ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н. Г.
ЧЕРНЫШЕВСКОГО»

А. М. Водолазов, О.А. Королева, В.В. Кривобок, Е.В. Сецинская

А Л Г Е Б Р А.

ЧАСТЬ I

Аннотация. В учебном пособии отражены основные темы первого семестра курсов «Алгебра» и «Алгебра и теория чисел»: определители, координатное линейное пространство, системы линейных уравнений, алгебра матриц, комплексные числа.

Для студентов младших курсов механико-математического факультета и факультета компьютерных наук и информационных технологий, изучающих курсы «Алгебра» и «Алгебра и теория чисел».

СОДЕРЖАНИЕ

Введение

Учебное пособие соответствует материалу, изучаемому студентами первого курса в курсе «Алгебра» механико-математического факультета, а также студентами первого курса факультета компьютерных наук и информационных технологий в курсах «Алгебра» и «Алгебра и теория чисел». В данном пособии отражены темы, рассматриваемые в первом семестре: определители, координатное линейное пространство, системы линейных уравнений, алгебра матриц, комплексные числа, многочлены.

Учебное пособие содержит курс лекций по предлагаемым разделам и может быть использовано при подготовке к экзамену по предметам «Алгебра» и «Алгебра и теория чисел» в первом семестре, а так же при самостоятельной работе студентов, обучающихся по заочной форме обучения.

Для более подробного изучения теоретического материала может быть рекомендована следующая литература:

1. *Воеводин В.В.* Линейная алгебра. М., 1974.
2. *Курош А.Г.* Курс высшей алгебры. М., 1975.
3. *Ильин В.А., Позняк Э.Г.* Линейная алгебра. М., 1978.
4. *Проскуряков И.В.* Сборник задач по линейной алгебре. М., 1970.
5. *Фадеев Д.К., Соминский И.С.* Сборник задач по высшей алгебре. М., 1968.

Глава 1

Определители

1.1. Числовые кольца и поля

Пусть $\mathbb{R}$ — множество действительных чисел и $k \subset \mathbb{R}$.

Определение 1.1.1. Числовое множество k называется числовым кольцом, если оно содержит сумму, разность и произведение двух любых своих чисел.

Пусть k — числовое кольцо и $a, b \in k$, то $a+b,\ a-b,\ a \cdot b \in k$.

Пример:

1. $k = \{0\}$ — тривиальное (нулевое) кольцо;
2. $k = \mathbb{Z} = \{0; \pm 1; \pm 2 \ldots\}$;
3. $k = \mathbb{Q} = \left\{ \frac{a}{b} \middle| \, a, b \in \mathbb{Z},\ b \neq 0 \right\}$;
4. $k = \mathbb{R}$;
5. $k = 2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$;
6. $k = \left\{ \sqrt{a + b\sqrt{2}} \middle| \, a, b \in \mathbb{Z}(\mathbb{Q}) \right\}$.

Свойства числовых колец

1. Любое числовое кольцо содержит ноль.

   Пусть k — числовое кольцо и $a \in k$, тогда $(a-a) \in k$, следовательно $0 \in k$.

Следствие. Нулевое кольцо является наименьшим, так как оно содержится в любом числовом кольце.

2. Если $a \in k$, то и $(-a) \in k$.
   Так как $a \in k$ и $0 \in k$, то $(0 - a) \in k$, следовательно $(-a) \in k$.

3. Если $a \in k$, то $(\forall\ n \in \mathbb{Z})\ na \in k$.
   Пусть $n \in \mathbb{N}$, тогда $na = \underbrace{a + a + ... + a}_{n \text{ раз}} \in k$.
   Если $n = 0$, то $na = 0 \cdot a = 0 \in k$.
   Если $n = -m,\ m \in \mathbb{N}$, то $na = (-m)a = -ma \in k$.

   Следствие. Ненулевое числовое кольцо содержит бесконечное множество элементов.

Определение 1.1.2. Ненулевое числовое кольцо k называется числовым полем, если оно содержит частное двух любых своих чисел (знаменатель отличен от нуля).

Если k — числовое поле, и $a, b \in k$, то $a+b,\ a-b,\ a \cdot b,\ \frac{a}{b} \in k,\ (b \neq 0)$.
Пример:

1. $k = \mathbb{Q}$;
2. $k = \mathbb{R}$;
3. $k = \left\{ \sqrt{a + b\sqrt{2}} \,\middle|\, a, b \in \mathbb{Q} \right\}$.

ТЕОРЕМА 1.1.1. *Поле рациональных чисел $\mathbb{Q}$ содержится в любом числовом поле k.*

Доказательство. Пусть k — любое числовое поле и $a \in k,\ a \neq 0$, тогда $\frac{a}{a} \in k$, то есть $1 \in k$. Так как k является числовым кольцом, то по свойству 3, $(\forall\ n \in \mathbb{Z})\ n \cdot 1 \in k$, следовательно $\mathbb{Z} \subset k$, следовательно $\left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z},\ b \neq 0 \right\} \subset k$, то есть $\mathbb{Q} \subset k$. □

1.2. Перестановки

Пусть M — конечное множество из n элементов. В интересующих нас вопросах природа элементов M не имеет значения, поэтому вместо элементов множества M будем иметь дело с их номерами. $M = \{1, 2, \ldots, n\}$. Эти числа можно располагать в различном порядке, например в порядке возрастания (естественном, нормальном, каноническом).

Определение 1.2.1. Любое расположение чисел $\{1, 2, 3, ..., n\}$ в какомлибо определенном порядке, называется перестановкой из n чисел (символов, индексов).

Пример:
$M = \{1, 2, 3\}$
$(1, 2, 3)$ — естественная перестановка,
$(2, 1, 3), (3, 1, 2), (1, 3, 2), (2, 3, 1), (3, 2, 1)$.

Общий вид перестановки из n чисел: $(i_1, i_2, ..., i_n)$, $1 \leqslant i_s \leqslant n$, $i_s \neq i_t$ при $i \neq t$ (все числа различны).

ТЕОРЕМА 1.2.1. *Количество всевозможных перестановок из n чисел равно произведению* $1 \cdot 2 \cdot 3 \cdot \ldots \cdot n = n!$.

Доказательство. Рассмотрим перестановку из n чисел общего вида: $(i_1, i_2, i_3, ..., i_n)$, i_1 можно выбрать n способами. Зафиксируем i_1. i_2 при фиксированном i_1 можно выбрать $n - 1$ способами. Пару (i_1, i_2) можно выбрать $n(n-1)$ способами. Зафиксируем пару (i_1, i_2). i_3 можно выбрать $n-2$ способами. Тройку (i_1, i_2, i_3) можно выбрать $n(n-1)(n-2)$ способами и так далее. $(i_1, i_2, i_3, ..., i_n)$ можно выбрать $n(n-1)(n-2)\cdot\ldots\cdot 2\cdot 1 = n!$ способами. □

Определение 1.2.2. Говорят, что числа i и j образуют инверсию (беспорядок) в перестановке, если $i > j$, но i стоит в перестановке раньше j.

Пример:
в перестановке $(4, 2, 3, 1)$, 4 и 2, 4 и 3, 4 и 1, 2 и 1, 3 и 1 — инверсии.

Определение 1.2.3. Перестановка называется четной или нечетной, в зависимости от того, четное или нечетное число инверсий образуют индексы этой перестановки.

Пример:

1. $(1, 2, 3, ..., n)$ — четная перестановка;

2. $(4, 2, 3, 1)$ — нечетная перестановка;

Определение 1.2.4. Транспозицией в перестановке называется взаимное перемещение каких-либо двух ее индексов.

Пример:
$(4, 2, 3, 1)$ переходит в $(3, 2, 4, 1)$ с помощью одной транспозиции.
В общем случае $(\ldots, i, \ldots, j, \ldots)$ переходит в $(\ldots, j, \ldots, i, \ldots)$.

ТЕОРЕМА 1.2.2. *Одна транспозиция меняет тип перестановки на противоположный.*

Доказательство. Рассмотрим два случая:
а) транспонируемые индексы стоят рядом

$$(..., i, j, ...) \to (...j, i, ...).$$

Ясно, что в этих перестановках индексы i и j образуют одни и те же инверсии с индексами, остающимися на месте. Поэтому количество инверсий будет зависеть только от взаимного расположения индексов i и j. Если $i < j$, то в первой перестановке они не образуют инверсии, а во второй она появляется и, следовательно, число инверсий увеличивается на 1. Если $i > j$, то в первой перестановке они образуют инверсию, а во второй она пропадает и, следовательно, число инверсий уменьшается на

1. В обоих случаях четность перестановки меняется на противоположную.

б) между транспонированными индексами стоят s индексов

$$(\ldots, i, i_1, i_2, \ldots, i_s, j, \ldots)\ (A) \to (\ldots, j, i_1, i_2, \ldots, i_s, i, \ldots)\ (B).$$

Покажем, что от перестановки (A) к перестановке (B) можно перейти с помощью $2s+1$ транспозиций соседних индексов. Для этого в перестановке (A) транспонируем последовательно i и i_1, затем i и i_2,..., i и i_s, i и j, после этого получим $(\ldots, i_1, i_2, ..., i_s, j, i, \ldots)$ (C). Чтобы перейти от (A) к (C) нужно осуществить $s+1$ транспозиций. В перестановке (C) транспонируем последовательно j и i_s, затем j и i_{s-1},...,j и i_1. После этого получаем перестановку (B). Чтобы перейти от (C) к (B) нужно осуществить s транспозиций соседних индексов. Итак, чтобы перейти от (A) к (B) нужно осуществить $2s+1$ транспозиций соседних индексов. Это нечетное число. Мы нечетное число раз меняем четность перестановки. Следовательно, перестановки (A) и (B) имеют противоположные четности. □

Следствие. Если $n \geqslant 2$, то количество четных перестановок из n символов равно количеству нечетных и равно $\frac{n!}{2}$.

Доказательство. Выпишем все $n!$ перестановок из n чисел

$$(1, 2, \ldots), (2, 1, \ldots), \ldots, (\ldots, 2, 1).$$

Обозначим через p — количество четных перестановок, а через q — количество нечетных перестановок, $p + q = n!$. Во всех перестановках транспонируем любые два числа. Например 1 и 2

$$(2, 1, \ldots), (1, 2, \ldots), \ldots, (\ldots, 1, 2).$$

Получим те же самые $n!$ перестановок, записанных уже в другом порядке. p — количество нечетных перестановок, q — количество четных

перестановок. Отсюда видно, что $p = q$. То есть $p + q = 2p = n!$, следовательно $p = q = \frac{n!}{2}$. □

1.3. Квадратные матрицы и определители

Определение 1.3.1. Квадратной матрицей порядка n называется таблица из n^2 чисел a_{ij} записанных в виде n-строк и n-столбцов.

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}. \tag{1.1}$$

Числа a_{ij} называются элементами матрицы A. Элементы снабжены двумя индексами. Первый индекс указывает на номер строки, а второй индекс на номер столбца, на пересечении которых стоит данный элемент. В матрице A выделяем две диагонали. Главная диагональ: $(a_{11}, a_{22}, \dots, a_{nn})$. Побочная диагональ: $(a_{1n}, a_{2\ n-1}, \dots, a_{n1})$. Матрицу (1.1) можно записать: $A = (a_{ij}),\ 1 \leqslant i, j \leqslant n$.

Определение 1.3.2. Транспонированием матрицы A называется такое преобразование этой матрицы, при которой ее строки становятся столбцами с теми же самыми номерами.

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

Матрица A' называется матрицей, транспонированной к матрице A. Если элементы матрицы A' обозначить a'_{ij}, то $a'_{ij} = a_{ji}$, $1 \leqslant i, j \leqslant n$. Ясно, что $(A')' = A$.

Рассмотрим произведение n-элементов матрицы A, взятых по одному из каждой строки и каждого столбца этой матрицы.

$$a_{1i_1} \cdot a_{1i_2} \cdot \ldots \cdot a_{ni_n}, \tag{1.2}$$

где $(i_1, i_2, \ldots, i_n)$ — перестановка из индексов столбцов (1,2,...,n).

Таких произведений вида (1.2) можно составить $n!$ штук. Все эти произведения в дальнейшем будут называться членами определителя n-порядка. Каждому члену (1.2) будем приписывать знак $(-1)^t$, где t — количество инверсий в перестановке $(i_1, i_2, \ldots, i_n)$. Таким образом приписываем знак «+» или «−» в зависимости от того, четную или нечетную перестановку образуют индексы столбцов элементов члена.

Определение 1.3.3. Определителем n-порядка соответствующего квадратной матрице A называется алгебраическая сумма $n!$ членов, каждый из которых состоит из произведения n-элементов матрицы A, взятых по одному из каждой строки и из каждого столбца, при этом каждому члену приписывается знак «+» или «−», в зависимости от того, четную или нечетную перестановку образуют вторые индексы элементов члена, при условии, что первые индексы идут в порядке следования строк в матрице.

$$|A| = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} = detA \text{ (детерминант матрицы } A).$$

Рассмотрим член определителя

$$a_{i_1 j_1} \cdot a_{i_2 j_2} \cdot \ldots \cdot a_{i_n j_n}. \tag{1.3}$$

С каким знаком этот член входит в состав определителя?

ТЕОРЕМА 1.3.1 (о знаке члена определителя)**.** *Член (1.3) входит в состав определителя n-порядка со знаком* $(-1)^{(s+t)}$*, где* s *— число инверсий в перестановке индексов строк* $(i_1, i_2, \ldots, i_n)$*, а* t *— число инверсий в перестановке индексов столбцов* $(j_1, j_2, \ldots, j_n)$*.*

Доказательство. Заметим, что четность числа $s+t$ не меняется, если мы в члене (1.3) поменяем местами каких-либо два элемента. Действительно, поменяем местами первые два элемента $a_{i_2 j_2}, a_{i_1 j_1}, \ldots, a_{i_n j_n}$. Обозначим s' — число инверсий в перестановке первых индексов $(i_2, i_1, \ldots, i_n)$, t' — число инверсий в перестановке вторых индексов $(j_2, j_1, \ldots, j_n)$. Чем отличается s от s'? Числа s и s' имеют различные четности (по теореме 1.2.2). t и t' имеют так же противоположные четности (по теореме 1.2.2). Рассмотрим разность $(s'+t')-(s+t) = (s'-s)+(t'-t) =$ нечетное число $+$ $+$ нечетное число $=$ четное число. Таким образом $s'+t'$ и $s+t$ имеют одинаковую четность. В члене (1.3) расположены элементы в порядке следования строк. Получим $a_{1\alpha_1}, a_{1\alpha_2}, \ldots, a_{n\alpha_n}$. По определению 1.3 этот член входит в состав определителя со знаком $(-1)^{t'}$, где t' — число инверсий в перестановке $(\alpha_1, \alpha_2, \ldots, \alpha_n)$. В этом случае $s' = 0$, так как в перестановке $(1, 2, \ldots, n)$ инверсий нет. По только что доказанному, числа $s'+t'$ и $s+t$ имеют одинаковые четности, поэтому $(-1)^{s'+t'} = (-1)^{s+t}$. Так как $s' = 0$, получаем $(-1)^{t'} = (-1)^{s+t}$. □

1.4. Свойства определителя

1. *Равноправие строк и столбцов.*

   Величина определителя не меняется при транспонировании.

   Действительно, рассмотрим определитель

$$|A| = \Delta = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}, \quad |A'| = \Delta_1 = \begin{vmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{vmatrix}.$$

Рассмотрим общий член определителя Δ

$$a_{1i_1} \cdot a_{2i_2} \cdot \ldots \cdot a_{ni_n}. \tag{1.4}$$

Видно, что элементы произведения (1.4) и в определителе Δ_1 стоят в различных строках и в различных столбцах, поэтому произведение (1.4) является членом определителя Δ_1. Следовательно, любой член определителя Δ является и членом определителя Δ_1. Верно и обратное: каждый член определителя Δ_1 является членом определителя Δ. Таким образом Δ и Δ_1 состоят из одних и тех же членов. Покажем, что знаки одинаковых членов в составе Δ и Δ_1 совпадают. Знак члена (1.4) в составе Δ (по определению 1.3.3) $(-1)^t$, где t — число инверсий в перестановке вторых индексов $i_1, i_2, \dots, i_n$. Знак члена (1.4) в составе Δ_1 (по теореме 1.3.1) совпадает со знаком $(-1)^{s'+t'}$, где s' — число инверсий в перестановке индексов строк $(i_1, i_2, \dots, i_n)$, t' — число инверсий в перестановке индексов столбцов (1,2,. . .,n). $s' = t,\ t' = 0,\ (-1)^{t+0} = (-1)^t$. Итак, знаки одинаковых членов в составе Δ и Δ_1 совпадают, и поэтому $\Delta = \Delta_1$.

Замечание 1.4.1. Если строки определителя обладают каким-либо свойством ε, то это свойство ε справедливо и для столбцов определителя. Для этого достаточно, не меняя значения определителя, транспонировать его, при этом строки его становятся столбцами. Так как при транспонировании обратно его столбцы становятся строками, то и любое свойство столбцов определителя справедливо для его строк. Поэтому в дальнейшем все свойства определителя будем формули-

ровать для его строк, имея в виду, что оно будет справедливо и для его столбцов.

2. *Знакопеременность.*

Если в определителе взаимно поменять местами какие-либо две его строки, то определитель изменит лишь знак на противоположный.

Рассмотрим общий член определителя Δ

$$a_{1k_1} \cdot \ldots \cdot a_{ik_i} \cdot \ldots \cdot a_{jk_j} \cdot \ldots \cdot a_{nk_n}. \tag{1.5}$$

Видно, что все элементы произведения (1.5) находятся в различных строках и различных столбцах определителя Δ_1. Поэтому произведение (1.5) является членом определителя Δ_1. Следовательно, любой член определителя Δ является членом определителя Δ_1. Верно и обратное: каждый член определителя Δ_1 является членом определителя Δ. Таким образом Δ и Δ_1 состоят из одних и тех же членов. Покажем, что знаки одинаковых членов в Δ и Δ_1 являются противоположными. Знак члена (1.5) в составе Δ совпадает со знаком $(-1)^t$, где t — число инверсий в перестановке вторых индексов $(k_1, \ldots, k_i, \ldots, k_j, \ldots, k_n)$. Рассмотрим произведение (1.5), как член определителя Δ_1: $a_{1k_1} \cdot \ldots \cdot a_{jk_j} \cdot \ldots \cdot a_{ik_i} \cdot \ldots \cdot a_{nk_n}$. Знак этого члена в составе Δ_1 (по определению 1.3.3) совпадает со знаком $(-1)^{t'}$, где t' — число инверсий в перестановке вторых индексов $(k_1 \ldots k_j \ldots k_i \ldots k_n)$. По теореме 1.2.2 числа t и t' имеют противоположные четности, значит знаки $(-1)^t$ и $(-1)^{t'}$ являются противоположными. Итак, Δ и Δ_1 состоят из одних и тех же членов, но знаки одинаковых членов в их составе являются противоположными. Следовательно, $\Delta_1 = -\Delta$.

3. Определитель с двумя одинаковыми строками равен нулю.

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \overset{\text{св-во } 2}{=} - \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = -\Delta.$$

$\Delta = -\Delta \ \Rightarrow 2\Delta = 0 \Rightarrow \Delta = 0.$

4. *Однородность.*

Если все элементы некоторой строки определителя имеют общий множитель, то этот общий множитель может быть вынесен за знак определителя.

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ ca_{i1} & ca_{i2} & \dots & ca_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} =$$

$= \text{алгебраическая сумма}\big\{(-1)^k a_{1k_1} \dots c \cdot a_{ik_i} \dots a_{nk_n}\big\} =$

$= c\cdot\text{алгебраическая сумма}\big\{(-1)^k a_{1k_1} \dots a_{ik_i} \dots a_{nk_n}\big\} =$

$$= c \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

5. Если одна из строк определителя состоит из нулей, то этот определитель равен нулю.

Достаточно в свойстве 4 положить $c = 0$.

Определение 1.4.1. Две строки определителя называются пропорциональными, если все элементы одной строки получаются из соответствующих элементов другой строки умножением на некоторое число.

6. Определитель с двумя пропорциональными строками равен нулю.

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ ka_{i1} & ka_{i2} & \dots & ka_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \overset{\text{св-во 4}}{=} k \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \overset{\text{св-во 3}}{=}$$

$= k \cdot 0 = 0.$

7. *Аддитивность.*

Если все элементы i-й строки определителя Δ представлены в виде суммы двух слагаемых, то этот определитель может быть представлен в виде суммы двух определителей, все элементы которых, кроме элементов i-й строки, совпадают с элементами определителя Δ, а в i-й строке первого определителя стоят первые слагаемые, в i-й строке второго определителя — вторые слагаемые элементов i-й строки определителя Δ.

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a'_{i1} + a''_{i1} & a'_{i2} + a''_{i2} & \dots & a'_{in} + a''_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} =$$

$= \text{алгебраическая сумма}\big\{(-1)^t a_{1k_1} \dots (a'_{ik_i} + a''_{ik_i}) \dots a_{nk_n}\big\} =$

$= \text{алгебраическая сумма}\big\{(-1)^t a_{1k_1} \dots a'_{ik_i} \dots a_{nk_n} + (-1)^t \times$

$a_{1k_1} \dots a''_{ik_i} \dots a_{nk_n}\} =$ алгебраическая сумма$\{(-1)^t a_{1k_1} \dots a'_{ik_i} \dots a_{nk_n}\} +$
$+$ алгебраическая сумма$\{(-1)^t a_{1k_1} \dots a''_{ik_i} \dots a_{nk_n}\} =$

$$= \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a'_{i1} & a'_{i2} & \dots & a'_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ \dots & \dots & \dots & \dots \\ a''_{i1} & a''_{i2} & \dots & a''_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Замечание 1.4.2. Свойство 7 легко распространяется на случай, когда все элементы i-й строки представлены в виде суммы m слагаемых ($m > 2$).

Определение 1.4.2. Говорят, что i-я строка определителя является линейной комбинацией остальных его строк, если существуют числа $k_1, \dots, k_{i-1}, k_{i+1}, \dots, k_n$ такие, что

$$(i) = k_1(1) + \dots + k_{i-1}(i-1) + k_{i+1}(i+1) + \dots + k_n(n).$$

Сложение строк понимается так, что складываются элементы, стоящие в одном и том же столбце.

Если не все числа k_j отличны от нуля, то i-я строка является линейной комбинацией только нескольких строк определителя. Если только одно число k_j не равно нулю, то получаем $(i) = k_j(j)$ — случай пропорциональных строк определителя. Ясно, что нулевая строка является линейной комбинацией других строк, в этом случае все коэффициенты $k_1 = \dots = k_{i-1} = k_{i+1} = \dots = k_n = 0$.

8. Если в определителе одна из строк является линейной комбинацией других его строк, то такой определитель равен нулю.
Пусть в определителе Δ i-я строка есть линейная комбинация $(i) =$
$= k_1(i_1) + k_2(i_2) + \dots + k_s(i_s)$.

$$\begin{vmatrix} \dots \\ (i_1) \\ \dots \\ (i_2) \\ \dots \\ k_1(i_1)+\ldots+k_s(i_s) \\ \dots \\ (i_s) \\ \dots \end{vmatrix} \overset{\text{св-во 7}}{=} \begin{vmatrix} \dots \\ (i_1) \\ \dots \\ (i_2) \\ \dots \\ k_1(i_1) \\ \dots \\ (i_s) \\ \dots \end{vmatrix} + \begin{vmatrix} \dots \\ (i_1) \\ \dots \\ (i_2) \\ \dots \\ k_2(i_2) \\ \dots \\ (i_s) \\ \dots \end{vmatrix} + \ldots + \begin{vmatrix} \dots \\ (i_1) \\ \dots \\ (i_2) \\ \dots \\ k_s(i_s) \\ \dots \\ (i_s) \\ \dots \end{vmatrix} \overset{\text{св-во 6}}{=}$$

$$= 0 + 0 + \ldots + 0 = 0$$

9. Величина определителя не изменится, если ко всем элементам его некоторой строки прибавить соответствующие элементы другой строки, умноженные на одно и то же число.

$$\Delta = \begin{vmatrix} \dots \\ (i) \\ \dots \\ (j) \\ \dots \end{vmatrix} + \begin{vmatrix} \dots \\ (i)+(j) \\ \dots \\ (j) \\ \dots \end{vmatrix} = \begin{vmatrix} \dots \\ (i) \\ \dots \\ (j) \\ \dots \end{vmatrix} + \begin{vmatrix} \dots \\ (j) \\ \dots \\ (j) \\ \dots \end{vmatrix} \overset{\text{св-во 3}}{=} \Delta + 0 = \Delta.$$

Замечание 1.4.3. Свойство 9 можно высказать более общей формой, а именно: величина определителя не изменится, если к одной из его строк прибавить любую линейную комбинацию других его строк.

1.5. Теорема Лапласа

Определение 1.5.1. Пусть даны матрица или определитель порядка n и натуральное число k, $1 \leqslant k \leqslant n$. Минором k-го порядка данной матрицы или определителя называется определитель, порожденный матрицей,

составленной из элементов, стоящих на пересечении любых k-строк и k-столбцов этой матрицы.

Определение 1.5.2. Пусть дан определитель Δ n-порядка и в нем минор M порядка k. Дополнительным минором для минора M называется минор $(n-k)$-го порядка, порожденный матрицей, составленной из элементов тех строк и столбцов, которые не вошли в исходный минор M.

$\widetilde{M}$ — дополнительный минор для M. Ясно, что дополнительным минором для $\widetilde{M}$ будет M. Поэтому можно говорить о паре взаимно дополнительных миноров.

Определение 1.5.3. Алгебраическим дополнением к M определителя Δ называется его дополнительный минор $\widetilde{M}$, взятый со знаком «+» или «−», в зависимости от того, четной или нечетной является сумма номеров строк и столбцов, на пересечении которых находится данный минор M.

A_M — алгебраическое дополнение минора M. Определение 1.5.3 означает, что

$$A_M = (-1)^{S_M} \cdot \widetilde{M},$$

где S_M — сумма номеров строк и столбцов, $S_M = i_1 + i_2 + \ldots + i_k + j_1 + +j_2 + \ldots + j_k$; $i_1, i_2, \ldots, i_k$ — номера строк, $j_1, j_2, \ldots, j_k$ — номера столбцов минора M.

ТЕОРЕМА 1.5.1 (Лапласа)**.** *Пусть дан определитель Δ порядка n и в нем выбрано k-строк, $1 \leqslant k \leqslant n$. Тогда определитель Δ равен сумме произведений всевозможных миноров k-го порядка, составленных из выбранных k-строк, на их алгебраические дополнения, то есть*

$$\Delta = M_1 \cdot A_{M_1} + M_2 \cdot A_{M_2} + \ldots + M_s \cdot A_{M_s}.$$

Положим в теореме Лапласа $k = 1$, то есть выбираем одну i-ю строку $(a_{i1}, a_{i2}, \ldots, a_{in}) = (M_1, M_2, \ldots, M_n)$. Через M_{ij} обозначим дополни-

тельный минор для элемента a_{ij}. M_{ij} — минор $(n-1)$-го порядка, получающийся из определителя Δ вычеркиванием i-строки и j-столбца. Алгебраическое дополнение a_{ij} будет $A_{ij} = (-1)^{i+j} \cdot M_{ij}$.

Следствие 1.5.1.1. Определитель равен сумме произведений всех его элементов некоторой строки на их алгебраические дополнения, то есть

$$\Delta = a_{i1} \cdot A_{i1} + a_{i2} \cdot A_{i2} + \ldots + a_{in} \cdot A_{in}.$$

Следствие 1.5.1.2. Пусть дан определитель Δ порядка n и произвольный набор чисел $b_1, b_2, \ldots, b_n$. Тогда сумма произведений чисел $b_1, b_2, \ldots, b_n$ на алгебраические дополнения соответственных элементов i-строки определителя Δ равна новому определителю, получающемуся из определителя Δ заменой элементов i-строки числами $b_1, b_2, \ldots, b_n$.

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{i1} & a_{i2} & \ldots & a_{in} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix};$$

$$\Delta_1 = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ b_1 & b_2 & \ldots & b_n \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} = b_1 \cdot A_{b_1} + b_2 \cdot A_{b_2} + \ldots + b_n \cdot A_{b_n} =$$

$$= b_1 \cdot A_{i1} + b_2 \cdot A_{i2} + \ldots + b_n \cdot A_{in}.$$

Следствие 1.5.1.3. Сумма произведений всех элементов в некоторой строке определителя на алгебраические дополнения соответствующих элементов в другой ето строке равна нулю.

Действительно, $b_1 = a_{k1},\ b_2 = a_{k2}, \ldots,\ b_n = a_{kn}$, где $k \neq i$. Получим,

$$a_{k1} \cdot A_{i1} + a_{k2} \cdot A_{i2} + \ldots + a_{kn} \cdot A_{in} = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{k1} & a_{k2} & \ldots & a_{kn} \\ \ldots & \ldots & \ldots & \ldots \\ a_{k1} & a_{k2} & \ldots & a_{kn} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} \begin{matrix} \\ \\ (i) \\ \\ (k) \\ \\ \\ \end{matrix} = 0.$$

1.6. Обозначения

Ради краткости в математике принимают следующие обозначения

$$a_1 + a_2 + \ldots + a_n = \sum_{i=1}^{n} a_i, \qquad a_1 \cdot a_2 \cdot \ldots \cdot a_n = \prod_{i=1}^{n} a_i.$$

1. $\sum\limits_{i=1}^{n} a_i = \sum\limits_{j=1}^{n} a_j$;
2. $\sum\limits_{i=1}^{n} ca_i = c \cdot \sum\limits_{i=1}^{n} a_i$;
3. $\sum\limits_{i=1}^{n} (a_i + b_i) = \sum\limits_{i=1}^{n} a_i + \sum\limits_{i=1}^{n} b_i$;
4. $\prod\limits_{i=1}^{n} a_i = \prod\limits_{j=1}^{n} a_j$;
5. $\prod\limits_{i=1}^{n} ca_i = c^n \cdot \prod\limits_{i=1}^{n} a_i$;
6. $\prod\limits_{i=1}^{n} a_i b_i = \prod\limits_{i=1}^{n} a_i \cdot \prod\limits_{i=1}^{n} b_i$;

Подсчитаем сумму чисел a_{ij}, $1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m$. Зафиксируем i:

$$a_{i1} + a_{i2} + \ldots + a_{im} = \sum_{j=1}^{m} a_{ij}.$$

$$\sum_{j=1}^{m} a_{1j} + \sum_{j=1}^{m} a_{2j} + \ldots + \sum_{j=1}^{m} a_{nj} = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij} = S.$$

Зафиксируем j:

$$a_{1j} + a_{2j} + \ldots + a_{nj} = \sum_{i=1}^{n} a_{ij}.$$

$$S = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij}; \qquad \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij} = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij}.$$

В конечном двойном суммировании можно переставлять знаки суммирования.

$$\Delta = \sum_{(i_1,i_2,\ldots,i_n)} (-1)^{t_i} a_{1i_1} a_{2i_2} \ldots a_{ni_n}.$$

Суммирование ведется по всем перестановкам. t_i — число инверсий в перестановке $(i_1, i_2, \ldots, i_n)$.

Следствие 1.5.1.1 можно записать как

$$\Delta = \sum_{j=1}^{n} a_{ij} \cdot A_{ij}.$$

Следствие 1.5.1.3 можно записать как

$$\sum_{j=1}^{n} a_{kj} \cdot A_{ij} = 0, \quad k \neq i.$$

Рассмотрим символ Кронекера:

$$\delta_{ik} = \begin{cases} 1, & \text{если } i = k; \\ 0, & \text{если } i \neq k. \end{cases}$$

Следствия 1.5.1.1 и 1.5.1.3 можно записать следующим образом

$$\sum_{j=1}^{n} a_{kj} \cdot A_{ij} = \delta_{ki}\Delta.$$

Глава 2

Координатное линейное пространство

2.1. n-мерные векторы и действия над ними

Пусть k — некоторое фиксированное числовое поле, которое называется основным. Элементы поля k будем обозначать греческими буквами $\alpha, \beta, \gamma, \alpha_1, \alpha_2, \ldots$ — скалярные элементы.

Определение 2.1.1. n-мерным вектором над полем k называется любая упорядоченная совокупность n-чисел поля k.

Обозначать векторы будем маленькими латинскими буквами $a, b, c, a_1, a_2, \ldots$

$a = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $b = (\beta_1, \beta_2, \ldots, \beta_n)$ — упорядоченная совокупность n-чисел поля k. Множество всех n-мерных векторов над полем k будем обозначать

$$k^n = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) \mid \alpha_i \in k\}.$$

Определение 2.1.2. Координатами вектора a называются числа, из которых состоит этот вектор a.

$\alpha_1, \alpha_2, \ldots, \alpha_n$ — координаты вектора a.

Определение 2.1.3. Два вектора $a = (\alpha_1, \ldots, \alpha_n)$ и $b = (\beta_1, \ldots, \beta_n)$ называются равными, если равны все их соответственные координаты, то есть

$$(\forall\ 1 \leqslant i \leqslant n) \quad \alpha_i = \beta_i.$$

Пример:

1. Строки (столбцы) квадратной матрицы A n-порядка могут быть рассмотрены как n-мерные векторы.

2. Вся квадратная матрица A n-порядка может быть рассмотрена как n^2-мерный вектор. Для этого достаточно выписать строки этой матрицы одну за другой (получится n^2-вектор).

Определение 2.1.4. Суммой двух векторов a и b называется вектор $a + b$, координаты которого равны суммам соответственных координат векторов a и b.

$$a + b = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_n + \beta_n).$$

Определение 2.1.5. Произведением вектора a на число α называется вектор αa, координаты которого равны соответственным координатам вектора a, умноженных на число α.

$$\alpha a = (\alpha a_1, \alpha a_2, \ldots, \alpha a_n).$$

Определение 2.1.6. Совокупность всех n-мерных векторов над полем k, рассмотренная вместе с определенными на ней операциями сложение векторов и умножение векторов на число, называется n-мерным координатным (векторным) пространством.

ТЕОРЕМА 2.1.1 (о свойствах операций в $\mathbf{k^n}$)**.** *Операции, определенные в k^n, обладают следующими свойствами:*

1. $a + b = b + a$ *(коммутативность сложения векторов);*

2. $a + (b + c) = (a + b) + c$ *(ассоциативность сложения векторов);*

3. $(\forall\ a, b \in k^n)\ \ (\exists\ x \in k^n) \quad b + x = a$ *(обратимость сложения векторов);*

4. $\alpha(a+b) = \alpha a + \alpha b$ *(дистрибутивность умножения относительно сложения векторов);*

5. $(\alpha+\beta)a = \alpha a + \beta a$ *(дистрибутивность умножения относительно сложения чисел);*

6. $(\alpha\beta)a = \alpha(\beta a) = \beta(\alpha a)$ *(ассоциативыность умножения на число);*

7. $1 \cdot a = a$.

Доказательство. Все эти свойства следуют из определений 2.1.4 и 2.1.5 и того факта, что эти свойства справедливы для сложения и умножения чисел.

1. $a+b = (\alpha_1+\beta_1, \alpha_2+\beta_2, \ldots, \alpha_n+\beta_n) = (\beta_1+\alpha_1, \beta_2+\alpha_2, \ldots, \beta_n+\alpha_n) = b+a$.

3. Пусть $a = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $b = (\beta_1, \beta_2, \ldots, \beta_n)$. Вектор x будем искать в виде $(x_1, x_2, \ldots, x_n)$, где $x_1, x_2, \ldots, x_n$ — неизвестные координаты. Перепишем $b + x = a$ в координатной форме:

$$(\beta_1+x_1, \beta_2+x_2, \ldots, \beta_n+x_n) = (\alpha_1, \alpha_2, \ldots, \alpha_n) \quad (\forall\ 1 \leqslant i \leqslant n) \quad \beta_i+x_i = \alpha_i$$

Отсюда находим, что

$$(\forall\ 1 \leqslant i \leqslant n) \quad x_i = \alpha_i - \beta_i.$$

Координаты вектора x найдены. Следовательно,

$$x = (\alpha_1 - \beta_1, \alpha_2 - \beta_2, \ldots, \alpha_n - \beta_n).$$

5. $(\alpha+\beta)a = ((\alpha+\beta)\alpha_1, (\alpha+\beta)\alpha_2, \ldots, (\alpha+\beta)\alpha_n) = (\alpha\alpha_1 + \beta\alpha_1, \alpha\alpha_2 + \beta\alpha_2, \ldots, \alpha\alpha_n+\beta\alpha_n) = (\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_n)+(\beta\alpha_1, \beta\alpha_2, \ldots, \beta\alpha_n) = \alpha a + \beta a$. □

Определение 2.1.7. Вектор x, удовлетворяющий уравнению $b + x = a$, называется разностью векторов a и b и обозначается $x = a - b$.

Простейшие следствия из теоремы 2.1.1.

1. Роль нуля при сложении векторов играет нулевой вектор $0 = (0, 0, \ldots, 0)$.
   Действительно, $(\forall\ a \in k^n) \quad a + 0 = (\alpha_1 + 0, \alpha_2 + 0, \ldots, \alpha_n + 0) = (\alpha_1, \alpha_2, \ldots, \alpha_n) = a$;

2. $(\forall\ a \in k^n)\ (\exists\ (-a) \in k^n) \quad a + (-a) = 0$.
   В самом деле, $(-a) = (-\alpha_1, -\alpha_2, \ldots, -\alpha_n)$. Вектор $(-a)$ называется противоположным вектором для вектора a;

3. Вектор x, удовлетворяющий уравнению $b + a = x$, может быть найден из условия $x = a + (-b)$.
   Действительно, $b + [a + (-b)] = b + [(-b) + a] = [b + (-b)] + a = 0 + a = a$. Из определения 2.1.7 следует, что $a - b = a + (-b)$;

4. $(-\alpha)a = \alpha(-a) = -\alpha a$;

5. $\alpha(a - b) = \alpha a - \alpha b$;

6. $(\alpha - \beta)a = \alpha a - \beta a$.

2.2. Линейно зависимые и линейно независимые системы векторов

Определение 2.2.1. Говорят, что вектор a является линейной комбинацией векторов $a_1, a_2, \ldots, a_s$, если существуют скаляры $\alpha_1, \alpha_2, \ldots, \alpha_s$ такие, что $a = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s$.

Определение 2.2.2. Система векторов $a_1, a_2, \ldots, a_s$ называется линейно зависимой (ЛЗ), если существуют скаляры $\alpha_1, \alpha_2, \ldots, \alpha_s$, не все равные нулю, такие, что $\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s = 0$.

Определение 2.2.2 означает, что для ЛЗ систем существуют нетривиальные линейные комбинации, обращающиеся в ноль.

Определение 2.2.3. Система векторов $a_1, a_2, \ldots, a_s$ называется линейно независимой (ЛНЗ), если из равенства $\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s = 0$ следует, что $\alpha_1 = \alpha_2 = \ldots = \alpha_s = 0$.

Определение 2.2.3 означает, что для ЛНЗ систем в ноль может обращаться только тривиальные линейные комбинации этих векторов.

Замечание 2.2.1. В случае одного вектора a_1 линейная зависимость означает, что $a_1 = 0$, а линейная независимость означает, что $a_1 \neq 0$.

ТЕОРЕМА 2.2.1 (критерий линейной зависимости)**.** *Система векторов $a_1, a_2, \ldots, a_s$, $(s \geqslant 2)$ линейно зависима тогда и только тогда, когда хотя бы один вектор системы линейно выражается через остальные векторы этой системы векторов.*

Доказательство. а) Необходимость.
Пусть система векторов $a_1, a_2, \ldots, a_s$ является ЛЗ. По определению 2.2.2 существуют скаляры $\alpha_1, \alpha_2, \ldots, \alpha_s$, не все равные нулю, такие, что $\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s = 0$. Пусть, для определенности, $\alpha_1 \neq 0$, тогда

$$a_1 = \left(-\frac{\alpha_2}{\alpha_1}\right) a_2 + \ldots + \left(-\frac{\alpha_s}{\alpha_1}\right) a_s.$$

Вектор a_1 является линейной комбинацией остальных векторов.
б) Достаточность.
Пусть, например, вектор a_1 линейно выражается через $a_2, \ldots, a_s$.

$$a_1 = \alpha_2 a_2 + \ldots + \alpha_s a_s \Rightarrow (-1)a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s = 0.$$

Это равенство указывает на то, что нетривиальная линейная комбинация векторов $a_1, a_2, \ldots, a_s$ равна нулю. По определению 2.2.2 векторы $a_1, a_2, \ldots, a_s$ линейно зависимы. □

Свойства линейной зависимости

1. Если какая-либо подсистема векторов является ЛЗ, то и вся система векторов также будет ЛЗ.

   Действительно, пусть $a_1, a_2, \ldots, a_s$ — вся система векторов и $a_1, a_2, \ldots, a_r$ $(r \leqslant s)$ является ЛЗ. По определению 2.2.2 существуют $\alpha_1, \alpha_2, \ldots, \alpha_r$, не все равные нулю, такие, что

   $$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_r a_r = 0.$$

   Мы не нарушим равенство, если запишем

   $$\alpha_1 a_1 + \ldots + \alpha_r a_r + 0 \cdot a_{r+1} + \ldots + 0 \cdot a_s = 0.$$

   Видно, что нетривиальная линейная комбинация векторов $a_1, a_2, \ldots, a_s$ равна нулю. Это означает, что система векторов $a_1, a_2, \ldots, a_s$ является ЛЗ.

2. Если система векторов является ЛНЗ, то и любая ее подсистема также является ЛНЗ.

   Действительно, допустим противное, то есть некоторая подсистема ЛНЗ системы оказалась ЛЗ. Тогда по свойству 1 и вся система будет ЛЗ, а это противоречит условию.

3. Если система векторов $a_1, a_2, \ldots, a_s$ является ЛНЗ, а система векторов $a_1, a_2, \ldots, a_s, b$ является ЛЗ, то вектор b является линейной комбинацией векторов $a_1, a_2, \ldots, a_s$.

   Действительно, так как $a_1, a_2, \ldots, a_s, b$ является ЛЗ, то существуют $\alpha_1, \alpha_2, \ldots, \alpha_s, \beta$, не все равные нулю, такие, что

   $$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s + \beta b = 0.$$

   Покажем, что $\beta \neq 0$. Допустим противное, то есть $\beta = 0$. Тогда получим

   $$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s = 0,$$

где не все $\alpha_1, \alpha_2, \ldots, \alpha_s$ равны нулю. А это означает, что система векторов $a_1, a_2, \ldots, a_s$ является ЛЗ, что противоречит условию. Следовательно, $\beta \neq 0$, тогда вектор

$$b = \left(-\frac{\alpha_1}{\beta}\right) a_1 + \ldots + \left(-\frac{\alpha_s}{\beta}\right) a_s.$$

Видно, что вектор b линейно выражается через $a_1, a_2, \ldots, a_s$, значит является линейной комбинацией этих векторов.

4. Два вектора ЛЗ тогда и только тогда, когда они пропорциональны.
   а) Необходимость.
   Пусть векторы a_1 и a_2 линейно зависимы. По определению 2.2.2 это означает, что существуют скаляры α_1 и α_2, одновременно не равные нулю, такие, что $\alpha_1 a_1 + \alpha_2 a_2 = 0$. Пусть, например, $\alpha_1 \neq 0$. Тогда из последнего равенства получаем

$$a_1 = \left(-\frac{\alpha_2}{\alpha_1}\right) a_2,$$

   то есть векторы a_1 и a_2 являются пропорциональными.
   б) Достаточность.
   Пусть векторы a_1 и a_2 являются пропорциональными. Это означает, что существует скаляр k такой, что $a_1 = ka_2$ (или $a_2 = ka_1$). Получаем $(-1)a_1 + ka_2 = 0$. Нетривиальная линейная комбинация векторов a_1 и a_2 равна нулю. Следовательно, векторы a_1 и a_2 линейно зависимы.

5. Система векторов, содержащая хотя бы два пропорциональных вектора или нулевой вектор, является ЛЗ.
   Это следует из свойства 4, замечания 2.2.1 и из свойства 1.

ТЕОРЕМА 2.2.2 (основная теорема о линейной зависимости)**.** *Пусть даны две системы векторов*

$$a_1, a_2, \ldots, a_p \quad (I) \quad и \quad b_1, b_2, \ldots, b_q \quad (II).$$

Если система векторов (I) является ЛНЗ и каждый вектор системы (I) линейно выражается через векторы системы (II), то число векторов в системе (I) не превосходит числа векторов системы (II), то есть $p \leqslant q$.

Доказательство. Доказательство проводим методом математической индукции по q.

1 шаг. Пусть $q = 1$. Надо показать, что $p \leqslant 1$. Имеем в системе (II) вектор b_1. Допустим противное, то есть $p \geqslant 2$. Это означает, что в системе имеется по крайней мере два вектора. Они линейно выражаются через b_1.

$$a_1 = \alpha_1 b_1; \quad a_2 = \alpha_2 b_1 \quad \alpha_1 \neq 0.$$

Если бы $\alpha_1 = 0$, то $a_1 = 0$. Тогда система (I) была бы ЛЗ (по свойству 3). Следовательно, $\alpha_1 \neq 0$. Тогда $b_1 = \frac{1}{\alpha_1} a_1$, подставим, получим $a_2 = \frac{\alpha_2}{\alpha_1} a_1$. Векторы a_1 и a_2 пропорциональны, а это опять означало бы линейную зависимость системы (I). Это противоречие доказывает, что $p \geqslant 2$, быть не может. Тогда $p \leqslant 1$ и теорема для $q = 1$ доказана.

2 шаг. Предположим, что теорема справедлива для случая, когда в системе (II) содержится $q-1$ вектор. Докажем ее справедливость для случая q векторов в системе (II). Запишем тот факт, что векторы системы (I) линейно выражаются через векторы системы (II).

$$\begin{array}{rcl} a_1 & = & \alpha_{11} b_1 + \ldots + \alpha_{1\ q-1} b_{q-1} + \alpha_{1q} b_q; \\ & \ldots & \\ a_{p-1} & = & \alpha_{p-1\ 1} b_1 + \ldots + \alpha_{p-1\ q-1} b_{q-1} + \alpha_{p-1\ q} b_q; \\ a_p & = & \alpha_{p1} b_1 + \ldots + \alpha_{p\ q-1} b_{q-1} + \alpha_{pq} b_q. \end{array} \tag{2.1}$$

Рассмотрим два случая.

а) Все скаляры при векторе b_q в равенствах (2.1) равны нулю $\alpha_{1q} = \ldots = \alpha_{p-1\ q} = \alpha_{pq} = 0$. В этом случае ЛНЗ система (I) $a_1, a_2, \ldots, a_p$ линейно выражается через векторы $b_1, b_2, \ldots, b_{q-1}$. Тогда по предположению индукции $p \leqslant q - 1$. Тогда $p \leqslant q$.

б) Не все скаляры при векторе b_q в равенствах (2.1) равны нулю. Пусть, например, $\alpha_{pq} \neq 0$. С помощью последнего равенства в (2.1) исключим вектор b_q из первых $p-1$ равенств. Для этого из i-го равенства $(1 \leqslant i \leqslant p-1)$ мы вычитаем последнее равенство, умноженное на $\frac{\alpha_{iq}}{\alpha_{pq}}$. После этих преобразований получим

$$\begin{aligned} a_1^* &= \beta_{11}b_1 + \ldots + \beta_{1\ q-1}b_{q-1}; \\ &\ldots \\ a_{p-1}^* &= \beta_{p-1,1}b_1 + \ldots + \beta_{p-1\ q-1}b_{q-1}. \end{aligned} \tag{2.2}$$

$$a_i^* = a_i - \frac{\alpha_{iq}}{\alpha_{pq}}a_p, \qquad (1 \leqslant i \leqslant p-1). \tag{2.3}$$

Рассмотрим две системы векторов:

$$a_1^*, \ldots, a_{p-1}^* \quad (I^*) \quad \text{и} \quad b_1, \ldots, b_{q-1} \quad (II^*).$$

Равенства (2.2) указывают на то, что система (I*) линейно выражается через систему (II*). Покажем, что система (I*) является ЛНЗ. По определению 2.2.3: пусть

$$\alpha_1 a_1^* + \ldots + \alpha_{p-1}a_{p-1}^* = 0.$$

Получим,

$$\alpha_1\left(a_1 - \frac{\alpha_{1q}}{\alpha_{pq}}a_p\right) + \ldots + \alpha_{p-1}\left(a_{p-1} - \frac{\alpha_{p-1\ q}}{\alpha_{pq}}a_p\right) = 0.$$

$$\alpha_1 a_1 + \ldots + \alpha_{p-1}a_{p-1} + \alpha a_p = 0.$$

Так как система (I) является ЛНЗ, то из последнего равенства следует

$$\alpha_1 = \ldots = \alpha_{p-1} = \alpha = 0$$

Следовательно, система (I*) является ЛНЗ. Тогда применяем предположение индукции, что число векторов в (I*) не превосходит число векторов в (II*), то есть $p-1 \leqslant q-1 \Rightarrow p \leqslant q$. □

ТЕОРЕМА 2.2.3 (о максимальном числе ЛНЗ векторов в $\mathbf{k^n}$)**.** *В n-мерном координатном линейном пространстве k^n существуют ЛНЗ системы, состоящие из n векторов, через которые линейно выражаются все векторы пространства k^n. Любая система векторов пространства k^n, содержащая более n векторов, является ЛЗ.*

Доказательство. Рассмотрим так называемую систему единичных векторов пространства k^n.

$$e_1 = (1, 0, \ldots, 0), \quad e_2 = (0, 1, \ldots, 0), \quad \ldots, \quad e_n = (0, \ldots, 0, 1).$$

Видно, что этих векторов n штук. Покажем, что они являются ЛНЗ. В самом деле, пусть

$$\alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n = 0,$$

$$(\alpha_1, 0, \ldots, 0) + (0, \alpha_2, \ldots, 0) + \ldots + (0, \ldots, 0, \alpha_n) = 0.$$

Получается $(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$. $(\forall\, 1 \leqslant i \leqslant n) \quad \alpha_i = 0$. Следовательно, $e_1, e_2, \ldots, e_n$ является ЛНЗ системой векторов. Покажем, что все векторы в пространстве k^n линейно выражаются через $e_1, e_2, \ldots, e_n$. В самом деле, пусть вектор $b = (\beta_1, \beta_2, \ldots, \beta_n)$ — любой вектор из k^n. Тогда

$$b = (\beta_1, 0, \ldots, 0) + (0, \beta_2, \ldots, 0) + \ldots + (0, \ldots, 0, \beta_n) = \beta_1 e_1 + \beta_2 e_2 + \ldots + \beta_n e_n.$$

Пусть $a_1, a_2, \ldots, a_p$ — любая ЛНЗ система векторов из k^n. Тогда все эти векторы линейно выражаются через $e_1, e_2, \ldots, e_n$. Тогда по основной теореме 2.2.2, число векторов (I) не превосходит число векторов во второй системе, то есть $p \leqslant n$. Мы видим, что в любой ЛНЗ системе векторов пространства k^n должно содержаться не более n векторов. Следовательно, если система содержит более n векторов, она должна быть ЛЗ. $\square$

Определение 2.2.4. ЛНЗ система векторов $a_1, a_2, \ldots, a_s$ называется максимальной ЛНЗ подсистемой системы векторов A, если добавление к ней любого вектора $a \in A$ превращает ее в ЛЗ систему.

Из результатов теоремы 2.2.3 следует, что в пространстве k^n любая ЛНЗ система, состоящая из n векторов является максимальной ЛНЗ подсистемой пространства k^n.

2.3. Базис и ранг системы векторов

В этом пункте в подсистеме векторов A мы будем понимать не пустое, а может быть даже бесконечное множество векторов.

Определение 2.3.1. Говорят, что система векторов A линейно выражается через систему векторов B, если каждый вектор $a \in A$ является линейной комбинацией конечного подмножества векторов системы B.

$$(\forall\ a \in A) \quad a = \sum_{b \in B} \alpha_b b,$$

где почти все $\alpha_b = 0$ (то есть только конечное множество $\alpha_b \neq 0$).

Если $A \subset B$, то A линейно выражается через B. Действительно, в этом случае

$$(\forall\ a \in A) \quad a = 1 \cdot a + 0 \cdot b_1 + 0 \cdot b_2 + \ldots = \sum_{b \in B} \alpha_b b.$$

Понятие линейного выражения одной системы через другую обладает свойством транзитивности, а именно, если A линейно выражается через B, а B линейно выражается через C, то A линейно выражается через C.

Определение 2.3.2. Две системы векторов A и B называются эквивалентными ($A \sim B$), если они линейно выражаются друг через друга.

Отношение эквивалентности системы векторов обладает следующими свойствами:

1. $A \sim A$ (рефлексивность).

2. Если $A \sim B$, то $B \sim A$ (симметричность).

3. Если $A \sim B$, $B \sim C$, то $A \sim C$ (транзитивность).

Справедливость этих свойств немедленно следует из определения 2.3.2 и отмеченной транзитивности понятия линейного выражения одной системы через другую.

ТЕОРЕМА 2.3.1 (о равносильных условиях, определяющих базис)**.** *Пусть B линейно независимая подсистема системы A. Тогда равносильны следующие утверждения:*

1. *Системы векторов A линейно выражаются через подсистему B.*
2. *Система векторов (B,a), получающаяся присоединением к B любого вектора $a \in A$, является линейно зависимой.*
3. *В системе векторов A не существует линейно независимых подсистем с числом векторов большим, чем в B.*

Доказательство. Прежде всего заметим, что если система A может быть как конечной, так и бесконечной, то система B обязательно должен быть конечной. Это следует из теоремы 2.2.3.

Покажем, что из утверждения 1 следует 2. Возьмем любой вектор $a \in A$. Составим (B, a). Так как вектор a линейно выражается через B, то по критерию линейной зависимости эта система (B, a) является линейно зависимой.

Замечание 2.3.1. Выполнение условия 2 означает, что B является максимальной линейно независимой подсистемой системы A.

Покажем, что из утверждения 2 следует 3. Пусть B' — любая линейно независимая подсистема векторов из A. Возьмем $a \in B'$ и составим (B, a). По условию 2 она является линейно зависимой, тогда по свойству 3 линейной зависимости векторов a выражается через B. Следовательно B' линейно выражается через B. Так как B' — линейно независима,

то по основной теореме о линейной зависимости число векторов в B' не превосходит числа векторов из B.

Покажем, что из условия 3 следует 1. Возьмем любой вектор $a \in A$ и составим (B, a). Так как в этой системе число векторов больше, чем в B, то по условию 3 она является линейно зависимой, отсюда по свойству 3 линейной зависимости, вектор a линейно выражается через B. Таким образом вся система A линейно выражается через B. □

Определение 2.3.3. Базисом системы векторов A называется любая ее линейно независимая подсистема B, удовлетворяющая любому из равносильных условий теоремы 2.3.1.

Определение 2.3.4. Базисом системы векторов A называется такая ее линейно независимая подсистема B, через которую выражаются все векторы системы A.

Определение 2.3.5. Базисом системы векторов A называется любая ее максимальная линейно независимая подсистема.

Пример:
$A = k^n$, $B = \{e_1, e_2, \ldots, e_n\}$. Из результатов теоремы 2.2.3 следует, что B является базисом A.

Свойства базисов

1. Система векторов A эквивалентна любому своему базису B.

   Действительно, A линейно выражается через B (определение 2.3.4) с другой стороны, так как $B \subset A$, то B линейно выражается через A. Тогда по определению 2.3.2: $A \sim B$.

2. Количество векторов во всех базисах системы векторов A одно и то же.

   Пусть B и B' — любые два базиса системы векторов A. Тогда, с одной стороны, B' — линейно независимое и линейно выражается

через B. Отсюда по основной теореме 2.2.2 следует, что число векторов в B' не превосходит числа векторов B. С другой стороны, поменяем ролями B и B'. B — является линейно независимым и линейно выражается через B'. Отсюда получаем, что число векторов B' равно числу векторов в B.

Определение 2.3.6. Рангом системы векторов называется число векторов в любом базисе этой системы.

Определение 2.3.7. Рангом системы векторов называется максимальное число ее линейно независимых векторов.

Свойства рангов

1. Если система векторов A линейно выражается через систему векторов B, то ранг системы A меньше или равен рангу системы B, то есть $r(A) \leqslant r(B)$, где r —ранг.

   Пусть A' — базис A, B' — базис B. Тогда A' линейно выражается через A, A линейно выражается через B (по условию), B линейно выражается через B'. Следовательно, по транзитивности A' линейно выражается через B'. Кроме того, A' линейно независимая система векторов, тогда число векторов в A' меньше или равно числу векторов в B', то есть $r(A) \leqslant r(B)$.

2. Ранги эквивалентных систем векторов равны.

   Действительно, пусть $A \sim B$. Тогда с одной стороны, A линейно выражается через B и по свойству 1: $r(A) \leqslant r(B)$. С другой стороны, B линейно выражается через A, тогда по свойству 1: $r(B) \leqslant r(A)$. Из этих двух неравенств следует, что $r(A) = r(B)$.

2.4. Ранг матрицы

Определение 2.4.1. Прямоугольной матрицей $n \times m$ называется прямоугольная таблица из $n \times m$ чисел a_{ij}, записанная в виде n строк и m столбцов

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}.$$

На столбцы матрицы можно смотреть как на векторы пространства k^n. На строки матрицы можно смотреть как на векторы пространства k^m.

Определение 2.4.2. Рангом матрицы называется ранг системы векторов, образованной ее столбцами.

Определение 2.4.3. Рангом матрицы называется максимальное число ее линейно независимых столбцов.

Определение 2.4.4. Пусть дана матрица $A_{n\times m}$ и максимальное число $1 \leqslant k \leqslant min(n, m)$. Минором k-порядка матрицы A называется определитель, порожденный матрицей, состоящей из элементов, стоящих на пересечении любых k строк и любых k столбов матрицы A.

В дальнейшем, нас будут интересовать не равные нулю миноры матрицы A, а именно: нас будет интересовать наивысший порядок, отличных от нуля миноров. При его разыскании надо иметь в виду следующее: если в матрице A равны нулю все миноры k-порядка, то равны нулю и все миноры более высокого порядка. Действительно, применяя к минору $(k + j)$-порядка теорему Лапласа мы можем представить его как сумму произведений миноров k-порядка на миноры j-порядка, а так как все миноры k-порядка равны нулю, то и этот минор $(k + j)$-порядка будет равным нулю.

ТЕОРЕМА 2.4.1 (о ранге матрицы)**.** *Ранг матрицы равен наивысшему порядку отличных от нуля миноров этой матрицы.*

Доказательство. Пусть наивысший порядок, отличных от нуля миноров матрицы A равно r. Без ограничения в общности будем считать, что не равный нулю минор M порядка r находится в левом верхнем углу матрицы A

$$A = \begin{pmatrix} a_{11} & \dots & a_{1r} & \dots & a_{1m} \\ \dots & \dots & \dots & \dots & \dots \\ a_{r1} & \dots & a_{rr} & \dots & a_{rm} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nr} & \dots & a_{nm} \end{pmatrix}, \ M \neq 0.$$

1) Покажем, что первые r столбцов матрицы A является линейно независимыми. Допустим противное, то есть первые r столбцов матрицы являются линейно зависимыми, тогда по критерию линейной зависимости, по крайней мере один столбец, например первый, линейно выражается через остальные $(r-1)$ столбцов. Переходя от столбцов матрицы A к столбцам минора M, мы получим, что первый столбец минора M линейно выражается через остальные $(r-1)$ столбцов. А тогда по свойству 8 определителей $M = 0$, а это противоречит тому, что $M \neq 0$. Следовательно, первые r столбцов матрицы A линейно независимы.

2) Покажем, что любой l-столбец, где $r \leqslant l \leqslant n$, линейно выражается через первые r столбцов матрицы A. Зафиксируем i, $1 \leqslant i \leqslant n$, и рассмотрим n определителей Δ_i, получающиеся приписыванием к минору M элементов i-строки и l-столбца матрицы A

$$\Delta_i = \begin{vmatrix} a_{11} & \dots & a_{1r} & a_{1l} \\ \dots & \dots & \dots & \dots \\ a_{r1} & \dots & a_{rr} & a_{rl} \\ a_{i1} & \dots & a_{ir} & a_{il} \end{vmatrix}.$$

Покажем, что все определители $\Delta_i = 0$. Действительно, если $1 \leqslant i \leqslant r$,

то $\Delta_i = 0$, так как он содержит две одинаковые строки. Если $r < i \leqslant n$, то Δ_i будет минором $(r+1)$-порядка матрицы A. Тогда он будет равен нулю, в силу выбора числа r. Значит, все $\Delta_i = 0$ при $1 \leqslant i \leqslant n$.

Разложим определитель Δ_i по элементам последней строки. Получим,

$$\Delta_i = a_{i1}A_{i1} + a_{i2}A_{i2} + \ldots + a_{ir}A_{ir} + a_{il}M = 0,$$

где $M, A_{i1}, A_{i2}, \ldots, A_{ir}$ —не зависят от i. Следовательно,

$$a_{il} = \left(-\frac{A_{i1}}{M}\right) a_{i1} + \left(-\frac{A_{i2}}{M}\right) a_{i2} + \ldots + \left(-\frac{A_{ir}}{M}\right) a_{ir}.$$

Это равенство справедливо для всех $1 \leqslant i \leqslant n$, при коэффициентах

$$-\frac{A_{i1}}{M_1}, -\frac{A_{i2}}{M_2}, \ldots, -\frac{A_{ir}}{M},$$

не зависящих от i.

Переписывая равенство для всех i, мы получим, что l-столбец матрицы A линейно выражается через первые r-столбцов этой матрицы с коэффициентами

$$-\frac{A_{i1}}{M}, -\frac{A_{i2}}{M}, \ldots, -\frac{A_{ir}}{M}.$$

Из 1) и 2) следует, что первые r-столбцов матрицы A образуют базис всех столбцов этой матрицы A, поэтому $r(A) = r$. □

Следствие 2.4.1.1. Максимальное число линейно независимых строк матрицы равно максимальному числу ее линейно независимых столбцов, то есть равно рангу матрицы.

Доказательство. Рассмотрим матрицы A и A' (транспонированная матрица). Ясно, что если матрица A содержит минор M, то матрица A' содержит минор M'. Верно и обратное. Напомним, что при транспонировании величина определителя не меняется. Из всего сказанного следует, что максимальные порядки, отличных от нуля миноров матриц A и A' совпадают. Тогда по теореме о ранге матрицы $r(A') = r(A)$. Таким

образом получаем следующую цепочку равенств: максимальное число линейно независимых столбцов матрицы A равно $r(A) = r(A')$ равно максимальному числу линейно независимых столбцов матрицы A' равно максимальному числу линейно независимых строк матрицы A. $\square$

Следствие 2.4.1.2 (критерий равенства нулю определителя). Определитель равен нулю тогда и только тогда, когда его строки линейно зависимы.

Доказательство. а) Достаточность.

Пусть строки определителя Δ является линейно зависимым. Тогда по критерию линейной зависимости хотя бы одна из строк линейно выражается через другие его строки, а тогда по 8 свойству определителей $\Delta = 0$.

б) Необходимость.

Пусть определитель $\Delta = 0$. Рассмотрим матрицу A этого определителя. Ее единственный минор n-порядка $\Delta = 0$. Тогда по теореме о ранге матрицы $r(A) < n$. А это означает по следствию 2.4.1.1, что максимальное число линейно независимых строк матрицы A меньше n, тогда все строки матрицы A (n-штук) должны быть линейно зависимыми. $\square$

Глава 3

Системы линейных уравнений

Пусть k — фиксированное числовое поле, которое будем называть основным. $\alpha, \beta, \gamma, \ldots$ — числа поля k. $a, b, c, \ldots$ — векторы над k. $x_1, x_2, \ldots, x_n$ — символы неизвестных.

3.1. Основные определения

Определение 3.1.1. Системой m линейных уравнений с n неизвестными называется совокупность уравнений вида:

$$\begin{aligned} &\alpha_{11}x_1 + \alpha_{12}x_2 + \ldots + \alpha_{1n}x_n = \beta_1, \\ &\alpha_{21}x_1 + \alpha_{22}x_2 + \ldots + \alpha_{2n}x_n = \beta_2, \\ &\ldots, \\ &\alpha_{m1}x_1 + \alpha_{m2}x_2 + \ldots + \alpha_{mn}x_n = \beta_m \end{aligned} \tag{3.1}$$

или

$$\sum_{j=1}^{n} \alpha_{ij}x_j = \beta_i, \qquad 1 \leqslant i \leqslant m,$$

где $\alpha_{ij}, \beta_i \in k$, а $x_1, x_2, \ldots, x_n$ — неизвестные.

Определение 3.1.2. Решением системы линейных уравнений (3.1) называется упорядоченная совокупность чисел $(\xi_1, \xi_2, \ldots, \xi_n)$, при подстановке которых во все уравнения системы вместо $x_1, x_2, \ldots, x_n$ эти уравнения обращаются в справедливые числовые равенства.

Определение 3.1.2 означает, что на решение системы можно смотреть как на векторы пространства k^n.

Определение 3.1.3. Система линейных уравнений называется совместной, если она имеет хотя бы одно решение. Система линейных уравнений называется несовместной (противоречивой), если она не имеет решений.

Определение 3.1.4. Совместная система линейных уравнений называется определенной, если она имеет единственное решение. Система линейных уравнений называется неопределенной, если она имеет более одного решения.

Определение 3.1.5. Исследовать систему линейных уравнений — это значит выяснить совместна она или противоречива, а в случае совместности выяснить, определена она или не определена.

Определение 3.1.6. Решить совместную систему линейных уравнений — это значит найти все ее решения или указать метод нахождения всех ее решений.

Определение 3.1.7. Две системы линейных уравнений с одним числом неизвестных называются эквивалентными (равносильными), если множество их решений совпадают.

Определение 3.1.8. Матрицей системы линейных уравнений (3.1) называется матрица, составленная из коэффициентов при неизвестных этой системы:

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

Определение 3.1.9. Расширенной матрицей системы линейных уравнений (3.1) называется матрица, составленная из коэффициентов при

неизвестных и столбца свободных членов этой системы:

$$A_1 = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} & \beta_1 \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} & \beta_2 \\ \dots & \dots & \dots & \dots & \dots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} & \beta_m \end{pmatrix}.$$

Обозначим через $r = rang\ A$; $r_1 = rang\ A_1$. Ясно, что $r \leqslant \leqslant min(m, n)$; $r \leqslant r_1 \leqslant r + 1$.

Обозначим столбцы матрицы A_1:

$$a_1 = \begin{pmatrix} \alpha_{11} \\ \alpha_{21} \\ \dots \\ \alpha_{m1} \end{pmatrix},\ a_2 = \begin{pmatrix} \alpha_{12} \\ \alpha_{22} \\ \dots \\ \alpha_{m2} \end{pmatrix},\ \dots,\ a_n = \begin{pmatrix} \alpha_{1n} \\ \alpha_{2n} \\ \dots \\ \alpha_{mn} \end{pmatrix},\ b = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \dots \\ \beta_m \end{pmatrix}.$$

Тогда система линейных уравнений (3.1) короче можно записать так:

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b \tag{3.2}$$

(3.2) — есть векторная запись системы линейных уравнений (3.1). Ясно, что $(\xi_1, \xi_2, \ldots, \xi_n)$ является решением системы (3.1) тогда и только тогда, когда

$$\xi_1a_1 + \xi_2a_2 + \ldots + \xi_na_n = b. \tag{3.3}$$

3.2. Исследование системы линейных уравнений

Вопрос о совместности системы линейных уравнений полностью решается следующей теоремой.

ТЕОРЕМА 3.2.1 (Кранекера-Капелли)**.** *Система линейных уравнений совместна тогда и только тогда, когда ранг матрицы системы равен рангу расширенной матрицы этой системы, то есть* $r = r_1$.

Доказательство. а) Необходимость.

Пусть система линейных уравнений (3.1) совместна. $\xi_1, \xi_2, \ldots, \xi_n$ — одно из ее решений. Это означает, что

$$\xi_1 a_1 + \xi_2 a_2 + \ldots + \xi_n a_n = b.$$

Рассмотрим две системы векторов: $\{a_1, a_2, \ldots, a_n\}$ (I) — столбцы матрицы A, $a_1, a_2, \ldots, a_n, b$ (II) — столбцы матрицы A_1. Система (I) полностью содержится в системе (II), то система (I) линейно выражается через систему (II). Обратно, система (II) линейно выражается через систему (I) так как векторы $a_1,\ a_2,\ \ldots,\ a_n$ выражаются через (I) тривиальным образом, а вектор b выражается через (I) по равенству (3.3). Это означает, что система (I) эквивалентна системе (II), но ранги эквивалентных систем равны, то есть $r(I) = r(II)$. Тогда $r = rang\ A = r(I) = r(II) = rang\ A_1 = r_1$ следовательно $r = r_1$.

б) Достаточность.

Пусть в системе линейных уравнений $r = r_1$. Рассмотрим какой-либо базис в системе (I). $a_1, a_2, \ldots, a_r$ — базис системы (I). Эти векторы будут образовывать и базис системы (II), так как эти векторы линейно независимы и количество их равно $r_1 = rang(II)$. Тогда любой вектор системы (II), в частности вектор b, линейно выражается через этот базис, то есть $b = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + 0a_{r+1} + \ldots + 0a_n$, где $\alpha_1 = \xi_1, \alpha_2 = = \xi_2, \ldots, 0 = \xi_{r+1}, \ldots, 0 = \xi_n$. Мы получили равенство вида (3.3). Следовательно, $(\alpha_1, \ldots, \alpha_r, 0, \ldots, 0)$ является решением системы (3.1). То есть система совместна. □

Определение 3.2.1. Если система линейных уравнений (3.1) совместна, то число r $(rang = r_1)$ называется рангом совместной системы.

ТЕОРЕМА 3.2.2 (Критерий определенности совместной системы линейных уравнений)**.** *Совместная система линейных уравнений является определенной тогда и только тогда, когда ее ранг равен числу неиз-*

вестных, то есть $r = n$.

Доказательство. а) Достаточность.

Пусть система линейных уравнений (3.1) совместна, $r = n$. Надо доказать, что она имеет единственное решение. Допустим противное, то есть система линейных уравнений (3.1) имеет более одного решения: $(\xi_1, \xi_2, \ldots, \xi_n)$ и $(\xi'_1, \xi'_2, \ldots, \xi'_n)$, то есть существует индекс $1 \leqslant i \leqslant n$ такой, что $\xi'_i \neq \xi_i$. Имеем выполнение равенства (3.3) и

$$\xi'_1 a_1 + \xi'_2 a_2 + \ldots + \xi'_n a_n = b. \tag{3.4}$$

Вычтем из равенства (3.3) (3.4), получим

$$(\xi_1 - \xi'_1)a_1 + (\xi_2 - \xi'_2)a_2 + \ldots + (\xi_n - \xi'_n)a_n = 0.$$

Обозначим $\xi_1 - \xi'_1 = \alpha_1, \xi_2 - \xi'_2 = \alpha_2, \ldots, \xi_n - \xi'_n = \alpha_n$, получим

$$\alpha_1 a_1 + \alpha_2 a_2 + \alpha_n a_n = 0. \tag{3.5}$$

Так как существует индекс $1 \leqslant i \leqslant n$, что $\xi'_i \neq \xi_i$, то $\alpha_i \neq 0$. Тогда равенство (3.5) указывает на то, что система векторов $\{a_1, a_2, \ldots, a_n\}$ (I) является линейно зависимой. А это означает, что $r(I) < n$, то есть $r < n$, а это противоречит тому, что дано.

б) Необходимость.

Пусть система линейных уравнений (3.1) совместна и имеет единственное решение $(\xi_1, \xi_2, \ldots, \xi_n)$. Надо доказать, что $r = n$. Допустим противное, то есть $r < n$. Это означает, что $r(I) < n$, то есть векторы $a_1, a_2, \ldots, a_n$ является линейно зависимыми. Это означает, что существуют скаляры $\alpha_1, \alpha_2, \ldots, \alpha_n$, не все равные нулю, такие, что выполняется равенство

$$\alpha_1 a_1 + \alpha_2 a_2 + \alpha_n a_n = 0.$$

Кроме того, имеем равенство (3.3). Вычтем из равенства (3.3) (3.5), получим

$$(\xi_1 - \alpha_1)a_1 + (\xi_2 - \alpha_2)a_2 + \ldots + (\xi_n - \alpha_n)a_n = b.$$

Обозначим $\xi_1 - \alpha_1 = \xi'_1, \xi_2 - \alpha_2 = \xi'_2, \ldots, \xi_n - \alpha_n = \xi'_n$.

$$\xi'_1 a_1 + \xi'_1 a_1 + \ldots + \xi'_n a_n = b.$$

Это равенство указывает на то, что вектор $\xi'_1, \xi'_2, \ldots, \xi'_n$ является решением системы линейных уравнений (3.1). Причем это решение отлично от решения $(\xi_1, \xi_2, \ldots, \xi_n)$, так как не все $\alpha_1, \alpha_2, \ldots, \alpha_n$ равны 0. Получаем, что система линейных уравнений (3.1) имеет 2 различных решения. А это противоречит тому, что дано. □

Замечание 3.2.1. Критерий определенности можно высказать в виде следующей эквивалентной формулировке: совместная система линейных уравнений (3.1) является неопределенной тогда и только тогда, когда ее ранг меньше числа неизвестных.

3.3. Теорема Крамера

В этом пункте будем рассматривать частный случай $m = n$, то есть число уравнений равно числу неизвестных. В этом случае матрица A системы линейных уравнений (3.1) является квадратной и можно говорить об ее определителе.

Определение 3.3.1. Определителем системы n-линейных уравнений с n-неизвестными называется определитель, порожденный матрицей этой системы, то есть

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

Зафиксируем натуральное число $k,\ 1 \leqslant k \leqslant n$.

Определение 3.3.2. Дополнительными (вспомогательными) определителями системы n линейных уравнений с n неизвестными называются

определители Δ_k, получающиеся из определителя Δ заменой в нем k-столбца столбцом свободных членов этой системы, то есть

$$\Delta_1 = \begin{vmatrix} \beta_1 & \alpha_{12} & \dots & \alpha_{1n} \\ \beta_2 & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \beta_n & \alpha_{n2} & \dots & \alpha_{nn} \end{vmatrix}, \quad \Delta_2 = \begin{vmatrix} \alpha_{11} & \beta_1 & \dots & \alpha_{1n} \\ \alpha_{21} & \beta_2 & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{n1} & \beta_n & \dots & \alpha_{nn} \end{vmatrix}, \quad \dots$$

ТЕОРЕМА 3.3.1 (Крамера)**.** *Если определитель Δ системы n линейных уравнений с n неизвестными не равен нулю, то эта система совместна и определена и ее единственное решение находится по формулам Крамера*

$$x_k = \frac{\Delta_k}{\Delta}, \qquad \text{где} \qquad 1 \leqslant k \leqslant n.$$

Доказательство. Всегда имеем $r \leqslant r_1 \leqslant min(m, n+1)$. Так как в нашем случае $m = n$, то $r \leqslant r_1 \leqslant n$. Так как $\Delta \neq 0$, то по теореме о ранге матрицы $r = n$. Таким образом, $n = r \leqslant r_1 \leqslant n \Rightarrow n = r = r_1$. Из этого следует, что система совместна и определена.

Пусть $x_1, x_2, \dots, x_n$ — это единственное решение системы линейных уравнений (3.1). Подставим это решение во все уравнения системы, получим числовые равенства:

$$\sum_{j=1}^{n} \alpha_{ij} x_j = \beta_i, \qquad 1 \leqslant i \leqslant n. \tag{3.6}$$

Как всегда через A_{ik} обозначим алгебраическое дополнение элемента α_{ik} определителя Δ. Зафиксируем k, $1 \leqslant k \leqslant n$. Умножим i-равенство (3.6) на A_{ik}, получим

$$A_{ik} \sum_{j=1}^{n} a_{ij} x_j = \beta_i A_{ik}, \qquad 1 \leqslant i \leqslant n.$$

Просуммируем эти равенства по $1 \leqslant i \leqslant n$. Получим

$$\sum_{i=1}^{n} A_{ik} \sum_{j=1}^{n} \alpha_{ij} x_j = \sum_{i=1}^{n} \beta_i A_{ik} = \Delta_k$$

применив следствие 1.5.1.2 из теоремы Лапласа. Имеем по следствию 1.5.1.1 и 1.5.1.3 из теоремы Лапласа

$$\sum_{i=1}^{n} \alpha_{ij} A_{ik} = \delta_{jk} \Delta,$$

получим

$$\sum_{j=1}^{n} \delta_{jk} \Delta x_j = \Delta_k,$$

следовательно

$$\Delta x_k = \Delta_k \Rightarrow x_k = \frac{\Delta_k}{\Delta}, \quad 1 \leqslant k \leqslant n.$$

□

3.4. Решение системы линейных уравнений в общем случае

Пусть дана система линейных уравнений

$$\sum_{j=1}^{n} \alpha_{ij} x_j = \beta_i, \quad 1 \leqslant i \leqslant m. \tag{3.7}$$

Как всегда через A и A_1 будем обозначать матрицу и расширенную матрицу системы (3.7). $r = r(A),\ r_1 = r(A_1)$. Будем считать, что $r_1 = r$, то есть система совместна.

Определение 3.4.1. Любой не равный нулю минор матрицы A максимального порядка называется базисным минором матрицы A.

$$M = \begin{vmatrix} \alpha_{11} & \dots & \alpha_{1r} \\ \dots & \dots & \dots \\ \alpha_{r1} & \dots & \alpha_{rr} \end{vmatrix} \neq 0$$

Будем предполагать, что базисный минор матрицы A системы (3.7) расположен в левом верхнем углу этой матрицы.

Определение 3.4.2. Базисной подсистемой системы линейных уравнений (3.7) называется система, состоящая из тех уравнений системы (3.7), коэффициенты при которых входят в состав базисного минора матрицы системы.

$$\begin{aligned} &\alpha_{11}x_1 + \ldots + \alpha_{1r}x_r + \ldots + \alpha_{1n}x_n = \beta_1, \\ &\ldots, \\ &\alpha_{r1}x_1 + \ldots + \alpha_{rr}x_r + \ldots + \alpha_{rn}x_n = \beta_r, \end{aligned} \tag{3.8}$$

ТЕОРЕМА 3.4.1. *Система линейных уравнений (3.7) эквивалентна любой своей базисной подсистеме (3.8).*

Доказательство. 1) Пусть $\xi_1, \xi_2, \ldots, \xi_n$ — любое решение системы (3.7). Это означает, что

$$\sum_{j=1}^{n} \alpha_{ij}\xi_j = \beta_i, \quad 1 \leqslant i \leqslant n.$$

Первые r справедливых числовых равенств указывает на то, что $\xi_1, \xi_2, \ldots, \xi_n$ является решением системы (3.8).

2) Пусть $\xi_1, \xi_2, \ldots, \xi_n$ — любое решение системы (3.8). В матрице A_1 рассмотрим строки, отвечающие базисному минору M, то есть первые r строк. Эти первые r строк будут линейно не зависимыми, и так как их число равно r_1, то они составляют базис всех строк матрицы A_1. Поэтому все строки матрицы A_1 линейно выражаются через первые r строк. Переходя к уравнениям, мы получим, что все уравнения системы (3.7) линейно выражаются через уравнения системы (3.8), а поэтому любое решение $\xi_1, \xi_2, \ldots, \xi_n$ системы (3.8), обращая в справедливые числовые равенства уравнения этой системы, будут обращать в справедливые числовые равенства и любую линейную комбинацию этих уравнений, в частности все уравнения системы (3.7). □

Теорема 3.4.1 сводит решение системы линейных уравнений (3.7) к решению базисной подсистемы (3.8).

Ранг системы (3.8) равен r. Ясно, что $r \leqslant n$. Если $r = n$, то система (3.8) содержит n линейных уравнений с n неизвестными и определителем $\Delta = M \neq 0$. Тогда по теореме Крамера она имеет единственное решение

$$x_k = \frac{\Delta_k}{\Delta}, \qquad 1 \leqslant k \leqslant n.$$

Рассмотрим случай $r < n$.

Определение 3.4.3. Свободными неизвестными системы линейных уравнений (3.7) называются те неизвестные, коэффициенты при которых не входят в базисный минор матрицы системы.

В наших обозначениях свободными неизвестными будут $x_{r+1}, x_{r+2}, \ldots, x_n$. В системе (3.8) числа, содержащие свободные неизвестные, перенесем направо, получим

$$\begin{aligned} \alpha_{11}x_1 + \alpha_{12}x_2 + \ldots + \alpha_{1r}x_r &= \beta_1 - \alpha_{1\ r+1}x_{r+1} - \ldots - \alpha_{1n}x_n, \\ &\ldots\ , \\ \alpha_{r1}x_1 + \alpha_{r2}x_2 + \ldots + \alpha_{rr}x_r &= \beta_r - \alpha_{r\ r+1}x_{r+1} - \ldots - \alpha_{rn}x_n, \end{aligned} \tag{3.9}$$

Объявим свободные неизвестные $x_{r+1}, \ldots, x_n$ параметрами, то есть им можно будет придавать произвольные числовые значения. Тогда на систему (3.9) можно смотреть как на систему r линейных уравнений с r неизвестными $x_1, \ldots, x_r$. Определитель этой системы $\Delta = M \neq 0$. Тогда по теореме Крамера эта система имеет единственное решение

$$x_k = \frac{\Delta_k}{\Delta}, \qquad 1 \leqslant k \leqslant r.$$

$$\Delta_k = \begin{vmatrix} \alpha_{11} & \ldots & \beta_1 - \alpha_{1\ r+1}x_{r+1} - \ldots - \alpha_{1n}x_n & \ldots & \alpha_{1r} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_{r1} & \ldots & \beta_r - \alpha_{r\ r+1}x_{r+1} - \ldots - \alpha_{rn}x_n & \ldots & \alpha_{rr} \end{vmatrix}.$$

Разложим определитель Δ_k по элементам k-столбца, получим

$$x_k = \frac{1}{\Delta}[(\beta_1 - \alpha_{1\ r+1}x_{r+1} - \ldots - \alpha_{1n}x_n)A_{1k} + \ldots +$$

$$+(\beta_r + \alpha_{r\ r+1}x_{r+1} - \ldots - \alpha_{rn}x_n)A_{ik}] =$$

$$= \gamma_k + \gamma_{k1}x_{r+1} + \gamma_{k2}x_{r+2} + \ldots + \gamma_{k\ n-r}x_n, \quad 1 \leqslant k \leqslant n. \tag{3.10}$$

Важно здесь то, что свободные неизвестные $(x_{r+1}, x_{r+2}, \ldots, x_n)$ входят линейным образом. Предадим свободным неизвестным $(x_{r+1}, x_{r+2}, \ldots, x_n)$ произвольные значения $(\xi_{r+1}, \xi_{r+2}, \ldots, \xi_n)$. Подставим эти значения в формулу (3.10), получим значения для не свободных неизвестных

$$\xi_k = \gamma_k + \gamma_{k1}\xi_{r+1} + \gamma_{k2}\xi_{r+2} + \ldots + \gamma_{k\ n-r}\xi_n, \quad 1 \leqslant k \leqslant r.$$

Объединяя найденные значения $(\xi_1, \xi_2, \ldots, \xi_r)$ с произвольными значениями $(\xi_{r+1}, \xi_{r+2}, \ldots, \xi_n)$, мы получим решение системы (3.8), а следовательно, и системы (3.7). Других решений у системы (3.7) нет. Действительно, любое решение $(\xi_1, \ldots, \xi_r, \xi_{r+1}, \ldots, \xi_n)$ системы (3.7) может быть представлено указанным выше способом. А именно, если свободным неизвестным в системе (3.9) дать значения $(\xi_{r+1}, \ldots, \xi_n)$, то числа $(\xi_1, \ldots, \xi_r)$ будут удовлетворять системе (3.9), а следовательно, давать то единственное решение, которое находится по формулам Крамера. Так как значения $(\xi_{r+1}, \xi_{r+2}, \ldots, \xi_n)$ для свободных неизвестных можно выбрать произвольным образом, то получаем бесчисленное множество решений системы (3.7). Это множество решений зависит от $(n - r)$ параметров. Условно пишут ∞^{n-r} решений. Формулы (3.10) называются формулами общего решения системы (3.7). Все выше сказанное можно сформулировать в виде следующей теоремы.

ТЕОРЕМА 3.4.2 (правила решения системы линейных уравнений)**.** *Для того, чтобы решить совместную систему линейных уравнений ранга r необходимо:*

1. *Выбрать базисный минор матрицы системы и выписать соответствующую ему базисную подсистему.*

2. *Объявить свободными неизвестными те, коэффициенты при которых не входят в базисный минор и перенести члены, содержащие свободные неизвестные, направо.*

3. *Объявить свободные неизвестные параметрами и решить каким-либо образом (например по формулам Крамера) полученную систему r линейных уравнений с r несвободными неизвестными.*

3.5. Однородные системы линейных уравнений

Определение 3.5.1. Система линейных уравнений называется однородной, если все ее свободные члены равны нулю, то есть

$$\begin{aligned} &\alpha_{11}x_1 + \alpha_{12}x_2 + \ldots + \alpha_{1n}x_n = 0, \\ &\alpha_{21}x_1 + \alpha_{22}x_2 + \ldots + \alpha_{2n}x_n = 0, \\ &\ldots, \\ &\alpha_{m1}x_1 + \alpha_{m2}x_2 + \ldots + \alpha_{mn}x_n = 0 \end{aligned} \tag{3.11}$$

или

$$\sum_{j=1}^{n} \alpha_{ij}x_j = 0, \qquad 1 \leqslant i \leqslant m,$$

Следствие. Однородная система линейных уравнений всегда совместна.

Действительно, решением системы (3.11) является нулевой вектор $(0, 0, \ldots, 0)$.

Определение 3.5.2. Решение $(0, 0, \ldots, 0)$ однородной системы линейных уравнений называется нулевым или тривиальным.

ТЕОРЕМА 3.5.1 (критерий наличия ненулевого решения однородной системы линейных уравнений)**.** *Однородная система линейных уравнений имеет ненулевые решения тогда и только тогда, когда ее ранг меньше числа неизвестных, то есть $r < n$.*

Доказательство. Пусть однородная система линейных уравнений (3.11) имеет ненулевые решения, значит эта система не определена, тогда по замечанию 3.2.1 $r < n$. □

Следствие 3.5.1.1. Если число уравнений в однородной системе линейных уравнений меньше числа неизвестных, то эта система всегда имеет ненулевые решения.

Действительно, всегда $r \leqslant m$, так как по условию $m < n$, то $r < n$. Следовательно, однородная система линейных уравнений имеет ненулевые решения.

Следствие 3.5.1.2. Однородная система n линейных уравнений с n неизвестными имеет не нулевые решения тогда и только тогда, когда определитель этой системы равен нулю.

В самом деле, пусть A — матрица системы (3.11) и пусть $\Delta = |A| = 0 \Leftrightarrow r(A) < n \Leftrightarrow r < n$, по следствию 3.5.1.1 однородная система линейных уравнений имеет ненулевые решения.

Если в однородной системе линейных уравнений $r = n$, то эта система имеет только нулевое решение. Этот случай не интересен, поэтому будем рассматривать случай, когда $r < n$. В этом случае однородная система линейных уравнений имеет бесчисленное множество решений. На эти решения $(\xi_1, \ldots, \xi_n)$ можно смотреть как на вектора пространства k^n. Множество всех решений однородной системы линейных уравнений обозначается $L \subset k^n$.

ТЕОРЕМА 3.5.2 (свойства решений однородной системы линейных уравнений)**.** *Сумма двух любых решений однородной системы линейных уравнений снова является решением этой системы. Произведение любого числа $\alpha \in k$ на любое решение однородной системы линейных уравнений снова является решением этой системы. Другими словами*

$$(\forall\ a, b \in L) \quad a + b \in L, \qquad (\forall\ \alpha \in k,\ a \in L) \quad \alpha a \in L.$$

Доказательство. 1) Пусть $a = (\xi_1, \xi_2, \ldots, \xi_n) \in L,\ b = (\eta_1, \eta_2, \ldots, \eta_n) \in$ $\in L$, то есть являются решениями системы (3.11). Рассмотрим вектор $(a + b) = (\xi_1 + \eta_1, \xi_2 + \eta_2, \ldots, \xi_n + \eta_n)$. Подставим координаты этого вектора в систему (3.11).

$$\sum_{j=1}^{n} \alpha_{ij}(\xi_j + \eta_j) = \sum_{j=1}^{n} (\alpha_{ij}\xi_j + \alpha_{ij}\eta_j) =$$

$$= \sum_{j=1}^{n} \alpha_{ij}\xi_j + \sum_{j=1}^{n} \alpha_{ij}\eta_i = 0 + 0 = 0.$$

Таким образом, получаем, что вектор $a + b$ тоже является решением системы (3.11), то есть $a + b \in L$.

2) Пусть $a = (\xi_1, \xi_2, \ldots, \xi_n) \in L$ и $a \in L$, тогда

$$\sum_{j=1}^{n} a_{ij}\xi_j = 0.$$

Возьмем любое $\alpha \in k$. Рассмотрим вектор $\alpha a = (\alpha\xi_1, \alpha\xi_2, \ldots, \alpha\xi_n)$.

$$\sum_{j=1}^{n} \alpha_{ij}(\alpha\xi_j) = \alpha \sum_{j=1}^{n} \alpha_{ij}\xi_j = \alpha 0 = 0 \Rightarrow \alpha a \in L.$$

□

Следствие. Любая линейная комбинация решений однородной системы линейных уравнений снова является решением этой системы.

Определение 3.5.3. Фундаментальной системой решений однородной системы линейных уравнений называется базис множества L всех решений этой системы.

Определение 3.5.4. Фундаментальной системой решений однородной системы линейных уравнений называется такая линейно независимая система решений, через которую линейно выражаются все решения этой системы.

Определение 3.5.5. Фундаментальной системой решений однородной системы линейных уравнений называется любая максимальная линейно независимая система решений этой однородной системы.

ТЕОРЕМА 3.5.3 (о фундаментальной системе решений однородной системы линейных уравнений)**.** *Если ранг r однородной системы линейных уравнений меньше числа неизвестных n, то фундаментальная система решений существует и число решений в любой из них равно $n - r$.*

Доказательство. Доказательство теоремы конструктивное, мы явно построим так называемую нормальную фундаментальную систему решений. Будем решать однородную систему линейных уравнений (3.11) методом базисного минора. Как всегда, будем предполагать, что базисный минор M находится в левом верхнем углу матрицы A, тогда система (3.11) равносильна базисной подсистеме:

$$\begin{array}{rcl} \alpha_{11}x_1 + \alpha_{12}x_2 + \ldots + \alpha_{1r}x_r & = & -\alpha_{1\ r+1}x_{r+1} - \ldots - \alpha_{1n}x_n, \\ & \ldots & , \\ \alpha_{r1}x_1 + \alpha_{r2}x_2 + \ldots + \alpha_{rr}x_r & = & -\alpha_{r\ r+1}x_{r+1} - \ldots - \alpha_{rn}x_n, \end{array} \tag{3.12}$$

Выпишем общее решение системы (3.12)

$$x_k = \gamma_{k1}x_{r+1} + \gamma_{k2}x_{r+2} + \ldots + \gamma_{k\ n-r}x_n, \qquad 1 \leqslant k \leqslant r. \tag{3.13}$$

Заметим, что здесь все $\gamma_k = 0$, так как $\beta_1 = \ldots = \beta_m = 0$. Построим $(n - r)$ частных решений этой системы (3.12), для построения первого решения предадим свободным неизвестным значения $x_{r+1} = 1,\ x_{r+2} = \ldots = x_n = 0$. Подставим эти значения в формулу (3.13), получим

$$x_k = \gamma_{k1}, \quad 1 \leqslant k \leqslant r.$$

Объединяя значения для несвободных и свободных неизвестных, получим первое частное решение системы (3.12)

$$b_1 = (\gamma_{11}, \gamma_{21}, \ldots, \gamma_{r1}, 1, 0, \ldots, 0).$$

Для получения второго частного решения системы (3.12) свободным неизвестным придадим значения $x_{r+1} = 0,\ x_{r+2} = 1,\ x_{r+3} = \ldots = x_n = 0$. Подставим эти значения в формулу (3.13), получим значения для несвободных неизвестных

$$x_k = \gamma_{k2}, \quad 1 \leqslant k \leqslant r.$$

Объединяя значения для несвободных и свободных неизвестных, получим второе частное решение системы (3.12):

$$b_2 = (\gamma_{12}, \gamma_{22}, \ldots, \gamma_{r2}, 0, 1, \ldots, 0).$$

И так далее. Наконец, для получения последнего $(n-r)$-го частного решения свободным неизвестным придадим значения: $x_{r+1} = \ldots = x_{n-1} = 0,\ x_n = 1$. Подставим эти значения в формулу (3.13), получим

$$x_k = \gamma_{k\ n-r}, \quad 1 \leqslant k \leqslant r.$$

Объединяя значения для несвободных и свободных неизвестных, получим последнее $(n-r)$-е решение

$$b_{n-r} = (\gamma_{1\ n-r}, \gamma_{2\ n-r}, \ldots, \gamma_{r\ n-r}, 0, 0, \ldots, 1).$$

Обозначим множество этих решений $\{b_1, b_2, \ldots, b_{n-r}\} = B$. Докажем, что B и есть фундаментальная система решений однородной системы линейных уравнений (3.11) по определению 3.5.4.

а) Покажем, что система B — линейно независимая. Найдем ранг системы векторов B. Составим матрицу C, строчками которого являются решение.

$$C = \begin{pmatrix} \gamma_{11} & \gamma_{21} & \ldots & \gamma_{r1} & 1 & 0 & \ldots & 0 \\ \gamma_{12} & \gamma_{22} & \ldots & \gamma_{r2} & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \gamma_{1\ n-r} & \gamma_{2\ n-r} & \ldots & \gamma_{r\ n-r} & 0 & 0 & \ldots & 1 \end{pmatrix}.$$

Можно выделить минор $(n-r)$-го порядка равный 1, то есть не равный нулю. Таким образом $r(C) = n - r$, то есть максимальное число

линейно независимых строк в матрице C равно $n-r$, то есть векторы $b_1, b_2, \ldots, b_{n-r}$ является линейно независимыми.

б) Покажем, что любое решение системы (3.11) линейно выражается через систему решений B. Пусть $y = (\eta_1, \ldots, \eta_r, \eta_{r+1}, \ldots, \eta_n)$ — любое решение однородной системы линейных уравнений (3.11). Рассмотрим вектор $a = y - (\eta_{r+1}b_1 + \eta_{r+2}b_2 + \ldots + \eta_n b_{n-r})$. Покажем, что последние $(n-r)$ координат вектора a равны нулю. Имеем,

$$a = (\eta_1, \ldots, \eta_r, \eta_{r+1}, \eta_{r+2}, \ldots, \eta_n) - \eta_{r+1}(\gamma_{11}, \ldots, \gamma_{r1}, 1, 0, \ldots, 0) -$$

$$-\eta_{r+2}(\gamma_{12}, \ldots, \gamma_{r2}, 0, 1, \ldots, 0) - \ldots - \eta_n(\gamma_{1\ n-r}, \ldots, \gamma_{r\ n-r}, 0, 0, \ldots, 1) =$$

$$= (\xi_1, \ldots, \xi_r, 0, 0, \ldots, 0).$$

Так как $y, b_1, b_2, \ldots, b_{n-r} \in L$, то по следствию к теореме 3.5.2 $a \in L$. В этом решении a значениями свободных неизвестных являются нули, то есть $\xi_{r+1} = 0, \ldots, \xi_n = 0$. Подставляя их в формулы (3.13), получим, что $\xi_1 = \ldots = \xi_r = 0$. Итак, вектор $a = 0 \Rightarrow y = \eta_{r+1}b_1 + \eta_{r+2}b_2 + \ldots + \eta_n b_{n-r}$.

Из пунктов а) и б) следует (по определению 3.5.4), что B является фундаментальной системой решений однородной системы линейных уравнений (3.11). Видно, что количество решений в B равно $(n-r)$. □

Следствие. Если $b_1, \ldots, b_{n-r}$ есть фундаментальная система решений однородной системы линейных уравнений (3.11), то общее решение этой системы может быть записано в виде:

$$\xi_1 b_1 + \xi_2 b_2 + \ldots + \xi_{n-r} b_{n-r},$$

где $\xi_1, \xi_2, \ldots, \xi_{n-r} \in k$. Это вытекает из того, что $b_1, b_2, \ldots, b_{n-r}$ составляют базис L, а тогда любой вектор $x \in L$ линейно выражается через этот базис.

Замечание 3.5.1. Из доказательства теоремы 3.5.3 следует правило нахождения так называемой нормальной фундаментальной системы решений однородной системы линейных уравнений:

1. найти общее решение однородной системы линейных уравнений;
2. придать свободным неизвестным значения $(1, 0, \ldots, 0)$, $(0, 1, \ldots, 0)$, $(0, 0, \ldots, 1)$;
3. по формулам общего решения найти значения для несвободных неизвестных;
4. объединить значения для несвободных и свободных неизвестных.

Глава 4

Алгебра матриц

Пусть k — некоторое фиксированное числовое поле (основное). $\alpha, \beta, \gamma \in$ $\in k$ — элементы поля k. $a, b, c, \ldots$ — векторы над полем k.

Объектом нашего изучения будут прямоугольные матрицы размерности $m \times n$

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{m1} & \alpha_{m2} & \ldots & \alpha_{mn} \end{pmatrix}, \qquad \alpha_{ij} = (A)_{ij}.$$

4.1. Сложение матриц и умножение матриц на число

Определение 4.1.1. Суммой двух матриц A и B, одинаковой размерности, называется матрица $A + B$ той же размерности, элементы которой равны суммам соответствующих элементов матриц A и B, то есть $(A + B)_{ij} = (A)_{ij} + (B)_{ij}$.

Определение 4.1.2. Произведение матрицы A на число α называется матрица αA, элементы которой получаются из соответствующих элементов матрицы A умножением на число α, то есть $(\alpha A)_{ij} = \alpha(A)_{ij}$.

Каждую матрицу $A_{m\times n}$ можно рассматривать как mn-мерный вектор над полем k. Для этого достаточно выписать строки этой матрицы

одна за другой. Это соответствие между матрицами и векторами является взаимнооднозначным. Операции сложения и умножения матриц на число при этом соответствии переходят в операции сложения векторов и умножение векторов на число. Поэтому множество всех прямоугольных матриц, размерности $m \times n$, можно рассмотреть как mn-мерные векторные пространства k^{mn}. Тогда можно применить результаты пункта 2.1.. Из этих результатов вытекает, что операции сложения и умножения матриц на число обладают следующими свойствами:

1. $A + B = B + A$;
2. $A + (B + C) = (A + B) + C$;
3. $\left(\forall\ A, B \in M_{(m\times n,k)}\right)\ \left(\exists\ X \in M_{(m\times n,k)}\right)\quad B + X = A$;
4. $\alpha(A + B) = \alpha A + \alpha B$;
5. $(\alpha + \beta)A = \alpha A + \beta A$;
6. $(\alpha\beta)A = \alpha(\beta A) = \beta(\alpha A)$;
7. $1 \cdot A = A$.

Из этих свойств вытекают простые следствия:

1. Роль нуля при сложении матриц играет нулевая матрица, то есть матрица, состоящая из одних нулей.
   Действительно, $(\forall\ A)\quad A + 0 = A$, где $(0)_{ij} = 0$.
2. $(\forall\ A)\ (\exists\ -A)\quad A + (-A) = 0$.
3. Матрица X, удовлетворяющая уравнению $B + X = A$, может быть найдена из условия $X = A + (-B)$.
   Действительно, $(A - B)_{ij} = (A)_{ij} + (-B)_{ij} = (A)_{ij} - (B)_{ij} = (X)_{ij}$.

Определение 4.1.3. Матрица X, удовлетворяющая условию $B + X = A$, называется разностью матриц A и B, и обозначается $X = A - B$.

4. $\alpha(A - B) = \alpha A - \alpha B$.

5. $(\alpha - \beta)A = \alpha A - \beta A$.

6. $(-\alpha)A = \alpha(-A) = -\alpha A$.

4.2. Умножение матриц

Определение 4.2.1. Произведением матрицы $A_{m\times n}$ на матрицу $B_{n\times p}$ называется матрица $(AB)_{m\times p}$, элемент которой, стоящий в i-строке и j-столбце, равен сумме произведений соответствующих элементов i-строки матрицы A и j-столбца матрицы B.

Определение 4.2.1 означает, что:
1) можно перемножать только такие матрицы, у которых число столбцов первой матрицы равно числу строк второй матрицы;
2) элемент матрицы $(AB)_{ij}$ считается по формуле

$$(AB)_{ij} = \sum_{k=1}^{n} (A)_{ik} \cdot (B)_{kj}.$$

Пример:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & 2 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 & 3 & -1 \\ -1 & 2 & 4 & -2 \\ 2 & 0 & 1 & 3 \end{pmatrix},$$

$$AB = \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & -1 \\ -1 & 2 & 4 & -2 \\ 2 & 0 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 5 & 6 & 14 & 4 \\ 5 & -2 & -2 & 8 \end{pmatrix}.$$

ТЕОРЕМА 4.2.1. *Операции сложения, умножения матриц и умножения матриц на число обладают следующими свойствами:*

1. $A(BC) = (AB)C$;

2. $(A + B)C = AC + BC, \quad A(B + C) = AB + AC$;

3. $\alpha(AB) = (\alpha A)B = A(\alpha B)$.

Доказательство. Прежде всего заметим, что если существует одна из частей равенства, то существует и другая часть этого равенства, и она будет матрицей той же размерности.

1) Допустим, что матрица $A(BC)$ существует. Это означает, что матрица A должна иметь размерность $m \times n$, а B размерность $n \times p$, тогда матрица AB имеет размерность $m \times p$, значит матрица C должна иметь размерность $p \times q$ и матрица $(AB)C$ размерность $m \times q$. Видно, что матрица BC существует и имеет размерность $n \times q$, а тогда имеем, что матрица $A(BC)$ существует и будет иметь размерность $m \times q$. Таким образом ясно, что если существует правая часть, доказываемого равенства, то существует и левая часть и она имеет ту же размерность, что и правая часть. Остается показать равенство соответствующих элементов матриц $A(BC)$ и $(AB)C$. Обозначим элементы матриц A, B, C следующим образом: $(A)_{ij},\ 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n$, $(B)_{jk},\ 1 \leqslant k \leqslant p$, $(C)_{kl},\ 1 \leqslant l \leqslant q$.

$$((AB)C)_{il} = \sum_{k=1}^{p} (AB)_{ik}(C)_{kl} = \sum_{k=1}^{p} \left(\sum_{j=1}^{n} (A)_{ij}(B)_{jk} \right) (C)_{kl} =$$

$$= \sum_{j=1}^{n} (A)_{ij} \sum_{k=1}^{p} (B)_{jk}(C)_{kl} = \sum_{j=1}^{n} (A)_{ij}(BC)_{jl} = (A(BC))_{il}.$$

Получаем

$$(\forall\ 1 \leqslant i \leqslant m,\ 1 \leqslant l \leqslant q) \quad (AB)C = A(BC).$$

2) Покажем, что $A(B+C) = AB + AC$. Предположим, что матрица $A(B+C)$ существует. Это означает, что матрицы B и C имеет одинаковую размерности $n \times p$, тогда матрица $(B+C)$ так же имеет размерность $n \times p$. Так как $A(B+C)$ существует, то матрица A должна иметь размерность $m \times n$, тогда матрица $A(B+C)$ будет иметь размерность $m \times p$. Видно, что матрицы AB и AC существуют. Они имеют размерность $m \times p$. Тогда их можно сложить, следовательно, тогда существует матрица $AB + AC$ и будет матрицей размерностью $m \times p$. Покажем равенство соответствующих элементов матриц $A(B+C)$ и $AB + AC$. Обозначим, $(A)_{ij},\ 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n$ — элементы матрицы A, $(B)_{jk},\ (C)_{jk},\ 1 \leqslant k \leqslant p$ — элементы матриц B и C.

$$(A(B+C))_{ik} = \sum_{j=1}^{n} (A)_{ij}(B+C)_{jk} = \sum_{j=1}^{n} (A)_{ij}\left[(B)_{jk} + (C)_{jk}\right] =$$

$$= \sum_{j=1}^{n} \left[(A)_{ij}(B)_{jk} + (A)_{ij}(C)_{jk}\right] = \sum_{j=1}^{n} (A)_{ij}(B)_{jk} + \sum_{j=1}^{n} (A)_{ij}(C)_{jk} =$$

$$= (AB)_{ik} + (AC)_{ik} = (AB + AC)_{ik}.$$

Получаем

$$(\forall\ 1 \leqslant k \leqslant p,\ 1 \leqslant i \leqslant n) \quad A(B+C) = AB + AC.$$

□

Замечание 4.2.1. Умножение матриц в общем случае не коммутативно, то есть $AB \neq BA$. Причин не коммутативности несколько:

1. Матрица AB существует, но BA не существует. Например, если матрица A размерности $m \times n$, а матрица B размерности $n \times p$, то AB размерности $m \times p$, а BA не существует.

2. AB и BA существуют, но имеют различную размерность. Например, если A размерности $m \times n$, B размерности $n \times m$, то AB имеет размерность $m \times m$, а BA имеет размерность $n \times n$.

3. AB и BA существуют и имеют одинаковые размерности, но $AB \neq$ $\neq BA$.

   Следствие. Матрицы AB и BA существуют и имеют одинаковые размерности, тогда и только тогда, когда они обе квадратные одинаковые размерности.

   Пример:

$$A = \begin{pmatrix} 5 & 6 \\ 3 & 4 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}.$$

$$AB = \begin{pmatrix} 5 & 6 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 17 & 34 \\ 11 & 22 \end{pmatrix},$$

$$BA = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 5 & 6 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 11 & 14 \\ 22 & 28 \end{pmatrix}.$$

Не коммутативность умножения требует осторожности при умножении матриц.

ТЕОРЕМА 4.2.2 (о транспонировании произведения матриц)**.** *Если A и B таковы, что AB существует, то $(AB)' = B'A'$.*

Доказательство. Так как AB существует, то матрица A размерности $m \times n$, B размерности $n \times p$, тогда матрица AB размерности $m \times p$, а $(AB)'$ размерности $p \times m$. Видно, что B' размерности $p \times n$, A' размерности $n \times m$. Ясно, что существует матрица $B'A'$ и она имеет размерность $p \times m$, то есть ту же что и матрица $(AB)'$. Покажем равенство соответствующих элементов этих матриц. Обозначим $(A)_{ij}$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$ — элементы матрицы A, $(B)_{jk}$, $1 \leqslant k \leqslant p$ — элементы матрицы B.

$$((AB)')_{ki} = (AB)_{ik} = \sum_{j=1}^{n} (A)_{ij}(B)_{jk} = \sum_{j=1}^{n} (B')_{kj}(A')_{ji} = (B'A')_{ki}.$$

Получаем

$$(\forall\ 1 \leqslant k \leqslant p,\ 1 \leqslant i \leqslant m) \quad ((AB)')_{ki} = (B'A')_{ki}.$$

Следовательно, $(AB)' = B'A'$. □

Обозначим через $M(n;k)$ множество квадратных матриц порядка n с элементами из поля k. В множестве $M(n;k)$ можно определить 3 операции: сложение, умножение матриц на число, умножение матриц. Относительно первых двух операций, которые обладают свойствами 1-7, отмеченными в пункте 4.1., это множество образует n^2-мерное линейное пространство над полем k. Относительно же всех 3-х операций, которые обладают еще свойствами 1-3 теоремы 4.2.1, это множество $M(n;k)$ образует алгебру квадратных матриц порядка n над полем k. Дальнейшее изучение свойств операции умножения матриц требует привлечения их определителей. Как всегда, определитель квадратной матрицы A будем обозначать $|A|$.

ТЕОРЕМА 4.2.3 (об определителе произведения матриц)**.** *Определитель произведения нескольких квадратных матриц равен произведению определителей этих матриц.*

Доказательство. Теорему достаточно доказать для произведения двух матриц, общий случай сводится к двум матрицам. Пусть A и B — две квадратные матрицы порядка n. Элементы матрицы A обозначим через α_{ij}, элементы матрицы B через β_{ij}. Произведение AB обозначим матрицей C с элементами $\gamma_{ij} = \alpha_{i1}\beta_{1j} + \alpha_{i2}\beta_{2j} + \ldots + \alpha_{in}\beta_{nj}$. Рассмотрим вспомогательный определитель Δ порядка $2n$. Он имеет следующий вид:

$$\Delta = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn} & 0 & 0 & \ldots & 0 \\ -1 & 0 & \ldots & 0 & \beta_{11} & \beta_{12} & \ldots & \beta_{1n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & -1 & \beta_{n1} & \beta_{n2} & \ldots & \beta_{nn} \end{vmatrix}.$$

Подсчитаем определитель Δ двумя способами:

1) Применим теорему Лапласа к первым n-строкам, тогда $\Delta = MA_M$, где M — определитель матрицы A. $A_M = (-1)^{S_M}\widetilde{M}$, где $\widetilde{M}$ — дополнительный минор для M. $\widetilde{M} = |B|$, $S_M = (1+2+\ldots+n)+(1+2+\ldots+n) =$ четному числу. Тогда $A_M = |B|$, таким образом $\Delta = |A| \cdot |B|$.

2) Для подсчета определителя Δ другим способом преобразуем матрицу этого определителя, не изменяя его значения. Все наши преобразования будут направлены на то, чтобы на местах элементов матрицы B получить нули. Зафиксируем $1 \leqslant k \leqslant n$. Затем к $(n+k)$-столбцу прибавим первый столбец, умноженный на β_{1k}, второй столбец, умноженный на β_{2k} и так далее, n-й столбец, умноженный на β_{nk}. После этого на местах элементов $\beta_{1k}, \beta_{2k}, \ldots, \beta_{nk}$ окажутся нули. Повторяя эту операцию для всех $1 \leqslant k \leqslant n$, мы получим, что все элементы матрицы B заменяются на нули. Однако, нули, стоящие в правом верхнем углу, испортятся.

$$(\Delta)_{i,n+k} = \alpha_{i1}\beta_{1k} + \alpha_{i2}\beta_{2k} + \ldots + \alpha_{in}\beta_{nk} = \gamma_{ik}.$$

Следовательно, в правом верхнем углу вместо нулей будут стоять элементы матрицы C.

$$\Delta = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} & \gamma_{11} & \gamma_{12} & \ldots & \gamma_{1n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn} & \gamma_{n1} & \gamma_{n2} & \ldots & \gamma_{nn} \\ -1 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & -1 & 0 & 0 & \ldots & 0 \end{vmatrix}.$$

Применим к определителю Δ теорему Лапласа к последним n столбцам. $\Delta = MA_M$, где M — определитель матрицы C. $\widetilde{M} = (-1)^n$,

$$S_M = 1+2+\ldots+n+((n+1)+(n+2)+\ldots+2n) = \frac{1+2n}{2}2n = n+2n^2.$$

Подсчитаем A_M

$$A_M = (-1)^{S_M}\widetilde{M} = (-1)^{n+2n^2}(-1)^n = (-1)^{2n+2n^2} = 1,$$

Таким образом $\Delta = |C| \cdot 1 = |C| = |AB|$.

Сравнивая эти два результата имеем: $|AB| = |A| \cdot |B|$. □

4.3. Обратимость матриц

Определение 4.3.1. Единичной матрицей порядка n называется квадратная матрица n-порядка E вида:

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

Вспоминаем обозначение символа Кранекера:

$$\delta_{ij} = \begin{cases} 1, & \text{если } i = j, \\ 0, & \text{если } i \neq j. \end{cases}$$

Таким образом можно записать, что $(E)_{ij} = \delta_{ij}$.

Предложение 4.3.1. *Единичная матрица играет роль единицы при умножении матриц, то есть*

$$(\forall\ A) \quad AE = EA = A. \tag{4.1}$$

Доказательство. Действительно, матрицы AE, EA, A — все квадратные n-порядка. Покажем равенство соответствующих элементов.

$$(AE)_{ik} = \sum_{j=1}^{n} (E)_{ij}(A)_{jk} = \sum_{j=1}^{n} \delta_{ij}(A)_{jk} = (A)_{ik}.$$

□

Замечание 4.3.1. Единичная матрица E, удовлетворяющая условию (4.1) единственна.

В самом деле, пусть наряду с E существует E_1, удовлетворяющие условию $(\forall B) \quad BE = EB = B$, тогда составим

$$EE_1 = \begin{cases} E, \\ E_1 \end{cases} \Rightarrow E = E_1.$$

Определение 4.3.2. Квадратная матрица A называется обратимой, если существует матрица X такая, что $AX = XA = E$, где E — единичная матрица. В этом случае, матрица X называется обратимой для матрицы A.

Если матрица A обратима, то обратная матрица X обозначается A^{-1}.

Предложение 4.3.2. *Квадратная матрица A может иметь не более одной обратной матрицы.*

Доказательство. Действительно, пусть X и Y две обратные матрицы для матрицы A. Тогда составим произведение

$$XAY = \begin{cases} (XA)Y = EY = Y, \\ X(AY) = XE = X \end{cases} \Rightarrow X = Y.$$

□

Определение 4.3.3. Квадратная матрица A называется особенной (вырожденной), если ее определитель равен нулю, и называется не особенной (не вырожденной), если ее определитель не равен нулю.

Из теоремы 4.2.3 вытекает следующее следствие.

Следствие 4.2.3.1. Произведение нескольких квадратных матриц не вырождено тогда и только тогда, когда каждая из перемножаемых матриц является не вырожденной.

Предложение 4.3.3. *Особенная матрица не имеет обратной матрицы, то есть она является не обратимой.*

Доказательство. Допустим противное, то есть матрица A — особенная, тем не менее, существует матрица X такая, что $AX = XA = E$. Перейдем к определителю $|A||X| = |AX| = |E| = 1$, получаем, что $0 \cdot |X| = 1$ — этого быть не может, следовательно, такой матрицы X не существует. □

Определение 4.3.4. Присоединенной (взаимной) матрицей для матрицы A называется матрица A^*, транспонированная к матрице, составленной из алгебраических дополнений соответствующих элементов матрицы A.

Определение 4.3.4 означает, что

$$A^* = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \dots & \dots & \dots & \dots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{pmatrix}^T = \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix}.$$

ТЕОРЕМА 4.3.1. *Произведение матрицы A слева или справа на присоединенную к ней матрицу A^* равно определителю матрицы A, умноженному на еденичную матрицу, то есть $AA^* = A^*A = |A|\, E$.*

Доказательство. Ясно, что матрицы AA^*, A^*A, $|A|\, E$ существуют и являются квадратными матрицами n-порядка. Покажем равенство соответствующих элементов этих матриц.

$$(AA^*)_{ik} = \sum_{j=1}^{n} (A)_{ij} A^*_{jk} = \sum_{j=1}^{n} \alpha_{ij} A_{jk} = \delta_{ik} |A| = |A|\, (E)_{ik} = (|A|\, E)_{ik}.$$

Сравним начало и конец записи: $(A^*)_{ik} = (|A|\, E)_{ik}, 1 \leqslant i, k \leqslant n$. Следовательно, $AA^* = |A|\, E$. Аналогично $A^*A = |A|\, E$. □

ТЕОРЕМА 4.3.2 (об обратимости матриц)**.** *Квадратная матрица A является обратимой тогда и только тогда, когда она не особенная. В случае не особенности матрицы A имеет место формула:*

$$A^{-1} = \frac{1}{|A|} A^*.$$

Доказательство. 1) Пусть матрица является обратимой. Тогда она должна быть не особенной, так как если бы она была особенной, то по предложению 4.3.3, она не имела бы обратной матрицы.

2) Пусть матрица является не особенной, то есть $|A| \neq 0$. Тогда рассмотрим соотношение: $AA^* = A^*A = E\,|A|$. Разделим все части этого равенства на $|A|$, получим

$$\frac{1}{|A|}(AA^*) = \frac{1}{|A|}(A^*A) = E.$$

$$A\left(\frac{1}{|A|}A^*\right) = \left(\frac{1}{|A|}A^*\right)A = E.$$

По определению 4.3.2 матрица A является обратимой, и обратной для нее матрицей является матрица

$$A^{-1} = \frac{1}{|A|}A^*.$$

□

Следствие. Если матрицы A и B обратимы, то справедливы следующие равенства:

1. $\left|A^{-1}\right| = |A|^{-1}$;
2. $(A^{-1})^{-1} = A$;
3. $(AB)^{-1} = (B)^{-1}(A)^{-1}$;
4. $(A^T)^{-1} = (A^{-1})^T$.

Доказательство. 1) Так как матрица A обратима, то существует матрица A^{-1} такая, что $AA^{-1} = A^{-1}A = E$. Перейдем к определителю в этом равенстве $\left|AA^{-1}\right| = |E|$.

$$|A|\left|A^{-1}\right| = 1 \Rightarrow \left|A^{-1}\right| = \frac{1}{|A|}.$$

2) Так как матрица A обратима, то существует матрица A^{-1} такая, что $AA^{-1} = A^{-1}A = E$. Эти равенства по определению 4.3.2 означают, что

матрица A^{-1} является обратимой и обратной для нее матрицей является матрица A, то есть $(A^{-1})^{-1} = A$.

3) Так как матрицы A и B обратимы, то существуют матрицы A^{-1} и B^{-1} такие, что $AA^{-1} = A^{-1}A = E$; $BB^{-1} = B^{-1}B = E$. Составим произведение $X = B^{-1}A^{-1}$. Подсчитаем

$$(AB)X = (AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AEA^{-1} = AA^{-1} = E.$$

Составим произведение в обратном порядке, то есть

$$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}EB = B^{-1}B = E.$$

Видно, что $(AB)X = X(AB) = E$. По определению 4.3.2 эти равенства означают, что матрица AB является обратимой и обратной для нее матрицей является матрица $X = B^{-1}A^{-1}$.

4) Так как матрица A обратима, то существует матрица A^{-1} такая, что $AA^{-1} = A^{-1}A = E$. Перейдем к транспонированным матрицам, получим:

$$(A^{-1})^T A^T = A^T (A^{-1})^T = E.$$

По определению 4.3.2 последние соотношения указывает на то, что матрица A^T является обратимой и обратной для нее матрицей является матрица $X = (A^{-1})^T$. Таким образом, $(A^T)^{-1} = (A^{-1})^T$. □

4.4. Матричные уравнения

Определение 4.4.1. Матричными уравнениями называются уравнения вида $A \cdot X = B$, $Y \cdot A = B$, где A, B — заданные матрицы, а X, Y — искомые матрицы.

Если матрица A является не особенной, то эти матричные уравнения решаются легко. Достаточно положить $X = A^{-1}B$, $Y = BA^{-1}$. Действительно,

$$A(A^{-1}B) = (AA)B^{-1} = EB = B, \qquad (BA^{-1})A = B(A^{-1}A) = BE = B.$$

В матричном виде можно записать систему линейных уравнений, изученную в главе 3. Рассмотрим систему:

$$\begin{aligned} &\alpha_{11}x_{11} + \alpha_{12}x_2 + \ldots + \alpha_{1n}x_n = \beta_1, \\ &\ldots, \\ &\alpha_{m1}x_1 + \alpha_{m2}x_2 + \ldots + \alpha_{mn}x_n = \beta_m. \end{aligned} \tag{4.2}$$

Как всегда через A обозначим матрицу этой системы

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{m1} & \alpha_{m2} & \ldots & \alpha_{mn} \end{pmatrix}, \quad X = \begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_n \end{pmatrix}, \quad B = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \ldots \\ \beta_m \end{pmatrix},$$

где X — столбец неизвестных, B — столбец свободных членов. Размерность $A : m \times n,\ X : n \times 1,\ B : m \times 1$. Видно, что произведение AX существует и будет матрицей размерности $m \times 1$, то есть той же размерности, что и матрица B. Покажем равенство соответствующих элементов матриц

$$(AX)_i = \alpha_{i1}x_1 + \alpha_{i2}x_2 + \ldots + \alpha_{in}x_n = \beta_i = (B)_i,$$

$$(\forall\ 1 \leqslant i \leqslant m) \quad (AX)_i = (B)_i, \quad \Rightarrow \quad AX = B. \tag{4.3}$$

(4.3) — есть матричная запись системы линейных уравнений (4.2). Рассмотрим частный случай $m = n$ и $|A| \neq 0$. Как известно из пункта 3.3., в этом случае система (4.2) имеет единственное решение

$$x_k = \frac{\Delta_k}{\Delta}, \quad 1 \leqslant k \leqslant n, \quad \Delta = |A|\,.$$

В то же время, уравнение (4.3) имеет своим решением $X = A^{-1}B$. Следовательно, $X = A^{-1}B$ представляет из себя матричную запись формул Крамера.

4.5. Ранг произведения матриц

Прежде всего отметим, что нет точного равенства, связывающего ранг произведения матриц с рангами перемножаемых матриц.

Пример:

$$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 6 & 0 \\ 0 & 0 \end{pmatrix}.$$

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

ТЕОРЕМА 4.5.1 (о ранге произведения матриц)**.** *Справедливы следующие два утверждения:*

1. *ранг произведения нескольких матриц не превосходит рангов каждой из перемножаемых матриц;*
2. *ранг произведения матрицы A слева или справа на не особенную матрицу B равен рангу матрицы A.*

Доказательство. 1) Первое утверждение достаточно доказать для произведения двух матриц. Общий случай сводится к двум матрицам. Пусть AB существует и $AB = C$.

$$A = (\alpha_{ij}),\ 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n,\ B = (\beta_{jk}),\ 1 \leqslant k \leqslant p.$$

Тогда

$$C = (\gamma_{ik}),\ \gamma_{ik} = \alpha_{i1}\beta_{1k} + \alpha_{i2}\beta_{2k} + \ldots + \alpha_{in}\beta_{nk}. \tag{4.4}$$

Зафиксируем $1 \leqslant k \leqslant p$ и запишем равенство (4.4) для всех $1 \leqslant i \leqslant m$. Имеем,

$$\begin{pmatrix} \gamma_{1k} \\ \gamma_{2k} \\ \ldots \\ \gamma_{mk} \end{pmatrix} = \beta_{1k} \begin{pmatrix} \alpha_{11} \\ \alpha_{21} \\ \ldots \\ \alpha_{m1} \end{pmatrix} + \beta_{2k} \begin{pmatrix} \alpha_{12} \\ \alpha_{22} \\ \ldots \\ \alpha_{m2} \end{pmatrix} + \ldots + \beta_{nk} \begin{pmatrix} \alpha_{1n} \\ \alpha_{2n} \\ \ldots \\ \alpha_{mn} \end{pmatrix}.$$

Видно, что k-столбец матрицы C линейно выражается через все столбцы матрицы A. Меняя $1 \leqslant k \leqslant p$, получим, что все столбцы матрицы C линейно выражаются через столбцы матрицы A. Тогда можно записать $r(AB) = r(C) = r\{\text{системы столбцов матрицы } C\} \leqslant r\{\text{системы столбцов матрицы } A\}$ (по первому свойству ранга) $= r(A)$. Следовательно, $r(AB) \leqslant r(A)$.

Обратимся опять к равенству (4.4). Зафиксируем $1 \leqslant i \leqslant m$ и запишем равенство (4.4) для всех $1 \leqslant k \leqslant p$. Получим, что i-строка матрицы C линейно выражается через все строки матрицы B с коэффициентами $\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{in}$. Меняя $1 \leqslant i \leqslant m$, получим, что все строки матрицы C линейно выражается через строки матрицы B. Тогда можно записать $r(AB) = r(C) = r\{\text{системы строк матрицы } C\}$ (по следствию 2.4.1.1 из теоремы о ранге матрицы) $\leqslant r\{\text{системы строк матрицы } B\}$ (по первому свойству ранга) $= r(B)$. Следовательно, $r(AB) \leqslant r(B)$.

2) Пусть B — не особенная матрица. Тогда $r(AB) \leqslant r(A)$. Обозначим $AB = C$, тогда $A = CB^{-1}$.

$$r(A) = r(CB^{-1}) \leqslant r(C) = r(AB).$$

Следовательно имеет место равенство $r(AB) = r(A)$. □

Глава 5

Комплексные числа

5.1. Поле комплексных чисел. Действия над комплексными числами

Определение 5.1.1. Полем комплексных чисел называется минимальное расширение поля действительных чисел, содержащее корень уравнения $x^2 + 1 = 0$.

Определение 5.1.2. Поле $\mathbb{C}$ называется полем комплексных чисел, если оно удовлетворяет следующим трем условиям:

1) $\mathbb{R} \subset \mathbb{C}$;

2) $(\exists\, i \in \mathbb{C}) \qquad i^2 = -1$;

3) если $\mathbb{R} \subset \mathbb{C}' \subset \mathbb{C}$, то все такие поля $\mathbb{C}'$ не обладают свойством 2).

ТЕОРЕМА 5.1.1. *Существует единственное, с точностью до обозначения корня уравнения* $x^2 + 1 = 0$, *поле комплексных чисел* $\mathbb{C}$. *Каждый элемент* z *поля* $\mathbb{C}$ *единственным образом представим в виде* $z = a + bi$, *где* $a, b \in \mathbb{R}, \quad i^2 = -1$.

Определение 5.1.3. Любой элемент z поля $\mathbb{C}$ называется комплексным числом. Элемент $i \in \mathbb{C}$, для которого $i^2 = -1$, называется мнимой единицей. Запись $z = a + bi$, где $a, b \in \mathbb{R},\ i^2 = -1$, называется алгебраической формой комплексного числа.

Определение 5.1.4. Если $z = a + bi$, то a называется действительной частью, а b называется мнимой частью комплексного числа z.

Обозначим $a = Re(z) = R(z)$ — действительная часть, $b = Im(z) = I(z)$ — мнимая часть.

Теорема 5.1.1 означает, что $a + bi = c + di$ тогда и только тогда, когда $a = c$ и $b = d$. Из этой же теоремы 5.1.1 следует, что действия с комплексными числами производятся так же, как с обычными двучленами $a + bi$ с заменой $i^2 = -1$. Поэтому, используя свойства сложения и умножения поля $\mathbb{C}$, получаем следующие правила действий над комплексными числами.

Пусть $z_1 = a + bi,\ z_2 = c + di$.

1. $z_1 + z_2 = (a + bi) + (c + di) = (a + c) + (b + d)i$;
2. $z_1 - z_2 = (a + bi) - (c + di) = (a - c) + (b - d)i$;
3. $z_1 \cdot z_2 = (a + bi) \cdot (c + di) = (ac - bd) + (ac + bc)i$;
4. Если $z_2 \neq 0$, то имеем $\dfrac{z_1}{z_2} = \dfrac{a + bi}{c + di} = \dfrac{(a + bi)(c - di)}{(c + di)(c - di)} = \dfrac{(ac + bd) + (bc - ad)i}{c^2 + d^2} = \dfrac{ac + bd}{c^2 + d^2} + \dfrac{bc - ad}{c^2 + d^2}i.$

Определение 5.1.5. Комплексно сопряженным для числа $z = a + bi$ называется комплексное число $\overline{z} = a - bi$.

Предложение 5.1.1. *Сумма и произведение двух комплексно сопряженных чисел есть числа действительные.*

Доказательство. В самом деле,

$$z + \overline{z} = (a + bi) + (a - bi) = 2a \in \mathbb{R};$$

$$z \cdot \overline{z} = (a + bi) \cdot (a - bi) = a^2 + b^2 \in \mathbb{R}, \quad (z \cdot \overline{z} \geqslant 0).$$

□

Предложение 5.1.2 (свойства комплексно сопряженных чисел)**.** *Имеют место следующие равенства:*

1. $\overline{z_1 \pm z_2} = \overline{z}_1 \pm \overline{z}_2$;

2. $\overline{z_1 \cdot z_2} = \overline{z}_1 \cdot \overline{z}_2$;

3. $\overline{\left(\dfrac{z_1}{z_2}\right)} = \dfrac{\overline{z}_1}{\overline{z}_2}, \quad (z_2 \neq 0)$;

4. *если* $z = a \in \mathbb{R}$, *то* $\overline{z} = z$.

Доказательство. Пусть $z_1 = a + bi,\ z_2 = c + di$.

1) $\overline{z_1 \pm z_2} = \overline{(a \pm c) + (b \pm d)i} = (a \pm c) - (b \pm d)i = (a - bi) \pm (c - di) = \overline{z}_1 \pm \overline{z}_2$.

2) $\overline{z_1 \cdot z_2} = \overline{(ac - bd) + (ad + bc)i} = (ac - bd) - (ad + bc)i = (a - bi)(c - di) = \overline{z}_1 \cdot \overline{z}_2$.

3) Обозначим $\dfrac{z_1}{z_2} = z$. Тогда $z_1 = z \cdot z_2$; $\quad \overline{z}_1 = \overline{z \cdot z_2} = \overline{z} \cdot \overline{z}_2$. То есть $\overline{z} = \dfrac{\overline{z}_1}{\overline{z}_2}$. Получили $\overline{\left(\dfrac{z_1}{z_2}\right)} = \dfrac{\overline{z}_1}{\overline{z}_2}$.

4) Если $z = a \in \mathbb{R}$, то $\overline{z} = \overline{a} = \overline{a + 0i} = a - 0i = a = z$. □

Определение 5.1.6. Модулем комплексного числа называется арифметическое значение квадратного корня из суммы квадратов его действительной и мнимой частей.

Определение 5.1.6 означает, что если $z = a + bi$, то модуль комплексного числа $|z| = \sqrt{a^2 + b^2}$.

Свойства модуля

1. $|z| \geqslant 0; \quad |z| = 0 \Leftrightarrow z = 0$.

2. Если $z = a \in \mathbb{R}$, то $|z| = |a|$.

3. $|\overline{z}| = |z|$.

4. $z \cdot \overline{z} = |z|^2$.

5. $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$.

6. $\left|\dfrac{z_1}{z_2}\right| = \dfrac{|z_1|}{|z_2|}, \quad (z_2 \neq 0)$.

7. $\dfrac{z_1}{z_2} = \dfrac{z_1 \cdot \overline{z_2}}{|z_2|^2}, \quad (z_2 \neq 0)$.

Доказательство. 1) $|z| = \sqrt{a^2+b^2} \geqslant 0$. $|z| = 0 \Leftrightarrow \sqrt{a^2+b^2} = 0 \Leftrightarrow$ $\Leftrightarrow a^2+b^2 = 0 \Leftrightarrow a = 0$ и $b = 0 \Leftrightarrow z = a+bi = 0$.

2) Если $z = a \in \mathbb{R}$, то $|z| = |a| = |a+0i| = \sqrt{a^2+0^2} = \sqrt{a^2} = |a|$.

Замечание 5.1.1. Второе свойство указывает на то, что понятие модуля комплексного числа есть обобщение понятия абсолютной величины действительного числа, то есть абсолютная величина числа — это частный случай модуля комплексного числа.

3) $|\overline{z}| = |a-bi| = \sqrt{a^2+(-b)^2} = \sqrt{a^2+b^2} = |z|$.

4) $z \cdot \overline{z} = a^2+b^2 = |z|^2$.

5) $|z_1 \cdot z_2| = |(ac-bd)+(ad+bc)i| = \sqrt{(ac-bd)^2+(ad+bc)^2} =$ $= \sqrt{a^2c^2+b^2d^2+a^2d^2+b^2c^2} = \sqrt{(a^2+b^2)(c^2+d^2)} = \sqrt{a^2+b^2} \times$ $\times \sqrt{c^2+d^2} = |z_1| \cdot |z_2|$.

6) $|z_1| = \left|\dfrac{z_1}{z_2} \cdot z_2\right| = \left|\dfrac{z_1}{z_2}\right| \cdot |z_2|$. Получили $\dfrac{|z_1|}{|z_2|} = \left|\dfrac{z_1}{z_2}\right|$.

7) $\dfrac{z_1}{z_2} = \dfrac{z_1 \cdot \overline{z_2}}{z_2 \cdot \overline{z_2}} = \dfrac{z_1 \cdot \overline{z_2}}{|z_2|^2}$. □

5.2. Геометрическое изображение комплексных чисел

Пусть $\mathbb{C}$ — поле комплексных чисел и $z = a+bi \in \mathbb{C}$. Можно рассматривать биекцию $f : \mathbb{C} \to \mathbb{R} \times \mathbb{R}$, которая комплексному числу $z = a+bi$ ставит в соответствие пару (a, b).

Возьмем прямоугольную систему координат XOY. Как известно, существует биекция $g : (a, b) \to M(a, b)$ или радиус-вектор $\overline{r}(a, b)$. Тогда рассмотрим композицию $g \circ f : z = a+bi \to \overline{r}(a, b)$.

В этом случае говорят, что точка M или вектор $\overline{r}$ изображают комплексное число z. В этом случае, ось OX называется действительной осью, ось OY — мнимой осью, а вся плоскость XOY называется комплексной плоскостью.

Заметим, что длина $|\overline{r}| = \sqrt{a^2 + b^2} = |z|$. Поэтому геометрически, модуль комплексного числа z есть длина вектора, изображающего это комплексное число z.

Коль скоро мы имеем геометрическое изображение комплексных чисел, то можно поставить вопрос о геометрическом изображении операций над комплексными числами. Для суммы и разности это делается легко. Пусть $z_1 = a + bi,\ z_2 = c + di$.

Сложим эти векторы по правилу параллелограмма. Тогда эта точка изображает сумму z_1 и z_2.

Очевидно, что $-z_2$ изображается вектором, противоположным для вектора, изображающего z_2. Тогда $z_1 - z_2 = z_1 + (-z_2)$.

Из геометрического смысла модуля и теоремы геометрии о длинах сторон треугольника вытекают следующие свойства модулей:

1. $|z_1 + z_2| \leqslant |z_1| + |z_2|$;
2. $|z_1 - z_2| \geqslant |z_1| - |z_2|$.

Эти 2 свойства можно объединить: $||z_1| - |z_2|| \leqslant |z_1 \pm z_2| \leqslant |z_1| + |z_2|$.

Определение 5.2.1. Аргументом ненулевого комплексного числа z называется величина угла между положительным направлением действительной оси OX и направлением вектора, изображающего это комплексное число z.

$arg\ z = \varphi$

Замечание 5.2.1. Угол между двумя направлениями понимается в широком смысле слова, как это делается в тригонометрии, то есть наряду с углом φ можно рассматривать и углы, получающиеся из него прибавлением целого числа полных оборотов.

Таким образом, у ненулевого комплексного числа z существует бесчисленное множество аргументов. Все они отличаются друг от друга на число, кратное 2π радианам: $2\pi k,\ k \in \mathbb{Z}$.

Замечание 5.2.2. Для комплексных чисел нельзя ввести понятие больше или меньше, так как эти числа изображаются точками плоскости, а не точками прямой, которые, естественно, упорядочены. Поэтому между комплексными числами никогда не ставятся знаки $>,\ <,\ \geqslant,\ \leqslant$.

5.3. Тригонометрическая форма комплексного числа

Определение 5.3.1. Тригонометрической формой ненулевого комплексного числа z называется любое его представление вида

$$z = \rho(\cos\varphi + i\sin\varphi), \qquad \text{где} \quad \rho > 0,\ \varphi \in \mathbb{R}.$$

Замечание 5.3.1. Если $z = \rho(\cos\varphi + i\sin\varphi)$, то

$$(\forall\ k \in \mathbb{Z}) \qquad z = \rho[\cos(\varphi + 2\pi k) + i\sin(\varphi + 2\pi k)].$$

Второе представление числа z существенно совпадает с первым представлением.

ТЕОРЕМА 5.3.1 (о существовании и единственности тригонометрической формы)**.** *Любое ненулевое комплексное число обладает единственной в существенном совпадающей тригонометрической формой.*

Доказательство. Пусть $z = a + bi \neq 0$.

Обозначим длину вектора $|\overline{r}| = |z| = \rho > 0$, а через $\varphi = \arg z$. Видно, что $a = \rho\cos\varphi;\ b = \rho\sin\varphi$. $z = a + bi = \rho(\cos\varphi + i\sin\varphi),\ \rho > 0$.

Установим единственность в существенном. Пусть наряду с $z = \rho(\cos\varphi + i\sin\varphi),\ \rho > 0$ есть и другое представление $z = r(\cos\psi + i\sin\psi),\ r > 0$. Тогда $\rho(\cos\varphi + i\sin\varphi) = (\cos\psi + i\sin\psi) \Leftrightarrow \rho\cos\varphi = r\cos\psi$ и $\rho\sin\varphi = r\sin\psi$. Возведем в квадрат обе части последних двух равенств и сложим их, получим $\rho^2(\cos^2\varphi + \sin^2\varphi) = r^2(\cos^2\psi + \sin^2\psi)$. То есть $\rho^2 = r^2$. Следовательно, так как $\rho, r > 0$, имеем $\rho = r$. Подставляем $\rho = r$ в соотношения, получим:

$$\left.\begin{array}{l}\cos\varphi = \cos\psi\\ \sin\varphi = \sin\psi\end{array}\right\} \Rightarrow \psi = \varphi + 2\pi k, \quad \text{где} \quad k \in \mathbb{Z}.$$

Вторая тригонометрическая форма будет выглядеть так:
$z = \rho[\cos(\varphi + 2\pi k) + i\sin(\varphi + 2\pi k)]$ — это второе представление в существенном совпадает с первым. □

Следствие. Если $z = \rho(\cos\varphi + i\sin\varphi)$, где $\rho > 0$, то $\rho = |z|,\ \varphi = \arg z$.

Это следует из доказательства теоремы и единственности представления.

Если $z = a + bi \neq 0$ — алгебраическая форма комплексного числа z, то тригонометрическую форму можно найти используя следующие формулы

$$\rho = \sqrt{a^2 + b^2}, \qquad \begin{cases}\sin\varphi = \dfrac{b}{\rho},\\ \cos\varphi = \dfrac{a}{\rho}.\end{cases}$$

Замечание 5.3.2. Угол φ можно находить из одного соотношения, а именно, $\operatorname{tg}\varphi = \dfrac{b}{a}$. Но в этом случае, угол φ надо выбирать из той четверти, в которой находится точка, изображающая число z.

Примеры:

1) $z = 1 + i$. Это число изображает точка, находящаяся в первой четверти. $\rho = \sqrt{1^2 + 1^2} = \sqrt{2}$; $\operatorname{tg}\varphi = \frac{1}{1} = 1 \Rightarrow \varphi = \frac{\pi}{4} + \pi k$. Выбираем $k = 0$, так как точка лежит в первой четверти, то есть $\varphi = \frac{\pi}{4}$. Имеем

$$z = \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right).$$

2) $z = -1 - i$.Это число изображает точка, находящаяся в третьей четверти. $\rho = \sqrt{(-1)^2 + (-1)^2} = \sqrt{2}$; $\operatorname{tg}\varphi = \frac{-1}{-1} = 1 \Rightarrow \varphi = \frac{\pi}{4} + \pi k$. Выбираем $k = 1$, так как точка лежит в третьей четверти, то есть $\varphi = \frac{5\pi}{4}$. Имеем

$$z = \sqrt{2}\left(\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}\right).$$

5.4. Действия с комплексными числами в тригонометрической форме

ТЕОРЕМА 5.4.1. *При умножении комплексных чисел в тригонометрической форме их модули перемножаются, а аргументы складываются. При делении двух комплексных чисел в тригонометрической форме их модули делятся, а аргументы вычитаются.*

Доказательство. Пусть

$$z_1 = \rho_1(\cos\varphi_1 + i\sin\varphi_1),\ \rho_1 > 0, \quad z_2 = \rho_2(\cos\varphi_2 + i\sin\varphi_2),\ \rho_2 > 0.$$

1) Первое утверждение достаточно доказать для произведения двух сомножителей. Общий случай сводится к двум сомножителям.

$$z_1 \cdot z_2 = \rho_1(\cos\varphi_1 + i\sin\varphi_1) \cdot \rho_2(\cos\varphi_2 + i\sin\varphi_2) =$$

$$= \rho_1\rho_2[(\cos\varphi_1 \cdot \cos\varphi_2 - \sin\varphi_1 \cdot \sin\varphi_2) + i(\sin\varphi_1 \cdot \cos\varphi_2 + \cos\varphi_1 \cdot \sin\varphi_2)] =$$

$$= \rho_1\rho_2[\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)].$$

2) Обозначим через $z = \frac{z_1}{z_2}$. Будем искать z в виде

$$z = \rho(\cos\varphi + i\sin\varphi),\ \rho > 0.$$

Найдем ρ и φ. $z_1 = z \cdot z_2$. Тогда в силу первой части теоремы $\rho_1 = \rho \cdot \rho_2$, а аргумент $\varphi_1 = \varphi + \varphi_2$. Отсюда находим, что

$$\rho = \frac{\rho_1}{\rho_2}, \quad \varphi = \varphi_1 - \varphi_2.$$

Подставим их в выражение для z, получим

$$\frac{z_1}{z_2} = z = \frac{\rho_1}{\rho_2}[\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)].$$

□

ТЕОРЕМА 5.4.2 (формула Муавра)**.** *Для любого $n \in \mathbb{Z}$ справедливо следующее равенство*

$$[\rho(\cos\varphi + i\sin\varphi)]^n = \rho^n(\cos n\varphi + i\sin n\varphi).$$

Доказательство. а) Пусть $n \in \mathbb{N}$. Докажем теорему для этого случая методом математической индукции по n.

1 шаг. Если $n = 1$, то $[\rho(\cos\varphi + i\sin\varphi)]^1 = \rho^1(\cos(1 \cdot \varphi) + i\sin(1 \cdot \varphi))$

2 шаг. Предположим, что формула верна для $n = k$, то есть

$$[\rho(\cos\varphi + i\sin\varphi)]^k = \rho^k(\cos k\varphi + i\sin k\varphi).$$

Докажем ее справедливость для $n = k + 1$.

$$[\rho(\cos\varphi + i\sin\varphi)]^{k+1} = [\rho(\cos\varphi + i\sin\varphi)]^k \cdot \rho(\cos\varphi + i\sin\varphi) =$$

$$= \rho^k(\cos k\varphi + i\sin k\varphi) \cdot \rho(\cos\varphi + i\sin\varphi) = \rho^{k+1}(\cos(k+1)\varphi + i\sin(k+1)\varphi).$$

б) Если $n = 0$, то $[\rho(\cos\varphi + i\sin\varphi)]^0 = \rho^0(\cos(0 \cdot \varphi) + i\sin(0 \cdot \varphi))$.

в) Рассмотрим $n = -m,\ m \in \mathbb{N}$.

$$[\rho(\cos\varphi + i\sin\varphi)]^n = [\rho(\cos\varphi + i\sin\varphi)]^{-m} =$$
$$= \frac{1}{\rho^m(\cos m\varphi + i\sin m\varphi)} = \frac{1(\cos 0 + i\sin 0)}{\rho^m(\cos m\varphi + i\sin m\varphi)} =$$
$$= \rho^{-m}(\cos(-m)\varphi + i\sin(-m)\varphi) = \rho^n(\cos n\varphi + i\sin n\varphi).$$

□

Определение 5.4.1. Корнем n-й степени ($n \in \mathbb{N},\ n \geqslant 2$) из комплексного числа z называется комплексное число x, n-я степень которого равна z, то есть $x^n = z$.

Операция извлечения корня n-й степени из ненулевого комплексного числа всегда неоднозначно. Множество всех корней n-й степени из числа z обозначается: $\sqrt[n]{z}$.

ТЕОРЕМА 5.4.3. *Из ненулевого комплексного числа*

$$z = r(\cos\varphi + i\sin\varphi)$$

можно извлечь точно n различных корней n-й степени. При этом имеет место формула

$$\sqrt[n]{z} = \left\{ \sqrt[n]{r}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right) \middle| \ 0 \leqslant k \leqslant n-1 \right\},$$

где $\sqrt[n]{r}$ — арифметический корень.

Доказательство. 1) Покажем, что все указанные числа являются корнями n-й степени из числа z. Обозначим через

$$z_k = \sqrt[n]{r}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right),\ 0 \leqslant k \leqslant n-1.$$

Возведем z_k в n-ю степень, получим

$$z_k^n = \left[\sqrt[n]{r}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right)\right]^n =$$

$$= (\sqrt[n]{r})^n \left[\cos(\varphi + 2\pi k) + i\sin(\varphi + 2\pi k)\right] = r(\cos\varphi + i\sin\varphi) = z.$$

2) Покажем, что все числа z_k различны. Пусть $z_k = z_l$ при $0 \leqslant k \leqslant$ $\leqslant l \leqslant n-1$. Покажем, что $k = l$.

$$\sqrt[n]{r}\left(\cos\frac{\varphi+2\pi k}{n} + i\sin\frac{\varphi+2\pi k}{n}\right) = \sqrt[n]{r}\left[\cos\frac{\varphi+2\pi l}{n} + i\sin\frac{\varphi+2\pi l}{n}\right].$$

В силу того, что тригонометрические формы совпадают в существенном, следует

$$\frac{\varphi+2\pi l}{n} = \frac{\varphi+2\pi k}{n} + 2\pi m,\ m \in \mathbb{Z}.$$

$$\varphi + 2\pi l = \varphi + 2\pi k + 2\pi mn \Rightarrow l = k + mn;$$

$$\left.\begin{array}{l} l - k = mn \\ 0 \leqslant l - k < n \end{array}\right\} \Rightarrow m = 0 \Rightarrow l = k.$$

3) Покажем, что других корней n-й степени из числа z не существует. Пусть x —любой корень n-й степени из числа z. Покажем, что он должен совпадать с одним из z_k. Пусть

$$x = \rho(\cos\psi + i\sin\psi), \quad \rho > 0, \quad x^n = z.$$

$$[\rho(\cos\psi + i\sin\psi)]^n = r(\cos\varphi + i\sin\varphi);$$

$$\rho^n(\cos n\psi + i\sin n\psi) = r(\cos\varphi + i\sin\varphi);$$

$$\rho^n = r, \quad n\psi = \varphi + 2\pi m,\ m \in \mathbb{Z};$$

$$\rho = \sqrt[n]{r}, \quad \psi = \frac{\varphi+2\pi m}{n},\ m \in \mathbb{Z};$$

$$x = \sqrt[n]{r}\Big(\cos\frac{\varphi+2\pi m}{n} + i\sin\frac{\varphi+2\pi m}{n}\Big).$$

Разделим m на n с остатком, получим $m = nq + k,\ 0 \leqslant k \leqslant n-1$.

$$\frac{\varphi+2\pi m}{n} = \frac{\varphi+2\pi k}{n} + 2\pi q;$$

$$x = \sqrt[n]{r}\left(\cos\frac{\varphi+2\pi k}{n} + i\sin\frac{\varphi+2\pi k}{n}\right),\ 0 \leqslant k \leqslant n-1 \Rightarrow x = z_k.$$

□

Замечание 5.4.1. Из формулы, доказанной в теореме 5.4.3, следует, что геометрически корни n-й степени из числа z изображаются точками окружности с центром в начале координат и радиуса $\sqrt[n]{|z|}$. Эти точки делят окружность на n равных частей.

5.5. Корни из единицы

Особо важным случаем является извлечение корня n-й степени из единицы. Как мы видим $1 = 1(\cos 0 + i \sin 0)$, где $r = 1$, $\varphi = 0$. Поэтому все корни n-й степени из единицы имеют вид

$$\sqrt[n]{1} = \left\{ \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} \middle| \, 0 \leqslant k \leqslant n-1 \right\}.$$

Геометрически корни n-й степени из единицы изображаются точками окружности с центром в начале координат и радиуса 1. Эти точки делят окружность на n равных частей, начиная с точки (1,0).

Видно, что не действительные корни n-й степени из единицы изображаются точками, симметричными относительно оси OX. Следовательно, они комплексно сопряжены.

В дальнейшем будем обозначать

$$\varepsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}, \; 0 \leqslant k \leqslant n-1.$$

Рассмотрим частные случаи

1. $n = 2$.

$$\varepsilon_k = \cos \pi k + i \sin \pi k, \quad k = 0, 1;$$

$$\varepsilon_0 = 1, \quad \varepsilon_1 = -1.$$

2. $n = 3$.

$$\varepsilon_k = \cos\frac{2\pi k}{3} + i\sin\frac{2\pi k}{3}, \quad k = 0, 1, 2;$$

$$\varepsilon_0 = 1, \quad \varepsilon_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \quad \varepsilon_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

3. $n = 4$.

$$\varepsilon_k = \cos\frac{\pi k}{2} + i\sin\frac{\pi k}{2}, \quad k = 0, 1, 2, 3;$$

$$\varepsilon_0 = 1, \quad \varepsilon_1 = i, \quad \varepsilon_2 = -1, \quad \varepsilon_3 = -i.$$

Обозначим через G_n — множество всех корней n-й степени из единицы, то есть

$$G_n = \left\{ \varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} \,\middle|\, 0 \leqslant k \leqslant n-1 \right\}.$$

Определение 5.5.1. Элемент ε называется образующим элементом G_n, если G_n состоит из степеней ε.

Предложение 5.5.1. *В множестве G_n всех корней n-й степени из единицы образующим элементом является ε_1.*

Доказательство. Действительно, $G_n = \{\varepsilon_0, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n-1}\}$. Возведем ε в степень k, $0 \leqslant k \leqslant n-1$.

$$\varepsilon_1^k = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = \varepsilon_k.$$

$\varepsilon_k = \varepsilon_1^k \Rightarrow G_n = \left\{\varepsilon_1^0, \varepsilon_1^1, \varepsilon_1^2, \ldots, \varepsilon_1^{n-1}\right\}$. Таким образом ε_1 — образующий элемент G_n. □

Предложение 5.5.2. *Если ε есть корень k-й степени из единицы, то он является и корнем n-й степени из единицы, если только $n = k \cdot q$.*

Доказательство. В самом деле, $\varepsilon^n = \varepsilon^{kq} = \left(\varepsilon^k\right)^q = 1^q = 1$. Поэтому среди всех корней G_n находятся все корни k-й степени из единицы, если только $n = k \cdot q$. □

Однако, для любого n среди корней n-й степени из единицы, существуют такие, которые не являются корнями из единицы никакой степени, меньшей, чем n.

Определение 5.5.2. Первообразным (примитивным) корнем n-й степени из единицы называется такой корень n-й степени из единицы, который не является корнем из единицы никакой степени, меньшей, чем n.

Определение 5.5.2 означает, что ε является первообразным корнем тогда и только тогда, когда:

1. $\varepsilon^n = 1$;

2. $(\forall\ 1 \leqslant k < n) \quad \varepsilon^k \neq 1$.

ТЕОРЕМА 5.5.1 (Первый критерий первообразности корня)**.** *Для того чтобы корень n-й степени из единицы был первообразным необходимо и достаточно, чтобы он был образующим элементом G_n.*

Доказательство. 1) Необходимость.

Пусть ε является первообразным корнем n-й степени из единицы. Это означает, что $\varepsilon^0, \varepsilon^1, \varepsilon^2, \ldots, \varepsilon^{n-1} \in G_n$. Покажем, что все эти n чисел различные. Допустим противное, то есть

$$\varepsilon^k = \varepsilon^l, \quad 0 \leqslant k < l \leqslant n-1.$$

$$\varepsilon^{l-k} = 1, \quad 0 < l-k \leqslant n-1.$$

Это противоречит первообразности корня ε. В результате имеем

$$G_n = \left\{\varepsilon^0, \varepsilon^1, \varepsilon^2, \ldots, \varepsilon^{n-1}\right\}.$$

Следовательно ε является образующим элементом G_n.

2) Достаточность.

Пусть ε является образующим элементом G_n. Тогда

$$G_n = \left\{\varepsilon^0, \varepsilon^1, \varepsilon^2, \ldots, \varepsilon^{n-1}\right\}.$$

Ясно, что $\varepsilon^n = 1$, но видно, что $(\forall\ 1 \leqslant k < n) \quad \varepsilon^k \neq 1$. Следовательно ε является первообразным корнем n-й степени из единицы. □

Определение 5.5.3. Наибольшим общим делителем двух целых чисел называется наибольшее натуральное число, на которое делятся оба этих числа.

Обозначим через (a, b) — наибольший общий делитель чисел a и b.
Пример: $(12, 15) = 3;\ (21, 16) = 1$.

Определение 5.5.4. Два целых числа a и b называются взаимно простыми, если их наибольший общий делитель $(a, b) = 1$.

ТЕОРЕМА 5.5.2 (второй критерий первообразности корня)**.** *Если ε является первообразным корнем n-й степени из единицы, то $\varepsilon' = \varepsilon^k$ также будет первообразным корнем n-й степени из единицы тогда и только тогда, когда k и n взаимно просты, то есть $(k, n) = 1$.*

Доказательство. 1) Необходимость.

Пусть ε' является первообразным корнем n-й степени из единицы. Надо доказать, что $(k, n) = 1$. Допустим противное, то есть $(k, n) = d > 1$. Тогда $k = k'd$, $n = n'd$, где $1 \leqslant n' < n$. Имеем

$$(\varepsilon')^{n'} = \left(\varepsilon^k\right)^{\frac{n}{d}} = \varepsilon^{n\frac{k}{d}} = (\varepsilon^n)^{k'} = 1^{k'} = 1.$$

Это противоречит первообразности корня ε'.

2) Достаточность.

Пусть $(k, n) = 1$. Надо показать, что ε' является первообразным корнем n-й степени из единицы. Допустим противное, то есть

$$(\exists\ 1 \leqslant s < n) \quad (\varepsilon')^s = 1.$$

Разделим ks на n с остатком, получим $ks = nq + r$, где $0 \leqslant r < n$. Тогда

$$1 = \varepsilon^{ks} = \varepsilon^{nq+r} = (\varepsilon^n)^q \cdot \varepsilon^r = 1^q \cdot \varepsilon^r = \varepsilon^r.$$

Получили $\varepsilon^r = 1$, где $0 \leqslant r < n$, но ε — первообразный корень n-й степени из единицы, значит, $r = 0$. Имеем $ks = nq$, где $q \in \mathbb{Z}$, следовательно $\frac{ks}{n} = q \in \mathbb{Z}$, где $1 \leqslant s < n$, то есть k делится на n. Это противоречит тому, что $(k, n) = 1$. □

ТЕОРЕМА 5.5.3. *Пусть z — ненулевое комплексное число и z_0 — одно из решений двучленного уравнения $x^n = z$. Тогда все решения этого уравнения и только они могут быть найдены в виде $x = z_0\varepsilon$, где ε пробегает все корни n-й степени из единицы.*

Доказательство. Указанные числа $z_0\varepsilon$ являются решениями данного двучленного уравнения. Действительно, $(z_0\varepsilon)^n = z_0^n \cdot \varepsilon^n = z \cdot 1 = z$. Далее, когда ε пробегает все корни n-й степени из единицы, то $z_0\varepsilon$ принимает n различных значений.

С другой стороны ясно, что уравнение $x^n = z$ имеет только n различных решений, так как существует только n различных значений корня n-й степени из z. Получаем, что множество $\{z_0\varepsilon\}$ исчерпывает все решения уравнения $x^n = z$. □

ТЕОРЕМА 5.5.4. *Чтобы найти все корни $\sqrt[n]{z}$ достаточно найти одно из значений этого корня и умножить его на все корни n–ой степени из единицы.*

Пример: $\sqrt[3]{27}$

$$z_0 = 3, \quad \varepsilon_0 = 1, \quad \varepsilon_{1,2} = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i.$$

$$\sqrt[3]{27} = \left\{3, -\frac{3}{2} + \frac{3\sqrt{3}}{2}i, \ -\frac{3}{2} - \frac{3\sqrt{3}}{2}i\right\}.$$

Глава 6

Многочлены

6.1. Кольцо многочленов

Пусть k — некоторое фиксированное поле.

Определение 6.1.1. Многочленом от неизвестного x над кольцом k называется формальное выражение вида

$$\sum_{i=0}^{\infty} \alpha_i x^i,$$

где x — символ неизвестного, α_i — элементы поля k, почти все равные 0, то есть $(\exists\ n \in \mathbb{N})\ (\forall\ i > n) \quad \alpha_i = 0$.

В дальнейшем многочлены будем обозначать $f(x)$, $g(x)$, $h(x)$, $f_1(x)$, $f_2(x)$,... или короче f, g, h, f_1, f_2,...

$$f(x) = \sum_{i=0}^{\infty} \alpha_i x^i. \tag{6.1}$$

Если в многочлене (6.1) $\forall\ 0 \leqslant i < \infty \quad \alpha_i = 0$, то многочлен будем называть нулевым и обозначать 0.

Определение 6.1.2. Слагаемые $\alpha_i x^i$ будем называть членами многочлена (6.1), а элементы α_i будем называть коэффициентами многочлена (6.1).

Если в многочлене (6.1) $\forall\ i > n \quad \alpha_i = 0$, то будем писать:

$$f(x) = \sum_{i=0}^{n} \alpha_i x^i \quad \text{или} \quad f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n. \tag{6.2}$$

Здесь при переходе от записи (6.1) к записи (6.2) мы пишем α_0 вместо $\alpha_0 x^0$. При этом α_0 называется свободным членом многочлена $f(x)$.

Определение 6.1.3. Степенью ненулевого многочлена $f(x)$ называется наибольший номер отличного от нуля коэффициента этого многочлена.

Обозначим через $\deg f(x)$ степень многочлена $f(x)$.

Если в записи (6.2) $\alpha_n \neq 0$, то степень многочлена $f(x)$ равна n, то есть $\deg f(x) = n$. В этом случае, $\alpha_n x^n$ называется старшим членом многочлена, α_n называется старшим коэффициентом многочлена.

Множество всех многочленов от неизвестного x над полем k обозначается $k[x]$ и называется кольцом многочленов над полем k.

Пусть

$$f(x) = \sum_{i=0}^{\infty} \alpha_i x^i,\ g(x) = \sum_{i=0}^{\infty} \beta_i x^i, \quad f, g \in k[x].$$

Определение 6.1.4. Два многочлена $f(x), g(x) \in k[x]$ называются равными, если равны все их коэффициенты при одинаковых степенях x, то есть $(\forall\ 0 \leqslant i < \infty) \quad \alpha_i = \beta_i$.

В множестве $k[x]$ введем две операции: сложения и умножения многочленов.

Определение 6.1.5. Суммой двух многочленов f и g называется многочлен

$$f + g = \sum_{i=0}^{\infty} (\alpha_i + \beta_i) x^i.$$

Произведением двух многочленов f и g называется многочлен

$$f \cdot g = \sum_{i=0}^{\infty} \gamma_i x^i, \quad \text{где} \quad \gamma_i = \sum_{\substack{\nu+\mu=i \\ \nu,\mu \geqslant 0}} \alpha_\nu \beta_\mu.$$

Замечание 6.1.1. Формула для умножения означает, что для того, чтобы перемножить два многочлена, достаточно каждый член первого многочлена умножить на каждый член второго многочлена и привести подобные члены.

Определение 6.1.5 корректно в том смысле, что $f+g$ и $f\cdot g$ действительно будут многочленами. Так как f и g — многочлены, то $(\exists\ n \in \in \mathbb{N})\ (\forall\ i > n) \quad \alpha_i = 0,\ \beta_i = 0$. Тогда $(\forall\ i > n) \quad \alpha_i + \beta_i = 0 \Rightarrow f+g$ является многочленом.

Для $f\cdot g$ подсчитаем $\gamma_i, \forall\ i > 2n$. Так как $i = \nu + \mu$, то из условия $i > 2n \Rightarrow \nu > n$ или $\mu > n \Rightarrow \alpha_\nu = 0$ или $\beta_\mu = 0 \Rightarrow \gamma_i = \sum \alpha_\nu\beta_\mu = 0$ для $i > 2n$. А это означает, что $f\cdot g$ является многочленом.

Рассмотрим вопрос о степени суммы и произведения двух многочленов.

Пусть $f \neq 0$ и $g \neq 0$ — многочлены из $k[x]$,

$$f(x) = \sum_{i=0}^{\infty} \alpha_i x^i, \quad g(x) = \sum_{i=0}^{\infty} \beta_i x^i.$$

Пусть $\deg f = n$, то есть $\alpha_n \neq 0,\ \deg g = m$, то есть $\beta_m \neq 0$. Обозначим через $N = \max(n, m)$.

Рассмотрим

$$f + g = \sum_{i=0}^{\infty} (\alpha_i + \beta_i) x^i.$$

Ясно, что $(\forall\ i > N) \quad \alpha_i = 0$ и $\beta_i = 0 \Rightarrow \gamma_i = \alpha_i + \beta_i = 0$. Следовательно, $\deg(f+g) \leqslant N$. Значит, $\underline{\deg(f+g) \leqslant \max(\deg f, \deg g)}$. Знак равенства достигается, например, при $n \neq m$.

Рассмотрим

$$f\cdot g = \sum_{i=0}^{\infty} \gamma_i x^i \quad \text{где} \quad \gamma_i = \sum_{\substack{\nu+\mu=i \\ \nu,\mu\geqslant 0}} \alpha_\nu\beta_\mu.$$

Если $i > n+m$, то $\nu > n$ или $\mu > m \Rightarrow \alpha_\nu = 0$ или $\beta_\mu = 0 \Rightarrow \gamma_i = 0$. Получаем $\deg f\cdot g \leqslant n+m$. Значит, $\deg f\cdot g \leqslant \deg f + \deg g$.

Сосчитаем

$$\gamma_{n+m} = \sum_{\nu+\mu=n+m} \alpha_\nu \beta_\mu = \alpha_n \beta_m.$$

Так как $\alpha_n \neq 0$ и $\beta_m \neq 0$, то $\alpha_n \beta_m \neq 0$. В этом случае $\gamma_{n+m} \neq 0$ и $\deg f \cdot g = \deg f + \deg g$.

6.2. Теорема о делении с остатком. Теорема Безу. Схема Горнера

ТЕОРЕМА 6.2.1 (о делении с остатком)**.** *Пусть k — поле, f и $g \in k[x]$, причем $g \neq 0$. Тогда существует единственная пара многочленов $q, r \in k[x]$ такая, что*

1) $f = gq + r$;

2) $r = 0$ (или $r \neq 0, \deg r < \deg g$).

Доказательство. I) Существование многочленов q и r.
а) Пусть $f = 0$ (или $f \neq 0, \deg f < \deg g$). В этом случае можно записать $f = 0 \cdot g + f, (q = 0,\ r = f)$. Условия 1) и 2) выполнены.
б) $f \neq 0$ и $\deg f \geqslant \deg g$. Пусть

$$f = \alpha_n x^n + \ldots + \alpha_0, \quad \alpha_n \neq 0,$$

$$g = \beta_m x^m + \ldots + \beta_0, \quad \beta_m \neq 0.$$

$\deg f = n,\ \deg g = m,\ n \geqslant m$. Построим многочлен

$$f_1 = f - \alpha_n \beta_m^{-1} x^{n-m} g. \tag{1}$$

Многочлен f_1 построен так, чтобы уничтожить старший член многочлена f. Имеем $f_1 = 0$ или $f_1 \neq 0$ и $\deg f_1 = n_1 < n$.

Если $n_1 < m$, то процесс построения многочленов заканчиваем. Если $n_1 \geqslant m$, то, обозначая через $\alpha_{n_1}^{(1)}$ старший коэффициент f_1, строим многочлен

$$f_2 = f_1 - \alpha_{n_1}^{(1)} \beta_m^{-1} x^{n_1-m} g. \tag{2}$$

Опять многочлен f_2 строится таким образом, чтобы уничтожить старший член многочлена f_1. Имеем $f_2 = 0$ или $f_2 \neq 0$ и $\deg f_2 = n_2 < n_1$.

Если $n_2 < m$, то процесс построения многочленов заканчиваем. Если $n_2 \geqslant m$, то продолжаем и т. д.

Заметим, что степени многочленов f, f_1, f_2, f_3,... образуют строго убывающую последовательность натуральных чисел, тогда в конце концов получим $n > n_1 > n_2 > \ldots > n_s$, где $n_s < m$.

$$f_s = f_{s-1} - \alpha_{n_{s-1}}^{(s-1)} \beta_m^{-1} x^{n_{s-1}-m} g, \qquad (s)$$

где $f_s = 0$ или $f_s \neq 0$ и $\deg f_s = n_s < m$.

Сложим почленно все равенства $(1), (2), \ldots, (s)$, получим

$$f_s = f - \left(\alpha_n \beta_m^{-1} x^{n-m} + \alpha_{n_1}^{(1)} \beta_m^{-1} x^{n_1-m} + \ldots + \alpha_{n_{s-1}}^{(s-1)} \beta_m^{-1} x^{n_{s-1}-m} \right) g.$$

Обозначим f_s через r,а содержимое скобки через q. Получим $r = f_s - qg \Rightarrow f = qg + r$, то есть получили равенство 1), где $\overline{r} = 0 \vee (\overline{r} \neq 0 \wedge \deg \overline{r} < \deg g)$ — условие 2).

II) Единственность q и r.

Допустим, что наряду с парой многочленов q и r, установленных в части I), существует другая пара многочленов $\overline{q}$ и $\overline{r}$, удовлетворяющая условиям 1) и 2), то есть $f = \overline{q}g + \overline{r}$ и $\overline{r} = 0 \vee (\overline{r} \neq 0 \wedge \deg \overline{r} < \deg g)$. Имеем

$$qg + r = \overline{q}g + \overline{r} \Rightarrow (q - \overline{q})g = \overline{r} - r. \qquad (*)$$

Покажем, что $q - \overline{q} = 0$. Допустим противное, то есть $q - \overline{q} \neq 0$. Пусть $\alpha \neq 0$ — старший коэффициент этого многочлена, тогда старший коэффициент многочлена $(q - \overline{q})g$ будет $\alpha\beta_m \neq 0$. Если бы $\alpha\beta_m = 0$, то $\alpha = 0$. Значит $\deg(q - \overline{q})g = \deg(q - \overline{q}) + \deg g \geqslant \deg g$.

С другой стороны $\overline{r} - r = 0$ или $\overline{r} - r \neq 0, \deg(\overline{r} - r) < \deg g$. Мы получили, что в равенстве $(*)$ слева стоит многочлен, степень которого не меньше $\deg g$, а справа стоит нулевой многочлен или многочлен, степень которого меньше $\deg g$. Это и есть противоречие. $\square$

Определение 6.2.1. В обозначениях теоремы 6.2.1 многочлены q и r называются соответственно неполным частным и остатком от деления многочлена f на многочлен g.

ТЕОРЕМА 6.2.2 (Безу)**.** *Остаток от деления многочлена $f(x)$ на $x-\gamma$ равен значению многочлена $f(x)$ при $x=\gamma$, то есть $f(\gamma)$.*

Доказательство. Пусть $f(x)=q(x)(x-\gamma)+r(x)$, $\quad r(x)=0 \vee (r(x)\neq \neq 0 \wedge \deg r(x)<1)$. Получаем $r(x)=0 \vee \deg r(x)=0$, в любом случае $r(x)=r\in k$.

Пусть $q(x)=\beta_0+\beta_1 x+\ldots+\beta_s x^s$, тогда $f(x)=q(x)\cdot x-q(x)\gamma+r= = \beta_0 x+\beta_1 x^2+\ldots+\beta_s x^{s+1}-\beta_0\gamma-\beta_1 x\gamma-\ldots-\beta_s x^s\gamma+r$.

Сосчитаем $f(\gamma)=\beta_0\gamma+\beta_1\gamma^2+\ldots+\beta_s\gamma^{s+1}-\beta_0\gamma-\beta_1\gamma^2-\ldots+\beta_s\gamma^{s+1}+r= = r$. Таким образом, $r=f(\gamma)$. □

Представляет интерес деление многочлена $f(x)$ на $(x-\gamma)$ по так называемой схеме Горнера.

Пусть $f(x)=\alpha_0 x^n+\alpha_1 x^{n-1}+\ldots+\alpha_n, \alpha_0\neq 0$. Разделим $f(x)$ на $(x-\gamma)$ с остатком, получим $f(x)=q(x)(x-\gamma)+r$. Многочлен $q(x)$ будем искать в виде $q(x)=\beta_0 x^{n-1}+\beta_1 x^{n-2}+\ldots+\beta_{n-1}$. Наша задача найти коэффициенты $\beta_0,\beta_1,\ldots,\beta_{n-1}$ и остаток r.

Подставим в это соотношение вместо $q(x)$ и $f(x)$ их значения. Имеем, $\alpha_0 x^n+\alpha_1 x^{n-1}+\ldots+\alpha_n=\left(\beta_0 x^{n-1}+\beta_1 x^{n-2}+\ldots+\beta_{n-1}\right)(x-\gamma)+r$. Два многочлена равны тогда и только тогда, когда равны их коэффициенты при соответствующих степенях. Сравним коэффициенты.

$$
\begin{array}{lll}
x^n: & \alpha_0=\beta_0 & \Rightarrow\ \beta_0=\alpha_0;\\
x^{n-1}: & \alpha_1=\beta_1-\beta_0\gamma & \Rightarrow\ \beta_1=\beta_0\gamma+\alpha_1;\\
x^{n-2}: & \alpha_2=\beta_2-\beta_1\gamma & \Rightarrow\ \beta_2=\beta_1\gamma+\alpha_2;\\
\ldots & & \\
x^1: & \alpha_{n-1}=\beta_{n-1}-\beta_{n-2}\gamma & \Rightarrow\ \beta_{n-1}=\beta_{n-2}\gamma+\alpha_{n-1};\\
x^0: & \alpha_n=r-\beta_{n-1}\gamma & \Rightarrow\ r=\beta_{n-1}\gamma+\alpha_n.
\end{array}
$$

Таким образом видно, что коэффициенты неполного частного и остаток находятся с помощью однотипных вычислений, а именно, чтобы найти $\beta_k = \beta_{k-1}\gamma + \alpha_k$. Эти вычисления удобно записывать в виде следующей схемы Горнера.

	α_0	α_1	α_2	$\dots$	α_{n-1}	α_n
γ	α_0	$\beta_0\gamma + \alpha_1$	$\beta_1\gamma + \alpha_2$	$\dots$	$\beta_{n-2}\gamma + \alpha_{n-1}$	$\beta_{n-1}\gamma + \alpha_n$
	$\|\|$	$\|\|$	$\|\|$		$\|\|$	$\|\|$
	β_0	β_1	β_2	$\dots$	β_{n-1}	$r = f(\gamma)$

Пример: $f(x) = x^5 - 2x^4 + 3x^3 - 4x^2 + x - 1$. Найдем $f(4)$.

	1	-2	3	-4	1	-1
4	1	2	11	40	161	643

$f(4) = 643, \quad f(x) = (x^4 + 2x^3 + 11x^2 + 40x + 161)(x - 4) + 643.$

6.3. Делимость многочленов. Наибольший общий делитель и наименьшее общее кратное

Определение 6.3.1. Говорят, что многочлен $f(x)$ делится на многочлен $g(x) \neq 0$ или, что многочлен $g(x)$ делит многочлен $f(x)$ или, что многочлен $g(x)$ является делителем многочлена $f(x)$ или, что многочлен $f(x)$ кратен многочлену $g(x)$, если существует такой многочлен $q(x)$, что $f(x) = q(x) \cdot g(x)$.

Определение 6.3.2. Говорят, что многочлен $f(x)$ делится на многочлен $g(x) \neq 0$, если остаток от деления $f(x)$ на $g(x)$ равен нулю.

То, что многочлен $g(x)$ делит $f(x)$ обозначается как $g|f$.

Определение 6.3.3. Два ненулевых многочлена $f(x)$ и $g(x)$ называются ассоциированными $f \sim g$, если они отличаются друг от друга множителем равным ненулевой константе, то есть $f = \alpha g$, $\alpha \in k^* = k \backslash \{0\}$.

Свойства делимости

1. $(\forall\ f \neq 0) \quad f|f$.

2. $(\forall\ g \neq 0) \quad g|0$.

3. Два ненулевых многочлена ассоциированы тогда и только тогда, когда они делят друг друга, то есть $f \sim g \Leftrightarrow f|g$ и $g|f$.

4. Если $h|g$, $g|f$, то $h|f$ (транзитивность).

5. Если $h|g$, $h|f$, то $(\forall\ u, v \in k[x]) \quad h|(ug + vf)$.

6. Делителями ненулевых констант могут быть только ненулевые константы, то есть если $g|f$ и $\deg f = 0$, то $\deg g = 0$.

7. Ненулевая константа делит ненулевой многочлен, то есть если $\deg g = 0$, то $(\forall\ f) \quad g|f$.

8. Если $g|f$ и $f \neq 0$, то $\deg g \leqslant \deg f$, причем знак равенства достигается тогда и только тогда, когда $g \sim f$.

9. Отношение делимости, есть отношение между классами ассоциированных многочленов, то есть если $g|f$, $g_1 \sim g$, $f_1 \sim f$, то $g_1|f_1$.

Доказательство. 1) $f(x) = 1 \cdot f(x)$, то есть $f|f$ и $q(x) = 1$.

2) $0 = 0 \cdot g(x)$, то есть $g|0$ и $q(x) = 0$.

3) a) Необходимость.

Пусть $f \sim g$, тогда $f = \alpha g$, где $\alpha \in k^*$, то есть $g|f$ и $q = \alpha$. Так как $\alpha \neq 0$, то $g = \alpha^{-1} f$, то есть $f|g$ и $q = \alpha^{-1}$.

b) Достаточность.

Пусть $g|f$ и $f|g$. Имеем, $f = qg$, $g = q_1 f$, следовательно $f = q(q_1 f)$, то есть $(1 - qq_1)f = 0$. Так как $f \neq 0$, то $1 - qq_1 = 0$, то есть $qq_1 = 1$. Значит $\deg qq_1 = 0 \Rightarrow \deg q + \deg q_1 = 0 \Rightarrow \deg q = \deg q_1 = 0$, следовательно q и q_1 — константы. Имеем $f = qg$, где $q \in k^* \Rightarrow f \sim g$.

4) Имеем $g = qh,\ f = q_1 g$. Тогда $f = q_1(qh) = (q_1 q)h \Rightarrow h|f$.

5) Имеем $g = qh$, $f = q_1 h$. Тогда $ug = uqh$, $vf = vq_1 h$. Рассмотрим $ug + vf = (uq + vq_1)h \Rightarrow h|(ug + vf)$.

6) Имеем $\deg f = 0$ и $f = qg \Rightarrow \deg f = \deg q + \deg g = 0 \Rightarrow \deg q = \deg g = 0$, то есть q и g — константы.

7) Так как $\deg g = 0$, то $g \in k^*$, поэтому существует $g^{-1} \in k^*$. Тогда $f = (fg^{-1})g \Rightarrow g|f$.

8) Имеем $f = qg \Rightarrow \deg f = \deg g + \deg q \Rightarrow \deg f \geqslant \deg g$. Видно, что знак равенства будет выполняться тогда и только тогда, когда $\deg q = 0 \Rightarrow q \in k^* \Leftrightarrow f \sim g$.

9) Имеем $f = qg$, $g = \alpha q_1$, $f = \beta f_1$, где $\alpha, \beta \in k^*$. Тогда $\beta f_1 = q\alpha g_1 \Rightarrow f_1 = (\beta^{-1} q\alpha) g_1 \Rightarrow g_1 | f_1$. □

В дальнейшем будем рассматривать конечную систему многочленов $\{f_1, f_2, \ldots, f_s\}$, среди которых по крайней мере один многочлен отличен от нуля.

Определение 6.3.4. Многочлен d называется общим делителем системы многочленов $\{f_1, f_2, \ldots, f_s\}$, если он делит все многочлены данной системы, то есть $(\forall\ 1 \leqslant i \leqslant s) \quad d|f_i$.

ТЕОРЕМА 6.3.1 (о равносильных условиях, определяющих НОД)**.** *Пусть $\{f_1, f_2, \ldots, f_s\}$ — система многочленов, среди которых по крайней мере один многочлен отличен от нуля, и d — некоторый ненулевой многочлен $(d \neq 0)$. Равносильны следующие два утверждения:*

1) *совокупность делителей многочлена d совпадает с совокупностью общих делителей системы многочленов $\{f_1, f_2, \ldots, f_s\}$;*

2) *многочлен d является общим делителем системы многочленов $\{f_1, f_2, \ldots, f_s\}$, который делится на любой другой общий делитель этой системы.*

Доказательство. 1) $\Rightarrow$ 2)

Так как среди делителей многочлена d находится сам многочлен d, то по условию 1), d является общим делителем $\{f_1, f_2, \ldots, f_s\}$.

Пусть теперь d' — любой общий делитель $\{f_1, f_2, \ldots, f_s\}$, тогда по условию 1) d' совпадает с одним из делителей многочлена d, то есть d делится на d'.

2) $\Rightarrow$ 1)

Выполнение условия 1) установим в два шага.

а) Пусть d' — любой делитель многочлена d. Имеем $d'|d$, а по условию 2) $(\forall\ 1 \leqslant i \leqslant s) \quad d|f_i \Rightarrow (\forall\ 1 \leqslant i \leqslant s) \quad d'|f_i$, то есть d' является общим делителем системы многочленов $\{f_1, f_2, \ldots, f_s\}$.

б) Обратно. Пусть d' — любой общий делитель системы многочленов $\{f_1, f_2, \ldots, f_s\}$. Тогда по условию 2) многочлен d делится на d', то есть d' является делителем многочлена d. □

Определение 6.3.5. Наибольшим общим делителем (НОД) системы многочленов $\{f_1, f_2, \ldots, f_s\}$, называется любой ненулевой многочлен d, удовлетворяющий любому из равносильных условий теоремы 6.3.1.

Определение 6.3.6. НОД системы многочленов называется такой общий делитель этой системы, который делится на любой другой общий делитель этой системы многочленов.

Следствие 6.3.1.1. Если НОД системы многочленов существует, то он определен однозначно с точностью до ассоциированности.

Доказательство. Пусть d_1, d_2 — два НОД системы многочленов $f_1, f_2, \ldots, f_s$, будем рассматривать d_1 как НОД системы, а d_2 как ОД системы $f_1, f_2, \ldots, f_s$. Тогда по определению 6.3.6 $d_2|d_1$. Поменяем ролями d_1 и d_2, то есть d_1 будем рассматривать как ОД, а d_2 — как НОД системы $f_1, f_2, \ldots, f_s$. По определению 6.3.6 $d_1|d_2$, тогда по 3 свойству делимости $d_1 \sim d_2$. □

Возникает естественный вопрос: существует ли НОД системы многочленов $\{f_1, f_2, \ldots, f_s\}$? Ответ на этот вопрос положительный. Убедимся в этом сначала для системы из 2-х многочленов. Мы докажем существование НОД 2-х многочленов и укажем алгоритм его нахождения. Этот алгоритм называется алгоритмом Евклида и он основан на методе последовательного деления. Пусть f и g — два ненулевых многочлена, $\deg f \geqslant \deg g$. Разделим f на g с остатком, получим

$$f = q_1 g + r_1, \quad \text{где} \quad r_1 = 0 \quad \text{или} \quad (r_1 \neq 0 \text{ и } \deg r_1 < \deg g).$$

Если $r_1 = 0$, то процесс деления заканчивается. Если $r_1 \neq 0$, то делим g на r_1 с остатком, получим

$$g = q_2 r_1 + r_2, \quad \text{где} \quad r_2 = 0 \quad \text{или} \quad (r_2 \neq 0 \text{ и } \deg r_2 < \deg r_1).$$

Если $r_2 = 0$, то процесс деления заканчивается. Если $r_2 \neq 0$, то делим r_1 на r_2 с остатком, получим

$$r_1 = q_3 r_2 + r_3, \quad \text{где} \quad r_3 = 0 \quad \text{или} \quad (r_3 \neq 0 \text{ и } \deg r_3 < \deg r_2).$$

И так далее. Возникает вопрос: наш процесс конечен или бесконечен? Заметим, что степени остатков образуют строго убывающую последовательность натуральных чисел, а именно $\deg g > \deg r_1 > \deg r_2 > \deg r_3 > \ldots$, которая не может быть бесконечной. В конце концов получим равенства

$$r_{k-2} = q_k r_{k-1} + r_k;$$

$$r_{k-1} = q_{k+1} r_k,$$

где r_k — последний не равный нулю остаток в алгоритме Евклида.

ТЕОРЕМА 6.3.2. *Наибольший общий делитель 2-х ненулевых многочленов f и g существует и равен последнему не равному нулю остатку в алгоритме Евклида, примененному к многочленам f и g.*

Доказательство. Запишем равенства, определяющие алгоритм Евклида к многочленам f и g

$$f = q_1 g + r_1 \Rightarrow r_1 = f - q_1 g; \tag{1}$$

$$g = q_2 r_1 + r_2 \Rightarrow r_2 = g - q_2 r_1; \tag{2}$$

$$r_1 = q_3 r_2 + r_3 \Rightarrow r_3 = r_1 - q_3 r_2; \tag{3}$$

$$\dots$$

$$r_{k-2} = q_k r_{k-1} + r_k \Rightarrow r_k = r_{k-2} - q_k r_{k-1}; \tag{k}$$

$$r_{k-1} = q_{k+1} r_k. \tag{$k+1$}$$

Из последнего равенства видно, что $r_k | r_{k-1}$.

Из равенства (k) видно, что $r_k | r_{k-2}$.

Из равенства $(k-1)$ видно, что $r_k | r_{k-3}$.

$\dots$

$r_k | r_2,\ r_k | r_1$

Из равенства (2) видно, что $r_k | g$.

Из равенства (1) видно, что $r_k | f$.

Следовательно r_k является общим делителем системы многочленов $\{f, g\}$. Пусть d — любой общий делитель $\{f, g\}$, тогда

из равенства (1) видно, что $d | r_1$,

из равенства (2) видно, что $d | r_2$,

$\dots$

из равенства (k) видно, что $d | r_k$,

то есть r_k — общий делитель $\{f, g\}$, который делится на любой другой общий делитель $\{f, g\}$. Тогда по определению 6.3.6 r_k — НОД $\{f, g\}$. $\square$

Существование НОД любой конечной системы многочленов устанавливается следующей теоремой, которая так же дает метод его нахождения.

ТЕОРЕМА 6.3.3 (рекуррентная формула)**.** *НОД конечной системы многочленов существует и при этом справедливо соотношение*

$$\mathcal{HOD}\{f_1, f_2, \ldots, f_{s-1}, f_s\} = \mathcal{HOD}\{\mathcal{HOD}\{f_1, f_2, \ldots, f_{s-1}\}, f_s\}.$$

Доказательство. Применим метод математической индукции по s. Если $s = 2$, то утверждение теоремы очевидно. Предположим, что теорема верна для $(s-1)$ многочленов, тем самым предполагается, что существует наибольший общий делитель d системы многочленов $\{f_1, f_2, \ldots, f_{s-1}\}$. Обозначим через $\bar{d} = \mathcal{HOD}\{d, f_s\}$. Имеем, $\bar{d}|d$, $\bar{d}|f_s$, кроме того $(\forall\ 1 \leqslant i \leqslant s-1)\quad d|f_i$, тогда по транзитивности делимости $(\forall\ 1 \leqslant i \leqslant s-1)\quad \bar{d}|f_i$, $\bar{d}|f_s$, следовательно $\bar{d}$ является общим делителем $\{f_1, f_2, \ldots, f_{s-1}, f_s\}$. Пусть d' — любой общий делитель $\{f_1, f_2, \ldots, f_{s-1}, f_s\}$, тогда $(\forall\ 1 \leqslant i \leqslant s-1)\quad d'|f_i$ и $d'|f_s$ следовательно d' является общим делителем $\{f_1, f_2, \ldots, f_{s-1}\}$. Тогда по определению 6.3.6 $d'|d$. Таким образом $d'|d$, $d'|f_s$ следовательно d' является общим делителем $\{d, f_s\}$. Тогда из определения 6.3.6 следует $d'|\bar{d}$. Итак $\bar{d}$ является общим делителем $\{f_1, f_2, \ldots, f_{s-1}, f_s\}$ и $\bar{d}$ делится на любой общий делитель $\{f_1, f_2, \ldots, f_{s-1}, f_s\}$. Тогда по определению 6.3.6 $\bar{d} = \mathcal{HOD}\{f_1, f_2, \ldots, f_{s-1}, f_s\}$. □

ТЕОРЕМА 6.3.4 (критерий НОД системы многочленов)**.** *Для того чтобы многочлен d являлся НОД системы многочленов $\{f_1, f_2, \ldots, f_s\}$ необходимо и достаточно, чтобы этот многочлен d был ОД этой системы и чтобы он линейно выражался через эти многочлены, то есть* $(\exists\ u_1, u_2, \ldots, u_s, \in k[x])\quad d = u_1f_1 + u_2f_2 + \ldots + u_sf_s$.

Доказательство. 1) Достаточность.

Пусть d является ОД $\{f_1, f_2, \ldots, f_s\}$ и $\exists\ u_1, u_2, \ldots, u_s \in k[x]\quad d = u_1f_1+u_2f_2+\ldots+u_sf_s$. Пусть d' — любой общий делитель $\{f_1, f_2, \ldots, f_s\}$. Это означает, что $(\forall\ 1 \leqslant i \leqslant s)\quad d'|f_i$. Тогда по 5 свойству делимости $d'|(u_1f_1 + u_2f_2 + \ldots + u_sf_s)$, то есть $d'|d$. По определению 6.3.6

$d = \mathcal{НОД}\{f_1, f_2, \ldots, f_s\}$.

2)Необходимость.

Пусть d является НОД $\{f_1, f_2, \ldots, f_s\}$. Тогда d является ОД $\{f_1, f_2, \ldots, f_s\}$. Остается показать, что d линейно выражается через $f_1, f_2, \ldots, f_s$. Установим этот факт методом математической индукции. Пусть $s = 2$. Обозначим $f_1 = f, f_2 = g$. Запишем равенство, определяющее алгоритм Евклида.

$$f = q_1 g + r_1; \tag{1}$$

$$g = q_2 r_1 + r_2; \tag{2}$$

$$\ldots$$

$$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}; \tag{$k-1$}$$

$$r_{k-2} = q_k r_{k-1} + r_k; \tag{k}$$

$$r_{k-1} = q_{k+1} r_k. \tag{$k+1$}$$

Известно, что НОД d многочленов $\{f, g\}$ равен r_k. Из равенства (k) видно, что

$$d = r_{k-2} - q_k r_{k-1} = r_{k-2} - q_k(r_{k-3} - q_{k-1} r_{k-2}) =$$

$$= (1 + q_k q_{k-1}) r_{k-2} - q_k r_{k-3} = \ldots = ug + vf.$$

Предположим, что утверждение теоремы справедливо для системы, состоящей из $(s-1)$ многочленов. Докажем ее справедливость для систем, состоящих из s многочленов. По теореме 6.3.3 наибольший общий делитель d системы многочленов $\{f_1, f_2, \ldots, f_s\}$ совпадает с НОД 2-х многочленов $\{d_1, f_s\}$, где d_1 — НОД $\{f_1, \ldots f_{s-1}\}$. По предположению индукции существуют многочлены $v_1, \ldots, v_{s-1} \in k[x]$ такие, что $d_1 = v_1 f_1 + v_2 f_2 + \ldots + v_{s-1} f_{s-1}$. Так как d является НОД $\{d_1, f_s\}$, то существуют многочлены $w_1, w_2 \in k[x]$ такие, что $d = w_1 d_1 + w_2 f_s$. Имеем $d = w_1 v_1 f_1 + \cdots + w_1 v_{s-1} f_{s-1} + w_2 f_s = u_1 f_1 + u_2 f_2 + \ldots + u_s f_s$. □

Определение 6.3.7. Многочлен называется нормированным, если его старший коэффициент равен 1.

Ясно, что в каждом классе ассоциированных многочленов существует нормированный многочлен. В частности среди НОД системы многочленов, которые определяются с точностью до ассоциированности, существует единственный нормированный НОД. Этот нормированный НОД будем обозначать $(f_1, f_2, \ldots, f_s)$.

Определение 6.3.8. Система многочленов $\{f_1, f_2, \ldots, f_s\}$ называется взаимнопростой в совокупности, если нормированный НОД $(f_1, f_2, \ldots, f_s) = 1$. В случае двух многочленов говорят, что они взаимнопростые.

ТЕОРЕМА 6.3.5 (свойства взаимнопростых многочленов)**.** *Справедливы следующие утверждения.*

1. *Система многочленов $\{f_1, f_2, \ldots, f_s\}$ взаимнопроста в совокупности тогда и только тогда, когда некоторая их линейная комбинация равна единице, то есть* $(\exists\, u_1, \ldots, u_s \in k[x])\ u_1 f_1 + \ldots + u_s f_s = 1$;
2. *Если* $\mathcal{HOD}\{f_1, \ldots f_s\} = d$, *то* $\left(\frac{f_1}{d}, \frac{f_2}{d}, \ldots, \frac{f_s}{d}\right) = 1$;
3. *Если* $(f, h) = 1$ *и* $(g, h) = 1$, *то* $(fg, h) = 1$;
4. *Если* $h | fg$ *и* $(h, g) = 1$,*то* $h | f$;
5. *Если* $h | f$ *и* $g | f$ *и* $(h, g) = 1$, *то* $hg | f$.

Доказательство. 1) Положим в теореме 6.3.4 $d = 1$. Ясно, что d является ОД системы $\{f_1, f_2 \ldots, f_s\}$, тогда по теореме 6.3.4 $d = 1$ будет НОД $\{f_1, f_2 \ldots, f_s\}$ тогда и только тогда, когда существуют многочлены $u_1, u_2, \ldots, u_s \in k[x]$ такие, что $u_1 f_1 + \ldots + u_s f_s = 1$.

2) Так как $\mathcal{HOD}\{f_1, f_2 \ldots, f_s\} = d$, то по теореме 6.3.4 существуют многочлены $u_1, u_2, \ldots, u_s \in k[x]$ такие, что $d = u_1 f_1 + \ldots + u_s f_s$. Разделим

обе части равенства на d. $1 = u_1\frac{f_1}{d} + \ldots + u_s\frac{f_s}{d}$, из свойства 1 следует, что $(\frac{f_1}{d}, \frac{f_2}{d}, \ldots, \frac{f_s}{d}) = 1$.

3) Так как $(f, g) = 1$, то по теореме 6.3.4 $\exists\ u, v \in k[x] \quad 1 = uf + vh$. Так как $(g, h) = 1$, то $(\exists\ u_1, v_1 \in k[x]) \quad 1 = u_1 g + v_1 h$. Почленно перемножим эти соотношения. $1 = (uu_1)fg + (vu_1 g + uv_1 f + vv_1 h)h$. По свойству 1 видно что линейная комбинация многочленов fg и h равна единице, следовательно $(fg, h) = 1$.

4) Так как $(h, g) = 1$, то $\exists\ u, v \in k[x] \quad uh + vg = 1$. Умножим обе части этого равенства на f, получим $uhf + vgf = f$. Так как $h|fg$, то $fg = qh$, тогда $uhf + vqh = f \Rightarrow (uf + vq)h = f \Rightarrow h|f$.

5) Так как $h|f$, то $f = qh$. Имеем $g|qh$ и $(g, h) = 1$, по свойству 4 получаем, что $g|q$, следовательно $q = q_1 g$. Таким образом $f = q_1 gh \Rightarrow$ $\Rightarrow gh|f$. □

Будем теперь рассматривать систему многочленов $\{f_1, f_2, \ldots, f_s\}$, каждый из которых не равен нулю. Для таких систем многочленов изложим теорию наименьшего общего кратного (НОК) по схеме, аналогичной изучению НОД.

Определение 6.3.9. Многочлен m называется общим кратным системы многочленов $\{f_1, f_2, \ldots, f_s\}$, каждый из которых отличен от нуля, если он делится на все многочлены этой системы, то есть $(\forall\ 1 \leqslant i \leqslant s) \quad f_i|m$.

ТЕОРЕМА 6.3.6. *Пусть $\{f_1, f_2, \ldots, f_s\}$ — система ненулевых многочленов и $m \neq 0$ (некоторый ненулевой многочлен). Равносильны следующие утверждения:*

1) *совокупность кратных многочлена m совпадает с совокупностью ОК системы многочленов $\{f_1, f_2, \ldots, f_s\}$;*

2) *многочлен m является ОК $\{f_1, f_2, \ldots, f_s\}$, которое делит любое другое ОК этой системы.*

Определение 6.3.10. Наименьшим общим кратным (НОК) системы многочленов $\{f_1, f_2, \ldots, f_s\}$ называется любой ненулевой многочлен m, удовлетворяющий любому из равносильных условий теоремы 6.3.6.

Определение 6.3.11. НОК системы многочленов называется такое общее кратное этой системы, которое делит любое другое общее кратное этой системы многочленов.

Следствие 6.3.6.1. Если НОК системы многочленов существует, то оно определено с точностью до ассоциированности.

ТЕОРЕМА 6.3.7. *Если существует НОК 2-х любых ненулевых многочленов, то существует НОК и любой конечной системы многочленов, при этом имеет место следующая индукционная формула:*

$$\mathcal{НОК}\{f_1, f_2, \ldots, f_{s-1}, f_s\} = \mathcal{НОК}\{\mathcal{НОК}\{f_1, f_2, \ldots, f_{s-1}\}, f_s\}.$$

Теорема 6.3.7 сводит нахождение НОК системы многочленов к нахождению НОК 2-х многочленов.

ТЕОРЕМА 6.3.8. *Если f и g — два ненулевых многочлена, то их НОК существует и равно $\frac{fg}{(f,g)}$.*

Доказательство. Обозначим многочлен $\frac{fg}{(f,g)} = m$. Видно, что

$$m = \frac{g}{(f,g)}f \Rightarrow f|m$$

и

$$m = \frac{f}{(f,g)}g \Rightarrow g|m,$$

то есть m является ОК многочленов $\{f, g\}$. Пусть M — любое ОК $\{f, g\}$. Это означает, что $M = uf,\ M = vg \Rightarrow uf = vg$. Разделим обе части этого равенства на (f, g). Получим

$$u\frac{f}{(f,g)} = v\frac{g}{(f,g)} \Rightarrow \frac{g}{(f,g)}\Big| u\frac{f}{(f,g)}.$$

По свойству 2 теоремы 6.3.5 имеем $\left(\frac{f}{(f,g)}, \frac{g}{(f,g)}\right) = 1$. По 4 свойству теоремы 6.3.5 имеем $\frac{g}{(f,g)} \Big| u$. Тогда $u = \frac{g}{(f,g)}q$. $M = uf = \frac{fg}{(f,g)}q = mq$. Видно, что $m|M$. По определению 6.3.11 m является НОК $\{f, g\}$. □

6.4. Неприводимость. Каноническое разложение. Кратность

Пусть f — многочлен положительной степени, $\alpha \in k^* = k\backslash\{0\}$. Известно, что $\alpha|f$ и $\alpha f|f$.

Определение 6.4.1. Тривиальными делителями многочлена f положительной степени называются ненулевые константы и многочлены, ассоциированные с многочленом f.

Следствие. Делитель d многочлена f является нетривиальным тогда и только тогда, когда $0 < \deg d < \deg f$.

Следствие. Многочлен f положительной степени имеет нетривиальные делители тогда и только тогда, когда его можно представить в виде произведения 2-х многочленов, степени которых меньше степени многочлена f, то есть $(\exists\, u, v \in k[x]) \quad f = uv$, где $\deg u, \deg v < \deg f$.

Определение 6.4.2. Многочлен P положительной степени называется неприводимым над полем k, если он имеет над этим полем только тривиальные делители. В противном случае, многочлен P называется приводимым.

Определение 6.4.3. Многочлен P положительной степени называется неприводимым над полем k, если его нельзя представить над этим полем в виде произведения 2-х многочленов, степени которых меньше степени многочлена P.

Замечание 6.4.1. Понятие неприводимости существенно зависит от основного поля k. Так, например, многочлен $f = x^2 - 2 = (x+\sqrt{2})(x-\sqrt{2})$ неприводим над полем $\mathbb{Q}$. Но он приводим над полем $\mathbb{R}$.

Замечание 6.4.2. Многочлены 1-й степени являются неприводимыми над любым полем.

Это следует из того, что многочлены 1-й степени имеют только тривиальные делители.

ТЕОРЕМА 6.4.1 (свойства неприводимых многочленов)**.** *Справедливы следующие утверждения:*

1. *Если многочлен P является неприводимым, то и любой ассоциированный с ним многочлен также является неприводимым.*

2. *Если P — неприводимый многочлен, f — любой многочлен, то либо $(P, f) = 1$, либо $P|f$.*

3. *Если P — неприводимый многочлен и $P|fg$, то $P|f$ или $P|g$.*

4. *Если P и Q — два неприводимых многочлена, то либо $(P, Q) = 1$, либо P и Q ассоциированы.*

Доказательство. 1) Пусть P — неприводимый многочлен. Рассмотрим αP, где $\alpha \in k^*$. Надо доказать, что αP является неприводимым. Допустим противное, то есть у αP есть нетривиальный делитель, то есть $(\exists\ d \in k[x])\quad d|\alpha P$, где $0 < \deg d < \deg \alpha P = \deg P$. Имеем, $d|\alpha P$ и $\alpha P|P \Rightarrow d|P$ и $0 < \deg d < \deg P$. Это противоречит неприводимости многочлена P.

2) Обозначим $(P, f) = d$. Имеем $d|P$. Так как P — неприводим, то d должен быть тривиальным делителем, то есть либо $d = \alpha \in k^*$, либо $d \sim P$. В первом случае имеем $(P, f) = 1$. Во втором случае, имеем $P|d$ и $d|f \Rightarrow P|f$.

3) Пусть $P|fg$. Если $P|f$, то все доказано. Если $P \nmid f$, то по свойству 2 $(P, f) = 1$. Итак, $P|fg$ и $(P, f) = 1$, тогда по свойству 4 теоремы 6.3.5 $P|g$.

4) Пусть P и Q — два неприводимых многочлена. Если $(P, Q) = 1$, то все доказано. Пусть $(P, Q) \neq 1$, тогда по свойству 2 $P|Q$. Меняя ролями P и Q, получаем $Q|P \Rightarrow P \sim Q$. □

ТЕОРЕМА 6.4.2 (о разложении на неприводимые множители)**.** *Любой многочлен f положительной степени над полем k может быть представлен в виде $f = \alpha P_1 \cdot P_2 \cdot \ldots \cdot P_s$, где $\alpha \in k^*$, P_i — нормированные неприводимые над k многочлены. Это представление единственно с точностью до порядка следования сомножителей и при этом необходимо, чтобы α являлась старшим коэффициентом многочлена f.*

Доказательство. 1) Существование.

Рассмотрим множество M всех нормированных делителей положительной степени многочлена f. В этом множестве M выберем многочлен P_1 наименьшей степени. Покажем, что многочлен P_1 является неприводимым. Допустим противное, то есть многочлен P_1 является приводимым. Следовательно $P_1 = du$, где $0 < \deg d < \deg P_1$, а это противоречит выбору многочлена P_1. Имеем

$$f = P_1 f_1, \quad \text{где} \quad 0 \leqslant \deg f_1 < \deg f. \tag{1}$$

Если $\deg f_1 = 0$, то процесс выделения неприводимых множителей заканчивается. Если $\deg f_1 > 0$, то с многочленом f_1 проводим те же рассуждения, что и с многочленом f. Получим, что у многочлена f_1 есть нормированный неприводимый множитель P_2. Будем иметь

$$f_1 = P_2 f_2, \quad \text{где} \quad 0 \leqslant \deg f_2 < \deg f_1. \tag{2}$$

Если $\deg f_2 = 0$, то процесс выделения неприводимых множителей заканчиваем. Если $\deg f_2 > 0$, то процесс продолжаем. И так далее. Возникает вопрос: наш процесс конечен или бесконечен? Заметим, что степени

многочленов $f_1, f_2, \ldots$ образуют строго убывающую последовательность натуральных чисел $\deg f > \deg f_1 > \deg f_2 > \ldots$, которая не может быть бесконечной. В конце концов получим

$$f_{s-1} = P_s f_s, \quad \text{где} \quad \deg f_s = 0. \qquad (s)$$

Это означает, что $f_s = \alpha \in k^*$. Перемножим почленно все равенства $(1), (2), \ldots, (s)$, получим $f = \alpha P_1 \cdot P_2 \cdot \ldots \cdot P_s$. Так как$P_i$ является нормированными многочленами, то сравнивая в этом равенстве коэффициенты при старшей степени x, получим, что α является старшим коэффициентом многочлена f.

2) Единственность.

Пусть наряду с представлением $f = \alpha P_1 \cdot P_2 \cdot \ldots \cdot P_s$ имеет место другое представление $f = \beta Q_1 \cdot Q_2 \cdot \ldots \cdot Q_t$, где $\beta \in k^*$, Q_j — нормированные неприводимые над k многочлены. Тогда, по доказанному выше, β является старшим коэффициентом многочлена f, то есть $\beta = \alpha$.

$$f = \alpha P_1 \cdot P_2 \cdot \ldots \cdot P_s = \beta Q_1 \cdot Q_2 \cdot \ldots \cdot Q_t. \qquad (*)$$

Равенство $(*)$ указывает на то, что $P_1 | (Q_1 \cdot Q_2 \cdot \ldots \cdot Q_t)$. По свойству 3 теоремы 6.4.1 $(\exists\, 1 \leqslant j \leqslant t) \quad P_1 | Q_j$. Будем считать, что $P_1 | Q_1$. Тогда по свойству 4 теоремы 6.4.1 $P_1 \sim Q_1$. Так как оба многочлена нормированы, то $P_1 = Q_1$. Тогда равенство $(*)$ сокращаем на P_1. Получим

$$P_2 \cdot \ldots \cdot P_s = Q_2 \cdot \ldots \cdot Q_t. \qquad (**)$$

С многочленом P_2 рассуждаем также, как с многочленом P_1. Равенство $(**)$ указывает на то, что $P_2 | (Q_2 \cdot \ldots \cdot Q_t) \Rightarrow (\exists\, 2 \leqslant j \leqslant t) \quad P_2 | Q_j$. Будем считать, что $P_2 | Q_2$. Тогда $P_2 \sim Q_2 \Rightarrow P_2 = Q_2$. И так далее. Если $s = t$, то в конце концов получим $P_s = Q_s$.

Может ли $s \neq t$? Предположим, что $s < t$, тогда сокращая равенство $(*)$ на $P_1 \cdot P_2 \cdot \ldots \cdot P_s$ получим, что $1 = Q_{s+1} \cdot \ldots \cdot Q_t$ — этого быть не

может так как слева стоит многочлен нулевой степени, а справа многочлен положительной степени. Аналогично не может быть и $s > t$ таким образом Q_j — те же самые P_i, только написанные возможно в другом порядке. □

ТЕОРЕМА 6.4.3 (о каноническом представлении)**.** *Любой многочлен f положительной степени над полем k может быть представлен в виде $f = \alpha P_1^{k_1} \cdot P_2^{k_2} \cdot \ldots \cdot P_t^{k_t}$, где $\alpha \in k^*$, P_i — различные нормированные, неприводимые над k многочлены, $k_i \in \mathbb{N}$. Это представление единственно с точностью до порядка следования сомножителей и при этом α необходимо являться старшим коэффициентом многочлена f.*

Доказательство. По теореме 6.4.2 имеем $f = \alpha P_1 \cdot P_2 \cdot \ldots \cdot P_s$. Объединяя в этом представлении произведение одинаковых множителей в степени, получим

$$f = \alpha P_1 \cdot P_2 \cdot \ldots \cdot P_s = \alpha P_1^{k_1} \cdot P_2^{k_2} \cdot \ldots \cdot P_t^{k_t}, \qquad (t \leqslant s).$$

□

Определение 6.4.4. Представление многочлена f в виде $f = \alpha P_1^{k_1} \cdot P_2^{k_2} \cdot \ldots \cdot P_t^{k_t}$ называется каноническим представлением многочлена f. Многочлены $P_1^{k_1}, P_2^{k_2}, \ldots, P_t^{k_t}$ называются элементарными делителями многочлена f. Натуральные числа $k_1, k_2, \ldots, k_t$ называются кратностями неприводимых многочленов $P_1, P_2, \ldots, P_t$ в многочлене f.

Пусть $\gamma \in k$. Мы уже заметили, что многочлены 1-й степени неприводимы над любым полем k. В частности $x - \gamma$ является нормированным неприводимым над k многочленом, поэтому можно говорить о кратности многочлена $x - \gamma$ в многочлене f.

Определение 6.4.5. Кратностью элемента $\gamma \in k$ в многочлене f называется кратность неприводимого многочлена $x - \gamma$ в многочлене f.

Определение 6.4.6. Элемент $\gamma \in k$ называется корнем многочлена $f(x)$, если $f(\gamma) = 0$.

Предложение 6.4.1. *Для того, чтобы элемент $\gamma \in k$ был корнем многочлена $f(x)$ необходимо и достаточно, чтобы многочлен f делился на $x - \gamma$, то есть, чтобы элемент γ имел положительную кратность в многочлене f.*

Доказательство. В самом деле, по теореме Безу $f(x) = Q(x)(x - \gamma) + + f(\gamma)$, тогда $(x - \gamma)|f(x) \Leftrightarrow f(\gamma) = 0$, то есть по определению 6.4.6 γ является корнем $f(x)$. □

Следствие. Элемент $\gamma \in k$ не является корнем многочлена $f(x)$ тогда и только тогда, когда элемент γ имеет нулевую кратность в многочлене $f(x)$.

Определение 6.4.7. Корень γ в многочлене $f(x)$ называется простым, если он имеет первую кратность.

Пусть каноническое представление многочлена f имеет вид

$$f = \alpha(x - \gamma_1)^{k_1} \dots (x - \gamma_s)^{k_s} P_1^{l_1} \dots P_t^{l_t}, \quad \text{где} \quad \deg P_i \geqslant 2.$$

Видно, что

$$\deg \left[(x - \gamma_1)^{k_1} \dots (x - \gamma_s)^{k_s}\right] \leqslant \deg f,$$

то есть

$$k_1 + k_2 + \dots + k_s \leqslant \deg f.$$

Ясно, что $(\forall\ 1 \leqslant i \leqslant s) \quad f(\gamma_i) = 0$, то есть $\gamma_1, \gamma_2, \dots, \gamma_s$ являются корнями многочлена f. Если каждый корень γ_i считать k_i раз, то число $k_1 + k_2 + \dots + k_s$ — число корней многочлена f с учетом их кратностей.

Предложение 6.4.2. *Число корней многочлена $f(x)$ с учетом их кратностей не превосходит степень многочлена f.*

6.5. Производная и кратность

Пусть k — некоторое фиксированное числовое поле.

Определение 6.5.1. Производной многочлена $f = \sum\limits_{i=0}^{\infty} \alpha_i x^i$ называется многочлен вида

$$f' = \sum_{i=0}^{\infty} i\alpha_i x^{i-1}.$$

ТЕОРЕМА 6.5.1 (основные правила дифференцирования)**.** *Имеют места следующие свойства:*

1. $\alpha' = 0$, *где* $\alpha \in k$;
2. $(\alpha f)' = \alpha f'$, *где* $\alpha \in k$;
3. $(f \pm g)' = f' \pm g'$;
4. $(fg)' = f'g + fg'$;
5. $(f^n)' = nf^{n-1}f',\ n \in \mathbb{N}$.

Определение 6.5.2. Полагают $f^{(0)} = f,\ f^{(l+1)} = (f^{(l)})'$, где $l \geqslant 0,\ l \in \mathbb{Z}$.

Ясно, что если $\deg f = n$, то $(\forall\ l > n) \quad f^{(l)} = 0$.

Лемма 6.5.1. Если f — многочлен положительной степени n, то $f' \neq 0$ и $\deg f' = n - 1$.

Доказательство. Имеем $f = \alpha_n x^n + \ldots + \alpha_1 x + \alpha_0$, где $\alpha_n \neq 0,\ n \geqslant 1$. По определению 6.5.1 $f' = n\alpha_n x^{n-1} + \ldots + \alpha_1$. Старший коэффициент у многочлена f' равен $n\alpha_n$, где $n \in \mathbb{N},\ \alpha_n \neq 0$. Тогда $n\alpha_n \neq 0$, следовательно $f' \neq 0$ и $\deg f' = n - 1$. □

ТЕОРЕМА 6.5.2. *Пусть f — многочлен положительной степени и неприводимый множитель P имеет положительную кратность k в многочлене f. Тогда этот неприводимый множитель P имеет кратность $k - 1$ в производной f'.*

Доказательство. Имеем $f = P^l g$, где $P \nmid g$. Составим $f' = lP^{l-1}P'g + + P^l g' = P^{l-1}(lP'g + Pg')$. Видно, что $P^{l-1}|f'$, то есть кратность P в f' не меньше, чем $l-1$. Покажем, что $P^l \nmid f'$. Допустим противное, то есть $P^l|f'$. Тогда $P|(lP'g + Pg')$. Видно, что $P|Pg'$, следовательно $P|(lP'g)$. Ясно, что $(P, l) = 1$. По лемме $P' \neq 0$ и $\deg P' < \deg P \Rightarrow (P, P') = 1$. По свойству 3 теоремы 6.4.1 имеем, что $P|g$, а это противоречит тому, что дано. Следовательно $P^l \nmid f'$ и кратность P в составе f' точно $l-1$. □

Следствие 6.5.2.1. Элемент γ имеет кратность k в многочлене f тогда и только тогда, когда $f(\gamma) = f'(\gamma) = \ldots = f^{(k-1)}(\gamma) = 0$, но $f^{(k)}(\gamma) \neq 0$.

Доказательство. 1) Необходимость.

Пусть γ имеет кратность k в многочлене f. По определению это означает, что $(x-\gamma)$ имеет кратность k в многочлене f. По теореме 6.5.2 $x-\gamma$ имеет кратность $k-1$ в f', $x-\gamma$ имеет кратность $k-2$ в f'', …, $x-\gamma$ имеет кратность 1 в $f^{(k-1)}$, $x-\gamma$ имеет кратность 0 в $f^{(k)}$. Применяя предложение 6.4.1 $f(\gamma) = f'(\gamma) = \ldots = f^{(k-1)}(\gamma) = 0$, но $f^{(k)}(\gamma) \neq 0$.
2) Достаточность.

Пусть $f(\gamma) = f'(\gamma) = \ldots = f^{(k-1)}(\gamma) = 0$, но $f^{(k)}(\gamma) \neq 0$. Пусть кратность γ в многочлене f равна l .Надо доказать, что $l = k$. Допустим противное. Пусть, например, $l < k$. Тогда по первой части доказательства будем иметь $f(\gamma) = f'(\gamma) = \ldots = f^{(l-1)}(\gamma) = 0$, но $f^{(l)}(\gamma) \neq 0$. Этого быть не может, потому что по условию $f^{(l)}(\gamma) = 0$ так как $l \leqslant k-1$. Аналогично приводит к противоречию и предположение, что $l > k$. □

Следствие 6.5.2.2. Кратность элемента γ в многочлене f равна наименьшему порядку производной многочлена f, не имеющего γ своим корнем.

ТЕОРЕМА 6.5.3 (об отделении кратных множителей)**.** *Пусть f — многочлен положительной степени над полем k. Тогда многочлен $F = \dfrac{f}{(f, f')}$ имеет те же самые неприводимые множители, что и многочлен f, но только первой кратности.*

Доказательство. Пусть $f = \alpha P_1^{k_1} P_2^{k_2} \dots P_t^{k_t}$ — каноническое разложение многочлена f. Тогда по теореме 6.5.2

$$f' = P_1^{k_1-1} P_2^{k_2-1} \dots P_t^{k_t-1} g, \quad \text{где} \quad (\forall\ 1 \leqslant i \leqslant t) \quad P_i \nmid g.$$

Составим $(f, f') = P_1^{k_1-1} P_2^{k_2-1} \dots P_t^{k_t-1}$.

$$F = \frac{f}{(f, f')} = \alpha P_1 P_2 \dots P_t.$$

□

6.6. Алгебраически замкнутые поля

Пусть k — основное поле.

ТЕОРЕМА 6.6.1 (о равносильных условиях, определяющих алгебраически замкнутое поле)**.** *Относительно фиксированного основного поля k справедливы следующие равносильные утверждения.*

1) *любой многочлен f положительной степени с коэффициентами из поля k, имеет в поле k, по крайней мере, один корень;*

2) *неприводимыми над полем k являются многочлены только первой степени;*

3) *многочлен поля k распадается над полем k на линейные множители;*

4) *любой многочлен f положительной степени с коэффициентами из поля k имеет в поле k столько корней с учетом их кратностей, какова степень многочлена f.*

Доказательство. 1) $\Rightarrow$ 2)

Пусть f — любой многочлен, $\deg f \geqslant 2$. Тогда по условию 1) этот многочлен имеет в поле k по крайне мере один корень γ. Тогда по предложению 6.4.1 $f = (x - \gamma)g$. Следовательно f является приводимым над k.

2) $\Rightarrow$ 3)

Пусть f многочлен положительной степени. Тогда по теореме 6.4.2 его можно представить в виде $f = \alpha P_1 \cdot P_2 \cdot \ldots \cdot P_s$, где $\alpha \in k^*$, P_i — нормированные неприводимые над k многочлены. Из условия 2) следует, что $P_i = x - \gamma_i \Rightarrow f = \alpha(x-\gamma_1)(x-\gamma_2)\ldots(x-\gamma_n)$. Таким образом многочлен распадается на линейные множители.

3) $\Rightarrow$ 4)

Имеем $f = \alpha(x-\gamma_1)(x-\gamma_2)\ldots(x-\gamma_s)$. Объединим произведение одинаковых множителей в степени.

$$f = (x-\gamma_1)^{k_1}(x-\gamma_2)^{k_2}\ldots(x-\gamma_t)^{k_t}, \quad k_i \in \mathbb{N}.$$

Видно, что $\gamma_1, \ldots, \gamma_t$ — корни многочлена f с кратностями $k_1, \ldots, k_t$ и $\deg f = k_1 + \ldots + k_t$. Таким образом число корней многочлена f с учетом их кратностей равно степени многочлена f.

4) $\Rightarrow$ 1)

Пусть многочлен f имеет $\deg > 0$. Тогда по условию 4) $k_1 + k_2 + \ldots + k_t = \deg f \geqslant 1 \Rightarrow (\exists\ 1 \leqslant i \leqslant t) \quad k_i \geqslant 1$. Значит, многочлен f имеет по крайней мере корень γ_i. □

Определение 6.6.1. Поле k называется алгебраически замкнутым, если оно удовлетворяет любому из равносильных условий теоремы 6.6.1.

Замечание 6.6.1. Поля $\mathbb{Q}$ и $\mathbb{R}$ не являются алгебраически замкнутыми, так как не выполняется 1) условие теоремы 6.6.1. Примером может служить многочлен $f = x^2 + 1$. Он не имеет ни одного корня ни в поле $\mathbb{Q}$, ни в поле $\mathbb{R}$.

Определение 6.6.2. Алгебраическим замыканием поля k называется наименьшее алгебраически замкнутое расширение поля k.

Определение 6.6.3. Поле $\overline{k}$ называется алгебраическим замыканием поля k, если выполнены следующие 3 условия:

1. $k \subset \overline{k}$;

2. $\overline{k}$ является алгебраически замкнутым полем;

3. если $k \subset k' \subset \overline{k}$ и k' — алгебраически замкнутое поле, то $k' = \overline{k}$.

ТЕОРЕМА 6.6.2 (основная теорема алгебры)**.** *Поле комплексных чисел* $\mathbb{C}$ *является алгебраически замкнутым полем.*

Следствие 6.6.2.1. Алгебраическим замыканием поля действительных чисел $\mathbb{R}$ является поле комплексных чисел, то есть $\overline{\mathbb{R}} = \mathbb{C}$.

Доказательство. Действительно, пусть $\overline{\mathbb{R}}$ — алгебраическое замыкание поля $\mathbb{R}$. Тогда $\mathbb{R} \subset \overline{\mathbb{R}}$. Далее, многочлен $x^2 + 1$ имеет корень в $\overline{\mathbb{R}}$, то есть $i \in \overline{\mathbb{R}}$. Это выполняется тогда и только тогда, когда $(\forall\ x, y \in \mathbb{R})\quad x + yi \in \overline{\mathbb{R}}$, то есть $\mathbb{C} \subset \overline{\mathbb{R}}$. Имеем $\mathbb{R} \subset \mathbb{C} \subset \overline{\mathbb{R}}$. По теореме 6.6.2 $\mathbb{C}$ является алгебраически замкнутым, тогда по определению 6.6.3 имеем $\mathbb{C} = \overline{\mathbb{R}}$. $\square$

Пусть $\gamma_1, \gamma_2, \ldots, \gamma_n$ — элементы поля k.

Определение 6.6.4. Элементарными симметрическими многочленами от элементов $\gamma_1, \ldots, \gamma_n$ называются суммы вида:

$$\sigma_1 = \gamma_1 + \gamma_2 + \ldots + \gamma_n;$$

$$\sigma_2 = \gamma_1\gamma_2 + \gamma_1\gamma_3 + \ldots + \gamma_1\gamma_n + \gamma_2\gamma_3 + \ldots + \gamma_2\gamma_n + \ldots + \gamma_{n-1}\gamma_n;$$

$$\ldots$$

$$\sigma_k = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} \gamma_{i_1} \ldots \gamma_{i_k};$$

$$\ldots$$

$$\sigma_n = \gamma_1 \ldots \gamma_n.$$

Предложение 6.6.1. *Если* $\gamma_1, \gamma_2, \ldots, \gamma_n \in k$, *то*

$$f(x) = (x+\gamma_1)(x+\gamma_2)\ldots(x+\gamma_n) = x^n + \sigma_1 x^{n-1} + \ldots + \sigma_k x^{n-k} + \ldots + \sigma_n,$$

где $\sigma_1, \sigma_2, \ldots, \sigma_n$ — *элементарные симметрические многочлены от* $\gamma_1, \gamma_2, \ldots, \gamma_n$.

Доказательство. Чтобы установить этот факт, достаточно перемножить скобки стоящие слева и привести подобные слагаемые. □

Следствие. Если $\gamma_1, \gamma_2, \ldots, \gamma_n \in k$, то $f(x) = (x - \gamma_1)(x - \gamma_2)\ldots(x - \gamma_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \ldots + (-1)^k \sigma_k x^{n-k} + \ldots + (-1)^n \sigma_n$, где $\sigma_1, \sigma_2, \ldots, \sigma_n$ — элементарные симметрические многочлены от $\gamma_1, \gamma_2, \ldots, \gamma_n$.

Доказательство. В самом деле, достаточно в предложении 6.6.1 вместо γ_i подставить $-\gamma_i$. Тогда σ_k заменится на $(-1)^k \sigma_k$ и тем самым следствие будет установлено. □

ТЕОРЕМА 6.6.3 (теорема Виета)**.** *Пусть* $f(x) = x^n + \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \ldots + \alpha_n$ *и этот многочлен имеет в алгебраическом замыкании* $\overline{k}$ *корни* $\gamma_1, \gamma_2, \ldots, \gamma_n$. *Тогда* $\sigma_k = (-1)^k \alpha_k$, *где* $\sigma_1, \sigma_2, \ldots, \sigma_n$ — *элементарные симметрические многочлены от корней* $\gamma_1, \gamma_1, \ldots, \gamma_n$.

Доказательство. Над полем $\overline{k}$ многочлен

$$f(x) = (x - \gamma_1)(x - \gamma_2)\ldots(x - \gamma_n),$$

где $\gamma_1, \gamma_2, \ldots, \gamma_n$ — корни $f(x)$ в $\overline{k}$. По следствию из предложения 6.6.1 имеем:

$$f(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \ldots + (-1)^k \sigma_k x^{n-k} + \ldots + (-1)^n \sigma_n.$$

С другой стороны, по условию $f(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$. Таким образом имеем два выражения одного и того же многочлена по убывающим степеням x. Тогда, коэффициенты при одинаковых степенях x должны совпадать. Имеем $-\sigma_1 = \alpha_1,\ \sigma_2 = \alpha_2, \ldots, (-1)^k \sigma_k = \alpha_k, \ldots, (-1)^n \sigma_n = \alpha_n$. Имеем $(\forall\ 1 \leqslant k \leqslant n)\quad (-1)^k \sigma_k = \alpha_k$. Умножим на $(-1)^k$, получим $\sigma_k = (-1)^k \alpha_k$. □

Частный случай теоремы 6.6.3:

n=2, $f(x) = x^2 + px + q$. Пусть $x_1,\ x_2$ — корни $f(x)$, тогда

$$\begin{cases} \sigma_1 = x_1 + x_2 = -p; \\ \sigma_2 = x_1 \cdot x_2 = q. \end{cases}$$

n=3, $f(x) = x^3 + px^2 + qx + r$. Пусть $x_1,\ x_2\ x_3$ — корни $f(x)$, тогда

$$\begin{cases} \sigma_1 = x_1 + x_2 + x_3 = -p; \\ \sigma_2 = x_1x_2 + x_1x_3 + x_2x_3 = q; \ . \\ \sigma_3 = x_1x_2x_3 = -r \end{cases}$$

6.7. Многочлены над числовыми полями

Рассмотрим случай, когда $k = \mathbb{C}$. По основной теореме алгебры, поле $\mathbb{C}$ является алгебраически замкнутым, поэтому многочлены над полем $\mathbb{C}$ обладают любым из равносильных условий теоремы 6.6.1. В частности, неприводимыми над полем $\mathbb{C}$ являются многочлены только первой степени. Далее, любой многочлен положительной степени над полем $\mathbb{C}$ имеет, по крайне мере, один корень. Наконец, каноническое разложение любого многочлена f положительной степени над полем $\mathbb{C}$ имеет вид:

$$f(x) = \alpha(x - \gamma_1)^{k_1}(x - \gamma_2)^{k_2} \dots (x - \gamma_t)^{k_t},$$

где $\gamma_1, \gamma_2, \dots, \gamma_t \in \mathbb{C}$.

Рассмотрим случай, когда $k = \mathbb{R}$. Пусть $\gamma = \alpha + \beta_i$, где $\alpha, \beta \in \mathbb{R},\ \beta \neq \neq 0$. В этом случае говорят, что γ — существенно комплексное число.

Предложение 6.7.1. *Если γ — существенно комплексное число, то многочлен $(x-\gamma)(x-\overline{\gamma})$ является квадратным трехчленом с действительными коэффициентами и отрицательным дискриминантом.*

Доказательство. Действительно, $(x - \gamma)(x - \bar{\gamma}) = x^2 - (\gamma + \bar{\gamma})x + \gamma\bar{\gamma} = = x^2 - 2\alpha x + \alpha^2 + \beta^2 \in \mathbb{R}[x]$, тогда $D = (-2\alpha)^2 - 4(\alpha^2 + \beta^2) = -4\beta^2 < 0$, так как γ — существенно комплексное число. □

ТЕОРЕМА 6.7.1. *Если существенно комплексное число γ является корнем многочлена f с действительными коэффициентами, то комплексно сопряженное число $\bar{\gamma}$ также является корнем этого многочлена и при том той же кратности, что и корень γ.*

Доказательство. Пусть $f(x) = \alpha_n x^n + \ldots + \alpha_1 x + \alpha_0$, где $\alpha_i \in \mathbb{R}$ и γ — существенно комплексный корень $f(x)$, то есть $f(\gamma) = 0$.

$$\alpha_n \gamma^n + \ldots + \alpha_1 \gamma + \alpha_0 = 0.$$

Перейдем к комплексно сопряженным числам, получим

$$\overline{\alpha_n \gamma^n + \ldots + \alpha_1 \gamma + \alpha_0} = \bar{0}.$$

Воспользуемся свойствами комплексно сопряженных чисел, а именно

$$\bar{\alpha}_n \cdot \bar{\gamma}^n + \ldots + \bar{\alpha_1} \cdot \bar{\gamma} + \bar{\alpha_0} = \bar{0}.$$

Так как α_i и $0 \in \mathbb{R}$, то $\bar{\alpha}_i = \alpha_i,\ \bar{0} = 0$. Получаем

$$\alpha_n (\bar{\gamma})^n + \ldots + \alpha_1 \bar{\gamma} + \alpha_0 = 0.$$

Это равенство указывает на то, что $f(\bar{\gamma}) = 0$ то есть $\bar{\gamma}$ является корнем многочлена $f(x)$. Покажем, что кратность корня $\bar{\gamma}$ совпадает с кратностью корня γ. Пусть кратность γ равна k, а кратность $\bar{\gamma}$ равна l. Необходимо доказать, что $k = l$. Допустим противное, то есть $k \neq l$. Пусть, например, $k > l$, тогда $f = (x-\gamma)^k (x-\bar{\gamma})^l g(x)$, где $g(\gamma) \neq 0, g(\bar{\gamma}) \neq 0$. Тогда $f(x) = [(x-\gamma)(x-\bar{\gamma})]^l (x-\gamma)^{k-l} g(x) = [(x-\gamma)(x-\bar{\gamma})]^l g_1(x)$, то есть $g_1 = \frac{f(x)}{[(x-\gamma)(x-\bar{\gamma})]^l}$. По предложению $(x-\gamma)(x-\bar{\gamma}) \in \mathbb{R}[x]$, поэтому

$$g_1 = \frac{f(x)}{[(x-\gamma)(x-\bar{\gamma})]^l} \in R[x].$$

Видно, что $g_1(x) = (x-\gamma)^{k-l} g(x)$ имеет γ своим корнем положительной кратности, $k - l > 0$, но не имеет своим корнем $\bar{\gamma}$. Это противоречит первому утверждению доказываемой теоремой. Аналогично приводит к противоречию предположение, что $l > k$. □

Следствие 6.7.1.1. Существенно комплексные корни многочлена с действительными коэффициентами попарно комплексно сопряжены.

ТЕОРЕМА 6.7.2 (о неприводимых многочленах над $\mathbb{R}$)**.** *Над полем действительных чисел $\mathbb{R}$ неприводимыми являются многочлены первой степени и те и только те квадратные трехчлены, дискриминант которых отрицательный.*

Доказательство. Пусть $f(x) \in \mathbb{R}[x]$ и $\deg f(x) \geqslant 3$. Этот многочлен имеет в алгебраическом замыкании $\overline{\mathbb{R}} = \mathbb{C}$ имеет по крайне мере один корень α. Если $\alpha \in \mathbb{R}$, то $f(x) = (x-\alpha)g(x)$, где $g(x) \in \mathbb{R}[x]$ то есть многочлен f приводим над $\mathbb{R}$. Если α — существенно комплексное число, то $\bar{\alpha}$ также будет корнем многочлена f. Получим

$$f(x) = (x-\alpha)(x-\bar{\alpha})g(x) = (x^2 - 2Re\alpha \cdot x + |\alpha|^2)g(x).$$

В этом случае

$$g(x) = \frac{f(x)}{(x-\alpha)(x-\bar{\alpha})} \in \mathbb{R}[x].$$

Видно, что $f(x)$ снова приводим над $\mathbb{R}$. Таким образом, любой многочлен f, степень которого $\deg f \geqslant 3$, является приводимым над $\mathbb{R}$.

Пусть $f = ax^2+bx+c, a \neq 0$. Известно, что этот квадратный трехчлен распадается на линейные множители $f = a(x-x_1)(x-x_2)$ над $\mathbb{R}$ тогда и только тогда, когда его дискриминант $D \geqslant 0$. В этом случае, многочлен f приводим над $\mathbb{R}$. Следовательно, он будет неприводим над $\mathbb{R}$ тогда и только тогда, когда $D = b^2 - 4ac < 0$. А многочлены первой степени являются неприводимыми над любым полем. □

Следствие 6.7.2.1. Любой многочлен положительной степени над полем действительных чисел имеет каноническое представление вида:

$$f = \alpha(x-\gamma_1)^{k_1} \dots (x-\gamma_t)^{k_t}(x^2+\beta_1 x+\delta_1)^{l_1} \dots (x^2+\beta_r x+\delta_r)^{l_r},$$

где $\alpha, \beta_i, \delta_i, \gamma_j \in \mathbb{R},\ \beta_i^2 - 4\delta_i < 0,\ k_j, l_i \in \mathbb{N}$ при $i = \overline{1,r},\ j = \overline{1,t}$.

Следствие 6.7.2.2. Любой многочлен с действительными коэффициентами нечетной степени имеет, по крайне мере, один действительный корень.

Доказательство. В самом деле, по следствию 6.7.2.1 $\deg f = k_1 + \ldots + k_t + 2l_1 + \ldots + 2l_r$. По условию степень f — число нечетное, следовательно $k_1 + \ldots + k_t$ — нечетное число, значит $(\exists\ 1 \leqslant i \leqslant t) \quad k_i \geqslant 1$, то есть γ_i является действительным корнем многочлена f. $\square$

Учебное пособие

СЕЦИНСКАЯ Елена Владимировна
КРИВОБОК Валерий Викторович

АЛГЕБРА. ЧАСТЬ I

Учебное пособие для студентов
механико-математического факультета

Технический редактор
Корректор

Подписано в печать . .2007. Формат 60×84 1/16. Бумага офсетная.
Гарнитура Times. Печать офсетная.
Усл.печ.л. ( ) Уч.-изд.л. Тираж экз. Заказ

Издательство Саратовского университета.
410012, Саратов, Астраханская, 83.
Типография Издательства Саратовского университета.
410012, Саратов, Астраханская, 83.