. А именно, векторы $\bar{a}_1, \ldots, \bar{a}_m$ мы назовём *линейно зависимыми*, если можно подобрать такие числа $c_1, \ldots, c_m$, не все равные нулю, что имеет место равенство

$$c_1\bar{a}_1+c_2\bar{a}_2+\ldots+c_m\bar{a}_m=\bar{0}.$$

Если же это равенство возможно только в том случае, когда все числа c_i равны нулю, то векторы $\bar{a}_1, \ldots, \bar{a}_m$ называются *линейно независимыми*.

Установив понятие линейной зависимости, перейдём к определению векторного подпространства.

Пусть $\bar{a}_1, \ldots, \bar{a}_m$ — векторы n-мерного пространства. Составим из этих векторов новый вектор $\bar{b}$, являющийся их линейной комбинацией:

$$\bar{b}=c_1\bar{a}_1+\ldots+c_m\bar{a}_m. \qquad (1)$$

Давая числам c_i произвольные значения (в том числе и нулевые), мы получим множество всевозможных векторов вида (1). Это множество называется *векторным подпространством* n-мерного векторного пространства; мы его

будем обозначать символом $\{\bar{a}_1, \ldots, \bar{a}_m\}$, а систему векторов $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_m$ называть *базисом* векторного подпространства. Легко заметить, что базисом может служить всякая система векторов, от которых линейно зависит любой вектор подпространства. Если $\bar{a}_1, \ldots, \bar{a}_m$ линейно зависимы, то зависимые векторы можно отбросить и вместо базиса $\bar{a}_1, \ldots, \bar{a}_m$ рассматривать линейно независимый базис $\bar{a}_1, \ldots, \bar{a}_r$. Максимальное число r линейно независимых векторов, входящих в состав системы $\bar{a}_1, \ldots, \bar{a}_m$, называется *числом измерений* векторного подпространства, вследствие чего само векторное подпространство получает наименование r-мерного.

Подведём итог. Из всего изложенного видно, что n-мерный вектор играет роль линейной формы, а r-мерное векторное подпространство — роль линейного модуля ранга r. Дальнейшая теория уже ничем не будет отличаться от теории линейного модуля. Придётся только всюду вместо линейной формы говорить о n-мерном векторе, вместо линейного модуля ранга r — о r-мерном векторном подпространстве и вместо ранга — о числе измерений векторного подпространства.

Применим все эти выводы к системе уравнений:

$$f_i = a_{i1}x_1 + \ldots + a_{in}x_n = b_i \quad (i = 1, \ldots, m). \tag{2}$$

Составим из коэффициентов при неизвестном x_k вектор

$$\bar{a}_k = (a_{1k}, a_{2k}, \ldots, a_{mk}) \quad (k = 1, 2, \ldots, n)$$

и из свободных членов вектор

$$\bar{b} = (b_1, \ldots, b_m).$$

Можно высказать следующий критерий совместности системы линейных уравнений:

Система линейных уравнений (2) *совместна тогда и только тогда, когда векторное подпространство* $\{\bar{a}_1, \ldots, \bar{a}_n\}$ *совпадает с векторным подпространством* $\{\bar{a}_1, \ldots, \bar{a}_n, \bar{b}\}$.

Доказательство. Заметим прежде всего, что система уравнений (2) равносильна одному векторному уравнению

$$\bar{a}_1x_1 + \bar{a}_2x_2 + \ldots + \bar{a}_nx_n = \bar{b}. \tag{3}$$

В самом деле, пусть уравнение (3) удовлетворяется числами $x_1, \ldots, x_n$. Согласно определениям II и III сложения векторов и умножения числа на вектор левая часть уравнения (3) должна равняться вектору $\bar{c}$ с компонентами

$$a_{i1}x_1 + \ldots + a_{in}x_n \quad (i = 1, 2, \ldots, n).$$

По определению I равенства двух векторов эти компоненты должны равняться соответствующим компонентам вектора b:

$$a_{i1}x_1 + \ldots + a_{in}x_n = b_i.$$

Мы видим отсюда, что числа $x_1, \ldots, x_n$ удовлетворяют также и системе (2). Обратно, пусть система уравнений (2) удовлетворяется числами $x_1, \ldots, x_n$. Тогда вектор $\bar{c}$ с компонентами $a_{i1}x_1 + \ldots + a_{in}x_n$ будет, очевидно, равен вектору $\bar{b}$. Но по определению сложения векторов и умножения числа на вектор мы можем написать, что

$$\begin{aligned}\bar{c} &= (a_{11}x_1 + \ldots + a_{1n}x_n, \ldots, a_{m1}x_1 + \ldots + a_{mn}x_n) = \\ &= (a_{11}x_1, a_{21}x_1, \ldots, a_{m1}x_1) + \ldots + (a_{1n}x_n, a_{2n}x_n, \ldots, a_{mn}x_n) = \\ &= (a_{11}, a_{21}, \ldots, a_{m1})\,x_1 + \ldots + (a_{1n}, a_{2n}, \ldots, a_{mn})\,x_n = \\ &= \bar{a}_1x_1 + \ldots + \bar{a}_nx_n.\end{aligned}$$

Таким образом мы получаем, что

$$\bar{a}_1x_1 + \ldots + \bar{a}_nx_n = \bar{b},$$

т. е. числа $x_1, \ldots, x_n$ должны удовлетворять векторному уравнению (3).

Теперь доказательство критерия не представит особого труда. А именно, если система уравнений (2) совместна, то должны существовать числа $x_1, \ldots, x_n$, удовлетворяющие векторному уравнению (3). Отсюда следует, что вектор $\bar{b}$ линейно зависит от векторов $\bar{a}_1, \ldots, \bar{a}_n$. Мы можем, следовательно, выкинуть $\bar{b}$ из базиса $\bar{a}_1, \ldots, \bar{a}_n, \bar{b}$ векторного подпространства $\{\bar{a}_1, \ldots, \bar{a}_n, \bar{b}\}$, в результате чего получится векторное подпространство

$$\{\bar{a}_1, \ldots, \bar{a}_n\}.$$

Обратно, пусть векторные подпространства $\{\bar{a}_1, \ldots, \bar{a}_n\}$ и $\{\bar{a}_1, \ldots, \bar{a}_n, \bar{b}\}$ совпадают. Тогда вектор $\bar{b}$ будет содержаться в векторном подпространстве $\{\bar{a}_1, \ldots, \bar{a}_n\}$, а потому будет линейно выражаться через базис $\bar{a}_1, \ldots, \bar{a}_n$:

$$\bar{a}_1 x_1 + \ldots + \bar{a}_n x_n = \bar{b}.$$

Мы видим отсюда, что существуют числа $x_1, \ldots, x_n$, удовлетворяющие векторному уравнению (3), в силу чего система уравнений (2) совместна.

Так как векторные подпространства $\{\bar{a}_1, \ldots, \bar{a}_n\}$ и $\{\bar{a}_1, \ldots, \bar{a}_n, \bar{b}\}$ совпадают тогда и только тогда, когда они одинакового измерения, то критерий совместности линейных уравнений можно сформулировать ещё иначе: *система линейных уравнений* (2) *совместна тогда и только тогда, когда* $\{\bar{a}_1, \ldots, \bar{a}_n\}$ и $\{\bar{a}_1, \ldots, \bar{a}_n, \bar{b}\}$ *являются векторными подпространствами одинакового измерения*

ГЛАВА ТРЕТЬЯ

ЛИНЕЙНЫЕ ПРЕОБРАЗОВАНИЯ И МАТРИЦЫ. ГРУППА, КОЛЬЦО И ПОЛЕ

§ 20. Линейные преобразования и матрицы

Учение о линейных преобразованиях обязано своим возникновением аналитической геометрии. Пусть, например, XOY декартова (вообще, косоугольная) система координат на плоскости. Повернём ось OX вокруг начала координат O на угол α и изменим её единицу масштаба в m раз, а ось OY повернём так, чтобы она образовала со старым положением оси OX угол β, и изменим её единицу масштаба в n раз. Такое преобразование системы координат называется *центро-аффинным*, причём, как легко видеть, старые координаты x, y какой-нибудь точки выражаются через новые координаты по формулам:

$$x = \frac{x' \sin(\omega - \alpha) + y' \sin(\omega - \beta)}{m \sin \omega}, \quad y = \frac{x' \sin \alpha + y' \sin \beta}{n \sin \omega},$$

где ω — угол XOY. Положим:

$$\frac{\sin(\omega - \alpha)}{m \sin \omega} = a_{11}, \quad \frac{\sin(\omega - \beta)}{m \sin \omega} = a_{12}, \quad \frac{\sin \alpha}{n \sin \omega} = a_{21}, \quad \frac{\sin \beta}{n \sin \omega} = a_{22};$$

тогда наши формулы примут следующий более компактный вид:

$$\left.\begin{aligned} x &= a_{11} x' + a_{12} y', \\ y &= a_{21} x' + a_{22} y'. \end{aligned}\right\} \tag{1}$$

Мы видим, что x, y линейно выражаются через x', y' или, как мы будем постоянно говорить, преобразование (1) есть *линейное преобразование переменных* x', y'.

Точно так же, рассматривая центро-аффинные преобразования в пространстве, мы снова будем иметь линейное преобразование, но уже не двух, а трёх переменных:

$$x = a_{11}x' + a_{12}y' + a_{13}z',$$
$$y = a_{21}x' + a_{22}y' + a_{23}z',$$
$$z = a_{31}x' + a_{32}y' + a_{33}z'.$$

Таким образом получается следующее общее определение.

Определение. *Преобразование*

$$\left.\begin{aligned} y_1 &= a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n, \\ y_2 &= a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ y_n &= a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n, \end{aligned}\right\} \qquad (S)$$

при котором переменные $y_1, y_2, \ldots, y_n$ являются линейными формами переменных $x_1, x_2, \ldots, x_n$, называется линейным преобразованием переменных $x_1, x_2, \ldots, x_n$.

Преобразование S вполне характеризуется матрицей

$$A = \begin{Vmatrix} a_{11} & \ldots & a_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ a_{n1} & \ldots & a_{nn} \end{Vmatrix}$$

из коэффициентов. Поэтому вместо преобразования можно говорить о матрице.

Заметим ещё, что определитель

$$D_S = \begin{vmatrix} a_{11} & \ldots & a_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ a_{n1} & \ldots & a_{nn} \end{vmatrix}$$

принято называть *определителем преобразования* S [1]).

Между подстановками n цифр (см. § 5) и линейными преобразованиями (матрицами) имеется довольно глубокая аналогия. Если подстановка каждую цифру заменяет другой, то линейное преобразование S переменные $x_1, \ldots, x_n$ заменяет новыми переменными $y_1, \ldots, y_n$. Но сходство простирается ещё дальше: можно определить умножение преобразований и матриц по тому же принципу, что и умножение подстановок. Возьмём ещё одно преобразование T, характеризующееся матрицей:

$$B = \begin{Vmatrix} b_{11} & \ldots & b_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ b_{n1} & \ldots & b_{nn} \end{Vmatrix},$$

[1]) При этом ради большей общности выводов мы будем рассматривать и такие линейные преобразования, у которых определитель D_S равен нулю.

и посмотрим, что произойдёт, если сперва применить преобразование S и затем T. Пусть преобразование T переменные $y_1, \ldots, y_n$ переводит в $z_1, \ldots, z_n$:

$$\left.\begin{aligned} z_1 &= b_{11}y_1 + b_{12}y_2 + \ldots + b_{1n}y_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ z_n &= b_{n1}y_1 + b_{n2}y_2 + \ldots + b_{nn}y_n. \end{aligned}\right\} \qquad (T)$$

Легко видеть, что при совместном действии преобразований S и T переменные $x_1, \ldots, x_n$ переходят в $z_1, \ldots, z_n$; с другой стороны, подставляя значения y_i из (S) в равенства (T), получим:

$$\begin{aligned} z_i = b_{i1}(a_{11}x_1 + \ldots + a_{1k}x_k + \ldots + a_{1n}x_n) + \ldots + \\ + b_{in}(a_{n1}x_1 + \ldots + a_{nk}x_k + \ldots + a_{nn}x_n) \\ (i = 1, 2, \ldots, n), \end{aligned}$$

или

$$\begin{aligned} z_i = (b_{i1}a_{11} + b_{i2}a_{21} + \ldots + b_{in}a_{n1})x_1 + \ldots + \\ + (b_{i1}a_{1k} + b_{i2}a_{2k} + \ldots + b_{in}a_{nk})x_k + \ldots + \\ + (b_{i1}a_{1n} + b_{i2}a_{2n} + \ldots + b_{in}a_{nn})x_n \quad (i = 1, 2, \ldots, n). \end{aligned} \qquad (U)$$

Мы пришли к преобразованию U, которое производит то же действие, что и последовательное применение преобразований S и T; следовательно, преобразование U можно назвать *произведением* S и T, а матрицу C, характеризующую U, *произведением матриц* A и B. Произведение преобразований и матриц мы будем записывать тем же символом, что и обычное произведение. Таким образом:

$$U = T \cdot S; \quad C = B \cdot A.$$

Заметим, что здесь преобразование, выполняемое первым, записывается первым справа; в том же порядке записываются сомножители матричного произведения.

Посмотрим, по какому закону составлена матрица-произведение C. Легко заметить, что элемент c_{ik} матрицы C, лежащий на пересечении i-й строки и k-го столбца, выражается через элементы матриц A и B следующим образом:

$$c_{ik} = b_{i1}a_{1k} + b_{i2}a_{2k} + \ldots + b_{in}a_{nk}.$$

Иными словами, матрицы B и A перемножаются по тому же правилу, что и определители (см. § 9): элемент c_{ik} равен сумме произведений элементов i-й строки матрицы B на соответствующие элементы k-го столбца матрицы A.

Отсюда между прочим следует, что $D_T D_S = D_U$, где D_S, D_T, D_U — определители преобразований S, T и U.

Пример 1.

$$\begin{Vmatrix} 1 & 2 & 3 \\ 2 & 0 & 1 \\ 3 & -1 & 1 \end{Vmatrix} \cdot \begin{Vmatrix} 5 & 0 & 7 \\ 1 & 2 & 3 \\ -1 & 0 & 2 \end{Vmatrix} =$$

$$= \begin{Vmatrix} 1\cdot 5+2\cdot 1+3\cdot(-1) & 1\cdot 0+2\cdot 2+3\cdot 0 & 1\cdot 7+2\cdot 3+3\cdot 2 \\ 2\cdot 5+0\cdot 1+1\cdot(-1) & 2\cdot 0+0\cdot 2+1\cdot 0 & 2\cdot 7+0\cdot 3+1\cdot 2 \\ 3\cdot 5+(-1)\cdot 1+1\cdot(-1) & 3\cdot 0+(-1)\cdot 2+1\cdot 0 & 3\cdot 7+(-1)\cdot 3+1\cdot 2 \end{Vmatrix} =$$

$$= \begin{Vmatrix} 4 & 4 & 19 \\ 9 & 0 & 16 \\ 13 & -2 & 20 \end{Vmatrix}.$$

Вычислим для контроля определители D_S, D_T и D_U:

$$D_S = \begin{vmatrix} 1 & 2 & 3 \\ 2 & 0 & 1 \\ 3 & -1 & 1 \end{vmatrix} = -3, \quad D_T = \begin{vmatrix} 5 & 0 & 7 \\ 1 & 2 & 3 \\ -1 & 0 & 2 \end{vmatrix} = 34,$$

$$D_U = \begin{vmatrix} 4 & 4 & 19 \\ 9 & 0 & 16 \\ 13 & -2 & 20 \end{vmatrix} = -102.$$

Легко видеть, что $-3\cdot 34 = -102$.

Пример 2.

$$\begin{Vmatrix} a & b \\ c & d \end{Vmatrix} \cdot \begin{Vmatrix} a_1 & b_1 \\ c_1 & d_1 \end{Vmatrix} = \begin{Vmatrix} aa_1+bc_1 & ab_1+bd_1 \\ a_1c+c_1d & b_1c+dd_1 \end{Vmatrix}.$$

Мы умножали матрицу B на A, в результате чего получилась матрица $C=BA$. Но если умножить A на B, то, как легко убедиться на конкретных примерах, получится, вообще говоря, другое произведение. Например,

$$AB = \begin{Vmatrix} 0 & -1 \\ 2 & 3 \end{Vmatrix} \cdot \begin{Vmatrix} 5 & 1 \\ 0 & 7 \end{Vmatrix} = \begin{Vmatrix} 0 & -7 \\ 10 & 23 \end{Vmatrix},$$

но

$$BA = \begin{Vmatrix} 5 & 1 \\ 0 & 7 \end{Vmatrix} \cdot \begin{Vmatrix} 0 & -1 \\ 2 & 3 \end{Vmatrix} = \begin{Vmatrix} 2 & -2 \\ 14 & 21 \end{Vmatrix}.$$

Таким образом порядок перемножения матриц (и тем самым преобразований) существенен—умножение матриц и преобразований некоммутативно, т. е., вообще говоря, $AB \neq BA$.

Затем можно доказать совершенно так же, как это было доказано для подстановок, что умножение преобразований и матриц подчиняется сочетательному (ассоциативному) закону: $U(TS)=(UT)S$.

В самом деле, пусть преобразование S переводит переменные $x_1, \ldots, x_n$ в $y_1, \ldots, y_n$, преобразование T переменные $y_1, \ldots, y_n$ переводит в $z_1, \ldots, z_n$ и, наконец, преобразование U переводит $z_1, \ldots, z_n$

в $u_1, \ldots, u_n$. Посмотрим, как ведёт себя $U(TS)$. Легко видеть, что произведение TS переводит $x_1, \ldots, x_n$ в $z_1, \ldots, z_n$, после чего U переводит $z_1, \ldots, z_n$ в $u_1, \ldots, u_n$. Таким образом $U(TS)$ переменные $x_1, \ldots, x_n$ переводит в $u_1, \ldots, u_n$. Но точно так же ведёт себя и $(UT)S$. Действительно, S переводит $x_1, \ldots, x_n$ в $y_1, \ldots, y_n$, после чего UT преобразует $y_1, \ldots, y_n$ в $u_1, \ldots, u_n$. Итак, мы вправе написать, что $U(TS) = (UT)S$ и тем самым $C(BA) = (CB)A$, где A, B, C — матрицы, характеризующие преобразования S, T, U.

Среди всевозможных преобразований выделяется одно, а именно:

$$\left.\begin{aligned} y_1 &= x_1, \\ y_2 &= x_2, \\ &\ldots \\ y_n &= x_n, \end{aligned}\right\} \qquad (I)$$

называемое *тождественным*; оно ведёт себя совершенно так же, как единичная подстановка, потому что переменные $x_1, \ldots, x_n$ преобразованием I не изменяются. Его матрица

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

называется *единичной* и ведёт себя при умножении, очевидно, как единица. В этом можно убедиться и непосредственно. В самом деле,

$$AE = \begin{Vmatrix} a_{11} & \ldots & a_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ a_{n1} & \ldots & a_{nn} \end{Vmatrix} \cdot \begin{Vmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & 1 \end{Vmatrix} = \begin{Vmatrix} a_{11} & \ldots & a_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ a_{n1} & \ldots & a_{nn} \end{Vmatrix} = A,$$

$$EA = \begin{Vmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & 1 \end{Vmatrix} \cdot \begin{Vmatrix} a_{11} & \ldots & a_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ a_{n1} & \ldots & a_{nn} \end{Vmatrix} = \begin{Vmatrix} a_{11} & \ldots & a_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ a_{n1} & \ldots & a_{nn} \end{Vmatrix} = A,$$

так как для AE

$$c_{ik} = a_{i1} \cdot 0 + a_{i2} \cdot 0 + \ldots + a_{ik} \cdot 1 + \ldots + a_{in} \cdot 0 = a_{ik},$$

а для EA

$$c_{ik} = 0 \cdot a_{1k} + 0 \cdot a_{2k} + \ldots + 1 \cdot a_{ik} + \ldots + 0 \cdot a_{nk} = a_{ik}.$$

Сходство с подстановками несколько нарушается в одном: если для всякой подстановки существует обратная подстановка, то для преобразований (и матриц) это не всегда имеет место. Под *обратным* преобразованием мы, по аналогии с подстановками, разумеем такое преобразование S^{-1}, что

$$SS^{-1} = S^{-1}S = I.$$

Подобным же образом матрицу A^{-1} мы назовём *обратной* по отношению к A, если $AA^{-1}=A^{-1}A=E$. Введём следующее определение.

Определение. *Преобразование S и его матрица A называются невырождающимися, если определитель преобразования D_S не равен нулю. Если же $D_S=0$, то S и A называются вырождающимися.*

А теперь мы можем высказать такую теорему. *Обратное преобразование S^{-1} (с матрицей A^{-1}) существует в том и только в том случае, когда преобразование S (с матрицей A) — невырождающееся.*

Доказательство. Рассмотрим сперва невырождающееся преобразование:

$$\left.\begin{aligned} y_1 &= a_{11}x_1+\ldots+a_{1n}x_n,\\ &\ldots\ldots\ldots\ldots\\ y_n &= a_{n1}x_1+\ldots+a_{nn}x_n \end{aligned}\right\} \qquad (S)$$

и покажем, что для него существует обратное преобразование S^{-1}. Для этой цели выразим x_i через y_i.

Мы имеем систему n уравнений с n неизвестными $x_1, \ldots, x_n$, причём определитель $D_S \neq 0$. Следовательно, формулы Крамера применимы и

$$x_1=\frac{D_1}{D_S},\quad x_2=\frac{D_2}{D_S},\ \ldots,\ x_n=\frac{D_n}{D_S},$$

причём

$$D_i=\begin{vmatrix} a_{11} & \ldots & a_{1i-1} & y_1 & a_{1i+1} & \ldots & a_{1n}\\ a_{21} & \ldots & a_{2i-1} & y_2 & a_{2i+1} & \ldots & a_{2n}\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\ a_{n1} & \ldots & a_{ni-1} & y_n & a_{ni+1} & \ldots & a_{nn} \end{vmatrix}.$$

Разлагая D_i по элементам i-го столбца, получим

$$D_i=A_{1i}y_1+A_{2i}y_2+\ldots+A_{ni}y_n \quad (i=1, 2, \ldots, n),$$

где $A_{1i}, \ldots, A_{ni}$ — алгебраические дополнения элементов i-го столбца определителя D_S. Таким образом находим окончательно, что

$$\left.\begin{aligned} x_1 &= \frac{A_{11}}{D_S}y_1+\ldots+\frac{A_{n1}}{D_S}y_n,\\ &\ldots\ldots\ldots\ldots\\ x_n &= \frac{A_{1n}}{D_S}y_1+\ldots+\frac{A_{nn}}{D_S}y_n. \end{aligned}\right\} \qquad (S')$$

Мы утверждаем, что полученное преобразование S' и есть обратное: $S'=S^{-1}$. В самом деле, матрицы произведений SS' и $S'S$ равны соответственно:

$$\begin{Vmatrix} a_{11} & \ldots & a_{1n}\\ \cdot & & \cdot\\ \cdot & & \cdot\\ \cdot & & \cdot\\ a_{n1} & \ldots & a_{nn} \end{Vmatrix} \cdot \begin{Vmatrix} \frac{A_{11}}{D_S} & \ldots & \frac{A_{n1}}{D_S}\\ \cdot & & \cdot\\ \cdot & & \cdot\\ \cdot & & \cdot\\ \frac{A_{1n}}{D_S} & \ldots & \frac{A_{nn}}{D_S} \end{Vmatrix} = \begin{Vmatrix} 1 & \ldots & 0\\ \cdot & & \cdot\\ \cdot & & \cdot\\ \cdot & & \cdot\\ 0 & \ldots & 1 \end{Vmatrix} = E$$

и

$$\begin{Vmatrix} \frac{A_{11}}{D_S} & \dots & \frac{A_{m1}}{D_S} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \frac{A_{1n}}{D_S} & \dots & \frac{A_{nn}}{D_S} \end{Vmatrix} \cdot \begin{Vmatrix} a_{11} & \dots & a_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ a_{n1} & \dots & a_{nn} \end{Vmatrix} = \begin{Vmatrix} 1 & \dots & 0 \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ 0 & \dots & 1 \end{Vmatrix} = E,$$

так как в первом случае

$$c_{ik} = a_{i1}\frac{A_{k1}}{D_S} + a_{i2}\frac{A_{k2}}{D_S} + \dots + a_{in}\frac{A_{kn}}{D_S} = \frac{a_{i1}A_{k1} + a_{i2}A_{k2} + \dots + a_{in}A_{kn}}{D_S},$$

а во втором случае

$$c_{ik} = \frac{A_{1i}}{D_S}a_{1k} + \dots + \frac{A_{ni}}{D_S}a_{nk} = \frac{a_{1k}A_{1i} + \dots + a_{nk}A_{ni}}{D_S}$$

равно нулю при $i \neq k$ и единице при $i = k$. Итак, мы показали, что $S' = S^{-1}$[1]) и вместе с тем мы показали, что обратной матрицей для A является

$$A^{-1} = \begin{Vmatrix} \frac{A_{11}}{D_S} & \dots & \frac{A_{n1}}{D_S} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \frac{A_{1n}}{D_S} & \dots & \frac{A_{nn}}{D_S} \end{Vmatrix}.$$

Остаётся разобрать случай вырождающегося преобразования S. Пусть, вопреки нашему утверждению, обратное преобразование S^{-1} существует; тогда для матрицы A также существует обратная матрица A^{-1}, и $AA^{-1} = E$. Обозначим через D_S, $D_S{}^{-1}$ и D_I определители, составленные соответственно из матриц A, A^{-1} и E. Имеем, очевидно, что $D_S D_{S^{-1}} = D_I$; но $D_S = 0$ (потому что преобразование S вырождающееся), а

$$D_I = \begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 1 \end{vmatrix} = 1,$$

[1]) То же самое можно показать иным путём. В самом деле, чему равны $S'S$ и SS'? Преобразование S переменные $x_1, \dots, x_n$ переводит в $y_1, \dots, y_n$, а преобразование S' переменные $y_1, \dots, y_n$ переводит в $x_1, \dots, x_n$. Следовательно, произведение $S'S$ переводит $x_1, \dots, x_n$ в $x_1, \dots, x_n$, т. е. $x_1, \dots, x_n$ остаются без изменения. Таким образом $S'S$ есть тождественное преобразование $S'S = I$. Подобным же образом можно показать, что $SS' = I$.

откуда получается нелепость: $0 = 1$. Таким образом предположение об обратном преобразовании S^{-1} следует отбросить [1]).

В заключение дадим определение степени матрицы.

Умножив некоторую матрицу A на самоё себя несколько раз, мы получим так называемую степень матрицы: $AA \ldots A = A^n$. Пользуясь сочетательным законом, можно, очевидно, написать, что

$$A^n = \underbrace{AA \ldots A}_{n \text{ раз}} = \underbrace{(AA \ldots A)}_{p \text{ раз}} \cdot \underbrace{(AA \ldots A)}_{(n-p) \text{ раз}} = A^p A^{n-p}.$$

Если, в частности, матрица A невырождающаяся, то можно говорить не только о положительной, но и об отрицательной степени. А именно, под A^{-n} мы будем разуметь произведение $\underbrace{A^{-1}A^{-1} \ldots A^{-1}}_{n \text{ раз}}$.

Наконец, под A^0 мы будем всегда понимать единичную матрицу: $A^0 = E$.

Задачи. 1. Перемножить матрицы

$$\begin{Vmatrix} 1 & 0 & 1 \\ 3 & 5 & 6 \\ -1 & 0 & 2 \end{Vmatrix} \cdot \begin{Vmatrix} 2 & 4 & 5 \\ 1 & 0 & 7 \\ 7 & 1 & 2 \end{Vmatrix} \cdot \begin{Vmatrix} 2 & 0 & 5 \\ 3 & 1 & 0 \\ -1 & -2 & 0 \end{Vmatrix};$$

2. Найти A^{-2}, если

$$A = \begin{Vmatrix} 1 & 0 & 1 \\ 3 & 5 & 6 \\ -1 & 0 & 2 \end{Vmatrix};$$

3. Показать, что произведение двух невырождающихся матриц есть снова невырождающаяся матрица.

§ 21. Группа

Свойства умножения подстановок, преобразований и матриц, изученные в § 5 и 20, приводят нас к одному из важнейших понятий современной алгебры—к понятию группы. Какими свойствами обладает, например, операция умножения подстановок? Она обладает следующими свойствами:

а) Произведение двух подстановок n элементов есть снова подстановка n элементов.

---

[1]) Смысл доказанного заключается в следующем. Если A—невырождающееся преобразование (его детерминант D не равен нулю), то формулы (S) любой системе значений $x_1, x_2, \ldots, x_n$ однозначно относят определённую систему значений $y_1, y_2, \ldots, y_n$; так как система уравнений (S) разрешима относительно $x_1, x_2, \ldots, x_n$, то и обратно, формулы (S^{-1}) любой системе значений $y_1, y_2, \ldots, y_n$ относят однозначно определённую систему значений $x_1, x_2, \ldots, x_n$.

Если же A—вырождающееся преобразование $(D=0)$, то между линейными формами, стоящими в правых частях, существует некоторая зависимость и, следовательно, такая же зависимость должна существовать между переменными $y_1, y_2, \ldots, y_n$. Поэтому переменные $y_1, y_2, \ldots, y_n$ не могут иметь произвольных значений, т. е. не каждой системе значений $y_1, y_2, \ldots, y_n$ соответствует некоторая система значений $x_1, x_2, \ldots, x_n$.

b) Умножение подчиняется сочетательному (ассоциативному) закону: $S_1(S_2S_3) = (S_1S_2)S_3$.

c) Существует такая подстановка I, называемая единичной, что $SI = S$ для любой подстановки S из n элементов.

d) Для всякой подстановки S из n элементов существует обратная подстановка S^{-1}, для которой $SS^{-1} = I$.

Если обратиться к другому примеру, к совокупности всех *невырождающихся* матриц n-го порядка (т. е. квадратных матриц, состоящих из n строк и n столбцов с не равным нулю определителем), то мы снова будем иметь те же четыре свойства умножения.

Вообще пусть $\mathfrak{G}$ — множество, состоящее из элементов $a, b, c, \ldots$ Этими элементами могут быть числа, подстановки, преобразования, матрицы, геометрические фигуры и пр. Допустим ещё, что над элементами множества можно установить некоторую операцию, которую мы условимся называть *символическим умножением*[1]). *Множество* $\mathfrak{G}$ *называется группой по отношению к символическому умножению, если выполняются следующие четыре требования:*

a) *Символическое произведение с двух элементов a и b множества есть снова элемент того же множества.*

Мы будем символическое произведение элементов a и b записывать так: $ab = c$.

b) *Символическое умножение подчиняется ассоциативному (сочетательному) закону:* $a(bc) = (ab)c$.

c) *Среди элементов* $\mathfrak{G}$ *существует по крайней мере один такой элемент e, называемый правой единицей, что* $ae = a$ *для любого a из* $\mathfrak{G}$.

d) *Для всякого элемента a из* $\mathfrak{G}$ *существует по крайней мере один такой элемент* a^{-1} *из* $\mathfrak{G}$, *называемый правым обратным элементом, что* $aa^{-1} = e$.

Если, сверх того, символическое умножение всегда коммутативно (всегда $ab = ba$), то группа $\mathfrak{G}$ называется *абелевой группой*, по имени впервые рассматривавшего эти группы гениального норвежского математика Н. Г. Абеля (N. H. Abel).

Из этого определения следует, что множество всех подстановок n элементов по отношению к операции умножения подстановок образует группу и притом неабелеву. Неабелеву группу образует и совокупность всех невырождающихся матриц n-го порядка по отношению к операции умножения матриц.

Напротив, множество всех целых положительных чисел не образует группы по отношению к операции умножения, так как требование d) не выполняется. В самом деле, если, например, $a \neq 1$ есть целое число, то $a^{-1} = \frac{1}{a}$ не будет уже целым.

Укажем ещё другие примеры групп.

Пример 1. Множество всех рациональных чисел, если из него исключить нуль, образует абелеву группу по отношению к арифметическому умножению. При этом роль элемента e играет число 1, роль обратного элемента для числа a — число $\frac{1}{a}$.

---

[1]) Мы ввели термин «символическое умножение» для того, чтобы читатель не смешивал это умножение с обычным арифметическим умножением.

Пример 2. Множество рациональных чисел образует группу и притом опять-таки абелеву, по отношению к операции сложения. Но здесь роль элемента e будет играть уже не число 1, а число 0, обратным элементом для a будет уже не $\frac{1}{a}$, а $-a$ (т. е. противоположное по знаку число).

Пример 3. Рассмотрим совокупность всех иррациональностей вида $a+b\sqrt{2}$, где a и b — рациональные числа, не равные одновременно нулю. Легко убедиться, что эта совокупность по отношению к умножению образует группу. Для этого надо проверить, выполняются ли все четыре требования, характеризующие группу.

Перемножим два числа

$$z_1=(a_1+b_1\sqrt{2}),\quad z_2=(a_2+b_2\sqrt{2})$$

нашей совокупности и получим:

$$z_1z_2=(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}.$$

Покажем, что $a_1a_2+2b_1b_2$ и $a_1b_2+a_2b_1$ не могут одновременно обращаться в нуль. В самом деле, если бы было

$$\begin{aligned}a_1a_2+2b_1b_2&=0,\\ a_1b_2+a_2b_1&=0,\end{aligned}$$

то система двух однородных уравнений с двумя неизвестными

$$\begin{aligned}a_1x+2b_1y&=0,\\ b_1x+a_1y&=0\end{aligned}$$

имела бы ненулевое решение $x=a_2$, $y=b_2$. Но это возможно лишь в том случае, когда определитель системы равен нулю:

$$\Delta=\begin{vmatrix}a_1 & 2b_1\\ b_1 & a_1\end{vmatrix}=a_1^2-2b_1^2=0.$$

Но из этого равенства имеем: $\frac{a_1}{b_1}=\sqrt{2}$, т. е. получается нелепость: $\sqrt{2}$, число заведомо иррациональное, в то же время является рациональным.

Итак, требование a) выполняется: z_1z_2 есть снова иррациональность вида $a+b\sqrt{2}$, где a и b — рациональные числа, не равные одновременно нулю.

Требование b), очевидно, выполняется, так как умножение чисел и в частности наших иррациональностей подчиняется сочетательному закону.

Столь же очевидно выполняется и третье требование c), так как роль элемента e играет число $1=1+0\cdot\sqrt{2}$.

Остаётся проверить последнее требование d). Пусть $z=a+b\sqrt{2}$ — какое-нибудь число рассматриваемой совокупности. Положим

$$z^{-1}=x+y\sqrt{2}$$

айдём, чему равны x и y. С одной стороны,

$$zz^{-1}=(a+b\sqrt{2})(x+y\sqrt{2})=(ax+2by)+(bx+ay)\sqrt{2}.$$

другой стороны, произведение zz^{-1} должно равняться единице; ледовательно, должно быть:

$$(ax+2by)+(bx+ay)\sqrt{2}=1.$$

это равенство возможно лишь тогда, когда

$$ax+2by=1,$$
$$bx+ay=0.$$

Решая полученную систему уравнений относительно x и y, будем меть $x=\frac{a}{a^2-2b^2}$, $y=-\frac{b}{a^2-2b^2}$, причём x и y не обращаются новременно в нуль. Таким образом мы нашли обратное число

$$z^{-1}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2},$$

ринадлежащее нашей совокупности; стало быть, требование d) выполняется.

Задачи: 1. Показать, что множество иррациональностей вида

$$a+b\sqrt{5},$$

где a и b—рациональные числа, не равные одновременно нулю, образуют абелеву группу по отношению к умножению. Образует ли это множество группу по отношению к операции сложения?

2. Образует ли множество матриц вида

$$\begin{Vmatrix} a & 0 \\ 0 & b \end{Vmatrix}$$

группу по отношению к операции умножения матриц (a и b—любые действительные числа)?

Вернёмся к общему определению группы. Согласно требованию в группе $\mathfrak{G}$ должна существовать по крайней мере одна правая единица e. Возникает естественный вопрос: могут ли помимо e существовать другие правые единицы и будет ли e также и *левой единицей*, т. е. будет ли $ea=a$ для любого элемента a группы $\mathfrak{G}$?

Можно высказать следующую теорему.

Теорема I. *Группа $\mathfrak{G}$ содержит только одну единицу e, которая является как правой, так и левой единицей.*

Доказательство. Покажем сперва, что для элемента a элемент a^{-1} будет не только правым, но и левым обратным элементом. В силу требования имеем:

$$aa^{-1}=e. \tag{1}$$

Умножим обе части равенства (1) слева на a^{-1}; тогда получится

$$a^{-1}aa^{-1}=a^{-1}e,$$

или согласно c)

$$a^{-1}aa^{-1}=a^{-1}. \tag{2}$$

С другой стороны, пусть b правый обратный элемент для a^{-1}, так что $a^{-1}b=e$. Тогда, умножив обе части равенства (2) справа на b, получим

$$a^{-1}aa^{-1}b=a^{-1}b,$$

или

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

или, окончательно, $a^{-1}a=e$, т. е. a^{-1} есть также и левый обратный элемент.

А теперь теорема доказывается очень легко. Умножив справа обе части равенства (1) на a, будем иметь

$$(aa^{-1})\,a=ea,$$

или $a\,(a^{-1}a)=ea$ или, окончательно, $ae=a=ea$, т. е. видим, что e является не только правой, но и левой единицей.

Остаётся показать, что других единиц, кроме e, не существует. Предположим, что e_1—другая единица $\mathfrak{G}$. Так как e_1—единица, то $ee_1=e$. Но, с другой стороны, e—также единица, откуда $ee_1=e_1$. Сравнивая равенства $ee_1=e$ и $ee_1=e_1$, получаем, что $e=e_1$, а это как раз и требовалось показать.

Из доказательства теоремы I видно, что можно также уточнить и требование d). А именно имеет место следующая теорема.

Теорема II. *Для всякого элемента a группы $\mathfrak{G}$ существует один и только один обратный элемент a^{-1}, который является как правым, так и левым обратным элементом.*

Доказательство. При доказательстве предыдущей теоремы мы уже показали, что a^{-1} есть также левый обратный элемент для a. Таким образом остаётся лишь показать, что кроме a^{-1} других обратных элементов не существует. Допустим, что кроме a^{-1} имеется другой обратный элемент b; $ab=e$. Тогда, умножив это равенство слева на a^{-1}, получим $a^{-1}(ab)=a^{-1}e$, или $(a^{-1}a)\,b=a^{-1}$, или $eb=a^{-1}$, или, окончательно, $b=a^{-1}$, что и требовалось показать.

Какие следствия можно вывести из доказанных теорем? Прежде всего отпадает необходимость в терминах «правая (левая) единица», «правый (левый) обратный элемент». Отныне мы можем говорить просто «единица» и «обратный элемент». Затем не мешает отметить такое важное следствие.

Следствие. *Если a и b—два элемента группы $\mathfrak{G}$, то уравнение $ax=b$ имеет единственное решение $x=a^{-1}b$. Точно так же уравнение $ya=b$ имеет единственное решение $y=ba^{-1}$.*

В самом деле, если первое уравнение умножить слева на a^{-1}, а второе справа на a^{-1}, то получится

$$x=a^{-1}b,\quad y=ba^{-1}.$$

§ 22. Общее определение кольца и поля

В § 20 мы дали определение операции умножения матриц и показали, что по отношению к умножению матрицы во многом ведут себя как обыкновенные числа. Однако это сходство с числами еще более усилится, если ввести вторую операцию, так называемую операцию сложения матриц.

Пусть даны две матрицы n-го порядка:

$$A=\begin{Vmatrix} a_{11}\dots a_{1n} \\ \cdot\quad\cdot \\ \cdot\quad\cdot \\ \cdot\quad\cdot \\ a_{n1}\dots a_{nn} \end{Vmatrix},\qquad B=\begin{Vmatrix} b_{11}\dots b_{1n} \\ \cdot\quad\cdot \\ \cdot\quad\cdot \\ \cdot\quad\cdot \\ b_{n1}\dots b_{nn} \end{Vmatrix}.$$

Суммой $A+B$ матриц A и B называется такая матрица C, каждый элемент которой есть сумма соответствующих элементов матриц A и B. Иными словами:

$$A+B=C=\begin{Vmatrix} a_{11}+b_{11}\dots a_{1n}+b_{1n} \\ \cdot\qquad\qquad\cdot \\ \cdot\qquad\qquad\cdot \\ \cdot\qquad\qquad\cdot \\ a_{n1}+b_{n1}\dots a_{nn}+b_{nn} \end{Vmatrix}.$$

Сходство матриц с числами можно иллюстрировать следующими примерами. Рассмотрим *нулевую матрицу*

$$\begin{Vmatrix} 0\dots 0 \\ \cdot\quad\cdot \\ \cdot\quad\cdot \\ \cdot\quad\cdot \\ 0\dots 0 \end{Vmatrix},$$

все элементы которой равны нулю. Она ведёт себя по отношению к сложению матриц как число нуль; поэтому нулевую матрицу обозначают символом 0. Итак, $A+0=A$, где A — любая матрица n-го порядка.

Ещё пример. Пусть A — какая-нибудь матрица

$$A=\begin{Vmatrix} a_{11}\dots a_{1n} \\ \cdot\quad\cdot \\ \cdot\quad\cdot \\ \cdot\quad\cdot \\ a_{n1}\dots a_{nn} \end{Vmatrix}.$$

Легко видеть, что матрицу

$$-A=\begin{Vmatrix} -a_{11}\dots -a_{1n} \\ \cdot\qquad\cdot \\ \cdot\qquad\cdot \\ \cdot\qquad\cdot \\ -a_{n1}\dots -a_{nn} \end{Vmatrix}$$

мы вправе назвать *противоположной*, потому что, как и для чисел, $A+(-A)=0$.

Мы сейчас покажем, что для множества матриц n-го порядка сохраняются следующие законы арифметического сложения:

a) Ассоциативный (сочетательный) закон: $(A+B)+C=A+(B+C)$.

b) Коммутативный (переста новочный) закон: $A+B=B+A$.

c) Разрешимость уравнения $A+x=B$ для любых двух матриц A и B.

d) Дистрибутивный (распределительный) закон

$$A(B+C)=AB+AC, \quad (B+C)A=BA+CA,$$

связывающий умножение со сложением.

Доказательство. В самом деле,

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

так как сложение матриц сводится к сложению соответствующих элементов, а для элементов ассоциативный и коммутативный законы, очевидно, справедливы. Столь же просто доказывается и закон c). Рассматривая уравнение

$$A+x=B,$$

убеждаемся без труда, что после прибавления матрицы $-A$ к обеим частям уравнения будет $x=B+(-A)$, так как $A+(-A)=0$. Это решение x мы будем называть *разностью матриц* A и B и писать

$$x=B-A$$

или подробно

$$x=\begin{Vmatrix} b_{11}-a_{11} \dots b_{1n}-a_{1n} \\ \cdot \qquad\qquad \cdot \\ \cdot \qquad\qquad \cdot \\ \cdot \qquad\qquad \cdot \\ b_{n1}-a_{n1} \dots b_{nn}-a_{nn} \end{Vmatrix}.$$

Таким образом матрицы можно не только складывать, но и вычитать.

Несколько сложнее доказывается закон d). Найдём, чему равно произведение $A(B+C)$. По правилу сложения матриц элемент суммы $B+C$, стоящий на пересечении j-й строки и k-го столбца, равен $b_{jk}+c_{jk}$. Затем по правилу перемножения матриц элемент d_{ik} произведения $A(B+C)$, находящийся в i-й строке и k-м столбце, равен:

$$d_{ik}=a_{i1}(b_{1k}+c_{1k})+\dots+a_{in}(b_{nk}+c_{nk}),$$

или, раскрывая скобки и группируя члены несколько иначе:

$$d_{ik}=(a_{i1}b_{ik}+\dots+a_{in}b_{nk})+(a_{i1}c_{1k}+\dots+a_{in}c_{nk}).$$

Мы видим, что в первой скобке находится элемент произведения AB, а во второй—элемент произведения AC, откуда ясно, что

$$A(B+C)=AB+AC.$$

Подобным же образом доказывается и второе соотношение

$$(B+C)A=BA+CA.$$

Однако у матриц есть и свои характерные особенности. Например, если произведение двух матриц AB равно нулю (т. е. нулевой

матрице), то мы не можем утверждать, как в обычной арифметике, что $A=0$ или $B=0$; напротив, может случиться, что

$$AB=0, \quad \text{но } A\neq 0, \quad B\neq 0. \tag{1}$$

Например,

$$\begin{Vmatrix} 0 & 0 \\ 0 & 1 \end{Vmatrix} \cdot \begin{Vmatrix} 1 & 0 \\ 0 & 0 \end{Vmatrix} = 0, \quad \text{но} \quad \begin{Vmatrix} 0 & 0 \\ 0 & 1 \end{Vmatrix} \neq 0, \quad \begin{Vmatrix} 1 & 0 \\ 0 & 0 \end{Vmatrix} \neq 0.$$

Матрицы A и B, удовлетворяющие условию (1), называются *делителями нуля*. Итак, существование делителей нуля—вот одно из резких отличий арифметики матриц от обычной арифметики [1]).

Вообще имеет место следующая теорема.

Теорема. *Матрица $A\neq 0$ является делителем нуля тогда и только тогда, когда она вырождающаяся.*

Доказательство. Пусть A—невырождающаяся матрица; покажем, что она не может быть делителем нуля. Умножим равенство $AB=0$ слева на A^{-1} [2]), тогда получим:

$$(A^{-1}A)\,B=EB=B=0,$$

т. е. условие (1) не выполняется.

Теперь пусть

$$A=\begin{Vmatrix} a_{11} \dots a_{1n} \\ \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \\ a_{n1} \dots a_{nn} \end{Vmatrix} \neq 0$$

—вырождающаяся матрица. Легко видеть, что A есть делитель нуля. В самом деле, система n однородных уравнений с n неизвестными

$$a_{i1}x_1+a_{i2}x_2+\dots+a_{in}x_n=0 \quad (i=1,\ 2,\dots,\ n)$$

имеет ненулевые решения

$$x_1=\alpha_1, \quad x_2=\alpha_2, \ \dots, \ x_n=\alpha_n,$$

так как определитель системы, как определитель вырождающейся матрицы A, равен нулю. Но в таком случае матрица

$$B=\begin{Vmatrix} \alpha_1 & \alpha_1 \dots \alpha_1 \\ \alpha_2 & \alpha_2 \dots \alpha_2 \\ \cdot & \cdot \quad \cdot \quad \cdot \\ \alpha_n & \alpha_n \dots \alpha_n \end{Vmatrix} \neq 0,$$

и произведение

$$AB=0,$$

---

[1]) Мы не говорим уже о некоммутативности умножения.

[2]) Обратная матрица A^{-1} наверное существует, так как матрица A невырождающаяся (см. § 20).

так как элемент c_{ik} произведения AB равен

$$a_{i1}x_1 + \ldots + a_{in}x_n = 0.$$

Мы видим, что условие (1) удовлетворяется.

Подмеченная аналогия с действительными числами присуща не только матрицам, но и целому ряду других объектов (комплексным, гиперкомплексным числам, многочленам, рациональным функциям и даже некоторым геометрическим операциям)[1]). Эта аналогия приводит нас к понятию кольца, столь же важному для современной алгебры, как и понятие группы. Мы сейчас дадим самое общее определение кольца.

Определение 1. *Пусть R некоторое множество элементов a, b, ... Эти элементы могут быть самой разнообразной природы: числа, матрицы, многочлены и пр. Пусть над элементами множества можно производить две операции: первую операцию мы назовём сложением, а вторую операцию—умножением и будем употреблять для обозначения этих действий обычные алгебраические символы*[2]). *Множество R называется кольцом по отношению к операциям сложения и умножения, если удовлетворяются следующие требования (аксиомы):*

a) *Замкнутость множества R по отношению к операциям сложения и умножения, т. е. сумма $a+b$ и произведение ab любых двух элементов a, b есть снова элемент R.*

b) *Выполняются сочетательные (ассоциативные) законы: $(a+b)+c=a+(b+c)$, $(ab)c=a(bc)$ для любых элементов a, b и c из R.*

c) *Операция сложения перестановочна (коммутативна): $a+b=b+a$ для любых элементов a, b из R.*

d) *Обратимость сложения, т. е. для любых двух элементов a, b из R уравнение $a+x=b$ разрешимо в R.*

e) *Выполняется распределительный (дистрибутивный) закон: $a(b+c)=ab+ac$ и $(b+c)a=ba+ca$ для любых элементов a, b, c из R.*

Примечание. Если коммутативный закон имеет место и для умножения:

$$ab=ba \text{ (для любых } a \text{ и } b \text{ из } R),$$

то кольцо называется *коммутативным*.

Эти пять требований нуждаются, однако, в некоторых комментариях.

Замечания относительно операции сложения. Очевидно, можно складывать не только два, но и любое число

---

[1]) О комплексных и гиперкомплексных числах и о многочленах речь будет ниже. Что касается геометрических преобразований, то в качестве примера можно сослаться на центро-аффинные преобразования на плоскости и в пространстве.

[2]) Само собой разумеется, что эти операции могут быть самой разнообразной природы, в зависимости от характера элементов множества R, а не только арифметическими.

элементов кольца R. Сумму нескольких элементов мы определим индуктивно:

$$a_1+a_2+a_3=(a_1+a_2)+a_3,$$
$$a_1+a_2+a_3+a_4=(a_1+a_2+a_3)+a_4,$$
$$a_1+a_2+a_3+a_4+a_5=(a_1+a_2+a_3+a_4)+a_5,$$

т. е. чтобы сложить три элемента, надо составить сумму первых двух и к полученному результату прибавить третий элемент; чтобы сложить четыре элемента, надо к сумме первых трёх прибавить четвёртый и т. д. Вообще, если сумма n элементов найдена, то сумма $n+1$ элементов найдётся из соотношения

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

Однако это не единственный способ сложения. Например, в случае трёх элементов можно было бы к первому прибавить сумму двух остальных:

$$a_1+(a_2+a_3).$$

На основании сочетательного закона легко видеть, что

$$a_1+(a_2+a_3)=(a_1+a_2)+a_3. \qquad (3)$$

Таким образом в случае трёх элементов отступление от принятого порядка сложения не влияет на результат. Мы сейчас покажем, что это обстоятельство имеет место и для любого числа элементов, т. е. во всякой сумме скобки можно расставлять по произволу:

$$(a_1+\ldots+a_p)+(a_{p+1}+\ldots+a_q)+\ldots+(a_r+\ldots+a_s)+$$
$$+(a_{s+1}+\ldots+a_{m-1}+a_m)=a_1+a_2+\ldots+a_{m-1}+a_m. \qquad (4)$$

Для доказательства воспользуемся методом индукции. При $m=3$, наше утверждение справедливо [см. соотношение (3)]; допустим, что утверждение верно для всех k; меньших некоторого m, и докажем, что тогда утверждение верно и для m.

По определению суммы левая часть равенства (4) есть не что иное, как

$$[(a_1+\ldots+a_p)+(a_{p+1}+\ldots+a_q)+\ldots+(a_r+\ldots+a_s)]+$$
$$+[a_{s+1}+\ldots+a_{m-1}+a_m]. \qquad (5)$$

В каждой из квадратных скобок число слагаемых меньше m; следовательно, согласно сделанному допущению мы можем выражение (5) переписать так:

$$[a_1+\ldots+a_s]+[(a_{s+1}+\ldots+a_{m-1})+a_m].$$

Отсюда в силу сочетательного закона:

$$[(a_1+\ldots+a_s)+(a_{s+1}+\ldots+a_{m-1})]+a_m. \qquad (6)$$

В квадратной скобке выражения (6) мы опять можем по-новому расставить круглые скобки. Объединим две скобки в одну:

$$[a_1+\ldots+a_{m-1}]+a_m,$$

но по определению суммы это будет

$$a_1 + \ldots + a_{m-1} + a_m.$$

Мы получили правую часть равенства (4), и тем самым наше утверждение для m доказано.

Таким образом, если утверждение верно для $m = 3$, то оно верно для 4, 5, 6,... и вообще для любого числа элементов.

Посмотрим теперь, что даёт аксиома c). Она утверждает, что сумма любых двух элементов кольца R не зависит от порядка следования слагаемых. Очевидно, что аксиому c) можно распространить и на любое число слагаемых, например,

$$a_1 + a_2 + a_3 + a_4 = a_2 + a_1 + a_3 + a_4 = a_2 + a_2 + a_1 + a_4$$

и т. д.

Наконец, разберём аксиому d). Пусть c—некоторый элемент кольца. Согласно аксиоме d) можно подобрать такой элемент x, что

$$c + x = c. \tag{7}$$

Мы покажем сейчас, что для любого элемента a из R

$$a + x = a,$$

т. е. x ведёт себя как число нуль. Для этой цели подбираем элемент y из R, удовлетворяющий уравнению

$$c + y = a. \tag{8}$$

Прибавим y к обеим частям уравнения (7), и получим, пользуясь сочетательным законом:

$$(c + y) + x = c + y,$$

или в силу (8):

$$a + x = a.$$

А теперь покажем, что другого «нулевого» элемента, кроме x, не существует. В самом деле, пусть x_1 тоже нулевой элемент. Так как x_1 ведёт себя как нуль, то

$$x + x_1 = x. \tag{9}$$

Но, с другой стороны, и x ведёт себя как нуль, значит,

$$x + x_1 = x_1. \tag{10}$$

Сравнивая (9) и (10), убеждаемся, что $x = x_1$. Это единственное x мы обозначим через 0 и назовём просто *нулём*.

Далее, рассмотрим уравнение типа

$$a + z = 0. \tag{11}$$

Оно имеет единственное решение. Действительно, пусть z_1 и z_2 — два корня уравнения (11), т. е.

$$a + z_1 = 0 \tag{12}$$

и

$$a + z_2 = 0.$$

Прибавив к обеим частям равенства (12) z_2, получим

$$(a+z_1)+z_2=z_2. \tag{13}$$

Но, с другой стороны,

$$(a+z_1)+z_2=(a+z_2)+z_1=0+z_1=z_1. \tag{14}$$

Сравнивая (13) и (14), получаем $z_1=z_2$.

Единственное решение уравнения (11) обозначается через $-a$ и называется элементом, противоположным по отношению к a.

Между прочим, решением уравнения $(-a)+z=0$ является, очевидно, a, откуда следует, что

$$-(-a)=a. \tag{15}$$

После того как мы определили нуль и противоположный элемент, нетрудно показать, как решается уравнение

$$a+x=b.$$

Если к обеим частям этого уравнения прибавить $-a$, то в результате получится единственное решение

$$x=b+(-a),$$

которое принято обозначать через $b-a$ и называть *разностью элементов* b и a.

Замечания относительно операции умножения. Очевидно, можно перемножать не только два, но и любое число элементов кольца. Произведение нескольких элементов мы определим по аналогии с суммой следующим образом:

$$a_1a_2a_3=(a_1a_2)\,a_3,$$
$$a_1a_2a_3a_4=(a_1a_2a_3)\,a_4$$

и вообще

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

т. е. чтобы перемножить n элементов, надо произведение первых $n-1$ элементов помножить на последний элемент.

Затем, буквально так же, как и в случае сложения, можно вывести, что произведение m сомножителей $a_1a_2\ldots a_m$ не зависит от расположения скобок:

$$(a_1a_2\ldots a_p)\,(a_{p+1}\ldots a_q)\ldots(a_{s+1}\ldots a_m)=a_1a_2\ldots a_pa_{p+1}\ldots a_q\ldots a_{s+1}\ldots a_m.$$

Однако произведение зависит от порядка следования сомножителей; мы не вправе, например, утверждать, что

$$a_1a_2a_3a_4=a_2a_1a_3a_4,$$

так как коммутативный закон для умножения, вообще говоря, не выполняется.

Если в кольце R вычитание возможно, то относительно деления этого сказать нельзя, так как мы нигде не требовали, чтобы уравнения $ax=b$ и $ya=b$ были разрешимы.

Заметим ещё, что произведение m одинаковых сомножителей $aa\ldots a$ принято называть m-й степенью элемента a и обозначать через a^m. Очевидно, что для степеней элементов множества R справедливы обычные алгебраические законы:

$$\left.\begin{aligned} a^n a^m &= a^{n+m}, \\ (a^n)^m &= a^{nm}. \end{aligned}\right\} \tag{16}$$

В самом деле,

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

Но произведение не зависит от того, как расставлены скобки, поэтому две скобки можно объединить в одну, в результате чего получится

$$a^n a^m = (aa\ldots a) = a^{n+m}.$$

Аналогично выводится и второе равенство (16).

Если кольцо R коммутативно, то к равенствам (16) можно присоединить ещё

$$(ab)^n = a^n b^n. \tag{17}$$

Доказывается соотношение (17) очень просто: согласно определению степени и в силу коммутативности умножения

$$(ab)^n = \underbrace{(abab\ldots ab)}_{n \text{ раз}} = \underbrace{(aa\ldots a}_{n \text{ раз}}\ \underbrace{bb\ldots b)}_{n \text{ раз}} = \underbrace{(aa\ldots a)}_{n \text{ раз}}\ \underbrace{(bb\ldots b)}_{n \text{ раз}} = a^n b^n.$$

Замечания относительно распределительного закона. Аксиома е) утверждает, что

$$a(b+c) = ab + ac, \quad (b+c)a = ba + ca.$$

Легко видеть, что не только для двух, но и для n элементов $b_1, \ldots, b_n$:

$$\left.\begin{aligned} a(b_1 + b_2 + \ldots + b_n) &= ab_1 + ab_2 + \ldots + ab_n, \\ (b_1 + b_2 + \ldots + b_n)a &= b_1 a + b_2 a + \ldots + b_n a. \end{aligned}\right\} \tag{18}$$

Действительно, при $n = 3$

$$\begin{aligned} a(b_1 + b_2 + b_3) &= a[(b_1 + b_2) + b_3] = a(b_1 + b_2) + ab_3 = \\ &= ab_1 + ab_2 + ab_3; \\ (b_1 + b_2 + b_3)a &= [(b_1 + b_2) + b_3]a = (b_1 + b_2)a + b_3 a = \\ &= b_1 a + b_2 a + b_3 a. \end{aligned}$$

Общая формула доказывается методом индукции; рекомендуем читателю провести это доказательство самому.

Благодаря распределительному закону многие правила обычной алгебры остаются в силе и для колец. Ведь сам этот закон есть не что иное, как правило умножения многочлена на одночлен.

Из (18) вытекает известное правило умножения одного многочлена на другой многочлен:

$$(a_1+a_2+\ldots+a_n)(b_1+b_2+\ldots+b_m)=a_1b_1+a_1b_2+\ldots+a_1b_m+\\+a_2b_1+a_2b_2+\ldots+a_2b_m+\ldots+a_nb_m.$$

В самом деле, легко видеть, что

$$(a_1+a_2+\ldots+a_n)(b_1+b_2+\ldots+b_m)=\\=(a_1+a_2+\ldots+a_n)b_1+(a_1+a_2+\ldots+a_n)b_2+\ldots+(a_1+a_2+\\+\ldots+a_n)b_m=a_1b_1+a_2b_1+\ldots+a_nb_1+a_1b_2+\ldots+a_nb_2+\\+\ldots+a_1b_m+a_2b_m+\ldots+a_nb_m.$$

Кроме того, распределительный закон справедлив и при вычитании:

$$a(b-c)=ab-ac,\quad (b-c)a=ba-ca. \tag{19}$$

Доказывается это следующим образом. Умножаем очевидное равенство $b-c+c=b$ слева на a и справа на a:

$$a[(b-c)+c]=ab,\quad [(b-c)+c]a=ba.$$

Затем к левым частям последних равенств применяем распределительный закон, в результате чего получается:

$$a(b-c)+ac=ab,\quad (b-c)a+ca=ba.$$

Теперь прибавляя к обеим частям соответственно $-ac$ и $-ca$, придём к соотношениям (19).

Из равенств (19) между прочим вытекает, что произведение двух сомножителей равно нулю, если один из сомножителей равен нулю. В самом деле,

$$a\cdot 0=a(a-a)=a\cdot a-a\cdot a=a^2-a^2=0,$$
$$0\cdot a=(a-a)a=a\cdot a-a\cdot a=a^2-a^2=0.$$

Однако, обратное не всегда верно. Если произведение равно нулю, то, как мы знаем уже из теории матриц, сомножители могут и не равняться нулю:

$$ab=0,\quad a\neq 0,\quad b\neq 0.$$

Такие элементы кольца называются *делителями нуля*.

Наконец, остаются в силе и правила знаков:

$$(-a)b=-ab,\quad a(-b)=-ab,\quad (-a)(-b)=ab.$$

Доказываются эти правила очень просто. Например,

$$(-a)b=(0-a)b=0\cdot b-ab=0-ab=-ab,$$
$$(-a)(-b)=-[a(-b)]=-[-ab]=ab$$

[см. равенство (15)].

Обратимся теперь к конкретным примерам—они помогут нам окончательно усвоить понятие кольца.

Примеры колец. 1. Простейшим примером является совокупность всех целых чисел. Эта совокупность, как легко видеть, образует по отношению к арифметическим операциям сложения и умножения (коммутативное) кольцо, потому что все аксиомы кольца удовлетворяются. В самом деле, сумма и произведение двух целых чисел есть снова целое число; сложение и умножение, очевидно, подчиняются сочетательному и коммутативному законам; для любых двух целых чисел a, b всегда можно подобрать такое целое число x, что $a+x=b$. Наконец, распределительный закон также выполняется.

2. Напротив, множество всех положительных чисел по отношению к сложению и умножению кольца не образуют, так как аксиома d) не имеет места. Так, для чисел 3 и 2 нельзя подобрать такого положительного числа x, чтобы $3+x=2$. Таким образом внутри множества положительных чисел операция вычитания невозможна.

3. Рассмотрим совокупность всех чётных чисел. Она по отношению к сложению и умножению образует кольцо, так как сумма и произведение чётных чисел есть снова чётное число, сумма и произведение чётных чисел подчиняются сочетательному и коммутативному законам, и, наконец, имеет место распределительный закон.

Напротив, совокупность нечётных чисел кольца не образует, так как сумма двух нечётных чисел равна чётному числу, числу, выходящему за пределы нашей совокупности.

4. Во всех примерах, приведённых выше, мы имели дело только с коммутативными кольцами (умножение чисел, как известно, подчиняется коммутативному закону). Но можно привести примеры и некоммутативных колец. Так, множество всех матриц n-го порядка образует по отношению к операциям сложения и умножения кольцо, так как удовлетворяются все пять аксиом, но это кольцо некоммутативно.

Возвращаемся снова к общей теории колец. Мы установили, что для колец сохраняются многие законы обычной алгебры и арифметики. Но алгебраические свойства кольца ещё более усилятся, если мы потребуем, чтобы 1) кольцо R было коммутативным и 2) уравнение $ax=b$ при $a\neq 0$ было всегда разрешимо в R. Введём следующее определение.

Определение 2. *Полем называется такое коммутативное кольцо, в котором существует по меньшей мере один элемент, отличный от нуля, и уравнение $ax=b$ при $a\neq 0$ всегда разрешимо* [1]) (*выполнимость деления*).

Какими же дополнительными свойствами обладает поле? Оказывается, что поле, кроме нуля и противоположных элементов, обладает ещё единицей и обратными элементами.

Пусть $c\neq 0$—некоторый элемент поля. По определению поля всегда можно подобрать такой элемент e, что

$$ce=ec=c. \tag{20}$$

[1]) Можно пойти ещё дальше и назвать полем любое (даже некоммутативное) кольцо, в котором уравнения $ax=b$, $ya=b$ при $a\neq 0$ всегда разрешимы.

Мы утверждаем, что e по отношению к умножению ведёт себя как число 1, т. е. для любого элемента a

$$ae = ea = a.$$

Для доказательства подберём из поля элемент x, удовлетворяющий уравнению:

$$cx = a, \tag{21}$$

и затем умножим обе части этого уравнения на e. Тогда, пользуясь сочетательным и коммутативным законами, получим:

$$(ce)x = ae,$$

или в силу (20) и (21):

$$a = ae.$$

Само собой разумеется, что ea также равно a, так как поле есть коммутативное кольцо.

Легко видеть, что другого «единичного» элемента, кроме e, не существует. В самом деле, пусть e_1 — также «единичный» элемент. Так как e и e_1 ведут себя как единица, то, с одной стороны, $ee_1 = e$, а с другой стороны, $ee_1 = e_1$, откуда видим, что $e = e_1$.

Обозначим это единственное e через 1 и назовём его *единицей*.

Далее, рассмотрим уравнение типа

$$ax = 1 \quad (a \neq 0). \tag{22}$$

Оно имеет единственное решение, в чём легко убедиться следующим образом. Допустим, что уравнение (22) имеет не одно, а два решения: $x = x_1$, $x = x_2$. Тогда

$$ax_1 = 1, \tag{23}$$

$$ax_2 = 1. \tag{24}$$

Умножим обе части равенства (23) на x_2:

$$(ax_1)x_2 = x_2.$$

Но, с другой стороны, в силу (24):

$$(ax_1)x_2 = (ax_2)x_1 = 1 \cdot x_1 = x_1,$$

откуда $x_1 = x_2$.

Единственное решение уравнения (22) принято обозначать через a^{-1} или $\frac{1}{a}$ и называть обратным по отношению к a элементом. Заметим ещё, что $(a^{-1})^{-1} = a$; это следует из того, что решением уравнения $a^{-1}x = 1$ является, очевидно, a:

$$a^{-1}a = aa^{-1} = 1.$$

Переходим теперь к общему случаю:

$$ax = b \quad (a \neq 0).$$

Если обе части умножить на $\frac{1}{a}$, то мы получим единственное решение $x = ba^{-1} = b\frac{1}{a}$, которое обычно записывается в виде дроби

$\frac{b}{a}$. Нетрудно видеть, что действия над символом $\frac{b}{a}$ ничем не отличаются от обычных операций с дробями, а именно:

$\frac{a}{b} = \frac{c}{d}$ тогда и только тогда, когда $ad = bc$ $(b \neq 0,\ d \neq 0)$;

$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$ (правило сложения) $(b \neq 0,\ d \neq 0)$;

$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ (правило умножения) $(b \neq 0,\ d \neq 0)$;

$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}$ (правило деления) $(b \neq 0,\ c \neq 0,\ d \neq 0)$.

Докажем все эти соотношения. Начнём с первого. Помножим обе части равенства $\frac{a}{b} = \frac{c}{d}$ на bd. Получим

$$\left(\frac{a}{b}\, b\right) d = b\left(\frac{c}{d}\, d\right), \quad \text{или} \quad ad = bc.$$

Обратно, пусть $ad = bc$. Умножив обе части этого равенства на $b^{-1}d^{-1}$, получим

$$add^{-1}b^{-1} = cbb^{-1}d^{-1} \quad \text{или} \quad \frac{a}{b} = \frac{c}{d}.$$

Для доказательства правила сложения умножим $\left(\frac{a}{b} \pm \frac{c}{d}\right)$ на bd и воспользуемся распределительным законом:

$$\left(\frac{a}{b} \pm \frac{c}{d}\right) bd = \frac{a}{b}\, bd \pm \frac{c}{d}\, bd,$$

или после очевидных сокращений:

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

Наконец, умножаем обе части последнего равенства на $(bd)^{-1}$; в результате чего будем иметь:

$$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}.$$

Буквально так же доказывается и третье соотношение (правило умножения). А именно:

$$\left(\frac{a}{b} \cdot \frac{c}{d}\right) bd = \frac{a}{b} \cdot b \cdot \frac{c}{d} \cdot d = ac,$$

откуда после умножения обеих частей на $(bd)^{-1}$ имеем

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Остаётся проверить правило деления. Легко видеть, что

$$\frac{1}{\frac{c}{d}} = \frac{d}{c}.$$

Действительно, $\frac{d}{c}$ является обратным элементом по отношению к $\frac{c}{d}$, так как согласно правилу умножения

$$\frac{c}{d} \cdot \frac{d}{c} = \frac{cd}{cd} = 1.$$

Таким образом

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{bc},$$

что и требовалось показать.

Поскольку в поле сохраняются обычные законы арифметики, можно все известные правила действий с целыми степенями вывести буквально так же, как в элементарной алгебре. При этом под степенью a^{-m} (m — целое положительное число) с отрицательным показателем мы подразумеваем $\frac{1}{a^m} = \left(\frac{1}{a}\right)^m$. Что касается степени a^m с положительным показателем, то она была определена выше (см. стр. 106).

В заключение не мешает указать, что в поле выполняется следующий арифметический закон: если произведение двух сомножителей равно нулю, то по крайней мере один из сомножителей равен нулю; иными словами, *поле не имеет делителей нуля.*

Доказывается это очень просто: пусть $a \neq 0$, тогда, умножив обе части равенства $ab = 0$ на $\frac{1}{a}$, получим $b = 0$.

Подведём итог вышеизложенному. Как мы уже убедились, поле обладает не только нулём и противоположными элементами, но и единицей и обратными элементами. Что это по существу означает? Это означает, что 1) поле есть абелева группа по отношению к сложению, 2) все элементы поля, кроме нуля, образуют абелеву группу по отношению к умножению (см. определение группы).

Примеры полей. 1. Простейшим примером поля может служить множество всех рациональных чисел. В самом деле, это множество образует коммутативное кольцо и уравнение $ax = b$, $a \neq 0$ при рациональных a и b всегда разрешимо, потому что частное двух рациональных чисел есть снова рациональное число.

Напротив, множество всех целых чисел образуют только коммутативное кольцо, а не поле, так как в нём уравнение $ax = b$ ($a \neq 0$) не всегда разрешимо, так как не всегда частное двух целых чисел есть также целое число.

2. Другой пример — множество всех действительных (т. е. рациональных и иррациональных) чисел образует поле, так как в нём деление всегда выполнимо.

В нашей книге мы будем иметь дело главным образом с числовыми полями, т. е. с такими множествами чисел которые образуют поле по отношению к арифметическим действиям.

В современной математике представление о числе является настолько широким, что трудно указать границы этого понятия. Употребляя в дальнейшем слово «число», мы будем иметь в виду не только числа рациональные, действительные и комплексные, с которыми читатель встречался ещё в средней школе, но и более широкую область чисел, о которых речь будет впереди (в § 42).

3. Множество всех диагональных матриц вида

$$\begin{Vmatrix} a & 0 \\ 0 & a \end{Vmatrix} = (a)\ ^{1}) \quad (a - \text{действительное число})$$

второго порядка образует поле.

Рассмотрим подробнее множество диагональных матриц (a). Покажем сначала, что они образуют кольцо.

Легко видеть, что сумма и произведение двух диагональных матриц есть снова диагональная матрица:

$$\begin{Vmatrix} a & 0 \\ 0 & a \end{Vmatrix} + \begin{Vmatrix} b & 0 \\ 0 & b \end{Vmatrix} = \begin{Vmatrix} a+b & 0 \\ 0 & a+b \end{Vmatrix}, \text{ или сокращённо: } (a)+(b)=(a+b)$$

$$\begin{Vmatrix} a & 0 \\ 0 & a \end{Vmatrix} \cdot \begin{Vmatrix} b & 0 \\ 0 & b \end{Vmatrix} = \begin{Vmatrix} ab & 0 \\ 0 & ab \end{Vmatrix}, \text{ или сокращённо: } (a)\cdot(b)=(ab).$$

Таким образом мы не только проверили аксиому a) о замкнутости множества, но и увидели, что сложение и умножение диагональных матриц ничем не отличаются от сложения и умножения чисел.

Разумеется, сложение и умножение диагональных матриц подчиняются коммутативному и сочетательному законам, так как этим же законам подчиняются сложение и умножение чисел.

Столь же просто проверяется аксиома d) о разрешимости уравнения $(a)+x=(b)$. Сразу видно, что решением этого уравнения является диагональная матрица $x=(b-a)$.

Распределительный закон в проверке не нуждается, так как мы знаем, что для матриц он верен (см. стр. 100).

Итак, все пять аксиом, характеризующих кольцо, выполняются, следовательно, наши диагональные матрицы образуют кольцо и притом коммутативное кольцо.

Покажем теперь, что мы имеем дело с полем. Возьмём уравнение

$$(a)\cdot x=(b), \quad (a)\neq 0 \quad [\text{т. е. } a\neq 0]$$

---

[1]) Символ (a) есть просто сокращённое обозначение рассматриваемой матрицы.

найдём его решение. Убедимся, что $x=\left(\frac{b}{a}\right)$. В самом деле, правилу перемножения диагональных матриц:

$$\begin{Vmatrix} a & 0 \\ 0 & a \end{Vmatrix} \cdot \begin{Vmatrix} \frac{b}{a} & 0 \\ 0 & \frac{b}{a} \end{Vmatrix} = \begin{Vmatrix} a\frac{b}{a} & 0 \\ 0 & a\frac{b}{a} \end{Vmatrix} = \begin{Vmatrix} b & 0 \\ 0 & b \end{Vmatrix}.$$

Мы видим, что матрицы (a), (b) складываются, вычитаются, множаются и делятся совершенно так же, как действительные исла a и b, несмотря на то, что по содержанию они отличаются от ействительных чисел. Если отвлечься от содержания, которое мы кладываем в понятие числа и в понятие матрицы, и ограничиться лько рассмотрением операций над ними, то поле диагональных атриц и поле действительных чисел можно считать тождественными ежду собой. Мы подходим здесь к важному понятию изомор-изма.

Прежде чем перейти к строгому определению изоморфизма, ведём понятие взаимно однозначного соответствия, которое хотя относится к области теории множеств; но тем не менее является новным для всех отделов математики.

Пусть M и N два конечных или бесконечных множества. Предположим, что каждому элементу множества M приведён в соответствие один элемент множества N, и наоборот. Тогда мы будем говорить, что элементы множеств M и N связаны *взаимно однозначным* соответствием, или что между множествами M и N установлено взаимно днозначное соответствие.

С понятием взаимно однозначного соответствия приходится гречаться уже при счёте предметов, когда каждому предмету иводится в соответствие натуральное число. Рассмотрим ещё та-й пример соответствия между бесконечными множествами. Возьм два бесконечных множества: множество натуральных чисел

$$1, 2, 3, \ldots$$

множество чётных чисел

$$2, 4, 6, \ldots$$

Между этими множествами легко установить взаимно одно-чное соответствие. А именно, умножая каждое натуральное исло на два, получаем соответствующее ему чётное число.

Теперь перейдём к определению изоморфизма.

Два кольца (в частности, два поля), которые ведут себя одинаково отношению к операциям сложения и умножения, принято назы-ть *изоморфными*. Точнее: *кольца R и $\overline{R}$ называются изоморфными, ли их элементы приведены во взаимно однозначное соответствие ким образом, что если элементам a и b кольца R отвечают элементы и $\overline{b}$ кольца $\overline{R}$, то* 1) сумме $a+b$ *элементов* a, b *кольца* R *отвечает*

сумма $\bar{a}+\bar{b}$ *элементов* $\bar{a}$, $\bar{b}$ *кольца* R; 2) *произведению* ab *элементов* a, b *кольца* R *отвечает произведение* $\bar{a}\,\bar{b}$ *элементов* $\bar{a}$, $\bar{b}$ *кольца* $\bar{R}$ [1]).

Отметим несколько важнейших свойств изоморфных колец.

Легко убедиться, что *нулю* 0 *кольца* R *взаимно однозначно соответствует нуль* 0 *изоморфного кольца* $\bar{R}$. Действительно, обозначим через a произвольный элемент кольца R, а через $\bar{a}$—соответственный элемент из $\bar{R}$. Пусть нулю 0 кольца R соответствует в $\bar{R}$ элемент $\bar{x}$. Тогда в силу изоморфизма равенству $a+0=a$ будет в кольце $\bar{R}$ отвечать равенство $\bar{a}+\bar{x}=\bar{a}$. Мы видим, что элемент $\bar{a}$ от прибавления $\bar{x}$ не меняется; значит, $\bar{x}$ представляет собой нуль кольца $\bar{R}$: $\bar{x}=0$.

Подобным же образом можно показать, что *противоположному элементу—*a *кольца* R *взаимно однозначно соответствует противоположный элемент* $-\bar{a}$ изоморфного кольца $\bar{R}$.

Наконец, *если одно кольцо, например* R, *образует поле, то изоморфное ему кольцо* $\bar{R}$ *также должно быть полем*. Для доказательства обозначим через a, b два каких-нибудь элемента поля R и через $\bar{a}$, $\bar{b}$ — соответственные элементы кольца $\bar{R}$. Из определения изоморфизма следует, что равенству $ab=ba$ должно соответствовать равенство $\bar{a}\,\bar{b}=\bar{b}\,\bar{a}$. Мы видим отсюда, что $\bar{R}$ — кольцо коммутативное. Далее, уравнение $ax=b$, $a\neq 0$ разрешимо в поле R; следовательно, в силу того же изоморфизма в $\bar{R}$ будет разрешимо и соответствующее уравнение $\bar{a}x=\bar{b}$. Таким образом $\bar{R}$ есть поле.

Понятие изоморфизма является характерной для алгебры формой эквивалентности, какой для арифметики является понятие равенства чисел, для теории множеств понятие взаимно однозначного соответствия, для проективной геометрии понятие перспективного соответствия. С точки зрения алгебры изоморфные кольца или поля одинаковы. Например, выше мы обнаружили изоморфизм поля диагональных матриц $\begin{Vmatrix} a & 0 \\ 0 & a \end{Vmatrix}$ с полем действительных чисел. С точки зрения современной алгебры было бы законно не делать между ними различия. Это и понятно—ведь современная алгебра занимается изучением природы алгебраических операций, а не изучением природы элементов кольца или поля. А с точки зрения свойств операций изоморфные кольца или поля одинаковы.

Такой взгляд придаёт алгебре ту же общность, какую современной геометрии придаёт аксиоматическая точка зрения Гильберта, позволяющая распространить её выводы на объекты любой природы, лишь бы они удовлетворяли её аксиомам.

В заключение этого параграфа рассмотрим ещё один пример по...

---

[1]) Аналогичным образом вводится понятие изоморфизма групп. Две группы $\mathfrak{G}$ и $\bar{\mathfrak{G}}$ называются изоморфными, если 1) каждому элементу a группы $\mathfrak{G}$ взаимно однозначно соответствует элемент $\bar{a}$ группы $\bar{\mathfrak{G}}$, 2) произведению ab элементов группы $\mathfrak{G}$ взаимно однозначно соответствует произведение $\bar{a}\,\bar{b}$ соответственных элементов $\bar{a}$, $\bar{b}$ группы $\bar{\mathfrak{G}}$.

4. Возьмём матрицы более общего типа

$$\begin{Vmatrix} a & b \\ b' & a \end{Vmatrix} \quad (a,\ b,\ b' - \text{действительные числа}) \tag{25}$$

и найдём, каким ограничениям должны удовлетворять элементы b и b', чтобы множество этих матриц было полем, содержащим как часть поле диагональных матриц вида $\begin{Vmatrix} a & 0 \\ 0 & a \end{Vmatrix}$.

Пусть матрицы (25) образуют поле M. Если $b \neq 0$ [1]), то вместе с $\begin{Vmatrix} a & b \\ b' & a \end{Vmatrix}$, $\begin{Vmatrix} a & 0 \\ 0 & a \end{Vmatrix}$ и $\begin{Vmatrix} \frac{1}{b} & 0 \\ 0 & \frac{1}{b} \end{Vmatrix}$ в поле M будет содержаться разность

$$\begin{Vmatrix} a & b \\ b' & a \end{Vmatrix} - \begin{Vmatrix} a & 0 \\ 0 & a \end{Vmatrix} = \begin{Vmatrix} 0 & b \\ b' & 0 \end{Vmatrix}$$

и произведение

$$\begin{Vmatrix} \frac{1}{b} & 0 \\ 0 & \frac{1}{b} \end{Vmatrix} \cdot \begin{Vmatrix} 0 & b \\ b' & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & 1 \\ \frac{b'}{b} & 0 \end{Vmatrix}.$$

Точно так же для другой матрицы $\begin{Vmatrix} a_1 & b_1 \\ b_1' & a_1 \end{Vmatrix}$ $(b_1 \neq 0)$ будем иметь матрицу $\begin{Vmatrix} 0 & 1 \\ \frac{b_1'}{b_1} & 0 \end{Vmatrix}$, содержащуюся в M. Таким образом равность

$$\begin{Vmatrix} 0 & 1 \\ \frac{b'}{b} & 0 \end{Vmatrix} - \begin{Vmatrix} 0 & 1 \\ \frac{b_1'}{b_1} & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & 0 \\ \frac{b'}{b} - \frac{b_1'}{b_1} & 0 \end{Vmatrix} \tag{26}$$

опять-таки должна содержаться в поле M. Мы утверждаем, что

$$\frac{b'}{b} - \frac{b_1'}{b_1} = 0.$$

В самом деле, если

$$\frac{b'}{b} - \frac{b_1'}{b_1} \neq 0,$$

---

[1]) Необходимо отметить, что если $b \neq 0$, то и $b' \neq 0$. Действительно, если бы было $b \neq 0$ и $b' = 0$, то матрица $\begin{Vmatrix} 0 & b \\ 0 & 0 \end{Vmatrix}$ была бы делителем нуля, так как, например, её квадрат был бы равен нулю.

то матрица (26) будет делителем нуля, так как её квадрат равен нулю. Но это невозможно, так как поле не имеет делителей нуля.

Итак,

$$\frac{b'}{b}-\frac{b_1'}{b_1}=0$$

или

$$\frac{b'}{b}=\frac{b_1'}{b_1}=c,$$

где c — постоянное число, не зависящее от b и b'. Покажем теперь, что $c<0$. Предположим противное: пусть $c>0$. Тогда $\sqrt{c}$ является действительным числом, и мы можем составить диагональную матрицу

$$\begin{Vmatrix}\sqrt{c} & 0\\ 0 & \sqrt{c}\end{Vmatrix}.$$

Отсюда ясно, что сумма и разность матриц

$$\begin{Vmatrix}\sqrt{c} & 0\\ 0 & \sqrt{c}\end{Vmatrix} \quad \text{и} \quad \begin{Vmatrix}0 & 1\\ c & 0\end{Vmatrix}$$

также принадлежат полю M. Но

$$\begin{Vmatrix}\sqrt{c} & 0\\ 0 & \sqrt{c}\end{Vmatrix}+\begin{Vmatrix}0 & 1\\ c & 0\end{Vmatrix}=\begin{Vmatrix}\sqrt{c} & 1\\ c & \sqrt{c}\end{Vmatrix},\quad \begin{Vmatrix}\sqrt{c} & 0\\ 0 & \sqrt{c}\end{Vmatrix}-\begin{Vmatrix}0 & 1\\ c & 0\end{Vmatrix}=\begin{Vmatrix}\sqrt{c} & -1\\ -c & \sqrt{c}\end{Vmatrix}$$

и легко видеть, что полученные матрицы являются делителями нуля:

$$\begin{Vmatrix}\sqrt{c} & 1\\ c & \sqrt{c}\end{Vmatrix}\cdot\begin{Vmatrix}\sqrt{c} & -1\\ -c & \sqrt{c}\end{Vmatrix}=\begin{Vmatrix}c-c & -\sqrt{c}+\sqrt{c}\\ c\sqrt{c}-c\sqrt{c} & -c+c\end{Vmatrix}=\begin{Vmatrix}0 & 0\\ 0 & 0\end{Vmatrix}=0,$$

а это невозможно.

Итак, c должно быть отрицательным. Полагая $c=-k$, где $k>0$, приходим к окончательному решению задачи: матрицы (25) должны иметь вид

$$\begin{Vmatrix}a & b\\ -kb & a\end{Vmatrix}.$$

Пусть, в частности, $k=1$. Множество матриц вида

$$\begin{Vmatrix}a & b\\ -b & a\end{Vmatrix}=(a,\ b)\ ^{1})\quad (a,\ b-\text{действительные числа})$$

образуют поле, содержащее как часть поле диагональных матриц.

---

[1]) Символ $(a,\ b)$ введём для сокращённого обозначения рассматриваемых матриц.

Выведем, по какому правилу складываются и умножаются матрицы $(a,\ b)$. Без особого труда находим, что

$$\begin{Vmatrix} a & b \\ -b & a \end{Vmatrix} + \begin{Vmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{Vmatrix} = \begin{Vmatrix} a+a_1 & b+b_1 \\ -(b+b_1) & a+a_1 \end{Vmatrix},$$

$$\begin{Vmatrix} a & b \\ -b & a \end{Vmatrix} \cdot \begin{Vmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{Vmatrix} = \begin{Vmatrix} aa_1-bb_1 & ab_1+a_1b \\ -(ab_1+a_1b) & aa_1-bb_1 \end{Vmatrix},$$

или в сокращённой записи:

$$(a,\ b)+(a_1,\ b_1)=(a+a_1,\ b+b_1),$$
$$(a,\ b)\cdot(a_1,\ b_1)=(aa_1-bb_1,\ ab_1+a_1b).$$

Если диагональные матрицы (a) можно отождествить с действительными числами, то весьма вероятно, что матрицам $(a,\ b)$ соответствуют числа новой природы. Мы в дальнейшем увидим, что ими будут комплексные числа.

Задачи. 1. Исследовать, образуют ли кольцо следующие множества: а) множество всех иррациональностей вида $a+b\sqrt{5}$, где a и b—целые числа, b) множество всех правильных дробей, c) множество всех целых чисел, кратных 3.

2. Исследовать, образуют ли поле следующие множества:

а) множество всех иррациональностей $a+b\sqrt{5}$, где a и b—рациональные числа, b) множество всех дробей $\frac{a}{b}$ $(a,\ b$—целые числа), у которых знаменатель делится на 5, c) множество всех диагональных матриц n-го порядка, имеющих вид:

$$\begin{Vmatrix} a_1 & 0 & 0 \dots 0 \\ 0 & a_2 & 0 \dots 0 \\ \cdot & \cdot & \cdot \ \cdot \ \cdot \\ 0 & 0 & 0 \dots a_n \end{Vmatrix},$$

где a_i — действительные числа.

ГЛАВА ЧЕТВЁРТАЯ

КВАДРАТИЧНЫЕ ФОРМЫ

§ 23. Квадратичные формы и приведение их к каноническому виду

Теория квадратичных форм тесно связана с задачей приведения уравнений кривых и поверхностей второго порядка к каноническому виду; поэтому вполне естественно начать с рассмотрения некоторых соотношений из аналитической геометрии.

Как известно, общее уравнение кривой второго порядка имеет следующий вид:

$$f(x,\ y)=a_{11}x^2+2a_{12}xy+a_{22}y^2+2a_{13}x+2a_{23}y+a_{33}=0. \qquad (1)$$

Если ввести однородные координаты

$$x=\frac{x_1}{x_3},\quad y=\frac{x_2}{x_3},$$

то уравнение этой кривой примет ещё более симметричный вид, а именно:

$$\varphi(x_1, x_2, x_3)=a_{11}x_1^2+2a_{12}x_1x_2+a_{22}x_2^2+2a_{13}x_1x_3+\\+2a_{23}x_2x_3+a_{33}x_3^2=0.$$

Мы получили в левой части уравнения однородный многочлен второй степени от трёх переменных, однородный, так как каждый член имеет одну и ту же степень, в данном случае вторую. Такой многочлен называется *квадратичной формой*.

Пусть (1) есть уравнение центральной кривой второго порядка; если уравнение (1) привести к каноническому виду, то в квадратичной форме $\varphi(x_1, x_2, x_3)$ исчезнут все члены с произведениями x_1x_2, x_1x_3, x_2x_3 и останутся только члены с квадратами переменных. Иными словами, квадратичная форма будет выглядеть так:

$$\varphi(x'_1, x'_2, x'_3)=c_1x_1'^2+c_2x_2'^2+c_3x_3'^2, \tag{2}$$

причём некоторые из коэффициентов могут оказаться равными нулю. Мы будем называть квадратичную форму, состоящую только из членов с квадратами переменных, *канонической*.

Дадим теперь задаче приведения уравнения кривой к каноническому виду алгебраическое истолкование.

Приведение уравнения к каноническому виду достигается с помощью преобразования системы координат. Запишем это преобразование алгебраически:

$$\left.\begin{aligned}x_1&=b_{11}x'_1+b_{12}x'_2+b_{13}x'_3,\\x_2&=b_{21}x'_1+b_{22}x'_2+b_{23}x'_3,\\x_3&=b_{31}x'_1+b_{32}x'_2+b_{33}x'_3,\\\Delta&=\begin{vmatrix}b_{11}&b_{12}&b_{13}\\b_{21}&b_{22}&b_{23}\\b_{31}&b_{32}&b_{33}\end{vmatrix}\neq 0,\end{aligned}\right\} \tag{3}$$

т. е. мы имеем просто невырождающееся линейное преобразование трёх переменных.

Итак, мы приходим к следующей алгебраической задаче: с помощью линейного невырождающегося преобразования (3) привести квадратичную форму

$$\varphi(x_1, x_2, x_3)=a_{11}x^2+2a_{12}x_1x_2+a_{22}x_2^2+2a_{13}x_1x_3+2a_{23}x_2x_3+a_{33}x_3^2$$

к каноническому виду (2).

Однако эту задачу можно обобщить на случай не только трёх, но и любого члена переменных. Назовём многочлен

$$\varphi(x_1, x_2, \ldots, x_n)=a_{11}x_1^2+2a_{12}x_1x_2+2a_{13}x_1x_3+\ldots+\\+2a_{1n}x_1x_n+\ldots+a_{nn}x_n^2 \tag{4}$$

квадратичной формой n переменных $x_1, x_2, \ldots, x_n$. Коэффициенты при x_i^2 мы всегда будем обозначать через a_{ii}, а коэффициенты при $x_i x_j$ через $2a_{ij}$ $(i \neq j)$.

В этой главе мы будем всюду, если не оговорено противное, считать, что коэффициенты a_{ij} и значения переменных x_k квадратичных форм принадлежат полю действительных чисел.

Можно ли такую форму привести к каноническому виду

$$\varphi(x_1', x_2', \ldots, x_n') = c_1 x_1'^2 + c_2 x_2'^2 + \ldots + c_n x_n'^2 \text{ [1]}$$

с помощью некоторого линейного невырождающегося преобразования

$$x_i = b_{i1}x_1' + b_{i2}x_2' + \ldots + b_{in}x_n' \quad (i = 1, 2, \ldots, n),$$

$$\Delta = \begin{vmatrix} b_{11} & \ldots & b_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ b_{n1} & \ldots & b_{nn} \end{vmatrix} \neq 0?$$

Мы покажем, что даже и в столь общей постановке задача имеет решение.

Форму (4) удобнее представить в несколько ином, более симметричном виде. Условимся считать $a_{ij} = a_{ji}$. Тогда $\varphi(x_1, x_2, \ldots, x_n)$ запишется следующим образом:

$$\begin{aligned} \varphi(x_1, x_2, \ldots, x_n) = {} & a_{11}x_1^2 + a_{12}x_1x_2 + \ldots + a_{1n}x_1x_n + \\ & + a_{21}x_2x_1 + a_{22}x_2^2 + \ldots + a_{2n}x_2x_n + \\ & + \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot + \\ & + a_{n1}x_nx_1 + a_{n2}x_nx_2 + \ldots + a_{nn}x_n^2 \end{aligned} \tag{5}$$

(так называемая симметричная запись).

Пример. Записать в симметричном виде квадратичную форму

$$\varphi(x_1, x_2, x_3, x_4) = 5x_1^2 - 3x_1x_2 + 5x_2x_3 + x_3x_4 - 2x_4^2.$$

Имеем:

$$\begin{aligned} \varphi(x_1, x_2, x_3, x_4) = {} & 5x_1^2 - \tfrac{3}{2}x_1x_2 + 0 \cdot x_1x_3 + 0 \cdot x_1x_4 - \\ & - \tfrac{3}{2}x_2x_1 + 0 \cdot x_2^2 + \tfrac{5}{2}x_2x_3 + 0 \cdot x_2x_4 + \\ & + 0 \cdot x_3x_1 + \tfrac{5}{2}x_3x_2 + 0 \cdot x_3^2 + \tfrac{1}{2}x_3x_4 + \\ & + 0 \cdot x_4x_1 + 0 \cdot x_4x_2 + \tfrac{1}{2}x_4x_3 - 2x_4^2. \end{aligned}$$

Для приведения квадратичной формы к каноническому виду воспользуемся одним простым методом, известным ещё Лагранжу.

[1] Некоторые коэффициенты c_i могут оказаться равными нулю.

Будем различать два случая: 1) форма φ не содержит членов с квадратами переменных, т. е. все коэффициенты $a_{ii}=0\,(i=1,2,\ldots,n)$, 2) форма φ содержит по меньшей мере один член с квадратом переменного, т. е. не все a_{ii} равны нулю.

Однако первый случай без особого труда приводится ко второму. А именно, если все $a_{ii}=0$, но имеется хотя бы одно $a_{ij}\neq 0$, то мы подвергаем переменные невырождающемуся преобразованию

$$\left.\begin{aligned} x_1&=x_1',\\ x_2&=x_2',\\ &\ldots\ldots\\ x_i&=x_i'-x_j',\\ &\ldots\ldots\\ x_j&=x_i'+x_j',\\ &\ldots\ldots\\ x_n&=x_n'. \end{aligned}\right\} \tag{6}$$

Легко видеть, что это преобразование невырождающееся, так как его определитель равен 2. Член $a_{ij}x_ix_j$ после преобразования, очевидно, превратится в

$$a_{ij}(x_i'-x_j')(x_i'+x_j')=a_{ij}x_i'^2-a_{ij}x_j'^2,$$

т. е. появятся члены с квадратами переменных. Таким образом можно ограничиться рассмотрением только случая 2).

Итак, пусть некоторое $a_{ii}\neq 0$. Мы сейчас покажем, что в форме φ можно уничтожить все члены, содержащие x_i.

Обратим внимание на i-ю строчку симметричной записи (5):

$$a_{i1}x_ix_1+a_{i2}x_ix_2+\ldots+a_{in}x_ix_n.$$

Если общий множитель x_i вынести за скобку, то в скобке останется линейная форма

$$f=a_{i1}x_1+a_{i2}x_2+\ldots+a_{in}x_n.$$

Вычтем затем из φ выражение $\frac{1}{a_{ii}}f^2$. Легко видеть, что

$$\varphi=2a_{i1}x_ix_1+2a_{i2}x_ix_2+\ldots+a_{ii}x_i^2+\ldots+2a_{in}x_ix_n+G,$$
$$\frac{1}{a_{ii}}f^2=2a_{i1}x_ix_1+2a_{i2}x_ix_2+\ldots+a_{ii}x_i^2+\ldots+2a_{in}x_ix_n+H.$$

Через G мы обозначили сумму членов φ, не содержащих x_i; точно так же H есть сумма членов $\frac{1}{a_{ii}}f^2$, не содержащих x_i.

Отсюда без труда обнаруживаем, что

$$\varphi(x_1,\ldots,x_n)-\frac{1}{a_{ii}}f^2=G-H=\varphi'(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n), \tag{7}$$

члены с x_i уничтожились.

А теперь подвергнем переменные $x_1, x_2, \ldots, x_n$ следующему невырождающемуся преобразованию:

$$\begin{aligned}
y_1 &= a_i x_1 + a_{i2} x_2 + \ldots + a_{ii} x_i + \ldots + a_{in} x_n,\\
y_2 &= \qquad\quad x_2\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
y_i &= x_1\ ^{1}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
y_n &= \qquad\qquad\qquad\qquad x_n.
\end{aligned}$$

Тогда равенство (7) примет более простой вид, а именно:

$$\varphi(x_1, \ldots, x_n) - \frac{1}{a_{ii}} y_1^2 = \varphi_1(y_2, y_3, \ldots, y_n)$$

или, перенося $\frac{1}{a_{ii}} y_1^2$ в правую часть и обозначив $\frac{1}{a_{ii}}$ через c_1:

$$\varphi(x_1, \ldots, x_n) = c_1 y_1^2 + \varphi_1(y_2, y_3, \ldots, y_n).$$

К новой форме φ_1 можно применить тот же метод уничтожения переменных. Пусть в φ_1 коэффициент $a'_{jj} \neq 0$ и j-я строчка симметричной записи формы φ_1 имеет вид:

$$a'_{j2} y_j y_2 + a'_{j3} y_j y_3 + \ldots + a'_{jn} y_j y_n.$$

Вынося общий множитель y_j за скобку, получим в скобке линейную форму

$$f_1 = a'_{j2} y_2 + \ldots + a'_{jj} y_j + \ldots + a'_{jn} y_n$$

и без особого труда уничтожаем y_j, составляя разность

$$\varphi_1(y_2, \ldots, y_n) - \frac{1}{a'_{jj}} f_1^2 = \varphi'_1(y_2, \ldots, y_{j-1}, y_{j+1}, \ldots, y_n).$$

Таким образом форма φ превращается в

$$\varphi(x_1, \ldots, x_n) = c_1 y_1^2 + \frac{1}{a'_{jj}} f_1^2 + \varphi_2(y_2, \ldots, y_{j-1}, y_{j+1}, \ldots, y_n).$$

Подвергнем переменные $y_1, y_2, \ldots, y_n$ невырождающемуся преобразованию

$$\begin{aligned}
z_1 &= y_1,\\
z_2 &= f_1 = a'_{j2} y_2 + \ldots + a'_{jn} y_n,\\
z_3 &= \qquad y_3,\\
&\ldots\ldots\ldots\ldots\\
z_j &= y_2\ ^{2}),\\
&\ldots\ldots\ldots\ldots\\
z_n &= \qquad\qquad y_n.
\end{aligned}$$

---

[1]) Если $i = 1$, то эта строчка пропадает.
[2]) При $j = 2$ эта строчка пропадает.

Получим, если a'_{jj} предварительно обозначим через c_2:

$$\varphi(x_1, \ldots, x_n) = c_1 z_1^2 + c_2 z_2^2 + \varphi_2(z_3, z_4, \ldots, z_n).$$

Пусть в новой форме φ_2 имеется коэффициент $a''_{kk} \neq 0$. Тогда мы можем уничтожить z_k, составив разность:

$$\varphi_2(z_3, \ldots, z_n) - \frac{1}{a''_{kk}} f_2^2 = \varphi'_2(z_3, \ldots, z_{k-1}, z_{k+1}, \ldots, z_n)$$

и т. д.

Действуя так, мы в конечном счёте придём к

$$\varphi(x_1, \ldots, x_n) = c_1 v_1^2 + c_2 v_2^2 + \ldots + c_m v_m^2 \quad (m \leqslant n \quad \text{и все} \quad c_j \neq 0).$$

Итак, с помощью последовательных невырождающихся преобразований форму φ удалось привести к каноническому виду. Эти преобразования могут быть, очевидно, заменены одним.

Разберём конкретный пример. Он поможет окончательно усвоить метод Лагранжа.

Пример. Приведём форму

$$\varphi = x_1 x_3 - 5x_2 x_3 + x_2 x_4$$

к каноническому виду. Она не содержит квадратов; поэтому необходимо предварительно совершить преобразование:

$$x_1 = x'_1 - x'_3, \quad x_2 = x'_2, \quad x_3 = x'_1 + x'_3, \quad x_4 = x'_4$$

или

$$\left.\begin{aligned} x'_1 &= \frac{1}{2} x_1 + \frac{1}{2} x_3, \quad x'_2 = x_2, \\ x'_3 &= -\frac{1}{2} x_1 + \frac{1}{2} x_3, \quad x'_4 = x_4. \end{aligned}\right\} \qquad (A)$$

Получаем

$$\varphi = x_1'^2 - x_3'^2 - 5x'_1 x'_2 - 5x'_2 x'_3 + x'_2 x'_4,$$

или в симметричной записи

$$\begin{aligned} \varphi = x_1'^2 &- \frac{5}{2} x'_1 x'_2 + 0 \cdot x'_1 x'_3 + 0 \cdot x'_1 x'_4 - \\ &- \frac{5}{2} x'_2 x'_1 + 0 \cdot x_2'^2 - \frac{5}{2} x'_2 x'_3 + \frac{1}{2} x'_2 x'_4 + \\ &+ 0 \cdot x'_3 x'_1 - \frac{5}{2} x'_3 x'_2 - x_3'^2 + 0 \cdot x'_3 x'_4 + \\ &+ 0 \cdot x'_4 x'_1 + \frac{1}{2} x'_4 x'_2 + 0 \cdot x'_4 x'_3 + 0 \cdot x_4'^2. \end{aligned}$$

Так как $a_{11} = 1 \neq 0$, то мы можем уничтожить все члены с x'_1. Для этой цели надо составить разность $\varphi - \frac{1}{a_{11}} f^2$. Имеем:

$$f = x'_1 - \frac{5}{2} x'_2,$$

откуда

$$\varphi - \left(x_1' - \frac{5}{2}x_2'\right)^2 = (x_1'^2 - x_2'^2 - 5x_1'x_2' - 5x_2'x_3' + x_3'x_4') - \left(x_1'^2 - 5x_1'x_2' + \frac{25}{4}x_2'^2\right) = -\frac{25}{4}x_2'^2 - x_3'^2 - 5x_2'x_3' + x_3'x_4'.$$

Теперь произведём преобразование

$$\left.\begin{aligned} y_1 &= x_1' - \frac{5}{2}x_2', \\ y_2 &= x_2', \\ y_3 &= x_3', \\ y_4 &= x_4', \end{aligned}\right\} \qquad (B)$$

в результате чего форма φ примет вид

$$\varphi = y_1^2 + \varphi_1,$$

где

$$\varphi_1 = -\frac{25}{4}y_2^2 - y_3^2 - 5y_2y_3 + y_2y_4.$$

В новой форме φ_1 можно уничтожить члены с y_2. Записываем φ_1 симметрично:

$$\varphi_1 = -\frac{25}{4}y_2^2 - \frac{5}{2}y_2y_3 + \frac{1}{2}y_2y_4 - \frac{5}{2}y_3y_2 - y_3^2 + 0\cdot y_3y_4 + \frac{1}{2}y_4y_2 + 0\cdot y_4y_3 + 0\cdot y_4^2,$$

откуда ясно, что

$$f_1 = -\frac{25}{4}y_2 - \frac{5}{2}y_3 + \frac{1}{2}y_4.$$

Следовательно, принимая во внимание, что $a_{22}' = -\frac{25}{4}$, получим:

$$\varphi_1 - \left[\frac{1}{-\frac{25}{4}}\left(-\frac{25}{4}y_2 - \frac{5}{2}y_3 + \frac{1}{2}y_4\right)^2\right] = -\frac{2}{5}y_3y_4 + \frac{1}{25}y_4^2,$$

а отсюда имеем:

$$\varphi = y_1^2 - \frac{4}{25}\left(-\frac{25}{4}y_2 - \frac{5}{2}y_3 + \frac{1}{2}y_4\right)^2 + \varphi_1',$$

где

$$\varphi_1' = -\frac{2}{5}y_3y_4 + \frac{1}{25}y^2.$$

Производим следующее невырождающееся преобразование:

$$\left.\begin{aligned} z_1 &= y_1, \\ z_2 &= -\frac{25}{4}y_2 - \frac{5}{2}y_3 + \frac{1}{2}y_4, \\ z_3 &= y_3, \\ z_4 &= y_4. \end{aligned}\right\} \qquad (C)$$

Тогда φ примет следующий вид:

$$\varphi = z_1^2 - \frac{4}{25}z_2^2 + \varphi_2(z_3, z_4),$$

причём

$$\varphi_2(z_3, z_4) = -\frac{2}{5}z_3z_4 + \frac{1}{25}z_4^2 = \left\{\begin{aligned} &0 \cdot z_3^2 - \frac{1}{5}z_3z_4 - \\ &-\frac{1}{5}z_4z_3 + \frac{1}{25}z_4^2. \end{aligned}\right.$$

Так как $a''_{44} = \frac{1}{25} \neq 0$, то мы можем в форме φ_2 уничтожить члены с z_4. Действуем по известному рецепту:

$$\varphi_2 - \frac{1}{\frac{1}{25}}\left[-\frac{1}{5}z_3 + \frac{1}{25}z_4\right]^2 = -z_3^2,$$

откуда

$$\varphi = z_1^2 - \frac{4}{25}z_2^2 + 25\left(-\frac{1}{5}z_3 + \frac{1}{25}z_4\right)^2 - z_3^2.$$

Если, наконец, переменные z_1, z_2, z_3, z_4 подвергнуть преобразованию

$$\left.\begin{aligned} u_1 &= z_1, \\ u_2 &= z_2, \\ u_3 &= -\frac{1}{5}z_3 + \frac{1}{25}z_4, \\ u_4 &= z_3, \end{aligned}\right\} \qquad (D)$$

то форма φ приведётся к каноническому виду:

$$\varphi = u_1^2 - \frac{4}{25}u_2^2 + 25u_3^2 - u_4^2.$$

Остаётся только найти преобразование, заменяющее все преобразования (A), (B), (C), (D). Выпишем их матрицы:

$$A = \begin{Vmatrix} \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 1 & 0 & 0 \\ -\frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \end{Vmatrix}; \qquad B = \begin{Vmatrix} 1 & -\frac{5}{2} & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{Vmatrix};$$

$$C = \begin{Vmatrix} 1 & 0 & 0 & 0 \\ 0 & -\frac{25}{4} & -\frac{5}{2} & \frac{1}{2} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{Vmatrix}; \qquad D = \begin{Vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -\frac{1}{5} & \frac{1}{25} \\ 0 & 0 & 1 & 0 \end{Vmatrix}.$$

Произведение $DCBA$ этих матриц и будет матрицей искомого преобразования. Пользуясь правилом перемножения матриц, нетрудно найти, что

$$DCBA=\begin{Vmatrix} \frac{1}{2} & -\frac{5}{2} & \frac{1}{2} & 0 \\ \frac{5}{4} & -\frac{25}{4} & -\frac{5}{4} & \frac{1}{2} \\ \frac{1}{10} & 0 & -\frac{1}{10} & \frac{1}{25} \\ -\frac{1}{2} & 0 & \frac{1}{2} & 0 \end{Vmatrix},$$

откуда

$$\left.\begin{aligned} u_1 &= \frac{1}{2}x_1-\frac{5}{2}x_2+\frac{1}{2}x_3, \\ u_2 &= \frac{5}{4}x_1-\frac{25}{4}x_2-\frac{5}{4}x_3+\frac{1}{2}x_4, \\ u_3 &= \frac{1}{10}x_1-\frac{1}{10}x_3+\frac{1}{25}x_4, \\ u_4 &= -\frac{1}{2}x_1+\frac{1}{2}x_3 \end{aligned}\right\} \qquad (DCBA)$$

и будет искомым преобразованием, переводящим заданную форму в каноническую.

Впрочем, преобразование $(DCBA)$ можно определить ещё так: подставим в (B) значения x_i' из (A), затем подставим значения y_i, выраженные через x_i в (C); тогда переменные z_i выразятся через x_i. Наконец, подставляем z_i, выраженные через x_i, в (D). Получим как раз искомое преобразование $(DCBA)$.

З а д а ч а. Привести следующие квадратичные формы к каноническому виду.

a) $\varphi=x_1^2-5x_1x_2+3x_2x_3$,

b) $\varphi=x_1x_2-x_1x_3+x_3x_4$,

c) $\varphi=5x_1x_2-x_3^2+x_3x_4$.

§ 24. Ранг квадратичной формы

Итак, всякую квадратичную форму можно методом Лагранжа привести к виду

$$\varphi=c_1v_1^2+c_2v_2^2+\ldots+c_mv_m^2. \qquad (1)$$

Возникает естественный вопрос: чему равно число m квадратов, входящих в каноническую форму (1)? Мы увидим ниже, что на этот вопрос можно дать вполне определённый ответ.

Обратимся опять к симметрической записи (5) предыдущего параграфа; её i-я строчка имеет вид

$$a_{i_1}x_ix_1+a_{i_2}x_ix_2+\ldots+a_{in}x_ix_n. \qquad (2)$$

Но это несколько громоздкое выражение можно записать короче, если воспользоваться часто употребляемым в математике символом $\sum$ (знак суммы).

С помощью $\sum$ выражение (2) сокращённо запишется так: $\sum_{j=1}^{n} a_{ij}x_ix_j$, причём $\sum_{j=1}^{n}$ означает, что в общем члене, стоящем под знаком суммы, последовательно полагается $j=1, 2, \ldots, n$, и получившиеся члены складываются.

Например:

$$\sum_{j=1}^{n} u^j = u + u^2 + \ldots + u^n,$$

$$\sum_{j=1}^{n} \frac{1}{j} = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}.$$

Очевидно, что сама форма φ есть сумма всех строчек симметрической записи, т. е.

$$\varphi = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_ix_j.$$

Составим теперь матрицу

$$A = \begin{Vmatrix} a_{11} & \ldots & a_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ a_{n1} & \ldots & a_{nn} \end{Vmatrix}$$

из коэффициентов 1-й, 2-й, ..., n-й строчек симметрической записи. Мы будем A называть *матрицей формы* φ, а ранг A—*рангом формы* φ. Нашей основной задачей является доказательство следующей теоремы.

Теорема. *От невырождающегося линейного преобразования ранг формы* φ *не меняется.*

Прежде всего займёмся некоторыми свойствами матриц n-го порядка, после чего наша теорема докажется без особого труда.

Пусть AB есть произведение матриц

$$A = \begin{Vmatrix} a_{11} & \ldots & a_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ a_{n1} & \ldots & a_{nn} \end{Vmatrix}, \qquad B = \begin{Vmatrix} b_{11} & \ldots & b_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ b_{n1} & \ldots & b_{nn} \end{Vmatrix}.$$

Что можно сказать относительно ранга AB? Мы сейчас покажем, что *ранг произведения двух матриц не выше ранга каждого из сомножителей.*

В самом деле, если c_{ik} — элемент матрицы AB, то по правилу перемножения

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \ldots + a_{in}b_{nk} = \sum_{s=1}^{n} a_{is}b_{sk} \quad (i, k = 1, 2, \ldots, n).$$

Таким образом каждый элемент AB есть сумма n слагаемых. Обозначим теперь ранг матрицы A через r_1, а ранг матрицы B через r_2 и покажем, что любой определитель Δ_p ($p > r_1$) p-го порядка матрицы AB равен нулю. Определитель Δ_p можно, очевидно, разложить на сумму определителей типа

$$\begin{vmatrix} a_{i_1 s_1}b_{s_1 k_1} & a_{i_1 s_2}b_{s_2 k_2} & \ldots & a_{i_1 s_p}b_{s_p k_p} \\ a_{i_2 s_1}b_{s_1 k_1} & a_{i_2 s_2}b_{s_2 k_2} & \ldots & a_{i_2 s_p}b_{s_p k_p} \\ \ldots & \ldots & \ldots & \ldots \\ a_{i_p s_1}b_{s_1 k_1} & a_{i_p s_2}b_{s_2 k_2} & \ldots & a_{i_p s_p}b_{s_p k_p} \end{vmatrix}, \tag{3}$$

так как элемент каждого столбца Δ_p есть сумма n слагаемых. Вынося из каждого столбца определителя (3) общий множитель, получим:

$$b_{s_1 k_1}b_{s_2 k_2} \ldots b_{s_p k_p} \begin{vmatrix} a_{i_1 s_1} & a_{i_1 s_2} & \ldots & a_{i_1 s_p} \\ a_{i_2 s_1} & a_{i_2 s_2} & \ldots & a_{i_2 s_p} \\ \ldots & \ldots & \ldots & \ldots \\ a_{i_p s_1} & a_{i_p s_2} & \ldots & a_{i_p s_p} \end{vmatrix}.$$

Последний определитель может иметь некоторые строки или столбцы одинаковыми, но может также иметь и различные строки и столбцы. В первом случае он, очевидно, равен нулю. Но и во втором случае определитель равен нулю, так как он будет определителем p-го порядка ($p > r_1$) матрицы A ранга r_1.

Итак, мы видим, что Δ_p равно нулю, так как все его слагаемые (3) равны нулю. Этим вполне доказано, что ранг AB не может быть выше ранга A.

Остаётся показать, что ранг AB не выше ранга второго сомножителя B. Опять повторяем аналогичные рассуждения. Возьмём определитель Δ_q q-го порядка ($q > r_2$) матрицы AB. Его можно разложить на сумму определителей типа

$$\begin{vmatrix} a_{i_1 s_1}b_{s_1 k_1} & a_{i_1 s_1}b_{s_1 k_2} & \ldots & a_{i_1 s_1}b_{s_1 k_q} \\ a_{i_2 s_2}b_{s_2 k_1} & a_{i_2 s_2}b_{s_2 k_2} & \ldots & a_{i_2 s_2}b_{s_2 k_q} \\ \ldots & \ldots & \ldots & \ldots \\ a_{i_q s_q}b_{s_q k_1} & a_{i_q s_q}b_{s_q k_2} & \ldots & a_{i_q s_q}b_{s_q k_q} \end{vmatrix},$$

так как элемент каждой строчки Δ_q есть сумма n слагаемых. Вынося за знак определителя общие множители строк, получим

$$a_{i_1 s_1} a_{i_2 s_2} \dots a_{i_q s_q} \begin{vmatrix} b_{s_1 k_1} b_{s_1 k_2} \dots b_{s_1 k_q} \\ b_{s_2 k_1} b_{s_2 k_2} \dots b_{s_2 k_q} \\ \dots\dots\dots\dots \\ b_{s_q k_1} b_{s_q k_2} \dots b_{s_q k_q} \end{vmatrix}.$$

Если в последнем определителе имеются одинаковые строки или столбцы, то он равен нулю. Если же в определителе все строки и столбцы различны, то он опять-таки будет равен нулю как определитель q-го ($q > r_2$) порядка матрицы B ранга r_2. Итак, Δ_q равно нулю, откуда становится очевидным, что ранг AB не превосходит ранг B.

Особенно важен для нас тот частный случай, когда один из сомножителей, например B, есть невырождающаяся матрица. *Если матрица A ранга r умножается на невырождающуюся матрицу B, то ранг произведения также равен r.*

Доказывается это довольно просто. С одной стороны, ранг произведения AB, как мы уже знаем, меньше или равен рангу матрицы A: $r_1 \leqslant r$. С другой стороны, умножив AB справа на B^{-1}, получим:

$$(AB)B^{-1} = A(BB^{-1}) = AE = A.$$

Здесь A является произведением AB на B^{-1}; поэтому ранг меньше или равен рангу матрицы AB: $r \leqslant r_1$. Но неравенства $r_1 \leqslant r$ и $r \leqslant r_1$ как раз свидетельствуют о том, что $r = r_1$.

Теперь мы в состоянии доказать нашу теорему.

Доказательство. Квадратичную форму

$$\varphi = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j$$

удобнее записать в виде

$$\varphi = x_1 f_1 + x_2 f_2 + \dots + x_n f_n,$$

где

$$f_i = a_{i_1} x_1 + \dots + a_{in} x_n = \sum_{j=1}^{n} a_{ij} x_j \quad (i = 1, 2, \dots, n).$$

В самом деле, что такое $x_i f_i$? Произведение $x_i f_i$ есть i-я строчка симметричной записи формы φ, а мы знаем, что форма φ равна сумме всех таких строчек.

Подвергнем теперь φ невырождающемуся линейному преобразованию

$$x_i = b_{i_1} y_1 + b_{i_2} y_2 + \dots + b_{in} y_n \quad (i = 1, 2, \dots, n).$$

Обозначим матрицу этого преобразования через B.

Форму φ мы будем преобразовывать постепенно. Сначала подвергнем преобразованию B линейные формы f_i. Получим

$$\varphi = x_1F_1 + x_2F_2 + \ldots + x_nF_n, \tag{4}$$

где

$$F_i = c_{i1}y_1 + c_{i2}y_2 + \ldots + c_{in}y_n \quad (i = 1, 2, \ldots, n).$$

Чему равны коэффициенты c_{ik} новых линейных форм F_i? Обозначим матрицу из коэффициентов F_i через C:

$$C = \begin{Vmatrix} c_{11} & \ldots & c_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ c_{n1} & \ldots & c_{nn} \end{Vmatrix}.$$

Что касается матрицы из коэффициентов f_i, то она равна матрице квадратичной формы. Линейные формы F_i получились из f_i с помощью преобразования B; отсюда ясно, что $C = AB$.

Займёмся теперь правой частью равенства (4). Если в (4) подставить значения F_i и затем сгруппировать члены, содержащие общий множитель $y_1, y_2, \ldots, y_n$, то получится

$$\varphi = y_1\Phi_1 + y_2\Phi_2 + \ldots + y_n\Phi_n,$$

где

$$\Phi_i = c_{1i}x_1 + c_{2i}x_2 + \ldots + c_{ni}x_n \quad (i = 1, 2, \ldots, n).$$

Мы видим, что матрица $\overline{C}$ из коэффициентов Φ_i есть не что иное, как транспонированная матрица [1]) C.

Теперь остаётся подвергнуть преобразованию B линейные формы Φ_i. Получим тогда

$$\varphi = y_1L_1 + y_2L_2 + \ldots + y_nL_n,$$

где

$$L_i = d_{i1}y_1 + d_{i2}y_2 + \ldots + d_{in}y_n \quad (i = 1, 2, \ldots, n).$$

Обозначим матрицу из коэффициентов L_i через A_1:

$$A_1 = \begin{Vmatrix} d_{11} & \ldots & d_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ d_{n1} & \ldots & d_{nn} \end{Vmatrix}.$$

Очевидно, A_1 есть вместе с тем матрица преобразованной квадратичной формы, при этом $A_1 = \overline{C}B$. Но B—невырождающаяся матрица,

[1]) Матрицу, получающуюся путём замены — транспонирования — строк столбцами, принято называть *транспонированной*.

откуда ранг A_1 равен рангу $\overline{C}$. В свою очередь ранг $\overline{C}$ равен рангу C, так как от транспонирования ранг матрицы не меняется. Чему же равен ранг C? Легко видеть, что ранг $C=AB$ равен рангу A, потому что B—невырождающаяся матрица. Итак, ранг A_1 равен рангу A; иными словами, мы показали, что ранг преобразованной квадратичной формы равен рангу первоначальной формы. Теорема доказана.

Вернёмся к вопросу, заданному в самом начале параграфа. Чему равно число членов m канонического вида (1)? Оказывается, что m равно рангу формы φ.

Следствие. *Если φ—квадратичная форма ранга r, то после приведения её линейным невырождающимся преобразованием к каноническому виду она будет содержать r членов.*

В самом деле, пусть квадратичная форма $\varphi=\sum\sum a_{ij}x_ix_j$ ранга r приведена к каноническому виду (1). Матрица формы (1), очевидно, равна

$$D=\begin{Vmatrix} c_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & c_2 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & c_m & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{Vmatrix},$$

откуда ясно, что ранг D равен m. Но, с другой стороны, ранг формы φ от невырождающегося преобразования не меняется; следовательно, $m=r$, что и требовалось показать.

В заключение разберём пример, иллюстрирующий вышеизложенное.

Пример. Рассмотрим форму

$$\varphi=x_1x_2-5x_1x_3+x_1x_4.$$

Её ранг равен двум, так как её матрица

$$\begin{Vmatrix} 0 & \frac{1}{2} & -\frac{5}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 & 0 \\ -\frac{5}{2} & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 \end{Vmatrix}$$

ранга 2. Следовательно, после приведения к каноническому виду должно получиться всего два члена. И, действительно, преобразуя по методом Лагранжа, получим канонический вид:

$$\varphi=z_1^2-z_2^2,$$

причём

$$z_1 = \frac{1}{2}x_1 + \frac{1}{2}x_2 - \frac{5}{2}x_3 + \frac{1}{2}x_4,$$
$$z_2 = -\frac{1}{2}x_1 + \frac{1}{2}x_2 - \frac{5}{2}x_3 + \frac{1}{2}x_4,$$
$$z_3 = x_3,$$
$$z_4 = x_4.$$

§ 25. Закон инерции. Классификация квадратичных форм

Квадратичная форма может быть приведена к каноническому виду весьма разнообразными способами. Например, форму

$$\varphi = x_1x_2 - 5x_1x_3 + x_1x_4,$$

разобранную в предыдущем параграфе, можно было подвергнуть несколько иным преобразованиям. А именно положим

$$y_1 = \frac{5}{2}x_1 + \frac{1}{2}x_2 - \frac{5}{2}x_3 + \frac{1}{2}x_4,$$
$$y_2 = -5x_1 + x_2 - 5x_3 + x_4,$$
$$y_3 = x_3,$$
$$y_4 = x_4.$$

Мы получим тогда вместо

$$\varphi = z_1^2 - z_2^2 \tag{1}$$

несколько иной канонический вид:

$$\varphi = \frac{1}{5}y_1^2 - \frac{1}{20}y_2^2. \tag{2}$$

Однако, сравнивая (1) и (2), мы замечаем, что в обоих случаях число положительных членов одинаково: в первом случае мы имеем один положительный член z_1^2, а во втором случае — тоже один положительный член $\frac{1}{5}y_1^2$.

Подмеченная закономерность не является случайной. Она открыта одновременно Якоби и Сильвестром и носит название закона инерции квадратичных форм. Однако этот закон справедлив только для действительных форм, т. е. форм с действительными коэффициентами. Для форм с комплексными коэффициентами закон инерции неверен.

Закон инерции квадратичных форм. *Если действительная квадратичная форма $\varphi(x_1, \ldots, x_n)$ ранга r приведена двумя действительными* [1]) *невырождающимися линейными преобразованиями соответственно к виду*

$$\varphi = c_1y_1^2 + c_2y_2^2 + \ldots + c_ry_r^2 \tag{3}$$

и к виду

$$\varphi = d_1z_1^2 + d_2z_2^2 + \ldots + d_rz_r^2, \tag{4}$$

[1]) Т. е. преобразованиями с действительными коэффициентами.

то формы (3) *и* (4) *имеют одно и то же число положительных членов.*

Доказательство. Без ограничения общности доказательства можно предположить, что в формах (3) и (4) сначала идут положительные члены, так как иначе мы изменили бы соответствующим образом нумерацию переменных. Итак, пусть

$$\varphi = c_1 y_1^2 + c_2 y_2^2 + \ldots + c_p y_p^2 - c_{p+1} y_{p+1}^2 - \ldots - c_r y_r^2 = \\ = d_1 z_1^2 + d_2 z_2^2 + \ldots + d_q z_q^2 - d_{q+1} z_{q+1}^2 - \ldots - d_r z_r^2. \qquad (5)$$

Нам надо доказать, что $p = q$. Предположим противное, пусть, например, $p > q$. Переменные $y_1, y_2, \ldots, y_n$ и $z_1, z_2, \ldots, z_n$ являются линейными формами старых переменных $x_1, \ldots, x_n$. Поэтому, если $y_{p+1}, \ldots, y_r, \ldots, y_n$ и $z_1, \ldots, z_q$ приравнять нулю, то получится система $q + (n - p)$ однородных уравнений:

$$z_1 = 0, \quad z_2 = 0, \quad \ldots, \quad z_q = 0,$$
$$y_{p+1} = 0, \quad y_{p+2} = 0, \quad \ldots, \quad y_r = 0, \quad y_{r+1} = 0, \quad \ldots, \quad y_n = 0$$

относительно n неизвестных $x_1, x_2, \ldots, x_n$. Очевидно, эта система допускает ненулевые решения, так как число уравнений меньше числа неизвестных: $q + (n - p) = n - (p - q) < n$.

Пусть

$$\alpha_1, \alpha_2, \ldots, \alpha_n$$

—одно из ненулевых решений системы. Заменим в равенстве (5) переменные $x_1, x_2, \ldots, x_n$ через $\alpha_1, \alpha_2, \ldots, \alpha_n$; тогда мы получим

$$c_1 y_1^2(\alpha_1, \ldots, \alpha_n) + \ldots + c_p y_p^2(\alpha_1, \ldots, \alpha_n) = \\ = -d_{q+1} z_{q+1}^2(\alpha_1, \ldots, \alpha_n) - \ldots - d_r z_r^2(\alpha_1, \ldots, \alpha_n).$$

Выражение в левой части не может быть отрицательным, а в правой части выражение не может быть положительным. Следовательно, обе части рассматриваемого равенства должны обращаться в нуль [1]), а это возможно только в том случае, когда

$$\left.\begin{aligned} y_1(\alpha_1, \ldots, \alpha_n) = 0, \ \ldots, \ y_p(\alpha_1, \ldots, \alpha_n) = 0, \\ z_{q+1}(\alpha_1, \ldots, \alpha_n) = 0, \ \ldots, \ z_r(\alpha_1, \ldots, \alpha_n) = 0. \end{aligned}\right\} \qquad (6)$$

Но выше мы подобрали $\alpha_1, \alpha_2, \ldots, \alpha_n$ так, чтобы

$$y_{p+1}(\alpha_1, \ldots, \alpha_n) = 0, \ \ldots, \ y_n(\alpha_1, \ldots, \alpha_n) = 0. \qquad (7)$$

Таким образом, сопоставляя равенства (6) и (7), мы приходим к выводу, что $\alpha_1, \alpha_2, \ldots, \alpha_n$ есть ненулевое решение системы

$$y_1 = 0, \quad y_2 = 0, \quad \ldots, \quad y_n = 0$$

n линейных однородных уравнений с n неизвестными. Но в таком случае определитель этой системы должен равняться нулю, т. е. пре-

[1]) Если бы квадратичная форма и преобразование не были действительными, то левая и правая части могли бы и не обращаться в нуль.

образование, переводящее старые переменные $x_1, x_2, \ldots, x_n$ в новые $y_1, y_2, \ldots, y_n$, является вырождающимся. Получилось противоречие, которое и доказывает теорему.

Мы будем называть *указателем* действительной квадратичной формы число положительных членов в её канонической записи.

Итак, всякая действительная квадратичная форма характеризуется двумя числами—рангом и указателем. Эти числа не зависят от действительного невырождающегося преобразования: они инвариантны относительно таких преобразований.

Закон инерции играет большую роль при классификации действительных квадратичных форм. Назовём две действительные формы φ и ψ *эквивалентными* по отношению к невырождающемуся действительному преобразованию S, если ψ получается из φ с помощью преобразования S. Очевидно, что в силу теоремы предыдущего параграфа и закона инерции *две эквивалентные формы φ и ψ должны обладать одним и тем же рангом и указателем.* Но справедливо и обратное утверждение: *если две действительные формы φ и ψ имеют одинаковый ранг и указатель, то они эквивалентны по отношению к действительному невырождающемуся преобразованию.*

Для доказательства этого утверждения введём следующее определение.

Определение. *Каноническая форма*

$$\varphi = c_1 y_1^2 + \ldots + c_p y_p^2 - c_{p+1} y_{p+1}^2 - \ldots - c_r y_r^2$$

называется нормальной, если все коэффициенты c_i равны единице, т. е.

$$\varphi = y_1^2 + \ldots + y_p^2 - y_{p+1}^2 - \ldots - y_r^2. \tag{8}$$

Очевидно, что всякую форму можно привести к нормальному виду. В самом деле, можно сначала методом Лагранжа привести к каноническому виду

$$\varphi = k_1 y_1^2 + \ldots + k_p y_p - k_{p+1} y_{p+1}^2 - \ldots - k_r y_r^2 \quad (k_i > 0),$$

а затем подвергнуть переменные $y_1, y_2, \ldots, y_n$ невырождающемуся преобразованию

$$z_1 = \sqrt{k_1}\, y_1, \quad z_2 = \sqrt{k_2}\, y_2, \quad \ldots, \quad z_r = \sqrt{k_r}\, y_r, \quad z_{r+1} = y_{r+1}, \quad \ldots, \quad z_n = y_n,$$

в результате чего получится форма нормального вида

$$\varphi = z_1^2 + z_2^2 + \ldots + z_p^2 - z_{p+1}^2 - \ldots - z_r^2.$$

Теперь вернёмся к доказательству нашего утверждения.

Доказательство. Итак, пусть две действительные формы $\varphi = \sum\sum a_{ij} x_i x_j$ и $\psi = \sum\sum b_{ij} x_i x_j$ имеют один и тот же ранг r и указатель p. Пусть φ приводится к нормальному виду действительным невырождающимся преобразованием S, а ψ—действительным невырождающимся преобразованием T. Согласно теореме предыду-

щего параграфа и закону инерции как φ; так и ψ приводятся к одному и тому же нормальному виду

$$z_1^2+z_2^2+\ldots+z_p^2-z_{p+1}^2-\ldots-z_r^2, \qquad (A)$$

потому что ранг и указатель у форм φ и ψ одинаковы.

Таким образом, если форму $\psi=\sum\sum b_{ij}x_ix_j$ подвергнуть преобразованию $S^{-1}T$, то получится форма φ. Действительно, с помощью преобразования T ψ переходит в нормальный вид (A), а затем с помощью преобразования S^{-1} в φ.

Для наглядности приведём пример, иллюстрирующий доказательство.

Пример. Рассмотрим две квадратичные формы

$$\left.\begin{aligned}\varphi&=x_1^2+2x_1x_2+2x_2^2-2x_2x_3,\\ \psi&=x_1^2-2x_1x_3-2x_2x_3+x_2^2+x_3^2.\end{aligned}\right\} \qquad (9)$$

Они имеют одинаковый ранг и указатель, а именно: $r=3$, $p=2$. Затем легко проверить, что невырождающиеся преобразования

$$\left.\begin{aligned}z_1&=x_1+x_2,\\ z_2&=\quad x_2-x_3,\\ z_3&=\quad x_3\end{aligned}\right\} \qquad (S)$$

$$\left.\begin{aligned}z_1&=x_1\quad -x_3,\\ z_2&=\quad x_2-x_3,\\ z_3&=\quad x_3\end{aligned}\right\} \qquad (T)$$

приводят соответственно формы φ и ψ к нормальному виду

$$z_1^2+z_2^2-z_3^2.$$

Следовательно, преобразование $S^{-1}T$ должно переводить ψ в φ. **Найдём** $S^{-1}T$, для этого выписываем матрицы S и T:

$$S=\begin{Vmatrix}1&1&0\\0&1&-1\\0&0&1\end{Vmatrix}, \qquad T=\begin{Vmatrix}1&0&-1\\0&1&-1\\0&0&1\end{Vmatrix},$$

откуда

$$S^{-1}=\begin{Vmatrix}1&-1&1\\0&1&1\\0&0&1\end{Vmatrix} \quad \text{и} \quad S^{-1}T=\begin{Vmatrix}1&-1&1\\0&1&0\\0&0&1\end{Vmatrix}.$$

Таким образом преобразование $S^{-1}T$ найдено: оно имеет вид

$$\left.\begin{aligned}y_1&=x_1-x_2-x_3,\\ y_2&=\quad x_2,\\ y_3&=\quad x_3\end{aligned}\right\} \qquad (S^{-1}T)$$

и превращает форму ψ в

$$y_1^2+2y_1y_2+2y_2^2-2y_2y_3. \qquad (10)$$

Но форма (10) тождественна с φ, так как отличается от неё только обозначением переменных.

Переходим к вопросу о классификации действительных квадратичных форм. Отнесём две эквивалентные формы к одному классу и не будем считать такие формы различными. Тогда все формы n переменных разобьются на конечное число классов.

Например, все формы ранга 3 от трёх переменных подразделяются на 4 класса, которые характеризуются следующими нормальными формами:

$$\begin{array}{lll} x_1^2-x_2^2-x_3^2 & \text{указатель равен} & 0, \\ x_1^2-x_2^2-x_3^2 & \text{»} \quad \text{»} & 1, \\ x_1^2+x_2^2-x_3^2 & \text{»} \quad \text{»} & 2, \\ x_1^2+x_2^2+x_3^2 & \text{»} \quad \text{»} & 3. \end{array}$$

Разберём более внимательно, какими характерными признаками обладают эти четыре класса при действительных значениях переменных.

Формы, принадлежащие к четвёртому классу, приводятся к нормальному виду

$$x_1^2+x_2^2+x_3^2. \tag{11}$$

Мы видим, что все члены (11) положительны и потому нормальная форма (11) не может принимать отрицательных значений.

Формы, принадлежащие ко второму и третьему классам, имеют нормальный вид:

$$x_1^2-x_2^2-x_3^2 \tag{12}$$

и

$$x_1^2+x_2^2-x_3^2. \tag{13}$$

Здесь уже встречаются как положительные, так и отрицательные члены; поэтому нормальные формы (12) и (13) могут принимать не только положительные, но и отрицательные значения.

Наконец, формы первого класса имеют нормальный вид:

$$-x_1^2-x_2^2-x_3^2, \tag{14}$$

в котором все члены отрицательны. Следовательно, нормальная форма (14) способна принимать только отрицательные значения.

Формы первого и четвёртого классов называются *определёнными*, а формы второго и третьего классов—*неопределёнными*. Вообще введём такое определение.

Определение. *Действительная квадратичная форма называется неопределённой, если её указатель p отличен от нуля и меньше её ранга r. Если же $p=0$ или $p=r$, то форма называется определённой, причём в первом случае она называется отрицательной, а во втором случае—положительной.*

Выбор терминов «определённая» и «неопределённая» форма становится понятным из следующей теоремы.

Теорема. *При всех действительных значениях переменных $x_1, \ldots, x_n$ положительная определённая форма равна нулю или положи-*

тельна, а отрицательная определённая форма равна нулю или отрицательна; что касается неопределённой формы, то она может принимать как положительные, так и отрицательные значения.

Доказательство. Пусть форма $\varphi = \sum \sum a_{ij}x_i x_j$ действительным невырождающимся преобразованием приведена к нормальному виду. Пусть φ положительная определённая форма. Тогда после преобразования она будет выглядеть так:

$$\varphi = z_1^2 + z_2^2 + \ldots + z_r^2$$

и, очевидно, $\varphi \geqslant 0$, как сумма положительных квадратов.

Точно так же для отрицательной определённой формы получим нормальный вид

$$\varphi = -z_1^2 - z_2^2 - \ldots - z_r^2,$$

так как все квадраты отрицательны.

Остаётся разобрать случай неопределённой формы. Пусть такая форма имеет следующий нормальный вид:

$$\varphi = z_1^2 + z_2^2 + \ldots + z_p^2 - z_{p+1}^2 - \ldots - z_r^2. \qquad (15)$$

Рассмотрим систему $n - p$ однородных линейных уравнений с n неизвестными $x_1, \ldots, x_n$

$$z_{p+1} = 0, \quad \ldots, \quad z_n = 0. \qquad (16)$$

Эта система наверное допускает ненулевые решения, например, $\alpha_1, \alpha_2, \ldots, \alpha_n$, так как число неизвестных больше числа уравнений. Подставляя $x_1 = \alpha_1, \ldots, x_n = \alpha_n$ в равенство (15), получим

$$\varphi(\alpha_1, \ldots, \alpha_n) = z_1^2(\alpha_1, \ldots, \alpha_n) + \ldots + z_p^2(\alpha_1, \ldots, \alpha_n).$$

Мы утверждаем теперь, что $\varphi(\alpha_1, \ldots, \alpha_n) > 0$. В самом деле, если бы $\varphi(\alpha_1, \ldots, \alpha_n)$ равнялось нулю, то отсюда следовало бы, что

$$z_1(\alpha_1, \ldots, \alpha_n) = 0, \quad \ldots, \quad z_p(\alpha_1, \ldots, \alpha_n) = 0. \qquad (17)$$

Но из (16) и (17) вытекает нелепость: система n однородных уравнений

$$z_1 = 0, \quad z_2 = 0, \quad \ldots, \quad z_n = 0$$

с n неизвестными имеет ненулевое решение $\alpha_1, \alpha_2, \ldots, \alpha_n$, несмотря на то, что определитель этой системы отличен от нуля, как определитель невырождающегося преобразования. Таким образом должно быть $\varphi(\alpha_1, \ldots, \alpha_n) > 0$.

Теперь рассмотрим несколько иную систему однородных уравнений

$$z_1 = 0, \quad \ldots, \quad z_p = 0.$$

Опять, как и выше, выводим, что написанная система допускает ненулевые решения, например $x_1 = \beta_1, x_2 = \beta_2, \ldots, x_n = \beta_n$, и затем

убеждаемся, что

$$\varphi(\beta_1, \ldots, \beta_n) = -z_{p+1}^2(\beta_1, \ldots, \beta_n) - \ldots - z_r^2(\beta_1, \ldots, \beta_n) < 0.$$

Итак, мы видим, что при $x_1 = \alpha_1, \ldots, x_n = \alpha_n$ неопределённая форма φ положительна, а при $x_1 = \beta_1, \ldots, x_n = \beta_n$ отрицательна. Теорема доказана полностью.

Задачи. 1. Найти ранг и указатель формы

$$\varphi = x_1^2 - 5x_1x_2 + x_1x_3 + x_2x_4.$$

Установить, при каких значениях переменных φ положительна и при каких отрицательна.

2. Показать, что действительная квадратичная форма с рангом r и указателем p тогда и только тогда может быть разложена на два действительных линейных множителя, когда

a) $r < 2$,

b) $r = 2$, но $p = 1$.

3. Показать, что существует всего $\frac{1}{2}(n+1)(n+2)$ классов действительных квадратичных форм от n переменных.

До сих пор мы говорили исключительно о действительных квадратичных формах и действительных преобразованиях. Но легко видеть, что результаты § 23 и 24 остаются в силе и для форм с комплексными коэффициентами. Однако для этих форм теряют смысл закон инерции и все его следствия.

Если не ограничиваться действительными преобразованиями, то можно любую форму привести к (арифметической) сумме квадратов. В самом деле, для этого следует форму сперва привести к каноническому виду:

$$\varphi = c_1y_1^2 + c_2y_2^2 + \ldots + c_ry_r^2,$$

а затем подвергнуть $y_1, \ldots, y_n$ невырождающемуся преобразованию

$$z_1 = \sqrt{c_1}y_1, \ \ldots, \ z_r = \sqrt{c_r}y_r, \ z_{r+1} = y_{r+1}, \ \ldots, \ z_n = y_n, \qquad (18)$$

в результате чего получится сумма квадратов:

$$\varphi = z_1^2 + z_2^2 + \ldots + z_r^2.$$

Преобразование (18) может и не оказаться действительным, как некоторые c_i могут быть отрицательными.

На этом мы заканчиваем общую теорию квадратичных форм. Отсылаем читателей, желающих более основательно познакомиться с этой теорией, к классической книге M. Bocher, Einführung in die höhere Algebra [1]).

[1]) Имеется русский перевод, М. Бохер, Введение в высшую алгебру, ОНТИ, 1935 г. Однако этим изданием следует пользоваться с осторожностью, так как оно содержит очень много опечаток.

ГЛАВА ПЯТАЯ

ЧИСЛА И ОБЩАЯ ТЕОРИЯ МНОГОЧЛЕНОВ

§ 26. Содержание современной алгебры

Что такое алгебра? Этот вопрос читатель наверное задавал себе не раз. Однако обрисовать с исчерпывающей полнотой содержание этой дисциплины представляется затруднительным, так как она, как и всякая наука, не является мёртвой и застывшей теорией, а изменяется и растёт.

Так называемая классическая алгебра (алгебра XVIII—XIX вв.) занималась главным образом решением уравнений высших степеней и изучением свойств рациональных функций. За последние десятилетия алгебра достигла небывалого расцвета. Содержанием современной алгебры является изучение некоторых операций над элементами какого-нибудь множества; как операции, так и элементы множества могут быть самой разнообразной природы, важно лишь, чтобы операции имели много черт, сближающих их с обыкновенными арифметическими действиями. Отметим ещё, что современная алгебра чаще всего имеет дело с множествами, образующими по отношению к вышеупомянутым операциям группу или кольцо (см. гл. III).

Такое расширение кругозора позволило решить ряд вопросов, не имеющих на первый взгляд ничего общего с алгеброй. Так, например, теория групп и колец с успехом применяется в теории дифференциальных уравнений, в топологии, в алгебраической геометрии и т. д. Область приложений алгебры, однако, не ограничена математическими дисциплинами. Можно, например, сослаться на квантовую физику, для которой теория групп имеет существенное значение.

Но все эти далеко идущие цели и методы алгебры сегодняшнего дня покоятся на двух основных понятиях—на понятии числа и многочлена. Можно смело утверждать, что без этих понятий алгебра как наука не существовала бы.

§ 27. Натуральные числа

Как известно, числа $1, 2, 3, 4, \ldots$ называются целыми положительными (натуральными) числами. Понятие натурального числа возникло в глубокой древности в связи с простым счётом предметов. Ныне представление о натуральном числе настолько прочно вошло в наше сознание, что основные свойства действий сложения и умножения над этими числами, а именно:

a) переместительный закон: $a+b=b+a$, $ab=ba$,

b) сочетательный закон: $(a+b)+c=a+(b+c)$, $(ab)c=a(bc)$,

c) распределительный закон: $a(b+c)=ab+ac$,

кажутся очевидными. Тем не менее существует обоснование этих законов; оно было предложено сравнительно недавно итальянским математиком Пеано. Мы не будем, однако, излагать тонкой и слож-

ной теории Пеано [1]), а ограничимся некоторыми замечаниями, относящимися к обратным действиям.

Начнём с вычитания. Натуральное число x, удовлетворяющее уравнению $a+x=b$ (a, b — натуральные числа), называется разностью и обозначается через $b-a$. Таким образом $a+(b-a)=b$. Если $b \leqslant a$, то разность $b-a$ не существует в области натуральных чисел. Что касается деления, то натуральное число b называется *делящимся* на натуральное число a или *кратным* a, если существует такое третье натуральное число c, что $ac=b$. Но мы хорошо знаем, что далеко не всегда одно натуральное число делится на другое, например 7 не делится на 3.

Отметим главнейшие свойства делимости натуральных чисел. Мы, однако, не будем доказывать все свойства, так как сходные доказательства будут даны ниже при рассмотрении свойств делимости многочленов (в § 28). Для краткости условимся в тех случаях, когда это не приводит к недоразумениям, натуральное число называть просто числом.

I. *Если число a больше b и не делится на b, то всегда можно подобрать такую пару чисел q и $r<b$ (частное и остаток), что*

$$a=bq+r. \tag{1}$$

Иными словами: делимое (a) равно делителю (b), умноженному на частное (q), плюс остаток (r).

Для доказательства вычтем из a число b. Если разность $a-b$ больше b, то мы снова вычтем b. Разность $(a-b)-b=a-2b$ в свою очередь может оказаться больше b; тогда мы опять вычтем b и т. д., пока не получится число, меньшее b. Таким образом после некоторого количества вычитаний мы будем иметь, что $a-bq=r$ или $a=bq+r$, причём $r<b$.

II. *Если a делится на b и b делится на c, то a также делится на c.*

III. *Если a и b делятся на c, то их сумма и разность также делятся на c.*

IV. *Если хотя бы одно из чисел a и b делится на c, то и их произведение ab делится на c.*

Дальнейшие арифметические свойства натуральных чисел тесно связаны с понятием общего делителя.

Общим делителем двух чисел a и b называется такое третье число c, на которое делятся как a, так и b. Например 15 и 10 имеют общим делителем 1 и 5, причём 5 может быть названо общим наибольшим делителем. Вообще введём следующее определение.

Определение. *Общим наибольшим делителем двух чисел a и b называется такой общий делитель d, который делится на всякий другой общий делитель.*

Общий наибольший делитель мы будем обозначать символом (a, b). Так, например, $(15, 10)=5$.

---

[1]) Изложение теории Пеано читатель может найти в книжке E. Landau, Grundlagen der Analysis, Leipzig, 1930.

Возникает естественный вопрос — если даны два числа a и b, то как определить их общий наибольший делитель? Для этой цели существует специальный способ, называемый *алгоритмом Эвклида*. Он состоит в следующем. Пусть $b > a$. Делим b на a; остаток и частное, полученные при делении, обозначим соответственно через r_1 и q_1. Затем делим a на остаток r_1, в результате чего получатся второй остаток r_2 и частное q_2. Снова делим r_1 на r_2 и получаем третий остаток r_3 и частное q_3 и т. д. Вообще каждый раз делим предыдущий остаток на последующий. При этом остатки $r_1, r_2, r_3, \ldots$ всё время убывают: $r_1 > r_2 > r_3 > \ldots$ и потому мы неизбежно должны притти к такому остатку r_n, на который целиком разделится предыдущий остаток r_{n-1}. Если бы это не имело места, то процесс деления продолжался бы без конца и мы имели бы бесконечную убывающую последовательность остатков

$$r_1 > r_2 > r_3 > \ldots > r_k > \ldots,$$

что невозможно для натуральных чисел.

Весь процесс деления можно записать в следующем виде:

$$\left.\begin{aligned} b &= q_1 a + r_1, \\ a &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ &\ldots\ldots\ldots\ldots \\ r_{n-2} &= q_n r_{n-1} + r_n, \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}\right\} \qquad (2)$$

Мы утверждаем теперь, что r_n *как раз и есть общий наибольший делитель*.

Докажем прежде всего, что r_n общий делитель. Возьмём предпоследнее равенство:

$$r_{n-2} = q_n r_{n-1} + r_n. \qquad (3)$$

Его правая часть есть сумма двух слагаемых, причём первое слагаемое $q_n r_{n-1}$ делится на r_n, так как r_{n-1} делится на r_n; что касается второго слагаемого, то оно есть само r_n. Таким образом мы видим, что вся правая часть равенства (3) делится на r_n, а это значит, что на r_n делится и r_{n-2}.

Переходим к предыдущему равенству:

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}.$$

Здесь r_{n-2} и r_{n-1} делятся на r_n, откуда ясно, что вся правая часть делится на r_n, а потому на r_n делится и r_{n-3}.

Переходя так постепенно вверх, мы в конце концов дойдём до чисел a и b и увидим, что как a, так и b делятся на r_n. Следовательно, утверждение о том, что r_n есть общий делитель можно считать доказанным.

Теперь покажем, что r_n есть общий *наибольший* делитель. Пусть m какой-нибудь общий делитель чисел a и b. Возьмём первое равенство

$$b = aq_1 + r_1.$$

В нём b и a делятся на m, поэтому на m должна делиться и разность $b - aq_1 = r_1$. Затем рассматриваем следующее равенство:

$$a = r_1 q_2 + r_2;$$

опять видим, что a и r_1 делятся на m, поэтому и r_2 делится на m. Так, передвигаясь постепенно вниз, мы, наконец, дойдём до r_n и убедимся, что m делит r_n, т. е. r_n действительно есть наибольший делитель.

Пример. Найдём (15 015, 45 885). Делим 45 885 на 15 015. Получаем $r_1 = 840$. Затем делим 15 015 на 840; получим $r_2 = 735$. Далее делим 840 на 735, в результате чего имеем $r_3 = 105$. Наконец, деля 735 на 105, убеждаемся, что деление происходит без остатка, откуда следует, что $r_3 = 105$ и есть общий наибольший делитель, т. е.

$$(15\,015,\ 45\,885) = 105.$$

В частности может случиться, что $(a, b) = 1$; в таком случае числа a и b называются *взаимно простыми*. Например 7 и 5 взаимно просты, потому что $(7, 5) = 1$.

Из алгоритма Эвклида получается одна важная теорема, значение которой мы уясним себе в § 28.

Теорема I. *Если d — общий наибольший делитель натуральных чисел a и b, то всегда можно подобрать два таких целых числа x и y* [1]), *что*

$$ax + by = d.$$

Все натуральные числа, как известно, разбиваются на два рода: простые и составные. *Простым* называется такое число, отличное от 1, которое делится только на единицу и само на себя. Остальные числа, не удовлетворяющие этому условию, называются *составными*. Например 7 является простым, а 15 составным числом. Простые числа обладают следующими важными свойствами.

a) *Если простое число p_1 делится на другое простое число p_2, то $p_1 = p_2$.*

b) *Если m не делится на простое число p, то m и p взаимно просты. Обратно, если m и p взаимно просты, то m не делится на p.*

c) *Если числа $a_1, a_2, \ldots, a_m$ не делятся на простое число p, то их произведение также не делится на p.*

d) *Если произведение ab делится на простое число p, то по крайней мере один из сомножителей делится на p.*

Само собой разумеется, что свойство d) можно распространить и на произведение любого числа сомножителей.

Значение простых чисел в арифметике видно из следующей теоремы, называемой часто основной теоремой арифметики.

---

[1]) x и y могут быть не только положительными, но и отрицательными целыми числами.

Теорема II. *Всякое (натуральное) число $m > 1$ может быть единственным образом разложено на произведение простых чисел:*

$$m = p_1 p_2 \dots p_r \text{ [1]}$$

(некоторые из простых чисел p могут быть равны между собой).

Некоторые из чисел p_i могут встречаться в разложении несколько раз. Пусть p_1 встречается α_1 раз, p_2 α_2 раз, ..., p_r α_r раз. Тогда разложение числа m на простые множители примет следующий окончательный вид:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}.$$

Пример. $3\,500 = 2^2 \cdot 5^3 \cdot 7$. Здесь

$$p_1 = 2,\ p_2 = 5,\ p_3 = 7;\ \alpha_1 = 2,\ \alpha_2 = 3,\ \alpha_3 = 1.$$

§ 28. Многочлены в поле P

Рассмотрим постоянные a, b, c, ..., взятые из некоторого числового поля P, например, из поля рациональных чисел, и переменные x, y, z, ... Переменные x, y, z, ... мы будем считать неизвестными величинами, над которыми можно производить арифметические действия, и не будем вводить для них никаких ограничений. Произведём над числами a, b, c, ... и x, y, z, ... операцию, состоящую лишь из комбинаций четырёх основных действий (сложения, вычитания, умножения и деления); мы получим некоторое выражение, известное в алгебре под названием *рациональной функции* от переменных x, y, z, ... Например, выражение

$$\frac{a + 2xy}{x - z}$$

является рациональной функцией от x, y, z, потому что это выражение составлено из постоянной a и переменных x, y, z при помощи четырёх основных действий. Можно указать ещё примеры рациональных функций, хотя бы

$$1 + 2xy - y^2, \quad \frac{x^3 + px + q}{x^2 + ax + b}, \quad \frac{1 + xy + yz + zu}{x^2 - y^2 + z^3} \text{ и т. д.}$$

Среди рациональных функций особенно важное значение имеют функции, не содержащие после надлежащих упрощений переменных в качестве делителей. Они называются *многочленами* или *целыми рациональными функциями* [2]. Чаще всего мы будем пользоваться первым термином. Легко понять, что всякая рациональная функция есть либо многочлен, либо отношение двух многочленов. Так, например,

$$\frac{1 + xy + yz + zu}{x^2 - y^2 + z^3}$$

[1] В частности произведение может состоять из одного простого числа. Это, очевидно, будет в том случае, когда само m простое.

[2] Например, функция $\frac{x^2 - 1}{x - 1}$ есть многочлен, так как после сокращения на $x - 1$ получается $x + 1$.

есть отношение многочленов $1 + xy + yz + zu$ и $x^2 - y^2 + z^2$. В настоящей главе рассматриваются только многочлены от одного переменного x; многочлены от многих переменных мы разберём позже.

Напишем теперь общий вид многочлена от одного переменного x. Это будет выражение вида

$$f(x) = c_1 x^{\alpha_1} + c_2 x^{\alpha_2} + \ldots + c_k x^{\alpha_k}, \qquad (1)$$

где $\alpha_1, \alpha_2, \ldots, \alpha_k$ — целые числа, положительные или равные нулю, а $c_1, c_2, \ldots, c_k$ — постоянные величины, называемые *коэффициентами*. Само собой понятно, что числа $\alpha_1, \alpha_2, \ldots, \alpha_k$ отличны друг от друга; в противном случае мы привели бы подобные члены. Введём несколько терминов, часто употребляемых в алгебре. Выражение $c_i x^{\alpha_i}$ называется *членом* многочлена, а показатель α_i — его *степенью*.

Однако выражение (1) удобнее несколько преобразовать. Расположим в нём x по убывающим степеням; тогда получим:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n, \quad a_0 \neq 0.$$

Некоторые из коэффициентов $a_1, a_2, \ldots, a_n$ могут оказаться равными нулю. Член $a_0 x^n$ мы часто будем называть *старшим членом*, его степень n — *степенью многочлена*, а a_0 — *старшим коэффициентом*. Необходимо заметить, что любое число $c \neq 0$ мы вправе также считать многочленом, именно, многочленом нулевой степени, потому что

$$c = cx^0.$$

Что касается числа 0, то его можно рассматривать как многочлен неопределённой степени.

Очень часто бывает важно знать, из какой числовой области берутся коэффициенты многочлена. Так, относительно многочлена

$$f(x) = x^5 - \frac{1}{2} x^3 + \frac{3}{5} x - \frac{1}{7}$$

можно сказать, что его коэффициенты принадлежат полю рациональных чисел.

Вообще, мы будем говорить, что функция

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$$

есть *многочлен в поле* P, если коэффициенты $a_0, a_1, \ldots, a_n$ взяты из поля P, при этом под полем P здесь подразумевается некоторое числовое поле, например, поле рациональных чисел или поле действительных чисел.

На протяжении §§ 28—31 нашей основной целью будет изучение свойств многочлена в поле P; при этом P может быть каким угодно числовым полем. Таким образом все выводы §§ 28—31 будут справедливы независимо от того, является ли P полем рациональных чисел или каким-нибудь другим числовым полем.

Обозначим множество всех многочленов в поле P символом $P[x]$. Два многочлена считаются равными (тождественно) тогда

и только тогда, когда они состоят из одинаковых членов. Например многочлены

$$f(x) = x^3 - 5x + 1, \quad f_1(x) = x^3 - 5x + 1$$

равны, так как члены $f(x)$ ничем не отличаются от членов $f_1(x)$; напротив, многочлены

$$g(x) = x^5 - x + 1, \quad g_1(x) = x^3 - x + 1$$

не равны, так как $g(x)$ содержит член x^5, не встречающийся в $g_1(x)$.

Многочлены складываются и перемножаются по правилам, известным из элементарной алгебры. Так, для

$$f(x) = x^3 - 2x + 1, \quad g(x) = x^4 - 3x^3 - x + 1$$

имеем:

$$f(x) + g(x) = x^4 - 2x^3 - 3x + 2,$$
$$f(x)\,g(x) = x^7 - 3x^6 - 2x^5 + 6x^4 - 3x^3 + 2x^2 - 3x + 1.$$

Вообще пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n,$$
$$g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m$$

два каких-нибудь многочлена в поле P. Предположим для определённости, что $n \geqslant m$, и напишем сумму и произведение этих многочленов:

$$f(x) + g(x) = a_0x^n + \ldots + a_{n-m-1}x^{m+1} + (a_{n-m} + b_0)x^m + \ldots + (a_{n-1} + b_{m-1})x + (a_n + b_m), \qquad (2)$$

$$f(x)\,g(x) = a_0b_0x^{m+n} + (a_0b_1 + a_1b_0)x^{n+m-1} + \ldots + a_nb_m. \qquad (3)$$

Мы видим, что сумма и произведение являются также многочленами в поле P; складывая или перемножая два многочлена с коэффициентами из поля P, мы снова получаем многочлен с коэффициентами из того же поля P.

Можно показать, что действия сложения и умножения многочленов подчиняются переместительному, сочетательному и распределительному законам. Мы ограничимся выводом сочетательности умножения.

Помножим (3) на

$$h(x) = c_0x^l + c_1x^{l-1} + \ldots + c_{l-1}x + c_l.$$

По правилу перемножения расположенных многочленов

$$[f(x)\,g(x)]\cdot h(x) = a_0b_0c_0x^{n+m+l} + (a_0b_0c_1 + a_0b_1c_0 + a_1b_0c_0)x^{n+m+l-1} + \ldots + a_nb_mc_l. \qquad (4)$$

С другой стороны:

$$g(x)\,h(x) = b_0c_0x^{m+l} + (b_0c_1 + b_1c_0)x^{m+l-1} + \ldots + b_mc_l,$$

откуда, пользуясь тем же правилом перемножения расположенных многочленов, имеем:

$$f(x)[g(x)h(x)] = a_0b_0c_0x^{n+m+l} + \\ + (a_0b_0c_1 + a_0b_1c_0 + a_1b_0c_0)x^{n+m+l-1} + \ldots + a_nb_mc_l,$$

т. е. мы пришли к тому же выражению (4); следовательно:

$$[f(x)g(x)]\cdot h(x) = f(x)\cdot[g(x)h(x)].$$

Наконец, разность двух многочленов из $P[x]$ всегда существует. А именно, чтобы получить $f(x) - g(x)$, надо в скобках правой части (2) вместо b_i писать $-b_i$.

Таким образом для множества $P[x]$ многочленов выполняются все аксиомы, характеризующие кольцо (см. главу III, § 22); *поэтому* $P[x]$ *образует кольцо, притом коммутативное.*

Обратимся теперь к четвёртому действию — к делению. Оно не всегда выполнимо, не всегда для двух многочленов $f(x)$, $g(x)$ можно подобрать такой третий многочлен $h(x)$, чтобы $f(x) = g(x)h(x)$. Например, $f(x) = x^3 + 1$ не делится на $g(x) = x - 1$. Таким образом $P[x]$—кольцо, но не поле.

По отношению к делению многочлены кольца $P[x]$ во многом ведут себя как натуральные числа, а именно: имеют место следующие свойства.

1. *Если $f(x)$ и $g(x)$ — два многочлена и $g(x)$ не равно тождественно нулю*[1]*, то всегда можно подобрать такую пару многочленов $q(x)$ и $r(x)$, частное и остаток, что*

$$f(x) = g(x)q(x) + r(x), \tag{5}$$

причём степень $r(x)$ ниже степени $g(x)$.

Действительно, пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n,$$
$$g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_m.$$

Представляются две возможности: либо $n < m$, либо $n \geqslant m$. В первом случае можно положить $q(x) = 0$, $r(x) = f(x)$ и равенство (5) становится очевидным.

Во втором случае делим $f(x)$ на $g(x)$, пользуясь обычным правилом деления многочленов. А именно старший член многочлена $f(x)$ делим на старший член многочлена $g(x)$; получаем старший член частного. Затем вычитаем из делимого произведение делителя на старший член частного, в результате чего степень $f(x)$ понижается и т. д. Так действуя, мы, наконец, получим искомые частное и остаток. В частности, остаток может оказаться равным нулю. Тогда многочлен $f(x)$ мы будем называть *делящимся на $g(x)$*.

Мы подчёркиваем, что частное $q(x)$ и остаток $r(x)$ суть многочлены поля P. В самом деле, операция деления двух многочленов сводится к тому, что мы производим все четыре арифметические действия над их коэффициентами. Но P — поле; поэтому коэффициенты $q(x)$ и $r(x)$ должны также принадлежать полю P.

---

[1]) Многочлен равен тождественно нулю, если все его коэффициенты равны нулю.

II. *Если $f(x)$ делится на $g(x)$ и $g(x)$ делится на $h(x)$, то $f(x)$, также делится на $h(x)$.*

По определению делимости существуют такие два многочлена $\varphi(x)$ и $\psi(x)$, что

$$f(x)=\varphi(x)\,g(x),\quad g(x)=\psi(x)\,h(x).$$

Подставив теперь значение $g(x)$ из второго равенства в первое равенство, получим:

$$f(x)=\varphi(x)\,\psi(x)\,h(x),$$

или, обозначив $\varphi(x)\,\psi(x)$ через $q(x)$:

$$f(x)=q(x)\,h(x),$$

откуда ясно, что $f(x)$ делится на $q(x)$.

III. *Если $f(x)$ и $g(x)$ делятся на $h(x)$, то их сумма и разность также делятся на $h(x)$.*

В самом деле, если существуют такие два многочлена $\varphi(x)$ и $\psi(x)$, что

$$f(x)=\varphi(x)\,h(x),\quad g(x)=\psi(x)\,h(x),$$

то

$$f(x)\pm g(x)=q(x)\,h(x),$$

где $q(x)=\varphi(x)\pm\psi(x)$. Последнее равенство как раз свидетельствует о том, что $f(x)\pm g(x)$ делится на $h(x)$.

IV. *Если хотя бы один из многочленов $f(x)$, $g(x)$ делится на $h(x)$, то и их произведение $f(x)\,g(x)$ делится на $h(x)$.*

Доказательство ничем не отличается от предыдущего. Пусть, например, $g(x)$ делится на $h(x)$, т. е.

$$g(x)=\varphi(x)\,h(x).$$

Тогда, очевидно,

$$f(x)\,g(x)=q(x)\,h(x),$$

где $q(x)=f(x)\,\varphi(x)$, и свойство IV доказано.

Наконец, многочлены нулевой степени, т. е. постоянные $c\neq 0$, ведут себя по отношению к делению совершенно так же, как единица в области натуральных чисел. Мы имеем в виду следующее свойство:

V. *Всякий многочлен $f(x)$ делится на любой многочлен нулевой степени.*

Действительно, если

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n,$$

то

$$\frac{1}{c}f(x)=\frac{a_0}{c}x^n+\frac{a_1}{c}x^{n-1}+\ldots+\frac{a_n}{c}$$

есть снова многочлен с коэффициентами из поля P.

Однако аналогия между многочленами и натуральными числами оказывается гораздо более глубокой. Мы сейчас увидим, что алгоритм Эвклида и все следствия, вытекающие из него, дословно распространяются и на многочлены в поле P.

Пусть два многочлена $f(x)$ и $g(x)$ делятся на $h(x)$; многочлен $h(x)$ называется *общим делителем* $f(x)$ и $g(x)$. В частности, $h(x)$ называется *наибольшим общим делителем*, если $h(x)$ делится на всякий общий делитель $f(x)$ и $g(x)$. Может случиться, что наибольшим общим делителем будет многочлен нулевой степени, т. е. постоянное; мы будем говорить тогда, что $f(x)$ и $g(x)$ *взаимно просты*.

Как и в случае натуральных чисел, условимся наибольший общий делитель $f(x)$ и $g(x)$ обозначать сокращённым символом $(f(x), g(x))$. При этом запись $(f(x), g(x)) = 1$ будет выражать, что $f(x)$ и $g(x)$ взаимно просты.

Покажем, что алгоритм Эвклида имеет место и для многочленов. Пусть степень $f(x)$ выше или в крайнем случае равна степени $g(x)$. Делим $f(x)$ на $g(x)$; остаток и частное, полученные при делении, обозначим соответственно через $r_1(x)$ и $q_1(x)$. Затем делим $g(x)$ на остаток $r_1(x)$, получим второй остаток $r_2(x)$ и частное $q_2(x)$. Снова делим $r_1(x)$ на $r_2(x)$ и получаем третий остаток $r_3(x)$ и частное $q_3(x)$ и т. д. Вообще мы каждый раз делим предыдущий остаток на последующий. При этом степени остатков $r_1(x)$, $r_2(x)$, $r_3(x)$, ... всё время убывают; следовательно, мы неизбежно должны притти к такому остатку $r_k(x)$, на который целиком разделится предыдущий остаток $r_{k-1}(x)$. Если бы это не имело места, то процесс деления продолжался бы без конца и мы получили бы нелепость: степени остатков убывают без конца.

Весь процесс деления можно записать в следующем виде:

$$\left.\begin{aligned} f(x) &= g(x)\,q_1(x) + r_1(x),\\ g(x) &= r_1(x)\,q_2(x) + r_2(x),\\ &\cdots\cdots\cdots\cdots\cdots\\ r_{k-2}(x) &= r_{k-1}(x)\,q_k(x) + r_k(x),\\ r_{k-1}(x) &= r_k(x)\,q_{k+1}(x). \end{aligned}\right\} \qquad (6)$$

А теперь, повторяя дословно рассуждения § 27, убеждаемся в том, что последний остаток $r_k(x)$ есть наибольший общий делитель $f(x)$ и $g(x)$: $(f(x), g(x)) = r_k(x)$.

Возникает, однако, вопрос, — является ли наибольший общий делитель $f(x)$, $g(x)$, найденный с помощью алгоритма Эвклида, единственным или же существуют и другие наибольшие общие делители? Оказывается, что $r_k(x)$ будет единственным только в том случае, если многочлены, отличающиеся друг от друга постоянным множителем, считать условно одинаковыми. Иными словами: *наибольший общий делитель* $f(x)$ и $g(x)$ *определяется с точностью до постоянного множителя.*

Для доказательства предположим, что $d_1(x)$ и $d_2(x)$ — два каких-нибудь наибольших общих делителя; их степени обозначим соответственно через n_1 и n_2. По определению наибольшего общего делителя $d_1(x)$ должно делиться на $d_2(x)$, т. е. существует такой многочлен $s(x)$, что

$$d_1(x) = d_2(x)\,s(x). \qquad (7)$$

С другой стороны, $d_2(x)$ как наибольший общий делитель должно делиться на $d_1(x)$, т. е.

$$d_2(x) = d_1(x)\, t(x). \tag{8}$$

Покажем, что $s(x)$ и $t(x)$ — постоянные. Из тождества (7) следует, что $n_2 \leqslant n_1$, а из (8), что $n_1 \leqslant n_2$. Но неравенства $n_2 \leqslant n_1$, $n_1 \leqslant n_2$ как раз свидетельствуют о том, что $n_1 = n_2$, а это возможно лишь тогда, когда $s(x)$ и $t(x)$ суть постоянные. Наше утверждение доказано.

Пример. Найдём наибольший общий делитель многочленов:

$$f(x) = x^4 - 2x^3 - 4x^2 + 4x - 3,$$
$$g(x) = 2x^3 - 5x^2 - 4x + 3.$$

Делим $f(x)$ на $g(x)$; чтобы избежать дробных коэффициентов при делении, умножим $f(x)$ предварительно на 2:

$$\begin{array}{l|l} 2x^4 - 4x^3 - 8x^2 + 8x - 6 & 2x^3 - 5x^2 - 4x + 3 \\ \underline{2x^4 - 5x^3 - 4x^2 + 3x} & \quad x \\ x^3 - 4x^2 + 5x - 6 & \end{array}$$

Теперь, чтобы избежать дробных коэффициентов, умножим полученную разность на 2. Правда, мы тем самым портим частное, но нас интересует не частное, а остаток. Разность $x^3 - 4x^2 + 5x - 6$ множится на постоянное число 2, но это допустимо, так как наибольший общий делитель определяется с точностью до постоянного множителя. Итак, продолжаем вычисления:

$$\begin{array}{l|l} 2x^4 - 4x^3 - 8x^2 + 8x - 6 & 2x^3 - 5x^2 - 4x + 3 \\ \underline{2x^4 - 5x^3 - 4x^2 + 3x} & \quad x + 1 \\ x^3 - 4x^2 + 5x - 6 & \end{array}$$

(умножаем на 2)

$$\begin{array}{r} 2x^3 - 8x^2 + 10x - 12 \\ \underline{2x^3 - 5x^2 - 4x + 3} \\ -3x^2 + 14x - 15 \end{array}.$$

С точностью до постоянного множителя многочлен

$$r_1(x) = -3x^2 + 14x - 15$$

есть остаток от деления $f(x)$ на $g(x)$.

Делим $g(x)$ на $r_1(x)$. Опять, чтобы избежать дробей, множим $g(x)$ на 3:

$$\begin{array}{l|l} 6x^3 - 15x^2 - 12x + 9 & -3x^2 + 14x - 15 \\ \underline{6x^3 - 28x^2 + 30x} & \quad -2x - 13 \\ 13x^2 - 42x + 9 & \end{array}$$

(умножаем на 3)

$$\begin{array}{r} 39x^2 - 126x + 27 \\ \underline{39x^2 - 182x + 195} \\ 56x - 168 = 56(x - 3). \end{array}$$

Как видим, получился остаток $56(x-3)$, который удобнее сократить на 56. Таким образом с точностью до постоянного множителя

$$r_2(x) = x - 3.$$

Делим $r_1(x)$ на $r_2(x)$:

$$\begin{array}{r|l} -3x^2+14x-15 & x-3 \\ \hline -3x^2+9x & -3x+5 \\ \hline 5x-15 & \\ 5x-15 & \\ \hline 0 & \end{array}$$

Мы видим, что $r_1(x)$ разделилось нацело на $r_2(x)$; следовательно $r_2(x) = x-3$ есть с точностью до постоянного множителя наибольший общий делитель $f(x)$ и $g(x)$.

Задача. Найти наибольший общий делитель многочленов:

а) $f(x) = x^5 - x^2 - x + 1$, $\quad g(x) = x^4 - 2x^3 - 4x^2 + 2x + 3$,

b) $f(x) = x^5 + x^4 + x^3 + x^2 + 1$, $\quad g(x) = 5x^4 + 4x^3 + 3x^2 + 2x$.

Переходим к следствиям, вытекающим из алгоритма Эвклида. Прежде всего укажем теорему, аналогичную теореме I § 27.

Теорема I. *Если $D(x)$ — наибольший общий делитель многочленов $f(x)$ и $g(x)$; то всегда можно подобрать два таких новых многочлена $\varphi(x)$ и $\psi(x)$, что*

$$f(x)\varphi(x) + g(x)\psi(x) = D(x). \tag{9}$$

Доказательство. Возьмём предпоследнее равенство (6) и перенесём произведение $r_{k-1}(x)\,q_k(x)$ в левую часть. Тогда, принимая во внимание, что $r_k(x) = cD(x)$, получим:

$$r_{k-2}(x) - r_{k-1}(x)\,q_k(x) = cD(x). \tag{10}$$

Но из равенства

$$r_{k-3}(x) = r_{k-2}(x)\,q_{k-1}(x) + r_{k-1}(x)$$

следует, что

$$r_{k-1}(x) = r_{k-3}(x) - r_{k-2}(x)\,q_{k-1}(x),$$

откуда, подставляя это значение $r_{k-1}(x)$ в (10), после очевидных преобразований имеем:

$$r_{k-2}(x)\,[1 + q_k(x)\,q_{k-1}(x)] - r_{k-3}(x)\,q_k(x) = cD(x),$$

или, обозначив $1 + q_k(x)\,q_{k-1}(x)$ через $\varphi_1(x)$, а $-q_k(x)$ — через $\psi_1(x)$:

$$r_{k-2}(x)\,\varphi_1(x) + r_{k-3}(x)\,\psi_1(x) = cD(x). \tag{11}$$

Вторично прибегаем к этому же приёму, а именно: из

$$r_{k-4}(x) = r_{k-3}(x)\,q_{k-2}(x) + r_{k-2}(x)$$

определяем $r_{k-2}(x)$ и подставляем в (11), в результате чего получим:

$$r_{k-3}(x)\,\varphi_2(x) + r_{k-4}(x)\,\psi_2(x) = cD(x),$$

и так продолжаем далее. В конце концов мы, очевидно, придём к равенству:

$$f(x)\varphi_k(x)+g(x)\psi_k(x)=cD(x),$$

или

$$f(x)\frac{\varphi_k(x)}{c}+g(x)\frac{\psi_k(x)}{c}=D(x).$$

Полагая $\frac{\varphi_k(x)}{c}=\varphi(x)$, $\frac{\psi_k(x)}{c}=\psi(x)$, получим (9).

Пример. Многочлены

$$f(x)=x^4+1,\quad g(x)=x^3-1$$

взаимно просты, т. е. их наибольшим общим делителем является постоянное, в частности единица. В этом нетрудно убедиться с помощью алгоритма Эвклида. Следовательно, должны существовать такие $\varphi(x)$ и $\psi(x)$, для которых

$$f(x)\varphi(x)+g(x)\psi(x)\equiv 1.$$

Найдём, чему равны многочлены $\varphi(x)$ и $\psi(x)$; заметим, что в данном случае существенное значение имеют не только остатки, но и частные, получаемые в процессе последовательного деления; поэтому делить следует *точно*, сокращать или умножать на постоянное число нельзя, так как от этого частные исказятся. Итак, применяем алгоритм Эвклида точно. Делим $f(x)$ на $g(x)$, затем $g(x)$ на остаток $r_1(x)$, $r_1(x)$ на $r_2(x)$ и т. д. Весь процесс деления можно записать в виде следующей схемы:

$$f(x)=g(x)\cdot x+(x+1),$$
$$g(x)=(x+1)\cdot(x^2-x+1)-2.$$

Результат деления $r_1(x)$ на $r_2(x)$ не записываем, — это излишне. А теперь, следуя общей теории, решаем последнее равенство относительно $r_2(x)=-2$:

$$-2=g(x)-(x+1)(x^2-x+1).$$

Затем решаем первое равенство относительно $r_1(x)=x+1$:

$$x+1=f(x)-g(x)\cdot x,$$

откуда

$$-2=g(x)-[f(x)-g(x)\cdot x](x^2-x+1)$$

или после очевидных преобразований:

$$f(x)\cdot\left(-\frac{1}{2}\right)(x^2-x+1)+g(x)\cdot\left(-\frac{1}{2}\right)(x^3-x^2+x+1)=1;$$

таким образом

$$\varphi(x)=-\frac{1}{2}(x^2-x+1),\quad \psi(x)=-\frac{1}{2}(x^3-x^2+x+1).$$

Следствие 1. *Если $f(x)$ и $g(x)$ взаимно просты с $h(x)$, то их произведение также взаимно просто с $h(x)$.*

Действительно, по доказанной теореме I можно подобрать такие $\varphi(x)$, $\psi(x)$, что

$$f(x)\varphi(x)+h(x)\psi(x)=1.$$

Умножим обе части этого равенства на $g(x)$. Получим:

$$f(x)g(x)\varphi(x)+h(x)g(x)\psi(x)=g(x). \qquad (12)$$

Мы утверждаем, что произведение $f(x)g(x)$ взаимно просто с $h(x)$:

$$(f(x)g(x),\ h(x))=1.$$

В самом деле, если бы $f(x)g(x)$ и $h(x)$ имели общим делителем многочлен $d(x)$, отличный от постоянной, то левая часть равенства (12) делилась бы на $d(x)$, а потому на $d(x)$ делилась бы правая часть, т. е. $g(x)$. Но тогда мы имели бы, что $g(x)$ и $h(x)$ не взаимно просты, что противоречит нашему предположению.

Это следствие обобщается без особого труда на любое число многочленов. А именно:

Следствие 2. *Если $f_1(x)$, $f_2(x)$, ..., $f_k(x)$ взаимно просты с $h(x)$, то и произведение $f_1(x)f_2(x)\dots f_k(x)$ взаимно просто с $h(x)$.*

Прежде всего ясно в силу следствия 1, что $f_1(x)f_2(x)$ взаимно просто с $h(x)$. Но если $f_1(x)f_2(x)$ и $f_3(x)$ взаимно просты с $h(x)$, то в силу того же следствия произведение

$$[f_1(x)f_2(x)]f_3(x)=f_1(x)f_2(x)f_3(x)$$

также должно быть взаимно просто с $h(x)$ и т. д. Действуя так, мы в конце концов докажем, что $f_1(x)f_2(x)\dots f_k(x)$ взаимно просто с $h(x)$.

Следствие 3. *Если $f(x)$ взаимно просто $h(x)$ и произведение $f(x)g(x)$ делится на $h(x)$, то $g(x)$ делится на $h(x)$.*

Снова, как и выше, пишем

$$f(x)\varphi(x)+h(x)\psi(x)=1,$$

и умножаем обе части этого равенства на $g(x)$. Получим:

$$f(x)g(x)\varphi(x)+h(x)g(x)\psi(x)=g(x).$$

Левая часть последнего равенства делится на $h(x)$, потому что в состав первого слагаемого входит множитель $f(x)g(x)$, делящийся на $h(x)$, а в состав второго слагаемого входит множителем само $h(x)$. Следовательно, на $h(x)$ должна делиться и правая часть, т. е. $g(x)$.

В § 27 мы рассмотрели понятие простого числа. Что же здесь соответствует этому понятию? Оказывается, что роль простого числа будут играть так называемые *неприводимые многочлены*.

Определение. *Многочлен $f(x)$, отличный от постоянной, называется приводимым (в поле P), если $f(x)$ разлагается на произведение двух многочленов $g(x)$ и $h(x)$ в поле P, отличных от постоянной:*

$$f(x)=g(x)h(x).$$

Если же $f(x)$ не может быть разложено на такое произведение, то многочлен $f(x)$ называется неприводимым (в поле P).

Пример 1. Покажем неприводимость многочлена

$$f(x) = x^2 - 2$$

в поле рациональных чисел. Пусть, напротив, $f(x)$ приводимо в поле рациональных чисел; тогда должны существовать такие два многочлена $g(x)$, $h(x)$ с рациональными коэффициентами и отличные от постоянной, что

$$f(x) = g(x)\,h(x). \tag{13}$$

Но равенство (13) возможно лишь тогда, когда $g(x)$ и $h(x)$ многочлены первой степени:

$$g(x) = ax + b,\ h(x) = cx + d.$$

Следовательно:

$$x^2 - 2 = (ax + b)(cx + d).$$

Если в последнее равенство подставить $x = -\frac{b}{a}$, то правая часть обратится в нуль. Таким образом

$$\frac{b^2}{a^2} - 2 = 0.$$

Мы пришли к нелепости: $\pm\sqrt{2}$ равен рациональному числу $\pm\frac{b}{a}$.

Этот же многочлен, однако, оказывается приводимым в поле действительных чисел, так как $x^2 - 2$ можно разложить на произведение многочленов с иррациональными коэффициентами:

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

Пример 2. Рассмотрим многочлен первой степени $ax + b$ с коэффициентами из поля P. Он неприводим в поле P. В самом деле, пусть $g(x)$ и $h(x)$ какие-нибудь многочлены, отличные от постоянной. Их произведение может быть многочленом второй, третьей, четвёртой и т. д. степени, но никак не первой степени.

Неприводимый[1]) многочлен обладает следующими важными свойствами.

I. *Если неприводимый многочлен $p_1(x)$ делится на другой неприводимый многочлен $p_2(x)$, то $p_1(x)$ и $p_2(x)$ совпадают с точностью до постоянного множителя.*

Действительно, по определению делимости

$$p_1(x) = p_2(x)\,h(x).$$

Многочлен $h(x)$ должен быть равен постоянной, так как иначе $p_1(x)$ было бы приводимым. Итак, $h(x) = c$, откуда $p_1(x) = cp_2(x)$, что и требовалось показать.

II. *Если $f(x)$ не делится на неприводимый многочлен $p(x)$, то $f(x)$ и $p(x)$ взаимно просты. Обратно, если $f(x)$ и $p(x)$ взаимно просты, то $f(x)$ не делится на $p(x)$.*

[1]) Здесь и ниже речь идёт о многочленах, неприводимых в поле P.

Обозначим общий наибольший делитель $f(x)$ и $p(x)$ через $d(x)$. Тогда имеем:

$$f(x) = d(x)\varphi(x), \quad p(x) = d(x)\psi(x).$$

Так как $p(x)$ неприводимо, то представляются только две возможности: либо 1) $\psi(x)$ есть постоянное, либо 2) $d(x)$ есть постоянное.

Но первый случай невозможен, так как если $\psi(x) = c$, то $p(x)$ будет совпадать с общим наибольшим делителем $d(x)$ с точностью до постоянной: $p(x) = cd(x)$, а потому $p(x)$ будет делителем $f(x)$, что невозможно. Таким образом остаётся лишь второй случай. Но если $d(x) = c$, то $f(x)$ и $p(x)$ взаимно просты.

Обратное очевидно, потому что $f(x)$ делится на $p(x)$ только тогда, когда общий наибольший делитель $f(x)$ и $p(x)$ равен $p(x)$, а не постоянной.

III. *Если многочлены* $f_1(x), f_2(x), \ldots, f_k(x)$ *не делятся на неприводимый многочлен* $p(x)$, *то и произведение этих многочленов* $f_1(x) f_2(x) \ldots f_k(x)$ *не делится на* $p(x)$.

В самом деле, поскольку $f_1(x), f_2(x), \ldots, f_k(x)$ не делятся на $p(x)$, они в силу свойства II неприводимого многочлена должны быть взаимно просты с $p(x)$; отсюда в силу следствия 2 теоремы 1 их произведение $f_1(x) f_2(x) \ldots f_k(x)$ должно быть взаимно просто с $p(x)$, т. е. $f_1(x) f_2(x) \ldots f_k(x)$ не делится на $p(x)$.

IV. *Если произведение* $f(x) g(x)$ *делится на неприводимый многочлен* $p(x)$, *то по крайней мере один из сомножителей делится на* $p(x)$.

Допустим, например, что $f(x)$ не делится на $p(x)$. Тогда в силу свойства II неприводимого многочлена и следствия 3 теоремы 1 $g(x)$ делится на $p(x)$. Само собою разумеется, что свойство IV можно распространить на произведение любого числа множителей.

Итак, неприводимый многочлен $p(x)$ ведёт себя как простое число. Мы сейчас покажем, что теорема о разложении § 27 почти дословно распространяется и на многочлены.

Теорема II. *Всякий многочлен* $f(x)$, *отличный от постоянной, может быть разложен на произведение неприводимых множителей*

$$f(x) = p_1(x) p_2(x) \ldots p_r(x) \tag{14}$$

[$p_i(x)$ — *неприводимы*], *и это разложение является единственным с точностью до постоянного множителя* [1]).

Доказательство. Для неприводимого $f(x)$ теорема очевидна, так как в этом случае разложение (14) будет состоять лишь из одного неприводимого множителя:

$$f(x) = f(x).$$

[1]) Иными словами, если

$$f(x) = q_1(x) q_2(x) \ldots q_s(x)$$

какое-нибудь другое разложение $f(x)$ на неприводимые множители, то

$$s = r, \; q_1(x) = c_1 p_1(x), \ldots, q_r(x) = c_r p_r(x) \quad (c_1 c_2 \ldots c_r = 1).$$

Кроме того, теорема верна и для многочленов $ax + b$ первой степени. В самом деле, мы выше показали, что многочлен $ax + b$ неприводим.

Докажем теперь нашу теорему методом полной индукции. Пусть теорема верна для всех многочленов, у которых степень меньше n. Докажем справедливость теоремы и для многочлена степени n.

Если $f(x)$ многочлен n-й степени, то представляются только две возможности: либо 1) $f(x)$ неприводим, либо 2) $f(x)$ приводим. Для первого случая, как мы выше указали, теорема очевидна. Таким образом, остаётся разобрать второй случай:

Раз $f(x)$ приводимо, то

$$f(x) = f_1(x) f_2(x), \tag{15}$$

где $f_1(x)$ и $f_2(x)$—многочлены, отличные от постоянной. Очевидно, что степень $f_1(x)$ и $f_2(x)$ меньше n; следовательно, для них теорема верна, т. е.

$$f_1(x) = p_1(x) p_2(x) \dots p_k(x),$$
$$f_2(x) = p_{k+1}(x) p_{k+2}(x) \dots p_r(x).$$

Подставляя эти значения $f_1(x)$ и $f_2(x)$ в (15), получим:

$$f(x) = p_1(x) p_2(x) \dots p_r(x). \tag{16}$$

Остаётся доказать единственность разложения на неприводимые множители. Пусть для $f(x)$, кроме (16), существует ещё такое разложение:

$$f(x) = q_1(x) q_2(x) \dots q_s(x) \tag{17}$$

[$q_i(x)$ — неприводимы]. Сравнивая (16) и (17), получаем:

$$p_1(x) p_2(x) \dots p_r(x) = q_1(x) q_2(x) \dots q_s(x). \tag{18}$$

Левая часть равенства (18) делится на $p_1(x)$, так как в число её множителей входит $p_1(x)$; следовательно, на $p_1(x)$ должна делиться и правая часть. Отсюда в силу свойства IV неприводимого многочлена вытекает, что на $p_1(x)$ должен делиться, по крайней мере, один из сомножителей правой части. Не нарушая общности рассуждений, можно предположить, что $q_1(x)$ делится на $p_1(x)$, так как иначе мы изменили бы порядок следования множителей $q_1(x)$, $q_2(x)$, ..., $q_s(x)$. Но если $q_1(x)$ делится на $p_1(x)$, то $q_1(x) = c_1 p_1(x)$ (см. свойство 1 неприводимого многочлена, стр. 152). Подставляя это значение $q_1(x)$ в равенство (18), будем иметь:

$$p_1(x) p_2(x) \dots p_r(x) = c_1 p_1(x) q_2(x) \dots q_s(x),$$

или, сокращая на $p_1(x)$:

$$p_2(x) \dots p_r(x) = c_1 q_2(x) \dots q_s(x). \tag{19}$$

Как правую, так и левую часть равенства (19) можно рассматривать как разложение многочлена $g(x) = \frac{f(x)}{p_1(x)}$ на неприводимые множители. Степень $g(x)$, очевидно, меньше n; поэтому для $g(x)$ тео-

рема по предположению верна. Стало быть, $g(x)$ разлагается единственным образом на неприводимые множители с точностью до постоянной. Не нарушая общности, можно принять, что с точностью до постоянного множителя $p_2(x)$ совпадает с $q_2(x)$, $p_3(x)$ совпадает с $q_3(x)$ и т. д., так как иначе мы в правой части (19) изменили бы порядок следования многочленов $q_2(x), \ldots, q_s(x)$. Итак:

$$s-1=r-1, \text{ или } s=r;\ q_2(x)=c_2p_2(x), \ldots, q_r(x)=c_rp_r(x),$$

или, присоединяя ещё равенство $q_1(x)=c_1p_1(x)$, полученное выше:

$$s=r,\ q_1(x)=c_1p_1(x),\ q_2(x)=c_2p_2(x), \ldots,\ q_r(x)=c_rp_r(x),$$

т. е. мы доказали единственность разложения.

А теперь видно, что теорема справедлива для любых степеней. Действительно теорема верна для многочленов $ax+b$ первой степени, поэтому по доказанному она верна и для многочленов второй степени; но если она верна для многочленов первой и второй степени, то она верна и для многочленов третьей степени и т. д.

Теорема о разложении играет исключительную роль в алгебре. Неприводимые множители $p_i(x)$ могут в разложении $f(x)$ встречаться несколько раз. Пусть $p_1(x)$ встречается α_1 раз, $p_2(x)$ встречается α_2 раз и т. д. Тогда разложение $f(x)$ на неприводимые множители примет следующий окончательный вид:

$$f(x)=cp_1^{\alpha_1}(x)p_2^{\alpha_2}(x)\ldots p_r^{\alpha_r}(x),$$

причём $p_i(x)$ уже все различны.

Введём следующее определение.

Определение. *Говорят, что многочлен $g(x)$ входит в многочлен $f(x)$ с кратностью α, если $f(x)$ делится на $g^{\alpha}(x)$, но не делится на $g^{\alpha+1}(x)$.*

Таким образом $p_1(x)$, $p_2(x)$, ..., $p_r(x)$ входят в разложение $f(x)$ с кратностями $\alpha_1, \alpha_2, \ldots, \alpha_r$. Ввиду важности последнего определения приведём несколько примеров.

Пример 1. Легко видеть, что $g(x)=x+1$ входит в $f(x)=x^2-1$ с кратностью, равной единице, так как x^2-1 делится на $x+1$, но не делится на $(x+1)^2$.

Пример 2. Многочлен $g(x)=x^2-2$ входит в $f(x)=x^7-4x^5+x^4+4x^3-4x^2+4$ с кратностью 2, так как $f(x)$ делится на $g^2(x)$, но не делится на $g^3(x)$.

Может случиться, что в разложении $f(x)$ на неприводимые множители все α_i равны единице. Мы в этом случае будем говорить, что $f(x)$ разлагается на однократные множители. Существует определённый метод, позволяющий узнать, разлагается ли $f(x)$ на однократные или многократные множители.

§ 29. Ряд Тэйлора и производные

Ближайшей нашей целью является решение следующей задачи: дан многочлен

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n, \tag{1}$$

требуется узнать, имеет ли $f(x)$ многократные множители.

Решение задачи основано на рассмотрении производной. В анализе производной от функции $f(x)$ называется предел отношения $\frac{f(x+h)-f(x)}{h}$ при $h \to 0$; впрочем, для многочленов можно дать другое определение производной, совершенно независимое от понятий предела и непрерывности.

Подставим в (1) вместо x сумму $x+h$. Тогда будем иметь

$$f(x+h) = a_0(x+h)^n + a_1(x+h)^{n-1} + \ldots + a_{n-1}(x+h) + a_n.$$

Если теперь скобки раскрыть по биному Ньютона, сгруппировать вместе члены с одинаковыми степенями h и, наконец, вынести за скобку общие множители, то получится:

$$\left.\begin{aligned} f(x+h) = (a_0x^n + a_1x^{n-1} + \ldots + a_n) + \\ + h\,[na_0x^{n-1} + (n-1)\,a_1x^{n-2} + \ldots + a_{n-1}] + \\ + \frac{h^2}{1\cdot 2}[n(n-1)\,a_0x^{n-2} + (n-1)(n-2)\,a_1x^{n-3} + \ldots + 2a_{n-2}] + \\ + \ldots + \frac{h^n}{1\cdot 2\ldots n}\,n!\,a_0. \end{aligned}\right\} \quad (2)$$

Мы видим, что в первой скобке находится не что иное, как $f(x)$. Что касается выражения, находящегося во второй скобке, то оно получается из $f(x)$ по весьма простому правилу. Умножим каждый член $f(x)$ на показателя его степени, понизим степень члена на 1 и преобразованные таким образом члены сложим; получится как раз выражение, стоящее во второй скобке [1]).

Обозначим многочлен во второй скобке через $f'(x)$ и назовём его *производной*, или, точнее, *первой производной* от $f(x)$. Итак:

$$f'(x) = na_0x^{n-1} + (n-1)\,a_1x^{n-2} + \ldots + a_{n-1}.$$

Это определение производной для нас весьма существенно, так как оно сохраняет свой смысл для таких полей P, к которым понятия непрерывности и предела неприменимы.

Пример 1. Найдём, чему равна производная от

$$f(x) = x^3 - 5x^2 + 3x - 1,$$

или, как принято говорить, продифференцируем $f(x)$.

По указанному правилу легко определяем, что

$$f'(x) = 3\cdot x^{3-1} + 2\cdot(-5x^{2-1}) + 1\cdot(3x^{1-1}) + 0\cdot(-1\cdot x^{0-1}) = \\ = 3x^2 - 10x + 3.$$

Пример 2. Производная от

$$f(x) = 7x^3 - 5x^2 + 10x - 8$$

равна

$$f'(x) = 21x^2 - 10x + 10.$$

---

[1]) В частности, свободный член a_n следует умножить на нуль, так как степень члена a_n равна нулю.

Пример 3. Рассмотрим многочлен

$$f(x) = ax^n \qquad (n > 0),$$

состоящий только из одного члена. Его производная, очевидно, равна $f'(x) = nax^{n-1}$. В частности, когда $n = 0$, т. е. когда $f(x)$ есть постоянное: $f(x) = ax^0 = a$, имеем $f'(x) = 0 \cdot ax^{0-1} = 0$. Мы видим, что *производная от постоянного равна нулю*—вывод, которым мы впоследствии воспользуемся.

В свою очередь, назовём производную от $f'(x)$ *второй производной* и обозначим через $f''(x)$, производную от $f''(x)$ назовём *третьей производной* и обозначим через $f'''(x)$ и т. д.; вообще производную от $f^{(k-1)}(x)$ мы назовём k-й производной и обозначим через $f^{(k)}(x)$[1]). Таким образом

$$\begin{aligned}
f''(x) &= (n-1)\,na_0x^{n-2} + (n-2)(n-1)\,a_1x^{n-3} + \ldots + 1 \cdot 2a_{n-2},\\
f'''(x) &= (n-2)(n-1)\,na_0x^{n-3} + (n-3)(n-2)(n-1)\,a_1x^{n-4} + \\
&\qquad + \ldots + 1 \cdot 2 \cdot 3a_{n-3},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
f^{(n-1)}(x) &= 2 \cdot 3 \cdot 4 \ldots (n-1)\,na_0x,\\
f^{(n)}(x) &= 1 \cdot 2 \cdot 3 \cdot 4 \ldots (n-1)\,na_0.
\end{aligned}$$

Последняя производная $f^{(n)}(x)$ уже не зависит от x.

Но мы видим, что в третьей скобке правой части равенства (2) стоит $f''(x)$, в четвёртой скобке стоит $f'''(x)$ и т. д., наконец, в $(n+1)$-й скобке стоит $f^{(n)}(x)$. Следовательно:

$$f(x+h) = f(x) + hf'(x) + \frac{h^2}{2!}f''(x) + \ldots + \frac{h^n}{n!}f^{(n)}(x). \qquad (3)$$

Получился так называемый ряд Тэйлора (Taylor). Он позволяет выразить значение $f(x+h)$ через $f(x)$, $f'(x)$, $\ldots$, $f^{(n)}(x)$.

Необходимо отметить, что *ряд Тэйлора является единственным разложением* $f(x+h)$ *по степеням* h. Точнее: *если*

$$f(x+h) = \varphi(x) + h\varphi_1(x) + \frac{h^2}{2!}\varphi_2(x) + \ldots + \frac{h^n}{n!}\varphi_n(x) \qquad (4)$$

какое-нибудь разложение $f(x+h)$ *по степеням* h, *то*

$$\varphi(x) = f(x),\ \varphi_1(x) = f'(x),\ \varphi_2(x) = f''(x),\ \ldots,\ \varphi_n(x) = f^{(n)}(x).$$

Для доказательства этого утверждения вычтем из (4) равенство (3). Получим:

$$[\varphi(x) - f(x)] + h[\varphi_1(x) - f'(x)] + \ldots + \frac{h^n}{n!}[\varphi_n(x) - f^{(n)}(x)] = 0. \qquad (5)$$

Полагая в (5) $h = 0$, будем иметь:

$$\varphi(x) - f(x) = 0, \text{ или } \varphi(x) = f(x),$$

---

[1]) Индекс k заключается в скобки для того, чтобы указатель порядка производной нельзя было принять за показатель степени.

после чего (5) принимает вид:

$$h[\varphi_1(x)-f'(x)]+\frac{h^2}{2!}[\varphi_2(x)-f''(x)]+\ldots+\frac{h^n}{n!}[\varphi_n(x)-f^{(n)}(x)]=0,$$

или по сокращении на h:

$$[\varphi_1(x)-f'(x)]+\frac{h}{2!}[\varphi_2(x)-f''(x)]+\ldots+\frac{h^{n-1}}{n!}[\varphi_n(x)-f^{(n)}(x)]=0.$$

Снова полагаем $h=0$ и получаем:

$$\varphi_1(x)-f'(x)=0, \text{ или } \varphi_1(x)=f'(x),$$

после чего имеем:

$$\frac{h}{2!}[\varphi_2(x)-f''(x)]+\ldots+\frac{h^{n-1}}{n!}[\varphi_n(x)-f^{(n)}(x)]=0,$$

или, сокращая на h:

$$\frac{1}{2!}[\varphi_2(x)-f''(x)]+\ldots+\frac{h^{n-2}}{n!}[\varphi_n(x)-f^{(n)}(x)]=0.$$

Опять полагаем $h=0$ и т. д. Дальнейший ход доказательства ясен.

Ряд Тэйлора иногда полезно записывать в несколько иной форме. Изменим обозначения в (3): вместо x введём a и вместо $x+h$ введём x. Очевидно, что h придётся обозначить через $x-a$, и ряд Тэйлора примет вид:

$$f(x)=f(a)+(x-a)f'(a)+\frac{(x-a)^2}{2!}f''(a)+\ldots+\frac{(x-a)^n}{n!}f^{(n)}(a). \quad (6)$$

Пример 4. Пусть многочлен $f(x)$—четвёртой степени и все его производные при $x=0$ имеют значения:

$$f(0)=1, \quad f'(0)=-1, \quad f''(0)=2, \quad f'''(0)=3, \quad f^{IV}(0)=2.$$

Требуется найти $f(x)$.

Воспользуемся для этой цели формулой (6). В нашем примере, очевидно, $a=0$; следовательно:

$$f(x)=f(0)+xf'(0)+\frac{x^2}{2!}f''(0)+\frac{x^3}{3!}f'''(0)+\frac{x^4}{4!}f^{IV}(0).$$

или, после подстановки значений $f(0)$, $f'(0)$, $f''(0)$, $f'''(0)$, $f^{IV}(0)$:

$$f(x)=1-x+x^2+\frac{1}{2}x^3+\frac{1}{12}x^4.$$

Пример 5. Разложим

$$f(x)=x^5-3x^2+x-1$$

по степеням $x-1$. Предварительно дифференцируем $f(x)$:

$$f'(x)=5x^4-6x+1, \quad f''(x)=20x^3-6, \quad f'''(x)=60x^2,$$
$$f^{IV}(x)=120x, \quad f^{V}(x)=120,$$

откуда

$$f(1)=-2, \quad f'(1)=0, \quad f''(1)=14, \quad f'''(1)=60, \quad f^{IV}(1)=120,$$
$$f^{V}(1)=120.$$

Таким образом, руководствуясь формулой (6), получаем следующее разложение по степеням $(x-1)$:

$$f(x) = -2 + 7(x-1)^2 + 10(x-1)^3 + 5(x-1)^4 + (x-1)^5.$$

Задачи. 1. Найти многочлен пятой степени $f(x)$, если известно, что $f(1) = -1$, $f'(1) = 5$, $f''(1) = -2$, $f'''(1) = 6$, $f^{IV}(1) = 24$, $f^{V}(1) = 60$.

2. Разложить по степеням $x+1$:

a) $f(x) = x^6 - x^4 + x^3 - x^2 + x - 1$,

b) $f(x) = x^4 - 3x^3 + x^2 - x + 5$,

c) $f(x) = x^7 - x^6 + 5x^5 - x^4 + 4x^3 - x^2 + 2x - 1$.

3. Известно, что $f(x)$ есть многочлен третьей степени и

$$f(-1) = 1,\ f'(-1) = 2,\ f''(-1) = 3,\ f'''(-1) = 4.$$

Чему равно $f(0)$?

Вернёмся снова к рассмотрению свойств производной и докажем такую теорему.

Теорема. *Если $f(x)$ и $g(x)$—два каких-либо многочлена, то производная от $f(x)+g(x)$ равна $f'(x)+g'(x)$, а производная от $f(x)\,g(x)$ равна $f'(x)\,g(x)+f(x)\,g'(x)$; или иначе:*

$$[f(x)+g(x)]' = f'(x)+g'(x), \tag{7}$$

$$[f(x)\cdot g(x)]' = f'(x)\,g(x)+f(x)\,g'(x). \tag{8}$$

Доказательство. Формулы (7) и (8) известны в анализе под названием формул дифференцирования суммы и произведения; но мы их выведем чисто алгебраически. Напишем для $f(x+h)$ и $g(x+h)$ разложение в ряд Тэйлора по степеням h:

$$f(x+h) = f(x) + hf'(x) + \frac{h^2}{2!}f''(x) + \ldots + \frac{h^n}{n!}f^{(n)}(x),$$

$$g(x+h) = g(x) + hg'(x) + \frac{h^2}{2!}g''(x) + \ldots + \frac{h^n}{n!}g^{(n)}(x).$$

А теперь сложим и перемножим два последние равенства. Получим следующие разложения в ряд Тейлора по степеням h:

$$f(x+h)+g(x+h) = [f(x)+g(x)] + h[f'(x)+g'(x)] + \ldots,$$

$$f(x+h)\,g(x+h) = [f(x)\,g(x)] + h[f'(x)\,g(x)+f(x)\,g'(x)] + \ldots,$$

откуда становится очевидным, что производная от $f(x)+g(x)$ равна $f'(x)+g'(x)$, а производная от $f(x)\,g(x)$ равна $f'(x)\,g(x)+f(x)\,g'(x)$; иными словами, имеют место формулы (7) и (8).

Следствие 1. Доказанную теорему можно без труда распространить на любое число многочленов, т. е.

$$[f_1(x)+f_2(x)+\ldots+f_k(x)]' = f_1'(x)+f_2'(x)+\ldots+f_k'(x),$$

$$[f_1(x)\,f_2(x)\ldots f_k(x)]' = f_1'(x)\,f_2(x)\ldots f_k(x) + f_1(x)\,f_2'(x)\ldots f_k(x) + \ldots + f_1(x)\,f_2(x)\ldots f_k'(x).$$

Следствие 2. Легко видеть, что $[cf(x)]' = cf'(x)$, где c—постоянное.

В самом деле, к $cf(x)$ можно применить формулу (8):

$$[cf(x)]' = (c)' f(x) + cf'(x) = cf'(x),$$

так как производная от постоянной равна нулю (см. пример

Следствие 3. Точно так же нетрудно вывести правило дифференцирования степени $f^s(x)$ функции $f(x)$:

$$[f^s(x)]' = sf^{s-1}(x) f'(x).$$

Действительно, s-ю степень $f^s(x)$ можно рассматривать как произведение s одинаковых сомножителей, откуда в силу следствия 1:

$$[f^s(x)]' = \underbrace{[f(x) \dots f(x)]'}_{s \text{ раз}} = f'(x) f(x) \dots f(x) + f(x) f'(x) \dots f(x) +$$
$$+ \dots + f(x) f(x) \dots f'(x) = sf^{s-1}(x) f'(x).$$

§ 30. Отделение кратных множителей

Теперь мы можем приступить к решению задачи, поставленной в самом начале § 29. Прежде всего имеет место следующая теорема:

Теорема. *Если неприводимый многочлен $p(x)$ входит в $f(x)$ с кратностью α, то $p(x)$ в производную $f'(x)$ войдёт с кратностью $\alpha - 1$.*

Доказательство. Согласно определению кратных множителей (см. § 28, стр. 155)

$$f(x) = p^\alpha(x) f_1(x), \qquad (1$$

где $f_1(x)$ уже не делится на $p(x)$. Дифференцируем правую часть (1 применяя формулы (8) и (9) § 29

$$f'(x) = \alpha p^{\alpha-1}(x) p'(x) f_1(x) + p^\alpha(x) f_1'(x) =$$
$$= p^{\alpha-1}(x) [\alpha p'(x) f_1(x) + p(x) f_1'(x)].$$

Второе слагаемое в квадратной скобке делится на $p(x)$, но первое не делится, так как $f_1(x)$ и $p'(x)$ не делятся на $p(x)$[1]); следовательно, и вся сумма в квадратной скобке не может делиться на $p(x)$. Тем самым доказано, что $p(x)$ входит в $f'(x)$ с кратностью $\alpha - 1$.

В частности, из этой теоремы следует, что простые (однократные) множители $f(x)$ не входят вовсе в производную $f'(x)$.

Наша задача теперь решается без особого труда. Пусть данный многочлен $f(x)$ следующим образом разлагается на неприводимые множители:

$$f(x) = p_1^{\alpha_1}(x) p_2^{\alpha_2}(x) \dots p_r^{\alpha_r}(x).$$

Обозначим через X_1 произведение всех однократных неприводимых множителей; через X_2—произведение всех двукратных неприводимых множителей, взятых по одному разу; через X_3—произведение всех трёхкратных неприводимых множителей, взятых по одному

---

[1]) Вполне очевидно, что $p'(x)$ не может делиться на $p(x)$, потому что степень производной $p'(x)$ меньше (а именно на единицу) степени $p(x)$.

X_1, и т. д. Может случиться, что $f(x)$ не имеет однократных множителей, мы тогда будем считать $X_1=1$. Вообще мы будем считать $X_k=1$, если $f(x)$ не имеет k-кратных множителей. Если s есть наивысшая кратность множителей многочлена $f(x)$, то

$$f(x)=X_1X_2^2X_3^3\dots X_s^s.$$

Например; пусть $f(x)$ следующим образом разлагается на неприводимые множители в поле рациональных чисел [1]):

$$f(x)=(x^2-2)^3(x-1)(x+1)(x-2).$$

Очевидно, здесь

$$X_1=(x-1)(x+1)(x-2),\quad X_2=1,\quad X_3=(x^2-2),$$

откуда

$$f(x)=X_1X_2^2X_3^3.$$

В производной $f'(x)$ всякий неприводимый множитель по доказанной теореме имеет кратность на единицу меньшую, чем в $f(x)$. Следовательно, X_1 вовсе не войдёт в $f'(x)$, X_2 войдёт в первой степени, X_3—во второй степени и т. д. Таким образом

$$f'(x)=X_2X_3^2X_4^3\dots X_s^{s-1}\varphi_1(x),$$

где $\varphi_1(x)$ есть произведение собственных множителей производной, т. е. множителей, не входящих в данный многочлен $f(x)$.

Обозначим общий наибольший делитель $f(x)$ и $f'(x)$ через $d_1(x)$. Он, очевидно, состоит из тех и только тех множителей, которые являются общими для $f(x)$ и $f'(x)$. Следовательно:

$$d_1(x)=X_2X_3^2X_4^3\dots X_s^{s-1}.$$

По предыдущему, производная многочлена $d_1(x)$ должна иметь вид

$$d_1'(x)=X_3X_4^2\dots X_s^{s-2}\varphi_2(x),$$

откуда общим наибольшим делителем $d_1(x)$ и $d_1'(x)$ будет

$$d_2(x)=X_3X_4^2\dots X_s^{s-2}.$$

Затем рассматриваем

$$d_2'(x)=X_4X_5^2\dots X_s^{s-3}\varphi_3(x)$$

приходим точно так же к выводу, что общим наибольшим делителем $d_2(x)$ и $d_2'(x)$ является

$$d_3(x)=X_4X_5^2\dots X_s^{s-3}$$

т. д. Наконец, имеем:

$$d_{s-1}(x)=X_s,\quad d_s(x)=1.$$

[1]) Как мы знаем из § 28 линейные многочлены и двучлен x^2-2 неприводимы в поле рациональных чисел.

Далее составляем:

$$E_1=\frac{f(x)}{d_1(x)}=X_1X_2X_3\ldots X_{s-1}X_s,$$
$$E_2=\frac{d_1(x)}{d_2(x)}=\quad X_2X_3\ldots X_{s-1}X_s,$$
$$E_3=\frac{d_2(x)}{d_3(x)}=\qquad X_3\ldots X_{s-1}X_s,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$E_{s-1}=\frac{d_{s-2}(x)}{d_{s-1}(x)}=\qquad X_{s-1}X_s,$$
$$E_s=\frac{d_{s-1}(x)}{d_s(x)}=\qquad X_s,$$

после чего без труда находим, что

$$\frac{E_1}{E_2}=X_1,\quad \frac{E_2}{E_3}=X_2,\ \ldots,\quad \frac{E_{s-1}}{E_s}=X_{s-1},\quad E_s=X_s.$$

Итак, мы выделили $X_1, X_2, \ldots, X_s$ и потому задачу считать решённой. Если $X_k \neq 1$ ($k=1, 2, \ldots, s$), то многочлен $f(x)$ имеет k-кратные множители.

Пример. Выделим кратные множители многочлена

$$f(x)=x^4-\frac{1}{2}x+\frac{3}{16}.$$

Составляем производную:

$$f'(x)=4x^3-\frac{1}{2}.$$

Далее ищем общий наибольший делитель $f(x)$ и $f'(x)$, для чего пользуемся алгоритмом Эвклида. Предварительно освобождаемся от дробей; умножаем $f(x)$ на 16, а $f'(x)$ на 2 и затем приступаем к делению:

$$\begin{array}{l|l} 16x^4-8x+3 & 8x^3-1 \\ \cline{2-2} 16x^4-2x & 2x \\ \quad -6x+3 & \end{array}$$

(сокращаем на -3)

$$2x-1.$$

Делим $8x^3-1$ на $2x-1$:

$$\begin{array}{l|l} 8x^3 \qquad\quad -1 & 2x-1 \\ \cline{2-2} 8x^3-4x^2 & 4x^2+2x+1 \\ \hline \quad 4x^2-1 & \\ \quad 4x^2-2x & \\ \hline \qquad 2x-1 & \\ \qquad 2x-1 & \\ \hline \qquad\ \ 0 & \end{array}$$

Мы видим, что $8x^3-1$ разделилось на $2x-1$; следовательно,

$$d_1(x)=2x-1.$$

Далее, следуя общей теории, находим $d_1'(x)$:

$$d_1'(x) = 2,$$

откуда

$$d_2(x) = 1.$$

А теперь составляем E_1 и E_2:

$$E_1 = \frac{x^4 - \frac{1}{2}x + \frac{3}{16}}{2x - 1} = \frac{1}{2}x^3 + \frac{1}{4}x^2 + \frac{1}{8}x - \frac{3}{16},$$

$$E_2 = \frac{2x - 1}{1} = 2x - 1.$$

Наконец, делим E_1 на E_2:

$$\frac{E_1}{E_2} = \frac{\frac{1}{2}x^3 + \frac{1}{4}x^2 + \frac{1}{8}x - \frac{3}{16}}{2x - 1} = \frac{1}{4}x^2 + \frac{1}{4}x + \frac{3}{16},$$

откуда

$$X_1 = \frac{1}{4}x^2 + \frac{1}{4}x + \frac{3}{16}, \quad X_2 = 2x - 1.$$

Итак, $f(x)$ имеет однократные и двукратные множители:

$$f(x) = \left(\frac{1}{4}x^2 + \frac{1}{4}x + \frac{3}{16}\right)(2x - 1)^2.$$

Задача. Выделить кратные множители следующих многочленов:
a) $x^4 + x^3 - 3x^2 - 5x - 2$, b) $x^5 - 3x^4 + 4x^3 - 4x^2 + 3x - 1$,
c) $x^7 - 3x^6 + 5x^5 - 7x^4 + 7x^3 - 5x^2 + 3x - 1$, d) $x^3 - 4x^4 - 16x^2 + 16$.

§ 31. Понятие корня

В § 28 было установлено, что всякий многочлен $f(x)$, отличный от постоянной, разлагается на произведение неприводимых множителей:

$$f(x) = p_1^{\alpha_1}(x)\, p_2^{\alpha_2}(x) \ldots p_r^{\alpha_r}(x).$$

Но может случиться, что в состав этого разложения войдёт и линейный многочлен $x - a$ [1]). Возникает вопрос—когда это будет? Иными словами, когда $f(x)$ делится без остатка на $x - a$?

Разделим многочлен $f(x)$ на $x - a$. Вообще при делении должны получиться остаток r и частное $q(x)$; так как делитель есть многочлен первой степени, то остаток r будет многочленом нулевой степени, т. е. постоянным. Как известно, делимое равно произведению делителя и частного плюс остаток. Таким образом

$$f(x) = (x - a)\, q(x) + r \qquad (1)$$

(r—постоянное).

Деление на $x - a$ особенно просто выполняется при помощи ме-

[1]) Поскольку всё время речь идёт о многочленах в поле P, очевидно, a есть число из поля P.

тода Горнера, который состоит в следующем. Пусть

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n.$$

Очевидно, что частное от деления $f(x)$ на $(x-a)$ будет многочленом $(n-1)$-й степени:

$$q(x) = b_0x^{n-1} + b_1x^{n-2} + b_2x^{n-3} + \ldots + b_{n-1}.$$

Подставляя эти значения $f(x)$ и $q(x)$ в равенство (1), получим:

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n = \\ = (b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1})(x-a) + r,$$

или, выполняя в правой части последнего равенства все необходимые действия, будем иметь:

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n = \\ = b_0x^n + (b_1 - ab_0)x^{n-1} + (b_2 - ab_1)x^{n-2} + \ldots + (b_{n-1} - ab_{n-2})x + \\ + (r - ab_{n-1}).$$

Два многочлена равны только в том случае, когда совпадают их коэффициенты при одинаковых степенях x; следовательно:

$$a_0 = b_0; \quad a_1 = b_1 - ab_0, \quad a_2 = b_2 - ab_1, \ldots \\ \ldots; \ a_k = b_k - ab_{k-1}, \ldots, \ a_{n-1} = b_{n-1} - ab_{n-2}, \ a_n = r - ab_{n-1},$$

откуда без труда определяем коэффициенты частного и остаток:

$$b_0 = a_0, \quad b_1 = a_1 + ab_0, \quad b_2 = a_2 + ab_1, \ldots \\ \ldots; \ b_k = a_k + ab_{k-1}, \ldots, \ b_{n-1} = a_{n-1} + ab_{n-2}, \quad r = a_n + ab_{n-1}.$$

Всё вычисление располагается в виде следующей схемы, называемой *схемой Горнера*:

	a_0	a_1	a_2	a_3	$\ldots$	a_{n-1}	a_n
a	a_0	ab_0+a_1	ab_1+a_2	ab_2+a_3	$\ldots$	$ab_{n-2}+a_{n-1}$	$ab_{n-1}+a_n$

В нижней строке схемы Горнера стоят последовательно искомые коэффициенты b_i многочлена $q(x)$.

Поясним метод Горнера на примерах.

Пример 1. Разделим $f(x) = x^5 - 2x^4 + 3x^2 - x + 7$ на $x-2$.

Располагаем выкладки в схему Горнера:

	1	-2	0	3	-1	7
2	1	$2\cdot1-2=0$	$2\cdot0+0=0$	$2\cdot0+3=3$	$2\cdot3-1=5$	$2\cdot5+7=17$

Итак, частное равно

$$q(x) = x^4 + 3x + 5,$$

а остаток равен 17.

Пример 2. Разделим теперь

$$f(x) = x^7 - 2x^6 + x^5 - 3x^4 + 4x^3 - x^2 + 6x - 1$$

на $x + \frac{3}{2}$.

Опять пользуемся схемой Горнера, причём выкладки проводим в стороне, а в схему вписываем лишь окончательные результаты

	1	-2	1	-3	4	-1	6	-1
$-\frac{3}{2}$	1	$-\frac{7}{2}$	$\frac{25}{4}$	$-\frac{99}{8}$	$\frac{361}{16}$	$-\frac{1115}{32}$	$\frac{3729}{64}$	$-\frac{11315}{128}$

Таким образом, получились следующие частное и остаток:

$$q(x) = x^6 - \frac{7}{2}x^5 + \frac{25}{4}x^5 - \frac{99}{8}x^3 + \frac{361}{16}x^2 - \frac{1115}{32}x + \frac{3729}{64};$$

$$r = -\frac{11315}{128}.$$

З а д а ч а. Пользуясь методом Горнера, разделить

а) $3x^4 - 2x^3 - x^2 + 5x + 7$ на $x - 4$, b) $x^5 + 6x^3 - 2x^2 + 6x + 3$ на $x + 2$,

c) $x^6 - x^5 - 2x^3 + x^2 - 7x - 10$ на $x - \frac{1}{2}$, d) $x^5 - \frac{1}{2}x^4 + \frac{1}{3}x^3 - 2x + \frac{11}{5}$ на $x + \frac{1}{2}$;

Вернёмся к равенству (1). Оно является тождеством относительно x; следовательно, (1) будет справедливо и при $x = a$. Но полагая в тождестве (1) $x = a$, будем иметь: $f(a) = r$.

Мы получили следующее предложение, известное под названием *теоремы Безу* (Bézou):

Остаток от деления многочлена $f(x)$ на $x - a$ равен значению $f(x)$ при $x = a$.

Например, при делении $f(x) = x^3 - x^2 + 1$ на $x - 1$ по теореме Безу должен получиться остаток, равный $f(1) = 1 - 1 + 1 = 1$. И, действительно, выполняя деление, получим в остатке 1.

Предположим, теперь, что $f(x)$ делится на $x - a$ без остатка; в таком случае $r = f(a) = 0$. Обратно, если $f(a) = 0$, то по теореме Безу остаток должен равняться нулю: $r = f(a) = 0$; поэтому $f(x)$ делится на $x - a$ нацело.

Мы подошли вплотную к понятиям алгебраического уравнения и корня.

Определение. *Уравнение*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n = 0 \quad (a_0 \neq 0), \tag{2}$$

левая часть которого есть многочлен $f(x)$ n-й степени, называется алгебраическим уравнением n-й степени.

Число a, обращающее в нуль левую часть уравнения (2), называется *корнем уравнения* или многочлена $f(x)$. Итак, *$f(x)$ делится на $x-a$ без остатка тогда и только тогда, когда a есть корень многочлена $f(x)$*. В некоторых случаях многочлен $f(x)$ может делиться не только на $x-a$, но и на $(x-a)^2$ и вообще на $(x-a)^k$, где k — некоторое натуральное число. Мы будем называть корень a *k-кратным корнем* многочлена $f(x)$, если $x-a$ входит в $f(x)$ с кратностью k; например,

$$f(x) = (x-1)(x+1)^2(x-3)^3$$

имеет $a_1 = 1$ однократным корнем, $a_2 = -1$ двукратным корнем и $a_3 = 3$ трёхкратным корнем.

Сколько корней может иметь многочлен (уравнение) в поле P? Если кратные корни считать столько раз, какова их кратность [1]), то ответом служит следующая теорема.

Теорема. *Если n степень многочлена $f(x)$ (или уравнения $f(x)=0$), то число корней $f(x)$ в поле P не превосходит n.*

Так, многочлен $f(x) = x^2 - 2$ в поле рациональных чисел не имеет вовсе корней, а в поле действительных чисел он будет иметь два корня $\sqrt{2}$ и $-\sqrt{2}$; в том и в другом случае число корней не превосходит степени многочлена.

Доказательство. Предположим противное: пусть число корней многочлена $f(x)$ превосходит n. Тогда $f(x)$ будет в поле P следующим образом разлагаться на множители:

$$f(x) = (x-a_1)^{k_1}(x-a_2)^{k_2}\ldots(x-a_s)^{k_s}\varphi(x). \tag{3}$$

Мы здесь через $a_1, \ldots, a_s$ обозначили корни многочлена $f(x)$. Так как число корней по нашему предположению должно превосходить n, то $k_1 + \ldots + k_s > n$. Но в таком случае правая часть равенства (3) должна представлять собой многочлен степени более высокой, чем n. Мы пришли к нелепости: многочлен $f(x)$ n-й степени вместе с тем является многочленом степени выше n.

Отметим одно следствие.

Следствие. *Если два многочлена $f(x)$ и $g(x)$ n-й степени совпадают при более чем n значениях переменного x из поля P, то они равны.*

Предположим противное: пусть $f(x)$ не равно $g(x)$, т. е. пусть разность $f(x)-g(x)=\varphi(x)$ отлична от нуля. Степень многочлена $\varphi(x)$, очевидно, не превосходит n. Но, с другой стороны, $\varphi(x)$ обращается в нуль более чем при n значениях переменного x. Получается противоречие с вышедоказанной теоремой, и мы вынуждены констатировать, что $\varphi(x)$ есть нуль. Но тогда $f(x)=g(x)$.

---

[1]) Например, двукратный корень будем считать дважды.

ГЛАВА ШЕСТАЯ

КОЛЬЦО МНОГОЧЛЕНОВ В ПОЛЕ РАЦИОНАЛЬНЫХ ЧИСЕЛ

§ 32. Границы рациональных корней

В этой главе мы будем рассматривать многочлены исключительно в поле рациональных чисел. Итак, пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \qquad (1)$$

— многочлен с рациональными коэффициентами. Как обнаружить рациональные корни $f(x)$?

При отыскании рациональных корней полезно знать, в каких границах они расположены. Мы разберём здесь четыре способа нахождения границ.

Первый способ. Обозначим через $|a|$ то из двух чисел a и $-a$, которое является положительным, и назовём $|a|$ *абсолютной величиной* числа a. Например $|-5| = 5$; $|+5| = 5$.

Мы покажем, что рациональные корни многочлена (1) следует искать между $-R$ и R, где

$$R = \frac{A}{|a_0|} + 1.$$

Здесь A—наибольшая из абсолютных величин коэффициентов, начиная с a_1. Предварительно нам придётся познакомиться со следующими свойствами абсолютной величины.

I. *Абсолютная величина произведения двух чисел равна произведению их обсолютных величин*: $|ab| = |a| \cdot |b|$.

В самом деле, если a и b оба положительны, то $ab = |ab|$, $|a| = a$, $|b| = b$, откуда $|a| \cdot |b| = |ab|$.

Если a и b оба отрицательны, то $ab = |ab|$ (потому что ab положительно), $|a| = -a$, $|b| = -b$, откуда $|a| \cdot |b| = (-a)(-b) = ab = |ab|$.

Наконец, a и b могут иметь противоположные знаки. Пусть, например, $a < 0$, $b > 0$. Тогда $-ab = |ab|$ (потому что $-ab$ положительно), $|a| = -a$, $b = b$, откуда $|a| \cdot |b| = -ab = |ab|$.

Очевидно, что свойство I верно для любого числа сомножителей:

$$|abc| = |ab| \cdot |c| = |a| \cdot |b| \cdot |c|; \quad |abcd| = |abc| \cdot |d| = |a| \cdot |b| \cdot |c| \cdot |d|$$

и т. д.

В частности $|a^n| = |a|^n$.

II. *Абсолютная величина суммы двух чисел меньше или равна сумме абсолютных величин слагаемых*: $|a + b| \leqslant |a| + |b|$.

Для доказательства возвысим $|a| + |b|$ в квадрат:

$$(|a| + |b|)^2 = |a|^2 + 2|a| \cdot |b| + |b|^2,$$

или

$$(|a| + |b|)^2 = a^2 + 2|a| \cdot |b| + b^2, \qquad (2)$$

так как $|a|^2 = a^2$, $|b|^2 = b^2$. Затем заменим $|a| \cdot |b|$ через ab; от этого выражение, стоящее в правой части равенства (2), либо не

изменится, либо уменьшится: оно не изменится при $ab \geqslant 0$ и уменьшится при $ab < 0$. Таким образом

$$(|a| + b|)^2 \geqslant a^2 + 2ab + b^2 = |a + b|^2,$$

откуда ясно, что

$$|a| + |b| \geqslant a + b|.$$

Нетрудно видеть, что свойство II верно для любого числа слагаемых:

$$|a + b + c| \leqslant |a + b| + |c| \leqslant |a + |b| + |c|;$$
$$|a + b + c + d| \leqslant |a + b + c| + |d| \leqslant |a + |b| + c| + |d|$$

и т. д.

III. *Абсолютная величина суммы двух чисел больше или равна разности их абсолютных величин*: $|a| - |b| \leqslant |a + b|$.

Воспользуемся очевидным равенством

$$|a| = |(a + b) + (-b)|.$$

По свойству II:

$$|a| = |(a + b) + (-b)| \leqslant |a + b| + |-b|;$$

откуда

$$|a| - |-b| \leqslant |a + b|.$$

Но $|-b| = |b|$; и потому окончательно

$$|a| - |b| \leqslant |a + b|.$$

Вернёмся к нашему утверждению о том, что рациональные корни многочлена (1) могут лежать лишь в пределах от $-R$ до R.

В силу свойств III и I абсолютной величины

$$|f(x)| = |a_0 x^n + (a_1 x^{n-1} + \ldots + a_n)| \geqslant$$
$$\geqslant |a_0 \cdot |x|^n - |a_1 x^{n-1} + \ldots + a_n|. \qquad (3)$$

Займёмся вычитаемым $|a_1 x^{n-1} + \ldots + a_n|$. В силу свойств II и I абсолютной величины:

$$|a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n| \leqslant |a_1 \cdot x^{n-1}| + |a_2| \cdot |x^{n-2}| + \ldots + |a_n|.$$

Последнее неравенство усилится, если мы $|a_1|, |a_2|, \ldots; |a_n|$ заменим через A, где A наибольшая из абсолютных величин коэффициентов $a_1, \ldots, a_n$. Получим:

$$|a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n| \leqslant A(|x^{n-1}| + |x^{n-2}| + \ldots + 1)$$

или, применяя формулу суммы членов геометрической прогрессии:

$$|a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n| \leqslant A \frac{|x^n| - 1}{|x| - 1}.$$

Отсюда следует, что при $|x| > 1$

$$|a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n| < A \frac{|x|^n}{|x| - 1}.$$

А теперь подставим в правую часть неравенства (3) вместо вычитаемого заведомо бо́льшую величину $A\frac{|x|^n}{|x|-1}$:

$$|f(x)|>|a_0|\cdot|x|^n-A\frac{|x|^n}{|x|-1}=\frac{|x|^n}{|x|-1}[|a_0|(|x|-1)-A].$$

Посмотрим, при каких значениях x

$$|a_0|(|x|-1)-A>0.$$

Решаем это неравенство и получаем, что

$$|x|>\frac{A}{|a_0|}+1. \tag{4}$$

Итак, если x удовлетворяет условию (4), то $|f(x)|>0$, т. е. $f(x)$ не обращается в нуль. Иными словами, рациональные корни могут лежать лишь между $-R$ и R, где $R=\frac{A}{|a_0|}+1$.

Пример. Рассмотрим уравнение

$$f(x)=2x^5+100x^2-5x-40=0. \tag{5}$$

Здесь; $a_0=2$ $A=100$, откуда $R=\frac{100}{2}+1=51$. Таким образом; рациональные корни следует искать между -51 и 51. Но это ещё не всё. Заменим x через $\frac{1}{y}$; после некоторых преобразований вместо уравнения (5) получится:

$$40y^5+5y^4-100y^3-2=0,$$

откуда $R_1=\frac{100}{40}+1=\frac{7}{2}$, и положительные корни последнего уравнения должны удовлетворять неравенству $y\leqslant\frac{7}{2}$. Но $y=\frac{1}{x}$; а потому $\frac{1}{x}\leqslant\frac{7}{2}$ или $x\geqslant\frac{2}{7}$. Следовательно, положительные корни уравнения (5) надо искать между $\frac{2}{7}$ и 51.

Чтобы получить границы отрицательных корней, полагаем $x=-\frac{1}{z}$, после чего имеем:

$$f\left(-\frac{1}{z}\right)=-2\cdot\frac{1}{z^5}+100\cdot\frac{1}{z^2}+5\cdot\frac{1}{z}-40=0$$

или, освобождаясь от знаменателей и меняя знаки на обратные;

$$40z^5-5z^4-100z^3+2=0.$$

Для этого уравнения $R_1=\frac{100}{40}+1=\frac{7}{2}$, и его положительные корни должны удовлетворять условию $z\leqslant\frac{7}{2}$. Но $z=-\frac{1}{x}$; откуда

$-\frac{1}{x} \leqslant \frac{7}{2}$ или $x \leqslant -\frac{2}{7}$. Таким образом, отрицательные корни уравнения (5) следует искать между -51 и $-\frac{2}{7}$.

Числа $\frac{2}{7}$ и 51 называются соответственно нижней и верхней границами положительных корней, а -51 и $-\frac{2}{7}$ — нижней и верхней границами отрицательных корней.

К сожалению, этот простой способ нахождения пределов корней обладает одним существенным недостатком: границы $-R$ и R слишком велики. Мы укажем сейчас другие более совершенные методы.

Второй способ (способ Маклорена). Мы вправе предположить, что в уравнении

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n = 0$$

старший коэффициент a_0 положителен; в противном случае мы помножили бы обе части уравнения на -1. Пусть a_k первый отрицательный коэффициент, начиная с a_0, B — наибольшая из абсолютных величин отрицательных коэффициентов; тогда, предполагая x положительным, получим:

$$f(x) = a_0x^n + \ldots + a_{l-1}x^{n-k-1} + a_kx^{n-k} + a_{k+1}x^{n-k-1} + \ldots + a_n \geqslant$$
$$\geqslant a_0x^n + a_1x^{n-1} + \ldots + a_{k-1}x^{n-k+1} - B(x^{n-k} + x^{n-k-1} + \ldots + 1).$$

Неравенство усилится, если отбросить члены a_1x^{n-1}, ..., $a_{k-1}x^{n-k+1}$, положительные при $x > 0$. Таким образом

$$f(x) \geqslant a_0x^n - B(x^{n-k} + x^{n-k-1} + \ldots + 1),$$

или, суммируя геометрическую прогрессию:

$$f(x) \geqslant a_0x^n - B\frac{x^{n-k+1} - 1}{x-1}.$$

Если предположить $x > 1$, то

$$f(x) > a_0x^n - B\frac{x^{n-k+1}}{x-1},$$

или

$$f(x) > \frac{x^{n-k+1}}{x-1}[a_0x^{k-1}(x-1) - B].$$

Снова усиливаем неравенство, заменяя в квадратной скобке x через $x-1$:

$$f(x) > \frac{x^{n-k+1}}{x-1}[a_0(x-1)^k - B].$$

Многочлен $f(x)$ будет наверное иметь положительное значение, если

$$a_0(x-1)^k - B > 0.$$

Решаем это неравенство относительно x и получаем:

$$x > \sqrt[k]{\frac{B}{a_0}} + 1. \qquad (6)$$

Итак, для значений x, удовлетворяющих условию (6), $f(x)$ не может обращаться в нуль; иными словами

$$\sqrt[k]{\frac{B}{a_0}} + 1$$

можно принять за верхнюю границу положительных корней.

Чтобы найти нижнюю границу положительных корней, заменяем, как и выше, x через $\frac{1}{y}$ и рассматриваем уравнение

$$g(y) = y^n f\left(\frac{1}{y}\right) = 0.$$

Если верхняя граница положительных корней $g(y)$ равна a, то $\frac{1}{a}$ будет нижней границей положительных корней $f(x)$.

Чтобы найти верхнюю границу отрицательных корней, полагаем $x = -\frac{1}{z}$ и рассматриваем уравнение

$$h(z) = (-z)^n f\left(-\frac{1}{z}\right) = 0.$$

Если верхняя граница положительных корней $h(z)$ равна b, то $-\frac{1}{b}$ будет верхней границей отрицательных корней $f(x)$.

Наконец, чтобы найти нижнюю границу отрицательных корней, полагаем $x = -u$ и рассматриваем уравнение

$$k(u) = (-1)^n f(-u) = 0.$$

Если c есть верхняя граница положительных корней $k(u)$, то $-c$ будет нижней границей отрицательных корней $f(x)$.

Пример. Применим способ Маклорена к уравнению (5); здесь $a_0 = 2$, $k = 4$, $B = 40$, откуда получаем, что

$$\sqrt[k]{\frac{B}{a_0}} + 1 = \sqrt[4]{\frac{40}{2}} + 1 < 3{,}3.$$

Таким образом 3,3 можно принять за верхнюю границу положительных корней.

Далее полагаем $x = \frac{1}{y}$ и получаем:

$$g(y) = 40y^5 + 5y^4 - 100y^3 - 2 = 0.$$

Для этого уравнения $a_0 = 40$, $k = 2$, $B = 100$, откуда

$$\sqrt[k]{\frac{B}{a_0}} + 1 = \sqrt[2]{\frac{100}{40}} + 1 < 2{,}6.$$

Следовательно, $\frac{1}{2{,}6} \approx 0{,}3$ [1]) можно принять за нижнюю границу положительных корней уравнения (5).

[1]) Знак $\approx$ обозначает приближённое равенство.

Находим верхнюю границу отрицательных корней, для чего полагаем $x = -\frac{1}{z}$. Имеем:

$$h(z) = 40z^5 - 5z^4 - 100z^3 + 2 = 0;$$

здесь $a_0 = 40$; $B = 100$, $k = 1$, откуда

$$\sqrt[k]{\frac{B}{a_0}} + 1 = \frac{100}{40} + 1 = \frac{7}{2}.$$

Следовательно, $-\frac{2}{7} \approx -0{,}2$ есть верхняя граница отрицательных корней уравнения (5). Наконец, полагаем $x = -u$ и получаем:

$$k(u) = 2u^5 - 100u^2 - 5u + 40 = 0.$$

Здесь $a_0 = 2$, $k = 3$, $B = 100$, а потому

$$\sqrt[k]{\frac{B}{a_0}} + 1 = \sqrt[3]{\frac{100}{2}} + 1 \approx 4{,}7.$$

Таким образом $-4{,}7$ можно принять за нижнюю границу отрицательных корней уравнения (5).

Итак, положительные корни следует искать между 0.3 и 3,3, а отрицательные между $-4{,}7$ и $-0{,}2$. Получились гораздо более тесные границы, чем ранее.

Третий способ (способ Ньютона). Этот способ основан на следующем предложении:

Если при $x = a$ $(a > 0)$ *многочлен* $f(x)$ *и все его производные* $f'(x)$, $f''(x), \ldots, f^{(n)}(x)$ *положительны, то* a *можно принять за верхнюю границу положительных корней уравнения* $f(x) = 0$.

В самом деле, разложим $f(x)$ в ряд Тэйлора:

$$f(x) = f(a) + (x-a)f'(a) + \frac{(x-a)^2}{2!}f''(a) + \cdots + \frac{(x-a)^n}{n!}f^{(n)}(a). \quad (7)$$

При $x \geqslant a$ правая часть, очевидно, положительна, так как $f(a)$, $f'(a), \ldots, {}^{(n)}(a)$ по условию больше нуля; следовательно, при $x \geqslant a$ многочлен $f(x)$ не может обращаться в нуль. Поэтому a есть верхняя граница положительных корней уравнения $f(x) = 0$.

Полагая $x = \frac{1}{y}$, $x = -\frac{1}{z}$, $x = -u$, получим, как и выше, все остальные границы корней.

Небесполезно иметь в виду следующие практические указания. Во-первых, значения $f(a)$, $f'(a), \ldots, f^{(n)}(a)$ удобнее всего вычислять с помощью метода Горнера. Дело в том, что ряд Тэйлора (7) можно переписать так:

$$f(x) = f(a) + (x-a)\varphi_1(x),$$

где

$$\varphi_1(x) = f'(a) + \frac{(x-a)}{2!}f''(x) + \ldots + \frac{(x-a)^{n-1}}{n!}f^{(n)}(a);$$

отсюда ясно, что $f(a)$ есть остаток от деления $f(x)$ на $x-a$, а $\varphi_1(x)$ частное. В свою очередь

$$\varphi_1(x) = f'(a) + (x-a)\varphi_2(x),$$

где

$$\varphi_2(x) = \frac{1}{2!}f''(a) + \frac{(x-a)}{3!}f'''(a) + \ldots + \frac{(x-a)^{n-2}}{n!}f^{(n)}(x).$$

Таким образом $f'(a)$ есть остаток от деления $\varphi_1(x)$ на $x-a$ и $\varphi_2(x)$ — частное. Далее имеем:

$$\varphi_2(x) = \frac{1}{2!}f''(a) + (x-a)\varphi_3(x),$$

откуда ясно, что $\frac{1}{2}f''(a)$ есть остаток от деления $\varphi_2(x)$ на $x-a$ и т. д.

Пример. В качестве примера вычислим значение

$$f(x) = x^4 - 5x^2 + 6x - 8$$

и всех производных $f(x)$ при $x=2$. Составляем схему Горнера:

	1	0	−5	6	−8
2	1	2	−1	4	0
2	1	4	7	18	
2	1	6	19		
2	1	8			
2	1				

Мы видим, что

$$f(2) = 0, \quad f'(2) = 18, \quad f''(2) = 2 \cdot 19 = 38;$$
$$f'''(2) = 3! \cdot 8 = 48, \quad f^{IV}(2) = 4! \cdot 1 = 24.$$

Если в процессе применения способа Ньютона числа какой-нибудь строки схемы Горнера окажутся все положительными, то дальнейшие выкладки становятся излишними, потому что все следующие строки схемы будут состоять исключительно из положительных чисел.

Опять возьмём в качестве примера уравнение (5). Значение $x = {}^1/_2$ не годится, так как $f\left(\frac{1}{2}\right) < 0$. Поэтому берём несколько большее значение, а именно $x=1$. Пользуемся схемой Горнера:

	2	0	0	100	−5	−40
1	2	2	2	102	97	57

Дальнейшие вычисления излишни, так как получилась строка с положительными числами. Следовательно, $f(1), f'(1), \ldots, f^{n}(1), \ldots$ — все положительны, и 1 можно принять за верхнюю границу положительных корней.

Остальные границы мы предлагаем читателю разыскать самостоятельно. Приведём только окончательный ответ: границы положительных корней равны $^1/_2$ и 1, границы отрицательных корней равны -4 и $-\frac{1}{2}$. Мы видим, что способ Ньютона оказался более выгодным, чем предыдущие способы.

Четвёртый способ. Предположим сперва, что в многочлене $f(x)$, расположенном по убывающим степеням x, сначала идут только положительные (при $x>0$) члены, а затем только отрицательные члены. Иными словами, пусть $f(x)$ имеет вид:

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_kx^{n-k}-a_{k+1}x^{n-k-1}-\ldots-a_n, \qquad (8)$$

где $a_i\geqslant 0$ $(i=0, 1, 2, \ldots, n)$. Можно высказать следующее предложение.

Если многочлен $f(x)$ вида (8) *неотрицателен при $x=a$ $(a>0)$, то он неотрицателен и при $x>a$.*

В самом деле, многочлен $f(x)$ можно представить так:

$$f(x)=x^{n-k}\left[(a_0x^k+a_1x^{k-1}+\ldots+a_k)-\left(\frac{a_{k+1}}{x}+\ldots+\frac{a_n}{x^{n-k}}\right)\right].$$

Многочлен, стоящий в первой круглой скобке, возрастает с возрастанием $x>0$; многочлен, стоящий во второй круглой скобке, убывает с возрастанием x. Таким образом $f(x)$ будет возрастать с возрастанием x. Следовательно, если $f(a)>0$, то $f(x)$ и подавно будет положительным при $x>a$.

Любой многочлен $f(x)$ всегда можно (не переставляя членов) записать в виде суммы

$$f(x)=f_1(x)+f_2(x)+\ldots+f_k(x),$$

где $f_i(x)$ — многочлены типа (8). Если при $x=a$ $f_1(x), f_2(x), \ldots, f_k(x)$ неотрицательны, то, очевидно, a можно принять за верхнюю границу положительных корней. Остальные границы найдутся с помощью подстановок $x=\frac{1}{y}$, $x=-\frac{1}{z}$, $x=-u$.

Пример.

$$f(x)=x^5-x^4+7x^3-5x^2-x+1$$

можно представить в виде

$$f(x)=f_1(x)+f_2(x)+f_3(x),$$

где

$$\left.\begin{aligned} f_1(x)&=x^5-x^4,\\ f_2(x)&=7x^3-5x^2-x,\\ f_3(x)&=1. \end{aligned}\right\} \qquad (9)$$

Легко заметить, что при $x=1$ многочлены (9) неотрицательны, следовательно, единицу можно принять за верхнюю границу положительных корней. Полагая $x=\frac{1}{y}$, найдём, что нижняя граница положительных корней рассматриваемого многочлена равна $\frac{1}{3}$. Полагая $x=-\frac{1}{z}$, найдём, что верхняя граница отрицательных корней равна $-\frac{1}{7}$. Наконец, полагая $x=-u$, найдём нижнюю границу отрицательных корней, равную -1.

Задача. Определить границы рациональных корней уравнений:

a) $x^4-12x^3-x-4=0$;
b) $x^7+2x^5-2x^4+4x^3+9x^2-x+13=0$;
c) $x^{10}-x^3+5x^2-x+10=0$;
d) $x^4-1,5x^3+8,5x^2-7=0$.

§ 33. Вычисление рациональных корней

Вычисление рациональных корней основано на следующих свойствах уравнения.

I. *Всякое уравнение с дробными коэффициентами можно преобразовать так, чтобы коэффициенты стали целыми.*

Действительно, для этого достаточно помножить обе части уравнения на общий знаменатель коэффициентов.

II. *Всякое уравнение*

$$a_0x^n+a_1x^{n-1}+\ldots+a_n=0$$

с целыми коэффициентами a_i можно преобразовать так, чтобы a_0 превратилось в единицу и все прочие коэффициенты остались попрежнему целыми.

Положим $x=\frac{t}{a_0}$; тогда рассматриваемое уравнение примет вид

$$\frac{t^n}{a_0^{n-1}}+\frac{a_1}{a_0^{n-1}}t^{n-1}+\frac{a_2}{a_0^{n-2}}t^{n-2}+\ldots+a_n=0$$

или, освобождаясь от дробей,

$$t^n+a_1t^{n-1}+a_0a_2t^{n-2}+\ldots+a_0^{n-1}a_n=0.$$

III. *Уравнение*

$$f(x)=x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n=0 \qquad (1)$$

с целыми коэффициентами a_i может иметь рациональными корнями только целые числа.

Допустим противное. Предположим, что уравнение (1) имеет дробный корень $x_0=\frac{a}{b}$ (a, b—целые числа); очевидно, дробь можно

считать несократимой. Подставляя $x_0 = \frac{a}{b}$ в уравнение, имеем

$$\frac{a^n}{b^n} + a_1 \frac{a^{n-1}}{b^{n-1}} + a_2 \frac{a^{n-2}}{b^{n-2}} + \ldots + a_n = 0.$$

Если умножить обе части этого равенства на b^{n-1} и перенести все слагаемые, кроме первого, в правую часть, то получится

$$\frac{a^n}{b} = -a_1 a^{n-1} - a_2 a^{n-2} b - \ldots - a_n b^{n-1}.$$

Так как дробь $\frac{a}{b}$ несократима, то несократима также дробь $\frac{a^n}{b}$. Мы таким образом пришли к нелепости: несократимая дробь равна целому числу.

IV. *Целый корень уравнения* (1) *должен быть делителем свободного члена* a_n.

Пусть a — целый корень уравнения (1).

Тогда

$$f(a) = a^n + a_1 a^{n-1} + a_2 a^{n-2} + \ldots + a_n = 0,$$

или

$$a_n = a(-a^{n-1} - a_1 a^{n-2} - \ldots - a_{n-1}).$$

Последнее равенство как раз свидетельствует о том, что a_n делится на a.

V. *Частное от деления левой части уравнения* (1) *на* $x - (a$—*целое число*) *есть многочлен с целыми коэффициентами.*

По схеме Горнера первый коэффициент частного b_0 равен единице, а второй коэффициент $b_1 = a_1 + a$. Но a и a_1—целые числа, следовательно, b_1 также целое число. Третий коэффициент частного $b_2 = a_2 + ab_1$ опять-таки является целым, потому что ab_1 и a_2 — целые и т. д. Наконец, последний коэффициент частного $b_{n-1} = a_{n-1} + ab_{n-2}$ есть целое число, так как a_{n-1} и ab_{n-2}—целые.

VI. *Если* a — *целый корень уравнения* (1), *то* $\frac{f(1)}{a-1}$ *и* $\frac{f(-1)}{a+1}$ — *целые числа.*

Действительно, можно написать, что

$$f(x) = (x - a)\, q(x),$$

или

$$\frac{f(x)}{a - x} = -q(x).$$

В силу свойства V коэффициенты $q(x)$ должны быть целыми. Отсюда следует, что каждое из чисел

$$-q(1) = \frac{f(1)}{a-1},$$

$$-q(-1) = \frac{f(-1)}{a+1}$$

есть целое число.

VII. *Число a может быть тогда и только тогда целым корнем уравнения* (1), *когда выполняются соотношения*

$$q_{n-1}=\frac{a_n}{a},\quad q_{n-2}=\frac{a_{n-1}+q_{n-1}}{a},\ \ldots,$$
$$q_1=\frac{a_2+q_2}{a},\quad q_0=-1=\frac{a_1+q_1}{a}. \qquad (2)$$

причём $q_1, q_2, \ldots, q_{n-1}$ числа целые.

Пусть a—целый корень нашего уравнения. Делим $f(x)$ на $x-a$ по схеме Горнера; получим тогда коэффициенты частного и остаток, равный нулю:

$$b_0=1,\quad b_1=a_1+a,\quad b_2=a_2+ab_1,\ \ldots,$$
$$b_{n-1}=a_{n-1}+ab_{n-2},\quad r=0=a_n+ab_{n-1},$$

откуда

$$-b_{n-1}=\frac{a_n}{a},\quad -b_{n-2}=\frac{a_{n-1}-b_{n-1}}{a},\ \ldots,\quad -b_0=-1=\frac{a_1-b_1}{a}.$$

Полагая $-b_{n-1}=q_{n-1}$, $-b_{n-2}=q_{n-2}$, $\ldots$, $-b_1=q_1$, $-b_0=q_0$, приходим к соотношениям (2). В силу свойства V числа q_{n-1}, q_{n-2}, $\ldots$, q_1 должны быть целыми.

Таким образом процесс вычисления рациональных корней представляется в следующем виде. Прежде всего приводят заданное уравнение к виду (1); затем испытывают всевозможные делители свободного члена a_n. Если ни один из делителей не будет корнем, то заданное уравнение не имеет совсем рациональных корней.

Испытание делителей рекомендуется проводить так. Сначала смотрят, делится ли нацело $f(1)$ на $a-1$ и $f(-1)$ на $a+1$; если $f(1)$ не делится на $a-1$ или $f(-1)$ не делится на $a+1$, то a следует отбросить (см. VI). После этого оставшиеся делители a испытываются с помощью свойства VII. А именно, составляют следующую таблицу:

	a_n	a_{n-1}	a_{n-2}	$\cdots$	a_1	1
a	q_{n-1}	q_{n-2}	q_{n-3}	$\cdots$	$q_0=-1$	

Первой строкой идут в обратном порядке коэффициенты рассматриваемого уравнения. Вторая строка получается из соотношений (2). Целое число a может быть корнем только в том случае, когда числа q_i целые и $q_0=-1$ (см. свойство VII).

Пример. Рассмотрим уравнение:

$$x^5-\frac{7}{10}x^4+\frac{11}{10}x^3-\frac{17}{10}x^2+\frac{8}{10}x-\frac{1}{10}=0.$$

Прежде всего освобождаемся от дробей. Имеем:

$$10x^5-7x^4+11x^3-17x^2+8x-1=0.$$

Затем приводим последнее уравнение к виду (1), для чего полагаем $x = \frac{t}{10}$. Получаем:

$$f(t) = t^5 - 7t^4 + 110t^3 - 1700t^2 + 8000t - 10\,000 = 0. \qquad (3)$$

Свободный член 10000 имеет довольно много делителей; для сокращения вычислений находим границы корней. С помощью четвёртого способа (см. § 32) можно легко установить, что положительные корни должны лежать между 0 и 16. Отрицательных корней уравнение (3) вовсе не имеет, так как, полагая $t = -z$, получаем

$$z^5 + 7z^4 + 110z^3 + 1700z^2 + 8000z + 10\,000 = 0.$$

Левая часть этого уравнения при $z \geqslant 0$ не может обращаться в нуль, откуда ясно, что (3) не имеет отрицательных корней.

Итак, достаточно ограничиться делителями 1, 2, 4, 5, 8, 10, 16 числа 10000. Находим, чему равно $f(1)$ и $f(-1)$:

$$f(1) = -3596, \quad f(-1) = -19\,818.$$

Число 4 не годится, потому что $f(-1)$ не делится на $4 + 1 = 5$. По той же причине не годится 10 и 16. Наконец, число 8 не годится, потому что $f(1)$ не делится на $8 - 1 = 7$. Остаются лишь два делителя: 2, 5.

Начнём с двойки. Составляем для неё табличку:

	10 000	8000	1700	110	7	1
2	5000	1500	400	5	1	

Мы видим, что 2 есть корень.

Затем испытываем 5:

	10 000	8000	1700	110	7	1
5	2000	1200	100	2	1	

Оказывается, что 5 также является корнем.

Итак, уравнение (3) имеет всего два целых корня $t_1 = 2$ и $t_2 = 5$, а потому рациональные корни заданного уравнения таковы:

$$x_1 = \frac{t_1}{10} = \frac{1}{5}, \quad x_2 = \frac{t_2}{10} = \frac{1}{2}.$$

Задача. Вычислить рациональные корни следующих уравнений:

а) $x^4 - 6x^3 + 12x^2 - 11x + 6 = 0$,

б) $x^5 - \frac{5}{6}x^4 + \frac{7}{6}x^3 - \frac{1}{6}x^2 - \frac{2}{3}x + 1 = 0$,

в) $x^4 - 3x^3 - \frac{1}{2}x^2 + \frac{5}{2}x - 3 = 0$.

§ 34. Критерий Эйзенштейна

В 1850 г. Эйзенштейном был предложен довольно простой критерий, позволяющий во многих случаях сразу обнаруживать неприводимость многочлена в поле рациональных чисел. Пусть $f(x)$ — многочлен в поле рациональных чисел. Коэффициенты многочлена

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

можно предполагать целыми, так как в противном случае мы умножили бы $f(x)$ на надлежащим образом подобранное целое число. При этих условиях имеет место следующая теорема.

Критерий Эйзенштейна. *Если все коэффициенты многочлена*

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

кроме a_n, делятся на какое-нибудь простое число p; а a_0, делясь на p, не делится на p^2; то многочлен $f(x)$ неприводим.

Доказательство этой теоремы основано на двух леммах Гаусса, связанных с понятием примитивного многочлена. Обозначим через d общий наибольший делитель коэффициентов $a_0, \ldots, a_n$ многочлена $f(x)$. Если d вынести за скобку, то получится

$$f(x) = dg(x),$$

причём $g(x)$ — многочлен уже с взаимно простыми коэффициентами. Мы будем называть $g(x)$ *примитивным многочленом*.

Обратимся теперь к леммам Гаусса.

Лемма I. *Произведение двух примитивных многочленов есть также примитивный многочлен.*

Доказательство. Пусть

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_s x^s,$$
$$h(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_t x^t$$

два примитивных многочлена. По правилу перемножения

$$g(x)\,h(x) = b_0 c_0 + \cdots + (b_0 c_{i+j} + b_1 c_{i+j-1} + \cdots + b_{i-1} c_{j+1} + b_i c_j + b_{i+1} c_{j-1} + \cdots + b_{i+j} c_0) x^{i+j} + \cdots + b_s c_t x^m \qquad (m = s+t).$$

Допустим, что, напротив, произведение $g(x)\,h(x)$ не примитивный многочлен; тогда его коэффициенты должны иметь общий делитель d, отличный от единицы. Если p простой множитель d, то p должно делить все коэффициенты $g(x)\,h(x)$. Пусть $b_0, b_1, \ldots, b_{i-1}$ делятся на p, но b_i не делится на p (такое b_i наверное существует, так как иначе $g(x)$ не было бы примитивным многочленом). Точно так же пусть $c_0, c_1, \ldots, c_{j-1}$ делятся на p, а c_j не делится на p. Коэффициент

$$b_0 c_{i+j} + b_1 c_{i+j-1} + \cdots + b_{i-1} c_{j+1} + b_i c_j + \cdots + b_{i+j} c_0 \qquad (1)$$

произведения $g(x)\,h(x)$ по предположению делится на p. Кроме того, на p делятся, очевидно, и все члены (1), кроме $b_i c_j$. Следовательно, $b_i c_j$ также должно делиться на p, потому что иначе выражение (1) не делилось бы на p. Но последнее невозможно, так как по условию ни b_i, ни c_j не делятся на p. Тем самым лемма доказана.

Лемма II. *Если многочлен $f(x)$ с целыми коэффициентами приводим, то его можно разложить на произведение многочленов с целыми коэффициентами.*

Доказательство. Поскольку $f(x)$ приводимо, мы можем написать, что

$$f(x) = \varphi(x)\,\psi(x),$$

где $\varphi(x)$, $\psi(x)$ — многочлены с рациональными коэффициентами.

Приведём в $\varphi(x)$ и $\psi(x)$ коэффициенты к одному знаменателю, получим тогда, что $\varphi(x)=\frac{1}{c}\varphi_1(x)$, $\psi(x)=\frac{1}{d}\psi_1(x)$, причём $\varphi_1(x)$, $\psi_1(x)$—многочлены уже с целыми коэффициентами. Затем вынесем за скобку общие наибольшие делители коэффициентов $\varphi_1(x)$ и $\psi_1(x)$. Получим $\varphi(x)=\frac{a}{c}g(x)$, $\psi(x)=\frac{b}{d}h(x)$, где $g(x)$, $h(x)$—примитивные многочлены. Таким образом

$$f(x)=\frac{ab}{cd}g(x)h(x).$$

Мы утверждаем, что $\frac{ab}{cd}$ есть целое число. В самом деле, всегда можно положить $\frac{ab}{cd}=\frac{q}{r}$, где q и r взаимно просты. Если e_i какой-нибудь коэффициент произведения $g(x)h(x)$, то qe_i должно делиться на r, так как $f(x)$—многочлен с целыми коэффициентами. Но q и r взаимно просты; поэтому e_i должно делиться на r. Итак, мы видим, что r есть общий делитель коэффициентов $g(x)h(x)$. По лемме I произведение $g(x)h(x)$ примитивно; следовательно, $r=\pm1$, откуда $\frac{ab}{cd}$ равно целому числу $\pm q$

Теперь лемма становится очевидной: $f(x)$ разлагается на произведение многочленов $g_1(x)=\pm qg(x)$ и $h(x)$ с целыми коэффициентами.

Мы можем приступить к доказательству критерия Эйзенштейна.

Доказательство. Допустим противное: пусть

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

где

$$g(x)=b_0+b_1x+\cdots+b_rx^r,\quad h(x)=c_0+c_1x+\cdots+c_sx^s$$
$$(r>0;\ s>0;\ r+s=n)$$

многочлены с целыми коэффициентами (см. лемму II). Согласно правилу перемножения многочленов

$$g(x)h(x)=b_0c_0+(b_1c_0+b_0c_1)x+\cdots$$
$$\cdots+(b_kc_0+b_{k-1}c_1+\cdots+b_0c_k)x^k+\cdots+b_rc_sx^n.$$

Отсюда следует, что

$$a_0=b_0c_0,\ a_1=b_1c_0+b_0c_1,\ \cdots$$
$$\cdots,\ a_k=b_kc_0+b_{k-1}c_1+\cdots+b_0c_k,\ \cdots,\ a_n=b_rc_s.$$

Коэффициент $a_0=b_0c_0$ делится на p; поэтому на p должно делиться либо b_0, либо c_0. Пусть, например, b_0 делится на p; тогда c_s не может делиться на p, так как иначе $a_0=b_0c_0$ делилось бы на p^2.

Далее, не все коэффициенты $g(x)$ могут делиться на p. В самом деле, если бы имело место противное, то в частности $a_n=b_rc_s$ делилось бы на p, а это противоречит условиям критерия. Итак, пусть b_k первый коэффициент $g(x)$, не делящийся на p. Рассмотрим

$$a_k=b_kc_0+b_{k-1}c_1+\ldots+b_0c_k.$$

a_k, b_{k-1}, b_{k-2}, ..., b_0 делятся на p. Следовательно, на p делятся a_k, $b_{k-1}c_1$, $b_{k-2}c_2$, ..., b_0c_k, а потому делится на p и b_lc_0. Получилось противоречие: ни b_k, ни c_0 не делятся на p; поэтому их произведение b_lc_0 не может делиться на p.

Итак, предположение о том, что $f(x)$ приводимо, неверно.

Пример 1. Многочлен

$$f(x)=x^5-8x^4+2x^3-2x+2$$

неприводим; потому что $a_n=1$ не делится на $p=2$, а $a_0=2$ делится на 2, но не делится на $2^2=4$ и все остальные коэффициенты делятся на 2.

Пример 2. К многочлену

$$f(x)=x^2+1$$

критерий Эйзенштейна непосредственно применить нельзя, так как 1 не делится ни на какое простое число. Но мы можем вместо x ввести новое переменное y: $x=y+1$. Тогда получится

$$f(y+1)=\varphi(y)=y^2+2y+2.$$

Теперь требования критерия выполняются при $p=2$. Следовательно, $\varphi(y)$ и тем самым $f(x)$ неприводимы.

Пример 3. Рассмотрим, наконец, многочлен

$$f(x)=x^{p-1}+x^{p-2}+\cdots+1=\frac{x^p-1}{x-1}\ (p\text{ — простое число}).$$

Чтобы можно было применить критерий Эйзенштейна, полагаем, как и выше, $x=y+1$. Получаем:

$$f(y+1)=\varphi(y)=\frac{(y+1)^p-1}{(y+1)-1}=\frac{y^p+py^{p-1}+\frac{p(p-1)}{2}y^{p-2}+\cdots+py}{y}=$$

$$=y^{p-1}+py^{p-2}+\frac{p(p-1)}{2}y^{p-3}+\cdots+p.$$

Мы видим, что все коэффициенты, кроме старшего, делятся на p, причём последний коэффициент p не делится на p^2; стало быть, $\varphi(x)$ и тем самым $f(x)$ неприводимы.

Из критерия Эйзенштейна вытекает одно важное следствие. А именно, *в поле рациональных чисел существуют неприводимые многочлены любой степени*. Например, многочлены вида

$$f(x)=x^n+px+p\quad(p\text{ — простое число})$$

неприводимы.

Мы ниже увидим, что для поля действительных и поля комплексных чисел это обстоятельство уже не имеет места. В поле действительных чисел неприводимыми могут быть только многочлены не выше второй степени, а в поле комплексных чисел неприводимыми оказываются лишь многочлены первой степени.

Задача. Показать неприводимость следующих многочленов:

а) $f(x)=x^m-p_1p_2\ldots p_r$, где $m>1$, а p_i — различные простые числа.
b) $f(x)=x^p-px+(2p-1)$, где p простое число. c) $f(x)=x^4-2x+3$.

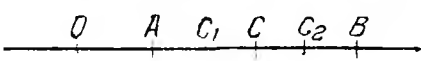
ГЛАВА СЕДЬМАЯ

КОЛЬЦО МНОГОЧЛЕНОВ В ПОЛЕ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ

§ 35. Действительные числа

Дальнейшее расширение области рациональных чисел тесно связано с уравнениями выше первой степени.

Пусть $f(x)$ многочлен выше первой степени, неприводимый в поле рациональных чисел. Разрешимо ли уравнение $f(x)=0$? Оказывается, что рациональных чисел недостаточно для решения этого уравнения, $f(x)$ не обращается в нуль ни при каком рациональном значении x. И в самом деле, если бы $f(x)$ равнялось нулю при некотором рациональном $x=a$, то $f(x)$ делилось бы на $x-a$ и потому было бы приводимым. Итак, мы снова вынуждены расширить область чисел для того, чтобы любое алгебраическое уравнение стало разрешимым. Это достигается введением иррациональных и мнимых чисел. Мы, однако, не собираемся давать строгого обоснования иррациональных чисел, так как оно принадлежит анализу, а не алгебре. Что касается мнимых чисел, то они будут рассмотрены в следующей главе.



Черт. 1.

Обратимся к геометрии; тогда мы скорее поймём, какую роль играет теория иррациональных чисел в анализе.

Из аналитической геометрии известно, что если на прямой линии выбрать начало и единицу масштаба, то рациональное число a изобразится точкой на прямой с абсциссой a. Так, число $-\frac{1}{2}$ представляется точкой, лежащей влево от начала координат на расстоянии, равном $\frac{1}{2}$ единицы масштаба, а число $\frac{5}{3}$ представляется точкой, лежащей вправо от начала на расстоянии $\frac{5}{3}$ единиц. Назовём точки, изображающие рациональные числа, *рациональными*.

Легко показать, что между всякими двумя рациональными точками находится бесчисленное множество других рациональных точек. Действительно, возьмём две точки A и B с рациональными абсциссами a и b; очевидно, середина C отрезка AB (см. черт. 1) будет также рациональной точкой, потому что её абсцисса равна $\frac{a+b}{2}$. В свою очередь, середины отрезков AC и CB дают новые рациональные точки C_1 и C_2 и т. д. И тем не менее рациональных чисел оказывается недостаточно для того, чтобы охарактеризовать все точки прямой. Так, например, откладывая на прямой вправо от начала координат отрезок, равный диагонали квадрата со стороной 1, мы получим точку, не имеющую рациональной абсциссы [1]).

[1]) Потому что диагональ квадрата, равная $\sqrt{2}$, несоизмерима с его стороной.

Но если ввести иррациональные числа, то всякая точка изобразится числом (рациональным или иррациональным) и область чисел приобретёт ту же полноту или, лучше сказать, ту же непрерывность, как и прямая линия. Уже отсюда мы видим, что иррациональные числа неразрывно связаны с понятием непрерывности, имеющим для анализа фундаментальное значение. Рациональные и иррациональные числа, взятые вместе, образуют систему действительных чисел. Эта система является полем, так как она удовлетворяет всем требованиям, определяющим поле.

Однако, не все действительные числа являются корнями уравнения с рациональными коэффициентами. Оказывается, что существуют два класса действительных чисел: числа алгебраические — корни уравнений с рациональными коэффициентами и числа трансцендентные, не удовлетворяющие никакому уравнению с рациональными коэффициентами. С алгебраической точки зрения более строгим было бы построение расширения, содержащего только алгебраические числа. Такое построение существует, но оно является тонким и чрезмерно абстрактным.

§ 36. Многочлены в поле действительных чисел

Мы будем теперь изучать многочлены не только с рациональными, но и с любыми действительными коэффициентами. Все определения и выводы, содержащиеся в §§ 28—31 главы V, можно дословно повторить и для многочленов с действительными коэффициентами, так как поле P может быть в частности и полем действительных чисел. А именно, понятия равенства, суммы и произведения многочленов остаются теми же, что и выше; относительно действий сложения и умножения многочлены с действительными коэффициентами образуют кольцо, которое мы будем называть кольцом многочленов в поле действительных чисел; остаётся в силе также алгоритм Эвклида со всеми его следствиями: как и выше (см. § 31), мы будем действительное число a называть корнем многочлена $f(x)$ или уравнения $f(x)=0$, если $f(a)=0$ и т. д. Мало того: остаются в силе и все выводы §32 о границах корней, надо только всюду вместо слова «рациональный корень» употреблять слово «действительный корень». В самом деле, понятие абсолютной величины, которое играет решающую роль в §32, без всяких изменений переносится и на действительные числа: попрежнему мы можем назвать абсолютной величиной числа a (действительного) то из значений a или $-a$, которое является положительным.

Но многочлены в поле действительных чисел обладают сверх того целым рядом дополнительных свойств, тесно связанных с понятием непрерывности. Мы ограничимся главнейшими свойствами.

1. *Многочлен и его производная непрерывны.*

Как известно из анализа, функция $f(x)$ называется непрерывной при $x=a$, если для любого сколь угодно малого (действительного) числа $\varepsilon>0$ можно подобрать такое малое число $\eta>0$, что

$$|f(a+h)-f(a)|<\varepsilon \text{ при } |h|<\eta.$$

лагаем $f(a+h)$ в ряд Тэйлора:

$$f(a+h)=f(a)+hf'(a)+\cdots+\frac{h^n}{n!}f^{n)}(a).$$

откуда

$$f(a+h)-f(a)=hf'(a)+\cdots+\frac{h^n}{n!}f^{(n)}(a).$$

Абсолютная величина суммы меньше или равна сумме абсолютных величин; следовательно:

$$|f(a+h)-f(a)|\leqslant|h||f'(a)|+\ldots+|h|^n\left|\frac{1}{n!}f^{(n)}(a)\right|.$$

Усилим неравенство, заменяя $|f'(a)|, \ldots, \left|\frac{1}{n!}f^{(n)}(a)\right|$ их наибольшей величиной A:

$$|f(a+h)-f(a)|\leqslant A(|h|+|h|+\cdots+|h|^n).$$

Приращение h можно выбрать столь малым, что $|h|<1$. Тогда очевидно, неравенство усилится, если степени $|h|^2, \ldots, |h|^n$ заменить большей величиной $|h|$. Таким образом имеем:

$$|f(a+h)-f(a)|<A(|h|+|h|+\cdots+|h|)=|h|nA.$$

Отсюда сразу видно, что при $|h|<\eta=\frac{\varepsilon}{nA}$

$$|f(a+h)-f(a)|<\varepsilon.$$

Непрерывность производной очевидна, так как производная от многочлена есть также многочлен.

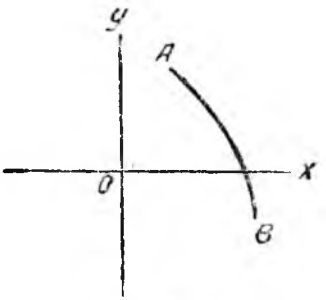
II. *Если значения $f(a)$ и $f(b)$ разных знаков, то в промежутке (a, b) лежит по меньшей мере один корень многочлена $f(x)$.*

Допустим для определённости, что $f(a)>0$ и $f(b)<0$. Поскольку многочлен есть функция непрерывная, он при изменении x от a до b должен перейти от положительного значения $f(a)$ к отрицательному $f(b)$ через все промежуточные значения, в том числе и через нуль. Следовательно, в промежутке (a, b) наша функция по меньшей мере один раз обращается в нуль.

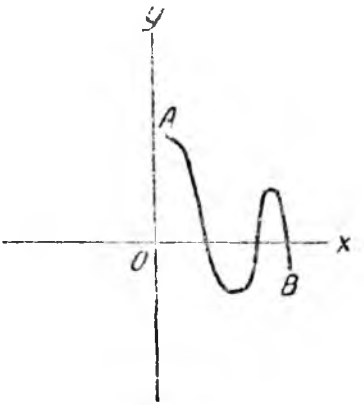
Геометрически это свойство вполне очевидно. В самом деле, многочлен $f(x)$ как непрерывная функция графически изображается непрерывной кривой $y=f(x)$. Если $f(a)>0$ и $f(b)<0$, то это значит, что точка A кривой с координатами $[a, f(a)]$ должна лежать над осью абсцисс, а точка кривой B с координатами $[b, f(b)]$ под осью абсцисс (см. черт. 2). Следовательно, кривая должна где-то между A и B пересечь ось x-ов, причём она может пересечь ось даже несколько раз (см. черт. 3).

Свойство II можно несколько уточнить. Дело в том, что ось абсцисс делит плоскость XOY на две части: на верхнюю и нижнюю полуплоскости. Если $f(a)$ и $f(b)$ имеют разные знаки, то точки A и B находятся в разных полуплоскостях. Если знаки у $f(a)$ и $f(b)$ одина-

ковы, то точки A и B лежат в одной полуплоскости. С другой стороны, из одной полуплоскости в другую можно перейти, пересекая ось OX один, три и вообще нечётное число раз. Напротив, пересекая ось OX чётное число раз, мы будем возвращаться в исходную полуплоскость. Таким образом получается следующий результат: *если $f(a)$ и $f(b)$ разных знаков, то в промежутке (a, b) лежит нечётное число корней многочлена $f(x)$. Если же знаки у $f(a)$ и $f(b)$ одинаковые,*



Черт. 2.



Черт. 3.

то в промежутке (a, b) либо вовсе нет действительных корней, либо имеется чётное число корней [1]).

Свойство II в соединении с теоремой Ролля оказывается весьма полезным при вычислении корней уравнений. Теорема Ролля должна быть известна из анализа, но мы, однако, приведем её здесь, сформулировав применительно к многочленам.

Теорема Ролля. *Между двумя корнями многочлена лежит по меньшей мере один корень его производной.*

Покажем на конкретном примере, как можно с помощью свойства II вычислить корни. Рассмотрим хотя бы уравнение

$$f(x) = x^3 - x^2 + 2x + 1 = 0. \qquad (1)$$

Прежде всего находим границы корней; с помощью четвёртого способа (см. § 32, стр. 174) устанавливаем, что все действительные корни лежат между -1 и $+1$. Кроме того, наше уравнение не может иметь более трёх действительных корней, так как оно третьей степени (см. § 31, стр. 166). Чтобы получить более совершенные результаты, воспользуемся свойством II многочленов. Легко видеть, что $f(-1) = -3$ и $f(1) = 3$; поэтому один действительный корень существует наверное. Но может быть существуют ещё корни? Производная от левой части нашего уравнения равна:

$$f'(x) = 3x^2 - 2x + 2$$

[1]) При этом кратный корень считается столько раз, какова его кратность.

и нетрудно заметить, что $f'(x)$ совсем не имеет действительных корней. Чтобы убедиться в этом, достаточно решить квадратное уравнение

$$3x^2 - 2x + 2 = 0$$

относительно x.

Следовательно, уравнение (1) более одного действительного корня иметь не может. В самом деле, если бы существовало два корня многочлена $f(x)$, то его производная $f'(x)$ по теореме Ролля имела бы по меньшей мере один действительный корень, а этого нет.

Итак, нам остаётся вычислить единственный действительный корень уравнения. Опять на помощь приходит свойство II. Составляем среднее арифметическое из нижней и верхней границ корня $\frac{-1+1}{2} = 0$ и подставляем значение 0 в левую часть (1). Мы видим, что

$$f(0) = 1 > 0, \quad f(-1) = -3 < 0,$$

стало быть, корень лежит между -1 и 0; получились более тесные пределы корня. Снова составляем среднее арифметическое из пределов: $\frac{-1+0}{2} = -\frac{1}{2}$. Видим, что $f\left(-\frac{1}{2}\right) < 0$, $f(0) > 0$, следовательно, корень лежит между $-\frac{1}{2}$ и 0. Опять сужаем границы $\frac{-\frac{1}{2}+0}{2} = -\frac{1}{4}$: $f\left(-\frac{1}{2}\right) > 0$, $f\left(-\frac{1}{4}\right) = -\frac{1}{64} - \frac{1}{16} - \frac{1}{2} + 1 > 0$. Получаются более тесные границы $-\frac{1}{2}$ и $-\frac{1}{4}$. Очевидно, что такой процесс вычисления можно продолжать бесконечно, и мы будем иметь сколь угодно близкие приближения к корню. Существуют, впрочем, гораздо более совершенные методы вычисления корней; они будут рассмотрены ниже.

§ 37. Число корней уравнения

Разобранное выше свойство II многочленов позволяет сделать некоторые выводы относительно числа действительных корней уравнения

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$$

с действительными коэффициентами.

Прежде всего докажем такое вспомогательное предложение: *при достаточно большом по абсолютной величине значении x знак многочлена $f(x)$ совпадает со знаком его старшего члена a_0x^n.*

Доказательство. Покажем, что при $|x| > \frac{A}{|a_0|} + 1$, где A — наибольшая из абсолютных величин коэффициентов $a_1, a_2, \ldots, a_n$, имеет место неравенство

$$|a_1x^{n-1} + \cdots + a_n| < a_0x^n. \qquad (1)$$

Действительно,

$$|a_1x^{n-1}+a_2x^{n-2}+\cdots+a_n|\leqslant|a_1|\,|x|^{n-1}+|a_2|\,|x|^{n-2}+\cdots+|a_n|,$$

или, заменяя $|a_1|, |a_2|, \ldots, |a_n|$ через A,

$$|a_1x^{n-1}+a_2x^{n-2}+\cdots+a_n|\leqslant A(|x|^{n-1}+|x|^{n-2}+\cdots+1)=$$
$$=A\frac{|x|^n-1}{|x|-1}. \qquad (2)$$

Но

$$|x|>\frac{A}{|a_0|}+1.$$

Стало быть

$$\frac{A}{|a_0|}<|x|-1 \text{ и } A<|a_0|(|x|-1),$$

откуда, подставляя в правую часть неравенства (2) вместо A заведомо бо́льшую величину $|a_0|(|x|-1)$, получаем:

$$|a_1x^{n-1}+a_2x^{n-2}+\cdots+a_n|<|a_0|(|x|-1)\frac{|x|^n-1}{|x|-1}=$$
$$=|a_0|(|x|^n-1)<|a_0||x|^n=|a_0x^n|,$$

т. е. мы пришли к неравенству (1).

А теперь теорема становится очевидной: если старший член a_0x^n по абсолютной величине больше, чем все остальные, взятые вместе, то знак многочлена $f(x)$ совпадает со знаком старшего члена.

После этого можно перейти к разбору следующей теоремы.

Теорема. *Уравнение нечётной степени имеет по крайней мере один действительный корень.*

Доказательство. При достаточно большом по абсолютной величине значении x многочлен

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$$

по доказанному имеет знак своего старшего члена a_0x^n. Но в силу нечётности n член a_0x^n имеет разные знаки при $x>0$ и $x<0$. Таким образом, если M достаточно большое положительное число, то $f(M)$ будет иметь знак, противоположный знаку $f(-M)$. Поэтому, в силу свойства II, должно существовать число $x=x_0$, лежащее между $-M$ и M, для которого $f(x)=0$.

Следствие. *Число действительных корней уравнения имеет ту же чётность, что и степень уравнения.*

В самом деле, если уравнение $f(x)=0$ степени n имеет s действительных корней $a_1, a_2, \ldots, a_s$, то

$$f(x)=(x-a_1)(x-a_2)\cdots(x-a_s)f_1(x),$$

где $f_1(x)$ многочлен степени $n-s$, не имеющий действительных корней. В силу только что доказанной теоремы степень $n-s$ функции $f_1(x)$ не может быть нечётной; следовательно, $n-s$ есть чётное число, а это как раз и требовалось показать.

Таким образом уравнение четвёртой степени имеет либо четыре, либо два, либо ни одного действительного корня, уравнение пятой степени имеет пять, три или один корень.

§ 38. Отделение корней. Теорема Штурма

Как известно из элементарной алгебры, квадратное уравнение $x^2+px+q=0$ без особого труда решается по формуле $x=-\frac{p}{2}\pm\sqrt{\frac{p^2}{4}-q}$. Гораздо сложнее обстоит дело с уравнениями высших степеней. Мы ниже увидим (глава IX), что далеко не все уравнения выше четвёртой степени допускают алгебраическое решение; таким образом поневоле приходится обращаться к приближённым методам вычисления корней. К тому же приближённые методы решения нередко в практическом отношении оказываются более удобными, чем точное вычисление по формуле.

Процесс вычисления действительных корней состоит из трёх частей:

1) Нахождение границ действительных корней. Этот вопрос можно считать уже выясненным (см. § 32).

2) Отделение корней, т. е. нахождение таких промежутков, в каждом из которых лежит один и только один действительный корень заданного уравнения.

3) Вычисление корней.

Существует довольно много приёмов отделения корней, но из них самым совершенным в теоретическом отношении является способ Штурма.

Сделаем предварительно несколько замечаний.

1. Пусть дана последовательность чисел, например:

$$5,\ -8,\ -7,\ 1. \tag{1}$$

Мы видим, что знаки чисел чередуются следующим образом:

$$+\ -\ -\ +$$

и меняются два раза: один раз в начале с плюса на минус и один раз в конце с минуса на плюс, т. е. в ряде чисел (1) наблюдаются две перемены знаков. Возьмём другой пример:

$$5,\ -8,\ 1,\ -3,\ 2,\ -5,\ -7.$$

Здесь наблюдается пять перемен знаков.

2. Пусть $f(x)$ — многочлен с действительными коэффициентами. Мы можем предположить, что многочлен $f(x)$ не имеет кратных множителей, т. е. он взаимно прост со своей производной $f'(x)$. В самом деле, если бы $f(x)$ имел кратные множители, то мы их заранее выделили бы (см. § 30).

Применим теперь алгоритм Эвклида к $f(x)$ и $f'(x)$ с тем только отступлением, что мы будем каждый раз знак остатка менять на обратный. Например, если $r(x)$ — остаток от деления $f(x)$ на $f'(x)$,

то мы вместо него будем рассматривать $f_1(x) = -r(x)$. Таким образом получаем:

$$\left.\begin{aligned} f(x) &= g(x) f'(x) - f_1(x), \\ f'(x) &= g_1(x) f_1(x) - f_2(x), \\ &\cdots\cdots\cdots\cdots\cdots \\ f_{m-2}(x) &= g_{m-1}(x) f_{m-1}(x) - f_m(x). \end{aligned}\right\} \qquad (2)$$

Последовательность многочленов

$$f(x),\quad f'(x),\ f_1(x),\ \ldots,\ f_{m-1}(x),\ f_m(x)$$

называется *рядом функций Штурма*. Очевидно, что последняя функция Штурма $f_m(x)$ должна быть постоянным числом, так как $f(x)$ и $f'(x)$ взаимно просты.

Пример. Рассмотрим

$$f(x) = x^4 - 5x^2 + 8x - 8.$$

Прежде всего следовало бы убедиться, не имеет ли многочлен $f(x)$ кратных множителей, но мы можем сразу начать с построения ряда функций Штурма; если последняя функция ряда Штурма окажется отличной от постоянного, то $f(x)$ имеет кратные множители и их придётся отделить. Находим производную:

$$f'(x) = 4x^3 - 10x + 8$$

и делим $f(x)$ на $f'(x)$. Так как знаки функций $f_i(x)$ здесь очень существенны, то, в отличие от алгоритма Эвклида, умножать и сокращать можно только на положительные числа. Итак, чтобы избежать дробных коэффициентов, умножаем $f(x)$ на 4 и делим на $f'(x)$:

$$\begin{array}{l|l} 4x^4 - 20x^2 + 32x - 32 & 4x^3 - 10x + 8 \\ \underline{4x^4 - 10x^2 + 8x} & \overline{x} \\ -10x^2 + 24x - 32 & \end{array}$$

(сокращаем на 2)

$$-5x^2 + 12x - 16.$$

Следовательно, меняя у остатка знаки на противоположные, получаем $f_1(x) = 5x^2 - 12x + 16$. Делим $f'(x)$ на $f_1(x)$, для чего предварительно умножаем $f'(x)$ на 25:

$$\begin{array}{l|l} 100x^3 - 250x + 200 & 5x^2 - 12x + 16 \\ \underline{100x^3 - 240x^2 + 320x} & \overline{20x + 48} \\ 240x^2 - 570x + 200 & \\ \underline{240x^2 - 576x + 768} & \\ 6x - 568 & \end{array}$$

откуда $f_2(x) = -3x + 284$. Наконец, делим $9f_1(x)$ на $f_2(x)$:

$$\begin{array}{r|l} 45x^2 - 108x + 144 & -3x + 284 \\ 45x^2 - 4260x & -15x - 346 \\ \hline 4152x + 144 & \end{array}$$

(сокращаем на 4)

$$\begin{array}{r} 1038x + 36 \\ 1038x - 98\,264 \\ \hline 98\,300 \end{array}$$

Остаток есть постоянное положительное число; поэтому $f_3(x)$ есть отрицательное число и можно просто положить $f_3(x) = -1$. В результате получился такой ряд функций Штурма:

$$\left.\begin{aligned} f(x) &= x^4 - 5x^2 + 8x - 8, \\ f'(x) &= 4x^3 - 10x + 8, \\ f_1(x) &= 5x^2 - 12x + 16, \\ f_2(x) &= -3x + 284, \\ f_3(x) &= -1. \end{aligned}\right\} \qquad (3)$$

Ряд функций Штурма обладает следующими важными свойствами:

a) *Никакие две соседние функции Штурма не имеют общих корней.*

Для доказательства обратимся к системе равенств (2).

Пусть два многочлена $f_k(x)$ и $f_{k+1}(x)$ имеют общий корень $x = a$; тогда $f_k(x)$ и $f_{k+1}(x)$ должны делиться на $x - a$. Рассмотрим теперь равенство

$$f_{k-1}(x) = g_k(x) f_k(x) - f_{k+1}(x).$$

Его правая часть, очевидно, делится на $x - a$; следовательно, и левая часть, т. е. $f_{k-1}(x)$ делится на $x - a$. Переходя к вышележащему равенству, точно так же получим, что $f_{k-2}(x)$ делится на $x - a$ и т. д. Поднимаясь шаг за шагом вверх, мы, наконец, дойдём до $f'(x)$ и $f(x)$ и обнаружим, что $f'(x)$ и $f(x)$ делятся на $x - a$. Но это невозможно, так как $f(x)$ и $f'(x)$ взаимно просты.

b) *Если какая-нибудь функция $f_k(x)$ обращается при $x = a$ в нуль, то две соседние функции $f_{k-1}(x)$ и $f_{k+1}(x)$ имеют противоположные знаки при $x = a$.*

Это свойство почти очевидно: из равенства

$$f_{k-1}(a) = g_k(x) f_k(x) - f_{k+1}(x)$$

получаем при $x = a$:

$$f_{k-1}(a) = -f_{k+1}(a);$$

так как по условию $f_k(a) = 0$.

c) *Если x, возрастая, проходит через корень какой-нибудь промежуточной функции Штурма, то число перемен знаков в ряду функций Штурма не меняется.*

Промежуточной функцией мы называем любую функцию ряда Штурма, кроме первой и последней.

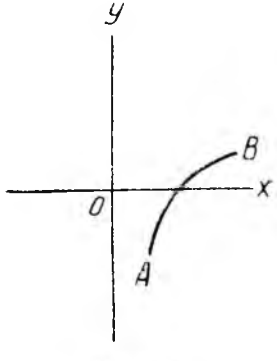
Пусть $x=a$ — корень $f_k(x)$. В силу свойств a) и b) $f_{k-1}(a)$ и $f_{k+1}(a)$ не равны нулю и имеют противоположные знаки. Выберем столь малый промежуток $(a-\varepsilon,\ a+\varepsilon)$, чтобы внутри и на его границах $f_{k-1}(x)$ и $f_{k+1}(x)$ не имели корней, т. е. сохраняли свой знак. Допустим для определённости, что для всех значений x в промежутке $(a-\varepsilon,\ a+\varepsilon)$ $f_{k+1}(x)<0$ и $f_{k-1}(x)>0$. Получается такая табличка знаков:

a	f_{k+1}	f_k	f_{k-1}
$x<a$	$-$		$+$
$x>a$	$-$		$+$

Какие бы знаки в пустых клетках ни ставить, всегда будет наблюдаться как при $x<a$, так и при $x>a$ одна перемена. Следовательно, при переходе через корень $x=a$ число перемен между f_{k+1}, f_k, f_{k-1} не меняется. В остальных частях ряда Штурма, где ни одна из функций не обращается при $x=a$ в нуль, число перемен измениться не может, а там, где при $x=a$ в нуль обращаются несколько промежуточных функций (эти промежуточные функции по a) не могут быть соседними), число перемен по только что доказанному также не меняется.

d) *Если x, возрастая, проходит через корень многочлена $f(x)$, то между многочленом $f(x)$ и его производной теряется одна перемена.*

Обозначим корень многочлена $f(x)$ через a. Попрежнему мы можем выбрать столь малый промежуток $(a-\varepsilon;\ a+\varepsilon)$, что внутри его производная $f'(x)$ не имеет корней, а $f(x)$ имеет только один корень $x=a$. При переходе через корень $x=a$ $f(x)$ меняет знак. Возможны только два случая: либо $f'(x)$ в промежутке $(a-\varepsilon,\ a+\varepsilon)$ положительна, либо $f'(x)$ в этом промежутке отрицательна. Пусть, например, $f'(x)>0$. Это означает, что в рассматриваемом промежутке многочлен $f(x)$ возрастает; поэтому $f(x)$ должно переходить от отрицательных значений к положительным (см. черт. 4). Получаем следующую табличку чередования знаков:



Черт. 4.

x	$f(x)$	$f'(x)$	*Число перемен*
$x<a$	$-$	$+$	1
$x>a$	$+$	$+$	0

таким образом между $f(x)$ и $f'(x)$ сперва была перемена знако
а после перехода через корень она потерялась. Подобный же р
зультат получается и при $f'(x)<0$ (здесь многочлен $f(x)$ буд
убывать).

Вернёмся к ряду функций (3). Если $x=0$, то

$$f(0)=-8,\quad f'(0)=8,\quad f_1(0)=16,\quad f_2(0)=284,\quad f_3(0)=-1;$$

если $x=2$, то

$$f(2)=4,\quad f'(2)=20,\quad f_1(2)=12,$$
$$f_2(2)=278,\quad f_3(2)=-1.$$

Получается такая табличка:

x	$f(x)$	$f'(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	*Число перемен*
0	—	+	+	+	—	2
2	+	+	+	+	—	1

Мы замечаем, что при переходе от $x=0$ к $x=2$ число перемен умен
шилось на 1; иными словами, потерялась одна перемена. Разгадк
этого явления кроется в теореме Штурма.

Теорема Штурма. *Число корней многочлена $f(x)$ в промежут
(a, b) равно числу потерянных перемен в ряду функций Штурма пр
возрастании x от a до b.*

Доказательство. В самом деле, что происходит при во
растании x? Если x проходит через корень промежуточной функци
то по свойству c) число перемен в ряду функций Штурма остаёт
без изменения. Если x проходит через корень многочлена $f(x)$,
по свойству d) между $f(x)$ и $f'(x)$, а потому и во всём ряду функций
Штурма, теряется одна перемена. Таким образом при возрастании
от a до b число перемен должно уменьшаться на столько едини
сколько корней имеется в промежутке (a, b).

Замечание. Может случиться, что для одной из границ
или b обращается в нуль одна или несколько промежуточных фун
ций Штурма. В этом случае при подсчёте числа перемен знако
можно просто отбросить все промежуточные функции, равные нулю
Действительно, пусть $f_i(x)$ равна нулю при $x=a$. По свойств
b) функции $f_{i-1}(x)$ и $f_{i+1}(x)$ при $x=a$ должны иметь противоположны
знаки, и какой бы знак ни приписывать $f_i(a)$, всегда $f_{i-1}(a)$, $f_i(a$
$f_{i+1}(a)$ будут давать одну перемену знака.

Пример. Возьмём

$$f(x)=3x^4-4x^3-6x^2-12x+1.$$

Составляем ряд функций Штурма:

$$f(x) = 3x^4 - 4x^3 - 6x^2 - 12x + 1,$$
$$\tfrac{1}{12} f'(x) = x^3 - x^2 - x - 1,$$
$$f_1(x) = 2x^2 + 5x,$$
$$f_2(x) = -31x + 4,$$
$$f_3(x) = -1.$$

Прежде всего найдём число действительных корней. При достаточно большом по абсолютной величине значении x знак каждой функции Штурма совпадает со знаком её старшего члена. Следовательно, обозначив достаточно большое положительное значение x через $+\infty$ и достаточно большое по абсолютной величине отрицательное значение x через $-\infty$, получим такую табличку:

x	$f(x)$	$f'(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	Число перемен	
$-\infty$	+	−	+	+	−	3	
0	+	−	0	+	−	3	потеряны две перемены
$+\infty$	+	+	+	−	−	1	

При возрастании x от $-\infty$ до 0 число перемен осталось без изменения; значит, наш многочлен совсем не имеет отрицательных корней. Зато, при возрастании x от 0 до $+\infty$ потерялись две перемены; поэтому многочлен имеет два положительных корня. Попробуем их отделить. С помощью способа Ньютона (см. § 32) нетрудно убедиться, что верхняя граница положительных корней равна 3. Применяем теорему Штурма:

x	$f(x)$	$f'(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	Число перемен	
0	+	−	0	+	−	3	потерялась одна перемена
1	−	−	+	−	−	2	
2	−	+	+	−	−	2	потерялась одна перемена
3	+	+	+	−	−	1	

Итак, корни отделены: первый корень лежит в промежутке (0, 1), а второй в промежутке (2, 3).

Недостатком метода Штурма является большая его громоздкость.

Задачи. 1. Отделить корни уравнений

$$\text{a) } x^4-2x^2+x-5=0, \quad \text{b) } x^3-6x^2-x+1=0.$$

2. Показать с помощью теоремы Штурма, что уравнение

$$x^3+px+q=0$$

при $\frac{p^3}{27}+\frac{q^2}{4}>0$ имеет один действительный корень, а при $\frac{p^3}{27}+\frac{q^2}{4}<0$ — три действительных корня.

3. Показать, что многочлен n-й степени с положительным коэффициентом при старшем члене тогда и только тогда имеет n действительных корней, когда ряд Штурма состоит из $n+1$ функций с положительными коэффициентами при старших членах.

4. С помощью теоремы Штурма показать, что производная $f'(x)$ не может сохранять знак между двумя корнями многочлена $f(x)$ (отсюда как простое следствие получается теорема Ролля).

Во многих случаях полезным оказывается следующее предложение.

Теорема Декарта. *Число положительных корней уравнения*

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n=0 \quad (a_0>0) \tag{4}$$

равно или на чётное число меньше числа перемен в ряду его коэффициентов [1]).

Например, в уравнении

$$f(x)=x^4-6x^3+8x^2+4x-1=0$$

наблюдаются три перемены; следовательно, уравнение имеет три или один положительный корень.

Сделаем предварительно несколько замечаний.

Замечание 1. Пусть производная $f'(x)$ многочлена $f(x)$ имеет s положительных корней. Тогда многочлен $f(x)$ должен иметь не более чем $s+1$ положительных корней. В самом деле, если бы $f(x)$ имел, например, $s+2$ положительных корня, то по теореме Ролля его производная имела бы по меньшей мере $s+1$, а не s положительных корней.

Замечание 2. В ряду чисел:

$$a_0,\ a_1,\ \ldots,\ a_n$$

может быть чётное число перемен лишь в том случае, когда a_0 и a_n одного знака. Напротив, нечётное число перемен возможно лишь в том случае, когда знаки у a_0 и a_n разные.

Так, в ряду чисел:

$$1,\ -2,\ 3,\ -5.\ 6$$

[1]) Само собой разумеется, что при подсчёте числа перемен коэффициенты, равные нулю, следует отбрасывать.

имеются четыре перемены, а в ряду чисел

$$-5,\ 1,\ 2,\ -7,\ 1$$

три перемены.

Замечание 3. Обозначим через p число перемен между коэффициентами уравнения (4). Мы утверждаем, что число положительных корней уравнения может отличаться от p только на чётное число. Действительно, если p чётное число, то согласно замечанию 2 a_n должно иметь тот же знак, что и a_0. При достаточно большом положительном значении $x = M$ знак многочлена, как известно (см. § 37), совпадает со знаком его старшего члена a_0x^n; следовательно, $f(0) = a_n$ и $f(M)$ одного знака. Таким образом мы видим, что в промежутке $(0, M)$, содержащем все положительные корни рассматриваемого уравнения, лежит чётное число корней.

Если же p нечётно, то согласно замечанию 2 a_0 и a_n должны иметь разные знаки; поэтому и $f(0) = a_n$ и $f(M)$ должны иметь разные знаки, откуда следует, что в промежутке $(0, M)$ должно лежать нечётное число корней.

Итак, число положительных корней и p должно быть одновременно либо чётным, либо нечётным, т. е. они отличаются друг от друга на чётное число.

Доказательство теоремы Декарта. Для уравнения $f(x) = ax + b = 0$ первой степени теорема очевидна: его единственный корень $x = -\frac{b}{a}$ может быть положительным только тогда, когда знаки у a и b разные, т. е. когда коэффициенты a, b дают одну перемену.

Проведём доказательство методом индукции: предположим, что теорема доказана для уравнений $(n-1)$-й степени; докажем её справедливость для уравнений n-й степени.

Обозначим число перемен в уравнении (4) через p. Тогда в ряду коэффициентов производной

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \ldots + a_{n-1}$$

будет не более p перемен. Но $f'(x)$ — многочлен $(n-1)$-й степени для него теорема предполагается справедливой; следовательно $f'(x)$ имеет не более p положительных корней, а потому уравнение (4) в силу замечания 1 имеет не более $p+1$ положительных корней. Но в силу замечания 3 число положительных корней уравнения (4) не может быть равно $p-1$, так как p и $p+1$ числа разной чётности. На основании того же замечания мы можем заключить, что число положительных корней равно p или меньше его на чётное число.

Таким образом, предполагая теорему Декарта справедливой для уравнений $(n-1$-й) степени, мы показали, что она верна и для уравнений n-й степени.

Но теорема верна для $n = 1$; стало быть, она верна для $n = 2$, 3, 4 и т. д., т. е. для любого n.

С помощью теоремы Декарта можно определять не только число положительных, но и число отрицательных корней уравнения. Обратимся к конкретному примеру. Рассмотрим уравнение

$$f(x) = x^3 - 2x - 1 = 0.$$

В ряду коэффициентов наблюдается только одна перемена. Следовательно, заданное уравнение имеет всего один положительный корень. Полагаем далее $x = -y$; получим

$$\varphi(y) = y^3 - 2y + 1 = 0.$$

В последнем уравнении наблюдаются две перемены; поэтому заданное уравнение имеет два или нуль отрицательных корней.

З а д а ч а. С помощью теоремы Декарта определить число положительных и отрицательных корней уравнений

а) $x^5 - x^3 - 1 = 0$,

b) $x^4 - 2x^3 - 2x^2 - 5x - 1 = 0$,

c) $x^7 + x^3 - 1 = 0$.

§ 39. Вычисление корней

Мы здесь разберём три метода вычисления корней.

Способ Горнера-Руффини. Идея этого способа состоит в следующем. Обозначим целую часть искомого корня уравнения $f(x) = 0$ через a. Тогда, полагая $x = a + y$ и разлагая $f(x) = f(a + y)$ в ряд Тэйлора по степеням y, получим уравнение

$$\varphi_1(y) = 0,$$

которое имеет корень между 0 и 1. Если затем положить $10y = z$, то получится уравнение

$$\varphi_2(z) = 0,$$

которое имеет корень между 0 и 10. Пусть целая часть этого корня равна a_1. Снова полагаем $z = a_1 + u$ и разлагаем $\varphi_2(z) = \varphi_2(a_1 + u)$ в ряд Тэйлора по степеням u, после чего получим уравнение

$$\varphi_3(u) = 0,$$

имеющее корень между 0 и 1, и т. д. Очевидно, что, повторяя достаточное число раз подобные преобразования, мы достигнем требуемой точности. При этом a будет целой частью искомого корня, a_1 — числом десятых корня, a_2 — числом сотых корня, a_3 — числом тысячных корня и т. д.

Поясним метод Горнера на конкретном примере.

Рассмотрим уравнение

$$f(x) = x^3 - 8x + 1 = 0.$$

По способу Ньютона можно установить, что корни лежат между -3 и $+3$. Чтобы отделить корни, воспользуемся теоремой Штурма. Для данного многочлена $f(x)$ получается такой ряд Штурма:

$$f(x) = x^3 - 8x + 1;$$
$$f'(x) = 3x^2 - 8,$$
$$f_1(x) = 16x - 3,$$
$$f_2(x) = 1,$$

откуда имеем следующую таблицу чередования знаков:

x	f	f'	f_1	f_2	*Число перемен*
-3	$-$	$+$	$-$	$+$	3
-2	$+$	$+$	$-$	$+$	2
-1	$+$	$-$	$-$	$+$	2
0	$+$	$-$	$-$	$+$	2
1	$-$	$-$	$+$	$+$	1
2	$-$	$+$	$+$	$+$	1
3	$+$	$+$	$+$	$+$	0

Таким образом первый корень лежит в промежутке $(-3, -2)$, второй в промежутке $(0, 1)$ и третий в промежутке $(2, 3)$.

Вычислим теперь способом Горнера один из корней, например, третий корень, с точностью до 0,001.

Целая часть корня, лежащего между 2 и 3, равна 2. Поэтому полагаем $x = 2 + y$ и разлагаем $f(2 + y)$ в ряд по степеням y. Разложение удобнее всего проводить с помощью схемы Горнера (см. § 32, стр. 172):

	1	0	-8	1
2	1	2	-4	-7
2	1	4	4	
2	1	6		
2	1			

Таким образом получается уравнение

$$y^3+6y^2+4y-7=0.$$

Далее заменяем y через $\frac{z}{10}$:

$$\left(\frac{z}{10}\right)^3+6\left(\frac{z}{10}\right)^2+4\left(\frac{z}{10}\right)-7=0$$

или в окончательном виде:

$$z^3+60z^2+400z-7000=0. \qquad (1)$$

Заметим, что уравнение (1) можно было сразу получить путём умножения чисел 1, 6, 4 и 7 соответственно на 1, 10, 100 и 1000.

Испытывая числа 0, 1, 2, 3, 4, 5, 6, 7 и 8; видим, что уравнение (1) имеет корень между 7 и 8; стало быть, $a_1=7$. Составляем схему Горнера:

	1	60	400	−7 000
7	1	67	869	−917
7	1	74	1 387	
7	1	81		
7	1			

Отсюда, умножив 1, 81, 1 387 и −917 соответственно на 1, 10, 100 и 1 000, получаем уравнение

$$u^3+810u^2+138\,700u-917\,000=0.$$

имеющее корень между 6 и 7. Следовательно, $a_2=6$. Снова составляем схему Горнера:

	1	810	138 700	−917 000
6	1	816	143 596	−55 424
6	1	822	148 528	
6	1	828		
6	1			

Получаем уравнение

$$v^3+8280v^2+14\,852\,800v-55\,424\,000=0,$$

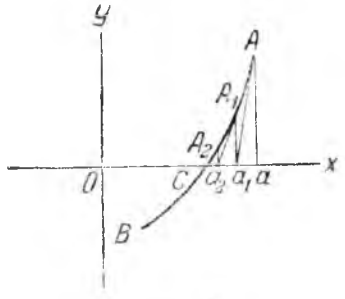
корень которого лежит между 3 и 4.

Итак, с точностью до 0,001 корень данного уравнения равен:

$$x\approx 2{,}763.$$

При дальнейших вычислениях получаются уравнения с настолько большими коэффициентами, что метод Горнера-Руффини оказывается невыгодным.

Мы сейчас разберём два других метода, позволяющих с большей быстротой приблизиться к корню. Без всякого нарушения общности выводов можно предположить, что многочлен $f(x)$ взаимно прост со своей производной; в противном случае мы отделили бы кратные множители.



Черт. 5.

Способ Ньютона. Пусть уравнение $f(x)=0$ имеет корень x_0, лежащий в промежутке (a, b). Геометрически этому корню соответствует точка пересечения C кривой $y=f(x)$ с осью OX (см. черт. 5)[1]). Мы можем приблизиться к корню следующим образом. Проведём через точку A с координатами a и $f(a)$ касательную к кривой. Она пересечёт ось OX в a_1, причём a_1 будет находиться ближе к корню, чем a. Через точку A_1 с координатами a_1 и $f(a_1)$ снова можно провести касательную, которая пересечёт ось OX в a_2, ещё ближе к корню, чем a_1 и т. д. В результате получится ряд значений a, a_1, a_2, a_3, $\cdots$, неограниченно приближающихся к корню x_0.

Найдём, чему равны a_1, a_2, a_3, $\cdots$ Угловой коэффициент касательной в точке $A\,[a, f(a)]$ равен $f'(a)$; отсюда получается такое уравнение касательной:

$$y-f(a)=f'(a)(x-a).$$

Чтобы найти точку пересечения a_1, полагаем $y=0$:

$$-f(a)=f'(a)(a_1-a),$$

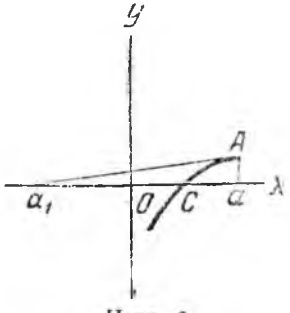
откуда

$$a_1=a-\frac{f(a)}{f'(a)}. \qquad (2)$$

Точно так же находим, что

$$a_2=a_1-\frac{f(a_1)}{f'(a_1)},$$

$$a_3=a_2-\frac{f(a_2)}{f'(a_2)} \text{ и т. д.}$$



Черт. 6.

Способ Ньютона следует применять, однако, с осмотрительностью. На черт. 5 кривая в точке A была обращена выпуклостью к оси OX. Посмотрим, что произойдёт в том случае, когда кривая обращена вогнутостью к оси OX (см. черт. 6). Если здесь провести

[1]) Кривая $y=f(x)$ не может касаться оси OX в точке C; если бы C была точкой касания, то $f(x_0)=0$ и $f'(x_0)=0$, что невозможно, так как многочлен $f(x)$ и его производная $f'(x)$ предполагаются взаимно простыми.

касательную в точке A, то мы не приблизимся, а удалимся от корня: a_1 отстоит гораздо дальше от C, чем a. Как известно из анализа, кривая в точке A тогда и только тогда обращена выпуклостью к оси OX, когда $f(a)$ и $f''(a)$ имеют одинаковые знаки или, что то же, когда

$$f(a)\,f''(a) > 0. \qquad (2')$$

Итак, способ Ньютона следует применять там, где выполняется условие (2').

На практике рекомендуется корень предварительно вычислять по способу Горнера-Руффини с точностью до 0,01 или 0,001 и затем уже вести дальнейшие вычисления с помощью метода Ньютона.

В качестве примера возьмём снова уравнение

$$f(x) = x^3 - 8x + 1 = 0.$$

Мы выше нашли, что один из корней этого уравнения равен 2,763 с точностью до 0,001. Так как

$$f(2{,}763) \approx -0{,}010791 < 0, \quad f(2{,}764) \approx 0{,}004119 > 0,$$

то корень лежит между 2,763 и 2,764. Воспользуемся теперь способом Ньютона; его надо применить к 2,764, потому что

$$f''(2{,}764)\ f(2{,}764) > 0.$$

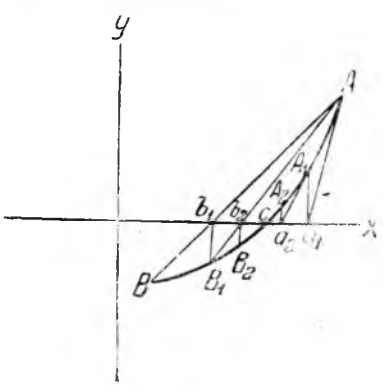
Имеем:

$$f'(2{,}764) \approx 14{,}9191,$$

$$a_1 = 2{,}764 - \frac{f(2{,}764)}{f'(2{,}764)} \approx 2{,}764 - \frac{0{,}004119}{14{,}9191} \approx 2{,}7637239.$$

Полученное приближение a_1 верно до шестого знака после запятой; в самом деле, подставляя значения 2,763723 и 2,763724 в многочлен $f(x)$, получим, что

$$f(2{,}763723) < 0, \quad f(2{,}763724) > 0.$$



Черт. 7.

Прямолинейное интерполирование [1]. С помощью геометрических соображений можно вывести ещё один способ приближённого вычисления корней. Пусть искомый корень уравнения находится в промежутке (a, b). Проведём через точки $A[a, f(a)]$ и $B[b, f(b)]$ кривой хорду AB (см. черт. 7). Она пересечёт ось OX в b_1, недалеко от точки C пересечения кривой с осью. Если затем провести хорду AB_1, где B_1 точка с координатами $[b_1, f(b_1)]$, то получится ещё более близкое приближение b_2 к корню. Этот процесс проведения хорд можно, очевидно, повторять безгранично; при этом каждый раз мы будем всё ближе и ближе подходить к корню.

[1]) Этот метод называется также способом ложного положения (Regula falsi).

Возникает вопрос: как определить значение b_1, b_2, ...? Тут на помощь приходит аналитическая геометрия. Составляем уравнение прямой, проходящей через точку A и B:

$$\frac{y-f(a)}{f(b)-f(a)}=\frac{x-a}{b-a}.$$

А теперь, чтобы найти b_1, полагаем $y=0$:

$$\frac{-f(a)}{f(b)-f(a)}=\frac{b_1-a}{b-a},$$

откуда

$$b_1=a-\frac{f(a)(b-a)}{f(b)-f(a)}. \qquad (3)$$

Формула (3) называется *формулой прямолинейного интерполирования*.

На черт. 7 видно, что приближения b_1, b_2, ..., получаемые прямолинейным интерполированием, лежат по другую сторону от корня, нежели приближения a_1, a_2, ..., полученные способом Ньютона. Таким образом, комбинируя прямолинейное интерполирование и способ Ньютона, мы будем приближаться к корню с двух сторон. На практике как раз и рекомендуется комбинировать оба эти способа.

Пример. Мы знаем, что уравнение

$$x^3-8x+1=0$$

имеет корень, лежащий в промежутке $(0, 1)$. Нетрудно убедиться с помощью метода Горнера-Руффини, что этот корень с точностью до 0,01 равен 0,12. Применяем теперь способы Ньютона и прямолинейного интерполирования. Так как

$$f(0{,}12)\approx 0{,}04173>0, \quad f(0{,}13)\approx -0{,}03780<0,$$

то корень лежит между 0,12 и 0,13. Способ Ньютона следует применить к 0,12, потому что $f(0{,}12)\,f''(0{,}12)>0$. Имеем

$$f'(0{,}12)\approx -7{,}9568,$$

$$a_1=0{,}12-\frac{f(0{,}12)}{f'(0{,}12)}\approx 0{,}12-\frac{0{,}04173}{-7{,}9568}\approx 0{,}125244.$$

Затем применяем прямолинейное интерполирование:

$$b_1=a-\frac{f(a)(b-a)}{f(b)-f(a)}\approx 0{,}12-\frac{0{,}04173\cdot 0{,}01}{-0{,}03780-0{,}04173}\approx 0{,}125247.$$

Приближения a_1 и b_1 отличаются лишь последними знаками; следовательно, корень с точностью до 0,00001 равен 0,12524. Продолжаем наши вычисления:

$$f(0{,}12524)\approx 0{,}00004439661>0, \quad f(0{,}12525)\approx -0{,}00003513280<0.$$

Стало быть, корень лежит между $a_1 = 0{,}12524$ и $b_1 = 0{,}12525$. Применяем к a_1 способ Ньютона:

$$f'(0{,}12524) \approx -7{,}95294482,$$

$$a_2 \approx 0{,}12524 - \frac{0{,}00004439661}{-7{,}95294482} \approx 0{,}125245582410.$$

Затем применяем к a_1 и b_1 прямолинейное интерполирование:

$$b_2 = a_1 - \frac{f(a_1)(b_1 - a_1)}{f(b_1) - f(a_1)} \approx 0{,}12524 - \frac{0{,}00004439661 \cdot 0{,}00001}{-0{,}00003513280 - 0{,}00004439661} \approx$$

$$\approx 0{,}125245582414.$$

Сравнивая a_2 и b_2, убеждаемся, что с одиннадцатью знаками после запятой корень равен 0,12524558241.

На этом мы заканчиваем главу VII. Более детальный разбор различных методов приближённого вычисления корней можно найти в книге Э. Уиттекер и Г. Робинсон. Математическая обработка результатов наблюдений, ГТТИ, 1933, а также в книге А. Н. Крылов, Лекции о приближённых вычислениях, 1933 (издание второе).

Задачи. 1. Вычислить с точностью до 0,001 положительный корень уравнения

$$x^3 - 2x - 5 = 0,$$

пользуясь методом Горнера-Руффини.

2. Комбинируя способы Ньютона и прямолинейного интерполирования, вычислить действительные корни уравнения

$$x^3 - 9x + 6 = 0$$

с четырьмя верными знаками после запятой.

3. Вычислить близкий к 1 корень уравнения

$$x^4 - x^3 + 8x^2 - 5 = 0$$

с точностью до 0,00001.

ГЛАВА ВОСЬМАЯ

КОМПЛЕКСНЫЕ ЧИСЛА И ОСНОВНАЯ ТЕОРЕМА АЛГЕБРЫ

§ 40. Комплексные числа

В предыдущей главе мы ввели действительные числа для того, чтобы добиться разрешимости *любого* алгебраического уравнения, но эта цель пока ещё не достигнута. Рассмотрим, например, квадратное уравнение вида

$$x^2 + px + q = 0, \tag{1}$$

где p и q — действительные числа. Как известно, действительные корни этого уравнения могут быть получены по формуле

$$x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

лишь в том случае, когда $\frac{p^2}{4}-q \geqslant 0$. Если же $\frac{p^2}{4}-q<0$, то уравнение (1) не будет иметь действительных корней. Таким образом область чисел нуждается в дальнейшем расширении для того, чтобы любое квадратное уравнение стало разрешимым.

В элементарной алгебре мнимая единица i определяется как корень квадратный из -1. Возникает вопрос, имеем ли мы право распространять действие извлечения квадратного корня, когда стоящее под корнем число отрицательно? Имеем ли мы право механически обобщать те или иные математические понятия? Что этот вопрос не лишён основания, показывает следующий пример.

Если распространить обычные правила действий над радикалами на корни квадратные из отрицательных чисел, то для $i=+\sqrt{-1}$ получится такое заведомо неверное равенство: $-1=i^2=+\sqrt{-1}\cdot+\sqrt{-1}=+\sqrt{(-1)^2}=+\sqrt{1}=1$.

Эти вопросы и возражения отпадут, если воспользоваться следующим методом. Именно, условимся изображать действительное число a в виде символа $(a, 0)$. Очевидно, что сумма и произведение двух действительных чисел a, b в новом обозначении запишутся так: $(a, 0)+(b, 0)=(a+b, 0)$ и $(a, 0)\cdot(b, 0)=(ab, 0)$. А теперь попытаемся расширить поле действительных чисел, воспользовавшись примером 4 в § 22 (см. стр. 115). А именно, введём следующие четыре требования:

I. Если действительное число b равно нулю, то символ (a, b) изображает действительное число a; если же $b\neq 0$, то (a, b) представляет число новой природы.

II. Символы (a, b) и (a_1, b_1) считаются равными только тогда, когда $a=a_1$ и $b=b_1$.

III.

$$(a, b)+(a_1, b_1)=(a+a_1, b+b_1).$$

IV.

$$(a, b)\cdot(a_1, b_1)=(aa_1-bb_1, ab_1+a_1b).$$

Требования I — IV нуждаются в некотором обосновании. Во-первых, надо показать, что операции сложения и умножения двух символов нисколько не противоречат обычным действиям сложения и умножения действительных чисел. Во-вторых, хотя мы и определили для символов (a, b) операции сложения и умножения, но будут ли они подчиняться сочетательному, переместительному и распределительному законам — пока неизвестно [1]).

Легко видеть, что в случае $b=b_1=0$ требования III и IV означают не что иное, как обыкновенное сложение и умножение действительных чисел:

$$(a, 0)+(a_1, 0)=(a+a_1, 0), \quad (a, 0)\cdot(a_1, 0)=(aa_1, 0).$$

[1]) Мы не говорим о равенстве двух символов: читатель может без особого труда убедиться, что оно обладает всеми свойствами обычного равенства двух чисел. Подробнее об этих свойствах см. в § 42.

Переходим ко второму пункту. Мы ограничимся выводом сочетательного закона. По определению сложения символов

$$[(a, b)+(a_1, b_1)]+(a_2, b_2)=(a+a_1, b+b_1)+(a_2, b_2)=$$
$$=(a+a_1+a_2, b+b_1+b_2), \qquad (2)$$
$$(a, b)+[(a_1, b_1)+(a_2, b_2)]=(a, b)+(a_1+a_2, b_1+b_2)=$$
$$=(a+a_1+a_2, b+b_1+b_2). \qquad (3)$$

Мы видим, что правая часть равенства (2) ничем не отличается от правой части равенства (3); следовательно:

$$[(a, b)+(a_1, b_1)]+(a_2, b_2)=(a, b)+[(a_1, b_1)+(a_2, b_2)],$$

т. е. мы доказали сочетательность сложения.

Точно так же выводится и сочетательность умножения. Именно, по определению умножения символов

$$[(a, b)\cdot(a_1, b_1)]\cdot(a_2, b_2)=(aa_1-bb_1, ab_1+a_1b)\cdot(a_2, b_2)=$$
$$=(aa_1a_2-ab_1b_2-a_1bb_2-a_2bb_1, aa_1b_2+aa_2b_1+a_1a_2b-bb_1b_2),$$
$$(a, b)\cdot[(a_1, b_1)\cdot(a_2, b_2)]=(a, b)\cdot(a_1a_2-b_1b_2, a_1b_2+a_2b_1)=$$
$$=(aa_1a_2-ab_1b_2-a_1bb_2-a_2bb_1, aa_1b_2+aa_2b_1+a_1a_2b-bb_1b_2),$$

и мы видим, что

$$[(a, b)\cdot(a_1, b_1)]\cdot(a_2, b_2)=(a, b)\cdot[(a_1, b_1)\cdot(a_2, b_2)].$$

Остальные законы (переместительный и распределительный) выводятся аналогичным образом; предоставляем читателю проделать самостоятельно все необходимые вычисления.

Итак, поскольку требования I—IV больше не вызывают сомнений, мы вправе назвать символ (a, b) числом; мы будем его называть *комплексным числом*. Очевидно, что действительное число $(a, 0)$ есть частный случай комплексного числа.

Мы до сих пор рассматривали прямые операции—сложение и умножение. Что же можно сказать о вычитании и делении? Оказывается, что для комплексных чисел вычитание всегда возможно, а деление возможно во всех случаях кроме, конечно, деления на нуль [1]). Иными словами, *множество комплексных чисел образует поле.*

Докажем это утверждение. Попробуем решить уравнение

$$(a, b)+z=(c, d). \qquad (4)$$

Обозначим z через (x, y); x и y пока неизвестны, их надо определить. Подставляя значение z в наше уравнение, получим:

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

или, вспомнив правило сложения комплексных чисел:

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

[1]) Нулём здесь служит, очевидно, число $(0, 0)$.

Но эти два комплексных числа могут быть равны только в том случае, когда

$$a + x = c; \quad b + y = d$$

(см. II); откуда

$$x = c - a, \quad y = d - b.$$

Итак, уравнение (4) решено, — мы нашли, что $z = (c - a, d - b)$. Стало быть, вычитание всегда возможно.

Переходим к делению. Возьмём уравнение

$$(a, b) \cdot z = (c, d) \quad \big((a, b) \neq (0, 0) = 0\big). \tag{5}$$

Попрежнему полагаем $z = (x, y)$. Если подставить это значение z в уравнение (5) и воспользоваться правилом умножения, то получится

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

откуда

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

Мы получили два линейных уравнения с двумя неизвестными; без особого труда находим, что

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

Следовательно:

$$z = \left(\frac{ac + bd}{a^2 + b^2}, \quad \frac{ad - bc}{a^2 + b^2}\right). \tag{6}$$

Итак, деление всегда возможно, если только делитель отличен от нуля.

Поле комплексных чисел, как всякое поле, должно обладать нулём и единицей. И действительно, роль нуля играет $(0, 0)$, т. е. действительное число 0, а роль единицы $(1, 0)$, т. е. действительное число единица.

До сих пор комплексное число мы изображали символом (a, b). Существует, однако, более удобная форма записи, при которой арифметические действия над комплексными числами приобретают особую наглядность. Рассмотрим число $(0, 1)$. Если его возвести в квадрат, то по определению умножения мы получим:

$$(0, 1)^2 = (-1, 0).$$

Но $(-1, 0)$ есть не что иное, как -1. Следовательно, $(0, 1)^2 = -1$. Мы видим, что в поле комплексных чисел квадратное уравнение $x^2 + 1 = 0$ разрешимо; его корнем является число $(0, 1)$, которое мы будем обозначать через i и называть мнимой единицей. Итак, $i = (0, 1)$ и $i^2 = -1$. Легко убедиться, что всякое число (a, b) можно представить в виде

$$(a, b) = (a, 0) + (0, b).$$

В свою очередь $(a, 0) = a$, $(0, b) = (b, 0) \cdot (0, 1) = bi$, поэтому

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

Мы получили обычную форму записи комплексного числа; здесь a называется действительной частью, bi—мнимой частью и b—коэффициентом мнимой части комплексного числа. Для дальнейшего полезно заметить, что согласно требованию II два комплексных числа равны между собой, когда их действительные части и коэффициенты мнимых частей равны между собой. В частности число $z = a + bi$ равно нулю лишь в том случае, когда $a = 0$, $b = 0$, т. е. когда равна нулю действительная часть и коэффициент мнимой части.

Теперь действия над комплексными числами становятся более наглядными. Мы сейчас увидим, что с выражениями $a + bi$ можно обращаться как с многочленами. В самом деле, по определению сложения:

$$(a, b) + (a_1, b_1) = (a + a_1, b + b_1)$$

или в обычной записи:

$$(a + bi) + (a_1 + b_1 i) = (a + a_1) + (b + b_1) i.$$

Таким образом комплексные числа $a + bi$, $a_1 + b_1 i$ складываются так, как складываются многочлены. Подобное же заключение можно вывести и относительно вычитания, а именно:

$$(a + bi) - (a_1 + b_1 i) = (a - a_1) + (b - b_1) i.$$

Далее, по определению умножения:

$$(a, b) \cdot (a_1, b_1) = (aa_1 - bb_1, ab_1 + a_1 b),$$

или в обычной записи:

$$(a + bi) \cdot (a_1 + b_1 i) = (aa_1 - bb_1) + (ab_1 + a_1 b) i.$$

Перемножим теперь $a + bi$ и $a_1 + b_1 i$ по правилу перемножения многочленов:

$$(a + bi)(a_1 + b_1 i) = aa_1 + ab_1 i + a_1 bi + bb_1 i^2.$$

Но $i^2 = -1$; поэтому

$$(a + bi)(a_1 + b_1 i) = (aa_1 - bb_1) + (ab_1 + a_1 b) i.$$

Мы пришли к тому же результату, что и выше.

Остаётся, наконец, разобрать деление. Мы знаем [см. формулу (6)], что

$$\frac{(c, d)}{(a, b)} = \left(\frac{ac + bd}{a^2 + b^2}, \frac{ad - bc}{a^2 + b^2} \right),$$

или в обычной записи:

$$\frac{c + di}{a + bi} = \frac{ac + bd}{a^2 + b^2} + \frac{ad - bc}{a^2 + b^2} i. \qquad (7)$$

Само собой разумеется, что $a+bi$ отлично от нуля. К этому же результату можно притти ещё иначе.

Назовём два комплексных числа *сопряжёнными*, если они отличаются друг от друга только знаком при мнимой части. Например, $2+i$ сопряжено с $2-i$. Легко показать, что произведение двух сопряжённых чисел есть действительное число; в самом деле:

$$(a+bi)(a-bi)=a^2-(bi)^2=a^2+b^2.$$

Постараемся теперь избавиться от мнимости в знаменателе дроби

$$\frac{c+di}{a+bi}.$$

Умножим для этой цели числитель и знаменатель на число, сопряжённое со знаменателем:

$$\frac{c+di}{a+bi}=\frac{(c+di)(a-bi)}{(a+bi)(a-bi)}=\frac{ac-bci+adi-bdi^2}{a^2+b^2}=$$
$$=\frac{(ac+bd)+(ad-bc)i}{a^2+b^2}=\frac{ac+bd}{a^2+b^2}+\frac{ad-bc}{a^2+b^2}i,$$

легко видеть, что получилось полное совпадение с формулой (7).

Примеры.

1. $(2+i)+(7-5i)=9-4i$,
2. $(3-i)-(8+11i)=-5-12i$,
3. $(3+i)(6-5i)=18-15i+6i-5i^2=23-9i$,
4. $\frac{3+i}{6-5i}=\frac{(3+i)(6+5i)}{(6-5i)(6+5i)}=\frac{18+15i+6i+5i^2}{36+25}=\frac{13+21i}{61}=\frac{13}{61}+\frac{21}{61}i$.

Задача. Вычислить следующие выражения:

a) $(2-i)+(3-12i)-(31+45i)-(8-7i)$,

b) $(2-i)\cdot(8-7i)-(20+11i)\cdot(1-3i)+(4-17i)\cdot(5-4i)$,

c) $\frac{(5-2i)\cdot(8+i)-(12-13i)(6+7i)}{(1-2i)^3+(1+2i)^3}$.

В поле комплексных чисел должны иметь место все основные законы алгебры. В частности всякое квадратное уравнение

$$x^2+px+q=0$$

с комплексными (а не только действительными) коэффициентами можно решить по формуле

$$x=-\frac{p}{2}\pm\sqrt{\frac{p^2}{4}-q}.$$

Очевидно, мы покажем, что всякое квадратное уравнение разрешимо в поле комплексных чисел, если докажем, что *из всякого комплексного числа можно извлечь квадратный корень.*

Для доказательства напишем уравнение

$$\alpha+\beta i=\sqrt{a+bi};$$

здесь α и β неизвестные, их надо определить. Если обе части уравнения возвысить в квадрат, то получится

$$(\alpha^2-\beta^2)+2\alpha\beta i=a+bi.$$

Но два комплексных числа равны; когда равны их действительные части и коэффициенты мнимых частей. Следовательно:

$$\alpha^2-\beta^2=a,\quad 2\alpha\beta=b.$$

Возвысим эти равенства во вторую степень и сложим. Получим в результате:

$$(\alpha^2+\beta^2)^2=a^2+b^2,$$

или

$$\alpha^2+\beta^2=+\sqrt{a^2+b^2}.$$

Корень квадратный мы взяли со знаком плюс, так как $\alpha^2+\beta^2$ должно быть, очевидно, положительно. Итак:

$$\alpha^2-\beta^2=a,\quad \alpha^2+\beta^2=+\sqrt{a^2+b^2}.$$

Решая эти уравнения относительно α^2 и β^2, без труда находим, что

$$\alpha^2=\frac{a+\sqrt{a^2+b^2}}{2},\quad \beta^2=\frac{-a+\sqrt{a^2+b^2}}{2}.$$

Таким образом имеем окончательно:

$$\left.\begin{aligned}\alpha&=\pm\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}};\\ \beta&=\pm\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}},\end{aligned}\right\}\qquad(8)$$

Выбирая знаки у α и β, нужно иметь в виду, что $2\alpha\beta=b$, т. е. α и β имеют знаки одинаковые, если $b>0$, и разные, если $b<0$.

Итак, цель, поставленная в начале этого параграфа, достигнута: *в поле комплексных чисел разрешимо любое квадратное уравнение.*

Пример 1. Уравнение

$$x^2-x+1=0$$

не имеет действительных корней, так как

$$\frac{p^2}{4}-q=\frac{1}{4}-1=-\frac{3}{4}<0.$$

Зато оно имеет комплексные корни

$$x_1=\frac{1}{2}+\sqrt{-\frac{3}{4}}=\frac{1}{2}+\frac{\sqrt{3}}{2}i,$$

$$x_2=\frac{1}{2}-\sqrt{-\frac{3}{4}}=\frac{1}{2}-\frac{\sqrt{3}}{2}i.$$

Пример 2. Решим квадратное уравнение

$$x^2-(4-6i)x+(10-20i)=0.$$

Здесь $p=-(4-6i)$, $q=10-20i$; поэтому

$$x=(2-3i)\pm\sqrt{(2-3i)^2-(10-20i)}=(2-3i)\pm\sqrt{-15+8i}.$$

Извлекаем корень квадратный из комплексного числа $-15+8i$ с помощью формул (8). Достаточно для α взять один знак, например плюс:

$$\alpha=\sqrt{\frac{-15+\sqrt{15^2+8^2}}{2}}=1.$$

Для β придётся взять тот же знак плюс, так как $2\alpha\beta=b=8$ положительно. Следовательно:

$$\beta=\sqrt{\frac{15+\sqrt{15^2+8^2}}{2}}=4,$$

откуда

$$\sqrt{-15+8i}=1+4i.$$

Итак:

$$x_1=(2-3i)+(1+4i)=3+i,$$
$$x_2=(2-3i)-(1+4i)=1-7i.$$

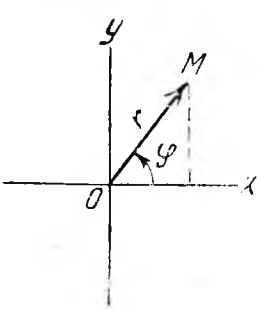
Задачи. 1. Извлечь корни: а) $\sqrt{1+i}$; b) $\sqrt{8-5i}$; c) $\sqrt{19-6i}$.

2. Решить квадратное уравнение

$$(1-i)x^2-(7-2i)x+(8-i)=0.$$

§ 41. Геометрическое представление комплексного числа

Гаусс предложил следующий наглядный способ изображения комплексного числа. Возьмём на плоскости прямоугольную систему координат XOY (см. черт. 8). Комплексное число $z=a+bi$ мы можем изобразить вектором $\overrightarrow{OM}$, оканчивающимся в точке M с координатами $(a,\ b)$. Очевидно, нулю будет соответствовать начало O, действительному числу—вектор, лежащий на оси X, а числу bi (так называемому мнимому числу)—вектор, лежащий на оси OY. Поэтому по абсциссе мы будем называть *действительной осью*, а ось ординат—*мнимой осью*.



Черт. 8

Легко подметить, что сумме комплексных чисел соответствует сумма векторов. В самом деле, пусть слагаемое $z=a+bi$ изображается вектором OM, а слагаемое $z_1=a_1+b_1i$ вектором OM_1 (см. черт. 9). Векторы складываются по правилу параллелограмма; следовательно, диагональ параллелограмма $OMNM_1$ и будет как раз суммой векторов OM и OM_1:

$$\overrightarrow{ON}=\overrightarrow{OM}+\overrightarrow{OM_1}.$$

Покажем, что ON изображает сумму $z+z_1$. Для этой цели спроектируем треугольник OMN на ось OX. Сумма проекций звеньев ломаной, как известно, равна проекции замыкающей; поэтому

$$\text{пр. } \overline{ON} = \text{пр. } \overline{OM} + \text{пр. } \overline{MN}.$$

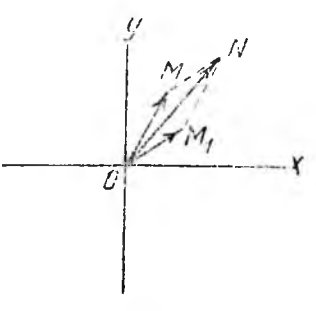
Но

$$\text{пр. } \overline{OM} = a, \quad \text{пр. } \overline{MN} = \text{пр. } \overline{OM_1} = a_1,$$

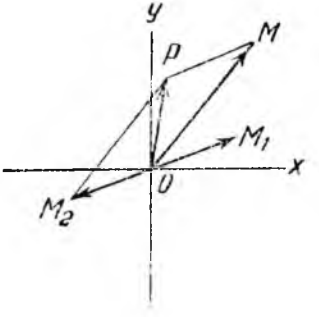
откуда окончательно

$$\text{пр. } \overline{ON} = a + a_1.$$

Затем, проектируя треугольник OMN на ось OY, найдём подобным же образом, что проекция ON на ось ординат равна $b+b_1$. Мы видим отсюда, что точка N, являющаяся концом вектора $\overline{ON}$, имеет координатами $a+a_1$ и $b+b_1$. Поэтому вектор $\overline{ON}$ изображает комплексное число $(a+a_1)+(b+b_1)i$, т. е. сумму $z+z_1$.



Черт. 9.



Черт. 10.

Обратная операция, вычитание, допускает аналогичное истолкование. А именно, разность $z-z_1$ можно записать в виде суммы $z+(-z_1)$. Если комплексному числу z_1 соответствовал вектор $\overline{OM_1}$, то теперь числу $-z_1$ соответствует вектор $\overline{OM_2}$, имеющий ту же длину, что и $\overline{OM_1}$, но направленный в противоположную сторону (см. черт. 10). Складывая два вектора $\overline{OM}$ и $\overline{OM_2}$, получим вектор $\overline{OP}$, изображающий разность $z-z_1$.

Чтобы дать геометрическую интерпретацию операции умножения, вернёмся к черт. 8. Вектор $\overline{OM}$, изображающий число $z=a+bi$, вполне определяется расстоянием r его конца M от начала координат и углом наклона φ к оси OX. В сущности говоря, r и φ есть не что иное, как полярные координаты точки M. Из чертежа легко усмотреть, что

$$r=\sqrt{a^2+b^2}; \quad a=r\cos\varphi; \quad b=r\sin\varphi.$$

Расстояние r есть величина существенно положительная; поэтому корень квадратный следует брать со знаком плюс. Таким образом $z=r\cos\varphi+ir\sin\varphi$ или, вынося r за скобку, $z=r(\cos\varphi+i\sin\varphi)$. Мы получили *тригонометрическую форму* комплексного числа. При этом r называется *модулем* числа z и обозначается так: $r=|z|$. Полярный угол φ называется *аргументом* или *амплитудой* числа z;

для него принята следующая запись: $\varphi = \arg z$. Для положительных действительных чисел аргумент равен нулю, а для отрицательных — равен π.

Пример. Приведём к тригонометрическому виду

$$z = -45 - 15i\sqrt{3}.$$

Очевидно, надо прежде всего определить модуль и аргумент. Так как здесь

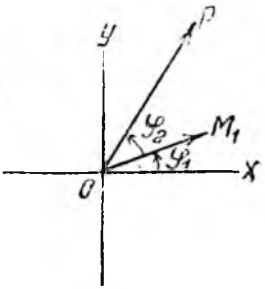
$$a = -45, \quad b = -15\sqrt{3},$$

то

$$r = \sqrt{a^2 + b^2} = \sqrt{(-45)^2 + (-15\sqrt{3})^2} = 30\sqrt{3},$$

$$\cos\varphi = \frac{a}{r} = \frac{-45}{30\sqrt{3}} = -\frac{\sqrt{3}}{2},$$

$$\sin\varphi = \frac{b}{r} = \frac{-15\sqrt{3}}{30\sqrt{3}} = -\frac{1}{2}.$$



Черт. 11.

Отсюда ясно, что $\varphi = \frac{7\pi}{6}$, и потому

$$z = 30\sqrt{3}\left(\cos\frac{7\pi}{6} + i\sin\frac{7\pi}{6}\right).$$

Заметим, что в силу периодичности тригонометрических функций аргумент определяется с точностью до числа, кратного 2π: мы могли бы вместо $\varphi = \frac{7\pi}{6}$ взять, например, $\varphi = \frac{7\pi}{6} + 2\pi$ и вообще $\varphi = \frac{7\pi}{6} + 2k\pi$ (k — целое число).

Посмотрим теперь, по какому правилу перемножаются и делятся комплексные числа, заданные в тригонометрической форме. Пусть

$$z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1);$$
$$z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2).$$

Перемножим z_1 и z_2:

$$z_1 z_2 = r_1(\cos\varphi_1 + i\sin\varphi_1)\cdot r_2(\cos\varphi_2 + i\sin\varphi_2) =$$
$$= r_1 r_2[(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + i(\sin\varphi_1\cos\varphi_2 + \cos\varphi_1\sin\varphi_2)].$$

Но

$$\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 = \cos(\varphi_1 + \varphi_2),$$
$$\sin\varphi_1\cos\varphi_2 + \cos\varphi_1\sin\varphi_2 = \sin(\varphi_1 + \varphi_2).$$

Следовательно:

$$z_1 z_2 = r_1 r_2[\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)].$$

Вообще:

$$z_1 z_2 \dots z_n = r_1 r_2 \dots r_n[\cos(\varphi_1 + \varphi_2 + \dots + \varphi_n) + i\sin(\varphi_1 + \varphi_2 + \dots + \varphi_n)],$$

т. е. *при перемножении комплексных чисел их модули перемножаются, а аргументы складываются.*

Это правило умножения допускает следующее геометрическое истолкование: если вектор $\overrightarrow{OM_1}$, соответствующий числу z_1, повернуть против часовой стрелки на угол, равный аргументу z_2, а затем растянуть во столько раз, сколько единиц содержится в модуле z_2,

то в результате получится вектор $\overrightarrow{OP}$, изображающий произведение $z_1 z_2$ (см. черт. 11).

Переходим теперь к операции деления. Частное двух комплексных чисел $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$ и $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$ можно записать в виде произведения:

$$\frac{z_1}{z_2} = z_1 \cdot \left(\frac{1}{z_2}\right) \quad (z_2 \neq 0).$$

Таким образом всё сводится к отысканию обратного числа $\frac{1}{z_2}$.

Пусть

$$\frac{1}{z_2} = \rho(\cos\theta + i\sin\theta),$$

ρ и θ пока неизвестные величины, их надо найти. По определению обратного числа имеем:

$$z_2 \cdot \frac{1}{z_2} = r_2(\cos\varphi_2 + i\sin\varphi_2) \cdot \rho(\cos\theta + i\sin\theta) = 1$$

или, после перемножения,

$$\rho r_2[\cos(\varphi_2 + \theta) + i\sin(\varphi_2 + \theta)] = 1.$$

Так как модуль единицы равен 1, а аргумент единицы равен нулю, то получаем:

$$\rho r_2 = 1, \quad \varphi_2 + \theta = 0,$$

откуда

$$\rho = \frac{1}{r_2}, \quad \theta = -\varphi_2.$$

Итак, $\frac{1}{z_2}$ найдено:

$$\frac{1}{z_2} = \frac{1}{r_2}[\cos(-\varphi_2) + i\sin(-\varphi_2)].$$

Теперь можно написать, чему равно частное $\frac{z_1}{z_2}$:

$$\frac{z_1}{z_2} = z_1 \cdot \frac{1}{z_2} = r_1(\cos\varphi_1 + i\sin\varphi_1) \cdot \frac{1}{r_2}[\cos(-\varphi_2) + i\sin(-\varphi_2)] =$$

$$= \frac{r_1}{r_2}[\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)],$$

т. е. *при делении модули делятся, а аргументы вычитаются.*

Как видим, тригонометрическая форма комплексного числа имеет некоторые преимущества перед обычной, так как позволяет с большей простотой перемножать и делить комплексные числа. Эти преимущества обнаруживаются также при возвышении в степень и извлечении корня.

Руководствуясь правилом умножения комплексных чисел, заданных в тригонометрической форме, без особого труда находим, что

$$[r(\cos\varphi + i\sin\varphi)]^n = r^n[\cos(n\varphi) + i\sin(n\varphi)], \qquad (1)$$

где n—целое положительное число. Получилась так называемая *формула Муавра*, которая выражает следующее простое правило:

при возвышении в степень модуль возводится в степень, а аргумент умножается на показатель степени.

Интересно отметить, что формула Муавра позволяет выразить косинус и синус кратного угла $n\varphi$ через $\cos\varphi$ и $\sin\varphi$. Именно, если возвысить левую часть равенства (1) по бином Ньютона и затем сравнить в обеих частях действительные части и коэффициенты при i, то получится

$$\cos n\varphi = \cos^n\varphi - C_n^2 \cos^{n-2}\varphi \sin^2\varphi + C_n^4 \cos^{n-4}\varphi \sin^4\varphi - \dots,$$
$$\sin n\varphi = n\cos^{n-1}\varphi \sin\varphi - C_n^3 \cos^{n-3}\varphi \sin^3\varphi + C_n^5 \cos^{n-5}\varphi \sin^5\varphi - \dots,$$

где C_n^k — биномиальные коэффициенты:

$$C_n^k = \frac{n(n-1)\dots(n-k+1)}{k!}.$$

Например, полагая $n=2$ и $n=3$, получаем следующие формулы:

$$\cos 2\varphi = \cos^2\varphi - \sin^2\varphi, \quad \sin 2\varphi = 2\sin\varphi\cos\varphi.$$
$$\cos 3\varphi = \cos^3\varphi - 3\cos\varphi\sin^2\varphi, \quad \sin 3\varphi = 3\cos^2\varphi\sin\varphi - \sin^3\varphi.$$

Рассмотрим теперь вторую задачу—извлечение корня из комплексного числа. Найдём, чему равен корень n-й степени из комплексного числа

$$z = r(\cos\varphi + i\sin\varphi).$$

Пусть ρ модуль искомого числа, а θ его аргумент. Тогда

$$\sqrt[n]{r(\cos\varphi + i\sin\varphi)} = \rho(\cos\theta + i\sin\theta),$$

или, возвышая обе части равенства в n-ю степень:

$$r(\cos\varphi + i\sin\varphi) = [\rho(\cos\theta + i\sin\theta)]^n.$$

Но по формуле Муавра

$$[\rho(\cos\theta + i\sin\theta)]^n = \rho^n(\cos n\theta + i\sin n\theta);$$

следовательно:

$$r(\cos\varphi + i\sin\varphi) = \rho^n(\cos n\theta + i\sin n\theta).$$

Два комплексных числа равны в том случае, когда равны их модули, а аргументы равны или отличаются на кратное 2π (вспомните, что аргумент определяется с точностью до числа, кратного 2π); поэтому

$$\rho^n = r, \quad n\theta = \varphi + 2\pi k$$

(k — целое число), откуда

$$\rho = \sqrt[n]{r}, \quad \theta = \frac{\varphi + 2\pi k}{n}.$$

Корень n-й степени из r берётся здесь в арифметическом смысле, так как модуль ρ есть число положительное. Итак, мы пришли к следующему ответу: корень n-й степени из z равен

$$u_k = \sqrt[n]{r}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right). \qquad (2)$$

Число k в формуле (2) может принимать любое целое значение; однако достаточно ограничиться значениями $k=0, 1, 2, \ldots, n-1$. Действительно, аргумент u_n равен $\frac{\varphi}{n}+2\pi$, т. е. отличается от аргумента u_0 на 2π; поэтому $u_n=u_0$. Точно так же убеждаемся, что $u_{n+1}=u_1$ и т. д.

Следовательно, *корень n-й степени из комплексного числа имеет n различных значений. Они получаются из формулы* (2) при $k=0, 1, 2, \ldots, n-1$.

Пример. Найдём $\sqrt[6]{2}$. В данном случае $\varphi=0$, $r=2$. Стало быть, формула (2) принимает вид

$$u_k=\sqrt[6]{2}\left(\cos\frac{2\pi k}{6}+i\sin\frac{2\pi k}{6}\right).$$

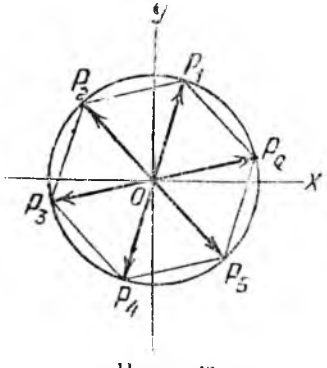
Полагаем $k=0, 1, 2, 3, 4, 5$:

$$\left.\begin{aligned}
u_0&=\sqrt[6]{2}(\cos 0+i\sin 0)=\sqrt[6]{2},\\
u_1&=\sqrt[6]{2}\left(\cos\frac{2\pi}{6}+i\sin\frac{2\pi}{6}\right)=\sqrt[6]{2}\left(\frac{1}{2}+\frac{\sqrt{3}}{2}i\right),\\
u_2&=\sqrt[6]{2}\left(\cos\frac{4\pi}{6}+i\sin\frac{4\pi}{6}\right)=\sqrt[6]{2}\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right),\\
u_3&=\sqrt[6]{2}(\cos\pi+i\sin\pi)=-\sqrt[6]{2},\\
u_4&=\sqrt[6]{2}\left(\cos\frac{8\pi}{6}+i\sin\frac{8\pi}{6}\right)=\sqrt[6]{2}\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right),\\
u_5&=\sqrt[6]{2}\left(\cos\frac{10\pi}{6}+i\sin\frac{10\pi}{6}\right)=\sqrt[6]{2}\left(\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)\ ^1).
\end{aligned}\right\}\quad(3)$$

Посмотрим, какой геометрический смысл имеет формула (2). Все n значений $u_0, u_1, \ldots, u_{n-1}$ имеют один и тот же модуль $\sqrt[n]{r}$; аргумент u_0 равен $\frac{\varphi}{n}$, а аргументы остальных u_i получаются последовательным прибавлением $\frac{2\pi}{n}$. Таким образом, числа

$$u_0,\ u_1, \ldots, u_{n-1}$$

изображаются векторами, концы которых находятся в вершинах правильного n-угольника, вписанного в окружность радиуса $\sqrt[n]{r}$ (см. черт. 12; он соответствует случаю $n=6$).



Черт. 12.

В заключение не мешает несколько подробнее остановиться на понятии модуля. Мы для модуля ввели то же обозначение, что и для абсолютной величины, и сделали это совершенно со-

[1]) Полезно заметить, что комплексные корни n-й степени из действительного числа попарно сопряжены между собой. Причину этого предоставляем установить самому читателю в качестве упражнения.

значительно. Пусть a — действительное число; его можно рассматривать как комплексное число $a+bi$, у которого $b=0$. Поэтому модуль a равен

$$r=\sqrt{a^2+b^2}=\sqrt{a^2}.$$

Но, в свою очередь, $\sqrt{a^2}$ есть не что иное, как абсолютная величина a. Следовательно, *в случае действительного числа понятия модуля и абсолютной величины совпадают.*

Мало того, в поле комплексных чисел модуль обладает всеми свойствами абсолютной величины. А именно:

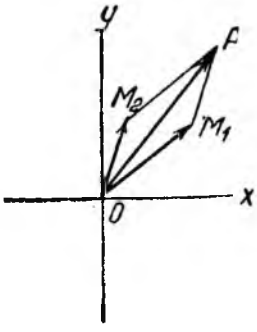
I. *Модуль произведения равен произведению модулей*:

$$|z_1z_2|=|z_1|\cdot|z_2|.$$

Это следует из правила перемножения комплексных чисел, заданных в тригонометрической форме.

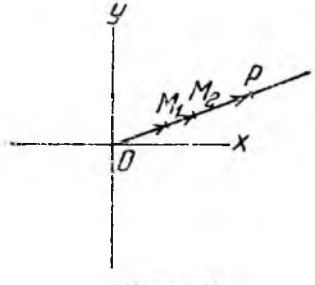
II. *Модуль суммы меньше или равен сумме модулей и больше или равен разности модулей*:

$$|z_1+z_2|\leqslant|z_1|+|z_2|,$$
$$|z_1|-|z_2|\leqslant|z_1+z_2|.$$

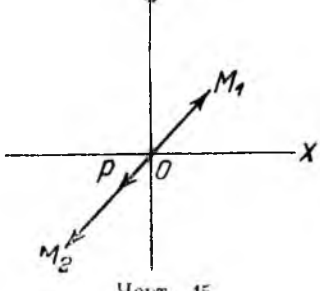


Черт. 13.

Рассмотрим сперва тот случай, когда аргумент z_1 отличен от аргумента z_2. На черт. 13 векторы $\overline{OM_1}$, $\overline{OM_2}$ и $\overline{OP}$ изображают соответственно числа z_1, z_2 и z_1+z_2. Обращаясь к треугольнику



Черт. 14.



Черт. 15.

OM_1P, мы видим, что длина стороны OM_1 равна $|z_1|$, длина стороны M_1P равна $|z_2|$ и длина стороны OP равна $|z_1+z_2|$. Сумма двух сторон треугольника, как известно, больше его третьей стороны, а разность — меньше третьей стороны. Поэтому мы можем написать следующие неравенства:

$$|z_1+z_2|<|z_1|+|z_2|,\quad |z_1|-|z_2|<|z_1+z_2|.$$

Рассмотрим теперь случай, когда аргумент z_1 равен аргументу z_2. Геометрически это означает, что векторы $\overline{OM_1}$ и $\overline{OM_2}$ должны лежать на одной прямой (см. черт. 14 и 15). Если $\overline{OM_1}$ и $\overline{OM_2}$ на-

правлены в одну сторону (см. черт. 14), то

$$|z_1+z_2|=|z_1|+|z_2|, \quad |z_1-z_2|<|z_1+z_2|.$$

Если $\overrightarrow{OM_1}$ и $\overrightarrow{OM_2}$ направлены в разные стороны (см. черт. 15), то длина вектора $\overrightarrow{OP}$ будет, очевидно, равна абсолютной величине разности длин векторов $\overrightarrow{OM_1}$ и $\overrightarrow{OM_2}$; иными словами,

$$|z_1+z_2|=|z_1-z_2|.$$

Отсюда как раз и следует, что

$$|z_1+z_2|\leqslant|z_1|+|z_2|, \quad |z_1-z_2|\leqslant|z_1|+|z_2|.$$

Итак, свойство II модуля доказано для всех случаев.

На этом мы заканчиваем общую теорию комплексных чисел.

Комплексные числа получили полное признание лишь в XIX веке. Они казались непонятными и удивительными таким гениальным математикам, как Декарт, Ньютон, Лейбниц. «Из иррациональностей» говорит Лейбниц, «возникают количества невозможные, или мнимые, удивительной природы, но пользы которых все же невозможно отрицать. Это есть тонкое и чудное пристанище человеческого духа, нечто, пребывающее между бытием и небытием». Только в конце XVIII и начале XIX века появляются первые работы, посвящённые конкретному истолкованию комплексных чисел. В 1799 г. норвежский землемер Вессель (Caspar Wessel, 1745—1818) опубликовал работу под названием «Об аналитическом представлении направления». В 1806 г. была опубликована работа французского учёного Аргана (Argand) «Об одном способе представления воображаемых количеств». Но окончательное признание комплексные числа получили лишь после работ Гаусса и Гамильтона. То обоснование комплексных чисел, которое мы привели в § 40, принадлежит Гамильтону.

Задачи. 1. Привести к тригонометрическому виду $1+i$, $1-i$, $7-2i$, $10-11i$ [1]).

2. Найти, чему равны

$$(-5+5i\sqrt{3})(1-i) \quad \text{и} \quad \frac{(-5+5i\sqrt{3})^3}{(1-i)^2},$$

пользуясь правилом умножения и деления комплексных чисел, заданных в тригонометрической форме.

3. Если аргумент числа $z=a+bi$ равен φ, то чему равен аргумент сопряжённого числа $\bar{z}=a-bi$?

4. Показать, что формула Муавра справедлива и для целых отрицательных значений n. Можно ли распространить ее на рациональные значения n?

5. Выразить $\cos 5z$ и $\sin 5z$ через $\cos z$ и $\sin z$.

6. Найти

$$\sqrt[3]{1-8i}.$$

[1]) Для нахождения аргументов можно пользоваться таблицами тригонометрических функций.

§ 42. Гиперкомплексные числа

Комплексное число, как мы скоро увидим, является частным случаем гораздо более общего понятия — гиперкомплексного числа.

Обозначим через A множество символов $(a_1, a_2, \ldots, a_n)$, составленных из n всевозможных действительных чисел $a_1, a_2, \ldots, a_n$. Два символа, отличающиеся друг от друга порядком следования чисел или самими числами, мы будем считать различными. Иными словами:

I. $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ *тогда и только тогда, когда* $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_n = b_n$.

Легко убедиться, что равенство двух символов обладает следующими свойствами обычного равенства.

а) Всякий символ равен самому себе (условие рефлексивности):

$$(a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, a_n).$$

Это следует из очевидных равенств $a_1 = a_1$, $a_2 = a_2$, $\ldots$, $a_n = a_n$.

b) Если первый символ равен второму, то, обратно, второй равен первому (условие симметрии).

В самом деле, по определению I из $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ должно следовать $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_n = b_n$. Но если $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_n = b_n$, то, обратно, $b_1 = a_1$, $b_2 = a_2$, $\ldots$, $b_n = a_n$. Отсюда (см. I)

$$(b_1, b_2, \ldots, b_n) = (a_1, a_2, \ldots, a_n).$$

c) Если первый символ равен второму, а второй — третьему, то первый символ равен третьему (условие транзитивности).

Опять рассуждаем аналогичным образом. По определению I из $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ и $(b_1, b_2, \ldots, b_n) = (c_1, c_2, \ldots, c_n)$ должно следовать $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_n = b_n$ и $b_1 = c_1$, $b_2 = c_2$, $\ldots$, $b_n = c_n$, откуда $a_1 = c_1$, $a_2 = c_2$, $\ldots$, $a_n = c_n$. Поэтому в силу того же определения I $(a_1, a_2, \ldots, a_n) = (c_1, c_2, \ldots, c_n)$.

Однако у нас ещё нет достаточных оснований для употребления термина «число». Символы $(a_1, a_2, \ldots, a_n)$ станут числами только тогда, когда мы для них введём операции сложения и умножения. Постараемся эти операции определить с таким расчётом, чтобы множество A оказалось кольцом.

Сложение мы определяем так:

II. $$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

Как видим, наше множество символов A по отношению к операции сложения замкнуто [1]).

Затем без особых затруднений можно проверить, что операция сложения удовлетворяет переместительному и сочетательному законам. Действительно:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) = (b_1 + a_1, b_2 + a_2, \ldots, b_n + a_n) = (b_1, b_2, \ldots, b_n) + (a_1, a_2, \ldots, a_n).$$

[1]) Кроме того, сложение есть операция однозначная.

Сочетательный закон выводится аналогичным образом.

Что можно сказать относительно обратной операции — вычитания? Оказывается, что уравнение

$$(a_1, a_2, \ldots, a_n) + z = (b_1, b_2, \ldots, b_n)$$

всегда разрешимо; легко проверить, что оно удовлетворяется значением

$$z = (b_1 - a_1, b_2 - a_2, \ldots, b_n - a_n).$$

Итак, остаётся ввести операцию умножения, и тогда наши символы станут числами.

Прежде всего освободимся от неудобного обозначения $(a_1, a_2, \ldots, a_n)$. Для этой цели введём понятие *скалярного умножения* действительного числа m на символ $(a_1, \ldots, a_n)$. Оно определяется следующим условием:

III. $m \cdot (a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, a_n) \cdot m = (ma_1, ma_2, \ldots, ma_n)$.

Скалярное произведение, во-первых, переместительно, как это видно из самого его определения. Во-вторых, для него имеет место распределительный закон. Действительно:

$$\begin{aligned} m[(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n)] &= m \cdot (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) = \\ &= (ma_1 + mb_1, ma_2 + mb_2, \ldots, ma_n + mb_n) = \\ &= (ma_1, ma_2, \ldots, ma_n) + (mb_1, mb_2, \ldots, mb_n) = \\ &= m(a_1, a_2, \ldots, a_n) + m(b_1, b_2, \ldots, b_n); \end{aligned}$$

$$\begin{aligned} (l + m)(a_1, a_2, \ldots, a_n) &= (la_1 + ma_1, la_2 + ma_2, \ldots, la_n + ma_n) = \\ &= (la_1, la_2, \ldots, la_n) + (ma_1, ma_2, \ldots, ma_n) = \\ &= l(a_1, a_2, \ldots, a_n) + m(a_1, a_2, \ldots, a_n). \end{aligned}$$

Теперь символ $(a_1, a_2, \ldots, a_n)$ можно заменить более удобным обозначением. Именно, по определению сложения и скалярного умножения

$$\begin{aligned} (a_1, a_2, \ldots, a_n) &= (a_1, 0, 0, \ldots, 0) + (0, a_2, 0, \ldots, 0) + \ldots + \\ &+ (0, 0, 0, \ldots, a_n) = a_1(1, 0, 0, \ldots, 0) + \\ &+ a_2(0, 1, 0, \ldots, 0) + \ldots + a_n(0, 0, 0, \ldots, 1). \end{aligned}$$

Если положить

$$\begin{aligned} (1, 0, 0, \ldots, 0) &= e_1, \\ (0, 1, 0, \ldots, 0) &= e_2, \\ &\ldots\ldots\ldots\ldots \\ (0, 0, 0, \ldots, 1) &= e_n, \end{aligned}$$

то получится окончательно, что

$$(a_1, a_2, \ldots, a_n) = a_1e_1 + a_2e_2 + \ldots a_ne_n,$$

при этом совокупность символов $e_1, e_2, \ldots, e_n$ называется *базисом* множества A, а каждый из символов e_i — *гиперкомплексной едини-*

цей. Вместе с тем условия I—III принимают следующий более наглядный вид:

I. *Условие равенства*: $a_1e_1+a_2e_2+\ldots+a_ne_n=b_1e_1+b_2e_2+\ldots+b_ne_n$ *тогда и только тогда, когда* $a_1=b_1,\ a_2=b_2,\ \ldots,\ a_n=b_n$.

II. *Сложение*

$$(a_1e_1+a_2e_2+\ldots+a_ne_n)+(b_1e_1+b_2e_2+\ldots+b_ne_n)=$$
$$=(a_1+b_1)e_1+(a_2+b_2)e_2+\ldots+(a_n+b_n)e_n$$

III. *Скалярное умножение*:

$$m(a_1e_1+a_2e_2+\ldots+a_ne_n)=(a_1e_1+a_2e_2+\ldots+a_ne_n)m=$$
$$=(ma_1)e_1+(ma_2)e_2+\ldots+(ma_n)e_n.$$

Мы видим, что выражения $a_1e_1+a_2e_2+\ldots+a_ne_n$ по отношению к сложению и скалярному умножению ведут себя как обыкновенные многочлены; в этом как раз и состоит выгода нового обозначения.

Теперь мы можем ввести операцию умножения одного символа на другой. Умножение должно подчиняться распределительному закону. Поэтому потребуем, чтобы $a_1e_1+a_2e_2+\ldots+a_ne_n$ и $b_1e_1+b_2e_2+\ldots+b_ne_n$ перемножались так, как перемножаются многочлены:

IV. $(a_1e_1+a_2e_2+\ldots+a_ne_n)\cdot(b_1e_1+b_2e_2+\ldots+b_ne_n)=$
$$=a_1b_1e_1^2+a_1b_2e_1e_2+\ldots+a_1b_ne_1e_n+\ldots+a_nb_1e_ne_1+\ldots+a_nb_ne_n^2.$$

Умножение, однако, определено не до конца, так как мы не знаем, какой смысл имеют выражения e_1^2, e_1e_2 и т. д. На помощь приходит следующее соображение. Мы хотим умножение ввести с таким расчётом, чтобы множество A стало кольцом. Но кольцо, как известно, должно быть замкнуто относительно умножения. Следовательно, произведения $e_1^2, e_1e_2, \ldots,$ гиперкомплексных единиц должны быть также символами множества A; иными словами,

V. $e_ie_j=c_{ij}^{(1)}e_1+c_{ij}^{(2)}e_2+\ldots+c_{ij}^{(n)}e_n$
$(i, j=1, 2, \ldots, n;\ c_{ij}^{(v)}$ — действительные числа).

Соотношения V называются *таблицей умножения гиперкомплексных единиц* или, просто, таблицей умножения.

Наконец, умножение должно подчиняться сочетательному закону. Если этот закон имеет место для гиперкомплексных единиц, то он будет иметь место и для их линейных комбинаций $a_1e_1+\ldots+a_ne_n$. Следовательно, мы должны ввести ещё одно требование:

VI. $e_i(e_je_k)=(e_ie_j)e_k \qquad (i, j, k=1, 2, \ldots, n)$.

Итак, задача, поставленная в самом начале параграфа, решена до конца, поскольку операции сложения и умножения определены. Теперь мы можем с полным основанием назвать выражения $a_1e_1+a_2e_2+\ldots+a_ne_n$ *гиперкомплексными числами*, а их множество

A — гиперкомплексной системой n-го порядка или линейной ассоциативной алгеброй.

Как и следовало ожидать, гиперкомплексная система A образует кольцо, потому что обладает всеми характерными признаками кольца (замкнутость относительно сложения и умножения, переместительность сложения, сочетательность сложения и умножения, выполнимость вычитания, распределительный закон — все эти свойства в ней имеют место). Множество A вообще образует некоммутативное кольцо, так как мы нигде не требовали коммутативности умножения. Легко видеть, что $0\cdot e_1+0\cdot e_2+\ldots+0\cdot e_n$ является нулём гиперкомплексной системы:

$$(a_1e_1+a_2e_2+\ldots+a_ne_n)+(0\cdot e_1+0\cdot e_2+\ldots+0\cdot e_n)=$$
$$=(a_1+0)\,e_1+(a_2+0)\,e_2+\ldots+(a_n+0)\,e_n=a_1e_1+a_2e_2+\ldots+a_ne_n.$$

Мы это число обозначим через 0. Очевидно, гиперкомплексное число $a_1e_1+a_2e_2+\ldots+a_ne_n$ равно нулю тогда и только тогда, когда $a_1=a_2=\ldots=a_n=0$ (это следует из условия равенства).

Приведём теперь в качестве иллюстрации несколько конкретных примеров. Проще всего начать с гиперкомплексных систем второго порядка. Их таблицы умножения имеют следующий вид:

$$\left.\begin{aligned} e_1^2&=c_{11}^{(1)}e_1+c_{11}^{(2)}e_2, & e_2^2&=c_{22}^{(1)}e_1+c_{22}^{(2)}e_2,\\ e_1e_2&=c_{12}^{(1)}e_1+c_{12}^{(2)}e_2, & e_2e_1&=c_{21}^{(1)}e_1+c_{21}^{(2)}e_2. \end{aligned}\right\} \qquad (1)$$

Давая коэффициентам $c_{ij}^{(r)}$ те или иные значения, мы будем получать ту или иную систему гиперкомплексных чисел. Следует, однако, всё время иметь в виду, что $c_{ij}^{(r)}$ не вполне произвольны: их надо выбирать с таким расчётом, чтобы выполнялось условие VI сочетательности умножения.

Пример 1. Положим в соотношениях (1)

$$c_{11}^{(1)}=c_{12}^{(2)}=c_{21}^{(2)}=1, \quad c_{22}^{(1)}=-1, \quad c_{11}^{(2)}=c_{22}^{(2)}=c_{12}^{(1)}=c_{21}^{(1)}=0.$$

Тогда получится такая таблица умножения:

$$e_1^2=e_1, \quad e_2^2=-e_1, \quad e_1e_2=e_2, \quad e_2e_1=e_2, \qquad (2)$$

и легко видеть, что она не противоречит условию VI. В самом деле:

$$e_1(e_1e_1)=e_1e_1^2=e_1e_1=e_1^2=e_1, \qquad (e_1e_1)e_1=e_1^2e_1=e_1e_1=e_1^2=e_1,$$
$$e_2(e_1e_1)=e_2e_1^2=e_2e_1=e_2, \qquad (e_2e_1)e_1=e_2e_1=e_2,$$
$$e_1(e_2e_2)=e_1e_2^2=-e_1e_1=-e_1^2=-e_1, \quad (e_1e_2)e_2=e_2e_2=e_2^2=-e_1$$

и т. д. [1]).

Выясним, с какой гиперкомплексной системой мы здесь имеем дело.

[1]) Всего придётся проверить восемь соотношений $e_i(e_je_k)=(e_ie_j)e_k$.

Пусть $z = ae_1 + be_2$, $z_1 = ce_1 + de_2$ два каких-нибудь числа нашей системы. По определению сложения и умножения имеем:

$$z + z_1 = (a + c)\, e_1 + (b + d)\, e_2,$$
$$zz_1 = (ae_1 + be_2)(ce_1 + de_2) = ace_1^2 + ade_1e_2 + bce_2e_1 + bde_2^2,$$

или, руководствуясь таблицей умножения (2), получаем:

$$zz_1 = (ac - bd)\, e_1 + (ad + bc)\, e_2.$$

Мы видим, что по отношению к сложению и умножению z и z_1 ведут себя как комплексные числа. Пока ещё преждевременно выражения $z = ae_1 + be_2$ считать комплексными числам, так как мы не знаем, что собой представляют e_1 и e_2.

Займёмся прежде всего e_1. Если $z = a_1e + be_2$ умножить на e_1, то получится:

$$ze_1 = (ae_1 + be_2)\, e_1 = ae_1^2 + be_2e_1 = ae_1 + be_2 = z.$$

Следовательно, e_1 является единицей гиперкомплексной системы, и мы можем e_1 обозначить через 1, т. е. $e_1 = 1$. Далее, из таблицы умножения (2) нетрудно усмотреть, что $e_2^2 = -1$. Поэтому e_2 можно отождествить с мнимой единицей: $e_2 = i = \sqrt{-1}$.

Итак, наша гиперкомплексная система — теперь это совершенно очевидно — есть не что иное, как поле комплексных чисел.

Пример 2. Обратимся к несколько иной таблице умножения. Пусть

$$e_1^2 = e_1, \quad e_2^2 = e_1, \quad e_1e_2 = e_2, \quad e_2e_1 = e_2\ ^1). \tag{3}$$

[Соотношения (3) не противоречат условию VI.] Здесь получаются числа совершенно новой природы, для которых многие законы арифметики нарушаются. Правда, переместительность умножения остаётся в силе, и это видно из самого правила (3) перемножения гиперкомплексных единиц. Но зато нарушается другой арифметический закон — произведение нескольких чисел может обращаться в нуль и тогда, когда все сомножители отличны от нуля; иными словами, рассматриваемая гиперкомплексная система обладает делителями нуля. Например,

$$(e_1 + e_2)(e_1 - e_2) = e_1^2 - e_2^2 = e_1 - e_1 = 0,$$

несмотря на то, что $e_1 + e_2 \neq 0$ и $e_1 - e_2 \neq 0$.

Выясним, какие $z = a_1e_1 + a_2e_2$ являются делителями нуля. Для этого рассмотрим уравнение $az = 0$. Полагая $z = x_1e_1 + x_2e_2$, будем иметь

$$az = a_1x_1e_1^2 + a_1x_2e_1e_2 + a_2x_1e_2e_1 + a_2x_2e_2^2 = 0,$$

или в силу таблицы умножения (3):

$$az = (a_1x_1 + a_2x_2)\, e_1 + (a_2x_1 + a_1x_2)\, e_2 = 0.$$

---

[1]) Мы могли бы e_1 обозначить через 1, так как e_1 ведёт себя как единица: $e_1^2 = e_1$, $e_1e_2 = e_2$.

Но гиперкомплексное число равно нулю тогда и только тогда, когда равны нулю коэффициенты при e_1 и e_2; следовательно:

$$\left.\begin{aligned} a_1x_1 + a_2x_2 &= 0, \\ a_2x_1 + a_1x_2 &= 0. \end{aligned}\right\} \tag{4}$$

Получилась линейная однородная система двух уравнений с двумя неизвестными x_1 и x_2. Она допускает ненулевые решения лишь в том случае, когда

$$\Delta = \begin{vmatrix} a_1 & a_2 \\ a_2 & a_1 \end{vmatrix} = a_1^2 - a_2^2 = 0$$

или когда

$$a_2 = \pm a_1.$$

Решая систему (4) при этих значениях коэффициентов, получаем, что

$$x_2 = \mp x_1.$$

Итак, делителями нуля могут быть только α, равные $a_1(e_1 \pm e_2)$ $(a_1 \neq 0)$; при этом уравнение $\alpha z = 0$ будет удовлетворяться значениями $z = x_1(e_1 \mp e_2)$. И действительно:

$$\alpha z = a_1x_1(e_1^2 - e_2^2) = a_1x_1(e_1 - e_1) = 0.$$

Теперь приведём пример гиперкомплексной системы более высокого порядка.

Пример 3. Мы не можем не остановиться на одном замечательном случае гиперкомплексной системы, на так называемых *кватернионах*, введённых Гамильтоном в 1843 г. Они характеризуются следующей таблицей умножения:

$$\left.\begin{aligned} &1^2 = 1, \quad i^2 = j^2 = k^2 = -1, \\ &1 \cdot i = i \cdot 1 = i, \quad 1 \cdot j = j \cdot 1 = j, \quad 1 \cdot k = k \cdot 1 = k, \\ &ij = k, \quad jk = i, \quad ki = j, \\ &ji = -k, \quad kj = -i, \quad ik = -j. \end{aligned}\right\} \tag{5}$$

Таким образом здесь $e_1 = 1$, $e_2 = i$, $e_3 = j$, $e_4 = k$ [при этом соотношения (5) не противоречат условию VI], и кватернионы имеют вид четырёх членов $a + bi + cj + dk$.

Уже с первого взгляда видно, что для кватернионов переместительность умножения нарушается. Так, например, $ij = k$, а $ji = -k$. Тем не менее кватернионы во многом ведут себя как комплексные числа.

Дело в том, что в кольце кватернионов, как и в поле комплексных чисел, деление всегда [1]) выполнимо. Правда, из-за некоммутативности умножения приходится различать два вида деления—левое и правое. Чтобы можно было доказать выполнимость деления, введём понятия сопряжённого кватерниона и нормы.

[1]) Мы, конечно, исключаем деление на нуль.

Пусть $q = a + bi + cj + dk$ какой-нибудь кватернион. Назовём кватернион $\bar{q} = a - bi - cj - dk$, отличающийся от q только знаками коэффициентов при i, j, k, *сопряжённым* с q; его принято обозначать той же буквой q, но с чертой наверху. Очевидно, что, обратно, q сопряжено с $\bar{q}$.

Далее, назовём *нормой* кватерниона q сумму квадратов его коэффициентов; норму принято обозначать через $N(q)$. Таким образом

$$N(q) = a^2 + b^2 + c^2 + d^2.$$

Очевидно, норма $N(q)$ равна нулю тогда и только тогда, когда $q = 0$.

Вернёмся к делению. Уравнения

$$xq = q_1, \quad qy = q_1 \quad (q \neq 0)$$

решаются теперь без особого труда. А именно, если умножить первое уравнение справа на $\frac{\bar{q}}{N(q)}$ и второе слева на $\frac{\bar{q}}{N(q)}$, то получится

$$x\frac{q\bar{q}}{N(q)} = \frac{q_1\bar{q}}{N(q)}, \quad \frac{q\bar{q}}{N(q)}y = \frac{\bar{q}q_1}{N(q)}.$$

Но, как легко убедиться непосредственным перемножением:

$$q\bar{q} = \bar{q}q = N(q).$$

Следовательно:

$$\frac{q\bar{q}}{N(q)} = \frac{\bar{q}q}{N(q)} = 1$$

и потому

$$x = \frac{q_1\bar{q}}{N(q)}, \quad y = \frac{\bar{q}q_1}{N(q)}.$$

Итак, наши уравнения решены; при этом x можно назвать *левым частным*, а y — *правым частным*.

В качестве иллюстрации покажем, как разделить $q_1 = 1 + 2i - j + k$ справа на $q = 1 - i + j - k$. Здесь

$$\bar{q} = 1 + i - j + k, \quad N(q) = 1^2 + (-1)^2 + 1^2 + (-1)^2 = 4,$$

$$\bar{q}q_1 = (1 + i - j + k)(1 + 2i - j + k) = 1 + 2i - j + k + i + 2i^2 - ij + ik - j - 2ji + j^2 - jk + k + 2ki - kj + k^2.$$

Если воспользоваться таблицей умножения (5) и привести затем подобные члены, то окончательно получится, что

$$\bar{q}q_1 = -3 + 3i - j + 3k.$$

После всех этих выкладок правое частное оказывается равным

$$y = \frac{\bar{q}q_1}{N(q)} = -\frac{3}{4} + \frac{3}{4}i - \frac{1}{4}j + \frac{3}{4}k.$$

До сих пор гиперкомплексные числа мы строили, исходя из поля действительных чисел. Этим, однако, методы построения гиперком-

плексных чисел не исчерпываются. Можно вместо поля действительных чисел взять любое известное нам числовое поле или кольцо (например, поле рациональных чисел или кольцо кватернионов) и построить относительно этого поля или кольца гиперкомплексную систему.

§ 43. Алгебраическое расширение

Мы ввели комплексные числа для того, чтобы обеспечить разрешимость любого квадратного уравнения. Возникает естественный вопрос—как быть с уравнением выше второй степени, если оно не решается с помощью действительных чисел? Очевидно, и здесь придётся итти по тому же пути—придётся расширить поле действительных чисел, присоединяя к нему числа новой природы, быть может и не только комплексные. Мы покажем, что такое расширение вполне возможно не только для поля действительных чисел, но и для всякого числового поля P.

Пусть $A_0, A_1, \ldots, A_n\ (n > 2)$ числа поля P и

$$F(x) = A_0x^n + A_1x^{n-1} + \ldots + A_n$$

многочлен, не имеющий корней в поле P. Без ограничения общности можно предположить, что $F(x)$ неприводимо в P; в противном случае мы взяли бы вместо многочлена $F(x)$ один из его неприводимых множителей. Постараемся поле P расширить с таким расчётом, чтобы многочлен $F(x)$ приобрёл по меньшей мере один корень. Для этой цели число a поля P будем записывать в виде символа $(a, 0, \ldots, 0)$, состоящего из числа a и $n-1$ нулей. При таком обозначении сумма и произведение чисел a и b представятся в виде:

$$\begin{aligned}(a, 0, \ldots, 0) + (b, 0, \ldots, 0) &= (a+b, 0, \ldots, 0),\\ (a, 0, \ldots, 0) \cdot (b, 0, \ldots, 0) &= (ab, 0, \ldots, 0).\end{aligned} \tag{1}$$

Символ $(a, 0, \ldots, 0)$, однако, является частным случаем символа $(a_0, a_1, \ldots, a_{n-1})$, состоящего из n чисел $a_0, a_1, \ldots, a_{n-1}$ поля P. Нет никаких оснований считать символы $(a_0, a_1, \ldots, a_{n-1})$ числами, пока мы не указали и не обосновали правил сравнения, сложения и перемножения символов. Тут на помощь приходит следующее обстоятельство: каждому символу $(a_0, a_1, \ldots, a_{n-1})$ можно поставить во взаимно однозначное соответствие многочлен $(n-1)$-й степени $g(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$. Определим понятие равенства и операции сложения и умножения так, чтобы сохранялось взаимно однозначное соответствие наших символов с многочленами $(n-1)$-й степени. Тогда определения примут следующий вид:

1. *Два символа* $(a_0, a_1, \ldots, a_{n-1})$ и $(b_0, b_1, \ldots, b_{n-1})$ *равны тогда и только тогда, когда равны соответствующие многочлены*

$$\begin{aligned}g(x) &= a_0 + a_1x + \ldots + a_{n-1}x^{n-1},\\ h(x) &= b_0 + b_1x + \ldots + b_{n-1}x^{n-1}.\end{aligned}$$

Иными словами, $(a_0, a_1, \ldots, a_{n-1}) = (b_0, b_1, \ldots, b_{n-1})$ тогда и только тогда, когда $a_0 = b_0, a_1 = b_1, \ldots, a_{n-1} = b_{n-1}$.

II. *Чтобы сложить два символа, надо сложить соответствующие многочлены.*

Следовательно,

$$(a_0, a_1, \ldots, a_{n-1}) + (b_0, b_1 \ldots, b_{n-1}) = \\ = (a_0 + b_0, a_1 + b_1, \ldots, a_{n-1} + b_{n-1}),$$

так как

$$g(x) + h(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_{n-1} + b_{n-1})x^{n-1}.$$

Аналогичным образом определить умножение символов уже нельзя, так как произведение соответствующих многочленов даст в общем случае многочлен степени большей, чем $n-1$, в соответствие которому мы не можем поставить никакого символа. Мы определим умножение символов следующим путём, сохраняя взаимно однозначное соответствие с многочленами $(n-1)$-й степени:

III. *Чтобы перемножить два символа, надо перемножить соответствующие многочлены и разделить полученное произведение на $F(x)$. Остаток от деления и будет соответствовать произведению символов.*

Следовательно,

$$(a_0, a_1, \ldots, a_{n-1}) \cdot (b_0, b_1 \ldots, b_{n-1}) = (c_0, c_1, \ldots, c_{n-1}),$$

где c_i — коэффициенты остатка

$$r(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1},$$

полученного при делении $g(x)\,h(x)$ на $F(x)$.

Постулаты I—III нуждаются, однако, в некотором обосновании. Во-первых, арифметические действия над символами не должны противоречить арифметическим действиям над числами поля P. В самом деле, равенства (1) находятся в полном согласии с постулатами, здесь $g(x) = a$, $h(x) = b$ и остаток от деления $g(x)\,h(x) = ab$ на $F(x)$ равен ab. Во-вторых, следует выяснить, имеют ли место замкнутость относительно сложения и умножения, переместительный, сочетательный и распределительный законы сложения и умножения. Но и это вполне очевидно, так как сложение и умножение символов приводятся к сложению и умножению многочленов в поле P, а для последних все перечисленные законы, конечно, справедливы. Мало того, выполнима и обратная операция—вычитание. А именно, легко видеть, что

$$(a_0, a_1, \ldots, a_{n-1}) - (b_0, b_1, \ldots, b_{n-1}) = \\ = (a_0 - b_0, a_1 - b_1, \ldots, a_{n-1} - b_{n-1}).$$

Короче говоря, *множество наших символов образует коммутативное кольцо.*

Теперь можно уже смело пользоваться термином «число». Мы будем каждый символ $(a_0, a_1, \ldots, a_{n-1})$ называть *алгебраическим числом относительно поля P*, кольцо этих символов — *алгебраическим расширением поля P.*

Остаётся показать, что рассматриваемый многочлен $F(x)$ в алгебраическом расширении имеет по меньшей мере один корень. Для этого найдём более удобную форму записи алгебраических чисел [1])

Легко видеть, что

$$a(b_0, b_1, \ldots, b_{n-1}) = (ab_0, ab_1, \ldots, ab_{n-1}). \qquad (2$$

Действительно, числу $a = (a, 0, \ldots, 0)$ поля P соответствует многочлен $g(x) = a$, а алгебраическому числу $(b_0, b_1, \ldots, b_{n-1})$—многочлен

$$h(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1};$$

поэтому многочлен

$$g(x)\,h(x) = ab_0 + ab_1 x + \ldots + ab_{n-1}x^{n-1}$$

как многочлен, имеющий более низкую степень, чем делитель $F(x)$, будет остатком. Отсюда, согласно постулату III, получается соотношение (2).

Далее, по определению сложения

$$(a_0, a_1, \ldots, a_{n-1}) = (a_0, 0, \ldots, 0) + (0, a_1, 0, \ldots, 0) + \ldots +$$
$$+ (0, \ldots, 0, a_{n-1}) = a_0 + (0, a_1, 0, \ldots, 0) + \ldots + (0, \ldots, 0, a_{n-1}),$$

или в силу соотношения (2):

$$(a_0, a_1, \ldots, a_{n-1}) = a_0 + a_1 \cdot (0, 1, 0, \ldots, 0) + \ldots +$$
$$+ a_{n-1} \cdot (0, \ldots, 0, 1). \qquad (3)$$

Что же собой представляют числа $(0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$? Обозначим $(0, 1, 0, \ldots, 0)$ через j и возвысим j в квадрат. Числу j соответствует многочлен $g(x) = x$; очевидно, что при делении $g^2(x) = x^2$ на $F(x)$ в остатке получится x^2. Следовательно, по определению умножения

$$j^2 = (0, 0; 1, 0, \ldots, 0).$$

Точно так же можно показать, что

$$j^3 = (0, 0, 0, 1, 0, \ldots, 0),$$
$$\ldots\ldots\ldots\ldots$$
$$j^{n-1} = (0, \ldots, 0, 1).$$

Итак, равенство (3) принимает следующий окончательный вид:

$$(a_0, a_1, \ldots, a_{n-1}) = a_0 + a_1 j + a_2 j^2 + \ldots + a_{n-1} j^{n-1}. \qquad (4$$

Мы получили многочленную форму записи алгебраического числа.

Подведём итог.

а) Алгебраические числа изображаются многочленами $(n-1)$ степени от j с коэффициентами из поля P [см. равенство (4)].

b) Алгебраические числа равны тогда и только тогда, когда они изображаются одинаковыми многочленами.

---

[1]) Ради краткости мы здесь и ниже употребляем выражение «алгебраические числа» вместо более точного выражения «алгебраические числа *относительно* поля P».

Точнее:

$$a_0 + a_1 j + \ldots + a_{n-1} j^{n-1} = b_0 + b_1 j + \ldots + b_{n-1} j^{n-1}$$

тогда и только тогда, когда $a_0 = b_0$, $a_1 = b_1, \ldots, a_{n-1} = b_{n-1}$ (см. постулат I).

c) Алгебраические числа складываются и вычитаются, как многочлены:

$$(a_0 + a_1 j + \ldots + a_{n-1} j^{n-1}) \pm (b_0 + b_1 j + \ldots + b_{n-1} j^{n-1}) =$$
$$= (a_0 \pm b_0) + (a_1 \pm b_1) j + \ldots + (a_{n-1} \pm b_{n-1}) j^{n-1}.$$

d) Чтобы перемножить два алгебраических числа

$$a_0 + a_1 j + \ldots a_{n-1} j^{n-1} \text{ и } b_0 + b_1 j + \ldots + b_{n-1} j^{n-1},$$

надо перемножить многочлены

$$g(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1},$$
$$h(x) = b_0 + b_1 x + \ldots + b_{n-1} x^{n-1},$$

разделить произведение $h(x)\, g(x)$ на $F(x)$ и в остатке $r(x)$ заменить x через j (см. постулат III).

Теперь вернёмся к нашей основной задаче. Мы покажем сейчас, что j как раз является корнем многочлена $F(x)$. Возвысим j в n-ю степень. Остаток от деления x^n на $F(x) = A_0 x^n + A_1 x^{n-1} + \ldots + A_n$ равен

$$-\frac{A_1}{A_0} x^{n-1} - \ldots - \frac{A_n}{A_0}.$$

Чтобы получить j^n, надо в этом остатке x заменить через j. Следовательно:

$$j^n = -\frac{A_1}{A_0} j^{n-1} - \ldots - \frac{A_n}{A_0}.$$

Отсюда, освобождаясь от знаменателя A_0 и перенося все члены в левую часть, имеем:

$$F(j) = A_0 j^n + A_1 j^{n-1} + \ldots + A_n = 0,$$

что и требовалось показать.

Читатель, вероятно, уже заметил, что построенное таким образом алгебраическое расширение представляет собою не что иное, как некоторую систему гиперкомплексных чисел.

В дальнейшем алгебраическое расширение поля P будет обозначаться символом $P(j)$, так как оно вполне определяется корнем j многочлена $F(x)$. А именно, стоит только ввести j, и $P(j)$ определится как кольцо выражений

$$a_0 + a_1 j + \ldots + a_{n-1} j^{n-1}.$$

Примеры алгебраических расширений. 1. Многочлен

$$F(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3),$$

очевидно; не имеет рациональных корней. Но мы можем расширить поле рациональных чисел так, чтобы у $F(x)$ появился по меньшей мере один корень. Для этого обратимся к одному из неприводимых множителей данного многочлена, например к

$$p(x) = x^2 - 2.$$

Его степень $n = 2$; поэтому согласно общей теории алгебраическое расширение должно состоять из линейных выражений

$$a + bj,$$

где a, b — рациональные числа, j — корень многочлена $p(x)$.

Выясним теперь, по каким правилам выражения $a + bj$ должны сравниваться, складываться и перемножаться. По определению равенства двух алгебраических чисел $a + bj = a_1 + b_1 j$ тогда и только тогда, когда $a = a_1$, $b = b_1$. Далее, по определению суммы

$$(a + bj) + (a_1 + b_1 j) = (a + a_1) + (b + b_1) j.$$

Наконец, легко видеть, что

$$(a + bx)(a_1 + b_1 x) = aa_1 + (ab_1 + a_1 b) x + bb_1 x^2$$

при делении на $p(x) = x^2 - 2$ даёт остаток, равный

$$(aa_1 + 2bb_1) + (ab_1 + a_1 b) x.$$

Следовательно, по определению, произведением будет:

$$(a + bj)(a_1 + b_1 j) = (aa_1 + 2bb_1) + (ab_1 + a_1 b) j.$$

Но точно так же ведут себя иррациональности $a + b\sqrt{2}$. А именно, кольцо выражений $a + bj$ изоморфно полю иррациональностей $a + b\sqrt{2}$: каждому выражению $a + bj$ взаимно однозначно соответствует иррациональность $a + b\sqrt{2}$; сумме $(a + bj) + (a_1 + b_1 j) = (a + a_1) + (b + b_1) j$ и произведению $(a + bj)(a_1 + b_1 j) = (aa_1 + 2bb_1) + (ab_1 + a_1 b) j$ отвечают взаимно однозначно сумма $(a + a_1) + (b + b_1)\sqrt{2}$ и произведение $(aa_1 + 2bb_1) + (ab_1 + a_1 b)\sqrt{2}$ соответственных иррациональностей $a + b\sqrt{2}$ и $a_1 + b_1\sqrt{2}$. Впрочем, это можно было заранее предвидеть, так как $j^2 = 2$. Нетрудно заметить, что в поле иррациональностей $a + b\sqrt{2}$ многочлен $F(x) = x^4 - 5x^2 + 6$ имеет два корня, а именно $\sqrt{2}$ и $-\sqrt{2}$.

Вместо неприводимого множителя $p(x) = x^2 - 2$ можно было взять $q(x) = x^2 - 3$; но тогда получилось бы другое алгебраическое расширение, изоморфное полю иррациональностей $a + b\sqrt{3}$.

2. Рассмотрим теперь многочлен

$$F(x) = x^2 + 1,$$

неприводимый в поле действительных чисел. И здесь $n = 2$; поэтому алгебраическое расширение должно состоять из линейных двучленов

$a+bi$, где a, b—действительные числа, а $i=(0, 1)$—корень многочлена $F(x)$; $i^2=-1$. Мы уже чувствуем близость к комплексным числам. Но посмотрим, как сравниваются выражения $a+bi$ и как они себя ведут по отношению к операциям сложения и умножения. Очевидно, что $a+bi=a_1+b_1i$ тогда и только тогда, когда $a=a_1$, $b=b_1$, т. е. имеем известное условие равенства двух комплексных чисел. Затем

$$(a+bi)+(a_1+b_1i)=(a+a_1)+(b+b_1)i,$$

а это обычное правило сложения комплексных чисел.

Наконец, нетрудно убедиться, что

$$(a+bx)(a_1+b_1x)=aa_1+(ab_1+a_1b)x+bb_1x^2$$

при делении на $F(x)=x^2+1$ даёт остаток, равный

$$(aa_1-bb_1)+(ab_1+a_1b)x.$$

Отсюда по определению произведения

$$(a+bi)\cdot(a_1+b_1i)=(aa_1-bb_1)+(ab_1+a_1b)i,$$

т. е. получилось обычное правило умножения комплексных чисел.

Итак, у нас получилось в качестве алгебраического расширения поле комплексных чисел.

Задача. Построить для многочлена $F(x)=x^3+2$, неприводимого в поле рациональных чисел, алгебраическое расширение.

В только что разобранных примерах алгебраические расширения оказались полями. Это не случайность. Можно доказать следующую теорему.

Теорема 1. *Всякое алгебраическое расширение $P(j)$ числового поля P в свою очередь является полем.*

Мы уже видели, что алгебраическое расширение $P(j)$ образует коммутативное кольцо. Таким образом надо только доказать выполнимость деления.

Пусть $F(x)=A_0x^n+A_1x^{n-1}+\ldots+A_n$ — неприводимый многочлен, с помощью которого построено алгебраическое расширение $P(j)$, и пусть

$$\begin{aligned} g(j)&=a_0+a_1j+\ldots+a_{n-1}j^{n-1} \qquad [g(j)\neq 0],\\ h(j)&=b_0+b_1j+\ldots+b_{n-1}j^{n-1} \end{aligned}$$

— два алгебраических числа $P(j)$. Покажем, что уравнение

$$g(j)z=h(j) \quad [g(j)\neq 0] \tag{5}$$

разрешимо.

Многочлен

$$g(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}$$

не может быть равен нулю, так как иначе было бы равно нулю и число $g(j)$. Следовательно, $g(x)$ как многочлен, не равный нулю и более низкой степени, чем $F(x)$, не может делиться на $F(x)$. Отсюда

в силу неприводимости $F(x)$ получается, что многочлены $g(x)$ и $F(x)$ взаимно просты [1]). Но в таком случае должно выполняться тождество

$$F(x)\varphi(x)+g(x)\psi(x)=1,$$

где $\varphi(x)$, $\psi(x)$—некоторые многочлены относительно x [см. стр. 149, формулу (9)]. Положим в этом тождестве $x=j$. Тогда $F(x)$ обратится в нуль, а многочлены $g(x)$, $\psi(x)$ превратятся в алгебраические числа $g(j)$, $\psi(j)$, и мы получим:

$$g(j)\psi(j)=1. \tag{6}$$

Мы утверждаем теперь, что

$$z=\psi(j)\,h(j)$$

является решением уравнения (5). И, действительно, согласно соотношению (6)

$$g(j)\cdot[\psi(j)\,h(j)]=[g(j)\psi(j)]h(j)=1\cdot h(j)=h(j).$$

Теорема I имеет для нас первостепенное значение. А именно, вся общая теория многочленов, изложенная в §§ 28—31 (см. главу V), справедлива и для алгебраического расширения $P(j)$, так как $P(j)$ по доказанному образует поле. В частности, если многочлен $F(x)$ имеет в $P(j)$ s корней j, j_1, ..., j_{s-1}, то

$$F(x)=(x-j)(x-j_1)\ldots(x-j_{s-1})F_1(x),$$

где $F_1(x)$ — многочлен с коэффициентами из $P(j)$.

Вернёмся теперь к многочленам с действительными коэффициентами. Обозначим для краткости поле комплексных чисел через K. Предположим самое худшее: пусть многочлен с действительными коэффициентами

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$$

(приводимый или неприводимый—безразлично) не имеет корней даже в поле K. Это обстоятельство уже не вызывает затруднений: мы можем построить алгебраическое расширение $K(j)$, в котором многочлен $f(x)$ будет иметь по меньшей мере один корень j. Вообще же в поле $K(j)$ многочлен $f(x)$ может иметь и большее число корней, например s корней j, j_1, ..., j_{s-1}. Если s равно степени n многочлена $f(x)$, то в поле $K(j)$ $f(x)$ разложится целиком на линейные множители:

$$f(x)=a_0(x-j)(x-j_1)\ldots(x-j_{n-1}).$$

Мы назовём в этом случае $K(j)$ *полем разложения* многочлена $f(x)$. Вообще *всякое числовое поле, в котором $f(x)$ разлагается целиком на линейные множители, мы будем называть полем разложения многочлена $f(x)$.*

[1]) См. § 28, свойства неприводимого многочлена, стр. 152.

Если же $s < n$, то

$$f(x) = (x - j)(x - j_1) \dots (x - j_{s-1}) f_1(x),$$

где $f_1(x)$ — многочлен с коэффициентами из $K(j)$; при этом $f_1(x)$ не имеет корней в $K(j)$. С многочленом $f_1(x)$ можно поступить так же, как и с $f(x)$. А именно, $K(j)$ можно расширить до нового алгебраического расширения, которое мы обозначим через $K(j)(j_s)$ в соответствии с символом $P(j)$, введённым на стр. 227. В этом расширении $f_1(x)$ будет иметь s_1 корней ($s_1 \geqslant 1$): $j_s, j_{s+1}, \dots, j_{s+s_1-1}$; так что

$$f(x) = (x - j)(x - j_1) \dots (x - j_{s-1})(x - j_s) \dots (x - j_{s+s_1-1}) f_2(x),$$

где $f_2(x)$—многочлен с коэффициентами из $K(j)(j_s)$ и т. д. Этот процесс последовательного расширения, однако, нельзя продолжать бесконечно; не более чем через n шагов мы придём к такому алгебраическому расширению $K(j)(j_s)\dots(j_{s_m})$, в котором $f(x)$ разлагается целиком на линейные множители:

$$f(x) = a_0(x - j)(x - j_1) \dots (x - j_{n-1}).$$

Таким образом $K(j)(j_s)\dots(j_{s_m})$ будет полем разложения $f(x)$.

Наконец, пусть многочлен $f(x)$ имеет комплексные корни. Представляются две возможности: либо K—поле разложения $f(x)$, либо число комплексных корней меньше степени n. В последнем случае с помощью последовательных расширений мы опять-таки придём к полю разложения.

Итак, доказана следующая теорема.

Теорема II. *Для всякого многочлена $f(x)$ с действительными коэффициентами существует такое поле разложения, которое совпадает с полем комплексных чисел или его содержит* [1]).

Мы показали, что всякий многочлен n-й степени имеет n корней. Но какова природа этих корней? Комплексные ли это числа? Не будут ли в некоторых случаях получаться какие-то совершенно новые числа? На эти вопросы мы скоро ответим.

§ 44. Симметрические функции

Пусть многочлен

$$f(x) = x^n - p_1 x^{n-1} + p_2 x^{n-2} - \dots + (-1)^n p_n$$

с действительными коэффициентами имеет n корней $\alpha_1, \alpha_2, \dots, \alpha_n$ (в поле разложения) [2]). Установим зависимость между корнями и коэффициентами p_i. Знание этой зависимости, несомненно, поможет

[1]) Ниже (в § 45) будет показано, что поле комплексных чисел есть поле разложения любого многочлена не только с действительными, но даже с комплексными коэффициентами.

[2]) Многочлен $f(x)$ записан в несколько необычном виде с чередующимися знаками у коэффициентов. Сделано это для большей симметрии дальнейших выводов. Что касается старшего коэффициента, то его всегда можно предполагать равным единице; в противном случае мы поделили бы на него все остальные коэффициенты.

ответить на вопросы, заданные в конце предыдущего параграфа. Разложим $f(x)$ на линейные множители

$$f(x)=x^n-p_1x^{n-1}+\ldots+(-1)^n p_n=(x-\alpha_1)\,(x-\alpha_2)\ldots(x-\alpha_n),$$

или, раскрывая в правой части скобки,

$$\begin{aligned}x^n-p_1x^{n-1}+\ldots+(-1)^{n-1}p_{n-1}x+(-1)^n p_n=\\ =x^n-(\alpha_1+\alpha_2+\ldots+\alpha_n)\,x^{n-1}+(\alpha_1\alpha_2+\alpha_1\alpha_3+\ldots+\alpha_{n-1}\alpha_n)\,x^{n-2}-\ldots+\\ +(-1)^{n-1}(\alpha_1\alpha_2\ldots\alpha_{n-1}+\alpha_1\alpha_3\ldots\alpha_n+\ldots+\alpha_2\alpha_3\ldots\alpha_n)\,x+\\ +(-1)^n\alpha_1\alpha_2\ldots\alpha_n.\end{aligned}\tag{1}$$

Сравнивая коэффициенты обеих частей равенства (1), получим так называемые *формулы Виета*:

$$\left.\begin{aligned}&p_1=\alpha_1+\alpha_2+\ldots+\alpha_n,\\ &p_2=\alpha_1\alpha_2+\alpha_1\alpha_3+\ldots+\alpha_{n-1}\alpha_n,\\ &\ldots\ldots\ldots\ldots\\ &p_{n-1}=\alpha_1\alpha_2\ldots\alpha_{n-1}+\alpha_1\ldots\alpha_{n-2}\alpha_n+\ldots+\alpha_2\alpha_3\ldots\alpha_n,\\ &p_n=\alpha_1\alpha_2\ldots\alpha_n.\end{aligned}\right\}\tag{2}$$

В правых частях соотношений (2) стоят всевозможные произведения корней по одному, по два, по три и т. д. С помощью формул Виета можно легко определить по корням уравнения его коэффициенты.

Пример. Составить уравнение, имеющее корнями $\alpha_1=1$; $\alpha_2=2$, $\alpha_3=3$ и $\alpha_4=-1$. Имеем:

$$\begin{aligned}&p_1=\alpha_1+\alpha_2+\alpha_3+\alpha_4=1+2+3-1=5,\\ &p_2=\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_3+\alpha_2\alpha_4+\alpha_3\alpha_4=\\ &\qquad=2+3-1+6-2-3=5,\\ &p_3=\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\alpha_1\alpha_3\alpha_4+\alpha_2\alpha_3\alpha_4=6-2-3-6=-5,\\ &p_4=\alpha_1\alpha_2\alpha_3\alpha_4=-6.\end{aligned}$$

Таким образом получается уравнение

$$x^4-5x^3+5x^2+5x-6=0.$$

Заметим, что формулы Виета остаются в силе при любой нумерации корней. Возьмём, например, первое из соотношений (2) и заменим α_1 через α_2, α_2 через α_1; получим

$$p_1=\alpha_2+\alpha_1+\ldots+\alpha_n,$$

т. е. первые два слагаемые просто поменялись местами. Ясное дело, что от этого сумма не изменяется. Впрочем, такое свойство формул Виета можно было и заранее предвидеть, так как совершенно безразлично, какой корень следует обозначать через α_1, какой через α_2 и т. д.

Мы будем называть многочлены

$$\sigma_1 = x_1 + x_2 + \ldots + x_n,$$
$$\sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n, \ldots,$$
$$\sigma_n = x_1x_2 \ldots x_n$$

основными симметрическими функциями переменных $x_1, x_2, \ldots, x_n$.

Помимо основных симметрических функций существует бесчисленное множество других многочленов нескольких переменных, не меняющих своего вида ни при какой перестановке переменных. Возьмём хотя бы функцию

$$F(x_1, x_2) = x_1^2x_2 + x_1x_2^2. \tag{3}$$

Если переставить x_1 и x_2, то получится

$$x_2^2x_1 + x_2x_1^2,$$

т. е. та же функция $F(x_1, x_2)$.

Многочлен $F(x_1, x_2, \ldots, x_n)$, не меняющийся при любой перестановке переменных $x_1, x_2, \ldots, x_n$, называется симметрической функцией от $x_1, x_2, \ldots, x_n$.

Из определения следует, что если симметрическая функция $F(x_1, x_2, \ldots, x_n)$ содержит член

$$Ax_1^{l_1}x_2^{l_2} \ldots x_n^{l_n},$$

то она содержит также все члены вида

$$Ax_1^{l_{s1}}x_2^{l_{s2}} \ldots x_n^{l_{sn}},$$

получающиеся из данного любыми перестановками показателей $l_1, l_2, \ldots, l_n$.

Вернёмся снова к симметрической функции (3). Её можно преобразовать следующим образом:

$$F(x_1, x_2) = x_1x_2(x_1 + x_2).$$

Но x_1x_2 и $x_1 + x_2$ — основные симметрические функции σ_1 и σ_2 от x_1, x_2. Следовательно:

$$F(x_1, x_2) = \sigma_1\sigma_2,$$

т. е. мы выразили нашу функцию через основные симметрические функции.

Вообще имеет место такая теорема:

Основная теорема теории симметрических функций. *Всякая симметрическая функция*

$$F(x_1, x_2, \ldots, x_n)$$

от $x_1, x_2, \ldots, x_n$ может быть представлена в виде многочлена от основных симметрических функций: $F(x_1, x_2, \ldots, x_n) = \varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$.

К доказательству этого предложения мы приступим, однако, не сразу. Прежде всего не мешает уточнить определение многочлена от нескольких переменных. Многочленом (в числовом поле P) от переменных $x_1, x_2, \ldots, x_n$ называется выражение

$$\Phi(x_1, x_2, \ldots, x_n) = A_1 x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} + \\ + A_2 x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n} + \ldots + A_r x_1^{s_1} x_2^{s_2} \ldots x_n^{s_n} \quad (A_i \neq 0),$$

где $a_i, b_i, \ldots, s_i$ — целые неотрицательные числа, $A_1, A_2, \ldots, A_r$ — коэффициенты (принадлежащие полю P). Выражение

$$A_i x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$$

принято называть *членом многочлена*, а сумму показателей $l_1 + l_2 + \ldots + l_n$ *степенью члена*. Наконец, наибольшая из степеней членов называется *степенью многочлена*. В частности многочлен называется *однородным*, или *формой* относительно $x_1, x_2, \ldots, x_n$, если все его члены имеют одинаковую степень.

Например, выражение

$$x_1^2 x_2 x_3 + 5x_1^3 x_3 - 2x_1 x_2^2 x_3^3 + 8$$

есть многочлен шестой степени от трёх переменных x_1, x_2, x_3, но не есть форма.

Затем следует ввести важное для доказательства теоремы понятие *высоты* члена. Условимся считать из двух членов многочлена $\Phi(x_1, x_2, \ldots, x_n)$ тот *выше*, у которого больше показатель при x_1, а из двух членов с одинаковыми показателями при x_1 тот, у которого больше показатель при x_2 и т. д. Иными слова, член

$$A_i x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$$

будет выше члена

$$A_j x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$$

тогда и только тогда, когда первая неисчезающая разность $l_k - m_k$ положительна.

Так, из двух членов

$$x_1^6 x_2^3 \quad \text{и} \quad x_1^6 x_2^2 x_3 x_4$$

первый выше второго.

Напишем впереди высший член многочлена, затем следующий по высоте член и т. д. Мы получим тогда так называемое *лексикографическое* расположение членов.

Пример. Расположить лексикографически

$$\Phi(x_1, x_2, x_3, x_4) = x_1 x_2 + x_1^2 x_4 + x_2^2 x_3 x_4 + x_2^3 x_4.$$

Здесь высшим членом является $x_1^2 x_4$; следующим по высоте членом будет $x_1 x_2$, затем пойдут $x_2^3 x_4$ и $x_2^2 x_3 x_4$. Таким образом

$$\Phi(x_1, x_2, x_3, x_4) = x_1^2 x_4 + x_1 x_2 + x_2^3 x_4 + x_2^2 x_3 x_4.$$

Ещё одно замечание. Для дальнейшего полезно иметь в виду следующую лемму.

Лемма. *Высший член произведения двух многочленов равен произведению высших членов сомножителей.*

В самом деле, обозначим через

$$Ax_1^{a_1}x_2^{a_2}\dots x_n^{a_n} \tag{4}$$

высший и через

$$Bx_1^{b_1}x_2^{b_2}\dots x_n^{b_n} \tag{5}$$

какой-нибудь более низкий члены первого многочлена. Поскольку член (4) выше члена (5), первая неисчезающая разность $a_k - b_k$ должна быть положительной.

Точно так же обозначим через

$$Lx_1^{l_1}x_2^{l_2}\dots x_n^{l_n} \tag{6}$$

и

$$Mx_1^{m_1}x_2^{m_2}\dots x_n^{m_n} \tag{7}$$

высший и какой-нибудь более низкий члены второго многочлена. Здесь первая неисчезающая разность $l_s - m_s$ также должна быть положительной. Пусть для определённости $k \leqslant s$ (при $k \geqslant s$ рассуждения остаются теми же, надо только везде вместо k писать s и $a_s - b_s$ считать равным нулю). Если перемножить высшие члены (4), (6) и члены (5), (7), то получится

$$ALx_1^{a_1+l_1}x_2^{a_2+l_2}\dots x_n^{a_n+l_n}, \tag{8}$$

$$BMx_1^{b_1+m_1}x_2^{b_2+m_2}\dots x_n^{b_n+m_n}. \tag{9}$$

Но первая неисчезающая разность показателей этих членов равна

$$(a_k+l_k)-(b_k+m_k)=(a_k-b_k)+(l_k-m_k)>0,$$

так как $a_k - b_k$ положительно, а $l_k - m_k$ равно нулю [1]). Следовательно, член (8) выше члена (9).

Подобным же образом доказывается, что член (8) выше произведения членов (4), (7) и произведения членов (5), (6).

Теперь можно приступить к доказательству теоремы.

Пусть $F(x_1, x_2, \dots, x_n)$ — симметрическая функция, расположенная лексикографически, и пусть её высшим членом является

$$Ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}. \tag{10}$$

[1]) Написанная разность действительно является первой неисчезающей разностью, так как при $i < k \leqslant s$

$$a_i - b_i = 0, \qquad l_i - m_i = 0$$

и потому

$$(a_i + l_i) - (b_i + m_i) = (a_i - b_i) + (l_i - m_i) = 0.$$

Мы утверждаем прежде всего, что показатели $k_1, k_2, \ldots, k_n$ должны удовлетворять неравенству:

$$k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n. \tag{11}$$

И в самом деле, симметрическая функция $F(x_1, x_2, \ldots, x_n)$ кроме члена (10) должна содержать также все члены, получающиеся из (10) с помощью перестановок переменных $x_1, x_2, \ldots, x_n$; например, симметрическая функция должна содержать член

$$Ax_1^{k_2}x_2^{k_1} \ldots x_n^{k_n}.$$

Но член (10) является высшим. Следовательно, $k_1 \geqslant k_2$. Подобным же образом, сравнивая член (10) с

$$Ax_1^{k_1}x_2^{k_3}x_3^{k_2} \ldots x_n^{k_n},$$

приходим к выводу, что $k_2 \geqslant k_3$ и т. д.

Попытаемся теперь в симметрической функции $F(x_1, x_2, \ldots; x_n)$ уничтожить высший член (10). Для этого обратимся к произведению

$$A\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3} \ldots \sigma_{n-1}^{k_{n-1}-k_n}\sigma_n^{k_n}, \tag{12}$$

где $\sigma_1, \sigma_2, \ldots, \sigma_n$ — основные симметрические функции.

Так как $\sigma_1, \sigma_2, \ldots, \sigma_n$ имеют высшими членами соответственно

$$x_1,\ x_1x_2,\ \ldots,\ x_1x_2 \ldots x_n,$$

то по доказанной лемме высшим членом произведения (12) должно быть

$$A(x_1)^{k_1-k_2}(x_1x_2)^{k_2-k_3} \ldots (x_1x_2 \ldots x_{n-1})^{k_{n-1}-k_n}(x_1x_2 \ldots x_n)^{k_n} = Ax_1^{k_1}x_2^{k_2} \ldots x_n^{k_n}.$$

Получился, как видим, высший член (10) симметрической функции $F(x_1, x_2, \ldots, x_n)$. Следовательно, симметрическая функция

$$F_1(x_1, x_2, \ldots, x_n) = F(x_1, x_2, \ldots, x_n) - A\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3} \ldots \sigma_n^{k_n}$$

уже не будет содержать члена (10), а также и всех тех членов, которые получаются из (10) всевозможными перестановками переменных $x_1, x_2, \ldots, x_n$. Наибольший по высоте член функции $F_1(x_1, x_2, \ldots, x_n)$ будет ниже высшего члена (10) функции $F(x_1, x_2, \ldots, x_n)$.

В свою очередь, тем же методом можно уничтожить высший член симметрической функции $F_1(x_1, x_2, \ldots, x_n)$; в результате получится функция $F_2(x_1, x_2 \ldots; x_n)$, состоящая из членов меньшей высоты и т. д. Легко видеть, что этот процесс понижения не бесконечен. В самом деле, пусть

$$Bx_1^{l_1}x_2^{l_2} \ldots x_n^{l_n} \tag{13}$$

— высший член одной из симметрических функций $F_1, F_2, \ldots$ Он должен быть ниже члена (10). Следовательно, должно иметь место неравенство

$$k_1 \geqslant l_1. \tag{14}$$

Кроме того

$$l_1 \geqslant l_2 \geqslant \ldots \geqslant l_n \qquad (15)$$

[см. неравенства (11)]. Но соотношениям (14) и (15) может удовлетворять лишь конечное число систем значений показателей l_i. Таким образом высших членов (13), а потому и функций $F_1, F_2, \ldots$, может быть только конечное множество.

Итак, указанный процесс понижения порядка не бесконечен, и мы в конце концов выразим симметрическую функцию $F(x_1, x_2, \ldots, x_n)$ полностью через $\sigma_1, \sigma_2, \ldots, \sigma_n$:

$$F(x_1, x_2, \ldots, x_n) = \varphi(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Мы доказали теорему даже с некоторым уточнением. Как видно из самого доказательства, *коэффициенты многочлена* $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ *должны принадлежать тому же числовому полю, что и коэффициенты данной функции* $F(x_1, x_2, \ldots, x_n)$. Так, если у $F(x_1, x_2, \ldots, x_n)$ коэффициенты действительные числа, то коэффициенты многочлена $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ также должны быть действительными.

Пример. Выразим симметрическую функцию

$$F(x_1; x_2; x_3) = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2$$

через $\sigma_1, \sigma_2, \sigma_3$.

Здесь высшим членом является $x_1^2x_2$, $k_1 = 2$, $k_2 = 1$, $k_3 = 0$.

Поэтому, следуя общей теории, составляем разность:

$$\begin{aligned} &F(x_1, x_2, x_3) - \sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\sigma_3^{k_3} = \\ &= (x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2) - \sigma_1\sigma_2 = \\ &= (x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2) - \\ &- (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) = -3x_1x_2x_3. \end{aligned}$$

Но $x_1x_2x_3 = \sigma_3$. Следовательно:

$$F(x_1; x_2; x_3) = \sigma_1\sigma_2 - 3\sigma_3.$$

Задача. Выразить через $\sigma_1, \sigma_2, \sigma_3$ следующие симметрические функции от трёх переменных:

a) $F(x_1, x_2, x_3) = x_1^3x_2 + x_1^3x_3 + x_1x_2^3 + x_1x_3^3 + x_2^3x_3 + x_2x_3^3$,

b) $H(x_1, x_2, x_3) = x_1^2x_2^2 + x_1^2x_3^2 + x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2 + x_2^2x_3^2$.

§ 45. Основная теорема алгебры

Теперь мы в состоянии ответить на вопросы, заданные в конце § 43. Оказывается, что комплексных чисел достаточно для решения любого алгебраического уравнения. Это вытекает из следующей теоремы:

Основная теорема алгебры. *Всякий многочлен с действительными коэффициентами имеет по меньшей мере один комплексный корень.*

Доказательство. Ранее мы уже установили, что всякий многочлен нечётной степени с действительными коэффициентами имеет по меньшей мере один действительный корень (см. стр. 187). Таким образом теорему остаётся доказать для многочленов чётных степеней. Для этой цели воспользуемся методом индукции.

Предположим; что теорема доказана для многочленов

$$g(x) = x^m - q_1 x^{m-1} + q_2 x^{m-2} - \ldots + (-1)^m q_m,$$

степень m которых равна $2^{k-1}Q$, где $k > 1$ и Q—*любое* нечётное число. Пусть

$$f(x) = x^n - p_1 x^{n-1} + p_2 x^{n-2} - \ldots + (-1)^n p_n$$

многочлен с действительными коэффициентами [1]) и пусть его степень $n = 2^k q$, где q—нечётное число. Докажем, что при нашем предположении теорема должна быть верна и для многочлена $f(x)$.

Мы знаем, что для многочлена $f(x)$ должно существовать поле разложения P, содержащее поле комплексных чисел или совпадающее с ним. Обозначим корни $f(x)$ в поле P через $\alpha_1, \alpha_2, \ldots, \alpha_n$ и составим многочлен $g(x)$, имеющий корнями всевозможные выражения $\alpha_i\alpha_j + c(\alpha_i + \alpha_j)$ (c — действительное число, $i \neq j$):

$$\begin{aligned} g(x) &= x^m - q_1 x^{m-1} + q_2 x^{m-2} - \ldots + (-1)^m q_m = \\ &= [x - \alpha_1\alpha_2 - c(\alpha_1 + \alpha_2)][x - \alpha_1\alpha_3 - c(\alpha_1 + \alpha_3)] \ldots \\ &\quad \ldots [x - \alpha_{n-1}\alpha_n - c(\alpha_{n-1} + \alpha_n)]. \end{aligned} \tag{1}$$

Очевидно, что выражений $\alpha_i\alpha_j + c(\alpha_i + \alpha_j)$ будет столько, сколько существует сочетаний из n по два, т. е.

$$C_n^2 = \frac{n(n-1)}{2} = \frac{2^k q(2^k q - 1)}{2} = 2^{k-1}Q,$$

где через Q мы обозначили нечётное число $q(2^k q - 1)$. Следовательно степень m многочлена $g(x)$ равна $2^{k-1}Q$.

Далее, если α_i заменить через α_j и α_j через α_i то многочлен $g(x)$ от этого не изменится, может произойти только перестановка его линейных множителей. Таким образом коэффициенты многочлена $g(x)$ являются симметрическими функциями от $\alpha_1, \ldots, \alpha_n$:

$$q_i = F_i(\alpha_1, \alpha_2, \ldots, \alpha_n) \quad (i = 1, 2, \ldots, m).$$

При этом коэффициенты симметрических функций F_i должны быть действительными, так как c — действительное число. Согласно основной теореме теории симметрических функций (см. § 44) отсюда следует, что q_i должны выражаться через $\sigma_1 = p_1$, $\sigma_2 = p_2$, $\ldots$, $\sigma_n = p_n$:

$$q_i = \varphi_i(p_1, p_2, \ldots, p_n),$$

где φ_i — многочлен с действительными коэффициентами. Следовательно, поскольку коэффициенты p многочлена $f(x)$ действительны должны быть также действительными и q_i.

[1]) Всегда можно считать старший коэффициент равным единице; в противном случае мы на него поделили бы все коэффициенты.

Итак, мы видим, что $g(x)$ — многочлен степени $2^{k-1}Q$ с действительными коэффициентами. Для таких многочленов теорема предполагается справедливой. Стало быть, $g(x)$ имеет по меньшей мере один комплексный корень.

Теперь станем давать c любые действительные значения $c_1, c_2, \ldots$ Мы получим тогда бесчисленное множество многочленов $g(x)$ типа (1) и каждый из них будет иметь по меньшей мере один комплексный корень. В нашем распоряжении, таким образом, имеется бесчисленное множество комплексных чисел.

Но из букв α можно составить лишь конечное число комбинаций $\alpha_i\alpha_j$ и $\alpha_i+\alpha_j$. Поэтому мы неизбежно должны встретиться по меньшей мере с двумя комплексными числами, которые состоят из одних и тех же букв α. Пусть это будут, например, $\alpha_i\alpha_j+c_1(\alpha_i+\alpha_j)$ и $\alpha_i\alpha_j+c_2(\alpha_i+\alpha_j)$. Тогда на помощь приходит следующая лемма.

Лемма. *Если для двух различных действительных значений c_1, c_2 и двух корней α_i и α_j рассматриваемого многочлена $f(x)$ выражения*

$$\alpha_i\alpha_j+c_1(\alpha_i+\alpha_j) \quad \text{и} \quad \alpha_i\alpha_j+c_2(\alpha_i+\alpha_j)$$

являются комплексными, то α_i и α_j также должны быть комплексными.

Действительно, пусть

$$\alpha_i\alpha_j+c_1(\alpha_i+\alpha_j)=k_1,$$
$$\alpha_i\alpha_j+c_2(\alpha_i+\alpha_j)=k_2,$$

где k_1 и k_2 предполагаются коплексными числами. Если из первого равенства вычесть второе, то получится

$$(c_1-c_2)(\alpha_i+\alpha_j)=k_1-k_2,$$

откуда:

$$\alpha_i+\alpha_j=-p. \tag{2}$$

Через $-p$ мы обозначили $\frac{k_1-k_2}{c_1-c_2}$.

Теперь находим $\alpha_i\alpha_j$, для чего подставляем найденное значение $\alpha_i+\alpha_j$ хотя бы в первое равенство. Получим:

$$\alpha_i\alpha_j-cp=k_1,$$

откуда

$$\alpha_i\alpha_j=q; \tag{3}$$

через q мы здесь обозначили k_1+cp.

Из соотношений (2) и (3) видно, что α_i и α_j являются корнями квадратного уравнения

$$x^2+px+q=0$$

с комплексными коэффициентами. Следовательно, поскольку поле разложения P многочлена $f(x)$ содержит поле комплексных чисел, α_i и α_j должны быть комплексными (см. § 40, стр. 208).

Возвращаемся к прерванному доказательству основной теоремы алгебры. По вышеприведённой лемме α_i и α_j должны быть комплекс-

ными. Таким образом многочлен $f(x)$ имеет не только один, но даже два комплексных корня.

Тем самым основная теорема алгебры доказана полностью. В самом деле, если она верна для многочленов нечётной степени, то она, как мы уже убедились, верна и для многочленов степени $2Q$; если она верна для многочленов степени $2Q$, то она верна для многочленов степени 2^2Q и т. д.

Теперь естественно спросить: будут ли многочлены с комплексными (а не только с действительными) коэффициентами иметь комплексные корни. Тут на помощь приходят следующие свойства комплексных чисел. Пусть $z=a+bi$ какое-нибудь комплексное число. Условимся обозначать той же буквой, но с чертой наверху число, сопряжённое с z. Таким образом $\overline{z}=a-bi$. В частности, при $b=0$ получается, что $z=a=\overline{z}$, т. е. действительное число сопряжено с самим собой.

Легко видеть, что *при сложении и умножении сопряжённых комплексных чисел получаются действительные числа*:

$$z+\overline{z}=2a, \qquad z\overline{z}=a^2+b^2.$$

Пусть далее $z_1=a_1+b_1i$, $z_2=a_2+b_2i$. Без особого труда можно показать, что

$$\overline{z_1+z_2}=\overline{z}_1+\overline{z}_2, \qquad \overline{z_1z_2}=\overline{z}_1\overline{z}_2. \tag{4}$$

Например,

$$z_1+z_2=(a_1+a_2)+(b_1+b_2)i.$$

Поэтому

$$\overline{z_1+z_2}=(a_1+a_2)-(b_1+b_2)i.$$

Но точно такой же результат получается и при сложении $\overline{z}_1$, $\overline{z}_2$:

$$\overline{z}_1+\overline{z}_2=(a_1-b_1i)+(a_2-b_2i)=(a_1+a_2)-(b_1+b_2)i.$$

Аналогичным образом доказывается и второе соотношение (4).

Соотношения (4), очевидно, имеют место и для большего числа слагаемых и множителей, а именно:

$$\overline{z_1+z_2+\ldots+z_n}=\overline{z}_1+\overline{z}_2+\ldots+\overline{z}_n, \quad \overline{z_1z_2\ldots z_n}=\overline{z}_1\overline{z}_2\ldots\overline{z}_n. \tag{5}$$

В частности,

$$\overline{z^n}=(\overline{z})^n. \tag{6}$$

Наконец, небесполезно такое замечание.

З а м е ч а н и е. Рассмотрим многочлен

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n \tag{7}$$

с комплексными коэффициентами. Если a_i заменить сопряжённым числом $\overline{a}_i$, то получится так называемый *сопряжённый многочлен*

$$\overline{f}(x)=\overline{a}_0x^n+\overline{a}_1x^{n-1}+\ldots+\overline{a}_n. \tag{8}$$

ы утверждаем; что *если* α *— корень* $f(x)$; то α *будет корнем* $\overline{f}(x)$; *обратно.* В частности; *если* α *— корень многочлена с действительными коэффициентами; то* $\overline{\alpha}$ *будет корнем того же многочлена* $f(x)$ потому что здесь $f(x)$ совпадает с $\overline{f}(x)$].

В самом деле; в силу соотношений (5) и (6)

$$\overline{f(\alpha)} = \overline{f}(\overline{\alpha});$$

е. комплексное число $\overline{f}(\overline{\alpha})$ сопряжено с $f(\alpha)$. Стало быть; если $(\alpha) = 0$, то равно нулю и $\overline{f}(\overline{\alpha}) = 0$, так как число, сопряжённое нулём; есть нуль. Обратно; по той же причине $f(\alpha) = 0$, если $\overline{\alpha}) = 0$.

После всех этих предварительных замечаний можно без труда казать такие важные следствия из основной теоремы алгебры.

Следствие 1. *Всякий многочлен с комплексными коэффициентами меет по меньшей мере один комплексный корень.*

Для доказательства умножим многочлен $f(x)$ на сопряжённый у многочлен $\overline{f}(x)$:

$$f(x)\overline{f}(x) = a_0\overline{a}_0x^{2n} + (a_0\overline{a}_1 + \overline{a}_0a_1)x^{2n-1} + \ldots + a_n\overline{a}_n.$$

олучился многочлен с действительными коэффициентами. Именно, $\overline{a}_0$ действительно; как произведение сопряжённых чисел a_0 и $\overline{a}_0$; $\overline{a}_0a_1 + \overline{a}_0a_1$ действительно; как сумма двух сопряжённых чисел $a_0\overline{a}_1$ и $\overline{a}_0a_1$ и т. д. Следовательно, в силу основной теоремы алгебры; огочлен $f(x)\overline{f}(x)$ имеет по меньшей мере один комплексный корень. сть это будет β, т. е. пусть $f(\beta)\overline{f}(\beta) = 0$. Отсюда либо $f(\beta) = 0$; бо $\overline{f}(\beta) = 0$. В первом случае корнем $f(x)$ будет β. Во втором чае корнем $f(x)$ будет согласно вышеприведённому замечанию ло, сопряжённое с β. В обоих случаях следствие 1 доказано.

Проанализируем несколько глубже следствие 1. Пусть $p(x)$ огочлен, неприводимый в поле комплексных чисел. Он по только доказанному должен иметь хотя бы один комплексный корень. овначим этот корень через α; тогда

$$p(x) = (x - \alpha)\varphi(x).$$

$p(x)$ неприводимо; поэтому $\varphi(x) = c$; где c — постоянное число. ким образом:

$$p(x) = c(x - \alpha);$$

. в поле комплексных чисел неприводимыми могут быть только ейные многочлены.

Возьмём теперь произвольный многочлен $f(x)$ n-й степени и раз им его на неприводимые множители. Как мы сейчас убедились; множители должны быть линейными. Следовательно

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n).$$

и комплексные числа $\alpha_1, \alpha_2, \ldots, \alpha_n$ являются корнями $f(x)$. Среди чисел $\alpha_1; \alpha_2, \ldots, \alpha_n$ могут быть одинаковые; поэтому окончательное разложение $f(x)$ таково:

$$f(x) = c(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\ldots(x-\alpha_s)^{k_s},$$

причем $k_1 + k_2 + \ldots + k_s = n$.

Мы пришли к такому следствию.

Следствие 2. *Всякий многочлен n-й степени с комплексными коэффициентами имеет ровно n комплексных корней.*

Иначе говоря, *поле комплексных чисел есть поле разложения любого многочлена с комплексными коэффициентами.*

Следствие 3. *В поле действительных чисел неприводимыми могут быть только многочлены не выше второй степени.*

В самом деле, пусть $p(x)$ многочлен выше первой степени, неприводимый в поле действительных чисел. Обозначим один из его комплексных корней через $a + bi$. Тогда сопряжённое комплексное число $a - bi$ также будет его корнем, потому что у многочлена с действительными коэффициентами комплексные корни попарно сопряжены (см. замечание на стр. 241). Следовательно, $p(x)$ должно делиться на

$$(x-a-bi)(x-a+bi) = (x^2 - 2ax + a^2 + b^2);$$

т. е. на многочлен второй степени с действительными коэффициентами. Но $p(x)$ неприводимо; поэтому $p(x)$ с точностью до постоянного множителя должно совпадать с квадратным многочленом $x^2 - 2ax + a^2 + b^2$.

Из этого следствия непосредственно вытекает, что всякий многочлен с действительными коэффициентами в поле действительных чисел разлагается на линейные и квадратные множители.

Еще в 1629 г. французский ученый Жирар предположил, что любое алгебраическое уравнение n-й степени имеет n корней, действительных и мнимых. Но математика в то время находилась на недостаточно высоком уровне развития, и потому Жирар не мог доказать это предложение. Прошло свыше ста лет. В 1746 г. французский учёный Даламбер впервые попытался доказать основную теорему алгебры, но его рассуждения оказались нестрогими. Столь же безуспешными оказались попытки таких учёных, как Эйлер и Лагранж. И только Гауссу в 1799 г. удалось решить вопрос до конца. Впоследствии Гаусс нашёл ещё три доказательства основной теоремы алгебр В нашем учебнике использована идея его второго доказательст

Скажем несколько слов о приближённом вычислении комплексных к ней уравнений. Об алгебраическом решении уравнений речь будет в следу щей главе. В настоящее время одним из самых удобных в практическом от шении является способ Греффе-Чике. В основе этого способа лежит ид высказанная ещё Даниилом Бернулли в 1728 г. Эту идею мы сейчас и приве; в самых общих чертах.

Пусть $\alpha_1, \alpha_2, \ldots, \alpha_n$ — корни уравнения $f(x) = 0$ n-й степени и пусть α_1 — н больший по модулю корень. Обозначим через s_k сумму k-ых степеней кор α_i: $s_k = \alpha_1^k + \alpha_2^k + \ldots + \alpha_n^k$. Легко заметить, что

$$\frac{s_k}{s_{k-1}} = \alpha_1 \frac{1 + \left(\frac{\alpha_2}{\alpha_1}\right)^k + \ldots \left(\frac{\alpha_n}{\alpha_1}\right)^k}{1 + \left(\frac{\alpha_2}{\alpha_1}\right)^{k-1} + \ldots + \left(\frac{\alpha_n}{\alpha_1}\right)^{k-1}}.$$

Увеличивая k неограниченно, получим, что

$$\lim \frac{s_k}{s_{k-1}} = z_1,$$

т. е. корень z_1 при достаточно большом k будет весьма мало отличаться от отношения $\frac{s_k}{s_{k-1}}$.

Подробное изложение способа Греффе-Энке можно найти почти во всех руководствах по приближённым вычислениям, например в книге акад. А. Н. Крылова, Лекции о приближённых вычислениях, 1933 (издание второе), в книге Дж. Скарборо, Численные методы математического анализа, ОНТИ, 1934.

§ 46. Теорема Фробениуса

Комплексные числа у нас получились в результате расширения области действительных чисел. Мы покажем, что поле комплексных чисел является в некотором смысле единственным расширением.

Назовём гиперкомплексную систему A относительно поля действительных чисел *системой с делением*, если в A существует по меньшей мере одно гиперкомплексное число $\alpha \neq 0$ и для всякого $\alpha \neq 0$ уравнения $\alpha x = \beta$ и $y\alpha = \beta$ разрешимы. В частности, если в A умножение коммутативно, то мы будем называть A коммутативной системой с делением. Простейшим примером системы с делением является система, изоморфная полю действительных чисел; она, очевидно, является коммутативной. Комплексные числа образуют также коммутативную систему с делением. Другим примером системы с делением может служить алгебра кватернионов; но это уже будет некоммутативная система. Оказывается, что этими примерами исчерпываются все возможные системы с делением относительно поля действительных чисел, а именно имеет место следующая замечательная теорема.

Теорема Фробениуса. *Относительно поля действительных чисел существуют (с точностью до изоморфизма) только три системы с делением—само поле действительных чисел, поле комплексных чисел и система кватернионов*[1]).

Прежде, чем переходить к доказательству этой теоремы, сделаем несколько замечаний.

Замечание 1. Во всякой системе A с делением существует единственная главная единица, т. е. в A существует такое единственное ε, что $\varepsilon\alpha = \alpha\varepsilon = \alpha$ для любого α из A.

В самом деле, пусть β—произвольное гиперкомплексное число системы A, отличное от нуля. По определению системы с делением уравнения $\beta x = \beta$ должно быть разрешимо в A. Обозначим одно из решений этого уравнения через ε и возьмём ещё одно произвольное число α системы A. Так как в системе A уравнение $y\beta = \alpha$ разрешимо, то в A должно существовать такое γ, для которого $\alpha = \gamma\beta$. Мы можем, следовательно, написать, что $\alpha\varepsilon = \gamma\beta\varepsilon = \gamma\beta = \alpha$. Далее, в системе A должно быть разрешимо уравнение $\alpha x = \varepsilon$ для всякого $\alpha \neq 0$. Мы видим отсюда, что все элементы системы A, кроме нуля, образуют группу относительно умножения, причём ε является единицей этой группы: для любого $\alpha \neq 0$ из A $\alpha\varepsilon = \varepsilon\alpha = \alpha$. Но последнее равенство, очевидно, остаётся в силе и при $\alpha = 0$. Следовательно, ε есть главная единица системы A и притом единственная, так как всякая группа обладает лишь единственной единицей.

Замечание 2. Пусть A—гиперкомплексная система n-го порядка относительно поля действительных чисел (она может и не быть системой с делением). Все определения и выводы § 18 можно дословно перенести и на гиперкомплексные числа системы A.

А именно, обозначим базис системы A через $e_1, \ldots, e_n$. Каждое гиперкомплексное число α из A будет представляться в виде линейной комбинации от $e_1, \ldots, e_n$:

$$\alpha = a_1 e_1 + \ldots + a_n e_n,$$

[1]) Таким образом поле комплексных чисел образует относительно поля действительных чисел единственную коммутативную систему с делением, содержащую совокупность действительных чисел, как часть.

где a_i—действительные числа. Система A таким образом играет роль линейного модуля, а её порядок n—роль ранга модуля. При этом гиперкомплексные числа $\alpha_1, \ldots, \alpha_m$ системы A будут называться *линейно зависимыми* (относительно поля действительных чисел), если существуют такие действительные числа $c_1, \ldots, c_m$, не все равные нулю, что

$$c_1\alpha_1 + \ldots + c_m\alpha_m = 0;$$

Нетрудно убедиться, применяя рассуждения § 18 что в системе A имеет место теорема Штейница о замене базиса, а также следствия из этой теоремы. Отсюда в частности вытекает, что в системе A всякое гиперкомплексное число α должно быть корнем некоторого алгебраического уравнения с действительными коэффициентами степени не выше $n+1$.

В самом деле, согласно следствию 1 из теоремы Штейница, $n+1$ последовательных степеней $\alpha, \alpha^2, \ldots, \alpha^{n+1}$ гиперкомплексного числа α должны быть линейно зависимыми; таким образом

$$c_0\alpha + c_1\alpha^2 + \ldots + c_n\alpha^{n+1} = 0,$$

где c_i—действительные числа, не все равные нулю. Мы получили алгебраическое уравнение относительно α степени не выше, чем $n+1$.

Теперь воспроизведём в основных чертах одно из наиболее простых доказательств теоремы Фробениуса.

Доказательство. Пусть A—система с делением n-го порядка относительно поля действительных чисел. Обозначим её базис через $e_1, \ldots, e_n$. Согласно теореме Штейница о замене одного базиса другим мы можем всегда предполагать, что $e_1 = \varepsilon$, где ε—главная единица системы A.

Если порядок n системы A равен 1, то всякое гиперкомплексное число из A будет иметь вид $\alpha = a\varepsilon$, где a—действительное число. Нетрудно убедиться, что система A будет в этом случае изоморфна полю действительных чисел. В самом деле, приведём во взаимно однозначное соответствие каждое $\alpha = a\varepsilon$ с действительным числом a. Читатель может сам без труда проверить, что это соответствие обладает всеми характерными чертами изоморфизма.

Если порядок n системы A больше или равен 2, то совокупность выражений $\alpha = a\varepsilon$ не будет, конечно, исчерпывать всей системы A. В этом случае в A будет содержаться как часть поле, изоморфное полю действительных чисел.

Условимся в силу указанного изоморфизма главную единицу ε отождествлять с числом 1, $a\varepsilon$ выражения $a\varepsilon$ с действительными числами a. Тогда при $n = 1$ система A будет совпадать с полем действительных чисел, а при $n > 1$ будет содержать поле действительных чисел.

Покажем теперь, что при $n \geqslant 2$ любое гиперкомплексное число α системы A, не содержащееся в поле действительных чисел, будет корнем квадратного уравнения с действительными коэффициентами.

Согласно замечанию 2, α должно быть корнем уравнения

$$c_0\alpha + c_1\alpha^2 + \ldots + c_n\alpha^{n+1} = 0$$

с действительными коэффициентами c_i. Вынесем α за скобку

$$(c_0 + c_1\alpha + \ldots + c_n\alpha^n)\alpha = 0.$$

Так как A есть система с делением, то в системе A произведение нескольких сомножителей может только тогда равняться нулю, когда равен нулю хотя бы один из сомножителей [1]). Отсюда следует, что

$$\alpha = 0 \quad \text{или} \quad c_0 + c_1\alpha + \ldots + c_n\alpha^n = 0.$$

Но α не может равняться нулю, так как 0 принадлежит полю действительных чисел, а α этому полю не принадлежит. Следовательно,

$$c_0 + c_1\alpha + \ldots + c_n\alpha^n = 0; \tag{1}$$

[1]) В самом деле, пусть $\alpha\beta = 0$, но $\alpha \neq 0$. В системе A должно существовать γ, для которого $\gamma\alpha = 1$. Умножим обе части уравнения $\alpha\beta = 0$ слева на γ. Получим $\gamma(\alpha\beta) = (\gamma\alpha)\beta = 1 \cdot \beta = \beta = 0$. Аналогично рассуждаем при $\beta \neq 0$.

Как известно, всякий многочлен в поле действительных чисел разлагается на произведение линейных и квадратных множителей. Стало быть,

$$f(x) = c_0 + c_1 x + \ldots + c_n x^n = c(x-a_1)\ldots(x-a_s)(x^2+p_1x+q_1)\ldots(x^2+p_tx+q_t), \quad (2)$$

$c \neq 0$, a_i, p_i и q_i — действительные числа.

Заменяя в разложении (2) x через α, получим на основании равенства (1), что

$$c(\alpha-a_1)\ldots(\alpha-a_s)(\alpha^2+p_1\alpha+q_1)\ldots(\alpha^2+p_t\alpha+q_t)=0.$$

Но, как мы уже знаем, в системе A произведение нескольких множителей только тогда равно нулю, когда равен нулю хотя бы один из множителей. Поэтому из последнего равенства вытекает, что

$$\alpha - a_i = 0, \text{ т. е. } \alpha = a_i$$

или

$$\alpha^2 + p_j\alpha + q_j = 0.$$

Первая возможность, однако, исключается, так как α по условию не содержится в поле действительных чисел. Следовательно, остается вторая возможность, и мы, таким образом, показали, что α есть корень квадратного уравнения с действительными коэффициентами.

Пользуясь только что полученным результатом, заменим базис $e_1 = 1$, $e_2, \ldots, e_n$ системы A другим базисом. В силу линейной независимости элементов базиса гиперкомплексные числа $e_2, \ldots, e_n$ не могут лежать в поле действительных чисел. Следовательно, эти $e_2, \ldots, e_n$ должны быть корнями квадратных уравнений:

$$e_j^2 + 2a_je_j + b_j = 0, \quad (j = 2, \ldots, n) \quad (3)$$

где a_j и b_j — действительные числа.

Уравнения (3) можно преобразовать в следующие уравнения:

$$(e_j + a_j)^2 = a_j^2 - b_j.$$

Полагая $a_j^2 - b_j = \pm c_j^2$ (c_j — некоторое действительное число), получаем, что

$$(e_j + a_j)^2 = [\pm c_j^2.$$

Легко убедиться, что впереди c_j^2 должен стоять только знак минус. В самом деле, если бы $(e_j + a_j)^2 = +c_j^2$, то мы бы имели, что

$$(e_j + a_j)^2 - c_j^2 = 0$$

или

$$(e_j + a_j + c_j)(e_j + a_j - c_j) = 0,$$

откуда

$$e_j = -a_j - c_j \text{ или } e_j = -a_j + c_j,$$

т. е. e_j было бы действительным числом, что невозможно.

Итак, $(e_j + a_j)^2 = -c_j^2$. Разделим обе части этого равенства на c_j^2. Получим в результате

$$\left(\frac{e_j + a_j}{c_j}\right)^2 = -1. \quad (4)$$

А теперь заменим базис $e_1 = 1, e_2, \ldots, e_n$ другим базисом $1, i_2, \ldots i_n$, где $i_j = \frac{a_j + e_j}{c_j}$. Согласно равенству (4) $i_2^2 = i_3^2 = \ldots = i_n^2 = -1$.

В случае $n = 2$ базис системы A будет таким образом состоять из элементов 1 и i_2, причём $i_2^2 = -1$. Мы видим отсюда, что система с делением второго порядка относительно поля действительных чисел есть не что иное, как (с точностью до изоморфизма) поле комплексных чисел.

Посмотрим теперь, что получается при $n > 2$.

Возьмём такие гиперкомплексные числа α и β системы A, чтобы $\alpha^2 = \beta^2 = -1$ и 1, α, β, были линейно независимыми. Поскольку 1, α, β линейно независимы, сумма $\alpha + \beta$ и разность $\alpha - \beta$ не могут лежать в поле действительных чисел. Поэтому $\alpha + \beta$ и $\alpha - \beta$ должны быть корнями квадратных уравнений:

$$(\alpha+\beta)^2 + a(\alpha+\beta) + b = 0,$$
$$(\alpha-\beta)^2 + a_1(\alpha-\beta) + b_1 = 0,$$

где a, b, a_1 и b_1—действительные числа. Отсюда, перенося последние два члена уравнений в правые части, получаем:

$$\left.\begin{aligned}(\alpha+\beta)^2 &= -a(\alpha+\beta) - b,\\ (\alpha-\beta)^2 &= -a_1(\alpha-\beta) - b_1.\end{aligned}\right\} \quad (5)$$

С другой стороны,

$$(\alpha+\beta)^2 = (\alpha+\beta)(\alpha+\beta) = \alpha^2 + \alpha\beta + \beta\alpha + \beta^2 = -2 + \alpha\beta + \beta\alpha. \quad (6)$$

Точно так же

$$(\alpha-\beta)^2 = -2 - \alpha\beta - \beta\alpha. \quad (7)$$

Сравнивая правые части уравнений (5) с правыми частями уравнений (6) и (7), видим, что

$$\left.\begin{aligned}-2 + \alpha\beta + \beta\alpha &= -a(\alpha+\beta) - b,\\ -2 - \alpha\beta - \beta\alpha &= -a_1(\alpha-\beta) - b_1.\end{aligned}\right\} \quad (8)$$

Сложим почленно последние два равенства; тогда получим:

$$-4 = -(a+a_1)\alpha - (a-a_1)\beta - (b+b_1),$$

или

$$(a+a_1)\alpha + (a-a_1)\beta + (b+b_1-4) = 0.$$

Но α, β и 1 линейно независимы. Следовательно, коэффициенты $a + a_1$, $a - a_1$ и $b + b_1 - 4$ должны равняться нулю, в силу чего $a = 0$ и $a_1 = 0$. Таким образом равенства (8) принимают более простой вид:

$$-2 + \alpha\beta + \beta\alpha = -b,$$
$$-2 - \alpha\beta - \beta\alpha = -b_1.$$

Отсюда вытекает, что

$$\alpha\beta + \beta\alpha = 2c, \quad (9)$$

где $2c = 2 - b = b_1 - 2$. Равенство (9) будет играть существенную роль.

Согласно равенству (9) $i_2 i_3 + i_3 i_2 = 2c$. Найдём такое $j = a_0 + a_1 i_2 + a_2 i_3$, чтобы

$$j^2 = -1, \quad (10_1)$$
$$i_2 j + j i_2 = 0. \quad (10_2)$$

Подставляя в левые части равенств (10) выражение j через i_2 и i_3, пользуясь линейной независимостью элементов 1, i_2, i_3 и равенством $i_2 i_3 + i_3 i_2 = 2c$, определим без труда коэффициенты a_0, a_1 a_2, входящие в выражение j через i_2 и i_3. Предоставляем читателю самостоятельно провести необходимые выкладки и убедиться, что $j = \dfrac{i_3 + c i_2}{\sqrt{1-c^2}}$.

Обратимся теперь к произведению $i_2 j$ и покажем, что оно линейно независимо от 1, i_2 и j. Предположим противное, пусть $i_2 j$ линейно зависит от 1, i_2, j:

$$i_2 j = c_0 + c_1 i_2 + c_2 j \quad (c_0,\ c_1,\ c_2 — \text{действительные числа}).$$

Умножая обе части этого равенства слева на i_2, получаем:

$$-j = c_0 i_2 - c_1 + c_2 i_2 j = c_0 i_2 - c_1 + c_2(c_0 + c_1 i_2 + c_2 j) =$$
$$= (c_0 c_2 - c_1) + (c_1 c_2 + c_0) i_2 + c_2^2 j.$$

Но 1, i_2 и j линейно независимы. Следовательно,

$$c_0c_2 - c_1 = 0, \quad c_1c_2 + c_0 = 0, \quad c_2^2 = -1.$$

Последнее из только что полученных равенств, однако, невозможно, так как c_2 — действительное число. Значит, i_2j не может линейно зависеть от 1, i_2 и j.

Таким образом базис $1, i_2, \ldots i_n$ можно заменить новым базисом $1, i, j, k, i_5, \ldots, i_n$, где $i = i_2$, $j = \dfrac{i_3 + ci_2}{\sqrt{1-c^2}}$, $k = ij$.

Отметим, что для первых четырёх элементов 1, i, j, k нового базиса имеет место та же таблица умножения, что и для кватернионов:

$$1^2 = 1, \quad 1 \cdot i = i \cdot 1 = i, \quad 1 \cdot j = j \cdot 1 = j, \quad 1 \cdot k = k \cdot 1 = k,$$
$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j,$$
$$ji = -k, \quad kj = -i, \quad ik = -j.$$

Соотношения в первой строчке очевидны. Что касается остальных соотношений, то мы ограничимся выводом только одного равенства $k^2 = -1$; другие равенства читатель пусть попытается вывести сам.

Так как $k = ij$, то $k^2 = ijij = i(ji)j$. Но из равенств (10_2) следует, что $ji = -ij$. Стало быть,

$$k^2 = i(-ij)j = -i^2j^2 = -1.$$

Для окончательного доказательства теоремы остаётся убедиться, что порядок системы A не может превосходить четырёх.

Предположим противное—пусть $n > 4$. Тогда базис 1, i, j, k, $i_5, \ldots, i_n$ системы A будет состоять по меньшей мере из пяти элементов и i_5 будет линейно независимо от 1, i, j, k. Согласно равенству (9) мы можем написать, что

$$ii_5 + i_5i = 2c_1, \quad ji_5 + i_5j = 2c_2,$$
$$ki_5 + i_5k = 2c_3.$$

Пользуясь этими равенствами, найдём, чему равно i_5k.

Так как $k = ij$, то

$$i_5k = i_5(ij) = (i_5i)j = (2c_1 - ii_5)j = 2c_1j - i(i_5j) =$$
$$= 2c_1j - i(2c_2 - ji_5) = 2c_1j - 2c_2i + iji_5 = 2c_1j - 2c_2i + ki_5$$

или, заменяя ki_5 через $2c_3 - i_5k$:

$$i_5k = 2c_1j - 2c_2i + 2c_3 - i_5k.$$

Отсюда находим, что

$$i_5k = c_3 - c_2i + c_1j.$$

Умножим теперь обе части последнего равенства справа на k:

$$i_5k^2 = c_3k - c_2ik + c_1jk$$

или, так как $k^2 = -1$, $ik = -j$, $jk = i$:

$$-i_5 = c_3k + c_2j + c_1i,$$

откуда

$$i_5 = -c_1i - c_2j - c_3k.$$

Мы пришли к противоречию: i_5 оказалось линейно зависимым от i, j, k.

Это доказательство теоремы Фробениуса принадлежит американскому математику Л. Е. Диксону.

ГЛАВА ДЕВЯТАЯ

АЛГЕБРАИЧЕСКОЕ РЕШЕНИЕ УРАВНЕНИЙ

§ 47. Двучленные уравнения

В настоящей главе основной нашей целью будет алгебраическое решение уравнений выше второй степени. Решить уравнение алгебраически это значит выразить его корни через коэффициенты с помощью конечного числа действий сложения, вычитания, умножения, деления, возвышения в степень и извлечения корня.

Операция извлечения корня n-й степени из комплексного числа a сводится к нахождению корней так называемого двучленного уравнения

$$u^n - a = 0. \tag{1}$$

В § 41 было установлено, что все n корней этого уравнения можно определить по формуле

$$u_k = \sqrt[n]{r}\left(\cos\frac{\varphi+2k\pi}{n} + i\sin\frac{\varphi+2k\pi}{n}\right) \qquad (k=0, 1, \ldots, n-1), \tag{2}$$

где r — модуль, φ — аргумент числа a.

Таким образом все, что необходимо для решения двучленного уравнения, нам известно. Для дальнейшего, однако, полезно внести некоторые дополнения.

Покажем прежде всего, что уравнение (1) можно привести к уравнению

$$x^n - 1 = 0.$$

Возьмём один из корней уравнения (1), например u_0 и введём новое неизвестное x, полагая $u = u_0 x$. Тогда уравнение (1) примет следующий вид:

$$u_0^n x^n - a = 0.$$

Отсюда, после сокращения на $u_0^n = a$, получаем

$$x^n - 1 = 0. \tag{3}$$

Итак, *все корни n-й степени из a можно получить путём умножения одного из корней на различные корни той же степени из единицы.*

В свою очередь корни из единицы легко определить по формуле

$$x_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} \qquad (k=0, 1, 2, \ldots, n-1). \tag{4}$$

Вывод её прост: модуль единицы равен, очевидно, 1, а аргумент — нулю. Поэтому, полагая в общей формуле (2) $r=1$, $\varphi=0$, приходим к соотношению (4).

Пример. Одно из значений корня третьей степени из i равно $-i$. Чтобы получить все корни, достаточно обратиться к уравнению

$$x^3 - 1 = 0.$$

По формуле (4) имеем:

$$x_0 = \cos 0 + i \sin 0 = 1,$$

$$x_1 = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2} i,$$

$$x_2 = \cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3} = -\frac{1}{2} - \frac{\sqrt{3}}{2} i.$$

Следовательно, все три корня третьей степени из i равны

$$u_0 = -ix_0 = -i, \quad u_1 = -ix_1 = \frac{\sqrt{3}}{2} + \frac{1}{2} i;$$

$$u_2 = -ix_2 = -\frac{\sqrt{3}}{2} + \frac{1}{2} i.$$

Корни двучленного уравнения (3) обладают целым рядом замечательных свойств. Пусть x_k, x_l два каких-нибудь корня n-й степени из единицы. Легко убедиться, что их произведение $x_k x_l$ и частное $\frac{x_k}{x_l}$ также являются корнями n-й степени из единицы. И в самом деле,

$$(x_k x_l)^n = x_k^n x_l^n = 1; \qquad \left(\frac{x_k}{x_l}\right)^n = \frac{x_k^n}{x_l^n} = 1;$$

так как $x_k^n = 1$; $x_l^n = 1$.

Наконец, всякая целая степень x_k как положительная, так и отрицательная, есть снова корень n-й степени из единицы. Действительно, возвысив обе части равенства $x_k^n = 1$ в целую степень s, получим $x_k^{ns} = 1$, или

$$(x_k^s)^n = 1,$$

т. е. x_k^s является корнем n-й степени из единицы. Таким образом бесконечный ряд степеней

$$x_k^0 = 1, \; x_k^1, \; x_k^2; \; x_k^3; \; \ldots; \tag{5}$$

состоит из корней уравнения (3). Но нам уже известно, что число корней уравнения (3) не бесконечно (а именно, равно n), поэтому в ряду (5) неизбежно должны быть повторения. Пусть, например,

$$x_k^s = x_k^t \quad (s > t);$$

Тогда по сокращении на x_k^t получится

$$x_k^{s-t} = 1.$$

Мы будем говорить, что *корень x_k из единицы принадлежит к показателю m; если m наименьшее натуральное число, для которого $x_k^m = 1$.*

Введя это определение, можно доказать следующую теорему.

Теорема. *Если x_k принадлежит к показателю m, то в ряду* (5) *степень x_k^s равна x_k^t тогда и только тогда, когда $s - t$ делится на m.* (В частности, $x_k^s = x_k^0 = 1$ тогда и только тогда, когда s делится на m).

Доказательство. Как мы уже видели, из $x_k^s = x_k^t$ следует, что

$$x_k^{s-t} = 1. \tag{6}$$

Разделим разность $s - t$ на m:

$$s - t = mq + r \quad (r < m),$$

где q, r частное и остаток. Так как $x_k^m = 1$, то $x_k^{mq} = 1$ и

$$x_k^{s-t} = x_k^{mq+r} = x_k^{mq} x_k^r = x_k^r.$$

Поэтому равенство (6) превращается в

$$x_k^r = 1.$$

Мы утверждаем теперь, что $r = 0$. В самом деле, если бы r было отлично от нуля, то m не было бы наименьшим натуральным числом, для которого $x_k^m = 1$. Итак, $r = 0$ и потому $s - t$ делится на m.

Обратное почти очевидно. Если $s - t$ делится на m, то $s - t = mq$. Таким образом $x_k^{s-t} = x_k^{mq} = (x_k^m)^q = 1^q = 1$. Отсюда, умножив обе части последнего равенства на x_k^t, получаем, что

$$x_k^s = x_k^t.$$

Из этой теоремы вытекает такое следствие:

Если корень x_k принадлежит к показателю m, то его степени

$$x_k^0 = 1, \quad x_k^1, \quad \ldots, \quad x_k^{m-1}$$

все различны.

Действительно, $s - t$ заведомо не делится на m, когда s и t меньше m и $s \neq t$.

Из самого определения показателя m видно, что m не может быть больше степени n уравнения (3). Возникает вопрос: существует ли такой корень уравнения (3), который принадлежит к показателю $m = n$? Если такой корень существует, то при возвышении его в степени 0, 1, 2, ..., $n - 1$ должны получиться n различных корней уравнения (3), т. е. все корни уравнения. Чтобы ответить на этот вопрос, рассмотрим число

$$x_1 = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}.$$

Легко убедиться, что x_1 как раз принадлежит к показателю n. В самом деле, по формуле Муавра

$$x_1^k = \left(\cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}\right)^k = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n} = x_k$$
$$(k = 0, 1, 2, \ldots, n-1)$$

и

$$x_1^n = \left(\cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}\right)^n = \cos 2\pi + i \sin 2\pi = 1.$$

Мы видим, что при возвышении x_1 в степени 0, 1, ..., $n - 1$ получаются все n корней уравнения (3) и n является наименьшей

степенью, для которой $x_1^n = 1$. Корни уравнения (3), принадлежащие к показателю n, мы будем называть *первообразными корнями* уравнения (3) или первообразными корнями n-й степени из единицы.

Помимо x_1 существуют и другие первообразные корни. А именно, имеет место теорема:

Теорема. *Корень*

$$x_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = x_1^k$$

уравнения (3) *тогда и только тогда является первообразным, когда* k *взаимно просто с* n.

Доказательство. Найдём, чему равно наименьшее натуральное число m, при котором

$$x_k^m = 1. \tag{7}$$

Так как $x_k = x_1^k$, то равенство (7) можно переписать следующим образом:

$$x_1^{km} = 1.$$

Но x_1 принадлежит к показателю n; поэтому в силу вышедоказанной теоремы km должно делиться на n:

$$km = nq; \tag{8}$$

Обозначим через d общий наибольший делитель k и n; если k и n взаимно просты, то $d = 1$. Мы можем положить

$$k = k_1 d, \quad n = n_1 d,$$

где k_1 и n_1 — взаимно простые числа. Подставляя эти значения k и n в равенство (8), мы после сокращения на d получим

$$k_1 m = n_1 q,$$

т. е. $k_1 m$ должно делиться на n_1. Но число k_1 взаимно просто с n_1; следовательно, m должно делиться на n_1. Из всех натуральных чисел, делящихся на n_1, наименьшим, очевидно, будет само n_1. Таким образом $m = n_1 = \frac{n}{d}$.

Теперь, если k и n взаимно просты, то $d = 1$ и $m = n$. Мы видим, что в этом случае x_k принадлежит к показателю n; т. е. первообразно. Если же k и n не взаимно просты, то $m = \frac{n}{d}$, $d > 1$; в этом случае x_k принадлежит к показателю $\frac{n}{d} < n$ и потому не первообразно.

Наше утверждение доказано, и вместе с тем мы получаем такое очевидное следствие:

Существует столько первообразных корней n*-й степени из единицы, сколько существует чисел взаимно простых с* n *и меньших* n.

Число первообразных корней n-й степени из единицы принято обозначать через $\varphi(n)$ [1]. В частности, $\varphi(1) = 1$, так как существует только один первообразный корень первой степени из единицы, а именно сама единица.

[1]) В теории чисел функция $\varphi(n)$ называется функцией Эйлера.

Пример. Найдём первообразные корни шестой степени из единицы, т. е. первообразные корни уравнения

$$x^6 - 1 = 0.$$

Среди чисел 1, 2, 3, 4, 5 только 1 и 5 взаимно просты с 6. Таким образом $\varphi(6) = 2$, и рассматриваемое уравнение имеет всего два первообразных корня

$$x_1 = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$$

и

$$x_5 = \cos\frac{10\pi}{6} + i\sin\frac{10\pi}{6} = \frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

Задача. Найти первообразные корни уравнений:

a) $x^4 - 1 = 0$, b) $x^8 - 1 = 0$, c) $x^{10} - 1 = 0$, d) $x^{12} - 1 = 0$.

В заключение укажем, по какому закону выражается $\varphi(n)$ через n. Докажем прежде всего следующее предложение:

Если n_1 и n_2—взаимно простые натуральные числа, то всякий первообразный корень n_1n_2-й степени из единицы можно представить единственным образом в виде произведения первообразного корня n_1-й степени из единицы на первообразный корень n_2-й степени из единицы.

Доказательство. По условию n_1 и n_2 взаимно просты; следовательно, для них можно подобрать такие числа k_1 и k_2, чтобы выполнялось равенство

$$n_1k_1 + n_2k_2 = 1. \tag{9}$$

Число k_1 должно быть взаимно просто с n_2. В самом деле, если бы k_1 и n_2 имели общий делитель d, отличный от единицы, то на этот делитель делилась бы левая часть равенства (9), а потому делилась бы и правая часть. Но последнее невозможно при $d \neq 1$. Точно так же k_2 взаимно просто с n_1. Заметив это, возьмём какой-нибудь первообразный корень x n_1n_2-й степени из единицы. Для него получаем:

$$x = x^{n_1k_1 + n_2k_2} = x^{n_2k_2}x^{n_1k_1}; \tag{10}$$

Обозначим показатель, к которому принадлежит $x^{n_2k_2}$, через m. Тогда

$$(x^{n_2k_2})^m = x^{n_2k_2m} = 1.$$

Но x как первообразный корень n_1n_2-й степени из единицы принадлежит к показателю n_1n_2. Следовательно, n_2k_2m должно делиться на n_1n_2:

$$n_2k_2m = n_1n_2q$$

или по сокращении на n_2:

$$k_2m = n_1q.$$

Из последнего равенства видно, что m должно делиться на n_1, так как k_2 взаимно просто с n_1. Отсюда мы заключаем, что $m = n_1$, т. е. $x^{n_2k_2}$ принадлежит к показателю n_1.

Иными словами, $x^{n_2k_2}$ есть первообразный корень n_1-й степени из единицы [1]). Точно так же $x^{n_1k_1}$ есть первообразный корень n_2-й степени из единицы.

---

[1]) Корень, принадлежащий к показателю m, есть в сущности первообразный корень уравнения $x^m - 1 = 0$.

Остаётся доказать единственность разложения (10). Пусть

$$x = y_1 y_2,$$

где y_1—первообразный корень n_1-й степени из единицы, а y_2—первообразный корень n_2-й степени из единицы. Возвысим обе части последнего равенства в $n_2 k_2$-ю степень:

$$x^{n_2 k_2} = y_1^{n_2 k_2} y_2^{n_2 k_2} = y_1^{(-n_1 k_1)} = y_1 y_1^{-n_1 k_1} = y_1.$$

Аналогичным образом убеждаемся, что

$$x^{n_1 k_1} = y_2.$$

Из доказанной теоремы вытекает следующее свойство функции $\varphi(n)$:

1. *Если n_1 и n_2 взаимно простые натуральные числа, то* $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n)$.

Вообще

$$\varphi(n_1 n_2 \dots n_k) = \varphi(n_1)\varphi(n_2)\dots\varphi(n_k), \tag{11}$$

если только числа $n_1, n_2, \dots, n_k$ взаимно простые.

Наконец, выведем второе свойство функции $\varphi(n)$.

2. Если p—простое натуральное число, то

$$\varphi(p^\alpha) = p^\alpha\left(1 - \frac{1}{p}\right) \tag{12}$$

(α—натуральное число).

Доказательство. Рассмотрим p^α последовательных натуральных чисел

$$1, 2, 3, \dots, p^\alpha - 1, p^\alpha.$$

Взаимно простыми с p будут те числа, которые не делятся на p. В нашем ряду на p делятся только числа

$$p, 2p, 3p, \dots, (p^{\alpha-1} - 1)p, p^{\alpha-1}p.$$

и их всего $p^{\alpha-1}$. Следовательно,

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

Теперь $\varphi(n)$ без труда можно выразить через простые множители числа n. Пусть

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

—разложение n на простые множители. В силу равенств (11) и (12) получается, что

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\dots\varphi(p_k^{\alpha_k}) =$$
$$= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right)\dots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right)$$

или окончательно:

$$\varphi(n) = p_1^{\alpha_1} p_2^{\alpha_2}\dots p_k^{\alpha_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right) \tag{13}$$

Примеры.

$$\varphi(6) = 2 \cdot 3\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 2,$$

$$\varphi(21) = 3 \cdot 7\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) = 12.$$

Задача. Вычислить по формуле (13) $\varphi(18)$, $\varphi(30)$, $\varphi(100)$, $\varphi(5896)$.

Попытаемся теперь решить алгебраически общее уравнение третьей степени

$$x^3 + ax^2 + bx + c = 0$$

с комплексными коэффициентами.

Преобразуем прежде всего это уравнение так, чтобы исчез член с квадратом неизвестного. Если положить

$$x = y - \frac{a}{3}$$

и подставить это выражение в наше уравнение, то после несложных выкладок получится более простое уравнение

$$y^3 + py + q = 0; \tag{1}$$

где

$$p = -\frac{a^2}{3} + b, \quad q = \frac{2a^3}{27} - \frac{ab}{3} + c.$$

Таким образом остаётся решить уравнение (1). Полагаем $y = u + v$, где u, v — два новых вспомогательных неизвестных, и подставляем это выражение y в уравнение (1). Мы получим:

$$(u+v)^3 + p(u+v) + q = 0,$$

или, раскрыв скобки и перегруппировав члены:

$$(u^3 + v^3 + q) + (3uv + p)(u+v) = 0. \tag{2}$$

Воспользуемся тем, что вместо одного неизвестного y мы ввели два: u и v, и потребуем, чтобы было

$$3uv + p = 0, \quad \text{или} \quad uv = -\frac{p}{3}.$$

Тогда уравнение (2) приведётся к уравнениям:

$$u^3 + v^3 = -q, \qquad u^3 v^3 = -\frac{p^3}{27}.$$

и мы видим, что u^3, v^3 являются корнями квадратного уравнения

$$z^2 + qz - \frac{p^3}{27} = 0.$$

Решая это уравнение, находим:

$$z = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

откуда

$$u = \sqrt[3]{z_1} = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

$$v = \sqrt[3]{z_2} = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Итак, неполное уравнение (1) нам удалось решить алгебраически:

$$y = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \tag{3}$$

начале XVI в. итальянский математик Ферро впервые решил один частный случай неполного кубического уравнения. В средние века математики старались держать свои открытия в секрете, чтобы блистать на обычных в то время математических состязаниях. Неудивительно поэтому, что Ферро свой результат не опубликовал; но он его сообщил одному ученику—Фиору Флоридусу. Последний, уже после смерти Ферро, вызвал на состязание одного из крупнейших математиков того времени, Николо Тарталью, и предложил ему несколько вопросов, относящихся к решению уравнений третьей степени. Тарталья вызов принял и за восемь дней до состязания нашел способ решения любого неполного кубического уравнения. Результатом состязания было поражение Флоридуса. Тарталья в два часа решил все задачи противника, между тем как Флоридус не мог решить ни одной из задач Тартальи [1]). Вскоре после этого известие об открытии Тартальи дошло до Кардана, профессора математики и физики в Милане. После усиленной просьбы со стороны Кардана, Тарталья согласился сообщить ему свою тайну, но с условием, чтобы тот хранил в глубоком секрете его открытие. Однако Кардан нарушил обещание и от своего имени опубликовал решение неполного кубического уравнения. С тех пор формула (3) стала называться формулой Кардана, несмотря на то, что её открыл Тарталья.

Формула Кардана, как видим, состоит из суммы двух кубических радикалов:

$$u=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},\quad v=\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}.$$

Каждый из таких радикалов имеет три значения. Комбинируя любое значение u с любым значением v, мы получим девять сумм $u+v$, но среди них только три будут корнями уравнения (1). Это будут те суммы $u+v$, для которых u, v связаны соотношением

$$uv=-\frac{p}{3}. \tag{4}$$

Обозначим через u_1, v_1 какую-нибудь пару значений u, v, удовлетворяющих соотношению (4), а через ε один из первообразных корней третьей степени из единицы, хотя бы, например, $\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}=\frac{-1+i\sqrt{3}}{2}$. Тогда остальные два значения u будут $u_2=\varepsilon u_1$, $u_3=\varepsilon^2 u_1$. Найдём, чему равны соответствующие значения v. Так как $\varepsilon^3=1$ и $v_1=-\frac{p}{3u_1}$, то для εu_1 и $\varepsilon^2 u_1$ находим:

$$v_2=-\frac{p}{3\varepsilon u_1}=-\frac{p\varepsilon^2}{3\varepsilon^3 u_1}=\varepsilon^2\left(-\frac{p}{3u_1}\right)=\varepsilon^2 v_1,$$

$$v_3=-\frac{p}{3\varepsilon^2 u_1}=-\frac{p\varepsilon}{3\varepsilon^3 u_1}=\varepsilon\left(-\frac{p}{3u_1}\right)=\varepsilon v_1.$$

Таким образом, складывая каждое значение u с соответствующими значениями v, получим все три корня уравнения (1):

$$y_1=u_1+v_1,\quad y_2=\varepsilon u_1+\varepsilon^2 v_1,\quad y_3=\varepsilon^2 u_1+\varepsilon v_1.$$

Здесь

$$\varepsilon=\frac{-1+i\sqrt{3}}{2},\quad \varepsilon^2=\frac{-1-i\sqrt{3}}{2}.$$

[1]) С обеих сторон было предложено 30 задач.

Поэтому окончательно имеем:

$$\left.\begin{aligned} y_1 &= u_1 + v_1, \\ y_2 &= -\frac{1}{2}(u_1 + v_1) + i\frac{\sqrt{3}}{2}(u_1 - v_1); \\ y_3 &= -\frac{1}{2}(u_1 + v_1) - i\frac{\sqrt{3}}{2}(u_1 - v_1). \end{aligned}\right\}$$

Пример. Определим по формуле Кардана корни уравнения

$$x^3 - 6x + 6 = 0.$$

Здесь $p = -6$, $q = 6$. Следовательно:

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = \sqrt[3]{-3 + \sqrt{9 - 8}} = \sqrt[3]{-3 + 1} = \sqrt[3]{-2}$$

В качестве u_1 удобнее всего взять действительное значение корня кубического из -2. Таким образом полагаем $u_1 = -\sqrt[3]{2}$. Что касается значения v_1, то

$$v_1 = -\frac{p}{3u_1} = -\frac{2}{\sqrt[3]{2}} = -\sqrt[3]{4}.$$

Отсюда по формулам (5) получаем три корня уравнения:

$$x_1 = u_1 + v_1 = -\sqrt[3]{2} - \sqrt[3]{4} \approx -2{,}843,$$

$$x_2 = -\frac{1}{2}(u_1 + v_1) + \frac{i\sqrt{3}}{2}(u_1 - v_1) \approx 1{,}422 + 0{,}327i,$$

$$x_3 = -\frac{1}{2}(u_1 + v_1) - i\frac{\sqrt{3}}{2}(u_1 - v_1) \approx 1{,}422 - 0{,}327i.$$

Рассмотрим теперь несколько детальнее уравнение

$$y^3 + py + q = 0 \qquad (6)$$

с действительными (а не комплексными, как выше) коэффициентами. Что можно сказать о корнях этого уравнения? Нам придётся разобрать три случая: а) выражение $\frac{q^2}{4} + \frac{p^3}{27}$, стоящее под знаком квадратного корня в формуле Кардана, положительно; b) $\frac{q^2}{4} + \frac{p^3}{27}$ равно нулю и c) $\frac{q^2}{4} + \frac{p^3}{27}$ отрицательно.

а) Если $\frac{q^2}{4} + \frac{p^3}{27} > 0$, то выражения

$$-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\ ;\ -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

будут действительными и притом различными числами. Мы можем за u_1 принять действительное значение корня кубического из $-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$. Тогда за v_1 придётся принять также действи-

ьное значение корня кубического из $-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$, так как произведение u_1v_1 должно равняться действительному числу $-\frac{p}{3}$. Следовательно, корень $y_1=u_1+v_1$ будет действительным. Два остальных корня

$$y_2=-\frac{1}{2}(u_1+v_1)+i\frac{\sqrt{3}}{2}(u_1-v_1),$$

$$y_3=-\frac{1}{2}(u_1+v_1)-i\frac{\sqrt{3}}{2}(u_1-v_1)$$

удут сопряжёнными комплексными числами.

Итак, в случае $\frac{q^2}{4}+\frac{p^3}{27}>0$ уравнение (6) имеет один действительный корень и два сопряжённых комплексных.

b) Если $\frac{q^2}{4}+\frac{p^3}{27}=0$, то

$$u=v=\sqrt[3]{-\frac{q}{2}}.$$

ким образом принимая за u_1 и v_1 действительное значение корня бического из $-\frac{q}{2}$, по формуле (5) получаем:

$$y_1=2u_1,\quad y_2=y_3=-u_1\ ^1).$$

Следовательно, *в случае* $\frac{q^2}{4}+\frac{p^3}{27}=0$ *три корня уравнения* (6) *ствительны, причём два из них равны.*

c) Наконец, если $\frac{q^2}{4}+\frac{p^3}{27}<0$, то подкоренные выражения кубических радикалов будут уже не действительными, а мнимыми числами. этому мнимыми будут и сами радикалы u, v. Покажем, что в формуле Кардана v должно быть сопряжено с u. Пусть $u=a+bi$. С одной стороны, модуль u равен $\sqrt{a^2+b^2}$. С другой стороны, согласно правилу извлечения корней n-й степени:

$$|u|=\left|\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}\right|=\sqrt[3]{\left|-\frac{q}{2}+i\sqrt{-\frac{q^2}{4}-\frac{p^3}{27}}\right|}=$$

$$=\sqrt[3]{\sqrt{\frac{q^2}{4}-\frac{q^2}{4}-\frac{p^3}{27}}}=\sqrt[3]{\sqrt{-\frac{p^3}{27}}}=\sqrt{-\frac{p}{3}}\ ^2).$$

---

1) Так как в данном случае $\frac{q^2}{4}=-\frac{p^3}{27}$, то $u_1=\sqrt[3]{-\frac{q}{2}}=\sqrt[3]{\frac{-\frac{q}{2}}{\sqrt{\frac{q^2}{4}}}}=\sqrt[3]{\frac{-\frac{q}{2}}{\sqrt{-\frac{p^3}{27}}}}=\frac{3q}{2p}$.

2) В силу неравенства $\frac{q^2}{4}+\frac{p^3}{27}<0$ коэффициент p должен быть отрицательным.

Теперь без труда убеждаемся, что v должно быть сопряжено с u:

$$v = -\frac{p}{3u} = -\frac{p\bar{u}}{3u\bar{u}} = -\frac{p\bar{u}}{3(a^2+b^2)} = -\frac{p\bar{u}}{3\left(-\frac{p}{3}\right)} = \bar{u}.$$

Найдём, чему равны корни уравнения в рассматриваемом случае. Если $u_1 = a + bi$ одно из значений радикала u, то по только что доказанному $v_1 = a - bi$. Поэтому

$$\left.\begin{aligned} y_1 &= u_1 + v_1 = 2a, \\ y_2 &= -\frac{1}{2}(u_1+v_1) - i\frac{\sqrt{3}}{2}(u_1 - v_1) = -a - b\sqrt{3}, \\ y_3 &= -\frac{1}{2}(u_1+v_1) - i\frac{\sqrt{3}}{2}(u_1 - v_1) = -a + b\sqrt{3}, \end{aligned}\right\} \qquad (7)$$

т. е. получились, как и следовало ожидать, действительные корни. Эти корни между собой различны. В самом деле, с помощью алгоритма Эвклида легко обнаружить, что общий наибольший делитель кубического трёхчлена $f(y) = y^3 + py + q$ и его производной $f'(y) = 3y^2 + p$ равен отрицательному постоянному числу $4 \cdot 27\left(\frac{q^2}{4} + \frac{p^3}{27}\right)$. Поэтому уравнение (6) кратных корней не имеет.

Итак, в случае $\frac{q^2}{4} + \frac{p^3}{27} < 0$ все три корня уравнения (6) действительны и между собой различны.

Для математиков XVI в. случай отрицательного $\frac{q^2}{4} + \frac{p^3}{27}$ казался парадоксальным. В то время операция извлечения квадратного корня из отрицательного числа считалась невозможной, понятие комплексного числа тогда ещё не было введено. Кардан и его современники не понимали, как могут в случае $\frac{q^2}{4} + \frac{p^3}{27} < 0$ получаться действительные корни с помощью этих невозможных операций. Все их усилия избавиться от мнимостей в формуле Кардана кончались неудачей; гораздо позднее было доказано, что этого и нельзя сделать. С тех пор случай $\frac{q^2}{4} + \frac{p^3}{27} < 0$ стал называться *неприводимым* (casus irreducibilis).

Мы сейчас покажем, что неприводимый случай тесно связан с знаменитой задачей о трисекции угла.

Для этой цели приведём формулы (7) к виду, удобному для логарифмирования.

Так как $\frac{q^2}{4} + \frac{p^3}{27} < 0$, то мы можем положить

$$\frac{q^2}{4} + \frac{p^3}{27} = -\Delta^2,$$

где Δ — положительное число. Тогда радикал u перепишется следующим образом:

$$u = \sqrt[3]{-\frac{q}{2} + i\Delta}.$$

Чтобы извлечь корень третьей степени из $-\frac{q}{2}+i\Delta$, придётся комплексное число $-\frac{q}{2}+i\Delta$ представить в тригонометрической форме. Находим его модуль r и аргумент φ:

$$r=\sqrt{\frac{q^2}{4}+\Delta^2}=\sqrt{-\frac{p^3}{27}},\quad \cos\varphi=-\frac{q}{2r},\quad \sin\varphi=\frac{\Delta}{r}.$$

Поскольку r и φ найдены, мы можем теперь приступить к извлечению корня:

$$u=\sqrt[3]{r(\cos\varphi+i\sin\varphi)}=\sqrt[3]{r}\left(\cos\frac{\varphi+2k\pi}{3}+i\sin\frac{\varphi+2k\pi}{3}\right).$$

Обращаемся к формулам (7). За u_1 проще всего принять:

$$\sqrt[3]{r}\left(\cos\frac{\varphi}{3}+i\sin\frac{\varphi}{3}\right).$$

При таком значении u_1 мы, очевидно, имеем:

$$a=\sqrt[3]{r}\cos\frac{\varphi}{3},\quad b=\sqrt[3]{r}\sin\frac{\varphi}{3},$$

откуда

$$y_1=2\sqrt[3]{r}\cos\frac{\varphi}{3},$$

$$y_2=-\sqrt[3]{r}\cos\frac{\varphi}{3}-\sqrt[3]{r}\sin\frac{\varphi}{3}\sqrt{3}=2\sqrt[3]{r}\cos\left(\frac{\varphi}{3}+\frac{2\pi}{3}\right),$$

$$y_3=-\sqrt[3]{r}\cos\frac{\varphi}{3}+\sqrt[3]{r}\sin\frac{\varphi}{3}\sqrt{3}=2\sqrt[3]{r}\cos\left(\frac{\varphi}{3}+\frac{4\pi}{3}\right).$$

Итак, мы пришли к следующим выражениям для трёх корней уравнения:

$$y_1=2\sqrt[3]{r}\cos\frac{\varphi}{3},\quad y_2=2\sqrt[3]{r}\cos\frac{\varphi+2\pi}{3},\quad y_3=2\sqrt[3]{r}\cos\frac{\varphi+4\pi}{3}. \qquad (8)$$

Из этих формул видно, что в случае неприводимости решение данного уравнения связано с делением угла φ на три равные части.

Пример. Решить уравнение

$$x^3-12x^2+24x-64=0.$$

Сперва уничтожаем член с квадратом неизвестного. Согласно общей теории надо для этого положить $x=y-\frac{12}{3}=y-4$. Подставляя в уравнение вместо x выражение $y-4$, получаем:

$$y^3-24y-32=0.$$

Здесь $\frac{q^2}{4}+\frac{p^3}{27}<0$, т. е. мы имеем дело с неприводимым случаем. Следовательно, находить корни уравнения придётся по формулам (8).

Определяем r и φ:

$$r=\sqrt{-\frac{p^3}{27}}=16\sqrt{2},$$

$$\Delta=\sqrt{-\frac{q^2}{4}-\frac{p^3}{27}}=\sqrt{-16^2+8^3}=16,$$

$$\cos\varphi=-\frac{q}{2r}=\frac{16}{16\sqrt{2}}=\frac{\sqrt{2}}{2},$$

$$\sin\varphi=\frac{\Delta}{r}=\frac{16}{16\sqrt{2}}=\frac{\sqrt{2}}{2}.$$

Стало быть, угол $\varphi=\frac{\pi}{4}$.

А теперь пишем:

$$y_1=2\sqrt[3]{r}\cos\frac{\varphi}{3}=4\sqrt{2}\cos\frac{\pi}{12},$$

$$y_2=2\sqrt[3]{r}\cos\frac{\varphi+2\pi}{3}=4\sqrt{2}\cos\frac{3\pi}{4}=-4,$$

$$y_3=2\sqrt[3]{r}\cos\frac{\varphi+4\pi}{3}=4\sqrt{2}\cos\frac{17\pi}{12}.$$

Таким образом

$$x_1=4\sqrt{2}\cos\frac{\pi}{12}-4,\ x_2=-8,$$

$$x_3=4\sqrt{2}\cos\frac{17\pi}{12}-4.$$

Остаётся подставить значения $\cos\frac{\pi}{12}$, $\cos\frac{17\pi}{12}$ и произвести соответствующие выкладки, но мы предоставляем читателю проделать это самостоятельно.

Переходим к исследованию общего уравнения

$$x^4+ax^3+bx^2+cx+d=0 \tag{9}$$

четвёртой степени. Оно было впервые решено Феррари, учеником Кардана. Его способ мы и собираемся изложить.

Перенесём три последних члена уравнения (9) в правую часть и прибавим к обеим частям $\frac{a^2x^2}{4}$. Тогда получится:

$$\left(x^2+\frac{ax}{2}\right)^2=\left(\frac{a^2}{4}-b\right)x^2-cx-d.$$

Затем прибавляем к обеим частям последнего уравнения сумму $\left(x^2+\frac{ax}{2}\right)y+\frac{y^2}{4}$. Уравнение примет вид:

$$\left(x^2+\frac{ax}{2}+\frac{y}{2}\right)^2=\left(\frac{a^2}{4}-b+y\right)x^2+\left(\frac{ay}{2}-c\right)x+\left(\frac{y^2}{4}-d\right). \tag{10}$$

Подберём вспомогательное неизвестное y так, чтобы правая часть последнего уравнения превратилась в полный квадрат. Это будет, очевидно, в том случае, когда

$$\left(\frac{a^2}{4}-b+y\right)=A^2,\quad \frac{ay}{2}-c=2AB,\quad \frac{y^2}{4}-d=B^2.$$

Но

$$4A^2B^2=(2AB)^2.$$

Поэтому должно быть:

$$4\left(\frac{a^2}{4}-b+y\right)\left(\frac{y^2}{4}-d\right)=\left(\frac{ay}{2}-c\right)^2.$$

Если раскрыть скобки, то после некоторых преобразований получится такое уравнение третьей степени относительно y:

$$y^3-by^2+(ac-4d)y-[d(a^2-4b)+c^2]=0.$$

Пусть y_0 какой-нибудь корень этого уравнения. Подставляя его в уравнение (10), мы превратим его правую часть в полный квадрат $(Ax+B)^2$:

$$\left(x^2+\frac{ax}{2}+\frac{y_0}{2}\right)^2=(Ax+B)^2.$$

Отсюда

$$x^2+\frac{ax}{2}+\frac{y_0}{2}=Ax+B,$$

или

$$x^2+\frac{ax}{2}+\frac{y_0}{2}=-Ax-B.$$

Эти два квадратных уравнения и дадут нам все четыре корня уравнения четвёртой степени.

Итак, решение уравнения четвёртой степени сводится к решению одного уравнения третьей степени и двух уравнений второй степени.

Пример. Найдём корни уравнения

$$x^4-8x^3+18x^2-27=0.$$

Здесь $a=-8$, $b=18$, $c=0$, $d=-27$. Следовательно, y должно удовлетворять уравнению

$$y^3-18y^2+108y-216=0.$$

Приводим последнее уравнение к трёхчленному виду, полагая в нём $y=z-\frac{-18}{3}=z+6$. Получаем $z^3=0$, откуда $z_1=z_2=z_3=0$, а потому $y_1=y_2=y_3=6$.

Затем находим A и B.

$$A^2=\frac{a^2}{4}-b+y=16-18+6=4,$$

$$2AB=\frac{ay}{2}-c=-24,$$

$$B^2=\frac{y^2}{4}-d=9+27=36.$$

Мы видим, что A и B имеют противоположные знаки, так как произведение $2AB$ отрицательно. Поэтому полагаем $A=2$, $B=-6$ (с таким же успехом можно было взять $A=-2$, $B=6$). Отсюда получаются такие квадратные уравнения:

$$x^2-4x+3=2x-6, \quad x^2-4x+3=-2x+6,$$

или

$$x^2-6x+9=0, \quad x^2-2x-3=0.$$

Решая первое уравнение, получаем $x_1=x_2=3$. Решая второе уравнение, получаем $x_3=-1$, $x_4=3$.

З а д а ч а. Определить корни следующих уравнений третьей и четвёртой степени.

a) $x^3+2x-1=0$, b) $x^3+3x^2-4=0$,

c) $x^3-3x^2+5x-1=0$, d) $x^4+3x^3-5x-3=0$.

Трудно себе представить, сколько безрезультатных усилий было затрачено на решение общего уравнения пятой степени. Без преувеличения можно сказать, что эта задача была вызовом человеческому разуму. В 1770—1771 гг. знаменитый французский учёный Лагранж подверг критическому пересмотру все известные до него приёмы алгебраического решения уравнений. В своём глубоком мемуаре «Réflexions sur la résolution algébrique» он выяснил, какую роль играют симметрические функции в процессе решения уравнений. Лагранж показал, что корни заданного уравнения можно с помощью симметрических функций выразить через корни некоторого вспомогательного уравнения, называемого по Лагранжу *резольвентой*. И тем не менее результаты Лагранжа оказались неутешительными. Если взять уравнения третьей и четвёртой степени, то всё обстоит благополучно: по сравнению с заданным уравнением степень резольвенты оказывается на единицу ниже. Совсем другое наблюдается, если обратиться к уравнению пятой степени; его резольвента имеет уже шестую степень. Таким образом для уравнений пятой степени способ Лагранжа перестаёт быть пригодным.

После мемуара Лагранжа перед учёными возник вопрос, достаточны ли алгебраические действия для решения уравнения выше четвёртой степени. В 1798 г. итальянский ученый Руффини попытался доказать, что *общее уравнение выше четвёртой степени не решается алгебраически*; но его рассуждения оказались неполными.

Строгое доказательство невозможности алгебраического решения уравнений выше четвёртой степени было впервые дано знаменитым норвежским математиком Абелем (1802—1829), успевшим в течение своей короткой жизни оставить глубокие исследования в различных отраслях математики.

Руффини и Абель, в сущности говоря, не дали исчерпывающего ответа на поставленный вопрос. Они доказали, что универсальной формулы решения, пригодной для всех уравнений данной степени $n(n\geqslant 5)$, не существует. Но отсюда отнюдь не следует, что любое конкретное уравнение нельзя решить с помощью алгебраических действий.

Ответ на этот вопрос был дан Эваристом Галуа (1811—1832), гениальным французским математиком. Галуа показал, что существуют такие конкретные уравнения, которые нельзя решить с помощью алгебраических действий. Вместе с тем он выяснил, от каких причин зависит возможность алгебраического решения уравнений.

Личность Галуа настолько исключительна, что мы не можем не остановиться на некоторых моментах его жизни. Дважды провалившись на вступительных экзаменах в Политехническую школу, Галуа в 1829 г. поступил в Нормальную школу, откуда был вскоре уволен (в 1830 г., после июльской революции) за выступление против директора. Галуа активно участвовал в бурной политической жизни Франции. Ярый республиканец и заклятый враг короля Людовика-Филиппа, он неоднократно арестовывался, и, наконец, погиб совсем

молодым (двадцати лет от роду) на дуэли. Глубокие идеи Галуа не были оценены по достоинству его современниками. Два мемуара, представленные им во Французскую академию наук, не только остались без ответа, но даже оказались потерянными. В настоящее время его теория играет руководящую роль в математике [1]).

ГЛАВА ДЕСЯТАЯ

ТЕОРИЯ ИСКЛЮЧЕНИЯ

§ 49. Результант. Дискриминант

Симметрические функции имеют многочисленные приложения; в частности они играют важную роль при решении системы алгебраических уравнений высших степеней со многими неизвестными. Отдел алгебры, в котором исследуются такие системы уравнений, называется *теорией исключения*.

Введём прежде всего существенное для теории исключения понятие результанта.

Рассмотрим два многочлена

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n,$$
$$g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_m. \qquad (a_0 \neq 0,\ b_0 \neq 0)$$

Пусть $\alpha_1, \ldots, \alpha_n$ корни $f(x)$, а $\beta_1, \ldots, \beta_m$ корни $g(x)$. *Результантом* многочленов $f(x)$ и $g(x)$ называется произведение

$$R(f, g) = a_0^m g(\alpha_1)\, g(\alpha_2) \ldots g(\alpha_n). \qquad (1)$$

Посмотрим, какими свойствами обладает функция $R(f, g)$. Прежде всего выясним, что произойдёт, если в функции $R(f, g)$ переставить f и g. По определению результанта, очевидно, должно получиться

$$R(g, f) = b_0^n f(\beta_1) f(\beta_2) \ldots f(\beta_m). \qquad (2)$$

Мы сейчас покажем, что *при перестановке многочленов f и g результант может только изменить знак*; точнее

$$R(g, f) = (-1)^{mn} R(f, g). \qquad (3)$$

Действительно:

$$g(\alpha_i) = b_0(\alpha_i - \beta_1)(\alpha_i - \beta_2) \ldots (\alpha_i - \beta_m),$$
$$f(\beta_i) = a_0(\beta_i - \alpha_1)(\beta_i - \alpha_2) \ldots (\beta_i - \alpha_n),$$

так как

$$g(x) = b_0(x - \beta_1)(x - \beta_2) \ldots (x - \beta_m),$$
$$f(x) = a_0(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n).$$

[1]) Изложение теории Галуа читатель может найти в книге проф. Н. Г. Чеботарёва. Теория Галуа, ч. 1.

Таким образом, подставляя эти значения $g(\alpha_i)$ и $f(\beta_i)$ в (1) и (2), будем иметь:

$$R(f, g) = a_0^m b_0^n (\alpha_1 - \beta_1)(\alpha_1 - \beta_2) \dots (\alpha_n - \beta_m) = a_0^m b_0^n \Pi (\alpha_i - \beta_j), \quad (4)$$

$$R(g, f) = a_0^m b_0^n (\beta_1 - \alpha_1)(\beta_1 - \alpha_2) \dots (\beta_m - \alpha_n) = a_0^m b_0^n \Pi (\beta_j - \alpha_i), \quad (4')$$

где Π—знак произведения.

А теперь без труда убеждаемся, что

$$R(g, f) = a_0^m b_0^n \Pi (\beta_j - \alpha_i) = (-1)^{mn} a_0^m b_0^n \Pi (\alpha_i - \beta_j) = (-1)^{mn} R(f, g).$$

Далее из равенства (4) усматриваем, что результант $R(f, g)$ есть однородный многочлен mn-й степени относительно корней $\alpha_1, \dots, \alpha_n$, $\beta_1; \dots; \beta_m$. В самом деле, произведение $\Pi (\alpha_i - \beta_j)$ состоит из mn линейных множителей $\alpha_i - \beta_j$.

Затем, из соотношения (3) вытекает, что

$$R(f; g) = a_0^m g(\alpha_2) g(\alpha_1) \dots g(\alpha_n) = (-1)^{mn} b_0^n f(\beta_1) f(\beta_2) \dots f(\beta_m). \quad (5)$$

Мы видим, что $R(f, g)$ есть симметрическая функция как корней многочлена $f(x)$, так и корней многочлена $g(x)$. Таким образом результант $R(f, g)$ можно всегда выразить (в силу основной теоремы теории симметрических функций) через коэффициенты $f(x)$ и $g(x)$. Более того, *результант $R(f, g)$ представляет собой однородный многочлен степени n относительно коэффициентов $b_0, b_1, \dots, b_m$ и однородный многочлен степени m относительно коэффициентов $a_0, a_1, \dots, a_n$.*

В самом деле, каждый из множителей

$$g(\alpha_i) = b_0 \alpha_i^m + b_1 \alpha_i^{m-1} + \dots + b_m$$

есть линейная форма коэффициентов $b_0, b_1, \dots, b_m$. Поэтому произведение $g(\alpha_1) g(\alpha_2) \dots g(\alpha_n)$, состоящее из n множителей, должно быть однородным многочленом степени n относительно $b_0, b_1, \dots, b_m$. Точно так же произведение $f(\beta_1) f(\beta_2) \dots f(\beta_m)$ должно быть однородным многочленом степени m относительно $a_0, a_1, \dots, a_n$. Отсюда в силу соотношения (5) и следует справедливость нашего утверждения.

Докажем теперь такую теорему.

Теорема. *Два многочлена $f(x)$ и $g(x)$ тогда и только тогда имеют общий корень, когда их результант $R(f, g)$ равен нулю.*

Доказательство. Если $f(x)$ и $g(x)$ имеют, например, общий корень α_i, то $g(\alpha_i) = 0$, откуда

$$R(f, g) = a_0^m g(\alpha_1) g(\alpha_2) \dots g(\alpha_i) \dots g(\alpha_n) = 0.$$

Обратно, если

$$R(f, g) = a_0^m g(\alpha_1) g(\alpha_2) \dots g(\alpha_i) \dots g(\alpha_n) = 0,$$

то должен равняться нулю по крайней мере один из сомножителей; например $g(\alpha_i) = 0$. Но тогда α_i будет общим корнем $f(x)$ и $g(x)$.

Пример 1. Определим результант двух многочленов второй степени:

$$f(x) = x^2 + a_1 x + a_2, \quad g(x) = x^2 + b_1 x + b_2.$$

Так как здесь $a_0 = b_0 = 1$, то мы получаем:

$$R(f, g) = g(\alpha_1)\, g(\alpha_2) = (\alpha_1^2 + b_1\alpha_1 + b_2)(\alpha_2^2 + b_1\alpha_2 + b_2)$$

или после перемножения

$$R(f, g) = \alpha_1^2\alpha_2^2 + b_1\alpha_1\alpha_2(\alpha_1 + \alpha_2) + b_2(\alpha_1^2 + \alpha_2^2) + \\ + b_1 b_2(\alpha_1 + \alpha_2) + b_2^2 + b_1^2\alpha_1\alpha_2.$$

Но $\alpha_1 + \alpha_2 = -a_1$, $\alpha_1\alpha_2 = a_2$; следовательно:

$$(\alpha_1 + \alpha_2)^2 = \alpha_1^2 + \alpha_2^2 + 2\alpha_1\alpha_2 = a_1^2,$$

откуда

$$\alpha_1^2 + \alpha_2^2 = a_1^2 - 2\alpha_1\alpha_2 = a_1^2 - 2a_2.$$

Таким образом, подставляя найденные значения $\alpha_1\alpha_2$, $\alpha_1 + \alpha_2$ и $\alpha_1^2 + \alpha_2^2$ в выражение $R(f, g)$, получаем:

$$R(f, g) = a_2^2 - a_1 a_2 b_1 + (a_1^2 - 2a_2) b_2 - a_1 b_1 b_2 + b_2^2 + a_2 b_1^2. \qquad (6)$$

Пример 2. Выясним, имеют ли многочлены

$$f(x) = x^2 - 3x + 2, \quad g(x) = x^2 - 5x + 6$$

общий корень. В данном случае

$$a_1 = -3, \quad a_2 = 2, \quad b_1 = -5, \quad b_2 = 6.$$

Подставляя эти значения коэффициентов в выражение (6), получаем:

$$R(f, g) = 2^2 - 3 \cdot 2 \cdot 5 + (3^2 - 2 \cdot 2) \cdot 6 - 3 \cdot 5 \cdot 6 + 6^2 + 2 \cdot 5^2 = 0.$$

Следовательно, $f(x)$ и $g(x)$ имеют по меньшей мере один общий корень. И в самом деле, их общим корнем, как легко проверить, является $x = 2$.

Пример 3. Найдём результант многочлена $f(x)$ и его производной $f'(x)$. По определению результанта

$$R(f, f') = a_0^{n-1} f'(\alpha_1) f'(\alpha_2) \ldots f'(\alpha_n) = a_0^{n-1} \prod f'(\alpha_i).$$

Вычисляем $f'(\alpha_i)$. Для этого нам придётся продифференцировать

$$f(x) = a_0 (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n).$$

Получаем:

$$f'(x) = a_0 (x - \alpha_2)(x - \alpha_3) \ldots (x - \alpha_n) + \\ + a_0 (x - \alpha_1)(x - \alpha_3) \ldots (x - \alpha_n) + \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ + a_0 (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_{n-1}).$$

Если в это выражение $f'(x)$ подставить $x=\alpha_i$, то все произведения, содержащие $x-\alpha_i$, обратятся в нуль, и мы будем иметь:

$$f'(\alpha_i)=a_0(\alpha_i-\alpha_1)(\alpha_i-\alpha_2)\ldots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\ldots(\alpha_i-\alpha_n).$$

Следовательно:

$$\begin{aligned}R(f;\ f')=a_0^{n-1}a_0^n&(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\ldots(\alpha_1-\alpha_n)\times\\&\times(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)\ldots(\alpha_2-\alpha_n)\times\\&\times(\alpha_3-\alpha_1)(\alpha_3-\alpha_2)\ldots(\alpha_3-\alpha_n)\times\\&\ldots\ldots\ldots\ldots\ldots\ldots\\&\times(\alpha_n-\alpha_1)(\alpha_n-\alpha_2)\ldots(\alpha_n-\alpha_{n-1}).\end{aligned}$$

Мы видим, что в правой части последнего равенства каждый из множителей $(\alpha_i-\alpha_j)$ $(i<j)$ встречается два раза: один раз со знаком плюс, а другой раз со знаком минус. Например, в правой части встречаются $\alpha_1-\alpha_2$ и $\alpha_2-\alpha_1=-(\alpha_1-\alpha_2)$. Так как число множителей $\alpha_i-\alpha_j$ $(i<j)$ равно $C_n^2=\frac{n(n-1)}{2}$, то мы получаем:

$$R(f,\ f')=(-1)^{\frac{n(n-1)}{2}}a_0^{2n-1}\prod_{i<j}(\alpha_i-\alpha_j)^2.$$

Выражение

$$D(f)=a_0^{2n-1}\prod_{i<j}(\alpha_i-\alpha_j)^2$$

называется *дискриминантом* многочлена $f(x)$; дискриминант отличается от результанта $R(f,\ f')$ только знаком $(-1)^{\frac{n(n-1)}{2}}$.

Из доказанной выше теоремы следует, что *многочлен $f(x)$ имеет тогда и только тогда кратные корни, когда его дискриминант равен нулю.*

Пример. В качестве иллюстрации возьмём квадратный трёхчлен $f(x)=x^2+px+q$. Его производная $f'(x)=2x+p$. Поэтому

$$R(f,\ f')=f'(\alpha_1)f'(\alpha_2)=(2\alpha_1+p)(2\alpha_2+p),$$

или

$$R(f,\ f')=4\alpha_1\alpha_2+2p(\alpha_1+\alpha_2)+p^2.$$

Но $\alpha_1\alpha_2=q$, $\alpha_1+\alpha_2=-p$. Подставляя эти значения $\alpha_1\alpha_2$ и $\alpha_1+\alpha_2$ в выражение результанта, получаем:

$$R(f,\ f')=4q-2p^2+p^2=4q-p^2.$$

Следовательно:

$$D(f)=(-1)^{\frac{2(2-1)}{2}}(4q-p^2)=p^2-4q.$$

В заключение этого параграфа введём понятие веса результанта; оно понадобится в дальнейшем.

Мы выше убедились, что результант $R(f, g)$ является однородным многочленом степени m по отношению к коэффициентам $f(x)$ и однородным многочленом степени n по отношению к коэффициентам $g(x)$. Это значит, что

$$R(f;\ g) = \sum A a_0^{\mu_0} a_1^{\mu_1} \ldots a_n^{\mu_n} b_0^{\nu_0} b_1^{\nu_1} \ldots b_m^{\nu_m}, \tag{7}$$

где

$$\mu_0 + \mu_1 + \ldots + \mu_n = m, \quad \nu_0 + \nu_1 + \ldots + \nu_m = n.$$

По формулам Виета:

$$\left.\begin{aligned}
a_1 &= -a_0(\alpha_1 + \alpha_2 + \ldots + \alpha_n),\\
a_2 &= +a_0(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
a_n &= (-1)^n a_0\alpha_1\alpha_2 \ldots a_n,\\
b_1 &= -b_0(\beta_1 + \beta_2 + \ldots + \beta_m),\\
b_2 &= +b_0(\beta_1\beta_2 + \beta_1\beta_3 + \ldots + \beta_{m-1}\beta_m);\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
b_m &= (-1)^m b_0\beta_1\beta_2 \ldots \beta_m.
\end{aligned}\right\} \tag{8}$$

Подставим в выражение результанта (7) значения коэффициентов из формул (8). Тогда результант превратится в однородный многочлен корней $\alpha_1, \alpha_2, \ldots, \alpha_n$ и $\beta_1, \beta_2, \ldots, \beta_m$. Спрашивается, чему будет равна степень этого многочлена.

Из формул (8) видно, что степень коэффициента a_k относительно корней $\alpha_1, \alpha_2, \ldots, \alpha_n$ равна его индексу k. Точно так же и степень коэффициента b_k относительно корней $\beta_1, \beta_2, \ldots, \beta_m$ равна его индексу k. Следовательно, степень каждого члена

$$A a_0^{\mu_0} a_1^{\mu_1} \ldots a_n^{\mu_n} b_0^{\nu_0} b_1^{\nu_1} \ldots b_m^{\nu_m}$$

выражения (7) относительно $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2 \ldots, \beta_m$ будет равна

$$\mu_1 + 2\mu_2 + \ldots + n\mu_n + \nu_1 + 2\nu_2 + \ldots + m\nu_m. \tag{9}$$

Выражение (9) называется *весом результанта*.

С другой стороны, мы знаем, что результант есть однородный многочлен mn-й степени относительно корней α_i и β_i. Таким образом можно высказать следующее предложение: *вес результанта* $R(f, g)$ равен произведению mn степеней многочленов $f(x)$ и $g(x)$.

§ 50. Результант в форме определителя

В настоящем параграфе мы укажем один практический приём вычисления результанта.

Рассмотрим наряду с многочленами

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n, \quad g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_m$$

выражения $xg(x), x^2g(x), \ldots, x^{n-1}g(x)$. Пусть $\alpha_1, \alpha_2, \ldots, \alpha_n$ корни многочлена $f(x)$. Нетрудно показать, что каждую из величин

$x_i^k g(x_i)$ $(k = 0, 1, \ldots, n-1)$ можно представить в виде многочлена не выше $(n-1)$-й степени относительно x_i.

В самом деле; разделим $x^k g(x)$ на $f(x)$. Пусть $q(x)$ частное, а

$$a_{k,0} + a_{k,1}x + \ldots + a_{k,\,n-1}x^{n-1}$$

остаток. Тогда мы будем иметь:

$$x^k g(x) = f(x)\,q(x) + (a_{k,0} + a_{k,1}x + \ldots + a_{k,\,n-1}x^{n-1}),$$

откуда, подставляя в это равенство $x = x_i$, получаем:

$$x_i^k g(x_i) = a_{k,0} + a_{k,1}x_i + \ldots + a_{k,\,n-1}x_i^{n-1} \qquad (1)$$
$$(k = 0,\ 1,\ 2,\ \ldots,\ n-1).$$

Теперь докажем; что

$$R(f,\ g) = a_0^m \begin{vmatrix} a_{0,0} & a_{0,1} \ldots & a_{0,\,n-1} \\ a_{1,0} & a_{1,1} \ldots & a_{1,\,n-1} \\ \ldots\ldots\ldots & \ldots\ldots & \ldots\ldots \\ a_{n-1,\,0} & a_{n-1,\,1} \ldots & a_{n-1,\,n-1} \end{vmatrix}.$$

Доказательство. Перепишем равенства (1) следующим образом:

$$a_{k,0} + a_{k,1}x_i + \ldots + [a_{k,k} - g(x_i)]\,x_i^k + \ldots + a_{k,\,n-1}x_i^{n-1} = 0$$
$$(k = 0,\ 1,\ \ldots,\ n-1).$$

Мы видим, что однородная система n уравнений с n неизвестными

$$a_{k,0}x_0 + a_{k,1}x_1 + \ldots + [a_{k,k} - g(x_i)]\,x_k + \ldots + a_{k,\,n-1}x_{n-1} = 0$$
$$(k = 0,\ 1,\ 2,\ \ldots,\ n-1)$$

допускает ненулевое решение

$$x_0 = 1,\ x_1 = x_i \ldots,\ x_k = x_i^k,\ \ldots,\ x_{n-1} = x_i^{n-1}.$$

Значит, определитель D системы должен равняться нулю:

$$D = \begin{vmatrix} a_{0,0} - g(x_i) & a_{0,1} \ldots & a_{0,\,n-1} \\ a_{1,0} & a_{1,1} - g(x_i) \ldots & a_{1,\,n-1} \\ \ldots\ldots\ldots & \ldots\ldots\ldots & \ldots\ldots\ldots \\ a_{n-1,\,0} & a_{n-1,\,1} \ldots & a_{n-1,\,n-1} - g(x_i) \end{vmatrix} = 0. \qquad (2)$$

Обращаемся к вспомогательному определителю:

$$F(z) = (-1)^n \begin{vmatrix} a_{0,0} - z & a_{0,1} \ldots & a_{0,\,n-1} \\ a_{1,0} & a_{1,1} - z \ldots & a_{1,\,n-1} \\ \ldots\ldots\ldots & \ldots\ldots\ldots & \ldots\ldots\ldots \\ a_{n-1,\,0} & a_{n-1,\,1} \ldots & a_{n-1,\,n-1} - z \end{vmatrix}.$$

Определитель $F(z)$, очевидно, есть многочлен n-й степени относительно z со старшим коэффициентом, равным единице. Легко

сообразить, что корнями многочлена $F(z)$ являются величины $g(\alpha_1), g(\alpha_2), \ldots, g(\alpha_n)$; это видно из равенства (2). С другой стороны, известно; что свободный член многочлена n-й степени; у которого старший коэффициент есть единица, равен произведению корней, взятому со знаком $(-1)^n$. Но свободный член многочлена $F(z)$ равен $F(0)$; следовательно:

$$F(0) = (-1)^n \begin{vmatrix} a_{0,0} & a_{0,1} \ldots & a_{0,\,n-1} \\ a_{1,0} & a_{1,1} \ldots & a_{1,\,n-1} \\ \ldots & \ldots & \ldots \\ a_{n-1,\,0} & a_{n-1,1} \ldots & a_{n-1,\,n-1} \end{vmatrix} =$$
$$= (-1)^n g(\alpha_1) g(\alpha_2) \ldots g(\alpha_n),$$

откуда

$$R(f, g) = a_0^m g(\alpha_1) g(\alpha_2) \ldots g(\alpha_n) = a_0^m \begin{vmatrix} a_{0,0} & a_{0,1} & \ldots a_{0,\,n-1} \\ a_{1,0} & a_{1,1} & \ldots a_{1,\,n-1} \\ \ldots & \ldots & \ldots \\ a_{n-1,\,0} & a_{n-1,1} & \ldots a_{n-1,\,n-1} \end{vmatrix}$$

и наше утверждение доказано.

Пример 1. Найдём результант многочленов

$$f(x) = x^2 - x + 1, \quad g(x) = x^4 - 2x^2 + 3.$$

Для этой цели делим $g(x)$ и $xg(x)$ на $f(x)$. Обозначив остатки соответственно через $r_1(x)$ и $r_2(x)$, будем иметь:

$$r_1(x) = 5 - 3x,$$
$$r_2(x) = 3 + 2x.$$

Итак, результант

$$R(f, g) = \begin{vmatrix} 5 & -3 \\ 3 & 2 \end{vmatrix} = 19.$$

Пример 2. Составим теперь результант для

$$f(x) = x^2 + a_1 x + a_2, \quad g(x) = x^2 + b_1 x + b_2.$$

Легко видеть, что при делении $g(x)$ и $xg(x)$ на $f(x)$ получаются остатки:

$$r_1(x) = (b_2 - a_2) + (b_1 - a_1) x,$$
$$r_2(x) = -a_2 (b_1 - a_1) + [(b_2 - a_2) - a_1 (b_1 - a_1)] x.$$

Поэтому

$$R(f, g) = \begin{vmatrix} b_2 - a_2 & b_1 - a_1 \\ -a_2 (b_1 - a_1) & (b_2 - a_2) - a_1 (b_1 - a_1) \end{vmatrix} =$$
$$= (b_2 - a_2)^2 - (a_1 b_2 - a_2 b_1) \cdot (b_1 - a_1).$$

Задача. Вычислить результант следующих многочленов:

a) $f(x) = x^2 - 3x + 1, \quad g(x) = x^5 - x^4 + x^3 - 1,$

b) $f(x) = x^3 - x^2 + 5x - 2, \quad g(x) = x^5 - 2x^3 + x^2 - x + 5.$

51. Исключение неизвестных

Мы вплотную подошли к главной задаче теории исключения — к решению уравнений высших степеней со многим неизвестными.

Мы ограничимся случаем двух уравнений с двумя неизвестными:

$$f(x,\ y)=0,\ g(x,\ y)=0. \tag{1}$$

Обозначим степень первого уравнения относительно x, y через n, а степень второго через m. Тогда, располагая многочлены $f(x, y)$ и $g(x, y)$ по степеням x, получим

$$\left.\begin{aligned} f(x,\ y) &= a_0x^n+a_1x^{n-1}+\ldots+a_n=0,\\ g(x,\ y) &= b_0x^m+b_1x^{m-1}+\ldots+b_m=0. \end{aligned}\right\} \tag{2}$$

Следует заметить, что коэффициенты $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m$ являются многочленами относительно y; при этом степень коэффициента a_i относительно y не может быть больше индекса i, так как степень многочлена $f(x, y)$ равна n; то же самое можно сказать и относительно коэффициента b_i.

Допустим теперь, что система уравнений (1) удовлетворяется значениями $x=x_0$, $y=y_0$. Что это по существу означает? Это означает, что уравнения (2) имеют общий корень $x=x_0$. Мы знаем, что в таком случае результант $R(f, g)$ должен равняться нулю. Но

$$R(f,\ g)=0 \tag{3}$$

есть уравнение относительно одного лишь y. Мы свели, таким образом, решение системы (1) двух уравнений с двумя неизвестными к решению уравнения (3) с одним неизвестным, а такие уравнения мы решать умеем[1]). Подставляя найденные значения y в одно из уравнений (1), получим соответствующие значения x. Остаётся установить, чему равна степень уравнения (3). Результант $R(f, g)$, как известно, представляет собой многочлен от коэффициентов a_0, $a_1, \ldots, a_n$, b_0, $b_1, \ldots b_m$. Поэтому мы можем написать:

$$R(f,\ g)=\sum Aa_0^{\mu_0}a_1^{\mu_1}\ldots a_n^{\mu_n}b_0^{\nu_0}b_1^{\nu_1}\ldots b_m^{\nu_m}.$$

Так как степень каждого коэффициента a_i, b_i относительно y не превосходит индекса i, то степень каждого члена суммы (4) не превосходит

$$\mu_1+2\mu_2+\ldots+n\mu_n+\nu_1+2\nu_2+\ldots+m\nu_m.$$

Но последнее выражение есть не что иное, как вес результанта, а мы в своё время установили, что этот вес равен mn (см. конец § 49).

Итак, *степень уравнения* (3) *не превосходит произведения* mn *степеней данных уравнений.*

Пример. Исключим неизвестное y из уравнений:

$$f(x,\ y)=2x^2-3xy+y^2+4x-5=0,$$
$$g(x,\ y)=-x^2+y^2-2x-3y-1=0.$$

[1]) Например, корни $R(f, g)=0$ можно вычислить приближённо.

Располагаем уравнения по степеням y:

$$f(x, y) = y^2 - 3xy + (2x^2 + 4x - 5) = 0,$$
$$g(x, y) = y^2 - 3y - (x^2 + 2x + 1) = 0.$$

Мы видим, что здесь:

$$a_0 = 1, \quad a_1 = -3x, \quad a_2 = 2x^2 + 4x - 5,$$
$$b_0 = 1, \quad b_1 = -3, \quad b_2 = -(x^2 + 2x + 1).$$

В § 50 было найдено, что результант многочленов

$$f(x) = x^2 + a_1 x + a_2 \quad g(x) = x^2 + b_1 x + b_2$$

равен

$$R(f, g) = (b_2 - a_2)^2 - (a_1 b_2 - a_2 b_1)(b_1 - a_1).$$

Следовательно, подставляя сюда значения коэффициентов, получим после некоторых алгебраических преобразований уравнение

$$9x^3 + 3x^2 + 42x - 29 = 0.$$

Степень этого уравнения, как и следовало ожидать, оказалась меньше $2 \cdot 2 = 4$.

Задача. Исключить x из уравнений.

а) $x^2 + 5xy - y^2 + 3 = 0, \quad 3x^2 - xy + 3y^2 - x + y - 2 = 0.$

b) $x^3 - 5y^2 + 2 = 0, \quad 2x^2 - y^2 + 7 = 0.$

§ 52. Преобразование Чирнгаузена

В некоторых случаях можно значительно упростить решение алгебраического уравнения, если воспользоваться следующим преобразованием, впервые предложенным Чирнгаузеном.

Пусть

$$f(x) = x^n - p_1 x^{n-1} + \ldots + (-1)^n p_n = 0 \qquad (1)$$

есть некоторое неприводимое уравнение в поле P со старшим коэффициентом, равным единице [1]). При этом под P будет всё время подразумеваться такое поле, которое является либо частью поля комплексных чисел, либо совпадает с полем комплексных чисел.

Преобразование Чирнгаузена заключается в том, чтобы составить новое уравнение

$$y^n - q_1 y^{n-1} + \ldots + (-1)^n q_n = 0, \qquad (2)$$

корни которого y_i связаны с корнями x_i первоначального уравнения заданным рациональным соотношением $y_i = \varphi(x_i)$, где $\varphi(x_i) = \frac{g(x_i)}{h(x_i)}$, $g(x)$ и $h(x)$ многочлены в поле P и $h(x_i) \neq 0$.

[1]) Если бы уравнение (1) было приводимо, то мы рассматривали бы уравнение $g(x) = 0$, где $g(x)$ — любой из неприводимых множителей многочлена $f(x)$.

Мы здесь воспроизведём весьма изящное решение этой задачи, принадлежащее Эрмиту. Но прежде всего покажем, что $\varphi(x)$ можно всегда предполагать целой рациональной функцией в поле P степени не выше $n-1$.

Легко видеть, что $h(x)$ взаимно просто с $f(x)$. Действительно, если бы многочлены $h(x)$ и $f(x)$ не были взаимно простыми, то в силу неприводимости $f(x)$ многочлен $h(x)$ делился бы на $f(x)$: $h(x)=f(x)\,q(x)$. Полагая в последнем равенстве $x=x_i$, получаем $h(x_i)=f(x_i)\,q(x_i)=0$, что невозможно. Но если многочлены $h(x)$ и $f(x)$ взаимно просты, то в поле P можно подобрать такие новые многочлены $u(x)$ и $v(x)$, чтобы

$$h(x)\,u(x)+f(x)\,v(x)=1.$$

Полагая в этом равенстве $x=x_i$, получаем:

$$h(x_i)\,u(x_i)=1.$$

Отсюда, умножая числитель и знаменатель дроби $\frac{g(x_i)}{h(x_i)}$ на $u(x_i)$, имеем, что $y_i=g(x_i)\,u(x_i)$. Разделим, наконец, $g(x)\,u(x)$ на $f(x)$. Пусть в частном у нас получается $q(x)$, а в остатке $r(x)=c_0+c_1x+\ldots+c_{n-1}x^{n-1}$. Тогда мы можем написать, что $g(x)\,u(x)=f(x)\,q(x)+r(x)$, откуда, полагая $x=x_i$, находим, что $y_i=r(x_i)$.

Итак, мы видим, что рациональную функцию $\varphi(x)$ можно заменить целой рациональной функцией $r(x)$, причём степень $r(x)$ не превосходит $n-1$.

Теперь приступим к непосредственному изложению метода Эрмита.

Пусть

$$y_i=c_0+c_1x_i+\ldots+c_{n-1}x_i^{n-1}. \tag{3}$$

Умножая обе части равенства (3) на x_i, получаем:

$$x_iy_i=c_0x_i+c_1x_i^2+\ldots+c_{n-1}x_i^n.$$

На основании уравнения (1) мы можем x_i^n заменить через $p_1x_i^{n-1}-\ldots-(-1)^np_n$. После такой замены у нас получится

$$x_iy_i=c_0'+c_1'x_i+\ldots+c_{n-1}'x_i^{n-1}, \tag{4}$$

где $c_0'=c_{n-1}p_n$, $c_1'=c_0+c_{n-1}p_{n-1}$, $\ldots$ В свою очередь, умножая обе части уравнения (4) на x_i и заменяя x_i^n через $p_1x_i^{n-1}-\ldots-(-1)^np_n$, получим

$$x_i^2y_i=c_0''+c_1''x_i+\ldots+c_{n-1}''x_i^{n-1}.$$

Обе части этого уравнения опять умножаем на x_i и т. д.; этот процесс продолжаем до тех пор, пока у нас не получится система равенств

$$x_i^ky_i=c_0^{(k)}+c_1^{(k)}x_i+\ldots+c_{n-1}^{(k)}x_i^{n-1}\ (k=0,\ 1,\ \ldots,\ n-1). \tag{5}$$

Перепишем равенства (5) следующим образом:

$$c_0^{(k)}+c_1^{(k}x_i+\ldots+[c_k^{(k)}-y_i]\,x_i^k+\ldots+c_{n-1}^{(k)}x_i^{n-1}=0.$$

Мы видим, что однородная система n уравнений

$$c_0^{(k)}z_0 + c_1^{(k)}z_1 + \ldots + [c_k^{(k)} - y_i]\,z_k + \ldots + c_{n-1}^{(k)}z_{n-1} = 0$$

с n неизвестными $z_0, \ldots, z_{n-1}$ допускает ненулевое решение $z_0 = 1$, $z_1 = c_i, \ldots, z_{n-1} = x_i^{n-1}$. Значит, определитель системы должен равняться нулю:

$$\begin{vmatrix} c_0 - y & c_1 \ldots & c_{n-1} \\ c_0' & c_1' - y \ldots & c_{n-1}' \\ \ldots\ldots\ldots\ldots & & \\ c_0^{(n-1)} & c_1^{(n-1)} \ldots & c_{n-1}^{(n-1)} - y \end{vmatrix} = 0.$$

Это и есть искомое преобразованное уравнение (2).

Пример. Применить преобразование Чирнгаузена $y_i = 1 - x_i + x_i^2$ к уравнению $x^3 - 2x + 2 = 0$.

Применяя метод Эрмита, получим:

$$y = 1 - x + x^2,$$
$$xy = x - x^2 + x^3 = x - x^2 + (2x - 2) = -2 + 3x - x^2,$$
$$x^2y = -2x + 3x^2 - x^3 = -2x + 3x^2 - (2x - 2) = 2 - 4x + 3x^2$$

$$\begin{aligned} (1 - y) - x + x^2 &= 0, \\ -2 + (3 - y)\,x - x^2 &= 0, \\ 2 - 4x + (3 - y)\,x^2 &= 0. \end{aligned}$$

Отсюда следует, что

$$\begin{vmatrix} 1 - y & -1 & 1 \\ -2 & 3 - y & -1 \\ 2 & -4 & 3 - y \end{vmatrix} = 0.$$

Для окончательного решения задачи остаётся раскрыть определитель, что это мы предоставляем проделать читателю самостоятельно.

Коэффициенты q_i уравнения (2) являются элементарными симметрическими функциями корней $y_1 = \varphi(x_1), \ldots, y_n = \varphi(x_n)$, а потому и коэффициенты будут также симметрическими функциями от корней $x_1, \ldots, x_n$ первоначального уравнения (1). Согласно основной теореме теории симметрических функций отсюда следует, что коэффициенты q_j должны выражаться через коэффициенты p_i первоначального уравнения (1), и мы могли бы найти выражения q_i через p_i, пользуясь известными способами вычисления симметрических функций.

Чирнгаузен применял своё преобразование для решения алгебраических уравнений. Он подбирал функцию $\varphi(x)$ так, чтобы в преобразованном уравнении уничтожалось возможно большее число коэффициентов q_i. Этим способом можно, в частности, решить уравнения 3-й и 4-й степени.

ГЛАВА ОДИННАДЦАТАЯ

ПОСТРОЕНИЯ С ПОМОЩЬЮ ЦИРКУЛЯ И ЛИНЕЙКИ [1])

§ 53. Постановка проблемы

Всякую геометрическую задачу на построение можно, как известно, реш чисто алгебраически, т. е. можно свести к отысканию корней некоторого а браического уравнения $f(x) = 0$. Например, знаменитая задача об удвое куба тесно связана с извлечением корня третьей степени из двойки.

Посмотрим, при каком условии корни алгебраического уравне

$$f(x) = 0$$

с рациональными коэффициентами можно построить с помощью цирку линейки.

Чтобы ответить на этот вопрос, обратимся к теореме.

Теорема. *Выражение u тогда и только тогда может быть постр с помощью циркуля и линейки, когда оно получается в результате решения уравнений не выше второй степени.*

Доказательство. Пусть рассматриваемое выражение u можно построить с помощью циркуля и линейки. Покажем, что в таком случае u можно получить, решая уравнения не выше второй степени. Возьмём на плоскости прямоугольную систему координат XOY. Каждое построение циркулем и линейкой сводится к проведению прямых, окружностей и к нахождению точек пересечения этих линий.

Чтобы найти точку пересечения двух прямых

$$\left.\begin{aligned} A_1x + B_1y + C_1 &= 0, \\ A_2x + B_2y + C_2 &= 0, \end{aligned}\right\} \tag{2}$$

надо, очевидно, решить систему уравнений (2), в результате чего получится уравнение первой степени относительно x (или y).

Чтобы найти точки пересечения прямой

$$Ax + By + C = 0 \tag{3}$$

и окружности

$$(x-a)^2 + (y-b)^2 = r^2, \tag{4}$$

придётся совместно решать уравнения (3) и (4). Мы получим тогда квадратное уравнение относительно x (или y).

Наконец, чтобы найти точки пересечения двух окружностей

$$\left.\begin{aligned} (x-a_1)^2 + (y-b_1)^2 &= r_1^2, \\ (x-a_2)^2 + (y-b_2)^2 &= r_2^2, \end{aligned}\right\} \tag{5}$$

придётся решать систему уравнений (5). Нетрудно убедиться, что для неизвестного x (или y) в результате получится квадратное уравнение.

Итак, u, действительно, можно получить путём решения уравнений не выше второй степени.

Теперь докажем справедливость обратного утверждения. Решение уравнений не выше второй степени с заданными коэффициентами сводится к следующим действиям над комплексными числами: сложению, вычитанию, умножению, делению и извлечению квадратного корня.

Чтобы сложить или вычесть два ком ных числа $z_1 = a_1 + b_1 i$ и $z_2 = a_2 + b_2 i$, надо, как известно, слож вычесть их действительные и мнимые части: $z_1 \pm z_2 = (a_1 \pm a$ Но выражения $a_1 \pm a_2$ и $b_1 \pm b_2$ с помощью циркуля и ли о построить.

Обращаемся к умножению. Что ва комплексных числа $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$ и $z_2 = r_2(\cos$ сложить аргументы и перемножить модули:

$$z_1 z_2 = r_1 r_2 [\cos(\varphi_1 +$$

[1]) Эта глава выходит за пределы уч раммы.

Но выражения $\varphi_1 + \varphi_2$ и $r_1 r_2$ можно без особого труда построить с помощью циркуля и линейки.

То же самое можно сказать и относительно деления:

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}[\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)],$$

а выражения $\frac{r_1}{r_2}$ и $\varphi_1 - \varphi_2$ с помощью циркуля и линейки построить, конечно, можно.

Рассмотрим, наконец, операцию извлечения корня квадратного из комплексного числа $z = r(\cos\varphi + i\sin\varphi)$. Чтобы определить

$$\sqrt{r(\cos\varphi + i\sin\varphi)},$$

надо угол φ разделить пополам и извлечь корень квадратный из модуля r. Но выражения $\frac{\varphi}{2}$ и $\sqrt{r}$ также можно построить с помощью циркуля и линейки. Теорема доказана полностью.

Таким образом, для того чтобы корни уравнения (1) получались построением посредством циркуля и линейки, необходимо и достаточно, чтобы это уравнение приводилось к уравнениям не выше второй степени.

Возникает вопрос, не существует ли критерия, позволяющего судить, будет ли данное уравнение приводиться к уравнениям не выше второй степени или нет? На этот вопрос мы ответим не сразу, нам прежде всего придётся познакомиться с так называемыми конечными расширениями.

§ 54. Конечные расширения

Прежде всего введём несколько необходимых понятий. Пусть Δ и Ω два поля, причём пусть поле Δ является частью [1]) поля Ω. Мы будем в таком случае говорить, что поле Ω есть *делитель* или *расширение* поля Δ: само поле Δ мы будем называть *подполем* поля Ω. Кроме того мы часто будем пользоваться следующим обозначением: $\Delta \subset \Omega$, выражающим, что Δ есть подполе поля Ω. На протяжении этой главы мы будем иметь дело только с такими полями, которы) являются либо частью поля комплексных чисел, либо самим этим полем [2]).

Для дальнейшего мы должны познакомиться с важным понятием линейной зависимости относительно Δ. Введём такое определение:

Определение. *Величины $u_1, u_2, \ldots, u_m$ расширения Ω поля Δ называются линейно зависимыми относительно Δ, если можно в Δ подыскать такие числа $c_1, c_2, \ldots, c_m$, не все равные нулю, чтобы*

$$c_1 u_1 + c_2 u_2 + \ldots + c_m u_m = 0. \qquad (1)$$

В противном случае величины $u_1, u_2, \ldots, u_m$ называются линейно независимыми относительно Δ (сравните с определением на стр. 62).

В равенстве (1) не все числа c_i равны нулю. Пусть, например, $c_1 \neq 0$, тогда u_1 можно будет выразить через остальные u_i: $u_1 = d_2 u_2 + \ldots + d_m u_m$. (Числа $d_i = -\frac{c_i}{c_1}$, очевидно, лежат в поле Δ.) В этом случае мы скажем, что u_1 *линейно зависит* от $u_2, \ldots, u_m$ (относительно Δ).

Мы вплотную подошли к понятию *конечного расширения*. Расширение Ω поля Δ называется *конечным*, если в Ω существует конечное множество элементов $u_1, \ldots, u_m$, от которых линейно зависит любой элемент u поля Ω:

$$u = c_1 u_1 + \ldots + c_m u_m \quad (c_i\text{—элементы } \Delta).$$

---

[1]) Т. е. все элементы Δ являются также элементами Ω и существует по меньшей мере один элемент Ω, не принадлежащий Δ.

[2]) Например Δ может быть полем рациональных чисел, а Ω—полем действительных чисел.

Совокупность элементов $u_1, \ldots, u_m$ мы будем называть *базисом* конечного расширения Ω и обозначать через $(u_1, \ldots, u_m)$; при этом базис, состоящий из линейно независимых (относительно Δ) элементов, будет называться *линейно независимым*.

Очевидно, что всякий базис $(u_1, \ldots, u_m)$ конечного расширения Ω можно сделать линейно независимым; для этого достаточно из $(u_1, \ldots, u_m)$ удалить все линейно зависимые элементы. Условимся называть число элементов линейно независимого базиса *степенью Ω относительно Δ*; мы её будем обозначать символом $(\Omega : \Delta)$.

Основные свойства конечных расширений, к изучению которых мы сейчас приступаем, легко получаются из знакомой нам теоремы Штейница (см. § 18). Дело в том, что эта теорема вместе со своими двумя следствиями оказывается справедливой не только для модуля линейных форм, но и для конечного расширения. Мы ограничимся только формулировками, так как рассуждения остаются дословно теми же.

Теорема Штейница. *Если $v_1, v_2, \ldots, v_s$ линейно независимые элементы конечного расширения Ω поля Δ и $(u_1, u_2, \ldots, u_m)$ базис Ω, то $s \leqslant m$ и базис $(u_1, \ldots, u_m)$ при $s < m$ может быть заменён новым базисом $(v_1, v_2, \ldots, v_s, u_{s+1}, \ldots, u_m)$, а при $s = m$ — новым базисом $(v_1, \ldots, v_m)$* [1].

Следствие 1. *Число s линейно независимых элементов не может быть больше степени $(\Omega : \Delta)$.*

Следствие 2. *Степень $(\Omega : \Delta)$ не зависит от выбора базиса.*

К этим следствиям можно добавить ещё несколько следствий. Приводим их.

Следствие 3. *Если $(\Omega : \Delta) = n$ то всякая система $n + 1$ элементов конечного расширения Ω линейно зависима.*

В самом деле, если бы $n + 1$ элементов были линейно независимы, то мы получили бы противоречие со следствием 1.

Следствие 4. *Если $(\Omega : \Delta) = n$, то каждый элемент u конечного расширения есть корень многочлена не выше n-й степени в поле Δ.*

Действительно, в силу предыдущего следствия 1, $u, u^2, \ldots, u^n$ должны быть линейно зависимыми, т. е.

$$a_0 u^n + a_1 u^{n-1} + \ldots + a_n = 0,$$

где a_i—элементы поля Δ.

Основную роль во всём дальнейшем изложении будут играть следующие две теоремы.

Теорема 1. *Если Ω_1—конечное расширение поля Δ, Ω_2—конечное расширение Ω_1, то Ω_2 есть конечное расширение Δ и*

$$(\Omega_2 : \Delta) = (\Omega_1 : \Delta) \cdot (\Omega_2 : \Omega_1).$$

Доказательство. Обозначим линейно независимый базис Ω_1 относительно Δ через $(u_1, u_2, \ldots, u_m)$, а линейно независимый базис Ω_2 относительно Ω_1 обозначим через $(v_1, v_2, \ldots, v_n)$. Любой элемент u поля Ω_2 должен линейно зависеть от $(v_1, v_2, \ldots, v_n)$:

$$u = \sum_{i=1}^{n} s_i v_i, \tag{2}$$

где s_i—элементы поля Ω_1. Но в свою очередь

$$s_i = \sum_{j=1}^{m} c_{ji} u_j,$$

где c_{ji}—элементы поля Δ. Подставляя эти значения s_i в равенство (2), получаем

$$u = \sum_{i=1}^{n} \sum_{j=1}^{m} (u_j v_i) c_{ji}.$$

[1]) В частности s может равняться единице.

Таким образом система mn элементов $u_1v_1, u_1v_2, \ldots, u_mv_n$ образует базис Ω_2 относительно Δ, т. е. мы показали, что Ω_2 есть конечное расширение Δ. Остаётся показать, что базис $(u_1v_1, u_1v_2, \ldots, u_mv_n)$ расширения Ω_2 линейно независим.

Пусть

$$\sum_{i=1}^{n}\sum_{j=1}^{m}(u_jv_i)\,c_{ji}=0.$$

Посмотрим, чему будут равны c_{ji}. Общий множитель v_i можно, очевидно, вынести за знак внутренней суммы. Мы получаем:

$$\sum_{i=1}^{n}s_iv_i=0, \tag{3}$$

где s_i—элементы Ω_1:

$$s_i=\sum_{j=1}^{m}c_{ji}u_j.$$

Но элементы $v_1, v_2, \ldots, v_n$ линейно независимы относительно Ω_1. Следовательно, в сумме (3) все s_i должны равняться нулю, иными словами

$$\sum_{j=1}^{m}c_{ji}u_j=0.$$

В свою очередь элементы $u_1, \ldots, u_m$ линейно независимы относительно Δ; отсюда следует, что все c_{ji} равны нулю, т. е. базис $(u_1v_1, \ldots, u_mv_n)$ конечного расширения Ω_2 поля Δ линейно независим (относительно Δ). Поэтому $(\Omega_2 : \Delta)=mn=(\Omega_1 : \Delta)\,(\Omega_2 : \Omega_1)$.

Теорема 2. *Пусть Ω конечное расширение поля Δ. Тогда всякое расширение Σ поля Δ, содержащееся в Ω, будет конечным расширением Δ. Степень $(\Sigma : \Delta)$ будет при этом делителем степени $(\Omega : \Delta)$.*

Доказательство. Возьмём из поля Σ максимальное число линейно независимых элементов $u_1, u_2, \ldots, u_m$. Такая система элементов в силу следствия 3 теоремы Штейница должна обязательно существовать. Обозначим через n степень конечного расширения Ω относительно Δ. В силу того же следствия 3 $m \leqslant n$. Мы утверждаем, что элементы $u_1, u_2, \ldots, u_m$ образуют базис Σ относительно Δ. В самом деле, если u произвольный элемент Σ, то $u, u_1, \ldots, u_m$ будут уже линейно зависимы; это следует из того, что m есть максимальное число линейно независимых элементов поля Σ. Таким образом,

$$cu+c_1u_1+\ldots+c_mu_m=0,$$

где c и c_i—элементы Δ. Элемент c не может равняться нулю, так как в противном случае $u_1, u_2, \ldots, u_m$ были бы линейно зависимы. Следовательно, u можно линейно выразить через $u_1, u_2, \ldots, u_m$, т. е. элементы $u_1, u_2, \ldots, u_m$ образуют базис Σ относительно Δ. Мы доказали, что Σ есть конечное расширение поля Δ.

Остаётся показать, что $(\Sigma : \Delta)$ делит $(\Omega : \Delta)$. Рассуждаем следующим образом. Поле Ω можно, очевидно, рассматривать как конечное расширение Σ. В самом деле, если $(v_1, v_2, \ldots, v_n)$ базис Ω относительно Δ, то $(v_1, \ldots, v_n)$ и подавно будет базисом Ω относительно Σ. Итак, Σ есть конечное расширение Δ, а Ω—конечное расширение Σ. Мы можем, следовательно, прибегнуть к теореме 1. По этой теореме

$$(\Omega : \Delta)=(\Omega : \Sigma)\,(\Sigma : \Delta),$$

т. е. $(\Omega : \Delta)$ делится на $(\Sigma : \Delta)$.

Теперь рассмотрим несколько примеров конечных расширений.

1. Пусть

$$F(x)=A_0x^n+A_1x^{n-1}+\ldots+A_n$$

неприводимый многочлен n-й степени в поле Δ. Обозначим один из корней многочлена $F(x)$ буквой j и рассмотрим множество P всевозможных выражений вида

$$g(j) = a_0 j^{n-1} + a_1 j^{n-2} + \ldots + a_{n-1}, \qquad (4)$$

a_i—элементы поля Δ. Мы сейчас увидим, что множество P есть не что иное, как алгебраическое расширение Δ (см. § 43).

Посмотрим, по каким правилам выражения (4) можно сравнивать, складывать и перемножать.

Пусть

$$a_0 j^{n-1} + a_1 j^{n-2} + \ldots + a_{n-1} = b_0 j^{n-1} + b_1 j^{n-2} + \ldots + b_{n-1}.$$

Перенесём все члены в левую часть равенства. Получим:

$$(a_0 - b_0) j^{n-1} + (a_1 - b_1) j^{n-2} + \ldots + (a_{n-1} - b_{n-1}) = 0.$$

В этом уравнении все коэффициенты должны равняться нулю, так как j— корень неприводимого многочлена n-й степени. Значит

$$a_0 = b_0, \quad a_1 = b_1, \ \ldots, \ a_{n-1} = b_{n-1}.$$

Итак, выражения (4) сравниваются так же, как элементы алгебраического расширения $\Delta(j)$.

То же самое можно сказать относительно операции сложения: если

$$g(j) = a_0 j^{n-1} + a_1 j^{n-2} + \ldots + a_{n-1},$$
$$h(j) = b_0 j^{n-1} + b_1 j^{n-2} + \ldots + b_{n-1},$$

то, очевидно,

$$g(j) + h(j) = (a_0 + b_0) j^{n-1} + (a_1 + b_1) j^{n-2} + \ldots + (a_{n-1} + b_{n-1}).$$

Переходим, наконец, к умножению. Обозначим произведение двух выражений $g(j)$ и $h(j)$ через $f(j)$. Разделим многочлен $f(x)$ на многочлен $F(x)$. Если $q(x)$—частное и $r(x)$—остаток, то

$$f(x) = F(x)\, q(x) + r(x).$$

В этом тождестве положим $x = j$. Тогда $F(x)$ обратится в нуль, и мы получим $f(j) = r(j)$.

Итак, $P = \Delta(j)$. Отсюда сразу следует, что P образует конечное расширение n-й степени поля Δ, а именно, конечное расширение с линейно независимым базисом $(1, j, j^2, \ldots, j^{n-1})$. Мы часто будем говорить, что поле $P = \Delta(j)$ есть *результат присоединения к полю* Δ *корня* j *многочлена* $F(x)$ [1]).

В заключение отметим следующее. Если степень n неприводимого многочлена $F(x)$ равна единице, то $\Delta(j) = \Delta$, т. е. в этом случае расширения фактически не получается.

2. Теперь обратимся к произвольному многочлену n-й степени

$$F(x) = A_0 x^n + A_1 x^{n-1} + \ldots + A_n$$

в поле Δ (приводимому или неприводимому—безразлично). Пусть он в поле Δ следующим образом разлагается на неприводимые множители:

$$F(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_s)\, p_1(x) \ldots p_r(x).$$

Через $p_i(x)$ мы обозначили неприводимые многочлены выше первой степени.

Присоединим к Δ последовательно корни $\alpha_1, \alpha_2, \ldots, \alpha_s$; от этого Δ не изменится, потому что $\alpha_1, \ldots, \alpha_s$ лежат в поле Δ. Затем присоединим к Δ какой-нибудь корень α_{s+1} многочлена $p_1(x)$. Получим тогда алгебраическое расширение $\Delta(\alpha_{s+1})$, в котором многочлен $F(x)$ будет распадаться уже на большее

[1]) Можно показать, что всякое конечное расширение Ω поля Δ есть результат последовательного присоединения к Δ корней некоторого многочлена.

число линейных множителей. В самом худшем случае многочлен $F(x)$ в поле $\Delta(\alpha_{s+1})$ будет следующим образом разлагаться на неприводимые множители:

$$F(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_s)(x-\alpha_{s+1})\,q_1(x)\dots q_t(x),$$

где $q_i(x)$—неприводимые в $\Delta(\alpha_{s+1})$ многочлены выше первой степени. Присоединяем далее к $\Delta(\alpha_{s+1})$ какой-нибудь корень α_{s+2} многочлена $q_1(x)$ и т. д. Через конечное число шагов мы должны притти к полю $\bar{P}$, в котором рассматриваемый многочлен $F(x)$ целиком распадается на линейные множители. Это поле $\bar{P}$, полученное в результате последовательного присоединения к Δ всех корней $F(x)$, мы будем называть *нормой* многочлена $F(x)$. Норма $\bar{P}$, очевидно, есть конечное расширение Δ.

§ 55. Разрешимость уравнения в квадратных радикалах

Теперь мы можем ответить на вопрос, поставленный в конце § 53. Прежде всего рассмотрим следующие леммы.

Лемма 1. *Если Ω — конечное расширение второй степени поля Δ, то Ω есть результат присоединения к Δ корня квадратного уравнения с коэффициентами из Δ.*

Доказательство. Возьмём в поле Ω какой-нибудь элемент α, не лежащий в Δ. В силу следствия 4 теоремы Штейница (см. § 54) α должно быть корнем уравнения

$$F(x) = a_0x^2 + a_1x + a_2 = 0 \quad (a_i\text{—элемент } \Delta);$$

α не может быть корнем уравнения первой степени, так как α не лежит в Δ. Отсюда получается, что $a_0 \neq 0$ и многочлен $F(x)$ неприводим (в Δ). Кроме того, отсюда следует, что элементы 1, α линейно независимы относительно Δ. Пусть u—произвольный элемент Ω. Тогда в силу следствия 3 теоремы Штейница элементы 1, α, u будут уже линейно зависимы:

$$c_0u + c_1\alpha + c_2 = 0 \quad (c_i\text{—элементы } \Delta).$$

Коэффициент c_0 не может равняться нулю, так как 1 и α линейно независимы. Следовательно:

$$u = b_0\alpha + b_1;$$

b_i—элементы Δ, а именно $b_0 = -\frac{c_1}{c_0}$, $b_1 = -\frac{c_2}{c_0}$. Этим лемма полностью доказана.

Лемма 2. *Если $f(x)$ многочлен в Δ, Ω—норма $f(x)$ и $p(x)$ неприводимый многочлен в Δ, делящий $f(x)$, то степень многочлена $p(x)$ должна делить $(\Omega:\Delta)$.*

Доказательство. Так как $p(x)$ делит $f(x)$, то корни многочлена $p(x)$ должны лежать в Ω. Отсюда следует, что алгебраическое расширение $\Delta(\alpha)$, где α—корень $p(x)$, есть подполе поля Ω. Поэтому $(\Delta(\alpha):\Delta)$ должно делить $(\Omega:\Delta)$ (см. § 54, теорему 2). Но $(\Delta(\alpha):\Delta)$ равно степени неприводимого многочлена $p(x)$. Следовательно, $(\Omega:\Delta)$ должно делиться на степень многочлена $p(x)$.

Лемма 3. *Пусть $f(x)$ многочлен в поле Δ, Ω—его норма. Если $(\Omega:\Delta) = 2^m$ $(m>1)$, то между Δ и Ω существует конечное расширение Δ_1 поля Δ второй степени относительно Δ: $\Delta \subset \Delta_1 \subset \Omega$, $(\Delta_1:\Delta) = 2$.*

Доказательство. Без ограничения общности рассуждений можно предположить, что многочлен $f(x)$ не имеет корней в поле Δ; в противном случае мы удалили бы из $f(x)$ соответствующие линейные множители.

Пусть $p(x)$ неприводимый многочлен в Δ наименьшей степени, делящий $f(x)$. В силу леммы 2 степень n многочлена $p(x)$ должна делить 2^m, т. е. $n = 2^k$ $(1 \leqslant k \leqslant m)$ [1]. Обозначим корни многочлена $p(x)$ через α_i. Представляются только следующие возможности: либо $k=1$, либо $k>1$. В первом случае лемма доказывается сразу: присоединяя к Δ какой-нибудь корень α непри-

[1]) $k \neq 0$, так как по предположению $f(x)$ не имеет корней в поле Δ.

водимого многочлена $p(x)$ второй степени ($n = 2^1 = 2$), получим требуемое поле $\Delta_1 = \Delta(\alpha)$.

Во втором случае дело обстоит гораздо сложнее. Воспользуемся приёмом, который мы применяли при доказательстве основной теоремы алгебры, и составим вспомогательный многочлен

$$g(x) = \Pi(x - \beta_k),$$

где $\beta_k = \alpha_i\alpha_j + c(\alpha_i + \alpha_j)$, c—элемент поля Δ. Мы утверждаем, что c можно выбрать так, чтобы все выражения $\alpha\,\alpha_j + c(\alpha_i + \alpha_j)$ не лежали в поле Δ. В самом деле, пусть такое c подобрать нельзя. Тогда должны существовать два значения c_1 и c_2, для которых

$$\alpha_i\alpha_j + c_1(\alpha_i + \alpha_j) \text{ и } \alpha_i\alpha_j + c_2(\alpha_i + \alpha_j)$$

будут элементами Δ (см. доказательство основной теоремы алгебры). Отсюда следует, что α_i и α_j являются корнями квадратного уравнения с коэффициентами из Δ. Последнее, однако, невозможно, так как α_i и α_j—корни неприводимого многочлена $p(x)$ выше второй степени [1]).

Итак, пусть c выбрано с таким расчётом, чтобы корни вспомогательного многочлена $g(x)$ не лежали в Δ. Рассуждая так же, как при доказательстве основной теоремы алгебры, приходим к выводу, что коэффициенты многочлена $g(x)$ лежат в Δ и степень $g(x)$ равна $2^{k-1}Q$, где Q—нечётное число.

Теперь роль многочлена $f(x)$ у нас будет играть $g(x)$. Пусть $p_1(x)$—неприводимый многочлен в Δ наименьшей степени, делящий $g(x)$. Легко сообразить, что степень многочлена $p_1(x)$ должна равняться 2^{k_1}, где k_1, с одной стороны, не меньше 1, а с другой стороны, *не превосходит* $k - 1$ [2]). Если $k_1 = 1$, то лемма доказывается сразу: $\Delta_1 = \Delta(\beta)$, здесь $\beta = \alpha_i\alpha_j + c(\alpha_i + \alpha_j)$ один из корней $p_1(x)$. Если $k_1 > 1$, то, как и выше, строим вспомогательный многочлен $g_1(x)$ и получаем неприводимый многочлен $p_2(x)$, у которого степень равна $2^{k_2}(1 \leqslant k_2 \leqslant k - 2)$, и т. д.

Продолжая такой процесс построения вспомогательных многочленов, мы в конце концов придём к неприводимому многочлену $p_s(x)$ второй степени. Присоединяя к Δ один из корней этого многочлена, получим требуемое поле Δ_1.

Для более удобной формулировки критерия разрешимости уравнения в квадратных радикалах введём следующее определение.

Пусть $f(x)$ многочлен в поле Δ. Мы скажем, что *уравнение* $f(x) = 0$ *приводится к цепи уравнений не выше второй степени, если его корни выражаются рационально через корни уравнений*

$$f_1(x) = 0,\ f_2(x) = 0,\ \ldots,\ f_s(x) = 0,$$

где $f_1(x)$—многочлен первой степени или неприводимый многочлен второй степени в поле Δ; $f_2(x)$—многочлен первой степени или неприводимый многочлен второй степени в поле $\Delta(\alpha)$, получающемся в результате присоединения к Δ корня $f_1(x)$; $f_3(x)$—многочлен первой степени или неприводимый многочлен второй степени в поле $\Delta(\alpha)(\beta)$, получающемся в результате присоединения к $\Delta(\alpha)$ корня $f_2(x)$, и т. д.

Теперь мы можем высказать следующую теорему.

Теорема. *Пусть $f(x)$ многочлен в поле Δ, Ω— его норма. Для того чтобы уравнение $f(x) = 0$ приводилось к цепи уравнений не выше второй степени, необходимо и достаточно, чтобы $(\Omega : \Delta) = 2^m$.*

Доказательство. Пусть уравнение $f(x) = 0$ приводится к цепи уравнений

$$f_1(x) = 0, \ldots, f_s(x) = 0 \qquad (1)$$

[1]) А именно, если α_i и α_j являются одновременно корнями многочлена $p(x)$ и квадратного многочлена $h(x)$ в поле Δ, то $p(x) = h(x) \cdot k(x)$, где $k(x)$—многочлен в Δ, отличный от постоянной. Получается нелепость: многочлен $p(x)$ оказывается приводимым.

[2]) Если бы k_1 превосходило $k - 1$, то $g(x)$ разлагалось бы на неприводимые множители степени 2^{s_i} ($s_i > k - 1$), вследствие чего степень многочлена $g(x)$ равнялась бы $2^t Q_1$ ($t > k - 1$), а не $2^{k-1}Q$.

не выше второй степени. Присоединим к Δ последовательно корни уравнений (1). Если уравнения (1)—все первой степени, то от таких присоединений Δ не изменится; следовательно, в этом случае $\Omega = \Delta$ и $(\Omega : \Delta) = 1 = 2^0$. Если не все уравнения (1) первой степени, то, в силу теоремы 1 § 54, получается конечное расширение P поля Δ степени 2^n относительно Δ. В поле P содержится, очевидно, норма Ω многочлена $f(x)$; поэтому по теореме 2 § 54 $(\Omega : \Delta)$ должна делить $(P : \Delta) = 2^n$. Отсюда $(\Omega : \Delta) = 2^m$.

Обратно, пусть $(\Omega : \Delta) = 2^m$. Разберём следующие случаи: 1) $m = 0$, 2) $m = 1$ и 3) $m > 1$.

В первом случае $\Omega = \Delta$, т. е. все корни уравнения $f(x) = 0$ лежат в поле Δ. Это значит, что уравнение $f(x) = 0$ приводится к цепи уравнений *первой* степени.

Во втором случае $(\Omega : \Delta) = 2$. Таким образом по лемме 1 Ω есть результат присоединения к Δ корня квадратного уравнения с коэффициентами из Δ. Отсюда становится очевидным, что уравнение $f(x) = 0$ в случае $(\Omega : \Delta) = 2$ приводится к цепи уравнений не выше второй степени.

В третьем случае рассуждаем следующим образом. Если $(\Omega : \Delta) = 2^m$, $m > 1$, то согласно лемме 3 должно существовать промежуточное конечное расширение Δ_1 поля Δ второй степени относительно Δ. При этом $(\Omega : \Delta_1) = 2^{m-1}$. Снова применяем лемму 3, рассматривая вместо Δ поле Δ_1. По этой лемме должно существовать промежуточное конечное расширение Δ_2 поля Δ_1 второй степени относительно Δ_1. Степень нормы Ω относительно Δ_2 ещё более понизится: $(\Omega : \Delta) = 2^{m-2}$ и т. д. В итоге мы получим последовательность конечных расширений

$$\Delta \subset \Delta_1 \subset \Delta_2 \subset \ldots \subset \Delta_{m-1} \subset \Delta_m = \Omega.$$

Каждое последующее расширение будет второй степени относительно предыдущего. По лемме 1 Δ_{i+1} есть результат присоединения к Δ_i корня квадратного уравнения с коэффициентами из Δ_i. Отсюда становится очевидным, что уравнение $f(x) = 0$ приводится к цепи уравнений не выше второй степени.

§ 56. Удвоение куба. Трисекция угла. Деление окружности на равные части

Задача об удвоении куба, как известно, связана с решением уравнения

$$f(x) = x^3 - 2 = 0. \tag{1}$$

Посмотрим, будет ли это уравнение приводиться к цепи уравнений не выше второй степени. Прежде всего обратим внимание на то обстоятельство, что многочлен $f(x) = x^3 - 2$ неприводим в поле Γ рациональных чисел. В самом деле, если бы многочлен третьей степени $f(x)$ разлагался в поле Γ на произведение двух множителей, отличных от постоянной, то по меньшей мере один из этих множителей был бы линейным, т. е. имел бы вид $ax + b$, где a и b—рациональные числа. Отсюда следовало бы, что многочлен $f(x)$ имеет рациональный корень $-\frac{b}{a}$. Но это невозможно, так как уравнение (1) рациональных корней, очевидно, иметь не может.

А теперь легко убедиться, что условия теоремы § 54 не выполняются. Действительно, в данном случае полем Δ является Γ. По теореме 2 § 54 степень $(\Omega : \Gamma)$ должна делиться на $(\Gamma(\alpha) : \Gamma)$, где α—корень уравнения (1). Но $(\Gamma(\alpha) : \Gamma) = 3$. Следовательно, $(\Omega : \Gamma)$ кратно 3, т. е. не может быть степенью двойки.

Итак, задача об удвоении куба не разрешима с помощью циркуля и линейки.

Обращаемся теперь к задаче о трисекции угла. Пусть дан угол α, требуется его разделить на три равные части. Обозначим искомый угол через φ; таким образом $\alpha = 3\varphi$. Как известно,

$$\cos\alpha = \cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi. \tag{2}$$

Поскольку угол α дан, мы можем считать его косинус известным. Поэтому полагаем $\cos\alpha = \frac{b}{2}$; $\cos\frac{x}{2}$, как неизвестную величину, приравниваем $\frac{x}{2}$. После этого уравнение (2) примет такой вид:

$$\frac{b}{2} = 4\left(\frac{x}{2}\right)^3 - 3\left(\frac{x}{2}\right),$$

или окончательно:

$$f(x) = x^3 - 3x - b = 0. \tag{3}$$

Нетрудно указать бесчисленное множество рациональных значений b, при которых многочлен третьей степени $f(x) = x^3 - 3x - b$ будет неприводим в поле Г рациональных чисел. Например, когда $b = 1$ $\left(\text{в этом случае } \alpha = \frac{\pi}{3}\right)$, уравнение (3) не имеет рациональных корней: таким образом многочлен $f(x)$ при $b = 1$ неприводим в Г. Следовательно, условия теоремы § 54 не выполняются: $(\Omega : \Gamma)$ кратно 3. Мы видим, что угол $\frac{\pi}{3}$ нельзя разделить на три равные части с помощью циркуля и линейки. С помощью аналогичных рассуждений можно показать, что угол $\alpha = \arccos\frac{1}{2p}$ (p—натуральное простое число) также нельзя разделить на три равные части с помощью циркуля и линейки. В самом деле, нетрудно убедиться, что уравнение

$$f(x) = x^3 - 3x - \frac{1}{p} = 0$$

не имеет рациональных корней: многочлен $f(x) = x^3 - 3x - \frac{1}{p}$, следовательно, неприводим в Г.

Итак, задача о трисекции угла в общем не может быть решена с помощью циркуля и линейки.

Наконец, рассмотрим задачу о делении окружности на n равных частей. Она связана с двучленным уравнением $x^n - 1 = 0$.

Сделаем предварительно несколько замечаний.

1. Пусть $n = n_1 n_2$, где n_1 и n_2 два взаимно простых натуральных числа. Окружность тогда и только тогда может быть разделена на n равных частей с помощью циркуля и линейки, когда её можно разделить с помощью этих инструментов на n_1 и на n_2 равных частей.

В самом деле, пусть окружность можно разделить циркулем и линейкой на n_1 равных частей и на n_2 равных частей. По условию n_1 и n_2 взаимно просты, поэтому для них можно подобрать такие целые x и y, чтобы

$$n_1 x + n_2 y = 1.$$

Если разделить обе части этого равенства на $n = n_1 n_2$, то получится

$$\frac{y}{n_1} + \frac{x}{n_2} = \frac{1}{n}, \tag{4}$$

т. е., зная $\frac{1}{n_1}$-ю и $\frac{1}{n_2}$-ю части окружности, мы, руководствуясь равенством (4), можем построить и $\frac{1}{n}$-ю часть окружности.

Обратно, пусть окружность делится с помощью циркуля и линейки на n равных частей. Тогда она и подавно будет делиться на n_1 и на n_2 равных частей. А именно, чтобы построить $\frac{1}{n_1}$-ю $\left(\frac{1}{n_2}\text{-ю}\right)$ часть окружности, надо её $\frac{1}{n}$-ю часть повторить n_2 (n_1) раз.

2. Вместо двучленного уравнения $x^n - 1 = 0$ можно рассматривать так называемое *уравнение деления окружности* на n частей:

$$\Phi_n(x) = \prod_{i=1}^{h} (x - \xi_i) = 0,$$

где ξ_i—первообразные корни n-й степени из единицы, h—число всех таких первообразных корней; оно, как мы знаем, равно эйлеровой числовой функции $\varphi(n)$ (см. § 47).

Для получения многочлена $\Phi_n(x)$ незачем составлять произведение линейных множителей $(x - \xi_i)$. Проще будет, если мы двучлен $x^n - 1$ освободим последовательно от множителей, входящих в двучлены $x^d - 1$, где d—всевозможные делители числа n.

3. Составим уравнение деления окружности для $n = p^\alpha$ (p—простое число). Согласно предыдущему замечанию

$$\Phi_{p^\alpha}(x) = \frac{x^{p^\alpha} - 1}{x^{p^{\alpha-1}} - 1} = x^{p^{\alpha-1}(p-1)} + x^{p^{\alpha-1}(p-2)} + \ldots + 1 = 0.$$

В самом деле, непервообразные корни двучленного уравнения $x^{p^\alpha} - 1 = 0$ будут, очевидно, также корнями $x^{p^{\alpha-1}} - 1 = 0$. Поэтому, производя деление $x^{p^\alpha} - 1$ на $x^{p^{\alpha-1}} - 1$, мы тем самым освобождаемся от непервообразных корней, т. е. получаем, согласно предыдущему определению, левую часть уравнения деления окружности.

Мы сейчас покажем, что многочлен $\Phi_{p^\alpha}(x)$ неприводим в поле Г рациональных чисел.

Для этой цели положим $x = z + 1$. Тогда получим

$$f(z) = \frac{(z+1)^{p^\alpha} - 1}{(z+1)^{p^{\alpha-1}} - 1} = \frac{z^{p^\alpha - 1} + C^1_{p^\alpha} z^{p^\alpha - 2} + \ldots + C^1_{p^\alpha}}{z^{p^{\alpha-1}-1} + C^1_{p^{\alpha-1}} z^{p^{\alpha-1}-2} + \ldots + C^1_{p^{\alpha-1}}}. \qquad (5)$$

Все коэффициенты многочлена, стоящего в числителе, кроме старшего коэффициента, делятся на p. То же самое можно сказать и относительно многочлена, находящегося в знаменателе. Нетрудно усмотреть из самого процесса деления, что в частном, которое получается при делении числителя на знаменатель, все коэффициенты, кроме старшего, также делятся на p. Чтобы узнать, чему равен свободный член частного, полагаем в дробном выражении (5) $z = 0$:

$$f(0) = \frac{C^1_{p^\alpha}}{C^1_{p^{\alpha-1}}} = \frac{p^\alpha}{p^{\alpha-1}} = p.$$

Мы видим, что свободный член частного равен p и потому не делится на p^2. Таким образом, многочлен $f(z)$ на основании критерия Эйзенштейна неприводим в Г. Следовательно, $\Phi_{p^\alpha}(x)$ также неприводимо в поле Г.

Теперь мы можем доказать следующую теорему, принадлежащую Гауссу.

Теорема. *Окружность тогда и только тогда можно разделить на n равных частей с помощью циркуля и линейки, когда*

$$n = 2^\omega q_1 q_2 \ldots q_s,$$

где ω—целое неотрицательное число, q_i—простые нечётные числа вида $2^k + 1$.

Доказательство. Напишем разложение числа n на простые множители:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}.$$

В силу замечания I достаточно ограничиться частным случаем $n = p^\alpha$ (p—простое число). Найдём норму многочлена деления окружности $\Phi_{p^\alpha}(x)$. В данном случае $\Delta = \Gamma$. Согласно замечанию 3 многочлен $\Phi_{p^\alpha}(x)$ неприводим в поле Γ. Присоединим к Γ какой-нибудь корень ξ многочлена $\Phi_{p^\alpha}(x)$. Мы утверждаем, что $\Gamma(\xi)$ есть норма $\Phi_{p^\alpha}(x)$. В самом деле, так как корни $\Phi_{p^\alpha}(x)$ и в частности само ξ являются первообразными корнями p^α-й степени из единицы, то корни $\Phi_{p^\alpha}(x)$ суть степени ξ. Поэтому в $\Gamma(\xi)$ должны лежать все корни $\Phi_{p^\alpha}(x)$.

Так как степень неприводимого многочлена $\Phi_{p^\alpha}(x)$ равна $p^{\alpha-1}(p-1)$ (см. замечание 3), то

$$(\Gamma(\xi):\Gamma) = p^{\alpha-1}(p-1).$$

Для того чтобы уравнение деления окружности

$$\Phi_{p^\alpha}(x) = 0$$

приводилось к цепи уравнений не выше второй степени, необходимо и достаточно, чтобы степень нормы многочлена $\Phi_{p^\alpha}(x)$ относительно Γ равнялась 2^m (см. теорему § 55). Следовательно:

$$(\Gamma(\xi):\Gamma) = p^{\alpha-1}(p-1) = 2^m.$$

Но это возможно только в следующих двух случаях: 1) когда $p = 2^m$, и 2) когда $\alpha = 1$, p—нечётное простое число вида $2^k + 1$.

Этим теорема Гаусса доказана полностью.

§ 57. О неприводимом случае

В заключение рассмотрим в основных чертах ещё одно применение теории, развитой в настоящей главе.

В свое время мы отметили, что в случае отрицательного $\frac{q^2}{4} + \frac{p^3}{27}$ нельзя избавиться от мнимостей в формуле Кардана кубического уравнения

$$x^3 + px + q = 0.$$

Мы покажем, что это явление наблюдается не только для уравнений третьей степени, но и для целого класса уравнений высших степеней.

Пусть $f(x)$—некоторый многочлен в поле Δ. Как известно, поле Ω называется нормой многочлена $f(x)$ *относительно* Δ, если Ω получается путём присоединения к Δ всех корней $x_1, x_2, \ldots, x_n$ многочлена $f(x)$. Мы будем часто норму Ω обозначать символом $\Delta(x_1, x_2, \ldots, x_n)$. Весьма важную роль будет играть следующее свойство нормы.

Основное свойство нормы. *Если Ω—норма многочлена $f(x)$ относительно Δ, то всякий многочлен $p(x)$, неприводимый в Δ, либо совсем не имеет корней в Ω, либо распадается в Ω целиком на линейные множители.*

Доказательство. Пусть $p(x)$ имеет в $\Omega = \Delta(x_1, x_2, \ldots, x_n)$ хотя бы один корень β. Тогда $\beta_1 = \beta$ будет целой рациональной функцией корней многочлена $f(x)$:

$$\beta_1 = \beta = r(x_1, x_2, \ldots, x_n).$$

Производя в функции $r(x_1, x_2, \ldots, x_n)$ всевозможные перестановки корней x_i, получим $n!$ значений β_i (включая и само β_1):

$$\beta_i = r(x_{i_1}, x_{i_2}, \ldots, x_{i_n}).$$

Составим следующий вспомогательный многочлен:

$$g(x) = \prod_{i=1}^{n} (x - \beta_i).$$

Коэффициенты этого многочлена, очевидно, являются симметрическими функциями x_i. Отсюда в силу основной теоремы теории симметрических функций коэффициенты $g(x)$ должны быть целыми рациональными функциями коэффициентов $p(x)$, т. е. должны лежать в поле Δ. Из самого построения многочлена $g(x)$ видно, что $g(x)$ имеет с $p(x)$ общий корень $\beta_1=\beta$. Отсюда следует, что, поскольку $g(x)$ и $p(x)$ — многочлены в Δ и $p(x)$, кроме того, неприводимо в Δ, многочлен $g(x)$ должен делиться на $p(x)$. В самом деле, в силу неприводимости $p(x)$ наибольший общий делитель $D(x)$ многочленов $g(x)$ и $p(x)$ равен 1 или $p(x)$. Но $D(x)$ не может равняться единице, так как $D(x)$ делятся на $x-\beta$. Значит, $D(x)=p(x)$, и потому $g(x)$ делится на $p(x)$.

А теперь теорема становится очевидной — многочлен $g(x)$ по построению целиком распадается в Ω на линейные множители. Следовательно, его делитель $p(x)$ и подавно распадается в Ω на линейные множители.

Для дальнейшего нам сверх того понадобится следующая лемма.

Лемма. *Если двучленное уравнение $x^p-a=0$, где a — элемент Δ, p — простое число, приводимо в Δ, то a должно быть точной p-й степенью в Δ: $a=\alpha^p$, где α — некоторый элемент Δ.*

Доказательство. Пусть $x^p-a=\varphi(x)\psi(x)$, где $\varphi(x)$ и $\psi(x)$ — некоторые многочлены в Δ. Обозначим через ε первообразный корень p-й степени из единицы и через θ_0 какой-нибудь корень уравнения $x^p-a=0$. Тогда для всякого корня θ_ν этого уравнения будем иметь:

$$\theta_\nu=\varepsilon^\nu\theta_0 \quad (\nu=0, 1, \ldots, p-1).$$

Отсюда следует, что свободный член b многочлена $\varphi(x)$ должен равняться

$$b=\theta_{\nu_1}\theta_{\nu_2}\ldots\theta_{\nu_r}=\varepsilon^{\nu_1+\nu_2+\ldots+\nu_r}\theta_0^r=\varepsilon_1\theta_0^r$$

$$(\varepsilon_1=\varepsilon^{\nu_1+\nu_2+\ldots+\nu_r},\quad 0<r<p).$$

Очевидно, что ε_1 есть какой-то корень p-й степени из единицы. Возведём теперь b в p-ю степень:

$$b^p=\varepsilon_1^p\theta_0^{pr}=\theta_0^{pr}=a^r.$$

Так как числа r и p взаимно просты (вспомним $-0<r<p$), то можно подобрать такие целые числа k_1 и k_2, чтобы

$$k_1r+k_2p=1.$$

Отсюда

$$a=a^{k_1r+k_2p}=a^{k_1r}a^{k_2p}=(a^r)^{k_1}a^{k_2p}=b^{k_1p}a^{k_2p}=(b^{k_1}a^{k_2})^p,$$

и лемма доказана.

Теперь мы можем высказать теорему, обобщающую до некоторой степени неприводимый случай (casus irr ducibilis) уравнения третьей степени.

Теорема. *Пусть Δ — некоторое подполе поля действительных чисел, $f(x)=0$ — уравнение n-й степени, неприводимое в Δ. Тогда если n делится на простое нечётное число p и все корни уравнения действительны, то корни уравнения нельзя выразить через действительные радикалы.*

Примечание. Говорят, что корни уравнения $f(x)=0$ выражаются в действительных радикалах, если они выражаются рационально через действительные корни двучленных уравнений $f_1(x)=0$, $f_2(x)=0, \ldots, f_s(x)=0$, где $f_1(x)$ — многочлен, неприводимый в поле $\Delta_1=\Delta$; $f_2(x)$ — многочлен, неприводимый в поле Δ_2, получающемся путём присоединения к Δ действительного корня $f_1(x)$; $f_3(x)$ — многочлен, неприводимый в поле Δ_3, получающемся путём присоединения к Δ_2 действительного корня $f_2(x)$ и т. д. При этом под радикалом $\lambda=\sqrt[m]{a}$ мы будем всегда подразумевать один из корней двучленного уравнения $x^m-a=0$. Очевидно, что показатель m радиката λ можно без ограничения общности выводов считать простым числом. В самом деле, если m составное, то можно λ заменить несколькими радикалами с простыми показателями. Например, $\lambda=\sqrt[12]{a}$ можно заменить радикалами $\lambda_1=\sqrt[3]{a}$, $\lambda_2=\sqrt{\lambda_1}$, $\lambda_3=\sqrt{\lambda_2}$.

Теперь приступаем к доказательству теоремы.

Доказательство. Пусть Ω — норма многочлена $f(x)$ относительно Δ. Обозначим корни $f(x)=0$ через $x_1, x_2, \ldots, x_n$. Очевидно, что $(\Omega:\Delta)=m$ должна делиться на степень n уравнения $f(x)=0$, в силу чего m делится на нечётное простое число p.

Допустим, что корни x_i выражаются через действительные радикалы $\lambda_k=\sqrt[p_k]{a_k}$ $(k=1, 2, \ldots, r)$, где p_k — простое число и a_k лежит в поле $\Delta(\lambda_1, \lambda_2, \ldots, \lambda_{k-1})$, получающегося путём присоединения к Δ радикалов $\lambda_1, \lambda_2, \ldots, \lambda_{k-1}$ (в частности a_1 лежит в Δ). Тогда, присоединяя к Δ все эти радикалы, получим действительное поле

$$\Sigma=\Delta(\lambda_1, \lambda_2, \ldots, \lambda_r),$$

содержащее Ω.

Некоторые показатели p_i радикалов могут равняться двойке. Пусть $p_{i_1}=p_{i_2}=\ldots=p_{i_l}=2$, а остальные p_i отличны от 2. Тогда

$$(\Sigma:\Delta)=2^l q_{l+1}q_{l+2}\cdots q_r, \tag{1}$$

где через q_i обозначены p_i, отличные от 2.

Будем теперь радикалы λ присоединять не к Δ, а к Ω. Пусть показатель p_k радикала λ_k равен двойке. Если λ_k приводимо в $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_{k-1})$ [1], то a_k будет в $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_{k-1})$ точной p_k-й степенью, а именно второй степенью (см. лемму), вследствие чего λ_k будет лежать в $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_{k-1})$. Таким образом, присоединяя λ_k к $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_{k-1})$, мы фактически никакого расширения не получим. Если же λ_k неприводимо в $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_{k-1})$, то получится расширение второй степени относительно $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_{k-1})$.

Пусть теперь показатель p_k радикала λ_k отличен от двойки, т. е. равен q_k. Посмотрим, может ли в этом случае λ_k быть приводимым в $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_{k-1})$. Если λ_k приводимо, то в силу вышеизложенной леммы λ_k будет лежать в $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_{k-1})$. Но

$$\Omega(\lambda_1, \lambda_2, \ldots, \lambda_{k-1})=\bar{\Delta}(x_1, x_2, \ldots, x_n), \text{ где } \bar{\Delta}=\Delta(\lambda_1, \ldots, \lambda_{k-1}),$$

есть норма многочлена $f(x)$ относительно поля $\bar{\Delta}=\Delta(\lambda_1, \ldots, \lambda_{k-1})$. По доказанному выше свойству нормы в $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_{k-1})$ должен лежать не только один корень λ_k уравнения $x^{p_k}-a_k=0$, но и все его корни. Однако, при $p_k\neq 2$ корни этого уравнения, кроме одного, являются мнимыми. Мы пришли к абсурду: действительное поле $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_{k-1})$ содержит мнимые числа. Следовательно, λ_k должно быть неприводимым в $\Omega(\lambda_1, \ldots, \lambda_{k-1})$.

Из всех этих рассуждений вытекает, что степень поля $\Sigma=\Omega(\lambda_1, \lambda_2, \ldots, \lambda_r)$ относительно Ω равна $2^t q_{l+1}\ldots q_r$, где $t\leqslant l$:

$$(\Sigma:\Omega)=2^t q_{l+1}q_{l+2}\cdots q_r.$$

Отсюда

$$(\Sigma:\Delta)=(\Sigma:\Omega)(\Omega:\Delta)=2^t q_{l+1}q_{l+2}\ldots q_r m. \tag{2}$$

Сравнивая равенства (1) и (2), получаем

$$m=2^{l-t},$$

что невозможно, так как m делится на простое нечётное число p.

---

[1] Т. е. уравнение $x^{p_k}-a_k=0$ приводимо в $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_{k-1})$.

ОТВЕТЫ

§ 2, стр. 13.

1. 1, −6, 0. **2.** 0, 1, −1.

4. a) $u=\frac{23}{57}$, $v=\frac{28}{57}$. b) $x=a\cos\alpha+b\sin\alpha$, $y=-a\sin\alpha+b\cos\alpha$.

c) $x=0$, $y=0$.

5. 18, 5, 0, 0.

7. Надо проверить тождества:

a) $$\begin{vmatrix} a_1+\alpha & b_1+\beta & c_1+\gamma \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} + \begin{vmatrix} \alpha & \beta & \gamma \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}.$$

b) $$\begin{vmatrix} a_1+\alpha_1 & b_1 & c_1 \\ a_2+\alpha_2 & b_2 & c_2 \\ a_3+\alpha_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} + \begin{vmatrix} \alpha_1 & b_1 & c_1 \\ \alpha_2 & b_2 & c_2 \\ \alpha_3 & b_3 & c_3 \end{vmatrix}.$$

d) $$a_1\begin{vmatrix} b_1 & c_1 & d_1 \\ b_2 & c_2 & d_2 \\ b_3 & c_3 & d_3 \end{vmatrix} - b_1\begin{vmatrix} a_1 & c_1 & d_1 \\ a_2 & c_2 & d_2 \\ a_3 & c_3 & d_3 \end{vmatrix} + c_1\begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix} - d_1\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = 0.$$

8. a) $x=1$, $y=2$, $z=3$. b) $x=-a$, $y=b$, $z=c$.

§ 4, стр. 21.

1. a) 6 инверсий. b) 25 инверсий. c) 6 инверсий. d) $\frac{n(n-1)}{2}$ инверсий. e) k^2 инверсий.

2. Надо произвести последовательно транспозиции (3, 5), (4, 1), (3, 1) и (1, 2).

3. $s=14$, $t=6$. Член имеет знак плюс.

4. Член имеет знак $(-1)^{\frac{n(n-1)}{2}}$.

§ 5, стр. 23.

1. 5, 6, 4, 3, 2, 1.

2. a) $\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}$.

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

c) $\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\4&3&2&1&8&7&9&10&6&5\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\4&3&1&8&5&7&6&10&2&9\end{pmatrix}=$

$=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\8&1&3&4&10&6&2&9&7&5\end{pmatrix}$.

3. $n!$ подстановок.

Стр. 24.

1. (1 6 2) (3 5) (4).

2. a) $\begin{pmatrix}1&2&3&4&5&6\\2&1&4&3&6&5\end{pmatrix}$. b) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\8&3&4&2&6&5&7&9&1\end{pmatrix}$.

c) $\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\10&2&4&5&1&6&8&9&7&3\end{pmatrix}$.

Стр. 26.

a) $n - s = 7 - 2 = 5$; расположение нечётного класса.

b) $n - s = 8 - 2 = 6$; расположение чётного класса.

c) $n - s = 10 - 3 = 7$; расположение нечётного класса.

§ 7, стр. 38.

1. 40, 1875, 306.

2. $(\alpha_1\beta_2 - \alpha_2\beta_1)(\alpha_1\beta_3 - \alpha_3\beta_1) \dots (\alpha_1\beta_{n+1} - \alpha_{n+1}\beta_1) \dots (\alpha_n\beta_{n+1} - \alpha_{n+1}\beta_n)$.

§ 9, стр. 52.

1. a) $\begin{vmatrix} ac + bc_1 & ad + bd_1 \\ a_1c + b_1c_1 & a_1d + b_1d_1 \end{vmatrix}$. b) $\begin{vmatrix} 10 & 19 & 31 \\ 12 & 35 & 57 \\ 10 & -4 & -2 \end{vmatrix}$. c) $\begin{vmatrix} 25 & 28 & 39 & 18 \\ 24 & 22 & 36 & 18 \\ 11 & 21 & 19 & 9 \\ 52 & 52 & 60 & 36 \end{vmatrix}$.

3. Для вывода способа 1) надо рассмотреть произведение $D_1\overline{D}_2$, где $\overline{D}_2$ — определитель, получающийся из определителя D_2 заменой строк столбцами. Аналогичным образом выводятся и остальные два способа.

§ 10, стр. 58.

1. a) $a^2 + b^2 + c^2 - 2ab - 2ac - 2bc$. b) $abcd\left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} + 1\right)$.

c) $(a+b+c+d)(a-b-c+d)(a+b-c-d)(a-b+c-d)$.

d) $(-1)^{n-1}\frac{n^{n-1}(n+1)}{2}$.

2. 93.

3. Определитель следует разложить по минорам, составленным из первых двух строк

4. a) $-(aef + bdf + cde)$. b) $-(aa_1 + bb_1 + cc_1)$. c) $-a^2(b+c)$.

5. $D^2 = (a^2 + b^2 + c^2 + d^2)^4$, откуда $D = (a^2 + b^2 + c^2 + d^2)^2$. Корень квадратный извлекается со знаком плюс, так как в определителе a^4 входит со знаком плюс.

§ 14, стр. 69.

1. Из k строк матрицы можно составить C_n^k определителей k-го порядка. В свою очередь k строк можно выбрать C_m^k способами. Таким образом всех определителей k-го порядка будет $C_n^k C_m^k$.

2. $f_1 + 2f_2 + 3f_3 - f_4 = 0$. **3.** Независимы.

4. Обозначим через r ранг матрицы данной системы форм. Тогда любые $r+1$ форм из этой системы будут линейно зависимы, так как ранг матрицы этих форм не может превосходить r.

§ 15, стр. 72.

1. $r_1 = 3$, $r_2 = 4$.

2. С помощью преобразования d) можно добиться того, чтобы элементы матрицы, отличные от нуля, встречались в разных строках и столбцах. С помощью преобразования b) эти ненулевые элементы можно перенести на первые места главной диагонали. Наконец, с помощью преобразования c) эти элементы можно превратить в единицы.

§ 16 стр. 76.

a) $x = -8z + 5u - 1$, $y = -13z + 9u - 3$.

b) $x_1 = x_3 - x_4$, $x_2 = 2x_3 - x_4 + 1$. c) Система несовместна.

d) $x_1 = 0$, $x_2 = \frac{1}{2}x_4$, $x_3 = \frac{7}{2}x_4$. e) $x_2 = 0x_1$, $x_3 = 5x_1$, $x_4 = 0$.

§ 17, стр. 80.

a) $-\frac{11}{2}$, $-\frac{7}{2}$, 1, b) $\frac{27}{13}$, $-\frac{17}{26}$, $-\frac{19}{26}$, 1.

c) $-2,\ 0,\ 1,\ 0,\ 0;\ -1,\ -1,\ 0,\ 1,\ 0$.

§ 20, стр. 94.

1. $\begin{Vmatrix} 26 & -9 & 45 \\ 98 & -106 & 265 \\ 19 & 0 & 60 \end{Vmatrix}$. **2.** $A^{-1}=\begin{Vmatrix} \frac{1}{3} & 0 & -\frac{1}{3} \\ -\frac{19}{25} & 1 & \frac{4}{25} \\ \frac{1}{3} & 0 & 0 \end{Vmatrix}$.

3. Это следует из того, что произведение определителей, отличных от нуля, не может быть равно нулю.

§ 21, стр. 97.

1. По отношению к операции сложения данное множество иррациональностей группу не образует.

2. Данное множество матриц группу не образует.

§ 22, стр. 117.

1. a) Кольцо. b) Данное множество не образует кольца, так как сумма двух правильных дробей может оказаться неправильной дробью. c) Данное множество кольцо образует.

2. a) Данное множество поле образует. b) Данное множество поля не образует, так как деление не всегда выполнимо. c) Данное множество поля не образует.

§ 23, стр. 125.

a) $\varphi = z_1^2 - \frac{4}{25} z_2^2 + \frac{9}{25} z_3^2$,

где

$$z_1 = x_1 - \frac{5}{2} x_2, \quad z_2 = -\frac{25}{4} x_2 + \frac{3}{2} x_3, \quad z_3 = x_3.$$

b) $\varphi = u_1^2 - u_2^2 + u_3^2 - u_4^2$,

где

$$u_1 = \frac{x_1 + x_2 - x_3}{2}, \quad u_2 = \frac{x_1 - x_2 + x_3}{2}, \quad u_3 = \frac{x_3 + x_4}{2}, \quad u_4 = -\frac{x_3 - x_4}{2}.$$

c) $\varphi = -z_1^2 + 5z_2^2 - 5z_3^2 + \frac{1}{4} z_4^2$,

где

$$z_1 = -x_3 + \frac{1}{2} x_4, \quad z_2 = \frac{x_1 + x_2}{2}, \quad z_3 = \frac{x_1 - x_2}{2}, \quad z_4 = x_4.$$

§ 25, стр. 137.

, а указатель 2.

и $\varphi = u^2$. В случае b) $\varphi = (u_1 + u_2) \times (u_1 - u_2)$. $\varphi = f_1 f_2$, где f, f_1, f_2—линейные формы, то, подкдающемуся преобразованию $u_1 = f_1$, $u_2 = x_2$, ... $f_1 - f_2$), $u_2 = \frac{1}{2}(f_1 + f_2)$, $u_3 = x_3, \ldots, u_n = x_n$, получающую $r = 1$, или $r = 2$, $p = 1$.

форм ранга $r + 1$ от n переменных. Поэтому число

$$\ldots + (n+1) = \frac{(n+1)(n+2)}{2},$$

. 1.) $(f(x), g(x)) = 1$.

$2x^3 - 3x^2 + \frac{17}{2} x - \frac{15}{2}$.

2. a) $f(x) = -4 + 4(x+1) + 5(x+1)^2 - 15(x+1)^3 + 14(x+1)^4 - 6(x+1)^5 + (x+1)^6$.

b) $f(x) = 11 - 16(x+1) + 16(x+1)^2 - 7(x+1)^3 + (x+1)^4$.

c) $f(x) = -16 + 58(x+1) - 105(x+1)^3 + 113(x+1)^3 - 76(x+1)^4 + 32(x+1)^5 - 8(x+1)^6 + (x+1)^7$.

3. $f(0) = \frac{31}{6}$.

§ 30, стр. 163.

a) $X_1 = x - 2$, $X_2 = 1$, $X_3 = x + 1$.

b) $X_1 = x^2 + 1$, $X_2 = 1$, $X_3 = x - 1$.

c) $X_1 = 1$, $X_2 = x^2 + 1$, $X_3 = x - 1$.

d) Многочлен не имеет кратных множителей.

§ 31, стр. 165.

a) $q(x) = 3x^3 + 10x^2 + 39x + 161$; $r = 651$.

b) $q(x) = x^4 - 2x^3 + 10x^2 - 22x + 50$; $r = -97$.

c) $q(x) = x^5 - \frac{1}{2}x^4 - \frac{1}{4}x^3 - \frac{17}{8}x^2 - \frac{1}{16}x - \frac{225}{32}$; $r = -\frac{865}{64}$.

d) $q(x) = x^4 - x^3 + \frac{1}{2}x^2 + \frac{1}{12}x - \frac{49}{24}$; $r = \frac{773}{240}$.

§ 33, стр. 178.

a) $x_1 = -2$, $x_2 = -3$. b) Рациональных корней не имеет. c) $x = 3$.

§ 34, стр. 181.

a) Данный многочлен удовлетворяет всем требованиям критерия Эйзенштейна. b) Полагая $x = y + 1$, получим многочлен, удовлетворяющий требованиям критерия Эйзенштейна. c) Надо положить $x = y + 1$.

§ 38, стр. 194.

1. a) Первый корень лежит в промежутке $(-2, -1)$, а второй — промежутке $(1, 2)$. b) Первый корень лежит в промежутке $(-1, 0)$, второй лежит в промежутке $(0, 1)$ и третий в промежутке $(6, 7)$.

3. При $x = -\infty$ в ряду функций Штурма будет n перемен, а при x ни одной перемены.

4. Пусть, напротив, производная $f'(x)$ сохраняет знак между двумя ними α и β $(\alpha > \beta)$ многочлена $f(x)$, например, пусть $f'(x)$ положит Тогда при переходе x через корень β будет наблюдаться не потеря, а п тение одной перемены.

Стр. 196.

a) Один положительный и два или нуль отрицательных корней. b положительный и три или один отрицательный корень. c) Один полож ный корень. Отрицательных корней нет.

§ 39, стр. 202.

1. 2,094.

2. $x_1 = 2.5842$; $x_2 = -3,2899$; $x_3 = 0,7057$.

3. 0,90506.

§ 40, стр. 207.

a) $-34 - 51i$. b) $-92 - 74i$. c) $\frac{398 + 241i}{58}$.

Стр. 209.

a) $1,099 + 0.455i$; $-1,099 - 0,455i$.

b) $2,95 - 0,85i$; $-2,95 + 0,85i$.

c) $4,41 - 0,68i$; $-4,41 + 0,68i$.

$x_1 = \frac{2+i}{1+i}$; $x_2 = 3 - 2i$.

41, стр. 216.

. $\sqrt{2}\left(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}\right)$; $\sqrt{2}\left(\cos\frac{7\pi}{4}+i\sin\frac{7\pi}{4}\right)$.

7,28 $(\cos 15°57'+i\sin 15°57')$; 14,86 $(\cos 312°17'+i\sin 312°17')$.

2. 10 $\sqrt{2}(\cos 75°+i\sin 75°)$; $5(\cos 210°+i\sin 210°)$.

3. $-\varphi$.

4. $[r(\cos\varphi+i\sin\varphi)]^{-n}=\frac{1}{[r(\cos\varphi+i\sin\varphi)]^{n}}=$

$=\frac{1}{r^{n}(\cos n\varphi+i\sin n\varphi)}=\frac{r^{-n}(\cos n\varphi-i\sin n\varphi)}{\cos^2 n\varphi+\sin^2 n\varphi}=$

$=r^{-n}[\cos(-n\varphi)+i\sin(-n\varphi)]$.

5. $\cos 5\varphi=\cos^5\varphi-10\cos^3\varphi\sin^2\varphi+5\cos\varphi\sin^4\varphi$;

$\sin 5\varphi=5\cos^4\varphi\sin\varphi-10\cos^2\varphi\sin^3\varphi+\sin^5\varphi$.

6. $\sqrt[4]{1-8i}\approx 1{,}3(\cos 40°+i\sin 40°)$.

§ 44, стр. 237.

a) $F=x_1^2x_2+x_1x_2^2+2x_1^2+2x_1x_2+2x_1$. b) $H=x_1^2-x_1x_2$.

§ 47, стр. 252.

a) i, $-i$. b) $\frac{1+i}{\sqrt{2}}$; $\frac{1-i}{\sqrt{2}}$; $\frac{-1+i}{\sqrt{2}}$; $\frac{-1-i}{\sqrt{2}}$.

c) $\cos\frac{\pi}{5}+i\sin\frac{\pi}{5}$; $\cos\frac{3\pi}{5}+i\sin\frac{3\pi}{5}$; $\cos\frac{7\pi}{5}+i\sin\frac{7\pi}{5}$;

$\cos\frac{9\pi}{5}+i\sin\frac{9\pi}{5}$.

d) $\frac{\sqrt{3}}{2}+\frac{1}{2}i$; $-\frac{\sqrt{3}}{2}+\frac{1}{2}i$; $\frac{\sqrt{3}}{2}-\frac{1}{2}i$; $-\frac{\sqrt{3}}{2}-\frac{1}{2}i$.

4, стр. 253.

$\varphi(18)=6$; $\varphi(30)=8$; $\varphi(100)=40$; $\varphi(5896)=2640$.

§ 48, стр. 263.

a) $x_1\approx 0{,}454$; $x_2\approx -0{,}227+1{,}468i$; $x_3\approx -0{,}227-1{,}468i$.

b) $x_1=1$; $x_2=x_3=-2$.

c) $x_1\approx 0{,}229$; $x_2\approx 1{,}385+1{,}564i$; $x_3\approx 1{,}385-1{,}564i$.

d) $x_1=x_2=1$; $x_3=\frac{-1+\sqrt{13}}{2}$; $x_4=\frac{-1-\sqrt{13}}{2}$.

§ 50, стр. 269.

a) $R(f,g)=-89$. b) $R(f,g)=21923$.

§ 51, стр. 271.

a) $26y^6-90y^5-239y^4+49y+124=0$.

$21y^4-160y^3+147y^2+311=0$.

ЛИТЕРАТУРА

Виноградов С. П., Основания теории детерминантов. М.—Л., 1935
Нетто Е., Начала теории определителей, Одесса, 1912.
Каган В. Ф., Основания теории определителей, Гиз, 1922.
Шапиро Г., Высшая алгебра, Учпедгиз, 1938.
Млодзеевский Б. К., Основы высшей алгебры, Гиз, М.—Л., 1923.
Граве Д. А., Элементы высшей алгебры, Киев, 1914.
Сушкевич А. К., Основы высшей алгебры, Гостехиздат, М.—Л., 1941.
Чезаро Э., Элементарный учебник алгебраического анализа и исчисл бесконечно малых, ГТТИ, 1936.
Бохер М., Введение в высшую алгебру, ГТТИ, 1934.
Шрейер и Шпернер Э., Введение в линейную алгебру, ГТТИ, 19
Баумгартнер Л., Теория групп, ГТТИ, 1933.
Шмидт О. Ю., Абстрактная теория групп, ГТТИ, 1933.
Чеботарёв Н. Г., Основы теории Галуа, ч. I, 1934, ч. II, 1938.
Ван-дер-Варден Б. А., Современная алгебра, т. I, II, ГТТИ.
Сушкевич А. К., Теория обобщённых групп, 1937.
Шрейер О. и Шпернер Е., Теория матриц, ОНТИ, 1936.
Чеботарёв Н. Г., Теория Галуа, ОНТИ, 1936.
Weber H., Lehrbuch der Algebra, Braunschweig, т. I—III.
Dickson L. E., Algebren und ihre Zahlentheorie, Zürich—Leipzig,
Диксон Л. Е., Линейные алгебры, 1935.
Hasse H., Höhere Algebra, Berlin—Leipzig, том I—II.
Haupt O., Einführung in die Algebra, Leipzig, 1929.
Steinitz E., Algebraische Theorie der Körper. Neuherausg. von R. u. Hasse, Berlin—Leipzig, 1930.
Wedderburn J. H. M., Lectures on Matrices, New-York, 1934.
Журавский А. М., Сборник задач по высшей алгебре, ГТТИ, 19