МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЯРОСЛАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМ. П.Г. ДЕМИДОВА

М.В. НЕВСКИЙ

ЛЕКЦИИ ПО АЛГЕБРЕ

Учебное пособие

Рекомендовано Научно-методическим советом
по прикладной математике и информатике
Учебно-методического объединения университетов РФ
для студентов университетов, обучающихся по специальности
"010200 - Прикладная математика и информатика"

ЯРОСЛАВЛЬ 2002

ББК В14я73
Н40

Рецензенты: кафедра алгебры Ярославского государственного педагогического университета им. К.Д. Ушинского; д-р пед. наук, профессор Е.И. Смирнов (ЯГПУ им. К.Д. Ушинского); канд. физ.-мат. наук, доцент Г.Д. Ким (МГУ им. М.В. Ломоносова, факультет вычислительной математики и кибернетики).

Невский М.В. Лекции по алгебре : Учеб. пособие / Яросл. гос. ун-т. Ярославль, 2002. 265 с.

ISBN 5-8397-0202-1

Учебное пособие предназначено для студентов университетов, обучающихся по специальности "010200 – Прикладная математика и информатика".

Пособие содержит материал по следующим разделам алгебры: системы линейных уравнений; матрицы; определители; линейные пространства, подпространства и ранг; евклидовы пространства; линейные операторы; билинейные и квадратичные формы; группы, кольца, поля; комплексные числа; многочлены.

Библиогр. : 27 назв.

ISBN 5-8397-0202-1

Содержание

Часть 2

Часть 3

Часть 4

Предисловие автора

Учебное пособие содержит лекции по ряду основных тем алгебры, изучаемых студентами первого курса университетов специальности "010200 – Прикладная математика и информатика". Эти темы содержатся в разделах "Линейная алгебра"и "Элементы общей алгебры"Примерной программы дисциплины "Геометрия и алгебра утверждённой в 2000 г. Министерством образования Российской Федерации. Автор в течение последних пятнадцати лет читает лекции по указанной дисциплине на математическом факультете Ярославского государственного университета им. П.Г. Демидова.

Пособие не является альтернативой общепризнанным или новым учебникам по алгебре, рекомендованным для специальностей "Прикладная математика"или "Прикладная математика и информатика"и не претендует на большую оригинальность, а лишь предназначено для более успешной организации самостоятельной работы студентов.

Первые три части пособия относятся к *линейной алгебре.* Первая часть содержит основные сведения по системам линейных уравнений, простейшие примеры линейных пространств (n-мерные и геометрические векторы, матрицы), а также введение в теорию определителей. Во вторую часть входят лекции по темам: линейные пространства; подпространства и ранг; евклидовы пространства. В третьей части изучаются темы: линейные операторы; собственные значения, диагонализируемость и каноническая форма матрицы оператора; билинейные и квадратичные формы; операторы в евклидовом пространстве.

Наконец, четвёртая часть относится к тематике *общей алгебры.* В ней содержатся разделы: классические алгебраические структуры (группа, кольцо, поле); комплексные числа; многочлены.

В начале каждого раздела приводятся исторические и иные справочные сведения. Некоторые справки подобного рода даются и в основном тексте.

Нумерация разделов и пунктов является общей для всех частей. При ссылках чаще всего указывается номер соответствующего раздела или пункта. Формулы нумеруются заново в пределах каждого раздела. Изложение сопровождается упражнениями, замечаниями и примерами; их нумерация осуществляется в пределах пункта. То же касается и теорем всех разделов, кроме первого.

Пособие было издано первоначально в трёх книгах с названием "Лекции по дисциплине "Геометрия и алгебра (части 1 – 2, часть 3, часть 4). В настоящем тексте исправлены некоторые неточности и устранены замеченные опечатки; было решено также изменить название на более соответствующее содержанию.

Автор считает своим приятным долгом выразить благодарность декану математического факультета ЯрГУ профессору В.Г. Дурневу за содействие в работе над книгой, а также заведующему кафедрой алгебры и математической логики ЯрГУ профессору Л.С. Казарину и доценту факультета вычислительной математики и кибернетики МГУ Г.Д. Ким за ряд важных замечаний.

Ярославль, январь 2002 г.

Часть 1

1. Системы линейных уравнений и их решение методом Гаусса

Основной метод решения систем линейных уравнений связан с именем великого немецкого математика Карла Фридриха Гаусса (C.F. Gauss, 1777 – 1855).

В связи с историей метода исключения переменных — так иначе называется метод Гаусса — приведём две цитаты.

Г. Стренг [24] : "Гаусс признан величайшим из математиков, но, разумеется, не из-за этого открытия, на которое ему потребовалось, вероятно, минут 10. Но по иронии судьбы среди всех идей, связанных с его именем, наиболее часто упоминается рассматриваемая нами идея исключения[1]."

А. Схрейвер [25] : "То, что мы сейчас называем методом исключения Гаусса, было описано явно в замечательном китайском источнике "9 книг по арифметике". Эта книга датируется ранним периодом Хань (202 г. до н.э. – 9 г. н.э.), однако, приведённый в ней метод был, видимо, разработан гораздо раньше. Книга 8 содержит метод исключения для задач, имеющих до 5 линейных уравнений с 5 неизвестными."

Естественно, системы линейных уравнений встречались и раньше (у вавилонян, греков, китайцев). Линейные уравнения и исключение исследовались также Диофантом Александрийским (примерно 3 век н.э.), индийским математиком Ариабхата (р. в 476 г.), уроженцем Хивы аль-Хорезми в его знаменитой книге "Аль-джебр ва-л-мукабал"(ок. 825 г.), другими математиками. После того, как Гаусс использовал в своих работах метод исключения, последний получил его имя.

Весьма интересно заметить, что Гаусс изучал линейные уравнения в связи с определением орбит небесных тел, положения которых даются с ошибками. Это приводит к задаче нахождения или оценки коэффициентов специальных алгебраических линий, а именно конических сечений. Для этой цели Гаусс в 1809 г. разработал знаменитый *метод наименьших квадратов*, введённый независимо Лежандром (A.Legendre, 1805). Этот метод свёлся к решению линейных уравнений. Авторство Гаусса датируется по его утверждению 1795 г. — он пишет об "обычном исключении".

Отметим здесь, что процедура исключения Гаусса относится к *точным методам* решения линейных систем, в отличие от *приближённых методов*, изучаемых в курсах вычислительной математики.

Кроме решения систем линейных уравнений, метод Гаусса применяется в ряде других задач (вычисление определителя и ранга, нахождение обратной матрицы).

[1]Важность и удивительное многообразие задач, решаемых с помощью систем линейных уравнений, гарантируют устойчивость памяти; ирония, таким образом, исчезает. — **М.Н.**

1.1. Общий вид системы линейных уравнений. Матрицы. Линейные функции n переменных

Система из m линейных уравнений с n неизвестными $x_1, \ldots, x_n$ имеет следующий вид:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{12}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ \ldots \qquad\quad \ldots \qquad\quad \ldots & \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m \end{aligned} \tag{1}$$

Натуральные m и n (число уравнений и число неизвестных соответственно) могут быть произвольными. Случай $m = 1$ соответствует одному уравнению с n неизвестными; случай $m = n$ означает, что число уравнений совпадает с числом неизвестных. Неизвестные x_i, коэффициенты a_{ij} и свободные члены уравнений b_i предполагаются действительными. Индекс i обозначает номер уравнения, индекс j — номер неизвестного, $i = 1, \ldots, m;\ j = 1, \ldots, n$.

Прямоугольная таблица из m строк и n столбцов, составленная из коэффициентов a_{ij}, называется *матрицей системы уравнений (1)* и обозначается $\mathbf{A} = (a_{ij})$, $i = 1, \ldots, m,\ \ j = 1, \ldots, n,$ или в развёрнутом виде

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}.$$

Если справа к матрице $\mathbf{A}$ дописать столбец свободных членов (b_i), то получится *расширенная матрица системы*. Для удобства столбец свободных членов отделяется вертикальной чертой.

Пример. Для системы уравнений

$$\begin{aligned} 2x_1 - x_2 + x_3 \qquad &= 1 \\ x_1 + 2x_2 + 5x_3 - x_4 &= -7 \end{aligned}$$

$m = 2$, $n = 4$. Расширенная матрица этой системы имеет вид

$$\left(\begin{array}{cccc|c} 2 & -1 & 1 & 0 & 1 \\ 1 & 2 & 5 & -1 & -7 \end{array}\right).$$

Система (1) называется *системой линейных уравнений*, или, коротко, *линейной системой*, потому что в левых частях уравнений стоят так называемые *линейные функции* n переменных $x_1, \ldots, x_n$.

Функция $f(x_1, \ldots, x_n)$ аргументов $x_1, \ldots, x_n \in \mathrm{R}$ называется *линейной* (точнее, *однородно-линейной*), если для некоторых фиксированных $d_1, \ldots, d_n \in \mathrm{R}$

$$f(x_1, \ldots, x_n) = d_1x_1 + \ldots + d_nx_n. \tag{2}$$

Нетрудно показать, что любая функция f такого вида удовлетворяет условиям:

$$(i) \qquad f(x_1 + y_1, \ldots, x_n + y_n) = f(x_1, \ldots, x_n) + f(y_1, \ldots, y_n);$$

$$(ii) \qquad f(\lambda x_1, \ldots, \lambda x_n) = \lambda f(x_1, \ldots, x_n), \qquad \lambda \in \mathrm{R}.$$

Упражнение. Показать, что выполнение равенств $(i), (ii)$ гарантирует существование для функции f чисел d_i из (2) . Поэтому равенства $(i), (ii)$ полностью характеризуют линейные функции n переменных.

1.2. Классификация систем по множеству решений Элементарные преобразования систем и их матриц

Решение системы (1) — упорядоченный набор $(x^*{}_1, \ldots, x^*{}_n)$ действительных чисел, удовлетворяющий всем уравнениям системы. В дальнейшем решение обозначается так же, как и неизвестные — $(x_1, \ldots, x_n)$.

Два решения $(x_1, \ldots, x_n)$ и $(y_1, \ldots, y_n)$ называются равными, если $x_1 = y_1$, $\ldots$, $x_n = y_n$. Каждое конкретное решение называется также *частным решением*. Совокупность всех частных решений системы называется её *общим решением*; чаще всего мы будем задавать его в *параметрическом виде*.

Анализ простых случаев — $m = n = 1$, $m = n = 2$ — показывает, что в зависимости от множества решений системы возможна одна из 3 ситуаций: наличие единственного решения, неединственность решения, отсутствие хотя бы одного решения (приведите примеры). Мы покажем, что и в общем случае $m, n \in \mathrm{N}$ наблюдается то же самое.

Система (1) называется *совместной*, если она обладает хотя бы одним решением; *несовместной (противоречивой)*, если у неё нет ни одного решения; *определённой*, если имеется ровно одно решение; *неопределённой*, если она имеет более одного решения. В последней ситуации, как отмечалось, множество решений бесконечно, но это требует обоснования.

Нулевое решение определяется равенствами $x_1 = \ldots = x_n = 0$. Ясно, что система (1) обладает нулевым решением тогда и только тогда, когда все свободные члены b_i равны нулю; такая система называется *однородной*. Итак, однородная система линейных уравнений всегда совместна и может быть определённой или неопределённой.

Задача решения системы (1) состоит в отыскании всех её решений или установлении того, что система несовместна.

Две линейные системы с одним и тем же числом n неизвестных называются *эквивалентными*, если они имеют одно и то же множество решений, то есть каждое решение одной системы является решением другой. Метод Гаусса решения системы линейных уравнений состоит в преобразовании её в эквивалентную систему, имеющую простой для анализа вид.

Метод Гаусса использует следующие преобразования систем (и их матриц), называемые *элементарными преобразованиями*.

1. Перестановка двух уравнений системы (двух строк матрицы системы).

2. Умножение j-го уравнения системы (j-й строки) на число $c \neq 0$.

3. Прибавление к j-му уравнению (j-й строке) i-го уравнения, умноженного на произвольное число $c \in \mathrm{R}$ (i-й строки, умноженной на $c \in \mathrm{R}$). Здесь $i \neq j$.

При выполнении каждого из преобразований второго или третьего типа меняется лишь одно уравнение системы (и лишь одна строка матрицы) — с номером j.

Теорема 1. *Элементарные преобразования переводят систему (1) в эквивалентную.*

Доказательство проведём лишь для преобразований третьего типа; первые два случая совсем очевидны. Пусть $(x_1, \ldots, x_n)$ — решение исходной системы (1). Тогда оно является также решением системы, преобразованной из (1) по типу 3: очевидно, набор $(x_1, \ldots, x_n)$ будет удовлетворять единственному преобразованному уравнению. Таким образом, каждое решение системы (1) является решением новой, преобразованной системы.

Остаётся заметить, что система (1) может быть восстановлена из новой системы с помощью преобразования того же типа 3 — достаточно к j-му уравнению последней прибавить её i-е уравнение, умноженное на число $-c$. Поэтому по доказанному выше каждое решение новой системы является также решением исходной системы (1).

Теорема доказана.

Часто рассматривают ещё одно преобразование системы, переводящее её в эквивалентную систему с меньшим числом уравнений: удаление нулевого уравнения, то есть уравнения вида

$$0 \cdot x_1 + \ldots + 0 \cdot x_n = 0;$$

ему соответствует вычёркивание нулевой строки расширенной матрицы системы.

1.3. Ступенчатые и специальные ступенчатые матрицы. Теорема о приведении матрицы к ступенчатому виду с помощью элементарных преобразований

Матрица $\mathbf{A} = (a_{ij})$ порядка $m \times n$ (то есть имеющая m строк и n столбцов: $i = 1, \ldots, m;\ j = 1, \ldots, n$) называется *ступенчатой*, если она состоит из одних нулей или имеет следующий вид:

$$\mathbf{A} = \begin{pmatrix} 0 & \ldots & 0 & a_{1k_1} & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & \ldots & 0 & a_{2k_2} & \ldots & \ldots & \ldots & \ldots & \ldots \\ \vdots & & \vdots & & & & & & & & \\ 0 & \ldots & 0 & 0 & \ldots & 0 & \ldots & 0 & a_{rk_r} & \ldots & \ldots \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 \\ \vdots & & & & & & & & & & \vdots \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 \end{pmatrix}.$$

Отмеченные элементы a_{ik_i}, $i = 1, \ldots, r$, являются первыми слева ненулевыми элементами в своих строках; они называются *ведущими элементами.* Верхняя (ступенчатая) часть матрицы состоит из r "ступеней"; это связано с тем, что номера столбцов, в которых расположены ведущие элементы, образуют строго возрастающую последовательность:

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

Нижняя часть матрицы содержит $m - r$ нулевых строк; в случае $r = m$ эта часть отсутствует.

Ясно, что всегда $r \leqslant m$ и $r \leqslant n$. Особо отметим ситуацию $r = n,\ m \geqslant n$. В этом случае $k_1 = 1,\ k_2 = 2,\ \ldots,\ k_n = n$, и ступенчатая часть матрицы имеет *верхний треугольный вид*:

$$\mathbf{A} = \begin{pmatrix} a_{11} & \ldots & \ldots & \ldots \\ 0 & a_{22} & \ldots & \ldots \\ \vdots & & & \\ 0 & 0 & \ldots & a_{nn} \\ 0 & \ldots & \ldots & 0 \\ \vdots & & & \vdots \\ 0 & \ldots & \ldots & 0 \end{pmatrix}$$

Будем говорить, что ступенчатая матрица $\mathbf{A}$ имеет *специальный ступенчатый вид*, если в отмеченной в начале пункта общей форме все ведущие элементы равны 1 и в столбцах над ведущими элементами стоят 0:

$$a_{ik_i} = 1, \quad i = 1, \ldots, r;$$
$$a_{jk_i} = 0, \quad j = 1, \ldots, i-1 \quad (i > 1).$$

Ключевым результатом в обосновании метода Гаусса является следующее утверждение.

Теорема 2. *Каждую матрицу при помощи элементарных преобразований над строками можно привести к ступенчатому и специальному ступенчатому виду.*

Доказательство. (Индукция по числу m строк матрицы).

В случае $m = 1$ матрица уже является ступенчатой. Предположим, что утверждение теоремы о приведении к ступенчатому виду верно для всех матриц с числом строк $m - 1$ и докажем, что оно верно для произвольной матрицы $\mathbf{A}$, имеющей m строк.

Если матрица $\mathbf{A}$ — нулевая, то она уже является ступенчатой. Предположим, что $\mathbf{A}$ — ненулевая. Пусть k — минимальный номер столбца, содержащего ненулевые элементы. Выполняя, если необходимо, преобразование типа 1, добьёмся того, что $a^*_{1k} \neq 0$ ($*$ обозначает элементы преобразованной матрицы). За счёт этого в столбце с номером k нетрудно получить нули в строках, начиная со второй: к i-й строке нужно прибавить первую, умноженную на число

$$l_i = -\frac{a^*_{ik}}{a^*_{1k}}, \quad i = 2, \ldots, m.$$

Рассмотрим, далее, подматрицу полученной матрицы, стоящую в строках с номерами $2, \ldots, m$. По предположению индукции, эту матрицу с $(m-1)$-й строкой можно привести к ступенчатому виду с помощью некоторой цепочки элементарных преобразований. Те же преобразования приведут к ступенчатому виду исходную матрицу $\mathbf{A}$.

Это рассуждение показывает, что каждая матрица может быть приведена к ступенчатому виду с помощью преобразований типов 1 и 3. Теперь с помощью преобразований типа 2 (деление на ведущие элементы) и типа 3 (получение нулей выше ведущих элементов в столбцах с номерами $k_r, k_{r-1}, \ldots, k_2$ поочерёдно — обозначения начала пункта) матрицу можно привести к специальному ступенчатому виду.

Теорема доказана.

Замечания. 1. Доказательство теоремы является, по сути, конструктивным и содержит алгоритм приведения матрицы к ступенчатому и специальному ступенчатому виду.

2. Первый этап описанной процедуры — приведение к ступенчатому виду — называется *прямым ходом метода Гаусса*, а её второй этап — приведение к специальному ступенчатому виду — называется *обратным ходом метода Гаусса*.

1.4. Анализ системы уравнений, имеющей специальный ступенчатый вид. Решение систем методом Гаусса

Предположим, что матрица системы линейных уравнений имеет специальный ступенчатый вид, описанный в предыдущем пункте, $b_1, \ldots, b_m$ — свободные члены уравнений. Мы сохраняем все обозначения предыдущего пункта.

Анализ такой системы осуществляется по следующей схеме.

1. *Если для некоторого* $i \geqslant r+1 \quad b_i \neq 0$, *то система несовместна.*
2. *Если* $b_{r+1} = \ldots = b_n = 0$, *то система совместна и при этом*
   (*a*) *если* $r = n$ *— система является определённой;*
   (*b*) *если* $r < n$ *— система является неопределённой.*

Обоснование первого утверждения очевидно: в этом случае i-е уравнение системы имеет вид

$$0 \cdot x_1 + \ldots + 0 \cdot x_n = b_i,$$

причём $b_i \neq 0$.

Во втором случае подобных уравнений нет, и из первых r уравнений можно выразить неизвестные с индексами $k_1, k_2, \ldots, k_r$ через остальные неизвестные; при этом x_{k_i} выражается из i-го уравнения. Формулы имеют вид

$$x_{k_i} = b_i - \sum_{j>k_i,\ j\neq k_{i+1},\ldots,\ k_r} a_{ij}x_j,$$

$i = 1, \ldots, r$. Неизвестные $x_{k_1}, \ldots, x_{k_r}$ называются *главными*, их число r равно числу ступеней и числу ведущих элементов матрицы. Остальные неизвестные, то есть те,

через которые выражаются главные, называются *свободными*; их можно считать свободными параметрами решений. Число свободных неизвестных $n - r$. Меняя произвольным образом значения свободных неизвестных и подставляя их в формулы для главных неизвестных, мы получим все решения системы.

Остаётся заметить, что если система совместна и $r = n$, то свободные неизвестные отсутствуют, и система имеет единственное решение

$$x_1 = b_1, \ \ldots, \ x_n = b_n.$$

Если же $r < n$, то наличие хотя бы одного свободного неизвестного означает, что система является неопределённой.

Сущность метода Гаусса состоит в приведении матрицы исходной системы к специальному ступенчатому виду с помощью элементарных преобразований и последующему анализу полученной системы по изложенной выше схеме.

Итак, мы получили следующий основной результат.

Теорема 3. *Пусть дана система m линейных уравнений с n неизвестными. Применим к строкам её расширенной матрицы такие преобразования, чтобы матрица системы привелась к специальному ступенчатому виду. Пусть r — число ненулевых строк этой матрицы (число ступеней), b_i — преобразованные свободные члены. Если для некоторого $i > r \quad b_i \neq 0$, то исходная система несовместна. Если $b_i = 0$ для всех $i = r+1, \ldots, m$, то исходная система совместна, причём она является определённой при $r = n$ и неопределённой при $r < n$.*

Следствие 1. *Если $m < n$, то система является либо несовместной, либо неопределённой.*

Следствие 2. *Однородная система линейных уравнений при $m < n$ обладает ненулевым решением.*

1.5. Вычислительные особенности решения систем линейных уравнений. Трудоёмкость метода Гаусса

На практике системы линейных уравнений возникают из математических моделей того или иного вида. При этом далеко не всегда коэффициенты и свободные члены уравнений известны точно. Если же используются приближённые вычисления, то следует иметь в виду первую и главную особенность линейных систем — задача решения таких систем является *неустойчивой*.

Неустойчивость задачи или метода её решения означает, что малые изменения в исходных данных приводят к существенным изменениям в результате. В случае линейных систем малые изменения коэффициентов уравнений могут изменить результат и качественно (совместность, определённость), и количественно (два решения, соответствующие близким значениям коэффициентов, могут различаться весьма существенно). Примеры такого сорта легко привести уже в простых ситуациях $m = n = 1, \ m = n = 2$.

Для решения неустойчивых задач созданы специальные методы. В этом тексте мы лишь указываем на то, что требуется иметь в виду.

Второе обстоятельство заключается в том, что разные методы решения систем линейных уравнений имеют различную *трудоёмкость*, что также сказывается на эффективности их применения.

Под трудоёмкостью алгоритма в простейшей ситуации понимают число арифметических операций, чаще всего — число операций умножения, требующихся для его реализации.

Оценим трудоёмкость метода Гаусса в случае $m = n$.

Рассмотрим систему линейных уравнений с расширенной матрицей

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} & b_n \end{array}\right).$$

Определим максимальное возможное число операций умножения-деления на двух этапах метода Гаусса.

Прямой ход. Чтобы получить нули в первом столбце ниже ведущего элемента a_{11}, для каждой из строк с номерами $2, \dots, n$ считается множитель l, затем выполняются n операций для преобразований элементов строки (с учётом свободных членов) — итого $(n+1)(n-1) = n^2 - 1$ операций для первого столбца. Для второго столбца число n заменяется на $n-1$, то есть требуется $(n-1)^2 - 1$ операций, чтобы получить нули ниже ведущего элемента a_{22}. Эти рассуждения показывают, что число умножений-делений при выполнении прямого хода метода Гаусса равно

$$n^2 - 1 + (n-1)^2 - 1 + \ldots + 1^2 - 1 = \sum_{k=1}^{n} k^2 - n =$$

$$= \frac{n(n+1)(2n+1)}{6} - n = \varphi_1(n).$$

Обратный ход. Требуется n операций для приведения к нужному виду последнего столбца коэффициентов, $n-1$ операция — для предпоследнего столбца и т. д., то есть всего для обратного хода

$$n + (n-1) + \ldots + 1 = \frac{n(n+1)}{2} = \varphi_2(n).$$

Таким образом, при решении системы n линейных уравнений с n неизвестными по методу Гаусса требуется

$$\varphi(n) = \varphi_1(n) + \varphi_2(n) = \frac{n(n+1)(2n+1)}{6} + \frac{n(n+1)}{2} - n$$

операций умножения-деления. Особое значение имеет оценка для $\varphi(n)$ при больших n:

$$\varphi(n) = O(n^3); \qquad \varphi(n) \approx \frac{n^3}{3}\ .$$

Запись $f(n) = O(g(n))$ означает, что при достаточно больших n выполняется неравенство $f(n) \leqslant cg(n)$, c — константа.

Итак, *метод Гаусса имеет трудоёмкость* $O(n^3)$ — этот факт нужно запомнить.

Некоторые весьма изощрённые методы решения систем с матрицей общего вида имеют меньшую трудоёмкость, например, $O(n^{log_2 7})$, но они являются логически существенно более сложными, чем метод Гаусса.

Ясно, что при конкретизации матрицы системы трудоёмкость решения задачи может быть понижена. Для систем с матрицами особого вида разработаны специальные методы. В качестве примера отметим описанный в специальной литературе *алгоритм Тренча* решения системы линейных уравнений с *ганкелевой матрицей*, то есть матрицей вида

$$\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_2 & a_3 & a_4 & \dots & a_{n+1} \\ a_3 & a_4 & a_5 & \dots & a_{n+2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_n & a_{n+1} & a_{n+2} & \dots & a_{2n-1} \end{pmatrix}.$$

Алгоритм Тренча имеет трудоёмкость $O(n^2)$.

Особые экономные методы применяются при решении систем с так называемыми *разреженными матрицами*, то есть матрицами, содержащими большую долю нулевых элементов; такие матрицы часто встречаются в приложениях.

Отметим в заключение, что с *приближёнными методами решения систем линейных уравнений* связан обширный раздел методов вычислений; в нём исследуются интересные и практически важные задачи. Некоторые из так называемых *итерационных алгоритмов* описаны, например, в учебнике В.А. Ильина, Э.Г. Позняка [9, с. 161 – 179]. Эти вопросы требуют от читателя определённой предварительной подготовки и здесь не рассматриваются.

2. Матрицы и действия с ними

Матрицы возникают там и тогда, где и когда решаются системы линейных уравнений или вычисляются определители — таков доисторический путь *теории матриц*, важной и интересной составляющей линейной алгебры.

Понятие матрицы введено в специальное рассмотрение лишь в середине 19 в. в работах английских математиков У. Гамильтона (W. Hamilton) и А. Кэли (A. Cayley). Сам термин *матрица* был предложен Дж. Сильвестром (J. Sylvester, 1850). Основной работой, в которой матрицы представлены абстрактно как особые объекты, хотя к тому времени они уже широко применялись, был мемуар Кэли (1858). Именно здесь обсуждаются важные свойства операций над матрицами, в первую очередь — матричного умножения.

Стоит отметить, что определение этой экзотической операции принадлежит Коши (A. Cauchy, 1815). Умножение 3×3 матриц ранее введено Гауссом (C. Gauss), который шёл, по существу, от суперпозиции операторов.

Фундаментальные результаты в теории матриц принадлежат также К. Вейерштрассу (K. Weirstraass), К. Жордану (C. Jordan), Г. Фробениусу (G. Frobenius) и др.

Рассматриваемое в первом пункте понятие n-мерного арифметического пространства связано с независимыми исследованиями А. Кэли в Англии и Г. Грассмана (H. Grassman) в Германии (ок. 1843 – 1845 гг.).

Для Кэли исходным пунктом был метод координат. Сложение двух n-мерных векторов и умножение на скаляр определялось естественным образом по аналогии с трёхмерным пространством; Кэли говорил, что это всего лишь удобный язык. Более оригинальный и непосредственно геометрический подход Грассмана позволил подойти к фундаментальному понятию *линейного пространства*.

2.1. Пространство $\mathrm{R^n}$. Действия с n-мерными векторами

Начнём со следующего определения.

Определение. *Пусть $n \in \mathrm{N}$. Действительным арифметическим n-мерным пространством $\mathrm{R^n}$ называется множество упорядоченных наборов $x = (x_1,\ldots,x_n)$ из n действительных чисел x_i, рассматриваемое вместе с определяемыми ниже операциями сложения и умножения на число.*

Каждый набор $x \in \mathrm{R^n}$ называется n-мерным вектором. Числа x_i называются компонентами вектора x.

Два n-мерных вектора $x = (x_1, \ldots, x_n)$ и $y = (y_1, \ldots, y_n)$ называются равными $(x = y)$ тогда и только тогда, когда $x_1 = y_1, \ldots, x_n = y_n$.

Сложение двух n-мерных векторов и умножение вектора на действительное число определяются с помощью равенств

$$x + y := (x_1 + y_1, \ldots, x_n + y_n),$$
$$\lambda x := (\lambda x_1, \ldots, \lambda x_n), \ \lambda \in \mathrm{R}.$$

Итак, равенство векторов из R^n, а также их сложение и умножение на число определяются *покомпонентно.*

В обозначении R^n символ n есть степень: R^n есть так называемое *прямое (декартово) произведение* n экземпляров множества R.

Прямое произведение двух множеств U и V, каждое — произвольной структуры, есть новое множество

$$W = U \times V := \{w = (u, v) : u \in U, v \in V\},$$

причём равенство элементов $W = U \times V$, то есть пар, понимается как два равенства соответствующих компонент. Прямое произведение n множеств определяется по индукции; натуральная степень соответствует одинаковым сомножителям.

Метод координат позволяет дать ясную геометрическую интерпретацию $\mathrm{R}^1 := \mathrm{R}$, R^2, R^3 как совокупностей точек прямой, плоскости, пространства, а также действий с ними, см. подробнее раздел 4. Простота этой аналогии лишает загадочности переход к большим размерностям. Однако R^4 "увидеть"уже нельзя, и с этим ничего не поделаешь.

Введённые операции сложения и умножения на число обладают следующими свойствами:

$$\begin{aligned}
&1^\circ. \quad x + y = y + x,\\
&2^\circ. \quad (x + y) + z = x + (y + z),\\
&3^\circ. \quad x + 0 = x,\\
&4^\circ. \quad \exists(-x) \ : \ x + (-x) = 0,\\
&5^\circ. \quad \alpha(\beta x) = (\alpha\beta)x,\\
&6^\circ. \quad 1 \cdot x = x,\\
&7^\circ. \quad \alpha(x + y) = \alpha x + \alpha y,\\
&8^\circ. \quad (\alpha + \beta)x = \alpha x + \beta x.
\end{aligned}$$

Здесь $x, y, z \in \mathrm{R}^n$, $\alpha, \beta \in \mathrm{R}$ — произвольны; $0 := (0, \ldots, 0)$ — *нулевой вектор* R^n. Вектор $(-x)$ называется *противоположным к* x; очевидно, $-x = (-x_1, \ldots, -x_n)$.

Отмеченные свойства очевидны — нужно лишь перейти к компонентам векторов.

Эти свойства операций сложения и умножения на число мы выделим особо. Выполнение свойств 1° – 8° означает, что относительно операций сложения и умножения на число R^n *образует так называемое линейное пространство.*

Благодаря свойствам 1° – 8° мы можем привычным образом обращаться с *линейными комбинациями векторов*, то есть суммами вида

$$x = \alpha a + \beta b + \ldots + \gamma c,$$

а также равенствами в R^n.

Вычитание в R^n определяется как действие, противоположное сложению: $z = x - y$, если $z + y = x$.

Упражнение. Система векторов

$$e^{(1)} := (1, 0, \ldots, 0, 0),$$

$$e^{(2)} := (0, 1, \ldots, 0, 0),$$

$$\ldots \qquad \ldots \qquad \ldots$$

$$e^{(n)} := (0, 0, \ldots, 0, 1)$$

называется стандартным, или каноническим, базисом $\mathrm{R^n}$. *Проверить для* $x = (x_1, \ldots, x_n)$ *равенство*

$$x = \sum_{i=1}^{n} x_i e^{(i)}.$$

2.2. Пространство матриц $M_{m,n}$. Простейшие операции над матрицами и их свойства

Пусть $m, n \in \mathrm{N}$. Под *матрицей* порядка $m \times n$ понимается прямоугольная таблица (чисел), имеющая m строк и n столбцов (мы уже рассматривали такие таблицы в разделе 1). Элементы матриц $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, ... обозначаются, как правило, теми же буквами: $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij})$, $\mathbf{C} = (c_{ij}), \ldots$

Две матрицы называются равными, если они имеют одинаковый порядок и все их соответствующие элементы совпадают:

$$\mathbf{A} = \mathbf{B} \iff \forall i, j \quad a_{ij} = b_{ij}.$$

Для фиксированных $m, n \in \mathrm{N}$ совокупность всех $m \times n$-матриц с действительными элементами обозначается $M_{m,n}(\mathrm{R})$ или $M_{m,n}$. Считаем, кроме того, $M_n := M_{n,n}$.

Простейшие операции над матрицами — это сложение матриц и умножение матрицы на число. Эти операции, как и равенство матриц, определяются *поэлементно*:

$$\mathbf{C} = \mathbf{A} + \mathbf{B} \qquad \Longleftrightarrow \qquad \forall i, j \quad c_{ij} = a_{ij} + b_{ij} \ ;$$

$$\mathbf{C} = \lambda \mathbf{A} \qquad \Longleftrightarrow \qquad \forall i, j \quad c_{ij} = \lambda a_{ij} \ .$$

Здесь $\mathbf{A}, \mathbf{B} \in M_{m,n}$, $\lambda \in \mathrm{R}$; результат $\mathbf{C}$ также принадлежит $M_{m,n}$. Заметим, что сложение определено лишь для матриц одинакового порядка.

Введённые операции, подобно действиям с n-мерными векторами, также обладают перечисляемыми ниже восемью свойствами; их выполнение означает, что относительно сложения и умножения на число $M_{m,n}$ *является линейным пространством.* Все свойства легко устанавливаются при переходе к элементам матриц.

1°. $\quad \mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$,

2°. $\quad (\mathbf{A} + \mathbf{B}) + \mathbf{C} = \mathbf{A} + (\mathbf{B} + \mathbf{C})$,

3°. $\mathbf{A} + \mathbf{0} = \mathbf{A}$,

4°. $\exists(-\mathbf{A}) : \ \mathbf{A} + (-\mathbf{A}) = \mathbf{0}$,

5°. $1 \cdot \mathbf{A} = \mathbf{A}$,

6°. $\alpha(\beta\mathbf{A}) = (\alpha\beta)\mathbf{A}$,

7°. $\alpha(\mathbf{A} + \mathbf{B}) = \alpha\mathbf{A} + \alpha\mathbf{B}$,

8°. $(\alpha + \beta)\mathbf{A} = \alpha\mathbf{A} + \beta\mathbf{A}$.

Нулевая матрица $\mathbf{0}$ по определению состоит из одних нулей; матрица $-\mathbf{A} = (-a_{ij})$ называется *противоположной* к $\mathbf{A}$.

Очевидным образом — как операция, обратная сложению, — вводится вычитание матриц.

Итак, мы мотивировали следующее определение.

Определение. *Пусть* $m, n \in \mathrm{N}$. *Множество* $M_{m,n}$, *рассматриваемое вместе с введёнными выше операциями сложения двух матриц и умножения матрицы на действительное число, называется пространством* $m \times n$*-матриц.*

Внимательный читатель, вероятно, заметил, что с точки зрения операций сложения и умножения на число действительное арифметическое пространство и пространство матриц устроены однотипно: действия и равенства определяются поэлементно, и между матрицами порядка $m \times n$ и векторами из R^{mn} легко устанавливается взаимно-однозначное соответствие, "сохраняющее операции". Говорят, что R^{mn} и $M_{m,n}$ *изоморфны как линейные пространства*. В этом пункте мы не будем останавливаться на этом подробно.

На множестве матриц можно ввести ещё одну несложную операцию — *транспонирование*. Попросту говоря, при транспонировании строки матрицы записываются по столбцам, и наоборот.

Если $\mathbf{A} = (a_{ij}) \in M_{m,n}$, то транспонированная к ней матрица $\mathbf{A}^T = (a'_{kl})$ принадлежит классу $M_{n,m}$, а элементы этих матриц связаны соотношениями

$$a'_{ij} = a_{ji} \ ; \quad i = 1, \ldots, n, \ j = 1, \ldots, m.$$

Ясно, что $(\mathbf{A}^T)^T = \mathbf{A}$ для любой матрицы $\mathbf{A}$.

Какие матрицы не меняются при транспонировании? Условие $\mathbf{A}^T = \mathbf{A}$ означает, что $\mathbf{A} \in M_n$ и для элементов a_{ij} выполнены равенства

$$a_{ji} = a_{ij} \ , \ i, j = 1, \ldots, n. \tag{1}$$

Квадратная матрица $\mathbf{A}$ порядка n, удовлетворяющая (1), называется *симметричной*. Совокупность всех действительных симметричных матриц порядка n обозначается через $SM_n(\mathrm{R})$ или SM_n. Симметричные матрицы обладают рядом интересных и важных для приложений свойств.

Упражнение. Показать, что для произвольной квадратной матрицы $\mathbf{A}$ *порядка* n *существуют единственная симметричная матрица* $\mathbf{B}$ *и единственная кососимметричная матрица* $\mathbf{C}$ $(c_{ji} = -c_{ij})$ *такие, что* $\mathbf{A} = \mathbf{B} + \mathbf{C}$. *Получить явные формулы для матриц* $\mathbf{B}$ *и* $\mathbf{C}$.

2.3. Умножение матриц. Свойства умножения

Умножение матриц — наиболее сложное из рассматриваемых действий с матрицами. Мы дадим подробное его описание.

Подход к определению матричного умножения, которое на первый взгляд выглядит весьма экзотическим, может быть обоснован в терминах *линейных операторов и их матриц*: матрица суперпозиции линейных операторов равна произведению матриц этих операторов. По понятным причинам прояснение этой связи несколько откладывается.

Прежде всего нужно иметь в виду, что умножать можно лишь матрицы подходящих размеров. Именно, произведение

$$\mathbf{C} = \mathbf{AB}$$

(именно в таком порядке) определено лишь в том случае, когда число столбцов матрицы $\mathbf{A}$ равно числу строк матицы $\mathbf{B}$. Если $\mathbf{A} \in M_{m,n}$, $\mathbf{B} \in M_{n,p}$, то $\mathbf{C} \in M_{m,p}$ и при этом для каждой фиксированной пары индексов $i = 1, \ldots, m, \quad j = 1, \ldots, p$

$$c_{ij} := \sum_{l=1}^{n} a_{il} b_{lj}. \tag{2}$$

Формула (2) означает, что для определения ij-го элемента матрицы $\mathbf{AB}$ элементы i-й строки левой матрицы умножаются на соответствующие элементы j-го столбца правой матрицы и затем все n таких произведений складываются. По этим причинам (2) часто называется правилом умножения "строка на столбец"; лучше всего оно постигается на практике.

Пример 1. Пусть

$$\mathbf{C} = \mathbf{AB} = \begin{pmatrix} 1 & -1 & 5 \\ 3 & 2 & 0 \end{pmatrix} \begin{pmatrix} -1 & 5 & 1 & 1 \\ -2 & 0 & 7 & 1 \\ -1 & 1 & 1 & 2 \end{pmatrix}.$$

Умножение в указанном порядке возможно, так как $\mathbf{A}$ — матрица размера 2×3 и $\mathbf{B}$ — матрица размера 3×4 ; общее значение n, таким образом, равно 3, и все суммы (2) содержат по три слагаемых. Например, $c_{23} = 3 \cdot 1 + 2 \cdot 7 + 0 \cdot 1 = 17$. Проверьте, что

$$\mathbf{C} = \begin{pmatrix} -4 & 10 & -1 & 10 \\ -7 & 15 & 17 & 5 \end{pmatrix}.$$

Пример 2. Используя матричное умножение, можно записать в компактной форме систему m линейных уравнений с n неизвестными. Если

$$\mathbf{A} = \begin{pmatrix} a_{11} & \ldots & \ldots & a_{1n} \\ \vdots & & & \vdots \\ a_{m1} & \ldots & \ldots & a_{mn} \end{pmatrix}, \quad \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

— матрица системы уравнений, столбец неизвестных и столбец свободных членов соответственно, то система имеет вид

$$\mathbf{Ax} = \mathbf{b}. \tag{3}$$

В левой части (3) стоит произведение матрицы $m \times n$ на матрицу $n \times 1$; результатом является матрица $m \times 1$. Обсудите эту запись и её связь с обычным видом системы линейных уравнений, см. пункт 1.1.

Перейдём к рассмотрению свойств умножения матриц. После формулировки свойства даётся его доказательство, а также комментарии, замечания, упражнения, относящиеся к этому свойству. В этот же фрагмент включены некоторые важные определения. Список свойств получается, таким образом, достаточно длинным.

Свойства умножения матриц

1°. *Умножение матриц ассоциативно*:

$$\mathbf{A}(\mathbf{BC}) = (\mathbf{AB})\mathbf{C}. \tag{4}$$

Точнее, если существует левая часть (4), то существует и правая часть, и наоборот, и при этом они равны. В дальнейшем подобный комментарий опускается.

Доказательство. Пусть определено левое произведение $\mathbf{X} := \mathbf{A(BC)}$. Если матрица $\mathbf{BC}$ имеет размеры $n \times q$ (при некоторых n, q), то $\mathbf{B}$ имеет размеры $n \times p$, $\mathbf{C}$ — размеры $p \times q$. Матрица $\mathbf{A}$ имеет порядок $m \times n$ — так как определено внешнее умножение в $\mathbf{A(BC)}$. Нетрудно видеть, что тогда существует произведение $\mathbf{Y} := \mathbf{(AB)C}$, правая часть (4). Обе матрицы $\mathbf{X, Y}$ имеют одинаковые размеры $m \times q$.

Пусть теперь i, j фиксированы, $i = 1, \ldots, m, \quad j = 1, \ldots, q$. Тогда в тех же обозначениях

$$x_{ij} = \sum_{k=1}^{n} a_{ik}(\sum_{l=1}^{p} b_{kl}c_{lj}) = \sum_{k=1}^{n}\sum_{l=1}^{p} a_{ik}b_{kl}c_{lj} =$$

$$= \sum_{l=1}^{p}\sum_{k=1}^{n} a_{ik}b_{kl}c_{lj} = \sum_{l=1}^{p}(\sum_{k=1}^{n} a_{ik}b_{kl})c_{lj} = y_{ij}.$$

В третьем равенстве изменён порядок повторного суммирования.

Свойство 1° доказано.

Следствие. *Пусть существует произведение n матриц вида*

$$\mathbf{G} = (\mathbf{A_1}(\mathbf{A_2}(\ldots(\mathbf{A_{n-1}A_n})\ldots))).$$

Тогда существует и равно $\mathbf{G}$ *любое произведение тех же матриц с другой расстановкой скобок. Иначе говоря, при вычислении произведения любого числа $n \geqslant 3$ сомножителей скобки можно расставлять произвольным способом (если порядок сомножителей не нарушается).*

Упражнение 1. Доказать следствие индукцией по n.

Замечание. В связи с вычислением произведения длинной цепочки сомножителей (не обязательно матриц) естественно возникает вопрос о количестве возможных способов расстановки скобок, то есть о количестве способов вычисления всего произведения без нарушения порядка сомножителей. Свойство ассоциативности гарантирует однозначность результата. Пусть c_k есть число способов расстановки скобок для $k+1$ сомножителей. Первые значения $c_1,\ c_2,\ c_3$ равны соответственно 1, 2 и 5. Значения $c_k,\ k \leqslant 10,$ приведены ниже.

k	1	2	3	4	5	6	7	8	9	10
c_k	1	2	5	14	42	132	429	1430	4862	16796

Бельгийский математик Шарль Эжен Каталан (C. Catalan, 1838) показал, что

$$c_k = \frac{1}{k+1}\left(\begin{array}{c} 2k \\ k \end{array}\right) = \frac{(2k)!}{k!(k+1)!}; \tag{5}$$

он решал именно эту задачу. В его честь c_k называются *числами Каталана.*

Числа Каталана возникают в совершенно различных, но эквивалентных (или изоморфных) задачах. Первым, кто рассматривал последовательность (c_k), был великий Леонард Эйлер (L. Euler, 1707 – 1783). Он показал, что число способов триангуляции (то есть разбиения на треугольники) правильного $(k+2)$-угольника с помощью непересекающихся диагоналей равно c_k. Задача Эйлера изоморфна задаче о расстановке скобок.

Многие интересные сведения о числах Каталана можно найти в книге М. Гарднера [6] — им посвящена там специальная глава.

Упражнение 2. Убедиться в справедливости (5) для $k \leqslant 5$.

Упражнение 3. Установить связь между задачами о числе способов расстановки скобок и числе способов триангуляции правильного многоугольника с помощью непересекающихся диагоналей.

2°. *Умножение матриц некоммутативно, то есть, вообще говоря,*

$$\mathbf{AB} \neq \mathbf{BA}. \tag{6}$$

Неравенство (6) имеет место в тех случаях, когда порядки $\mathbf{AB}$ и $\mathbf{BA}$ не совпадают; оно не подлежит обсуждению, если одно из произведений не определено. Оба этих случая легко могут быть проиллюстрированы примерами. Если произведения из (6) существуют и имеют одинаковый порядок, то $\mathbf{A}$ и $\mathbf{B}$ — квадратные матрицы одного порядка. Но и в этой ситуации (6) может иметь место, например,

$$\left(\begin{array}{cc} 1 & 1 \\ -1 & 0 \end{array}\right)\left(\begin{array}{cc} 2 & -1 \\ 0 & 5 \end{array}\right) = \left(\begin{array}{cc} 2 & 4 \\ -2 & 1 \end{array}\right) \neq$$

$$\neq \left(\begin{array}{cc} 3 & 2 \\ -5 & 0 \end{array}\right) = \left(\begin{array}{cc} 2 & -1 \\ 0 & 5 \end{array}\right)\left(\begin{array}{cc} 1 & 1 \\ -1 & 0 \end{array}\right).$$

Существуют, конечно же, квадратные матрицы, порядок умножения которых не является существенным — для них (6) превращается в равенство. Такие матрицы называются *перестановочными, или коммутирующими.*

3°. *Умножение и сложение связаны свойствами дистрибутивности:*

$$(\mathbf{A}+\mathbf{B})\mathbf{C} = \mathbf{AC}+\mathbf{BC},$$

$$\mathbf{C}(\mathbf{A}+\mathbf{B}) = \mathbf{CA}+\mathbf{CB}.$$

Доказательство. Переходя к элементам матриц, имеем:

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

Это соответствует первому свойству дистрибутивности. Второе доказывается аналогично.

4°. Пусть $\mathbf{E} = (e_{ij}) \in M_n$ — матрица с элементами

$$e_{ij} = \begin{cases} 1 & , \quad i = j \\ 0 & , \quad i \neq j \end{cases} .$$

Матрица $\mathbf{E}$ называется *единичной матрицей (или матричной единицей)* порядка n. *Для любой* $\mathbf{A} \in M_n$

$$\mathbf{AE} = \mathbf{EA} = \mathbf{A}.$$

Доказательство. Пусть $\mathbf{C} := \mathbf{AE}$. Тогда при фиксированных i, j

$$c_{ij} = \sum_{k=1}^{n} a_{ik}e_{kj} = a_{ij}$$

(вклад в сумму даёт лишь слагаемое с номером j). Поэтому $\mathbf{AE} = \mathbf{A}$.

Замечание. Выполнение свойств 1° – 4° сложения матриц, см. пункт 2.2, и свойств 1° - 4° настоящего пункта означает, что совокупность M_n относительно операций сложения и умножения матриц образует так называемое *кольцо* (точнее, *ассоциативное некоммутативное кольцо с единицей* — эти уточнения касаются свойств умножения матриц). Это важный пример нечислового кольца (ср. с коммутативным кольцом целых чисел).

Итак, разный выбор операций над квадратными матрицами порядка n приводит к различным *алгебраическим структурам* — сложение матриц и умножение их на число соответствуют линейному пространству, а сложение и умножение матриц соответствуют кольцу.

5°. (Связь с транспонированием.)

$$(\mathbf{AB})^T = \mathbf{B}^T\mathbf{A}^T. \tag{7}$$

Доказательство. Очевидно, что из существования левой части (7) следует существование правой, и наоборот. Пусть $\mathbf{C} = \mathbf{AB}$ и x'_{ij} — элементы матрицы $\mathbf{X}^T$. Тогда

$$c'_{ij} = c_{ji} = \sum_k a_{jk}b_{ki} = \sum_k a'_{kj}b'_{ik} = \sum_k b'_{ik}a'_{kj},$$

что соответствует равенству (7).

6°. (Связь с умножением на число.) *Для* $\lambda \in \mathrm{R}$

$$(\lambda \mathbf{A})\mathbf{B} = \lambda(\mathbf{AB}).$$

Доказательство очевидно.

7°. *Следом* квадратной матрицы называется сумма элементов её главной диагонали:

$$\mathrm{tr}(\mathbf{A}) := \sum_i a_{ii}.$$

Если оба произведения $\mathbf{AB}$ *и* $\mathbf{BA}$ *существуют, то*

$$\mathrm{tr}(\mathbf{AB}) = \mathrm{tr}(\mathbf{BA}). \tag{8}$$

Упражнение 4. Доказать равенство (8) в общей ситуации (порядки двух произведений не обязательно совпадают).

Натуральная степень квадратной матрицы определяется по индукции:

$$\mathbf{A}^k := \underbrace{\mathbf{A} \cdot \ldots \cdot \mathbf{A}}_{k} .$$

Кроме того, для $\mathbf{A} \in M_n$ полагают $\mathbf{A}^0 := \mathbf{E}$, где $\mathbf{E}$ — единичная матрица из M_n.

8°. *В кольце* $M_n, n \geqslant 2$, *имеются ненулевые решения уравнения*

$$\mathbf{A}^k = \mathbf{0} \tag{9}$$

при $k > 1$.

Пример.

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

Ненулевая матрица $\mathbf{A}$, для которой равенство (9) выполнено с $k > 1$, называется *нильпотентной*, а наименьшее значение k — *индексом нильпотентности* этой матрицы. Такие матрицы возникают в ряде важных вопросов линейной алгебры.

9°. *Трудоёмкость умножения двух квадратных матриц порядка* n *есть* $O(n^3)$.

Точнее, при вычислениях по обычной схеме (по равенствам (2)) умножение двух сомножителей порядка n требует n^3 числовых операций умножения и $n^2(n-1)$ числовых операций сложения. Так, в случае $n = 2$ (умножение двух матриц второго порядка) необходимо 8 умножений и 4 сложения.

Удивительно, но был изобретён способ умножения матриц второго порядка, который требует 7 умножений и 18 сложений. Число умножений уменьшено по сравнению с обычной схемой на 1 (хотя число сложений значительно возросло). Этот

метод назван по фамилии изобретателя *алгоритмом Штрассена* (V. Strassen, 1969). Алгоритм Штрассена состоит в последовательном вычислении следующих значений (вычисляется произведение $\mathbf{C} = \mathbf{AB}$):

$$d_1 := (a_{11} + a_{22})(b_{11} + b_{22}),$$
$$d_2 := (a_{21} + a_{22})b_{11}, \qquad d_3 := a_{11}(b_{12} - b_{22}),$$
$$d_4 := a_{22}(b_{21} - b_{11}), \qquad d_5 := (a_{11} + a_{12})b_{22},$$
$$d_6 := (a_{21} - a_{11})(b_{11} + b_{12}), \qquad d_7 := (a_{12} - a_{21})(b_{21} + b_{22}),$$

и затем

$$c_{11} := d_1 + d_4 - d_5 + d_7, \qquad c_{12} := d_3 + d_5,$$
$$c_{21} := d_2 + d_4, \qquad c_{22} := d_1 + d_3 - d_2 + d_6.$$

Упражнение 5. Проверить, что $\mathbf{C} = \mathbf{AB}$.

Модификации алгоритма Штрассена позволяют снизить трудоёмкость вычисления произведения двух $n \times n$-матриц до $O(n^{log_2 7})$.

Важное свойство матричного умножения, использующее понятие определителя, устанавливается в четвёртом разделе.

2.4. Обратная матрица: определение и простейшие свойства

В настоящем пункте содержатся те сведения об обратимости матриц, которые не связаны явно с понятием определителя. Этот материал должен быть дополнен материалом пункта 4.8 (обратимость и невырожденность, формула для обратной матрицы).

Всюду ниже речь идёт о квадратных матрицах порядка n, то есть элементах множества M_n.

Определение. *Матрица* $\mathbf{A}^{-1}$, *для которой выполнены равенства*

$$\mathbf{A}\mathbf{A}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{E}, \tag{10}$$

называется обратной к матрице $\mathbf{A} \in M_n$. *Матрица* $\mathbf{A}$, *для которой существует обратная, называется обратимой.*

Справа в (10) стоит единичная матрица того же порядка.

Простые примеры показывают, что не всякая матрица из M_n обладает обратной (например, нулевая или состоящая из одних 1 — подумайте, почему). Однако если обратная матрица существует, то она определяется единственным образом.

Упражнение 1. Доказать последнее свойство.

Существование обратной матрицы связано с разрешимостью *матричного уравнения*

$$\mathbf{AX} = \mathbf{E}. \tag{11}$$

Уравнение (11) эквивалентно n системам линейных уравнений для столбцов неизвестной матрицы $\mathbf{X}$ с одной и той же матрицей коэффициентов $\mathbf{A}$ — выпишите их самостоятельно. Так как у всех этих систем матрица коэффициентов одна и

та же, то преобразования метода Гаусса можно проводить одновременно для всех систем.

На этом основан *метод Гаусса вычисления* $\mathbf{A}^{-1}$. Компактная запись имеет вид:

$$(\mathbf{A}|\mathbf{E}) \to \ldots \to (\mathbf{E}|\mathbf{A^{-1}}).$$

Стрелочки обозначают элементарные преобразования над строками удвоенной длины, с помощью которых в левой части получается единичная матрица $\mathbf{E}$. Справа в результате получается обратная матрица $\mathbf{A}^{-1}$.

Нетрудно понять, что трудоёмкость этой процедуры есть $O(n^3)$.

Из свойств обратимых матриц отметим здесь следующие.

1°. $\quad (\mathbf{A}^{-1})^{-1} = \mathbf{A}$.

2°. $\quad (\mathbf{AB})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1}$.

3°. $\quad (\mathbf{A}^T)^{-1} = (\mathbf{A}^{-1})^T$.

Упражнение 2. Установить свойства 1° – 3°.

Отметим особо, что обращение матриц тесно связано с решением систем n уравнений с n неизвестными. Именно, если существует $\mathbf{A}^{-1}$, то матричные равенства

$$\mathbf{Ax} = \mathbf{b}, \quad \mathbf{x} = \mathbf{A}^{-1}\mathbf{b}$$

эквивалентны. Здесь $\mathbf{x}$, $\mathbf{b}$ — столбцы неизвестных и свободных членов соответственно.

2.5. Многочлен от матрицы, аннулирующий многочлен и другие вопросы

Пусть $p(x) = a_0 + a_1 x + \ldots + a_k x^k$ — многочлен с действительными коэффициентами a_i от переменной x; $\mathbf{A} \in M_n$. Положим по определению

$$p(\mathbf{A}) := a_0\mathbf{E} + a_1\mathbf{A} + \ldots + a_k\mathbf{A}^k.$$

Очевидно, $p(\mathbf{A})$ — квадратная матрица порядка n. Так определяется *многочлен от матрицы*.

Если $p(\mathbf{A}) = \mathbf{0}$, то многочлен $p(x)$ называют *аннулирующим многочленом* для $\mathbf{A}$. Оказывается, что для каждой матрицы существует ненулевой аннулирующий многочлен. Простое доказательство даёт оценку степени аннулятора $deg\ p \leqslant n^2$; оно связано с линейной зависимостью системы из $n^2{+}1$ следующих матриц порядка n:

$$\mathbf{E},\ \mathbf{A},\ \ldots\ , \mathbf{A}^{n^2}\ .$$

Существенным усилением является следующий результат (*теорема Гамильтона – Кэли*): если p — так называемый *характеристический многочлен* матрицы $\mathbf{A}$, то $p(\mathbf{A}) = \mathbf{0}$. Здесь мы лишь отметим простую форму этой теоремы для $n = 2$.

Упражнение. Пусть $\mathbf{A}$ *— квадратная матрица второго порядка,*

$$p(x) := |\mathbf{A} - x\mathbf{E}| = x^2 - \mathrm{tr}(\mathbf{A})x + |\mathbf{A}|$$

— её характеристический многочлен. Проверить с помощью прямого вычисления, что $p(\mathbf{A}) = \mathbf{0}$.

Разложение функций в степенные ряды (частичные суммы таких рядов есть многочлены) даёт возможность определить некоторые *функции от матриц.* Например, для всех $x \in \mathrm{R}$

$$e^x = \sum_{j=0}^{\infty} \frac{x^j}{j!},$$

в связи с чем для $\mathbf{A} \in M_n$ полагают

$$\exp(\mathbf{A}) = e^{\mathbf{A}} := \sum_{j=0}^{\infty} \frac{1}{j!}\mathbf{A}^j \quad .$$

Для того, чтобы придать смысл сходимости последнего ряда, состоящего из матриц, на пространстве M_n вводят какую-либо *норму*, после чего даётся обычное в анализе определение.

Интересные свойства функций от матриц связаны с понятиями подобия, жордановой формы матрицы и др.

В этом разделе мы привели лишь часть важнейших сведений о матрицах. В дальнейшем эти сведения будут существенно пополнены (*определители, ранг, подобие, собственные числа и собственные значения, положительная определённость, каноническая форма, свойства симметричных и ортогональных матриц и др.*).

Отметим, что в приложениях часто используются и специальные свойства матриц. Заинтересованный читатель может ознакомиться с ними, например, в монографиях Р. Беллмана [3], Ф.Р. Гантмахера [5], Р. Хорна и Ч. Джонсона [26]. (Последняя книга содержит, в частности, большой набор полезных задач и упражнений.)

3. Линейное пространство геометрических векторов. Линейная зависимость и независимость

Основное содержание этого раздела состоит в том, что подобно матрицам и n-мерным векторам обычные геометрические векторы прямой, плоскости или пространства образуют совокупности со структурой линейных пространств.

Особое значение имеют понятия *линейной зависимости и независимости, базиса, размерности*.

Алгебраический подход позволяет действовать по единой схеме для всех отмеченных совокупностей, однако, в геометрической ситуации эти понятия могут быть прояснены с помощью геометрической характеризации.

В простейшем варианте рассматривается свойство *изоморфности линейных пространств*.

Рассматриваемые вопросы лежат в основе *метода координат*, который ввели в математику французы Рене Декарт (R. Descartes, 1596 – 1650) и Пьер Ферма (P. Fermat, 1601 – 1665).

Этот метод является главным оружием *аналитической геометрии* и средством исследования *конечномерных линейных пространств*.

3.1. Геометрические векторы: основные понятия. Сложение и умножение на число. Пространство $\mathrm{V_n},\ n = 1, 2, 3$

Обычный *геометрический вектор* — это объект, который характеризуется *направлением и длиной*. Для наглядности вектор часто представляют как *направленный отрезок*; при этом два таких отрезка считаются равными, если они совпадают при некотором параллельном переносе.

Длина вектора $\vec{a}$ (то есть расстояние между *началом* и *концом* этого вектора) обозначается ниже $|\vec{a}|$. *Нулевой вектор* $\vec{a} = \vec{0}$ определяется равенством $|\vec{a}| = 0$.

Векторы, лежащие на одной прямой (или параллельные одной прямой), называются *коллинеарными* — для двух таких векторов пишем $\vec{a} \parallel \vec{b}$. Коллинеарные векторы могут быть *противоположно или одинаково направленными*. Векторы, лежащие в одной плоскости (или параллельные одной и той же плоскости), называются *компланарными*.

Простейшими действиями с векторами, как известно, являются *сложение векторов и умножение вектора на действительное число*.

Сложение двух векторов осуществляется по *правилу треугольника* или эквивалентному ему *правилу параллелограмма*. Умножение на число выглядит сложнее. Именно, запись $\vec{b} = \lambda\vec{a}\ ,\ \lambda \in \mathrm{R}$, означает по определению:

(i) $\qquad \vec{b} \parallel \vec{a}$;

(ii) $\qquad |\vec{b}| = |\lambda||\vec{a}|$;

(*iii*) если $\lambda > 0$, то $\vec{b},\ \vec{a}$ одинаково направлены;
если $\lambda < 0$, то $\vec{b},\ \vec{a}$ противоположно направлены.

Заметим, что (*ii*) содержит важное свойство длины: $|\lambda\vec{a}| = |\lambda||\vec{a}|$ по определению.

Упражнение 1. Пусть $\vec{a} \neq \vec{0}$. *Дать интерпретацию векторам*

$$\frac{1}{|\vec{a}|}\vec{a}, \quad -\frac{1}{|\vec{a}|}\vec{a}.$$

Упражнение 2. Доказать, что векторы $\vec{a}, \vec{b}$ *коллинеарны тогда и только тогда, когда они связаны скалярным множителем (то есть либо* $\vec{b} = \lambda\vec{a}$ *, либо* $\vec{a} = \lambda\vec{b}$ *).*

Определённые таким образом операции обладают теми же свойствами, что и действия с n-мерными векторами или $m \times n$-матрицами, см. раздел 2. Проверка этих свойств предоставляется читателю.

1°. $\vec{a} + \vec{b} = \vec{b} + \vec{a}$,

2°. $(\vec{a} + \vec{b}) + \vec{c} = \vec{a} + (\vec{b} + \vec{c})$,

3°. $\vec{a} + \vec{0} = \vec{a}$,

4°. $\exists\ (-\vec{a})\ :\ \vec{a} + (-\vec{a}) = \vec{0}$,

5°. $1 \cdot \vec{a} = \vec{a}$,

6°. $\alpha(\beta\vec{a}) = (\alpha\beta)\vec{a}$,

7°. $\alpha(\vec{a} + \vec{b}) = \alpha\vec{a} + \alpha\vec{b}$,

8°. $(\alpha + \beta)\vec{a} = \alpha\vec{a} + \beta\vec{a}$.

Отметим теперь, что по своему определению основные операции над векторами не выводят за пределы данной прямой или данной плоскости (например, при сложении двух векторов фиксированной плоскости получается вектор, лежащий в той же плоскости, и т.д.); свойства 1° – 8° выполнены во всех ситуациях.

Определение. *Совокупность всех векторов фиксированной прямой, фиксированной плоскости или всего пространства, рассматриваемая вместе с операциями сложения и умножения на число, называется пространством геометрических векторов и обозначается через* V_1, V_2, V_3 *соответственно.*

Выполнение свойств $1^\circ - 8^\circ$ означает, что каждое из множеств $\mathrm{V_n}$, $n = 1, 2, 3$, *является линейным пространством.*

Итак, наряду с линейными пространствами n-мерных векторов $\mathrm{R^n}$ и $m \times n$-матриц $M_{m,n}$, см. раздел 2, мы ввели в рассмотрение линейные пространства геометрических векторов $\mathrm{V_n}$ (здесь в отличие от предыдущих ситуаций $n = 1, 2, 3$; ограничение на n связано с нашим физическим восприятием).

Вычитание геометрических векторов определяется обычным образом через сложение. Укажите свойства этой операции.

3.2. Линейная зависимость векторов из $\mathrm{V_n}$, $n = 1, 2, 3,$ и $\mathrm{R^n}$, $n \in \mathrm{N}$. Свойства линейно зависимых и линейно независимых систем

В этом пункте даётся определение важнейшего понятия — линейной зависимости конечной системы векторов. Так как наш подход является алгебраическим (он базируется на операциях сложения и умножения на число), то он охватывает каждое из пространств $\mathrm{V_n}$, $\mathrm{R^n}$, $M_{m,n}$. Все определения, свойства и доказательства свойств этого пункта подходят для всех ситуаций; имеется лишь формальная разница в их записи. Мы будем использовать обозначения, связанные с пространством геометрических векторов $\mathrm{V_n}$, n фиксировано, $n = 1, 2, 3$.

Линейной комбинацией векторов $\vec{a}_1, \ldots, \vec{a}_k$ *с коэффициентами* $\lambda_1, \ldots, \lambda_k \in \mathrm{R}$ называется вектор $\lambda_1\vec{a}_1 + \ldots + \lambda_k\vec{a}_k$.

Линейная комбинация называется *тривиальной*, если все её коэффициенты равны нулю, и *нетривиальной*, если хотя бы один из коэффициентов $\lambda_i \neq 0$. Соответствующие наборы коэффициентов этих линейных комбинаций также называются тривиальным и нетривиальным. Ясно, что тривиальная линейная комбинация любых векторов есть $\vec{0}$.

Определение. *Система векторов* $\vec{a}_1, \ldots, \vec{a}_k$ *называется линейно зависимой, если некоторая нетривиальная линейная комбинация векторов этой системы равна* $\vec{0}$. *Система называется линейно независимой, если она не является линейно зависимой.*

Таким образом, вопрос о линейной зависимости системы векторов $\vec{a}_1, \ldots, \vec{a}_k$ сводится к рассмотрению соотношения

$$\sum_{i=1}^{k} \lambda_i \vec{a}_i = \vec{0}. \tag{1}$$

Если (1) выполнено для некоторых чисел λ_i , среди которых есть хотя бы одно, отличное от 0, то система векторов является линейно зависимой. Если же равенство (1) выполняется лишь в случае $\lambda_1 = \ldots = \lambda_k = 0$ (то есть слева в (1) может стоять лишь тривиальная линейная комбинация), то эта система векторов является линейно независимой.

Нетрудно понять, что линейно независимые системы и только они обладают свойством: любая нетривиальная линейная комбинация векторов отлична от $\vec{0}$. Приведём ряд других важных свойств линейной зависимости.

Свойства линейной зависимости

1°. Система из одного вектора $\vec{a}$ линейно зависима $\iff$ $\vec{a} = \vec{0}$.

2°. Система, содержащая $\vec{0}$, линейно зависима.

3°.(*Обобщение.*) Если некоторая подсистема линейно зависима, то и вся система линейно зависима.

4°.(*Характеризация.*) Пусть $k > 1$. Система $\vec{a}_1, \ldots, \vec{a}_k$ линейно зависима $\iff$ один из векторов есть линейная комбинация других.

5°. Пусть система $\vec{a}_1, \ldots, \vec{a}_k$ — линейно независима, система $\vec{a}_1, \ldots, \vec{a}_k, \vec{b}$ — линейно зависима. Тогда $\vec{b}$ есть линейная комбинация $\vec{a}_1, \ldots, \vec{a}_k$.

6°. Пусть $\vec{b}$ есть линейная комбинация $\vec{a}_1, \ldots, \vec{a}_k$:

$$\vec{b} = \sum_{i=1}^{k} \alpha_i \vec{a}_i. \tag{2}$$

Представление (2) является единственным $\iff$ система $\vec{a}_1, \ldots, \vec{a}_k$ линейно независима. *Эквивалентная формулировка*: представление (2) не является единственным $\iff$ система $\vec{a}_1, \ldots, \vec{a}_k$ линейно зависима.

Два разложения вида (2) считаются одинаковыми, если все соответствующие коэффициенты правых частей этих соотношений равны.

Доказательство.

1°. $\Longleftarrow$. Следует из равенства $1 \cdot \vec{0} = \vec{0}$.

$\Longrightarrow$. Если $\lambda \vec{a} = \vec{0}$, $\lambda \neq 0$, то $\vec{a} = \vec{0}$.

2°. Для любых $\vec{a}_i$ выполнено равенство

$$1 \cdot \vec{0} + 0 \cdot \vec{a}_1 + \ldots + 0 \cdot \vec{a}_k = \vec{0}.$$

3°. Пусть подсистема $(\vec{a}_i)$ системы $\vec{a}_1, \ldots, \vec{a}_k, \vec{b}_1, \ldots, \vec{b}_l$ линейно зависима. Это означает, что для некоторого нетривиального набора коэффициентов λ_i выполнено равенство (1). Взяв все $\mu_j := 0$, очевидно, получим:

$$\sum_{i=1}^{k} \lambda_i \vec{a}_i + \sum_{j=1}^{l} \mu_j \vec{b}_j = \vec{0}.$$

Последнее равенство гарантирует линейную зависимость всей системы, так как среди коэффициентов левой части имеется хотя бы один ненулевой.

4°. $\Longrightarrow$. Если выполнено (1), причём $\lambda_i \neq 0$ для некоторого i, то $\vec{a}_i$ линейно выражается через остальные векторы системы (каким образом?).

$\Longleftarrow$. Если для некоторого i

$$\vec{a}_i = \sum_{j \neq i} \gamma_j \vec{a}_j,$$

то, очевидно,

$$1 \cdot \vec{a}_i + \sum_{j \neq i} (-\gamma_j) \vec{a}_j = \vec{0}.$$

В левой части стоит нетривиальная линейная комбинация.

5°. Для некоторого набора чисел $\alpha_1, \ldots, \alpha_k, \beta$, среди которых имеется хотя бы одно ненулевое, выполнено равенство

$$\sum_{i=1}^{k} \alpha_i \vec{a}_i + \beta \vec{b} = \vec{0}.$$

Простой анализ показывает, что $\beta \neq 0$ — иначе система $\vec{a}_1, \ldots, \vec{a}_k$ линейно зависима. Поэтому $\vec{b}$ линейно выражается через $\vec{a}_i$.

6°. Докажем это свойство в приведённой выше эквивалентной формулировке.

$\Longrightarrow$. Пусть представление (2) не является единственным: для другого набора коэффициентов выполнено ещё равенство

$$\vec{b} = \sum_{i=1}^{k} \beta_i \vec{a}_i.$$

Вычитая из (2) последнее представление, получим

$$\sum_{i=1}^{k} (\alpha_i - \beta_i) \vec{a}_i = \vec{0}.$$

Среди коэффициентов левой части есть хотя бы один ненулевой. Поэтому система $\vec{a}_1, \ldots, \vec{a}_k$ линейно зависима.

$\Longleftarrow$. Пусть система $\vec{a}_1, \ldots, \vec{a}_k$ линейно зависима, тогда с нетривиальным набором коэффициентов $\lambda_1, \ldots, \lambda_k$ выполнено равенство (1). Прибавим его к равенству (2) и запишем результат в виде

$$\vec{b} = \sum_{i=1}^{k} (\alpha_i + \lambda_i) \vec{a}_i.$$

Нетрудно понять, что мы получили новое представление для $\vec{b}$ — хотя бы при одном значении i выполнено $\alpha_i + \lambda_i \neq \alpha_i$, поэтому последнее соотношение отличается от (2).

Свойства доказаны.

3.3. Связь линейной зависимости в $\mathrm{V_n}$ с коллинеарностью и компланарностью

Дадим в этом пункте простую геометрическую интерпретацию линейной зависимости и независимости в пространствах геометрических векторов. Как вы помните, основное определение является алгебраическим.

Теорема. *(0) Один вектор образует линейно зависимую систему $\Longleftrightarrow$ этот вектор является нулевым.*

(1) Два вектора линейно зависимы $\Longleftrightarrow$ они коллинеарны.

(2) Три вектора линейно зависимы $\Longleftrightarrow$ они компланарны.

(3) Любые два вектора из $\mathrm{V_1}$, три вектора из $\mathrm{V_2}$, четыре вектора из $\mathrm{V_3}$ (и большее число векторов во всех ситуациях) линейно зависимы.

Доказательство вполне элементарно; логическая схема использует свойства линейной зависимости предыдущего пункта. Часть (0) совпадает со свойством 1° и приводится для полноты.

(1) Два вектора линейно зависимы $\iff$ они связаны скалярным множителем (характеризация из свойства 4°) $\iff$ они коллинеарны.

(2) $\Longrightarrow$. Если три вектора линейно зависимы, то один из них есть линейная комбинация двух других (свойство 4°) и, значит, лежит в плоскости этих двух векторов (геометрия операций).

$\Longleftarrow$. Пусть $\vec{a}, \vec{b}, \vec{c}$ компланарны. Если $\vec{a}, \vec{b}$ коллинеарны, то они линейно зависимы по предыдущему; тогда и вся система линейно зависима (свойство 3°). Если же $\vec{a}, \vec{b}$ неколлинеарны, то $\vec{c}$ нетрудно представить в виде $\vec{c} = \alpha\vec{a} + \beta\vec{b}$ (выполните соответствующее геометрическое построение.)

(3) Замечание в скобках связано со свойством 3°. Далее, два вектора из V_1 коллинеарны, три вектора из V_2 компланарны и, значит, линейно зависимы по предыдущему.

Пусть $\vec{a}, \vec{b}, \vec{c}, \vec{d} \in \mathrm{V}_3$. Если $\vec{a}, \vec{b}, \vec{c}$ компланарны, то они линейно зависимы (часть (2)); тогда и вся система из четырёх векторов линейно зависима (свойство 3°). Если же $\vec{a}, \vec{b}, \vec{c}$ некомпланарны, то $\vec{d}$ нетрудно представить в виде $\vec{d} = \alpha\vec{a} + \beta\vec{b} + \gamma\vec{c}$ (выполните соответствующее геометрическое построение.)

Теорема доказана.

Изложенная геометрическая интерпретация линейной зависимости в $\mathrm{V_n}$ даёт возможность не выходить здесь за рамки понятий коллинеарности и компланарности. Преимущество исходного алгебраического определения линейной зависимости состоит в *степени общности* — этот подход без изменений переносится в дальнейшем на произвольные линейные пространства.

3.4. Решение задачи о линейной зависимости векторов из $\mathrm{R^n}$, $n \in \mathrm{N}$. Линейная зависимость k произвольных n-мерных векторов при $k > n$

Пусть $a^{(1)}, \ldots, a^{(k)}, b$ — некоторые n-мерные векторы; их компоненты в этом пункте из технических соображений удобнее записать по столбцам:

$$a^{(1)} = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix}, \ldots, \; a^{(k)} = \begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{nk} \end{pmatrix}, \; b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

Вопрос о представлении вектора b в виде линейной комбинации векторов $a^{(1)}, \ldots, a^{(k)}$ (или, как говорят, о *разложении* одного вектора по системе других) есть вопрос о справедливости и коэффициентах равенства

$$\lambda_1 a^{(1)} + \ldots + \lambda_k a^{(k)} = b,$$

или в компонентах

$$\lambda_1 \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix} + \ldots + \lambda_k \begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{nk} \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{pmatrix} .$$

Таким образом, вопрос сводится к анализу системы n линейных уравнений с k неизвестными $\lambda_1, \ldots, \lambda_k$. Расширенная матрица этой системы имеет вид

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \ldots & a_{1k} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2k} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nk} & b_n \end{array} \right)$$

Заметим, что система уравнений может быть и несовместной — в этой ситуации b нельзя представить в виде линейной комбинации $a^{(i)}$.

Обратимся теперь к анализу линейной зависимости системы из k данных n-мерных векторов $a^{(1)}, \ldots, a^{(k)}$. Ясно, что в предыдущих рассмотрениях надо взять $b = 0$. В этом случае система уравнений с неизвестными λ_i будет однородной и, следовательно, всегда совместной. Если эта однородная система уравнений является определённой, то есть обладает только нулевым решением

$$\lambda_1 = \ldots = \lambda_k = 0 \ ,$$

то исходная система векторов $a_1, \ldots, a_k$ является линейно независимой. Если же система однородных уравнений с матрицей (a_{ij}), $i = 1, \ldots, n$, $j = 1, \ldots, k$, является неопределённой, то исходная система n-мерных векторов является линейно зависимой. Эти простые рассуждения приводят к следующему важному результату.

Теорема. *Пусть $k > n$. Система, состоящая из k произвольных n-мерных векторов, является линейно зависимой.*

Доказательство состоит из одной фразы: однородная система n линейных уравнений с k неизвестными является неопределённой.

Очевидно, что в каждом из пространств $\mathrm{R^n}$ существуют линейно независимые системы, состоящие ровно из n векторов; подумайте над простейшим примером.

Упражнение 1. Сформулировать аналог теоремы для пространства матриц $M_{m,n}$. Какая система из mn матриц является линейно независимой?

Упражнение 2. Доказать, что для любой квадратной матрицы $\mathbf{A}$ порядка n существует ненулевой аннулирующий многочлен. (Указание. Воспользоваться линейной зависимостью в M_n матриц $\mathbf{E}$, $\mathbf{A}$, $\mathbf{A}^2$, $\ldots$, $\mathbf{A}^{n^2}$.)

3.5. Базис и координаты в $\mathrm{V_n}$. Характеризация базисов в $\mathrm{V_1}$, $\mathrm{V_2}$, $\mathrm{V_3}$. Размерность. Изоморфизм $\mathrm{V_n}$ и $\mathrm{R^n}$, $n = 1, 2, 3$

Наличие базиса — важнейшее характеристическое свойство нетривиальных *конечномерных линейных пространств*, простейшими примерами которых являются рассматриваемые в этой части пространства геометрических векторов, n-мерных векторов и матриц.

Естественно, в определении базиса в пространствах $\mathrm{V_n}$ можно обойтись простыми геометрическими понятиями и действовать в стиле характеризации приводимой ниже теоремы. Однако, опять исходя из соображений *общности*, мы предпочитаем алгебраический подход.

Поэтому определение базиса и координат без изменений переносится на пространства $\mathrm{R^n}$ и $M_{m,n}$.

Определение. *Базисом* $\mathrm{V_n}$ *называется конечная совокупность векторов, которая обладает свойствами:*

1) эта система линейно независима;

2) каждый вектор $\mathrm{V_n}$ *есть линейная комбинация векторов этой системы.*

Коэффициенты разложения вектора $\vec{x}$ по базисным векторам называются *координатами* $\vec{x}$ в этом базисе.

Теорема. (*Характеризация.*) *(1) Всякий базис* $\mathrm{V_1}$ *состоит из одного ненулевого вектора. При этом любой ненулевой вектор из* $\mathrm{V_1}$ *образует базис.*

(2) Всякий базис $\mathrm{V_2}$ *состоит из двух неколлинеарных векторов. При этом любая пара неколлинеарных векторов из* $\mathrm{V_2}$ *образует базис.*

(3) Всякий базис $\mathrm{V_3}$ *состоит из трёх некомпланарных векторов. При этом любая тройка некомпланарных векторов* $\mathrm{V_3}$ *образует базис.*

Доказательство. Остановимся для примера на части (2); части (1), (3) рассмотрите самостоятельно.

Пусть сначала имеется некоторый базис $\mathrm{V_2}$. Так как система из трёх (и большего числа) векторов $\mathrm{V_2}$ линейна зависима, то базис может содержать один ненулевой или пару неколлинеарных векторов. Первый вариант отпадает — векторы, неколлинеарные данному, через него линейно не выражаются.

Пусть теперь $\vec{a}, \vec{b}$ — любая фиксированная пара неколлинеарных векторов $\mathrm{V_2}$. Ясно, что эти векторы линейно независимы. Если $\vec{x} \in \mathrm{V_2}$ — произвольный вектор, то простое геометрическое построение означает, что

$$\vec{x} = \alpha\vec{a} + \beta\vec{b}.$$

Поэтому $\vec{a}, \vec{b}$ — базис $\mathrm{V_2}$.

Следствие. *Каждый базис* $\mathrm{V_n}$ *состоит из* n *векторов.*

Число n — количество элементов базиса $\mathrm{V_n}$ — называется *размерностью* $\mathrm{V_n}$ и обозначается $\dim \mathrm{V_n}$. Таким образом, результат следствия означает, что $\dim \mathrm{V_n} = n$.

Упражнение 1. Приведите примеры базисов в пространствах $\mathrm{R^n}$ *и* $M_{m,n}$.

Пусть $\vec{x} \in \mathrm{V_n}$, $\vec{e}_1, \ldots, \vec{e}_n$ — некоторый фиксированный базис $\mathrm{V_n}$. Здесь n — любое из чисел 1, 2, 3. Будем использовать запись

$$\vec{x} = \alpha_1\vec{e}_1 + \ldots + \alpha_n\vec{e}_n = \{\alpha_1, \ldots, \alpha_n\}.$$

Числа $\alpha_1, \ldots, \alpha_n$ — координаты $\vec{x}$ в данном базисе — определены единственным образом, см. свойство 6° линейной зависимости из пункта 3.2. Кроме того, если

$\lambda \in \mathrm{R}$, $\vec{y} = \{\beta_1, \ldots, \beta_n\}$, то, как нетрудно понять,

$$\vec{x} + \vec{y} = \{\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n\},$$

$$\lambda\vec{x} = \{\lambda\alpha_1, \ldots, \lambda\alpha_n\}.$$

Эти равенства соответствуют *действиям с векторами в координатах.*

Рассмотрим теперь соответствие между геометрическими векторами $\vec{x}$ из $\mathrm{V_n}$ и n-мерными векторами x из $\mathrm{R^n}$, осуществляемое по простому правилу:

$$\vec{x} \longleftrightarrow x = (\alpha_1, \ldots, \alpha_n), \qquad \text{если } \vec{x} = \{\alpha_1, \ldots, \alpha_n\}.$$

Иначе говоря, вектору $\vec{x}$ сопоставляется набор его координат, обозначаемый через x. Сказанное выше означает, что это соответствие взаимно-однозначно и сохраняет операции сложения и умножения на число. Последнее есть вольная интерпретация следующей записи:

$$\begin{array}{ll} \text{если} & \vec{x} \longleftrightarrow x\ , \quad \vec{y} \longleftrightarrow y, \qquad \lambda \in \mathrm{R}\ , \\ \text{то} & \vec{x} + \vec{y} \longleftrightarrow x + y\ , \quad \lambda\vec{x} \longleftrightarrow \lambda x. \end{array}$$

Соответствие $\longleftrightarrow$ является примером *изоморфизма.* Говорят также, что пространства $\mathrm{V_n}$ и $\mathrm{R^n}$ *изоморфны* и записывают это, например, так:

$$\mathrm{V_n} \simeq \mathrm{R^n}\ , \quad n = 1, 2, 3.$$

Итак, изоморфизм — это взаимно-однозначное соответствие между элементами двух линейных пространств, сохраняющее основные операции.

Переход от одного объекта к другому, изоморфному первому, позволяет решать задачи, поставленные для первого объекта, с помощью техники, разработанной для второго объекта. (В широком смысле, два объекта изоморфны, если они имеют одинаковую структуру или форму — почти буквальный перевод с греческого термина *изоморфизм.*)

В нашей ситуации это позволяет решать геометрические задачи в числах. Как пример, отметим анализ линейной зависимости геометрических векторов в координатах.

Упражнение 2. Показать, что при изоморфизме линейно независимой системе в $\mathrm{V_n}$ *соответствует линейно независимая система в* $\mathrm{R^n}$*, и наоборот.*

В настоящем тексте мы не вводим общего понятия изоморфизма линейных пространств; однако некоторые простые ситуации могут быть рассмотрены по аналогии.

Упражнение 3. При каком натуральном k *имеет место изоморфизм* $M_{m,n} \simeq \mathrm{R^k}$? *Как осуществить в этой ситуации взаимно-однозначное соответствие, сохраняющее операции сложения и умножения на число? Какова роль базисов пространств при установлении изоморфизма?*

4. Определители

У истоков истории понятия определителя стоят великий немецкий математик Готфрид Вильгельм Лейбниц (G.W. Leibniz) и японский математик Сёки Кова — ими независимо предложена идея определителя (в 1678 г. и 1683 г. соответственно).

Первые публикации принадлежат Крамеру (G. Cramer, 1750) и Лагранжу (J.L. Lagrange, 1770). Термин *детерминант (определитель)* введён Гауссом (C. Gauss, 1801); современное обозначение принадлежит Кэли (A. Cayley, 1841).

Теория определителей создана в конце 18 – первой половине 19 столетий трудами Вандермонда (A.T. Vandermonde), Лапласа (P.S. Laplace), Коши (A.L. Cauchy) и Якоби (C.G. Jacobi).

Самой важной из работ в этой области является статья Карла Густава Якоби *"De formatione et proprietatibus determinantium"*

("О построении и свойствах определителей 1841), которая сделала теорию определителей общим достоянием математиков. Чтобы воздать должное достижениям Якоби в алгебре, Сильвестр назвал *якобианом* важный функциональный определитель.

Из многочисленных приложений определителей отметим *решение систем линейных уравнений и вычисление объёмов*. В различных разделах математики рассматриваются, разумеется, и другие связанные с ними задачи.

В литературе отражены следующие подходы к построению определителей.

1°. Индукция по порядку n определителя (разложение по строке или столбцу).

2°. Введение определителя как функции строк матрицы с некоторыми заданными свойствами. В пункте 4.2 эта функция обозначается как $F(X_1, \ldots, X_n)$.

3°. Определитель как обобщённый ориентированный объём.

4°. Прямое определение через перестановки. При таком подходе содержание пунктов 1° – 3° имеет вид следствий или свойств.

В настоящем тексте используется последний подход. Он реализован, например, в учебниках А.И. Кострикина [13] и А.Г. Куроша [16].

4.1. Перестановки и инверсии. Свойства перестановок. Определитель порядка n

Перестановкой чисел $1, 2, \ldots, n$ называется их некоторое расположение в строку. Иначе говоря, перестановка порядка n есть упорядоченный набор $\alpha := (\alpha_1, \ldots, \alpha_n)$ такой, что все компоненты α_j попарно различны и принадлежат множеству $W_n := \{1, \ldots, n\}$.

С перестановкой α естественным образом связывают понятие *подстановки порядка* n, то есть взаимно-однозначного отображения множества W_n на себя. Подстановка, обозначаемая тем же символом α, изображается в виде двустрочной таблицы

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}.$$

Имеется в виду, что $j \mapsto \alpha_j$ или $\alpha_j := \alpha(j)$ (как и всегда для функций натурального аргумента).

На множестве всех подстановок порядка n можно рассмотреть *операцию суперпозиции* $\circ$, определяемую, как обычно, равенством

$$\alpha \circ \beta(j) := \alpha(\beta(j)),\ j = 1, \ldots, n.$$

Пример 1. Если $n = 4$ и

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

то

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \neq \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

Упражнение 1. Проверить, что операция суперпозиции ассоциативна и для любой подстановки α существует обратная подстановка α^*, то есть такая, что $\alpha \circ \alpha^* = \alpha^* \circ \alpha = e$. Здесь e — тождественная подстановка; для неё $e(j) = j$, в связи с чем $\alpha \circ e = e \circ \alpha = \alpha$ для любой α. Выполнение этих свойств означает, что относительно операции $\circ$ совокупность S_n всех подстановок порядка n образует группу (некоммутативную при $n > 2$), называемую группой подстановок. См. также пункт 12.1.

В дальнейшем $\alpha = (\alpha_1, \ldots, \alpha_n)$ считается перестановкой. Нам потребуется несколько простых определений.

Пусть $i < k$. Будем говорить, что компоненты перестановки α_i и α_k образуют *инверсию*, если $\alpha_i > \alpha_k$, и образуют *порядок*, если $\alpha_i < \alpha_k$. Число всех инверсий в перестановке α обозначим $s(\alpha)$. В зависимости от чётности $s(\alpha)$ перестановка α называется *чётной* или *нечётной*.

Транспозицией называется такая операция с перестановкой, при которой меняются местами некоторые две её компоненты, а остальные остаются на своих местах.

Наиболее сложным выглядит понятие обратной перестановки α^*. Пусть α — некоторая перестановка. Построим новую перестановку β по правилу: для всех значений $j = 1, \ldots, n$ β_j есть номер числа j как компоненты перестановки α. Иначе говоря, $\alpha_{\beta_j} = j$ при всех j. Так как при таком подходе β_{α_j} есть номер числа α_j в перестановке α, то есть j, то одновременно $\beta_{\alpha_j} = j$. Таким образом, выполнены равенства

$$\alpha_{\beta_j} = \beta_{\alpha_j} = j,\ j = 1, \ldots, n. \tag{1}$$

Пример 2. Пусть $\alpha = (2, 3, 4, 1)$. Тогда $\beta = (4, 1, 2, 3)$.

Построенная таким образом перестановка β называется *обратной к перестановке* α и обозначается α^*.

Замечание. Ситуация заметно проясняется, если в этом месте привлечь к рассмотрению подстановки. На языке отображений равенства (1) означают, что $\alpha \circ \beta = \beta \circ \alpha = e$, то есть α^* есть обратная к α подстановка, см. упражнение 1.

1°. Количество всех перестановок порядка n равно $n!$.

2°. Любая транспозиция меняет чётность перестановки.

3°. Число чётных перестановок порядка $n > 1$ совпадает с числом нечётных и равно $n!/2$.

4°. Если $\beta = \alpha^*$, то $\beta^* = \alpha$. Иначе говоря, $(\alpha^*)^* = \alpha$.

5°. $s(\alpha^*) = s(\alpha)$.

Доказательство. 1° легко устанавливается индукцией по n.

Утверждение свойства 2° очевидно для транспозиции соседних компонент. Общий результат следует из того, что произвольная транспозиция может быть получена в результате выполнения нечётного числа транспозиций соседних членов. Если между теми компонентами, которые требуется поменять местами, имеется k членов, нетрудно найти нужную цепочку из $2k + 1$ транспозиций соседних компонент.

Приведём элегантное доказательство свойства 3°. На множестве всех чётных перестановок порядка n рассмотрим операцию транспозиции первых двух компонент. При выполнении этой операции каждая чётная перестановка переходит в нечётную; различные перестановки переходят в различные. Поэтому общее число M чётных перестановок и общее число N нечётных перестановок связаны неравенством $M \leqslant N$. Аналогичное рассуждение даёт $N \leqslant M$. Поэтому $M = N = n!/2$.

Для доказательства 4° положим $\beta = \alpha^*$ и $\gamma = \beta^*$. Тогда в соответствии с равенствами (1) будет выполнено

$$\alpha_{\beta_j} = j = \gamma_{\beta_j},\ j = 1, \ldots, n\ ,$$

в связи с чем $\alpha = \gamma$.

Наконец, установим интересное свойство 5°. Пусть компоненты α_i, α_k образуют инверсию в перестановке α. Это означает, что одновременно $i < k$ и $\alpha_i > \alpha_k$. Заметим, что тогда числа i и k составляют инверсию в обратной перестановке α^*, поскольку в α^* они стоят на местах α_i и α_k соответственно. Таким образом, каждой инверсии в перестановке α соответствует некоторая инверсия в перестановке α^*. Поэтому $s(\alpha) \leqslant s(\alpha^*)$. В силу двойственности свойства 4° выполняется и противоположное неравенство. Поэтому $s(\alpha^*) = s(\alpha)$.

Свойства доказаны.

Перейдём теперь к центральному определению этого пункта. Пусть $\mathbf{A} = (a_{ij})$ — квадратная матрица порядка n, то есть $\mathbf{A} \in M_n$.

Определение. *Число*

$$|\mathbf{A}| = \det(\mathbf{A}) := \sum_{\alpha} (-1)^{s(\alpha)} a_{1\alpha_1} a_{2\alpha_2} \ldots a_{n\alpha_n} \tag{2}$$

называется определителем матрицы $\mathbf{A}$*. Суммирование в (2) осуществляется по множеству всех перестановок порядка* n*.*

Анализ формулы (2) показывает, что $|\mathbf{A}|$ есть алгебраическая сумма произведений n элементов матрицы, в каждом из которых присутствует ровно один элемент

из каждой строки и ровно один элемент из каждого столбца. Всего таких произведений $a_{1\alpha_1}\dots a_{n\alpha_n}$ — так называемых *членов определителя* — набирается ровно $n!$; каждое произведение соответствует некоторой перестановке α порядка n. В зависимости от чётности соответствующей перестановки член определителя снабжается знаком плюс или минус. Например, произведение элементов главной диагонали матрицы входит в определитель со знаком плюс, так как соответствующая перестановка $\alpha = (1, 2, \dots, n)$ является чётной (для неё $s(\alpha) = 0$).

Упражнение 2. Убедиться, что при $n = 1, 2, 3$ формула (2) содержит привычные выражения для определителей соответствующего порядка. Составить графическое правило для вычисления определителя четвёртого порядка.

Упражнение 3. Дополнить произведение элементов $a_{13}a_{24}a_{35}a_{46}a_{57}$ определителя седьмого порядка так, чтобы получить член этого определителя, входящий в него со знаком минус.

4.2. Свойства определителя. Вычисление методом Гаусса

Ряд из приводимых в этом пункте свойств характеризует определитель *как функцию строк матрицы.*

Пусть $X_1, \dots, X_n \in \mathrm{R^n}$ — строки матрицы $\mathbf{A} = (a_{ij}) \in M_n$. Определим функцию F равенством

$$F(X_1, \dots, X_n) := |\mathbf{A}|.$$

Таким образом,

$$F : \underbrace{\mathrm{R^n} \times \dots \times \mathrm{R^n}}_{n} \to \mathrm{R}.$$

Содержание этого пункта, в частности, означает, что F — *линейная по каждому аргументу и кососимметричная функция* (свойства 1 – 2 и 6 соответственно).

Свойство 1. *Пусть* $a_{kj} = b_{kj} + c_{kj},\ j = 1, \dots, n$. *Тогда*

$$|\mathbf{A}| = \ {}_{(k)}\begin{vmatrix} \dots & \dots & \dots \\ b_{k1} & \dots & b_{kn} \\ \dots & \dots & \dots \end{vmatrix} \ + \ {}_{(k)}\begin{vmatrix} \dots & \dots & \dots \\ c_{k1} & \dots & c_{kn} \\ \dots & \dots & \dots \end{vmatrix} \tag{3}$$

(выделены k-е строки определителей; остальные — такие же, как в $\mathbf{A}$).

Аналогичный результат справедлив, когда одна из строк определителя представляется в виде суммы m строк.

Свойство 1 означает, что функция F *аддитивна* по каждому аргументу. Например, для $k = 1$ и произвольного $m \in \mathrm{N}$ имеем:

$$F(\sum_{i=1}^{m} Y_i, X_2, \dots, X_n) = \sum_{i=1}^{m} F(Y_i, X_2, \dots, X_n).$$

Доказательство. Равенство (3) имеет вид

$$|\mathbf{A}| = \sum_{\alpha} (-1)^{s(\alpha)} a_{1\alpha_1} \dots (b_{k\alpha_k} + c_{k\alpha_k}) \dots a_{n\alpha_n} =$$

$$= \sum_{\alpha} (-1)^{s(\alpha)} a_{1\alpha_1} \dots b_{k\alpha_k} \dots a_{n\alpha_n} + \sum_{\alpha} (-1)^{s(\alpha)} a_{1\alpha_1} \dots c_{k\alpha_k} \dots a_{n\alpha_n}.$$

Общий случай получается индукцией по m.

Свойство 2. *При умножении некоторой одной строки на число с определитель умножается на это число.*

Это означает, что F — функция, *однородная* по каждому аргументу. Например, $F(cX_1, X_2, \dots, X_n) = cF(X_1, X_2, \dots, X_n)$.

Доказательство содержится в равенстве

$$\sum_{\alpha} (-1)^{s(\alpha)} a_{1\alpha_1} \dots (ca_{k\alpha_k}) \dots a_{n\alpha_n} = c \sum_{\alpha} (-1)^{s(\alpha)} a_{1\alpha_1} \dots a_{n\alpha_n}.$$

Свойство 3. *Определитель матрицы с нулевой строкой равен нулю.* Например, $F(0, X_2, \dots, X_n) = 0$; в левой части $0 = (0, \dots, 0)$.

Следует из определения или предыдущего свойства (при $c = 0$).

Свойство 4. *Определитель, содержащий две одинаковые строки, равен нулю.* Например, $F(X, X, X_3, \dots, X_n) = 0$.

Доказательство. Пусть $i < k$ и $a_{ij} = a_{kj}$ при всех $j = 1, \dots, n$.

Рассмотрим произвольную перестановку α и ту перестановку β, которая получается из α транспозицией i-й и k-й компонент. Сумма двух соответствующих членов определителя, взятых с нужными знаками, равна нулю. Действительно, $s(\beta)$ отличается от $s(\alpha)$ на 1. Поэтому

$$\begin{aligned} &(-1)^{s(\beta)} a_{1\beta_1} \dots a_{i\beta_i} \dots a_{k\beta_k} \dots a_{n\beta_n} = \\ &= -(-1)^{s(\alpha)} a_{1\alpha_1} \dots a_{i\alpha_k} \dots a_{k\alpha_i} \dots a_{n\alpha_n} = \\ &= -(-1)^{s(\alpha)} a_{1\alpha_1} \dots a_{k\alpha_k} \dots a_{i\alpha_i} \dots a_{n\alpha_n} = \\ &= -(-1)^{s(\alpha)} a_{1\alpha_1} \dots a_{i\alpha_i} \dots a_{k\alpha_k} \dots a_{n\alpha_n}. \end{aligned}$$

В связи с этим $|\mathbf{A}|$ есть сумма $N = n!/2$ слагаемых, равных 0.

Следствие 1. *Определитель, содержащий две пропорциональные строки, равен нулю.*

Следствие 2. *Определитель, у которого одна из строк есть линейная комбинация других, равен нулю.*

Для доказательства достаточно использовать свойства 1, 2 и 4. Следствие 2 (обобщающее следствие 1) означает, что, в частности,

$$F(\sum_{j=2}^{n} c_j X_j, X_2, \dots, X_n) = 0 \ , \ c_j \in \mathrm{R}.$$

Свойство 5. *Определитель не изменится, если к любой его строке прибавить произвольную линейную комбинацию других.*

Сразу следует из свойства 1 и следствия 2. Таким образом, например,

$$F(X_1 + \sum_{j=2}^{n} c_j X_j, X_2, \dots, X_n) = F(X_1, X_2, \dots, X_n) \ , c_j \in \mathrm{R}.$$

Свойство 6. *При перестановке двух строк определитель меняет знак.*

Таким образом, $F(X_1, \ldots, X_n)$ меняет знак при любой перестановке пары аргументов, например,

$$F(X, Y, X_3, \ldots, X_n) = -F(Y, X, X_3, \ldots, X_n). \tag{4}$$

Такие функции F называют *кососимметричными*.

Доказательство. Из свойств 1 и 4 получаем

$$0 = F(X+Y, X+Y, \ldots) = F(X, X+Y, \ldots) + F(Y, X+Y, \ldots) =$$

$$= F(X, X, \ldots) + F(X, Y, \ldots) + F(Y, X, \ldots) + F(Y, Y, \ldots) =$$

$$= F(X, Y, \ldots) + F(Y, X, \ldots),$$

что даёт равенство (4). Общий случай получается аналогично.

Свойство 7. *Определитель не меняется при транспонировании:*

$$|\mathbf{A}^T| = |\mathbf{A}|.$$

Поэтому все свойства, сформулированные выше для строк, справедливы и для столбцов.

Доказательство. Обозначим $\mathbf{A}^T = (a'_{ij})$. Тогда

$$|\mathbf{A}^T| = \sum_\alpha (-1)^{s(\alpha)} a'_{1\alpha_1} \ldots a'_{n\alpha_n} =$$

$$= \sum_\alpha (-1)^{s(\alpha)} a_{\alpha_1 1} \ldots a_{\alpha_n n} = \sum_\alpha (-1)^{s(\alpha)} a_{\alpha_1 \beta_{\alpha_1}} \ldots a_{\alpha_n \beta_{\alpha_n}}.$$

В последнем выражении $\beta := \alpha^*$ — перестановка, обратная к α. Мы использовали то, что для всех $j = 1, \ldots, n$ выполнено $j = \beta_{\alpha_j}$, см. равенство (1) предыдущего пункта.

Учтём теперь, что по свойствам перестановок $s(\alpha) = s(\beta)$. Упорядочение сомножителей по первому индексу и замена $\sum_\alpha$ на $\sum_\beta$ даёт с учётом предыдущего

$$|\mathbf{A}^T| = \sum_\beta (-1)^{s(\beta)} a_{1\beta_1} \ldots a_{n\beta_n} = |\mathbf{A}|.$$

Свойство 8. *Определитель треугольной матрицы равен произведению элементов главной диагонали.*

Под треугольной понимается матрица $\mathbf{A}$, удовлетворяющая условию $a_{ij} = 0$ при $i > j$ (*верхняя треугольная матрица*) или тому же условию при $i < j$ (*нижняя треугольная матрица*).

Доказательство. Ясно, что произведение $a_{11} \ldots a_{nn}$ входит в $|\mathbf{A}|$ со знаком плюс. Остаётся заметить, что все остальные члены определителя равны 0.

На использовании указанных свойств базируется *метод Гаусса вычисления определителей*. В основе этого метода лежит возможность приведения произвольной квадратной матрицы к (верхнему) треугольному виду с помощью цепочки элементарных преобразований трёх следующих типов:

(1) перестановка строк;

(2) умножение строки на ненулевое число;

(3) прибавление к данной строке линейной комбинации других строк (см. раздел 1, пункты 1.2, 1.3).

Если внимательно следить за тем, как меняется определитель в ходе этих преобразований, то ответ получается с учётом свойства 8.

В ходе вычислений можно активно применять и другие свойства (например, проводить преобразования со столбцами).

Замечание. Преобразования типа (2) используются только для удобства вычислений; алгоритм приведения матрицы к ступенчатому виду (прямой ход метода Гаусса) требует операций лишь первого и третьего типов (см. доказательство теоремы 2 пункта 1.3).

Упражнение. Сравнить трудоёмкости вычислений определителя порядка n по методу Гаусса и с прямым использованием формулы (2).

4.3. Приложение определителей к анализу и решению линейных систем. Правило Крамера

В этом пункте мы рассматриваем систему линейных уравнений с матрицей $\mathbf{A} = (a_{ij}) \in M_n$. В стандартных обозначениях (см. раздел 1) эта система имеет вид

$$\sum_{j=1}^{n} a_{ij}x_j = b_i \ , i = 1, \ldots, n \ , \tag{5}$$

или в матричной форме $\mathbf{Ax} = \mathbf{b}$.

Явные формулы для $x_1, \ldots, x_n,\ n \in \mathrm{N},$ из условия теоремы 2 составляют знаменитое *правило Крамера* — главное приложение определителей к решению линейных систем. Швейцарский математик Габриель Крамер (G. Cramer) получил их (с точностью до современных обозначений) в 1750 г.; при $n = 2, n = 3$ эти формулы получил несколько ранее Колин Маклорен (C. Maclaurin).

Прежде всего приведём важный критерий определённости системы (5) в терминах $|\mathbf{A}|$.

Теорема 1. *Система (5) является определённой тогда и только тогда, когда* $|\mathbf{A}| \neq 0$.

Доказательство. Обозначим через $\mathbf{A}'$ ступенчатую матрицу, получающуюся из $\mathbf{A}$ в результате прямого хода метода Гаусса. Так как на этом этапе используются преобразования над строками лишь первого и третьего типов (см. замечание в конце предыдущего пункта), то по свойствам определителя

$$|\mathbf{A}| = \pm\, |\mathbf{A}'|. \tag{6}$$

Пусть r — число ступеней матрицы $\mathbf{A}'$. Система (5) является определённой тогда и только тогда, когда $r = n$ (см. пункт 1.4), то есть $|\mathbf{A}'| \neq 0$ (свойство 8 определителя). Остаётся учесть (6).

Теорема доказана.

Следствие 1. *Однородная система (5) ($b_1 = \ldots = b_n = 0$) имеет ненулевое решение* $\iff |\mathbf{A}| = 0$.

Следствие 2. $|\mathbf{A}| = 0 \iff$ *строки (и столбцы)* $\mathbf{A}$ *образуют линейно зависимую систему в* $\mathrm{R^n}$*, то есть одна из строк (один из столбцов) есть линейная комбинация других.*

Отметим, что утверждение $\Longleftarrow$ нами установлено в предыдущем пункте (см. там следствие 2 и свойство 7).

Следствие 1 очевидно. Для доказательства следствия 2 достаточно переписать однородную систему (5) в виде

$$x_1 Y_1 + \ldots + x_n Y_n = 0,$$

где $Y_1, \ldots Y_n$ — столбцы матрицы $\mathbf{A}$, и воспользоваться следствием 1; так получается результат для столбцов. Утверждение для строк получается с учётом свойства 7 предыдущего пункта.

Замечание. Теорема 1 часто применяется в следующем виде: *определённость системы (5) с любыми* b_i *эквивалентна тому, что соответствующая однородная система имеет только нулевое решение.*

Проверка последнего условия может быть проще, чем явный подсчёт $|\mathbf{A}|$.

Теорема 2. *Пусть* $d := |\mathbf{A}| \neq 0$ *. Тогда единственное решение системы (5) имеет вид*

$$x_i = \frac{d_i}{d}\ , \quad i = 1, \ldots, n. \tag{7}$$

Здесь d_i *— определитель, получающийся из* d *заменой* i*-го столбца на столбец свободных членов.*

Доказательство. Пусть $x_1, \ldots, x_n$ — единственное (в силу теоремы 1) решение системы (5); i фиксировано. По свойствам определителей с учётом равенств (5) имеем:

$$d_i = \begin{vmatrix} \ldots & b_1 & \ldots \\ & \vdots & \\ \ldots & b_n & \ldots \end{vmatrix} = \begin{vmatrix} \ldots & \sum\limits_{j=1}^{n} a_{1j}x_j & \ldots \\ & \vdots & \\ \ldots & \sum\limits_{j=1}^{n} a_{nj}x_j & \ldots \end{vmatrix} =$$

$$= \sum_{j=1}^{n} \begin{vmatrix} \ldots & a_{1j}x_j & \ldots \\ & \vdots & \\ \ldots & a_{nj}x_j & \ldots \end{vmatrix}.$$

Выделены i-е столбцы; остальные столбцы — такие, как в d. Остаётся заметить, что

$$m_j := \begin{vmatrix} \ldots & a_{1j}x_j & \ldots \\ & \vdots & \\ \ldots & a_{nj}x_j & \ldots \end{vmatrix} = \begin{cases} x_i d & , \quad j = i \\ 0 & , \quad j \neq i \end{cases}$$

(при $j \neq i$ определитель m_j содержит пропорциональные столбцы). Поэтому

$$d_i = \sum_{j=1}^{n} m_j = x_i d,$$

откуда следует (7). Теорема доказана.

Могут ли определители использоваться при анализе ситуации $d = |\mathbf{A}| = 0$?

Если при этом некоторый (хотя бы один) вспомогательный определитель d_i отличен от нуля, то система (5) несовместна. В этом случае предположение существования решения $x_1, \ldots, x_n$ приводит по схеме доказательства теоремы 2 к невозможному равенству $d_i = x_i d$.

В ситуации же $d = d_1 = \ldots = d_n = 0$ система (5) может быть как несовместной, так и неопределённой! Более точно: существуют как несовместные, так и неопределённые системы с этим свойством. В этом случае анализ должен проводиться другими методами, например, методом Гаусса.

Упражнение. Привести примеры несовместной и неопределённой систем линейных уравнений с $n = 3$ *и* $d = d_1 = d_2 = d_3 = 0$.

Наконец, отметим, что решение системы (5) с помощью определителей (в случае $d \neq 0$) имеет на порядок большую трудоёмкость, чем метод Гаусса. Если все определители d, d_i считаются приведением к треугольному виду, то трудоёмкость метода Крамера составляет $O(n^4)$ операций (по сравнению с $O(n^3)$ для метода Гаусса).

Итак, применение определителей для решения систем линейных уравнений, о котором шла речь в этом пункте, имеет следующие недостатки:

(1) анализу подвергаются лишь системы с квадратной матрицей;

(2) в случае $d = d_1 = \ldots = d_n = 0$ анализ принципиально не является полным;

(3) трудоёмкость метода сравнительно высока.

Преимуществом метода Крамера является наличие явных формул для решения, которые не столь эффективно применяются в расчётах, но часто с успехом используются в теоретических вопросах. См. для примера упражнения пунктов 4.6, 4.8.

4.4. Миноры и алгебраические дополнения. Вычисление определителя с нулевым углом

В этом пункте вводятся важные понятия, используемые в дальнейшем.

Пусть $\mathbf{A} = (a_{ij}) \in M_{m,n}$. *Минором порядка* k этой матрицы называется определитель, образованный элементами, стоящими на пересечении выделенных k строк и k столбцов матрицы.

Таким образом, если $1 \leqslant k \leqslant \min(m, n)$, а номера выделенных строк $i_1, \ldots, i_k$ и столбцов $j_1, \ldots, j_k$ упорядочены по возрастанию:

$$1 \leqslant i_1 < \ldots < i_k \leqslant m, \quad 1 \leqslant j_1 < \ldots < j_k \leqslant n,$$

то соответствующий минор есть определитель порядка k

$$M = \begin{vmatrix} a_{i_1 j_1} & \ldots & a_{i_1 j_k} \\ \vdots & & \vdots \\ a_{i_k j_1} & \ldots & a_{i_k j_k} \end{vmatrix} .$$

Пусть теперь $\mathbf{A} \in M_n$ и минор M определён так, как выше. Определитель M' порядка $n - k$, стоящий на пересечении оставшихся строк и столбцов, называется

дополнительным к M, а число

$$A := (-1)^t M'$$

— *алгебраическим дополнением минора* M. Здесь t есть сумма номеров всех строк и столбцов, образующих минор M :

$$t := (i_1 + \ldots + i_k) + (j_1 + \ldots j_k).$$

В важном частном случае $k = 1$ минор M представляет собой выделенный элемент a_{ij} ; в этой ситуации дополнительный минор получается вычёркиванием из $|\mathbf{A}|$ i-й строки и j-го столбца. Получившийся определитель порядка $n-1$ обозначается M_{ij} и называется *минором, дополнительным к элементу* a_{ij}, а число

$$A_{ij} := (-1)^{i+j} M_{ij}$$

— *алгебраическим дополнением элемента* a_{ij}.

Пример. Пусть

$$\mathbf{A} = \begin{pmatrix} -1 & 2 & 3 & 4 \\ -1 & 0 & 5 & 6 \\ 7 & 8 & 5 & 3 \\ 1 & -1 & 0 & 2 \end{pmatrix}$$

Минор второго порядка, соответствующий строкам с номерами $i_1 = 1, i_2 = 4$ и столбцам с номерами $j_1 = 2, j_2 = 3,$ равен

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

В этом случае

$$M' = \begin{vmatrix} -1 & 6 \\ 7 & 3 \end{vmatrix} = -45 \ , \ A = (-1)^{2+3+1+4}(-45) = -45.$$

Для элемента $a_{32} = 8$ дополнительный минор и алгебраическое дополнение есть

$$M_{32} = \begin{vmatrix} -1 & 3 & 4 \\ -1 & 5 & 6 \\ 1 & 0 & 2 \end{vmatrix} = -6, \ A_{32} = (-1)^5 \begin{vmatrix} -1 & 3 & 4 \\ -1 & 5 & 6 \\ 1 & 0 & 2 \end{vmatrix} = (-1)^5(-6) = 6.$$

Приведём в этом пункте вспомогательный результат об определителе с нулевым углом.

Пусть матрица $\mathbf{A} = (a_{ij})$ порядка n имеет следующую блочную структру:

$$\mathbf{A} = \begin{pmatrix} \mathbf{B} & \mathbf{0} \\ \mathbf{D} & \mathbf{C} \end{pmatrix}.$$

Здесь $\mathbf{B} \in M_r$, $\mathbf{C} \in M_{n-r}$, $\mathbf{D} \in M_{n-r,r}$ — произвольные подматрицы; $\mathbf{0} \in M_{r,n-r}$ — состоит из одних нулей. Число r лежит в пределах $1 \leqslant r \leqslant n-1$.

Лемма. *Имеет место равенство*

$$|\mathbf{A}| = |\mathbf{B}||\mathbf{C}|. \tag{8}$$

Доказательство. В наших обозначениях

$$|\mathbf{B}| = \sum_{(\alpha_1,\ldots,\alpha_r)} (-1)^{s'} a_{1\alpha_1}\ldots a_{r\alpha_r},$$

$$|\mathbf{C}| = \sum_{(\alpha_{r+1},\ldots,\alpha_r)} (-1)^{s''} a_{r+1,\alpha_{r+1}}\ldots a_{n\alpha_n}.$$

Здесь $(\alpha_1,\ldots,\alpha_r)$ — перестановки чисел $1,\ldots,r$; $(\alpha_{r+1},\ldots,\alpha_n)$ — перестановки чисел $r+1,\ldots,n$; s' , s'' — соответствующие количества инверсий. Поэтому

$$|\mathbf{B}||\mathbf{C}| = \sum_{\alpha} (-1)^{s'+s''} a_{1\alpha_1}\ldots a_{n\alpha_n}. \tag{9}$$

Суммирование в правой части (9) осуществляется по тем перестановкам α чисел $1,\ldots,n$, в которых $(\alpha_1,\ldots,\alpha_r)$ есть некоторая перестановка чисел от 1 до r, а $(\alpha_{r+1},\ldots\alpha_n)$ — некоторая перестановка чисел от $r+1$ до n . Так как для каждой такой перестановки общее число инверсий $s(\alpha)$ равно сумме $s'+s''$, то (9) содержит некоторые члены $|\mathbf{A}|$, взятые с нужными знаками.

Остаётся заметить, что члены $|\mathbf{A}|$, не вошедшие в произведение $|\mathbf{B}||\mathbf{C}|$ (то есть в правую часть (9)), соответствуют тем перестановкам α, у которых среди первых r компонент встретится число $\geqslant r+1$. Каждый такой член содержит некоторый элемент $a_{ij},\ 1\leqslant i\leqslant r,\ j\geqslant r+1,$ и поэтому равен нулю.

Равенство (8) доказано.

4.5. Разложение определителя по строке (столбцу). Теорема Лапласа

Результаты этого пункта связаны с именем великого французского математика Пьера Симона Лапласа (P.S. Laplace, 1749 – 1827).

Мы установим правило разложения определителя по строке или столбцу, которое позволяет ввести определитель порядка n по индукции. Более общий результат — *теорема Лапласа* — приводится без доказательства (его можно найти, например, в учебнике А.Г. Куроша [16, с. 51]).

Пусть $\mathbf{A} = (a_{ij}) \in M_n$, A_{ij} — алгебраическое дополнение к элементу a_{ij}.

Теорема. *При любом $i = 1,\ldots,n$ имеет место равенство (разложение определителя по i-й строке):*

$$|\mathbf{A}| = \sum_{j=1}^{n} a_{ij}A_{ij}. \tag{10}$$

Доказательство. Представим i-ю строку в виде

$$(a_{i1}\ a_{i2}\ldots a_{in}) = (a_{i1}\ 0\ldots 0) + (0\ a_{i2}\ldots 0) + \ldots + (0\ 0\ldots a_{in}).$$

Так как определитель — аддитивная функция строк, то

$$|\mathbf{A}| = \sum_{j=1}^{n} \Delta_j \ ; \qquad \Delta_j := \ {}_{(i)} \begin{vmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & a_{ij} & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \dots & a_{nj} & \dots & a_{nn} \end{vmatrix} .$$

В каждом из определителей Δ_j выделена i-я строка; остальные строки — такие, как в $\mathbf{A}$. Убедимся в том, что $\Delta_j = a_{ij}A_{ij}$, что и даст (10).

С помощью перестановок строк и столбцов Δ_j преобразуется к виду

$$\Delta_j = (-1)^{i-1+j-1} \begin{vmatrix} a_{ij} & 0 & \dots & 0 \\ \vdots & & \mathbf{A_{ij}} & \end{vmatrix} .$$

Здесь $\mathbf{A_{ij}}$ — матрица, получающаяся из $\mathbf{A}$ вычёркиванием i-й строки и j-го столбца. Применяя лемму об определителе с нулевым углом (пункт 4.4), приходим к равенству

$$\Delta_j = (-1)^{i+j} a_{ij} |\mathbf{A_{ij}}| = a_{ij} \cdot (-1)^{i+j} M_{ij} = a_{ij} A_{ij}.$$

Теорема доказана.

Следствие 1. *Если* $i \neq k$, *то* $\sum\limits_{j=1}^{n} a_{ij} A_{kj} = 0$.

Таким образом, сумма произведений элементов некоторой строки на соответствующие алгебраические дополнения к элементам другой строки равна нулю.

Доказательство. Рассмотрим вспомогательный определитель Δ, у которого в k-й строке записана (второй раз) i-я строка матрицы $\mathbf{A}$, а все остальные строки — такие же, как в $\mathbf{A}$. Очевидно, $\Delta = 0$. Равенство следствия 1 совпадает с разложением этого определителя по k-й строке.

Результаты теоремы и следствия 1 можно объединить в следующем виде:

$$\sum_{j=1}^{n} a_{ij} A_{kj} = \delta_{ik} \cdot |\mathbf{A}| \ , \tag{11}$$

где δ_{ik} — *символ Кронекера*:

$$\delta_{ik} := \begin{cases} 1 \ , & i = k \\ 0 \ , & i \neq k \end{cases}$$

Следствие 2. *Аналог свойства (11) справедлив и для столбцов:*

$$\sum_{j=1}^{n} a_{ji} A_{jk} = \delta_{ik} \cdot |\mathbf{A}| \ . \tag{12}$$

Можно получить (12) по той же схеме с заменой строк на столбцы. Внимательный читатель заметит также, что равенства (11) и (12) эквивалентны в связи с инвариантностью определителя относительно транспонирования.

Приведём теперь утверждение, обобщающее отмеченные результаты.

Теорема Лапласа. *Пусть в определителе d порядка n выделены k строк (столбцов), $k = 1, \ldots, n-1$. Определитель d равен сумме произведений всех миноров k-го порядка, содержащихся в этих строках (столбцах), на их алгебраические дополнения.*

Пример. Выделяя в определителе вторую и четвёртую строки, имеем равенство:

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 7 & 8 \\ 4 & 3 & 2 & 1 \\ 0 & 0 & 6 & 5 \end{vmatrix} =$$

$$= \begin{vmatrix} 7 & 8 \\ 6 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 & 2 \\ 4 & 3 \end{vmatrix} \cdot (-1)^{3+4+2+4} = (-13) \cdot (-5) \cdot (-1) = -65.$$

Упражнение. Получить из теоремы Лапласа лемму об определителе с нулевым углом.

Естественно, результаты этого пункта могут с успехом применяться для счёта определителей. Иногда понижение порядка позволяет получить общую формулу для определителя с некоторой структурой. На этом основан *метод рекуррентных соотношений* вычисления определителей порядка n, описанный, например, в задачнике И.В. Проскурякова [23, с. 32].

Однако понижение порядка в общей ситуации (например, как основа вычислительного алгоритма) менее эффективно, чем метод Гаусса.

4.6. Определитель Вандермонда и задача интерполяции многочленами

Пусть $x_1, \ldots, x_n \in \mathrm{R}$. *Определителем Вандермонда* $V_n(x_1, \ldots, x_n)$ называется следующий определитель порядка n :

$$V_n(x_1, \ldots, x_n) := \begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ x_1 & x_2 & x_3 & \ldots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \ldots & x_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \ldots & x_n^{n-1} \end{vmatrix}.$$

Определитель V_n был рассмотрен впервые А. Вандермондом для $n = 3$ (A.T. Vandermonde, 1771) и позднее О. Коши (A.L. Cauchy, 1815).

Теорема 1. *При любом $n \geqslant 2$*

$$V_n(x_1, \ldots, x_n) = \prod_{j>i} (x_j - x_i). \tag{13}$$

В частности, $V_n(x_1, \ldots, x_n) \neq 0 \iff x_i \neq x_j$ при $i \neq j$.

Доказательство. Вычтем из каждой строки определителя, начиная со второй, предыдущую, умноженную на x_1. Затем разложим получившийся определитель по 1 столбцу и, наконец, вынесем общие множители из столбцов.

$$V_n(x_1,\dots,x_n)=\begin{vmatrix} 1 & 1 & \dots & 1 \\ 0 & x_2-x_1 & \dots & x_n-x_1 \\ 0 & x_2^2-x_1x_2 & \dots & x_n^2-x_1x_n \\ \vdots & \vdots & & \vdots \\ 0 & x_2^{n-1}-x_1x_2^{n-2} & \dots & x_n^{n-1}-x_1x_n^{n-2} \end{vmatrix}=$$

$$=\begin{vmatrix} x_2-x_1 & \dots & x_n-x_1 \\ x_2(x_2-x_1) & \dots & x_n(x_n-x_1) \\ \vdots & & \vdots \\ x_2^{n-2}(x_2-x_1) & \dots & x_n^{n-2}(x_n-x_1) \end{vmatrix}=\prod_{j>1}(x_j-x_1)\begin{vmatrix} 1 & \dots & 1 \\ x_2 & \dots & x_n \\ \vdots & & \vdots \\ x_2^{n-2} & \dots & x_n^{n-2} \end{vmatrix}=$$

$$=\prod_{j>1}(x_j-x_1)\cdot V_{n-1}(x_2,\dots,x_n).$$

Аналогично получаются равенства

$$V_{n-1}(x_2,\dots,x_n)=\prod_{j>2}(x_j-x_2)\cdot V_{n-2}(x_3,\dots,x_n),$$

и т. д. Последнее из них имеет вид: $V_2(x_{n-1},x_n)=x_n-x_{n-1}$. Собирая все эти соотношения вместе, получим (13). Теорема доказана.

Определители (матрицы) со структурой Вандермонда или транспонированные к ним возникают во многих задачах прикладной математики. Мы рассмотрим лишь одно важное их приложение — *задачу полиномиальной интерполяции.*

Постановка задачи интерполяции заключается в следующем.

Пусть $x_0,x_1,\dots,x_n\in\mathrm{R}$ — попарно различные точки (*узлы интерполяции*), $b_0,b_1,\dots,b_n$ — произвольные числа. Требуется найти многочлен $f(x)$ степени $\leqslant n$ такой, что

$$f(x_k)=b_k,\quad k=0,1,\dots,n. \tag{14}$$

Без ограничения $\deg f\leqslant n$ нарушается единственность решения (приведите пример). В сформулированном виде задача интерполяции является вполне корректной в следующем смысле.

Теорема 2. *Существует единственный многочлен f степени $\leqslant n$ такой, что выполнены равенства (14).*

Доказательство. Полагая $f(x)=a_0+a_1x+\ldots+a_nx^n$, перепишем соотношения (14) в виде системы линейных уравнений относительно неизвестных коэффициентов a_k с квадратной матрицей порядка $n+1$:

$$\begin{pmatrix} 1 & x_0 & \dots & x_0^n \\ 1 & x_1 & \dots & x_1^n \\ \vdots & \vdots & & \vdots \\ 1 & x_n & \dots & x_n^n \end{pmatrix}\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix}=\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_n \end{pmatrix}. \tag{15}$$

Определитель матрицы системы равен $V_{n+1}(x_0, x_1, \ldots, x_n)$; он отличен от 0, так как $x_i \neq x_j,\ i \neq j$. Поэтому система, а значит, и задача интерполяции имеет единственное решение.

Явный вид многочлена f можно получить, решая систему (15). Однако чаще пользуются следующей *интерполяционной формулой Лагранжа* (J.L. Lagrange, 1795):

$$f(x) = \sum_{i=0}^{n} b_i L_i(x)\ ; \quad L_i(x) := \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}\ ,\ i = 0, 1, \ldots, n.$$

Непосредственная проверка показывает, что многочлены Лагранжа L_i обладают свойствами $\deg L_i = n,\ L_i(x_k) = \delta_{ik}$, и поэтому все условия интерполяции выполнены. Действительно, если $f(x)$ имеет форму Лагранжа, то

$$\deg f \leqslant n\ ; \quad f(x_k) = \sum_{i=0}^{n} b_i L_i(x_k) = \sum_{i=0}^{n} b_i \delta_{ik} = b_k.$$

Упражнение 1. Показать, что многочлены Лагранжа имеют вид

$$L_i(x) = \frac{\Delta_i(x)}{\Delta}, \quad i = 0, \ldots, n,$$

где Δ — определитель системы (15), а $\Delta_i(x)$ получается из Δ заменой $(i+1)$-й строки на строку

$$(1\ x\ x^2\ \ldots\ x^n).$$

Упражнение 2. Получить интерполяционную формулу Лагранжа непосредственно из системы (15). Использовать формулы Крамера.*

Интересные вопросы *аппроксимации функции* $F : [a, b] \to \mathrm{R}$ *её интерполяционным многочленом* f по данной системе узлов $x_i \in [a, b]$ изучаются в курсах методов вычислений, (прикладной) теории приближения и других. В этом случае $b_i := F(x_i)$; тем самым, в узлах выполнено $F(x_i) = f(x_i)$. Если же $x \in [a, b]$ не является узлом, то вовсе не обязательно $F(x) = f(x)$. Речь идёт о точности приближённого представления $F(x) \approx f(x)$ *на всём отрезке* $[a, b]$.

Некоторые сведения на эту тему (эффективный выбор узлов, двумерные аналоги формулы Лагранжа и пр.) приводятся в учебном пособии М.В. Невского, И.П. Иродовой [19]. Там же представлена и соответствующая библиография.

4.7. Теорема об определителе произведения двух матриц

В приложениях часто используется тот факт, что две сложные операции — вычисление произведения двух квадратных матриц и взятие определителя — связаны очень простым образом.

Теорема. *Пусть* $\mathbf{A}, \mathbf{B} \in M_n$. *Тогда*

$$|\mathbf{AB}| = |\mathbf{A}| \cdot |\mathbf{B}|. \tag{16}$$

Доказательство. Рассмотрим вспомогательный определитель Δ порядка $2n$, имеющий такой блочный вид:

$$\Delta := \begin{vmatrix} \mathbf{A} & \mathbf{0} \\ -\mathbf{E} & \mathbf{B} \end{vmatrix}.$$

Здесь $\mathbf{0}$ — нулевая, $\mathbf{E}$ — единичная матрицы порядка n. Вычислим Δ следующими двумя способами.

Первый способ. По лемме об определителе с нулевым углом (пункт 4.4) $\Delta = |\mathbf{A}| \cdot |\mathbf{B}|$.

Второй способ. С помощью некоторых преобразований над последними n столбцами Δ может быть приведён к виду

$$\Delta = \begin{vmatrix} \mathbf{A} & \mathbf{C} \\ -\mathbf{E} & \mathbf{0} \end{vmatrix}, \qquad \mathbf{C} := \mathbf{AB}. \tag{17}$$

Разберём для примера случай $n = 3$, то есть

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & a_{13} & 0 & 0 & 0 \\ a_{21} & a_{22} & a_{23} & 0 & 0 & 0 \\ a_{31} & a_{32} & a_{33} & 0 & 0 & 0 \\ -1 & 0 & 0 & b_{11} & b_{12} & b_{13} \\ 0 & -1 & 0 & b_{21} & b_{22} & b_{23} \\ 0 & 0 & -1 & b_{31} & b_{32} & b_{33} \end{vmatrix}.$$

Пусть X_i — столбцы Δ. Равенство (17) получается после таких преобразований (проведите аккуратную проверку):

$$\begin{aligned} X_4 &\to X_4 + b_{11}X_1 + b_{21}X_2 + b_{31}X_3, \\ X_5 &\to X_5 + b_{12}X_1 + b_{22}X_2 + b_{32}X_3, \\ X_6 &\to X_6 + b_{13}X_1 + b_{23}X_2 + b_{33}X_3. \end{aligned}$$

Эта схема легко обобщается на случай произвольного n.

Из (17) следует, что $\Delta = |-\mathbf{E}| \cdot |\mathbf{C}| \cdot (-1)^t$, где

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

Надо применить теорему Лапласа к последним n строкам преобразованного определителя. Так как $|-\mathbf{E}| = (-1)^n$, то $\Delta = |\mathbf{C}| = |\mathbf{AB}|$. (Последний результат также может быть получен с помощью нужных перестановок строк определителя (17) и применения затем леммы об определителе с нулевым углом.)

Сравнение результатов вычисления даёт равенство (16). Теорема доказана.

4.8. Обратимость и невырожденность. Теорема об обратной матрице

Напомним, что *обратимой* называется матрица $\mathbf{A}$, для которой существует матрица $\mathbf{A}^{-1}$ (*обратная к* $\mathbf{A}$) такая, что $\mathbf{A}\mathbf{A}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{E}$. Матрицы имеют порядок n.

Некоторые свойства обратимых матриц отмечены в пункте 2.4. Здесь мы подчеркнём важную связь между обратимостью и невырожденностью, а также получим явную формулу для $\mathbf{A}^{-1}$.

Определение. *Матрица $\mathbf{A} \in M_n$ такая, что $|\mathbf{A}| = 0$, называется вырожденной (или особенной, сингулярной). Если же $|\mathbf{A}| \neq 0$, то $\mathbf{A}$ называется невырожденной (неособенной, несингулярной).*

Теорема. *Матрица $\mathbf{A}$ является обратимой тогда и только тогда, когда эта матрица является невырожденной. Если $|\mathbf{A}| \neq 0$, то*

$$\mathbf{A}^{-1} = \frac{1}{|\mathbf{A}|}\mathbf{\Lambda}^T, \tag{18}$$

где $\mathbf{\Lambda} := (A_{ij})$ — матрица из алгебраических дополнений к элементам матрицы $\mathbf{A}$.

Матрица $\mathbf{\Lambda}^T$ из условия теоремы называется *присоединённой к* $\mathbf{A}$.

Доказательство. $\Longrightarrow$. Пусть $\mathbf{A}$ обратима. Из определения $\mathbf{A}^{-1}$ и теоремы об определителе произведения матриц (пункт 4.7) следует, что $|\mathbf{A}| \cdot |\mathbf{A}^{-1}| = |\mathbf{E}| = 1$. Это гарантирует невырожденность $\mathbf{A}$ и сверх того полезное равенство

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

$\Longleftarrow$. Пусть $\mathbf{A}$ — невырожденная матрица. Обозначим через $\mathbf{B}$ матрицу, стоящую в правой части (18), и убедимся, что $\mathbf{A}\mathbf{B} = \mathbf{B}\mathbf{A} = \mathbf{E}$. Проверим лишь первое из этих равенств, второе получается аналогично.

Пусть $\mathbf{C} = \mathbf{A}\mathbf{B}$. Тогда по результатам пункта 4.5 о разложении определителя (см. там равенство (11))

$$c_{ik} = \frac{1}{|\mathbf{A}|}(a_{i1}A_{k1} + \ldots + a_{in}A_{kn}) = \delta_{ik} = \begin{cases} 1 & , \quad i = k \\ 0 & , \quad i \neq k \end{cases}$$

Значит, $\mathbf{C} = (c_{ik}) = \mathbf{E}$.

Таким образом, установлены и обратимость $\mathbf{A}$, и формула (18).

Теорема доказана.

Упражнение. Получить формулу (18) из матричного уравнения $\mathbf{A}\mathbf{X} = \mathbf{E}$. Использовать формулы Крамера для столбцов матрицы $\mathbf{X}$.

Сведения о приложениях определителей, не вошедшие в этот раздел, будут пополняться в дальнейшем. Так, теорема о ранге матрицы (называемая также теоремой о базисном миноре) доказывается в разделе 6. Характеристический многочлен и его роль в задачах о собственных значениях изучаются в разделе 8. Определитель Грама возникает при решении задач на расстояние в евклидовых пространствах, см. раздел 7.

Часть 2

5. Линейные пространства

В различных разделах математики (не только в алгебре, а и других — например, в анализе и многочисленных приложениях) рассматриваются множества, элементы которых можно складывать и умножать на числа.

Если эти операции имеют восемь естественных свойств, мы говорим, что все эти совокупности являются *линейными пространствами.* Большой список примеров даётся в пункте 5.1. Теория линейных пространств позволяет изучать множества различной природы с единой точки зрения; в этом проявляется алгебраический подход.

Понятие *линейной зависимости* приводит к выделению *конечномерных и бесконечномерных линейных пространств*; их можно охарактеризовать также с точки зрения существования (конечного) *базиса.* В конечномерной ситуации определяется *максимальное число линейно независимых элементов пространства*; оно оказывается равным числу элементов базиса, то есть *размерности.* Важную роль в построении этой теории играет лемма о двух системах векторов из пункта 5.4.

Наконец, выясняется, что каждое конечномерное линейное пространство положительной размерности *изоморфно* одному из пространств R^{n}, $n \in \mathrm{N}$.

Основным объектом нашего исследования являются именно конечномерные пространства; бесконечномерные пространства изучаются более подробно в курсе *функционального анализа.*

Становление теории линейных пространств происходило примерно с середины 19 в. и связано с именами многих математиков.

Отметим прежде всего работы Артура Кэли (A. Cayley, 1821 – 1895) и Германа Грассмана (H. Grassman, 1809 – 1877). Последний, например, дал определение линейной зависимости, размерности и доказал некоторые фундаментальные результаты. Грассманом получен, в частности, классический результат о размерностях суммы и пересечения двух линейных подпространств (см. раздел 6).

Аксиоматическое определение действительного линейного пространства и линейного отображения из одного такого пространства в другое дал в 1888 г. итальянский математик Джузеппе Пеано (G. Peano, 1858 – 1932).

5.1. Определение линейного пространства. Следствия из аксиом. Примеры линейных пространств

Перед ознакомлением с содержанием этого пункта читателю рекомендуется вспомнить материал разделов 2 и 3, где множества n-мерных векторов R^{n}, $m \times n$-матриц

$M_{m,n}$, $m, n \in \mathrm{N}$, и геометрических векторов V_n, $n = 1, 2, 3$, вводятся как (действительные) линейные пространства. Там же даётся и мотивация следующего более общего определения.

Определение. *Непустое множество L элементов $x, y, z, \ldots$ называется действительным линейным пространством, если в L заданы две операции — сложения двух элементов L и умножения элемента L на произвольное действительное число. Результаты этих действий обозначаются $x+y$ и λx; сказанное означает, что $x + y, \lambda x \in L$ при всех $x, y \in L, \lambda \in \mathrm{R}$.*

При этом справедливы следующие восемь условий (аксиомы линейного пространства):

$$1^\circ. \quad x + y = y + x \ ;$$

$$2^\circ. \quad (x + y) + z = x + (y + z) \ ;$$

$$3^\circ. \quad \exists 0 \in L : \ x + 0 = x \ ;$$

$$4^\circ. \quad \exists (-x) \in L : \ x + (-x) = 0 \ ;$$

$$5^\circ. \quad 1 \cdot x = x \ ;$$

$$6^\circ. \quad \alpha(\beta x) = (\alpha\beta)x \ ;$$

$$7^\circ. \quad \alpha(x + y) = \alpha x + \alpha y \ ;$$

$$8^\circ. \quad (\alpha + \beta)x = \alpha x + \beta x \ .$$

Здесь $x, y, z \in L$; $\alpha, \beta \in \mathrm{R}$.

Элементы линейного пространства называются *векторами* (отсюда другой термин для L — *векторное пространство*).

Аксиомы линейного пространства распадаются на свойства сложения ($1^\circ - 4^\circ$), умножения на число ($5^\circ - 6^\circ$) и их связи (законы дистрибутивности $7^\circ - 8^\circ$).

Первые четыре условия означают, что алгебраическая структура $(L, +)$ является так называемой *коммутативной (или абелевой) группой*. Вектор 0 из 3° называется *нулевым, или нулём* L, вектор $(-x)$ из 4° — *противоположным* к x.

В пятом условии 1 есть обычная единица. Аксиомы дистрибутивности 7° и 8° различны: одна связана со сложением в L, а другая — со сложением в R; оба действия обозначены символом $+$.

Замечание 1. Если множители $\lambda, \alpha, \beta, 1$ считать комплексными числами, получается определение *комплексного линейного пространства*. Аналогично вводится общее понятие *линейного пространства над полем* F; 1 в этом случае обозначает единичный элемент F. Ниже под линейным пространством понимается действительное линейное пространство.

Как действие, обратное сложению, в L вводится *вычитание*. Именно, для $x, y \in L$ полагаем $z := x - y$, если $z + y = x$.

Из аксиом линейного пространства вытекает ряд полезных следствий; мы отметим основные из них.

Следствия. *1) Нулевой вектор* 0 *из* 3° *и противоположный* $(-x)$ *(для каждого* $x \in L$*) определяются единственным образом.*

2) $\alpha x = 0 \iff \alpha = 0$ *или* $x = 0$.

3) $\alpha(-x) = (-\alpha)x = -(\alpha x)$.

4) Для $x, y \in L$ разность $z = x - y$ определена единственным образом. При этом $z = x + (-y)$.

5) Имеют место равенства

$$\alpha(x - y) = \alpha x - \alpha y, \qquad (\alpha - \beta)x = \alpha x - \beta x \ .$$

Дадим **доказательство** следствий 1) – 3). Первая часть 1) следует из элегантного равенства

$$0' = 0' + 0'' = 0''$$

для *двух* нулей L.

Если $0 = x + a = x + b$, то $a = b$: к обеим частям правого равенства надо прибавить $(-x)$.

2) $\Longleftarrow$. Имеем:

$$\alpha \cdot 0 = \alpha \cdot (0 + 0) = \alpha \cdot 0 + \alpha \cdot 0 \ ,$$

$$x = 1 \cdot x = (1 + 0) \cdot x = 1 \cdot x + 0 \cdot x = x + 0 \cdot x \ ,$$

поэтому

$$\alpha \cdot 0 = 0 \cdot x = 0$$

(нули здесь обозначают различные объекты).

$\Longrightarrow$. Если $\alpha \neq 0$, достаточно умножить на число α^{-1} равенство $\alpha x = 0$ — получим с учётом предыдущего, что $x = 0$.

3) Из результата следствия 2) получается, что

$$\alpha x + (-\alpha)x = (\alpha + (-\alpha))x = 0 \cdot x = 0 \ ,$$

$$\alpha x + \alpha(-x) = \alpha(x + (-x)) = \alpha \cdot 0 = 0 \ ,$$

и равенство следствия 3) установлено.

Упражнение 1. Доказать следствия 4) – 5).

Перейдём теперь к важнейшим примерам линейных пространств.

П р и м е р ы л и н е й н ы х п р о с т р а н с т в

1. Пусть L — произвольное множество с единственным элементом x. Положим $x + x := x, \lambda x := x$ для всех $\lambda \in \mathrm{R}$. Очевидно, L является линейным пространством (обе части каждого равенства 1° — 8° равны x). Из 3° следует, что $x = 0$.

Тривиальный пример линейного пространства $L = \{0\}$, содержащего единственный нулевой вектор, является очень важным.

Упражнение 2. Пусть действительное линейное пространство $L \neq \{0\}$. Показать, что L содержит бесконечное число элементов. Поэтому выше приведён единственный возможный пример линейного пространства с конечным числом элементов (это число равно 1).

2. Линейное пространство геометрических векторов $\mathrm{V_n}, n = 1, 2, 3$, с обычными операциями сложения векторов и умножения их на число, см. пункт 3.1.

Упражнение 3. Пусть L — совокупность векторов $\mathrm{V_n}$, концы которых принадлежат данному множеству G (все векторы откладываются из одной точки). При

каких G множество L является линейным пространством? Рассмотреть отдельно случаи $n = 1, 2, 3$.

3. Действительное n-мерное арифметическое пространство $\mathrm{R^n}, n \in \mathrm{N}$, с покомпонентными операциями сложения n-мерных векторов и умножения вектора на число, см. пункт 2.1.

4. Пространство матриц $M_{m,n}(\mathrm{R})$ порядка $m \times n$, $m, n \in \mathrm{N}$, с поэлементными операциями сложения матриц и умножения на число, см. пункт 2.2. Особо выделим важный случай $m = n$. Напомним, что $M_{n,n}$ обозначается как M_n.

5. Линейное пространство $P_n := \mathrm{R_n}[t]$ алгебраических многочленов от переменного t с действительными коэффициентами *степени* $\leqslant n$, $\quad n = 0, 1, 2, \ldots$.

Для $f, g \in P_n$ полагаем

$$f(t) + g(t) := (a_0 + b_0) + (a_1 + b_1)t + \ldots + (a_n + b_n)t^n \ ,$$

$$\lambda f(t) := (\lambda a_0) + (\lambda a_1)t + \ldots (\lambda a_n)t^n \ .$$

Здесь a_i и b_i — коэффициенты при t^i многочленов f и g соответственно.

Напомним, что равенство $f = g$ в P_n эквивалентно условию $a_i = b_i$ для всех i. Нулевой многочлен — это многочлен, все коэффициенты которого равны нулю (его степень, как и степень любой другой константы, по определению также равна 0). Равенства 1° — 8° проверяются на коэффициентах многочленов. Весьма существенно то, что в связи с ограничением $\deg f \leqslant n$ совокупность P_n замкнута относительно введённых операций.

Замечание. Каждое из пространств матриц $M_{m,n}$ или многочленов P_n по своей структуре устроено так же, как некоторое пространство $\mathrm{R^k}$ (при подходящем значении k): равенства и операции во всех этих классах покомпонентные. Это наблюдение развивается через понятие *изоморфизма*, см. ниже пункт 5.5.

6. Совокупность $P := \mathrm{R}[t]$ многочленов *произвольной степени*, то есть

$$P = \bigcup_n P_n,$$

также образует линейное пространство относительно введённых операций. Таким образом, имеется бесконечная цепочка возрастающих линейных пространств многочленов:

$$P_0 \subset P_1 \subset P_2 \subset P_3 \subset \ldots \subset P.$$

7. *Функциональные линейные пространства* — это линейные пространства, элементами которых являются функции. Многие из них являются объектами пристального изучения в анализе и приложениях. Здесь мы ограничимся рассмотрением функций $f : E \longrightarrow \mathrm{R}$, E — подмножество R.

Две фунции $f, g : E \longrightarrow \mathrm{R}$ называются равными, если $f(t) = g(t)$ при всех $t \in E$. Нулевая функция — это функция, тождественно равная 0 на E. Сумма двух функций и произведение функции на число также определяются *поточечно*:

$$(f + g)(t) := f(t) + g(t), \ (\lambda f)(t) := \lambda f(t), \ t \in E \ .$$

Нетрудно убедиться, что совокупность *всех* функций, определённых на данном множестве E, образует линейное пространство (аксиомы 1° — 8° сводятся к очевидным поточечным равенствам).

Эта совокупность необозрима даже в ситуации $E = [a, b]$. Дальнейшая конкретизация связана с уточнением свойств функций. Например, для $E = [a, b]$ такими свойствами могут быть ограниченность, непрерывность, дифференцируемость и т.д. Так возникают следующие классы функций:

$B[a, b]$ — совокупность *ограниченных* на $[a, b]$ функций f, то есть таких, что

$$\sup_{a \leqslant x \leqslant b} |f(x)| =: M_f < \infty$$

(*bounded* по-английски означает "ограниченный");

$C[a, b]$ — совокупность *непрерывных* на $[a, b]$ функций (*continuous* по-английски "непрерывный");

$C^k[a, b], k \in \mathrm{N}$, — совокупность функций, имеющих на $[a, b]$ непрерывные производные *вплоть до порядка* k;

$C^\infty[a, b]$ — совокупность функций, имеющих (непрерывные) производные *всех порядков*, и т.д.

Каждая из рассмотренных совокупностей является линейным пространством. Здесь существенны известные в анализе простые свойства функций (сумма двух ограниченных функций есть функция ограниченная, то же — для непрерывных и дифференцируемых функций, и т.д.). Важно и то, что функция, тождественно равная нулю, входит в любой из отмеченных классов. Очевидно, имеют место строгие включения

$$C^\infty[a, b] \subset \ldots \subset C^2[a, b] \subset C^1[a, b] \subset C[a, b] \subset B[a, b] \ .$$

8. *Пространства последовательностей* — это такие линейные пространства, элементами которых являются бесконечные последовательности действительных чисел $x = (x_1, x_2, x_3, \ldots) = (x_i)_{i=1}^\infty$.

Так как каждая последовательность является функцией натурального аргумента, то эта ситуация сводится к предыдущей (надо взять $E = \{1, 2, 3, \ldots\} = \mathrm{N}$). Рассмотрим, однако, этот случай отдельно.

Две последовательности $x = (x_i)$ и $y = (y_i)$ называются равными, если $x_i = y_i$ для всех $i = 1, 2, \ldots$. Нулевая последовательность состоит из одних 0. Действия с последовательностями осуществляются покомпонентно. Легко видеть, что совокупность *всех* действительных последовательностей имеет структуру линейного пространства.

Конкретизация свойств последовательностей приводит, например, к таким совокупностям (их принято обозначать малыми буквами — в отличие от функциональных множеств):

b (или l_∞) — совокупность *ограниченных* последовательностей x, то есть таких, что

$$\sup_i |x_i| =: M_x < \infty \ ;$$

c — совокупность *сходящихся* последовательностей (каждая сходится к своему пределу);

c_0 — совокупность последовательностей, *сходящихся к нулю*;

l_1 — совокупность *суммируемых* последовательностей x, то есть таких, для которых

$$\sum_i |x_i| =: S_x < \infty \ .$$

Каждое из этих множеств последовательностей является линейным пространством (дайте обоснование). Отметим также строгие включения

$$l_1 \subset c_0 \subset c \subset b\ .$$

5.2. Линейная зависимость и независимость. Свойства линейной зависимости. Лемма о двух системах векторов

На произвольные линейные пространства распространяются все основные определения, которые мы ввели для пространств геометрических или n-мерных векторов. Прежде всего речь идёт о важнейшем понятии линейной зависимости и независимости конечной системы векторов.

Пусть L — линейное пространство, $x_1, \ldots, x_k \in L$, $\lambda_1, \ldots, \lambda_k \in \mathrm{R}$. Вектор $y = \lambda_1 x_1 + \ldots + \lambda_k x_k$ называется *линейной комбинацией* векторов $x_1, \ldots, x_k$. Совокупность всех линейных комбинаций такого вида (с любыми коэффициентами λ_i) называется *линейной оболочкой* $x_1, \ldots, x_k$ и обозначается в дальнейшем $\mathrm{lin}(x_1, \ldots, x_k)$:

$$\mathrm{lin}(x_1, \ldots, x_k) := \{y \in L :\ y = \sum_{i=1}^{k} \lambda_i x_i,\ \lambda_i \in \mathrm{R}\}.$$

Важная задача состоит в построении для данного линейного пространства L такой минимальной (по количеству элементов) системы $x_1, \ldots, x_k$, что $L = \mathrm{lin}(x_1, \ldots, x_k)$. Мы выясним, что эта задача имеет решение лишь для так называемых конечномерных линейных пространств.

Определение. *Система векторов $x_1, \ldots, x_k$ называется линейно зависимой, если некоторая нетривиальная линейная комбинация этих векторов равна* 0, *и линейно независимой, если равенство*

$$\sum_{i=1}^{k} \lambda_i x_i = 0 \tag{1}$$

возможно лишь в ситуации $\lambda_1 = \ldots = \lambda_k = 0$.

Весьма важно заметить, что (1) рассматривается *как равенство в L*, и в решении конкретных задач в каждом из пространств предыдущего пункта следует использовать идентификацию элементов L и определение операций в этом пространстве.

Линейная зависимость в $\mathrm{V_n}$ тесно связана с геометрическими понятиями (коллинеарность и компланарность), см. пункт 3.3; вопрос о линейной зависимости в *пространствах координатного типа* — $\mathrm{R^n}, M_{m,n}, \mathrm{R}[t]$, пространствах последовательностей — сразу сводится к анализу системы линейных однородных уравнений, см. пункт 3.4.

В функциональной ситуации могут использоваться средства математического анализа.

Пример 1. Линейная независимость любой системы степеней t^{m_1}, ..., t^{m_k} как элементов $\mathrm{R}[t]$ (m_i — целые неотрицательные, $m_1 < \ldots < m_k$) очевидна, так как в правой части равенства

$$\sum_{i=1}^{k} \lambda_i t^{m_i} = 0 \tag{2}$$

стоит нулевой многочлен; это вовсе не уравнение относительно t. Оно выполняется в пространстве многочленов, поэтому сравнение коэффициентов в (2) сразу даёт $\lambda_1 = \ldots = \lambda_k = 0$.

В пространстве $C[0,1]$ то же равенство (2) имеет совсем другой смысл: это тождество относительно $t \in [0,1]$, а в правой части стоит функция, тождественно равная 0. Так как ненулевой многочлен не может иметь корней больше, чем его степень, то все $\lambda_i = 0$, и система функций t^{m_i} линейно независима. Это рассуждение использует *основную теорему алгебры многочленов*.

Пример 2. Вопрос о линейной независимости функций $\cos t, \sin t$ в пространстве $[0, 2\pi]$ сводится к анализу тождества

$$\alpha \cos t + \beta \sin t \equiv 0, \ t \in [0, 2\pi] \ .$$

Достаточно подставить $t_1 = 0, t_2 = \frac{\pi}{2}$ — мы получим $\alpha = \beta = 0$.

Пример 3. Пусть требуется установить линейную независимость функций 1, $\cos t$, $\sin t$ как элементов $C^1[0, 2\pi]$. Дифференцируя соответствующее равенство, мы сведём задачу к предыдущей. Это не единственный возможный путь решения.

Упражнение 1. Установить линейную независимость системы функций 1, $\cos t$, $\sin t$, $\cos 2t$, $\sin 2t$, ..., $\cos kt$, $\sin kt$ *в пространстве* $C^\infty[0, 2\pi]$ *при любом* $k \in \mathrm{N}$.

Напомним основные свойства линейной зависмости; они устанавливаются так же, как и для пространства $\mathrm{V_n}, n = 1, 2, 3$ (по поводу доказательства см. пункт 3.3).

Свойства линейной зависимости

1°. Система из одного вектора x линейно зависима $\Longleftrightarrow x = 0$.

2°. Система, содержащая 0, линейно зависима.

3°. Если некоторая подсистема линейно зависима, то и вся система линейно зависима.

4°. Пусть $k > 1$. Система $x_1, \ldots, x_k$ линейно зависма $\Longleftrightarrow$ один из векторов есть линейная комбинация других.

5°. Пусть система $x_1, \ldots, x_k$ — линейно независима, система $x_1, \ldots, x_k, y$ —линейно зависима. Тогда $y \in \mathrm{lin}(x_1, \ldots, x_k)$.

6°. Пусть $y \in \mathrm{lin}(x_1, \ldots, x_k)$. Представление y через $x_1, \ldots, x_k$ является единственным $\Longleftrightarrow$ система $x_1, \ldots, x_k$ линейно независима.

Остановимся подробнее на следующем важном свойстве, играющем в теории линейных пространств фундаментальную роль.

Лемма о двух системах векторов. *Пусть $x_1, \ldots, x_k$ и $y_1, \ldots, y_m$ — две системы векторов L, причём вторая система линейно независима и $y_j \in \lin(x_1, \ldots, x_k)$ для всех $j = 1, \ldots, m$. Тогда $m \leqslant k$. Иначе говоря, среди линейных комбинаций данных k векторов может быть не более k линейно независимых.*

Доказательство осуществляется индукцией по числу k векторов первой системы. При $k = 1$ утверждение очевидно (два вектора вида αx_1 и βx_1 линейно зависимы). Предположим, что лемма верна для $k-1$ векторов первой системы и установим её справедливость для k векторов. Пусть

$$\begin{gathered} y_1 = \alpha_{11}x_1 + \ldots + \alpha_{1,k-1}x_{k-1} + \alpha_{1k}x_k \ , \\ \ldots \quad \ldots \quad \ldots \quad \ldots \\ y_{m-1} = \alpha_{m-1,1}x_1 + \ldots + \alpha_{m-1,k-1}x_{k-1} + \alpha_{m-1,k}x_k \ , \\ y_m = \alpha_{m1}x_1 + \ldots + \alpha_{m,k-1}x_{k-1} + \alpha_{mk}x_k \ , \end{gathered}$$

и при этом $y_1, \ldots, y_m$ линейно независимы. Покажем, что $m \leqslant k$.

Если все коэффициенты при x_k равны 0, то $y_j \in \lin(x_1, \ldots, x_{k-1})$, и по предположению индукции $m \leqslant k-1 \leqslant k$.

Пусть, например, $\alpha_{mk} \neq 0$. Построим новую систему линейно независимых векторов $z_1, \ldots, z_{m-1} \in \lin(x_1, \ldots, x_{k-1})$. По предположению индукции будем иметь $m-1 \leqslant k-1$, то есть $m \leqslant k$.

Для этого выразим из последнего равенства x_k:

$$x_k = \frac{1}{\alpha_{mk}}y_m - \frac{\alpha_{m1}}{\alpha_{mk}}x_1 - \ldots - \frac{\alpha_{m,k-1}}{\alpha_{mk}}x_{k-1} \ ,$$

и подставим затем это выражение во все предыдущие равенства. После простых преобразований мы получим, что

$$\begin{gathered} z_1 := y_1 - \frac{\alpha_{1k}}{\alpha_{mk}}y_m \in \lin(x_1, \ldots, x_{k-1}) \ , \\ \ldots \quad \ldots \quad \ldots \\ z_{m-1} := y_{m-1} - \frac{\alpha_{m-1,k}}{\alpha_{mk}}y_m \in \lin(x_1, \ldots, x_{k-1}) \ . \end{gathered}$$

Линейная независимость системы $z_1, \ldots, z_{m-1}$ легко следует из линейной независимости $y_1, \ldots, y_m$ (убедитесь в этом самостоятельно). Осталось использовать предположение индукции. Лемма доказана.

Упражнение 2. Пусть в условии леммы дополнительно сказано, что система $x_1, \ldots, x_k$ линейно зависима. Показать, что тогда $m < k$.

5.3. Конечномерные и бесконечномерные пространства. Максимальное число линейно независимых элементов. Примеры

Определение. *Бесконечная система векторов линейного пространства L называется линейно независимой, если любая её конечная подсистема линейно независима. Линейное пространство, в котором есть бесконечная линейно независимая система, называется бесконечномерным. Пространство, в котором нет ни одной бесконечной линейно независимой системы, называется конечномерным.*

Введём в рассмотрение также *максимальное число $d(L)$ линейно независимых элементов линейного пространства L*. Это такое натуральное число, которое определяется следующими двумя условиями:

1). В L существует линейно независимая система с числом векторов, равным $d(L)$.

2). Любая система, содержащая большее число векторов, линейно зависима.

Ясно, что в бесконечномерной ситуации такого $d(L)$ не существует.

Примеры. 1. Пространство $L = \{0\}$ является конечномерным: в нём нет ни одной линейно независимой (или бесконечной) системы.

2. Пространства геометрических векторов $\mathrm{V_n}, n = 1, 2, 3$, конечномерны: любая система из $n+1$ векторов $\mathrm{V_n}$ линейно зависима. Очевидно, $d(\mathrm{V_n}) = n$.

3. Пространство $\mathrm{R^n}$ при любом $n \in \mathrm{N}$ конечномерно, причём $d(\mathrm{R^n}) = n$. Действительно, система векторов

$$e^{(1)} := (1, 0, \ldots, 0, 0),$$
$$e^{(2)} := (0, 1, \ldots, 0, 0),$$
$$\ldots \quad \ldots \quad \ldots$$
$$e^{(n)} := (0, 0, \ldots, 0, 1)$$

линейно независима, а произвольная система n-мерных векторов с числом элементов $k > n$ линейно зависима, см. пункт 3.4.

4. Пространство матриц $M_{mn}, m, n \in \mathrm{N}$, конечномерно и $d(M_{mn}) = mn$. Линейно независимой является, например, следующая система из mn матриц $\mathbf{A_{ij}}$: ij-й элемент матрицы $\mathbf{A_{ij}}$ равен 1, а остальные элементы равны 0. Линейная зависимость системы, содержащей большее количество матриц, устанавливается по схеме пункта 3.4.

5. Пространство многочленов $\mathrm{R_n}[t], n = 0, 1, 2, \ldots$, также является конечномерным. Каноническая система степеней $1, t, t^2, \ldots, t^n$ линейно независима (см. пример 1 предыдущего пункта); система из большего числа многочленов степени $\leqslant n$ линейно зависима. Поэтому $d(\mathrm{R_n}[t]) = n + 1$.

6. Пространство $\mathrm{R}[t]$ многочленов произвольной степени бесконечномерно. Бесконечной линейно независимой системой является система $1, t, t^2, \ldots, t^n, \ldots$, так как любая её конечная подсистема линейно независима, см.пример 1 пункта 5.2.

7. Каждое из функциональных пространств $B[a, b]$, $C[a, b]$, $C^k[a, b]$, $C^\infty[a, b]$ бесконечномерно, так как в любом из них содержится система функций $1, t, t^2, \ldots, t^n, \ldots$.

Важный пример бесконечной линейно независимой системы в ситуации $[a,b] = [0,2\pi]$ — тригонометрическая система $1, \cos t, \sin t, \cos 2t, \sin 2t, \ldots, \cos nt, \sin nt, \ldots$, см. упражнение 1 предыдущего пункта. Тригонометрическая система активно используется в анализе и многочисленных приложениях.

Упражнение. Показать, что каждое из пространств последовательностей b, c, c_0, l_1 бесконечномерно.

Установим в этом пункте следующий результат.

Теорема. *Пусть линейное пространство $L \neq \{0\}$ является конечномерным. Тогда определённое выше число $d(L)$ (максимальное число линейно независимых элементов L) существует.*

Доказательство. По условию в L найдётся ненулевой вектор x_1.

Если все системы вида x_1, y линейно зависимы, то, как мы покажем, $d(L) = 1$. В противном случае найдётся линейно независимая система x_1, x_2. Если все системы x_1, x_2, y линейно зависимы, то $d(L) = 2$.

Продолжая этот процесс, построим такую линейно независимую систему x_1, x_2, $\ldots$, x_k, что все системы вида $x_1, x_2, \ldots, x_k, y$ линейно зависимы. В соответствии со свойством 5° линейной зависимости это означает, что каждый вектор $y \in L$ есть линейная комбинация векторов $x_1, x_2, \ldots, x_k$, то есть $L = \operatorname{lin}(x_1, x_2, \ldots, x_k)$.

Процесс построения такой цепочки линейно независимых векторов x_i обязательно оборвётся, иначе в L найдётся бесконечная линейно независимая система $x_1, x_2, \ldots$.

Покажем, что число векторов в построенной системе не зависит от способа выбора линейно независимых векторов. Пусть наряду с системой $x_1, \ldots, x_k$ описанным методом построена линейно независимая система $y_1, \ldots, y_m$. Тогда, как отмечалось, при всех $i = 1, \ldots, k$ и $j = 1, \ldots, m$

$$x_i \in \operatorname{lin}(y_1, \ldots, y_m)\ ,\ y_j \in \operatorname{lin}(x_1, \ldots, x_k)\ .$$

Применяя дважды лемму предыдущего пункта о двух системах векторов, мы получим, что одновременно $k \leqslant m$ и $m \leqslant k$. Это означает, что $m = k = d(L)$.

Теорема доказана.

Замечание. Отметим ещё раз, что если $x_1, \ldots, x_k$ — любая линейно независимая система с числом векторов $k = d(L)$, то обязательно $L = \operatorname{lin}(x_1, \ldots, x_k)$. В конечномерном пространстве $L \neq \{0\}$ система с такими свойствами, как мы показали, обязательно существует.

5.4. Базис, размерность, координаты. Характеризация конечномерных пространств в терминах базиса

Мы установили, что для конечномерного пространства $L \neq \{0\}$ существует максимальное число линейно независимых элементов $d(L)$, а также конечная система векторов, *порождающая* L, то есть дающая L в линейной оболочке.

В этом пункте мы дадим эквивалентную характеризацию конечномерных пространств, используя важное понятие базиса. Число $d(L)$ при таком подходе оказывается равным количеству элементов базиса, то есть размерности L.

Определение 1. *Конечная совокупность векторов $e_1, \ldots, e_n \in L$ называется базисом L тогда и только тогда, когда выполнены два условия:*

1) система $e_1, \ldots, e_n$ линейно независима;

2) $L = \lin(e_1, \ldots, e_n)$.

Второе условие означает в точности, что каждый вектор $x \in L$ есть линейная комбинация элементов базиса:

$$x = \alpha_1 e_1 + \ldots + \alpha_n e_n. \tag{3}$$

Теорема 1. *Если в L существует базис, то любые два базиса L имеют одинаковое количество элементов. Далее, коэффициенты разложения вектора $x \in L$ по данному базису (то есть числа $\alpha_1, \ldots, \alpha_n$ из (3)) определяются единственным образом.*

Доказательство первой части использует лемму о двух системах векторов, см. пункт 5.2, и определение базиса.

Вторая часть следует из свойства 6° линейной зависимости.

Мы мотивировали, таким образом, следующие определения.

Определение 2. *Количество элементов базиса называется размерностью L и обозначается* $\dim L$. *Если $L = \{0\}$, считаем* $\dim L := 0$.

Если $\dim L = n$, то говорят также, что пространство L является *n-мерным*. Отметим также, что символическая запись $\dim L < \infty$ в ряде текстов означает, что L конечномерно.

Определение 3. *Числа $\alpha_1, \ldots, \alpha_n$ из (3) называются координатами вектора x в базисе $e_1, \ldots, e_n$.*

При фиксированном базисе мы будем использовать также запись

$$x = \{\alpha_1, \ldots, \alpha_n\}.$$

Примеры. 1. Пространство $L = \{0\}$ не имеет базиса: в нём нет ни одной линейно независимой системы.

2. Характеризация базисов в пространствах $\mathrm{V_n}, n = 1, 2, 3$, в геометрических терминах дана в пункте 3.5.

3. *Канонические (или стандартные) базисы* в пространствах координатного типа, то есть $\mathrm{R^n}$, M_{mn}, $\mathrm{R_n}[t]$, $m, n \in \mathrm{N}$, описаны в примерах 3 – 5 предыдущего пункта. Разложение по такому базису сразу получается из общего вида вектора.

Например, для векторов из $\mathrm{R^n}$ очевидно равенство:

$$x = (\xi_1, \ldots, \xi_n) = \xi_1 e^{(1)} + \ldots + \xi_n e^{(n)} \ .$$

Это эквивалентно тому, что набор векторов канонического базиса может быть получен из *общего (параметрического) вида элемента L* по следующему простому правилу: одному параметру присваивается значение 1, а всем остальным — 0, и так поочерёдно для всех параметров. Обсудите эту схему для всех пространств.

4. Ни одно из отмеченных бесконечномерных пространств не обладает базисом — это является отражением устанавливаемого ниже общего факта.

Теорема 2. *Линейное пространство L конечномерно $\Longleftrightarrow$ L обладает базисом или $L = \{0\}$.*

Доказательство. $\Longrightarrow$. Пусть L — конечномерное пространство. Если $L \neq \{0\}$, то существует такая конечная линейно независимая система, которая даёт в линейной оболочке всё L, — иными словами, существует базис L. См. по этому поводу результаты предыдущего пункта, в частности, замечание после доказательства теоремы.

$\Longleftarrow$. Если в L существует базис, то L обязательно конечномерно: число элементов любой линейно независимой системы не превосходит $\dim L$. Это сразу следует из леммы о двух системах векторов.

Конечномерность пространства $L = \{0\}$ отмечалась в предыдущем пункте.

Теорема доказана.

Следствие. *Бесконечномерное пространство не имеет базиса.*

Таким образом, конечномерные пространства (по исходному определению — те, в которых нет ни одной бесконечной линейно независимой системы) могут быть охарактеризованы следующим образом.

Прежде всего к ним относится пространство, состоящее только из нуля. Далее, во всех остальных конечномерных пространствах существует (конечный) базис, причём других пространств с базисом нет.

Иными словами, для нетривиальных конечномерных пространств L определено максимальное число $d(L)$ линейно независимых элементов. Любая линейно независимая система с таким количеством элементов является базисом L, в силу чего $d(L) = \dim L$.

Отметим ещё в этом пункте следующий важный результат.

Теорема 3. *Пусть L обладает базисом. Тогда произвольная линейно независимая система может быть дополнена до базиса.*

Доказательство предоставляется читателю в качестве полезного упражнения.

5.5. Действия с векторами в координатах. Изоморфизм линейных пространств и его свойства. Теорема об изоморфизме

Мы уже отмечали (см. пункт 3.5), что линейные пространства $\mathrm{V_n}$ и $\mathrm{R^n}$, $n = 1, 2, 3,$ изоморфны, то есть имеют в некотором смысле одинаковую внутреннюю структуру (последней фразе можно придать точный смысл).

Ниже важное понятие изоморфизма распространяется на линейные пространства произвольной размерности — в том числе и бесконечномерные. Что же касается конечномерных пространств, то это понятие сводит их к цепочке пространств $\mathrm{R^n}, n \in \mathrm{N},$ — любое действительное n-мерное линейное пространство изоморфно $\mathrm{R^n}$.

Прежде всего отметим, что основные действия с векторами n-мерного пространства L легко *осуществляются в координатах в любом фиксированном базисе* e_1, $\ldots$, e_n.

Если $\lambda \in \mathrm{R}$ и $x = \{\alpha_1, \ldots, \alpha_n\}$, $y = \{\beta_1, \ldots, \beta_n\} \in L$, то непосредственно из определения координат следует, что в том же базисе $x + y = \{\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n\}$, $\lambda x = \{\lambda\alpha_1, \ldots, \lambda\alpha_n\}$.

Таким образом, мы действуем с векторами из L как элементами $\mathrm{R^n}$. (Чтобы избежать путаницы, мы используем для векторов L фигурные скобки.)

Дадим теперь следующее определение.

Определение. *Два действительных линейных пространства L_1 и L_2 называются изоморфными, если между их элементами можно установить взаимно-однозначное соответствие, обладающее свойствами:*

1) если $x \longleftrightarrow x', y \longleftrightarrow y'$, то $x + y \longleftrightarrow x' + y'$;

2) если $x \longleftrightarrow x'$, то $\lambda x \longleftrightarrow \lambda x'$.

Здесь $x, y \in L_1,\ x', y' \in L_2$; λ — произвольное число. Это соответствие называется изоморфизмом. Для изоморфных пространств мы будем использовать запись $L_1 \simeq L_2$.

Примеры. 1. $\mathrm{R_n}[t] \simeq \mathrm{R^{n+1}}$. Естественный изоморфизм устанавливается равенством

$$a_0 + a_1 t + \ldots + a_n t^n \ \longleftrightarrow\ (a_0, a_1, \ldots, a_n) \ .$$

2. $M_{mn} \simeq \mathrm{R^k}$ при $k = mn$. В частности, $M_n \simeq \mathrm{R^{n^2}}$. Изоморфизм представляет собой способ оформления двумерного массива в одномерный и может быть осуществлён различными способами.

Упражнение 1. Построить бесконечномерное пространство последовательностей действительных чисел, изоморфное $\mathrm{R}[t]$.

Отметим основные свойства изоморфизма. Пусть $L_1 \simeq L_2$; элементы этих пространств обозначаются, как и ранее, x и x'.

1°. Нулевой вектор L_1 при изоморфизме соответствует нулевому вектору L_2 : $0 \longleftrightarrow 0'$.

2°. Если $x_i \longleftrightarrow x_i'$ и $\lambda_i \in \mathrm{R},\ i = 1, \ldots, n,$ то

$$\lambda_1 x_1 + \ldots + \lambda_k x_k \ \longleftrightarrow\ \lambda_1 x_1' + \ldots + \lambda_k x_k' \ .$$

3°. При изоморфизме линейно независимая система соответствует линейно независимой, а линейно зависимая — линейно зависимой.

Первые два свойства сразу следуют из определения.

Установим ключевое свойство 3°. Если для элементов $x_1, \ldots, x_k \in L_1$ выполнено равенство

$$\lambda_1 x_1 + \ldots + \lambda_k x_k = 0 \ , \tag{4}$$

то для их образов $x_1', \ldots, x_k' \in L_2$ имеет место

$$\lambda_1 x_1' + \ldots + \lambda_k x_k' = 0' \tag{5}$$

— надо воспользоваться предыдущими свойствами и взаимной однозначностью изоморфизма. Ясно, что наличие или отсутствие нулевых коэффициентов в (4) или (5) равнозначно.

Изоморфность является так называемым *отношением эквивалентности* на совокупности всех действительных линейных пространств. Это означает одновременное выполнение следующих условий (убедитесь самостоятельно):

$L \simeq L$ для любого L *(рефлексивность)*;
если $L_1 \simeq L_2$, то $L_2 \simeq L_1$ *(симметричность)*;
если $L_1 \simeq L_2$ и $L_2 \simeq L_3$, то $L_1 \simeq L_3$ *(транзитивность)*.

В связи с этим вся совокупность линейных пространств разбивается на непересекающиеся классы изоморфных пространств (в одном классе содержатся все попарно изоморфные пространства). Как следует из доказываемой ниже теоремы, для конечномерных пространств это разбиение есть в точности разбиение по их размерности, когда в один класс попадают все пространства одинаковой (конечной) размерности.

Теорема. *Два пространства различной размерности не изоморфны. Любые два конечномерных пространства одинаковой размерности являются изоморфными.*

Доказательство. Пусть $\dim L_1 = m > \dim L_2 = n$. Допустим, что при этом $L_1 \simeq L_2$.

Так как любой линейно независимой системе из m элементов L_1 при изоморфизме соответствует аналогичная система в L_2 (свойство 3°), то в L_2 существует линейно независимая система из m векторов. Это противоречит нашему предположению, и первая часть теоремы доказана.

Пусть теперь $\dim L_1 = \dim L_2 = n$. Зафиксируем два базиса в L_1 и L_2 — соответственно $e_1, \ldots, e_n$ и $f_1, \ldots, f_n$.

Рассмотрим соответствие между элементами $x \in L_1$ и $x' \in L_2$, устанавливаемое по следующему правилу:

$$x = \alpha_1 e_1 + \ldots + \alpha_n e_n \;\longleftrightarrow\; x' = \alpha_1 f_1 + \ldots + \alpha_n f_n \ .$$

Иначе говоря, соответствующими друг другу объявляются векторы, имеющие одинаковые координаты в выбранных базисах. Заметим, что тогда $e_i \longleftrightarrow f_i$.

Указанное соответствие является изоморфизмом. Взаимная однозначность сразу следует из единственности координат. Выполнение условий 1) и 2) из определения изоморфизма есть следствие того, что сложение и умножение на число в линейном пространстве может осуществляться в координатах.

Таким образом, $L_1 \simeq L_2$, и теорема полностью доказана.

Следствие. *Пусть* $\dim L = n$. *Тогда* $L \simeq \mathrm{R^n}$.

Замечание. Если в $\mathrm{R^n}$ зафиксировать канонический базис, то изоморфизм из доказательства теоремы будет иметь вид:

$$L \ni x = \{\alpha_1, \ldots, \alpha_n\} \;\longleftrightarrow\; x' = (\alpha_1, \ldots, \alpha_n) \in \mathrm{R^n} \ .$$

Упражнение 2. Убедиться, что первая часть теоремы справедлива и в ситуации, когда ровно одно из пространств является бесконечномерным.

5.6. Матрица перехода от одного базиса к другому, её невырожденность. Изменение координат при изменении базиса

Этот пункт имеет технический характер. Мы покажем, как связаны координаты одного и того же вектора в двух различных базисах.

Пусть $e_1, \ldots, e_n$ и $f_1, \ldots, f_n$ — два базиса n-мерного линейного пространства L.

Определение. *Матрица* $\mathbf{C} = (c_{ij}) \in M_n$, *столбцы которой содержат коэффициенты разложения векторов второго базиса* $f_1, \ldots, f_n$ *по первому базису* $e_1, \ldots, e_n$, *называется матрицей перехода от первого базиса ко второму.*

Таким образом, для $\mathbf{C}$ имеют место равенства:

$$f_1 = c_{11}e_1 + c_{21}e_2 + \ldots + c_{n1}e_n \ ,$$

$$f_2 = c_{12}e_2 + c_{22}e_2 + \ldots + c_{n2}e_n \ ,$$

$$\ldots \quad \ldots \quad \ldots$$

$$f_n = c_{1n}e_1 + c_{2n}e_2 + \ldots + c_{nn}e_n \ ,$$

или

$$f_k = \sum_{j=1}^{n} c_{jk}e_j, \ k = 1, \ldots, n. \tag{6}$$

Матрица $\mathbf{C}$ является невырожденной, то есть $|\mathbf{C}| \neq 0$. Действительно, её столбцы образуют линейно независимую систему в $\mathrm{R^n}$, так как они образованы координатами линейно независимой в L системы $f_1, \ldots, f_n$ (используйте канонический изоморфизм L и $\mathrm{R^n}$, см. предыдущий пункт).

Отсюда, в частности, следует существование обратной матрицы $\mathbf{C}^{-1}$.

Упражнение. Показать, что $\mathbf{C}^{-1}$ *есть матрица перехода от базиса* $f_1, \ldots, f_n$ *к базису* $e_1, \ldots, e_n$.

Пусть далее $\{\xi_1, \ldots, \xi_n\}$ и $\{\xi'_1, \ldots, \xi'_n\}$ есть наборы координат одного и того же вектора $x \in L$ в базисах $e_1, \ldots, e_n$ и $f_1, \ldots, f_n$ соответственно.

Теорема. *В наших обозначениях имеют место равенства:*

$$\begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{pmatrix} = \mathbf{C} \begin{pmatrix} \xi'_1 \\ \xi'_2 \\ \vdots \\ \xi'_n \end{pmatrix} \ , \qquad \begin{pmatrix} \xi'_1 \\ \xi'_2 \\ \vdots \\ \xi'_n \end{pmatrix} = \mathbf{C}^{-1} \begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{pmatrix} \ . \tag{7}$$

Доказательство. Установим левое из двух эквивалентных равенств (7). По определению матрицы перехода (см. (6)) получим:

$$x = \sum_{k=1}^{n} \xi'_k f_k = \sum_{k=1}^{n} \xi'_k \sum_{j=1}^{n} c_{jk}e_j =$$

$$= \sum_{k=1}^{n} \sum_{j=1}^{n} \xi'_k c_{jk} e_j = \sum_{j=1}^{n} (\sum_{k=1}^{n} c_{jk} \xi'_k) e_j$$

(мы поменяли порядок суммирования). С другой стороны, j-я координата x в базисе $e_1, \ldots, e_n$ равна ξ_j. Используя единственность координат, приходим к соотношениям

$$\xi_j = \sum_{k=1}^{n} c_{jk} \xi'_k \ , \ j = 1, \ldots, n \ ,$$

которые в точности соответствуют левому равенству в (7).

Теорема доказана.

6. Подпространства и ранг

Этот раздел является прямым продолжением предыдущего. Мы выделяем его в связи с исключительной важностью соответствующей тематики.

Первые пункты знакомят читателя с основными понятиями и примерами, связанными с *линейными подпространствами.*

От *ранга системы векторов линейного пространства* (то есть размерности их линейной оболочки) мы переходим к *рангу $m \times n$-матрицы* (то есть рангу системы её столбцов в R^{m}) — важнейшему прикладному понятию теории матриц. Фундаментальная теорема из пункта 6.4 означает, что *ранг матрицы можно ввести и через систему строк как элементов* R^{n} — результат от этого не изменится. Этот факт является весьма интересным.

6.1. Подпространства линейного пространства. Примеры. Ранг и база системы векторов

Пусть L — произвольное линейное пространство.

Определение. *Непустое подмножество $L_1 \subset L$ называется линейным подпространством, если L_1 замкнуто относительно операций сложения и умножения на число:*

1) для любых $x, y \in L_1 \quad x + y \in L_1$;

2) для любого $x \in L_1$ и любого $\alpha \in \mathrm{R} \quad \alpha x \in L_1$.

Иначе говоря, L_1 есть линейное подпространство L, если L_1 *само является линейным пространством* относительно операций, введённых в более широком множестве L.

Условия 1) – 2) можно объединить, потребовав, чтобы для всех $x, y \in L_1$ и $\alpha, \beta \in \mathrm{R}$ выполнялось $\alpha x + \beta y \in L_1$; это приводит к эквивалентному определению.

Смысл этих условий состоит в том, что произвольная линейная комбинация любого числа элементов L_1 также принадлежит L_1, то есть для $x_1, \ldots, x_k \in L_1$ имеет место включение $\mathrm{lin}(x_1, \ldots, x_k) \subset L_1$.

Особо отметим, что $0 \in L_1$ (это сразу следует из второго условия при $\alpha = 0$) .Таким образом, все линейные подпространства одного пространства L обязательно содержат общий элемент, а именно нулевой вектор L. Подмножество, не содержащее нуля, линейным подпространством не является.

Как правило, проверка того, что данное подмножество $L_1 \subset L$ есть линейное подпространство, является весьма простой.

На линейные подпространства переносятся все понятия, введённые выше для линейных пространств (конечномерность и бесконечномерность, базис, размерность и т.д.).

Примеры и упражнения.

1. Линейными подпространствами являются $\{0\}$ и всё L. Они называются *несобственными подпространствами* L; все остальные подпространства называются *собственными*.

2. Собственные подпространства V_3 — прямые и плоскости, проходящие через т.О; для них соответственно $\dim L_1 = 1$ и $\dim L_1 = 2$. Других собственных подпространств в V_3 нет.

3. Совокупность L_1 n-мерных векторов $x = (x_1, \ldots, x_n)$ таких, что

$$x_1 + \ldots + x_n = 0$$

(в этой записи x_i числа), образует линейное подпространство в $L = \mathrm{R^n}$; как будет показано, $\dim L_1 = n - 1$.

Совокупность тех $x \in \mathrm{R^n}$, для которых $\sum x_i = 1$, линейным подпространством не является (почему?).

4.(*Обобщение.*) Пусть $\mathbf{A} \in M_{m,n}$ — фиксированная матрица. Обозначим через L_1 подмножество пространства $L = \mathrm{R^n}$, состоящее из всех $x = (x_1, \ldots, x_n)$ таких, что

$$\mathbf{A} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{1}$$

Из свойств умножения матриц следует, что L_1 является линейным подпространством. Мы будем говорить о нём как о *подпространстве, задаваемом системой линейных однородных уравнений (или подпространстве решений системы (1))*, см. подробнее пункт 6.6.

Предыдущий пример соответствует ситуации

$$m = 1,\ \mathbf{A} = \begin{pmatrix} 1 & 1 & \ldots & 1 \end{pmatrix}.$$

5. Совокупности многочленов $\mathrm{R_j}[t],\ j = 0, 1, 2, \ldots, n-1,$ степени $\leqslant j$ составляют расширяющуюся (по включению) цепочку собственных линейных подпространств одного пространства $\mathrm{R_n}[t]$. Их размерности равны $1, 2, 3, \ldots, n$.

Совокупность многочленов *степени ровно* j является линейным подпространством лишь при $j = 0$ (почему?).

6. Каждое из функциональных пространств $C^\infty[a,b]$, $C^k[a,b]$, $C[a,b]$ является бесконечномерным подпространством пространства $B[a,b]$ ограниченных на $[a,b]$ функций.

Совокупность функций $f : [a,b] \longrightarrow \mathrm{R}$, удовлетворяющих условию

$$|f(x)| \leqslant 1,\ a \leqslant x \leqslant b,$$

линейным подпространством $B[a,b]$ не является (подумайте, почему).

7. Каждое из пространств последовательностей l_1, c_0, c является бесконечномерным линейным подпространством пространства $b = l_\infty$ ограниченных последовательностей.

Совокупность последовательностей $x = (x_i)_{i=1}^{\infty}$ таких, что

$$\lim_{i\to\infty} x_i = \varrho,$$

является линейным подпространством в c или в b лишь при $\varrho = 0$ (подумайте, почему).

8. Особо выделим следующий важный пример.

Пусть L — произвольное линейное пространство, $x_1, \ldots, x_k$ — произвольные элементы L. Тогда, очевидно, их линейная оболочка $L_1 := \operatorname{lin}(x_1, \ldots, x_k)$ является конечномерным линейным подпространством L; ясно, что $\dim L_1 \leqslant k$.

Размерность подпространства $L_1 = \operatorname{lin}(x_1, \ldots, x_k)$ называется *рангом системы векторов* $x_1, \ldots, x_k$, а базис L_1, состоящий из каких-то (возможно, не всех) векторов x_i, называется *базой системы* $x_1, \ldots, x_k$.

Ясно, что ранг системы векторов равен числу элементов в любой базе этой системы (то есть максимальному числу линейно независимых векторов этой системы).

Для обозначения ранга здесь и ниже используется запись $\operatorname{rg}(\cdot)$. Итак, по нашему определению,

$$\operatorname{rg}(x_1, \ldots, x_k) := \dim \operatorname{lin}(x_1, \ldots, x_k).$$

Способ *задания линейного подпространства в виде линейной оболочки*, отмеченный в последнем примере, является вторым основным способом задания подпространства. Естественно, при таком подходе удобнее выбирать линейно независимые векторы x_i.

Замечание. В дальнейшем мы убедимся, что два основных способа задания линейного подпространства в R^{n}, то есть задание его в виде линейной оболочки и задание с помощью системы линейных однородных уравнений, *являются в некотором смысле двойственными.*

6.2. Сумма и пересечение подпространств. Теорема о размерностях суммы и пересечения

По двум подпространствам одного и того же линейного пространства можно построить новые подпространства — сумму и пересечение исходных.

Определение. *Сумма и пересечение подпространств L_1, L_2 линейного пространства L определяются следующим образом:*

$$L_1 + L_2 := \{x \in L :\ x = x_1 + x_2,\ x_i \in L_i,\ i = 1, 2\ \}\ ,$$

$$L_1 \bigcap L_2 := \{x \in L :\ x \in L_i,\ i = 1, 2\ \}\ .$$

Таким образом, $L_1 + L_2$ состоит из всевозможных сумм векторов $x_1 + x_2$, где $x_1 \in L_1$, а $x_2 \in L_2$ (мы можем их складывать, так как $x_i \in L$). Пересечение подпространств определяется обычным способом. Как мы покажем ниже, эти операции не выводят нас за пределы класса линейных подпространств L.

Читателю рекомендуется подумать над примерами в ситуации $L = \mathrm{V}_3$. Убедитесь также, что множество $L_1 \bigcup L_2$, вообще говоря, не является линейным подпространством L. По этой причине привычное объединение множеств заменяется в этом разделе более тонкой операцией $L_1 + L_2$.

Отметим здесь очевидные, но важные включения

$$L_1 \bigcap L_2 \ \subset \ L_1, L_2 \ \subset \ L_1 + L_2 \ .$$

Докажем теперь основное утверждение этого пункта. Классическая формула (2) с соотношением между размерностями суммы и пересечения получена Г. Грассманом (H. Grassman, 1862).

Теорема. *$L_1 + L_2$, $L_1 \bigcap L_2$ — линейные подпространства L. Если основное пространство L конечномерно, то имеет место равенство*

$$\dim(L_1 + L_2) + \dim L_1 \bigcap L_2 = \dim L_1 + \dim L_2 \ . \tag{2}$$

Доказательство. Первую часть теоремы докажем лишь для суммы подпространств; рассмотрение пересечения предоставляется читателю.

Пусть $x, y \in L_1 + L_2,\ \lambda \in \mathrm{R}$. Тогда

$$x = x_1 + x_2,\ y = y_1 + y_2$$

с некоторыми $x_i, y_i \in L_i$, $i = 1, 2$. Из этих равенств нетрудно получить представления

$$x + y = (x_1 + y_1) + (x_2 + y_2),\ \lambda x = \lambda x_1 + \lambda x_2,$$

первые слагаемые которых принадлежат L_1, а вторые — L_2. Здесь используется то, что каждое L_i является линейным подпространством.

Поэтому $x + y, \lambda x \in L_1 + L_2$, то есть $L_1 + L_2$ — линейное подпространство L.

Получим теперь равенство (2). Будем считать, что каждое из подпространств L_i имеет положительную размерность; случай $L_1 = \{0\}$ тривиален.

Пусть $\dim L_1 \bigcap L_2 = k$. Рассмотрим сначала ситуацию $k > 0$.

Дополним базис пересечения $e_1, \ldots, e_k$ до базисов L_1 и L_2 векторами $f_1, \ldots, f_l$ и $g_1, \ldots, g_m$ соответственно (каждое из этих дополнений может отсутствовать). В наших обозначениях $\dim L_1 = k + l$, $\dim L_2 = k + m$.

Покажем, что объединённая система

$$f_1, \ldots, f_l, e_1, \ldots, e_k, g_1, \ldots, g_m \tag{3}$$

является базисом $L_1 + L_2$. Это будет означать, что $\dim(L_1 + L_2) = k + l + m$, и равенство (2) примет вид тождества

$$(k + l + m) + (k) = (k + l) + (k + m).$$

Очевидно, что каждый вектор из $L_1 + L_2$ есть линейная комбинация векторов (3). Поэтому достаточно доказать их линейную независимость.

Пусть

$$\sum \alpha_i f_i + \sum \beta_j e_j + \sum \gamma_s g_s = 0 \ .$$

Тогда вектор

$$z := \sum \alpha_i f_i + \sum \beta_j e_j = -\sum \gamma_s g_s$$

принадлежит одновременно и L_1, и L_2. Значит, $z \in L_1 \bigcap L_2$. Но тогда z есть линейная комбинация векторов e_j. Мы приходим к равенству

$$-\sum \gamma_s g_s = \sum \delta_j e_j \ .$$

Линейная независимость векторов e_j, g_s (они образуют базис L_2) даёт

$$\gamma_s = \delta_j = 0 \ , s = 1, \ldots, m, \ j = 1, \ldots, k \ .$$

Подставляя значения γ_s в самое первое из этой цепочки равенств, приходим к соотношению

$$\sum \alpha_i f_i + \sum \beta_j e_j = 0 \ .$$

Теперь следует воспользоваться линейной независимостью векторов f_i, e_j, образующих базис L_1.

Таким образом, для всех значений индексов

$$\alpha_i = \beta_j = \gamma_s = 0 \ ,$$

и линейная независимость векторов системы (3) установлена. Это завершает доказательство в случае $k > 0$.

Рассмотрим более сжато ситуацию $k = \dim L_1 \bigcap L_2 = 0$. В этом случае $L_1 \bigcap L_2 = \{0\}$. Пусть $\dim L_1 = l, \ \dim L_2 = m$ и соответствующие базисы подпространств образуют векторы $f_1, \ldots, f_l$ и $g_1, \ldots, g_m$. Нетрудно показать, что объединение этих базисов, то есть система

$$f_1, \ldots, f_l, \ g_1, \ldots, g_m$$

есть базис в $L_1 + L_2$. В доказательстве нуждается лишь линейная независимость последней системы.

Равенство

$$\sum \alpha_i f_i + \sum \gamma_s g_s = 0$$

означает, что

$$z := \sum \alpha_i f_i = -\sum \gamma_s g_s \in L_1 \bigcap L_2 \ ,$$

то есть $z = 0$. Отсюда следует, что все числа α_i и γ_s равны нулю.

Теорема доказана.

Операции суммы и пересечения могут быть очевидным образом перенесены на любое число $k > 2$ линейных подпространств $L_1, \ldots, L_k$ одного и того же пространства L. Мы предоставляем читателю дать соответствующие определения, а заодно подумать над возможными аналогами равенства (2).

6.3. Прямая сумма подпространств. Теорема о прямой сумме

Пусть L — произвольное линейное пространство, L_1, L_2 — два его подпространства. Если их сумма $S := L_1 + L_2$ обладает одним из нескольких эквивалентных свойств, мы будем говорить, что эта сумма является прямой.

Итак, прямая сумма подпространств — это результат их сложения при выполнении некоторых дополнительных условий. Исходным мы будем считать следующее определение.

Определение. *Сумма $S = L_1 + L_2$ называется прямой, если для любого $x \in S$ представление $x = x_1 + x_2$, $x_1 \in L_1$, $x_2 \in L_2$, является единственным.*

Прямая сумма в этом тексте обозначается $S = L_1 \oplus L_2$ (другое стандартное обозначение: $S = L_1 \dot{+} L_2$).

Примеры. 1. Пусть $L = \mathrm{V}_3$, L_1 — вертикальная прямая, L_2 — горизонтальная плоскость (рассматриваемые стандартным образом как совокупности геометрических векторов). Тогда, очевидно,

$$L_1 \oplus L_2 = \mathrm{V}_3. \tag{4}$$

Обратим внимание на то, что равенства, подобные (4), объединяют сразу два утверждения (здесь: сумма является прямой и результат есть всё V_3).

2. Пусть в предыдущей ситуации L_1 — вертикальная плоскость. Тогда в (4) знак $\oplus$ мы должны заменить на обычный $+$. Для каждого $\vec{x} \in \mathrm{V}_3$ (в том числе для $\vec{0}$), как нетрудно убедиться, существует бесконечно много разложений по подпространствам L_1 и L_2, в связи с чем их сумма не является прямой.

3. Простой пример прямой суммы в R^{n} дают подпространства

$$L_1 := \{(\alpha_1, 0, \ldots, 0)\}\ , L_2 := \{(0, \alpha_2, \ldots, \alpha_n)\}\ .$$

Ясно, что $L_1 \oplus L_2 = \mathrm{R}^{\mathrm{n}}$.

Этот пример построен по аналогии с примером 1.

Докажем теперь основную теорему о прямой сумме, дающую целый ряд условий, эквивалентных исходному определению.

Теорема. *Сумма $S = L_1 + L_2$ является прямой, то есть $S = L_1 \oplus L_2$, тогда и только тогда, когда выполнено любое из следующих эквивалентных условий.*

1°. $L_1 \bigcap L_2 = \{0\}$.

2°. $\dim(L_1 + L_2) = \dim L_1 + \dim L_2$.

3°. *Если $f_1, \ldots, f_l$ — базис L_1, $g_1, \ldots, g_m$ — базис L_2, то $f_1, \ldots, f_l, g_1, \ldots, g_m$ — базис $L_1 + L_2$.*

4°. *Единственность разложения по L_1 и L_2 имеет место для нулевого вектора: если $x_1 + x_2 = 0$, $x_1 \in L_1$, $x_2 \in L_2$, то обязательно $x_1 = x_2 = 0$.*

Доказательство. Реализуем следующую схему: 1° эквивалентно каждому из условий 2°, 3°, 4°; далее, 4° эквивалентно исходному определению этого пункта.

Эквивалентность $1^\circ \iff 2^\circ$ есть прямое следствие теоремы пункта 6.2. Кроме равенства (2) надо использовать лишь, что $\dim W = 0$ лишь для $W = \{0\}$.

$1^\circ \iff 3^\circ$. Следует из той же теоремы. По поводу направления $1^\circ \Longrightarrow 3^\circ$ см. конец её доказательства для ситуации $L_1 \bigcap L_2 = \{0\}$.

$1^\circ \Longrightarrow 4^\circ$. Пусть $L_1 \bigcap L_2 = \{0\}$ и $x_1 + x_2 = 0$ для $x_i \in L_i,\ i = 1, 2$. Тогда $x_1 = -x_2 \in L_1 \bigcap L_2,$ поэтому $x_1 = x_2 = 0$.

$1^\circ \Longleftarrow 4^\circ$. Пусть $x \in L_1 \bigcap L_2$. Тогда равенство $x + (-x) = 0$ есть разложение для нуля по L_1 и L_2 . Если же выполнено 4°, то обязательно имеем $x = 0$, что даёт 1°.

Покажем теперь, что при выполнении 4° сумма S является прямой по основному определению. Пусть для произвольного $x \in S$ имеется два каких-то разложения по L_i:

$$x = x_1 + x_2,\ x = y_1 + y_2;\ x_i, y_i \in L_i,\ i = 1, 2\ .$$

Из последнего равенства легко получается разложение для нуля:

$$0 = (x_1 - y_1) + (x_2 - y_2)\ .$$

Если же выполнено условие 4°, то обязательно $x_1 = y_1,\ x_2 = y_2,$ то есть оба представления для x совпадают. В силу произвольности $x \in S$ это означает, что сумма S является прямой.

Остаётся заметить, что условие 4° является более слабым, чем условие исходного определения (в котором единственность представления требуется *для любого, а не только нулевого вектора из* S). Поэтому четвёртое условие эквивалентно определению.

Теорема доказана.

Из условий теоремы наиболее просто выглядит 1°, хотя эти условия могут эффективно комбинироваться. В качестве интересной иллюстрации приведём следующее известное утверждение (см. упражнение пункта 2.2).

Утверждение. *Каждая матрица* $\mathbf{A} \in M_n$ *единственным образом представляется в виде суммы симметричной* $\mathbf{B}$ $(b_{ji} = b_{ij})$ *и кососимметричной* $\mathbf{C}$ $(c_{ji} = -c_{ij})$ *матриц.*

Доказательство. Пусть S и T обозначают совокупности соответственно симметричных и кососимметричных матриц порядка n. Очевидно, каждая из них является линейным подпространством M_n.

Прежде всего заметим, что $S \bigcap T = \{\mathbf{0}\}$ (если матрица одновременно является симметричной и кососимметричной, то она является нулевой). Для нас важно, что в силу условия 1° теоремы *сумма* S *и* T *является прямой.*

Используя общий вид элементов этих подпространств, можно показать, что

$$\dim S = \frac{n(n+1)}{2},\ \dim T = \frac{n(n-1)}{2}\ .$$

Так как их сумма является прямой, то в соответствии с условием 2°

$$\dim(S \oplus T) = \dim S + \dim T = \frac{n(n+1)}{2} + \frac{n(n-1)}{2} = n^2 = \dim M_n\ .$$

Единственное подпространство в M_n, имеющее размерность n^2, это всё M_n. Таким образом, мы имеем равенство

$$M_n = S \oplus T. \tag{5}$$

Остаётся заметить, что (5) равносильно нашему утверждению (надо применить исходное определение). Это завершает доказательство.

Определение прямой суммы по аналогии переносится на произвольное число $k > 2$ подпространств L_i одного линейного пространства L. Именно, *сумма* $U = L_1 + \ldots + L_k$ *называется прямой*, если для каждого $x \in U$ имеется *единственное* представление

$$x = x_1 + \ldots + x_k,\ x_i \in L_i,\ i = 1, \ldots, k.$$

Можно показать, что сумма k подпространств является прямой, если выполнено любое из эквивалентных условий, аналогичных $2°, 3°, 4°$ (сформулируйте их самостоятельно). Что же касается $1°$, то с ним нужно быть более аккуратным.

Упражнение 1. Привести пример трёх линейных подпространств V_3 *таких, что* $L_1 \bigcap L_2 \bigcap L_3 = \{\vec{0}\}$, *но сумма* $L_1 + L_2 + L_3$ *не является прямой.*

Упражнение 2. Сформулируйте и докажите критерий прямой суммы по типу условия $1°$.

Наконец, специально отметим, что основное определение и некоторые результаты этого пункта переносятся без изменения на бесконечномерный случай.

Упражнение 3. Пусть L_1 *— подпространство* $C[0,1]$, *состоящее из тех функций* $x(t)$, *для которых* $x(1) = 0$. *Показать, что* L_1 *бесконечномерно, и найти такое подпространство* $L_2 \subset C[0,1]$, *что*

$$C[0,1] = L_1 \oplus L_2.$$

6.4. Ранг матрицы. Теорема о ранге. Методы вычисления и свойства ранга матрицы

Пусть $\mathbf{A} = (a_{ij})$ — произвольная матрица порядка $m \times n$. Мы свяжем с ней некоторое целое неотрицательное число, называемое рангом $\mathbf{A}$ и обозначаемое ниже $\mathrm{rg}(\mathbf{A})$. Отметим также другие стандартные обозначения — $\mathrm{rang}(\mathbf{A})$ или $\mathrm{rank}(\mathbf{A})$.

Ранг матрицы — фундаментальное понятие, активно используемое в приложениях. Вот почему материал этого пункта является очень важным.

Обозначим через $X_1, \ldots, X_n$ столбцы, а через $Y_1, \ldots, Y_m$ — строки $\mathbf{A}$. Ясно, что $X_i \in \mathrm{R}^{\mathrm{m}}$, $Y_j \in \mathrm{R}^{\mathrm{n}}$. Мы будем рассматривать линейные оболочки совокупностей столбцов и строк в соответствующих пространствах:

$$\mathrm{lin}(X_1, \ldots, X_n) \subset \mathrm{R}^{\mathrm{m}},\ \mathrm{lin}(Y_1, \ldots, Y_m) \subset \mathrm{R}^{\mathrm{n}}.$$

Из результатов этого пункта следует, что размерности этих двух подпространств совпадают (весьма неожиданный и нетривиальный факт!); их общее значение и называется рангом $\mathbf{A}$.

В нашем подходе *основное определение связано со столбцами матрицы.*

Определение. *Рангом матрицы* $\mathbf{A}$ *называется ранг системы её столбцов как элементов* R^{m}*, то есть размерность линейной оболочки системы столбцов* $X_1, \ldots, X_n$:

$$\mathrm{rg}(\mathbf{A}) := \mathrm{rg}(X_1, \ldots, X_n) = \dim \mathrm{lin}(X_1, \ldots, X_n).$$

Проще говоря, ранг матрицы равен *максимальному числу линейно независимых столбцов этой матрицы.* В этом варианте надо добавить, что ранг нулевой матрицы считается равным 0.

Ключевым результатом, гарантирующим отмеченную выше инвариантность при переходе к строкам, является следующая *теорема о ранге матрицы.*

Теорема. *Ранг матрицы равен максимальному порядку* r *отличного от нуля минора этой матрицы.*

(Для нулевой матрицы считаем $r = 0$.)

Доказательство. Пусть, как и ранее, $\mathbf{A} \in M_{m,n}$. В случае $r = 0$ матрица $\mathbf{A}$ является нулевой и для неё $\mathrm{rg}(\mathbf{A}) = 0 = r$. Пусть $r \geqslant 1$, то есть $\mathbf{A} \neq \mathbf{0}$.

Без ограничения общности можно считать, что отличным от нуля минором порядка r является минор Δ, стоящий в первых r строках и первых r столбцах $\mathbf{A}$.

Действительно, перестановки столбцов или строк матрицы не меняют связанного с ней числа r (по свойствам определителя). Эти же действия не меняют $\mathrm{rg}(\mathbf{A})$ как размерности линейной оболочки столбцов, так как сводятся либо к изменению порядка столбцов, либо к переобозначению их компонент.

Итак, считаем, что главный минор Δ порядка r матрицы $\mathbf{A}$ не равен 0, а все миноры большего порядка равны 0. Покажем, что тогда

1) первые r столбцов $X_1, \ldots, X_r$ матрицы $\mathbf{A}$ линейно независимы;

2) каждый столбец X_l при $l > r$ есть их линейная комбинация.

Это будет означать, что $X_1, \ldots, X_r$ образуют базис линейной оболочки всех столбцов $\mathbf{A}$, то есть гарантирует равенство $\mathrm{rg}(\mathbf{A}) = r$.

Линейная независимость $X_1, \ldots, X_r$ сразу следует из свойств определителя. Если эта система была бы линейно зависимой, то таковой была бы и система столбцов длины r, составляющих Δ; таким образом, мы имели бы $\Delta = 0$.

Покажем, что $X_l \in \mathrm{lin}(X_1, \ldots, X_r)$ при всех $l > r$. Для этого рассмотрим так называемое *окаймление* минора Δ с помощью элементов i-й строки, $i = 1, \ldots, m$, и l-го столбца, то есть определитель порядка $r + 1$

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

Определитель D имеет две одинаковые строки (в случае $i \leqslant r$) или является минором матрицы $\mathbf{A}$ порядка $r + 1$ (в случае $i > r$). Поэтому $D = 0$.

Запишем разложение D по последней строке. Алгебраическое дополнение к элементу a_{il}, очевидно, равно Δ. Алгебраические дополнения к другим элементам этой

строки не зависят от i и обозначаются $A_1, \ldots, A_r$. Таким образом, при всех $i = = 1, \ldots, m$

$$a_{i1}A_1 + \ldots + a_{ir}A_r + a_{il}\Delta = 0,$$

или, так как $\Delta \neq 0$,

$$a_{il} = -\frac{A_1}{\Delta}a_{i1} - \ldots - \frac{A_r}{\Delta}a_{ir}. \tag{6}$$

Так как коэффициенты в левой части равенства (6) не зависят от i, оно равносильно равенству для столбцов

$$X_l = -\frac{A_1}{\Delta}X_1 - \ldots - \frac{A_r}{\Delta}X_r.$$

Поэтому $X_l \in \mathrm{lin}(X_1, \ldots, X_r)$. В связи с предыдущим $\mathrm{rg}(\mathbf{A}) = r$.

Теорема доказана.

Замечание. Минор максимального порядка r, отличный от нуля, называют *базисным минором матрицы* $\mathbf{A}$. Мы фактически доказали, что столбцы $\mathbf{A}$, соответствующие любому базисному минору, образуют базис линейной оболочки всех столбцов, в связи с чем $\mathrm{rg}(\mathbf{A}) = r$. В такой форме утверждение иногда называют теоремой о базисном миноре.

Следствие. *Для каждой* $\mathbf{A} \in M_{m,n}$ $\quad \mathrm{rg}(\mathbf{A^T}) = \mathrm{rg}(\mathbf{A})$.

Действительно, число r из условия теоремы не меняется при транспонировании матрицы. Это связано с соответствующим свойством определителя.

Результат следствия означает, что исходное определение ранга матрицы можно дать через систему строк $Y_1, \ldots, Y_m$. Иными словами,

$$\mathrm{rg}(X_1, \ldots, X_n) = \mathrm{rg}(Y_1, \ldots, Y_m) = \mathrm{rg}(\mathbf{A}).$$

Основной способ вычисления ранга матрицы связан с приведением её к ступенчатому виду с помощью элементарных преобразований над строками, то есть является *методом Гаусса,* см. раздел 1. Он обосновывается следующими обстоятельствами.

1) Ранг матрицы не меняется при элементарных преобразованиях строк.

2) Ранг ненулевой ступенчатой матрицы равен числу её ступеней.

Первый факт связан с очевидными равенствами:

$$\mathrm{lin}(Y_2, Y_1, Y_3, \ldots, Y_m) = \mathrm{lin}(Y_1, Y_2, Y_3, \ldots, Y_m),$$
$$\mathrm{lin}(cY_1, Y_2, \ldots, Y_m) = \mathrm{lin}(Y_1, Y_2, \ldots, Y_m),\ c \neq 0,$$
$$\mathrm{lin}(Y_1 + Y_2, Y_2, Y_3, \ldots, Y_m) = \mathrm{lin}(Y_1, Y_2, Y_3, \ldots, Y_m)$$

(мы ограничиваемся преобразованиями первых строк). В силу совпадения этих линейных оболочек равны и их размерности, то есть ранги соответствующих матриц.

Второе обстоятельство связано с тем, что строки, образующие ступени, линейно независимы; остальные же строки ступенчатой матрицы, если они есть, являются нулевыми.

Упражнение 1. Вывести утверждение 2) из доказанной выше теоремы.

Другим методом вычисления ранга матрицы является *метод окаймления миноров*.

Для определения ранга достаточно найти число r из условия теоремы — максимальный порядок минора, отличного от 0. Полный перебор всех миноров является весьма трудоёмким. Однако, как следует из доказательства теоремы, мы можем ограничиться лишь минорами, окаймляющими данный ненулевой (то есть содержащими его в качестве подминора). Таким образом мы повышаем порядок ненулевого минора, насколько это возможно. Если все окаймляющие миноры равны 0 (или их не существует), то значение r найдено, и процесс завершается.

Пример. Вычислим с помощью метода окаймления миноров ранг матрицы

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

Взяв в качестве минора первого порядка элемент a_{53}, строим последовательности миноров $D_i \neq 0$, D_i окаймляет D_{i-1}, и чисел r_i – порядков D_i. Первые значения

$$D_1 := a_{53} = -1 \neq 0,\ r_1 := 1; \quad D_2 := \begin{vmatrix} 1 & 2 \\ -1 & 4 \end{vmatrix} = 6 \neq 0,\ r_2 := 2 .$$

Далее рассматриваем девять миноров третьего порядка, *окаймляющих* D_2. Три из них стоят в столбцах с номерами 1, 3, 4:

$$\begin{vmatrix} 4 & -8 & 2 \\ 4 & 1 & 2 \\ 8 & -1 & 4 \end{vmatrix}, \qquad \begin{vmatrix} 8 & -7 & 4 \\ 4 & 1 & 2 \\ 8 & -1 & 4 \end{vmatrix}, \qquad \begin{vmatrix} 4 & -5 & 2 \\ 4 & 1 & 2 \\ 8 & -1 & 4 \end{vmatrix}.$$

Три минора располагаются в столбцах с номерами 2, 3, 4:

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

Наконец, в столбцах с номерами 3, 4, 5 располагаются миноры

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

Первый ненулевой из этих девяти миноров был бы принят нами за D_3. Однако, все они равны нулю (вычисление предоставляется читателю; впрочем, каждый из первых шести содержит пропорциональные столбцы). Процесс, таким образом, заканчивается, что даёт нам $\mathrm{rg}(\mathbf{A}) = r_2 = 2$.

Одновременно мы выяснили, что минор D_2 является базисным, то есть третий и четвёртый столбцы $\mathbf{A}$ образуют базис линейной оболочки всех столбцов $\mathbf{A}$.

Упражнение 2. Найти ранг матрицы

$$\begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}$$

в зависимости от параметров $a, b, c, d \in \mathrm{R}$.

Трудоёмкость метода Гаусса вычисления ранга матрицы $\mathbf{A} \in M_n$ совпадает с трудоёмкостью приведения к ступенчатому виду, то есть *равна* $O(n^3)$, см. пункт 1.5.

Упражнение 3. Оценить трудоёмкость метода окаймления миноров для $\mathbf{A} \in M_n$.

В заключение этого пункта дополним уже отмеченные свойства ранга матрицы некоторыми другими. Безусловно, этот список может быть расширен.

1°. Для $\mathbf{A} \in M_{m,n}$ $\operatorname{rg}(\mathbf{A}) \leqslant \min(m, n)$.

2°. Пусть $\mathbf{A} \in M_n$. $\operatorname{rg}(\mathbf{A}) = n \iff |\mathbf{A}| \neq 0$.

3°. Пусть $\mathbf{A} \in M_n$. Матрица $\mathbf{A}$ обратима $\iff \operatorname{rg}(\mathbf{A}) = n$.

4°. Если $\mathbf{AB}$ существует, то $\operatorname{rg}(\mathbf{AB}) \leqslant \min(\operatorname{rg}(\mathbf{A}), \operatorname{rg}(\mathbf{B}))$.

5°. Пусть $\mathbf{B} \in M_n$ и $\operatorname{rg}(\mathbf{B}) = n$. Если $\mathbf{AB}$ существует, то $\operatorname{rg}(\mathbf{AB}) = \operatorname{rg}(\mathbf{A})$. То же — для произведения $\mathbf{BA}$.

6°. Для $\mathbf{A} \in M_{m,k}, \mathbf{B} \in M_{k,n}$ $\operatorname{rg}(\mathbf{A}) + \operatorname{rg}(\mathbf{B}) \leqslant \operatorname{rg}(\mathbf{AB}) + k$.

7°. Для $\mathbf{A}, \mathbf{B} \in M_{m,n}$ $\operatorname{rg}(\mathbf{A} + \mathbf{B}) \leqslant \operatorname{rg}(\mathbf{A}) + \operatorname{rg}(\mathbf{B})$.

8°. Если все произведения существуют, то

$$\operatorname{rg}(\mathbf{AB}) + \operatorname{rg}(\mathbf{BC}) \leqslant \operatorname{rg}(\mathbf{B}) + \operatorname{rg}(\mathbf{ABC}) \ .$$

Свойства 1° – 2° следуют непосредственно из определения или из теоремы о ранге матрицы. Свойство 3° равносильно 2° (связь обратимости и невырожденности, см. пункт 4.8).

Доказательство свойств $4^\circ - 5^\circ$ дано в учебнике А.Г. Куроша [16, с. 101].

Интересные соотношения $6^\circ - 8^\circ$ приводятся, например, в монографии Р. Хорна и Ч. Джонсона [26, с. 25]. Наиболее тонкое из них неравенство 8° называется *неравенством Фробениуса* — по имени математика Георга Фробениуса (G. Frobenius, 1849 – 1917).

6.5. Применение понятия ранга к анализу систем линейных уравнений. Теорема Кронекера – Капелли. Критерий определённости

С привлечением понятия ранга матрицы нетрудно дать необходимые и достаточные условия совместности и определённости произвольной системы линейных уравнений.

Отметим, что практическая проверка этих условий фактически совпадает с прямым ходом метода Гаусса решения системы, см. раздел 1.

Пусть дана система m уравнений с n неизвестными $x_1, \ldots, x_n$ и матрицей коэффициентов $\mathbf{A} = (a_{ij}) \in M_{m,n}$:

$$\begin{array}{ccccccc} a_{11}x_1 & + & \ldots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & \ldots & + & a_{2n}x_n & = & b_2 \\ \ldots & & \ldots & & \ldots & & \ldots \\ a_{m1}x_1 & + & \ldots & + & a_{m1}x_n & = & b_m \end{array} \tag{7}$$

Пусть $X_1, \ldots, X_n$ — столбцы матрицы $\mathbf{A}$, $\mathbf{b}$ — столбец свободных членов. Обозначим через $\mathbf{A}|\mathbf{b}$ расширенную матрицу системы (7). Ясно, что всегда

$$\operatorname{rg}(\mathbf{A}) \leqslant \operatorname{rg}(\mathbf{A}|\mathbf{b}) \leqslant \operatorname{rg}(\mathbf{A}) + 1.$$

Сначала ответим на *вопрос о совместности системы (7).*

Приводимое ниже утверждение называется *теоремой Кронекера – Капелли.* У немецкого математика Леопольда Кронекера (L. Kronecker, 1823 – 1891) эта теорема содержится в его лекциях, читавшихся в Берлинском университете в 1883 – 1891 гг. Формулировку теоремы с использованием термина *ранг матрицы*, как считается, впервые дал А. Капелли (A. Capelli, 1892).

Теорема 1. *Система (7) является совместной тогда и только тогда, когда*

$$\operatorname{rg}(\mathbf{A}|\mathbf{b}) = \operatorname{rg}(\mathbf{A}). \tag{8}$$

Доказательство является совсем несложным.

Пусть система (7) совместна. Тогда для чисел x_i, составляющих любое частное решение, выполняется

$$x_1X_1 + \ldots + x_nX_n = b. \tag{9}$$

Это означает, что $b \in \operatorname{lin}(X_1, \ldots, X_n)$, в связи с чем

$$\operatorname{lin}(X_1, \ldots, X_n, b) = \operatorname{lin}(X_1, \ldots, X_n).$$

Поэтому равны и размерности этих линейных оболочек (ранг матрицы есть размерность линейной оболочки её столбцов), что даёт равенство (8).

Пусть имеет место (8). Тогда любая база системы $X_1, \ldots, X_n$ является базой расширенной системы $X_1, \ldots, X_n, b$. Поэтому b есть линейная комбинация некоторых, а значит, и всех X_i. Это означает, что для некоторых чисел x_i выполнено равенство (9). Таким образом, система уравнений (7) совместна — она имеет решение $x_1, \ldots, x_n$.

Теорема доказана.

Второе утверждение этого пункта содержит *критерий определённости системы (7).*

Теорема 2. *Система линейных уравнений (7) является определённой тогда и только тогда, когда выполняются одновременно два равенства*

$$\mathrm{rg}(\mathbf{A}|\mathbf{b}) = \mathrm{rg}(\mathbf{A}) = n. \tag{10}$$

Доказательство. Пусть система (7) является определённой (то есть имеет ровно одно решение). Тогда она является совместной, что даёт с учётом теоремы 1 левое равенство в (10).

Напомним, что определённой является лишь та совместная система, матрица которой может быть приведена элементарными преобразованиями строк к ступенчатой форме с n ступенями, см. теорему 3 пункта 1.4. Ранг такой ступенчатой матрицы равен n; он совпадает с рангом исходной матрицы $\mathbf{A}$ (ранг матрицы не меняется при элементарных преобразованиях строк). Это гарантирует правое равенство в (10).

Предположим, что выполнены оба равенства (10). Левое из них обеспечивает совместность системы, а правое (при условии выполнения левого) — её определённость. Действительно, если $\mathrm{rg}(\mathbf{A}) = n$, то соответствующая ступенчатая форма будет иметь ровно n ступеней. Остаётся использовать те факты, которые мы отметили выше.

Теорема доказана.

Упражнение. Привести примеры, показывающие, что выполнение лишь одного из двух равенств в (10) не обеспечивает определённости системы уравнений.

6.6. Размерность и базис подпространства $\mathrm{R^n}$, задаваемого системой линейных однородных уравнений. Фундаментальная система решений

Рассмотрим систему линейных однородных уравнений

$$\mathbf{A}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{11}$$

с данной матрицей коэффициентов $\mathbf{A} \in M_{m,n}$.

Пусть $L \in \mathrm{R^n}$ определяется равенством

$$L := \{x = (x_1, \ldots, x_n) : \ x \text{ удовлетворяет (11)}\}.$$

Как уже отмечалось (см. пример 4 пункта 6.1), L является линейным подпространством в $\mathrm{R^n}$; это сразу следует из свойств умножения матриц. Мы говорим, что

L задаётся системой уравнений (11) или является подпространством решений этой системы.

Исследуем задачу определения размерности и базиса L.

Теорема. $\dim L = n - \mathrm{rg}(\mathbf{A})$.

Доказательство является конструктивным: в нём указан явный способ построения базиса L.

Найдём сначала общий вид элемента L, то есть общее решение системы (11). Пусть $\mathrm{rg}(\mathbf{A}) = r$.

Если $r = 0$, то $\mathbf{A} = \mathbf{0}$, и L совпадает со всем $\mathrm{R^n}$. В этом случае равенство из условия теоремы имеет вид $n = n$. Заметим также, что базисом L является любой базис $\mathrm{R^n}$.

Если $r > 0$, то с помощью элементарных преобразований строк матрица $\mathbf{A}$ может быть приведена к ступенчатой форме с r ступенями, см. пункт 6.4. Это означает, что общее решение будет иметь r главных и $n-r$ свободных неизвестных. Последние мы называем *параметрами*, а общий вид элемента L, в котором главные компоненты выражаются через свободные, называется *параметрическим видом*.

Пусть для простоты записи главными неизвестными являются $x_1, \ldots, x_r$, а параметрами — $x_{r+1}, \ldots, x_n$. Убедимся, что размерность L равна числу параметров $n - r$.

Общее решение системы (11) имеет вид

$$x_1 = \alpha_{r+1}^{(1)} x_{r+1} + \ldots + \alpha_n^{(1)} x_n,$$

$$x_2 = \alpha_{r+1}^{(2)} x_{r+1} + \ldots + \alpha_n^{(2)} x_n,$$

$$\ldots \quad \ldots \quad \ldots$$

$$x_r = \alpha_{r+1}^{(r)} x_{r+1} + \ldots + \alpha_n^{(r)} x_n.$$

Параметрический вид элемента $x \in L$ получается из стандартной формы $x = (x_1, \ldots, x_r, x_{r+1}, \ldots, x_n)$ с помощью замены главных компонент через параметры.

Рассмотрим теперь совокупность n-мерных векторов из L, которая получается по следующему правилу: один из параметров принимает значение 1, а все остальные — значение 0 (поочерёдно для всех параметров).

$$f^{(r+1)} := (\alpha_{r+1}^{(1)}, \alpha_{r+1}^{(2)}, \ldots, \alpha_{r+1}^{(r)}, 1, 0, 0, \ldots, 0, 0),$$

$$f^{(r+2)} := (\alpha_{r+2}^{(1)}, \alpha_{r+2}^{(2)}, \ldots, \alpha_{r+2}^{(r)}, 0, 1, 0, \ldots, 0, 0),$$

$$\ldots \quad \ldots \quad \ldots$$

$$f^{(n)} := (\alpha_n^{(1)}, \alpha_n^{(2)}, \ldots, \alpha_n^{(r)}, 0, 0, 0, \ldots, 0, 1).$$

Нетрудно понять, что эта совокупность векторов является базисом L. Линейная независимость $f^{(r+1)}, \ldots, f^{(n)}$ следует из того, что определитель порядка $n-r$, образованный последними компонентами $f^{(j)}$, равен 1, значит, эта система векторов имеет ранг $n-r$.

Если x — элемент L, который получается из общего вида при данных значениях параметров $x_{r+1}, \ldots, x_n$, то

$$x = x_{r+1} f^{(r+1)} + \ldots + x_n f^{(n)}.$$

Это равенство следует из способа построения $f^{(j)}$.

Таким образом, мы построили базис L из $n-r$ векторов. Поэтому $\dim L = n-r$.

Теорема доказана.

Замечание. Совокупность векторов $f^{(r+1)}, \ldots, f^{(n)}$, построенная при доказательстве теоремы, называется *фундаментальной системой решений* для системы линейных уравнений (11). Как мы показали, эта совокупность образует специальный базис подпространства решений системы (11).

Таким образом, каждое решение есть линейная комбинация решений, составляющих фундаментальную систему.

В заключение этого раздела подчеркнём, что с каждой матрицей $\mathbf{A} \in M_{m,n}$ можно связать два линейных подпространства $\mathrm{R^n}$, которые здесь мы обозначим L_1 и L_2.

1) L_1 — линейная оболочка строк матрицы $\mathbf{A}$. Размерность $\dim L_1 = \mathrm{rg}(\mathbf{A})$. Базис L_1 образует любая система из $r = \mathrm{rg}(\mathbf{A})$ линейно независимых строк.

2) L_2 — подпространство решений системы линейных однородных уравнений. Размерность $\dim L_2 = n - \mathrm{rg}(\mathbf{A})$. Базис L_2 образует фундаментальная система решений данной системы уравнений.

Наконец, заметим, что задачи нахождения базиса или размерности подпространств в конечномерных линейных пространствах, отличных от $\mathrm{R^n}$ (многочленов, матриц и т.д.), решаются с помощью изоморфного перехода в $\mathrm{R^n}$ с нужным значением n.

7. Евклидовы пространства

Евклидово (или эвклидово) пространство — это линейное пространство, в котором наряду с операциями сложения и умножения на число введено *скалярное умножение векторов*. Чаще говорят о результате такого умножения, то есть *скалярном произведении*. Скалярное произведение есть действительное число; в определении аксиоматически задаются его четыре свойства.

При таком подходе пространство геометрических векторов $\mathrm{V_n}$ со стандартным определением скалярного произведения (произведение длин и косинуса угла между векторами) — лишь один из многочисленных примеров евклидовых пространств, которые даются в пункте 7.1.

Следует хорошо запомнить, что в рассматриваемой абстрактной ситуации *длина вектора и угол между векторами определяются через скалярное произведение,* а не наоборот, как в частном случае пространства $\mathrm{V_n}$.

Ключевыми темами этого раздела являются *процесс ортогонализации, ортогональное дополнение, простейшие задачи на расстояние*. В каждой из них содержатся важные алгоритмы.

В этом тексте мы ограничиваемся действительным случаем; комплексное евклидово пространство и некоторые приложения рассматриваются, например, в лекциях И.М. Гельфанда [7].

Лишь немногие примеры связаны с бесконечномерной ситуацией. Бесконечномерные евклидовы пространства — важный предмет изучения анализа (в частности, *теории разложения функций в ортогональные ряды*).

Терминология сохраняет память об одном из гениев науки — древнегреческом математике Евклиде (365 – ок. 300 до н.э.), а также ряда учёных нового времени. Некоторые справки даются в соответствующих пунктах.

7.1. Определение евклидова пространства. Примеры. Ортогональная система, её линейная независимость

Рассмотрим произвольное действительное линейное пространство L.

Определение. *Будем говорить, что в L определено скалярное произведение векторов, если каждым $x, y \in L$ поставлено в соответствие действительное число (x, y), причём это соответствие обладает следующими свойствами (аксиомы скалярного произведения):*

1°. $(x, y) = (y, x)$ *(коммутативность)* ;

2°. $(\lambda x, y) = \lambda(x, y)$, $\lambda \in \mathrm{R}$ *(однородность)* ;

3°. $(x + y, z) = (x, z) + (y, z)$ *(дистрибутивность)* ;

4°. $(x, x) \geqslant 0$; $(x, x) = 0 \Longleftrightarrow x = 0$ *(положительная определённость)* .

Линейное пространство, в котором задано скалярное произведение, называется евклидовым. В дальнейшем евклидово пространство обозначается через E.

Ясно, что $(x, 0) = 0$ для всех $x \in E$. Отметим менее очевидное следствие аксиом скалярного произведения.

Упражнение 1. Показать, что если $(x, y) = (x, z)$ для некоторых $y, z \in E$ и всех $x \in E$, то обязательно $y = z$.

Каждое из отмеченных в пункте 5.1 линейных пространств является евклидовым относительно специальным образом введённого скалярного произведения.

Примеры.

1. Для $\vec{x}, \vec{y} \in V_n,\ n = 1, 2, 3,$ полагают $(\vec{x}, \vec{y}) := |\vec{x}||\vec{y}| \cos\varphi,$ φ — угол между $\vec{x}, \vec{y}$.

Выполнение свойств 1°, 4° очевидно. Более сложные равенства 2°–3° могут быть установлены, например, с помощью линейных свойств проекции вектора на ось.

Обращаем особое внимание на то, что этот пример является единственным, в котором скалярное произведение определяется через длину и угол; при аксиоматическом подходе ситуация обратная, см. пункт 7.2.

2. Стандартное скалярное произведение в R^n задаётся равенством

$$(x, y) := x_1y_1 + \ldots + x_ny_n;\ x = (x_1, \ldots, x_n),\ y = (y_1, \ldots, y_n) \in \mathrm{R}^n.$$

Проверка свойств 1°–4° очевидна и предоставляется читателю.

3. *(Обобщение.)* Пусть $\mathbf{A} = (a_{ij}) \in M_n$ — произвольная матрица, удовлетворяющая условиям:

1) $a_{ji} = a_{ij}$, то есть $\mathbf{A}$ является симметричной ($\mathbf{A} \in SM_n$) ;

2) Для всех $x = (x_1, \ldots, x_n) \neq (0, \ldots, 0)$ выполнено $\sum_{i,j} a_{ij}x_ix_j > 0$.

Матрица $\mathbf{A}$, удовлетворяющая 2), называется *положительно определённой.*

Положим для $x, y \in \mathrm{R}^n$

$$(x, y) := \sum_{i,j=1}^{n} a_{ij}x_iy_j \tag{1}$$

Предыдущий пример соответствует ситуации $\mathbf{A} = \mathbf{E}$.

Упражнение 2. Показать, что выполнение условий 1) – 2) гарантирует, что (1) является скалярным произведением в R^n.

Замечание. Отметим здесь без доказательства (см. подробнее пункт 10.3), что для положительной определённости матрицы необходимым и достаточным является любое из двух эквивалентных условий:

— все её главные миноры положительны;

— все её собственные значения положительны.

Первое из этих условий (положительность главных миноров) называется *критерием Сильвестра положительной определённости* матрицы $\mathbf{A}$ или соответствующей ей квадратичной формы $F(x) = \sum a_{ij}x_ix_j$. Оно названо в честь английского математика Джеймса Джозефа Сильвестра (J.J. Sylvester, 1814 – 1897).

Упражнение 3. Привести примеры недиагональных матриц $\mathbf{A}$, порождающих скалярное произведение в R^2 и R^3. Воспользоваться критерием Сильвестра.

4. Пространство $\mathrm{R}_n[t]$ многочленов степени $\leqslant n$ становится евклидовым, если в качестве скалярного произведения выбрать одно из следующих выражений:

$$(f,g) := a_0b_0 + a_1b_1 + \ldots + a_nb_n \ ; \tag{2}$$

$$(f,g) := f(t_1)g(t_1) + \ldots + f(t_{n+1})g(t_{n+1}) \ ; \tag{3}$$

$$(f,g) := \int\limits_a^b f(t)g(t)dt \ . \tag{4}$$

Здесь a_j, b_j — коэффициенты многочленов f, g при t^j; $\quad t_1, \ldots, t_{n+1}$ — любой набор из $n+1$ попарно различных чисел; $[a,b]$ — произвольный фиксированный отрезок.

Упражнение 4. Проверить, что каждое из равенств (2) – (4) задаёт скалярное произведение в $\mathrm{R}_n[t]$. *Выяснить, в частности, какова роль числа узлов* $n+1$ *в равенстве (3).*

5. Пространство $C[a,b]$ непрерывных функций $f : [a,b] \to \mathrm{R}$ является евклидовым относительно скалярного произведения (4).

Отметим, что формула (3) не задаёт скалярного произведения в $C[,b]$ ни при каком n. Убедитесь в этих фактах самостоятельно.

Бесконечномерные евклидовы пространства изучаются в анализе и многочисленных приложениях — там они называются *гильбертовыми пространствами*, по имени великого немецкого математика Давида Гильберта (D. Hilbert, 1862 – 1943).

Рассмотренное выше пространство $C[a,b]$ со скалярным произведением (4), более точно, является *предгильбертовым*; для того, чтобы получить гильбертово пространство, класс непрерывных на $[a,b]$ функций надо в некотором смысле расширить (как говорят, *пополнить*). Полученное таким образом важное функциональное пространство $L_2[a,b]$ — *пополнение* $C[a,b]$ — уже является гильбертовым.

Два вектора $x, y \in E$ называются *ортогональными*, если $(x,y) = 0$; иногда используется геометрическое обозначение $x \perp y$.

Конечная система, состоящая из ненулевых попарно ортогональных векторов, называется *ортогональной системой*.

Отметим следующее важное свойство ортогональных систем.

Утверждение. *Ортогональная система линейно независима.*

Доказательство совершенно очевидно. Пусть $(e_i, e_j) = 0, i \neq j$, и $e_i \neq 0, \ i,j = = 1, \ldots, n$. Скалярно умножим на e_i равенство

$$\alpha_1 e_1 + \ldots + \alpha_n e_n = 0.$$

После простых преобразований мы получим $\alpha_i = 0$. Так как i может быть любым, то $\alpha_1 = \ldots = \alpha_n = 0$.

Упражнение 5. Найти многочлены степени 1 и 2, ортогональные $f(t) = 1$ *относительно скалярных произведений (2) и (4). В последнем случае взять* $[a,b] = [0,1]$.

Упражнение 6. Установить линейную независимость системы функций $1, \cos t, \sin t, \ldots, \cos nt, \sin nt$ *при любом* $n \in \mathrm{N}$, *показав, что она является ортогональной в* $C[0, 2\pi]$ *относительно скалярного произведения (4) с* $a = 0, b = 2\pi$.

7.2. Длина и угол в евклидовом пространстве. Неравенство Коши – Буняковского и его частные виды

Пусть E — произвольное евклидово пространство. Так как $(x,x) \geqslant 0$, для любого $x \in E$ имеет смысл величина

$$|x| := \sqrt{(x,x)}\ ,$$

которая называется *длиной вектора* x.

Часто (но не в этом тексте) та же величина называется *нормой* x; в этом случае она обозначается $\|x\|$.

Примеры.

1. Длина геометрического вектора $\vec{x}$ как элемента евклидова пространства $\mathrm{V_n}, n = 1,2,3$, совпадает с его обычной длиной $|\vec{x}|$. Это, очевидно, мотивирует общее определение.

2. Каноническая длина вектора $x = (x_1, \ldots, x_n)$ в $\mathrm{R^n}, n \in \mathrm{N}$, связана со стандартным скалярным произведением $(x,y) = \sum x_i y_i$ и равна

$$|x| = \sqrt{x_1^2 + \ldots + x_n^2}\ .$$

Однако это не единственный вариант. Каждая симметричная положительно определённая матрица $\mathbf{A} \in M_n$ порождает скалярное произведение (1) и соответствующую ему длину

$$|x| = \Big(\sum_{i,j=1}^{n} a_{ij} x_i x_j\Big)^{\frac{1}{2}}\ .$$

3. Скалярное произведение (4) в $C[a,b]$ соответствует длине

$$|f|_{C[a,b]} = \Big(\int_a^b |f(t)|dt\Big)^{\frac{1}{2}}.$$

Чтобы избежать путаницы в обозначениях, в этом случае принято говорить о *норме* f. Заметим, однако, что стандартная норма в $C[a,b]$ — так называемая *равномерная норма*

$$\|f\|_{C[a,b]} := \max_{a \leqslant t \leqslant b} |f(t)|$$

— не порождается никаким скалярным произведением. Этот факт выходит за пределы нашей тематики.

Длина в евклидовом пространстве имеет следующие свойства.

1°. $|x| \geqslant 0; |x| = 0 \iff x = 0$.

2°. $|\lambda x| = |\lambda||x|,\ \lambda \in \mathrm{R}$.

3°. $|x+y| \leqslant |x| + |y|$.

Первые два свойства сразу следуют из аксиом скалярного произведения. Свойство 3°, называемое *неравенством треугольника*, получается из доказываемого ниже неравенства Коши – Буняковского (5).

Действительно, после возведения в квадрат (обе части 3° неотрицательны) и простых преобразований мы приходим к эквивалентному неравенству $(x, y) \leqslant |x||y|$, содержащемуся в (5).

Упражнение 1. Дайте обоснование следующим двум фактам.

Теорема Пифагора. Если $x \perp y$, *то* $|x + y|^2 = |x|^2 + |y|^2$.

Равенство параллелограмма. Для $x, y \in E \;\; 2(|x|^2 + |y|^2) = |x + y|^2 + |x - y|^2$.

Угол φ между векторами $x, y \neq 0$ определяется соотношением

$$\cos\varphi = \frac{(x, y)}{|x||y|}.$$

Из неравенства Коши – Буняковского следует, что это определение является корректным (правая часть по абсолютной величине не превосходит 1).

Ясно, что последняя формула мотивируется геометрией — в ситуации $E = \mathrm{V_n}$ она задаёт обычный угол между геометрическими векторами. Следует привыкнуть, однако, что при нашем подходе рассматриваются одновременно евклидовы пространства с различной природой элементов. Тем самым приобретают смысл выражения: угол между n-мерными векторами, многочленами, функциями и т.д.

Перейдём теперь к очень важному *неравенству Коши – Буняковского.*

Теорема. *Для любых векторов* $x, y \in E$ *выполняется неравенство*

$$|(x, y)| \leqslant |x||y|. \tag{5}$$

Равенство в (5) имеет место только для коллинеарных x, y *(различающихся скалярным множителем).*

Часто используется следующая эквивалентная форма (5):

$$(x, y)^2 \leqslant (x, x)(y, y). \tag{6}$$

Доказательство. Если $y = 0$, неравенства (5) и (6) обращаются в равенство. Зафиксируем пару $x, y \in E, \;\; y \neq 0$.

Рассмотрим функцию $h(t), t \in \mathrm{R}$, определённую равенством

$$h(t) := (x - ty, x - ty) = (y, y)t^2 - 2(x, y)t + (x, x).$$

Из четвёртого свойства скалярного произведения следует, что $h(t) \geqslant 0$ при всех действительных t. В связи с этим дискриминант $h(t)$ должен быть неположительным:

$$D := 4(x, y)^2 - 4(x, x)(y, y) \leqslant 0,$$

что эквивалентно (6).

Подстановка $x = \lambda y$ или $y = \lambda x$ приводит к совпадению обеих частей (5). Покажем, что иных ситуаций равенства нет.

Если в (5) имеет место равенство и $y \neq 0$, то обязательно $D = 0$. Поэтому $h(t_0) = 0$ для некоторого $t_0 \in \mathrm{R}$. Это означает, что

$$(x - t_0 y, x - t_0 y) = 0,$$

то есть $x = t_0 y$.

Теорема доказана.

Общность алгебраического подхода позволяет этим простым путём получить частные варианты неравенства (5) в самых различных ситуациях.

1. Для пространства $\mathrm{V_n}, n = 1, 2, 3,$ неравенство (5) эквивалентно $|\cos\varphi| \leqslant 1$ и не даёт ничего нового.

2. Для $\mathrm{R^n}$ с каноническим скалярным произведением соотношение (5) записывается как

$$\Big|\sum_{i=1}^{n} x_i y_i\Big| \leqslant \Big(\sum_{i=1}^{n} x_i^2\Big)^{\frac{1}{2}} \cdot \Big(\sum_{i=1}^{n} y_i^2\Big)^{\frac{1}{2}} . \tag{7}$$

Неравенство (7) имеет место для любых $x_i, y_i \in \mathrm{R}$. Именно это неравенство доказал О. Коши (A. Cauchy, 1821).

Отметим, что в курсе математического анализа неравенство (7) распространяется на бесконечные суммы с помощью простого предельного перехода.

3. Пусть $\mathbf{A} = (a_{ij}) \in M_n$ — *любая* симметричная матрица, главные миноры которой положительны. Тогда для всех чисел x_i, y_i

$$\Big|\sum_{i,j=1}^{n} a_{ij} x_i y_j\Big| \leqslant \Big(\sum_{i,j=1}^{n} a_{ij} x_i x_j\Big)^{\frac{1}{2}} \cdot \Big(\sum_{i,j=1}^{n} a_{ij} y_i y_j\Big)^{\frac{1}{2}} . \tag{8}$$

Эта форма неравенства (5) соответствует $\mathrm{R^n}$ и скалярному произведению (1).

Упражнение 2. Предложить вариант неравенства (8) с конкретной матрицей $\mathbf{A} \in M_2$.

4. Пусть $f, g : [a, b] \to \mathrm{R}$ — непрерывные функции. Пользуясь интегральным скалярным произведением (4), получаем из (5) неравенство

$$\Big|\int_a^b f(t)g(t)dt\Big| \leqslant \Big(\int_a^b |f(t)|^2 dt\Big)^{\frac{1}{2}} \cdot \Big(\int_a^b |g(t)|^2 dt\Big)^{\frac{1}{2}} . \tag{9}$$

Неравенство (9) имеет место для более широкого класса функций, чем $C[a, b]$. Это соотношение установлено В.Я. Буняковским в 1859 г. Его же иногда называют *неравенством Шварца*, хотя Г.А. Шварц (H.A. Schwarz) опубликовал (9) не ранее 1884 г.

Замечание. Неравенства (7) и (9) являются также частными случаями так называемых *неравенств Гёльдера* (O. Hölder, 1889), часто применяемых в анализе:

$$\Big|\sum_{i=1}^{n} x_i y_i\Big| \leqslant \Big(\sum_{i=1}^{n} |x_i|^p\Big)^{\frac{1}{p}} \cdot \Big(\sum_{i=1}^{n} |y_i|^q\Big)^{\frac{1}{q}} ,$$

$$\Big|\int_a^b f(t)g(t)dt\Big| \leqslant \Big(\int_a^b |f(t)|^p dt\Big)^{\frac{1}{p}} \cdot \Big(\int_a^b |g(t)|^q dt\Big)^{\frac{1}{q}} .$$

Здесь $p, q > 1$ — произвольные числа, удовлетворяющие соотношению двойственности

$$\frac{1}{p} + \frac{1}{q} = 1.$$

Евклидовы пространства соответствуют значениям $p = q = 2$.

7.3. Определитель Грама системы векторов и его свойства

Определителем Грама системы векторов $e_1, \ldots, e_k$ евклидова пространства E называется определитель матрицы $\mathbf{G} \in M_k$, составленной из элементов $g_{ij} := (e_i, e_j)$:

$$Gr(e_1, \ldots, e_k) := |\mathbf{G}| = \begin{vmatrix} (e_1, e_1) & (e_1, e_2) & \ldots & (e_1, e_k) \\ (e_2, e_1) & (e_2, e_2) & \ldots & (e_2, e_k) \\ \vdots & \vdots & & \vdots \\ (e_k, e_1) & (e_k, e_2) & \ldots & (e_k, e_k) \end{vmatrix} .$$

Матрица $\mathbf{G}$ называется *матрицей Грама*. Эта матрица всегда является симметричной, а для ортогональной системы векторов — диагональной.

Определители и матрицы Грама возникают во многих задачах этого раздела. Они введены впервые И.П. Грамом (J.P. Gram, 1879) в связи с разложением функций в ортогональные ряды и наилучшим приближением функций в евклидовых пространствах.

В этом пункте мы отметим некоторые основные свойства определителя Грама. Особый интерес представляет следующая теорема.

Теорема. $Gr(e_1, \ldots, e_k) = 0 \iff$ *система* $e_1, \ldots, e_k$ *линейно зависима.*

Доказательство. $\Longleftarrow$. Пусть система $e_1, \ldots, e_k$ линейно зависима. Покажем, что $Gr(\cdot) = 0$. Линейная зависимость означает существование таких чисел α_i, не равных нулю одновременно, что

$$\alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_k e_k = 0. \tag{10}$$

Умножая это равенство скалярно на e_j и записывая этот множитель первым, получаем, что числа α_i являются решением однородной системы k уравнений с k неизвестными

$$\alpha_1 (e_j, e_1) + \alpha_2 (e_j, e_2) + \ldots + \alpha_k (e_j, e_k) = 0, \qquad j = 1, 2, \ldots, k \; . \tag{11}$$

Таким образом, эта система уравнений имеет ненулевое решение, и поэтому её определитель $Gr(e_1, \ldots, e_k) = 0$.

$\Longrightarrow$. Пусть $Gr(e_1, \ldots, e_k) = 0$. Покажем, что векторы $e_1, \ldots, e_k$ линейно зависимы.

Система линейных уравнений (11) имеет ненулевое решение, так как её определитель равен нулю. Поэтому существует нетривиальный набор чисел α_i, для которого выполнены равенства

$$(e_j, \alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_k e_k) = 0, \qquad j = 1, 2, \ldots, k, \tag{12}$$

(это просто эквивалентная форма записи (11)). Умножая соотношения (12) на соответствующие числа $\alpha_j, j = 1, 2, \ldots, k$, и затем суммируя их, мы получим:

$$(\alpha_1 e_1 + \ldots + \alpha_k e_k, \alpha_1 e_1 + \ldots + \alpha_k e_k) = 0.$$

Отсюда в силу четвёртой аксиомы скалярного произведения получаем равенство (10) с некоторым нетривиальным набором коэффициентов, что и означает линейную зависимость системы $e_1, \ldots, e_k$.

Теорема доказана.

Можно дополнительно показать, что для любых $e_1, \ldots, e_k \in E$

$$Gr(e_1, \ldots, e_k) \geqslant 0. \tag{13}$$

Мы не будем останавливаться на доказательстве этого факта. Отметим лишь, что в случае $k = 2$ (13) равносильно неравенству Коши – Буняковского для векторов e_1, e_2.

Напомним также, что для геометрических векторов из V_3

$$Gr(\vec{e}_1, \vec{e}_2) = S^2, \quad Gr(\vec{e}_1, \vec{e}_2, \vec{e}_3) = V^2 \ ,$$

где S и V есть соответственно площадь параллелограмма и объём параллелепипеда, построенных на векторах $\vec{e}_i$. Это иллюстрирует неравенство (13) и доказанную выше теорему.

В общей ситуации неравенство (13) может быть устанавлено с привлечением аппарата квадратичных форм, см., например, [7]. По поводу непосредственного доказательства см. упражнения 5 – 6 следующего пункта.

Таким образом, для линейно независимой системы векторов всегда выполнено $Gr(e_1, \ldots, e_k) > 0$. Это означает, что для такой системы *матрица Грама является положительно определённой.*

7.4. Ортогональный и ортонормированный базисы. Преимущества ортонормированного базиса. Ортогонализация Грама – Шмидта

Пусть E — евклидово пространство размерности $n \geqslant 1$.

Определение. *Базис $e_1, \ldots, e_n$ называется ортогональным, если $(e_i, e_j) = 0$, $i \neq j$, и ортонормированным, если дополнительно $|e_i| = 1$, $i = 1, \ldots, n$.*

Другими словами, ортонормированный базис определяется соотношениями

$$(e_i, e_j) = \delta_{ij} := \begin{cases} 1 & , \quad i = j \\ 0 & , \quad i \neq j \end{cases} . \tag{14}$$

Ортонормированный базис $e_1, \ldots, e_n$ может быть получен из ортогонального базиса $f_1, \ldots, f_n$ с помощью простой процедуры *нормировки*:

$$e_i := \frac{1}{|f_i|} f_i, \quad i = 1, \ldots, n.$$

Упражнение 1. Обосновать последнее утверждение.

Ортогональный и, в частности, ортонормированный базис имеет целый ряд преимуществ по сравнению с произвольным базисом E. Эти преимущества для ортонормированного базиса состоят в следующем: во-первых, для $x \in E$ просто считаются соответствующие координаты; во-вторых, основные вычисления могут сравнительно легко осуществляться в координатном виде.

Теорема 1. *Пусть $e_1, \ldots, e_n$ — некоторый ортонормированный базис, $x = \{\alpha_1, \ldots, \alpha_n\}$, $y = \{\beta_1, \ldots, \beta_n\}$ — произвольные векторы E (их координаты соответствуют базису $e_1, \ldots, e_n$). Имеют место следующие равенства.*

1) $\alpha_i = (x, e_i),\ i = 1, \ldots, n.$

Таким образом, для $x \in E$ выполняется тождество

$$x = \sum_{i=1}^{n} (x, e_i) e_i. \tag{15}$$

2) $(x, y) = \alpha_1\beta_1 + \ldots + \alpha_n\beta_n.$

3) $|x| = \sqrt{\alpha_1^2 + \ldots + \alpha_n^2}.$

4) Если $x, y \neq 0$, φ — угол между x, y, то

$$\cos\varphi = \frac{\alpha_1\beta_1 + \ldots + \alpha_n\beta_n}{\sqrt{\alpha_1^2 + \ldots + \alpha_n^2}\sqrt{\beta_1^2 + \ldots + \beta_n^2}}.$$

Доказательство. 1). Скалярно умножим на e_i равенство

$$x = \alpha_1 e_1 + \ldots + \alpha_n e_n.$$

Используем свойства скалярного произведения и равенства (14). Мы получим, что $(x, e_i) = \alpha_i$.

2). Опять с учётом (14) имеем:

$$(x, y) = (\alpha_1 e_1 + \ldots + \alpha_n e_n, \beta_1 e_1 + \ldots + \beta_n e_n) =$$

$$= \sum_{i,j=1}^{n} \alpha_i\beta_j (e_i, e_j) = \alpha_1\beta_1 + \ldots + \alpha_n\beta_n.$$

3). По определению, $|x|^2 = (x, x)$. Остаётся воспользоваться 2), заменив y на x.

4) сразу следует из предыдущего и равенства

$$\cos\varphi = \frac{(x, y)}{|x||y|}.$$

Теорема доказана.

Упражнение 2. Пусть некоторый базис обладает свойством 1). Показать, что этот базис является ортонормированным. То же — для свойства 2). Иначе говоря, других базисов (кроме ортонормированных) с этими условиями нет.

Таким образом, каждое из свойств 1) – 2) *является характеристическим свойством ортонормированного базиса.*

Пример. Система векторов

$$f^{(1)} = (\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}), \qquad f^{(2)} = (\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}),$$

$$f^{(3)} = (\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}), \qquad f^{(4)} = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$$

является ортонормированным базисом R^4 относительно стандартного скалярного произведения. Поэтому координаты произвольного вектора x в этом базисе равны $(x, f^{(i)})$, $i = 1, 2, 3, 4$.

Пусть, например, $x = (1, 2, 3, 4)$. Мы сразу вычисляем $(x, f^{(1)}) = 0$, $(x, f^{(2)}) = -1$, $(x, f^{(3)}) = -2$, $(x, f^{(4)}) = 5$. Поэтому

$$x = \sum_{i=1}^{4} (x, f^{(i)}) f^{(i)} = -f^{(2)} - 2f^{(3)} + 5f^{(4)} = \{0, -1, -2, 5\}.$$

Проанализируем этот пример подробнее. Для того, чтобы найти координаты x в произвольном (не обязательно ортонормированном) базисе, требуется решить систему линейных уравнений, матрица которой состоит из компонент базисных векторов, записанных по столбцам, а столбец свободных членов совпадает с x, см. пункт 3.4.

В нашем случае столбец неизвестных координат является решением матричного уравнения

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}.$$

Обозначим через $\mathbf{A}$ матрицу, стоящую в левой части; её столбцы есть компоненты $f^{(i)}$. Ясно, что

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix} = \mathbf{A}^{-1} \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}.$$

Однако описанный выше метод нахождения α_i связан с использованием вместо обратной $\mathbf{A}^{-1}$ транспонированной матрицы $\mathbf{A}^T$. Действительно, равенства $\alpha_i = (f^{(i)}, x)$ эквивалентны (по построению $\mathbf{A}$)

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix} = \mathbf{A}^T \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}.$$

Оказывается, что $\mathbf{A}^{-1} = \mathbf{A}^T$ — в этом всё дело.

Таким образом, смысл нашей экономии заключается в *возможности заменить обращение матрицы её транспонированием*; фактически мы минуем решение системы линейных уравнений. Такая возможность связана со специальной структурой матрицы $\mathbf{A}$.

Упражнение 3. Пусть $\mathbf{A} \in \mathrm{R}^{\mathrm{n}}$ *— матрица, столбцы которой образованы компонентами векторов ортонормированного базиса* R^{n}. *Показать, что* $\mathbf{A}^{-1} = \mathbf{A}^T$. *Использовать анализ предыдущего примера и произвольность выбора вектора* x.

Упражнение 4. Матрица $\mathbf{A}$, *для которой выполняется равенство из упр.3, называется ортогональной. Показать, что определитель ортогональной матрицы равен* ± 1.

Перейдём теперь к возможности и методам построения ортогонального базиса в произвольном конечномерном евклидовом пространстве E. Как отмечалось, ортонормированный базис может быть получен затем с помощью нормировки.

Центральный результат этого пункта — знаменитая *теорема об ортогонализации*. Описываемый в ней алгоритм называется *процессом ортогонализации*; этот процесс по какому-то исходному базису подпространства строит его ортогональный базис.

Процесс ортогонализации связывают с именами математиков И. Грама (J.P. Gram) и Э. Шмидта (E. Schmidt).

Теорема 2. *Пусть* $f_1, \ldots, f_m$ *— произвольная линейно независимая система векторов* E. *Существует такая ортогональная система* $e_1, \ldots, e_m$, *что* $e_k \in \mathrm{lin}(f_1, \ldots, f_k)$, $f_k \in \mathrm{lin}(e_1, \ldots, e_k)$, $k = 1, \ldots, m$.

Доказательство. Положим по определению

$$e_1 := f_1,$$

$$e_k := f_k - \sum_{i=1}^{k-1} \lambda_i e_i, \ k = 2, \ldots, m. \tag{16}$$

Таким образом, векторы $e_1, \ldots, e_m$ строятся последовательно. При построении e_k вектор f_k корректируется с помощью уже построенных к этому k-му шагу попарно ортогональных векторов $e_1, \ldots, e_{k-1}$.

Соответствующие множители λ_i пересчитываются отдельно на каждом шаге. В формуле (16) они выбираются из условий ортогональности

$$(e_k, e_1) = (e_k, e_2) = \ldots = (e_k, e_{k-1}) = 0.$$

Для нахождения числовых коэффициентов умножим скалярно обе части (16) на $e_1, \ldots, e_{k-1}$ и воспользуемся после каждого умножения попарной ортогональностью e_i при всех $i \leqslant k$. Например, после умножения (16) на e_1 мы получим выражение для λ_1:

$$\lambda_1 = \frac{(f_k, e_1)}{(e_1, e_1)}.$$

После умножения (16) на e_2 и т.д. получаются аналогичные формулы для всех множителей. Таким образом, на k-м шаге надо взять

$$\lambda_i := \frac{(f_k, e_i)}{(e_i, e_i)}, \qquad i = 1, \ldots, k-1.$$

Деление возможно, так как $e_i \neq 0$. Формула (16) теперь принимает вид:

$$e_k = f_k - \sum_{i=1}^{k-1} \frac{(f_k, e_i)}{(e_i, e_i)} e_i, \qquad k = 2, \ldots, m.$$

Векторы $e_1, \ldots, e_m$ попарно ортогональны по построению. Двигаясь сверху вниз, получаем, что e_1 — линейная комбинация f_1; e_2 — линейная комбинация f_1, f_2; e_3 — линейная комбинация f_1, f_2, f_3, и т.д., то есть $e_k \in \mathrm{lin}(f_1, \ldots, f_k)$ при всех k.

Включение $f_k \in \mathrm{lin}(e_1, \ldots, e_k)$ очевидно — надо лишь перенести все слагаемые с e_i в левую часть.

В определении ортогональной системы требуется, чтобы все векторы были ненулевыми. То, что $e_k \neq 0$, сразу следует из того, что в правой части (16) коэффициент при f_k есть 1. В связи с предыдущим справа в (16) стоит нетривиальная линейная комбинация линейно независимых векторов $f_1, \ldots, f_k$. Естественно, эта линейная комбинация отлична от нуля.

Теорема доказана.

Замечание. Приведём другую схему процесса ортогонализации, содержащую явные формулы для векторов e_i. Положим

$$e_1 := f_1; \quad e_k := \begin{vmatrix} (f_1, f_1) & \ldots & (f_1, f_{k-1}) & f_1 \\ (f_2, f_1) & \ldots & (f_2, f_{k-1}) & f_2 \\ \vdots & & \vdots & \vdots \\ (f_{k-1}, f_1) & \ldots & (f_{k-1}, f_{k-1}) & f_{k-1} \\ (f_k, f_1) & \ldots & (f_k, f_{k-1}) & f_k \end{vmatrix}, \; j = 2, \ldots, m. \qquad (17)$$

Определитель понимается в смысле разложения по последнему столбцу. Обратите внимание на то, что коэффициент при f_k в правой части (17) отличен от нуля — он равен определителю Грама $Gr(f_1, \ldots, f_{k-1})$.

Формулы (17), как правило, менее пригодны для практических вычислений, но имеют теоретическое значение.

Упражнение 5^*. *Доказать, что система векторов $e_1, \ldots, e_m$, построенная по формулам (17) из линейно независимой системы $f_1, \ldots, f_m$, удовлетворяет заключению теоремы 2.*

Упражнение 6. *Используя для векторов из (17) соотношения $(e_k, e_k) > 0$, доказать, что $\Delta_k := Gr(f_1, \ldots, f_k) > 0$. Для этого представить второй сомножитель в виде $e_k = \alpha_{k1} f_1 + \ldots + \alpha_{k,k-1} f_{k-1} + \alpha_{kk} f_k$ и затем обратить внимание на то, что $(e_k, f_1) = \ldots = (e_k, f_{k-1}) = 0$, $\alpha_{kk} = \Delta_{k-1}$, $(e_k, f_k) = \Delta_k$.*

Следствие. *В конечномерном евклидовом пространстве $E \neq \{0\}$ существуют ортогональный и ортонормированный базисы.*

Доказательство следствия очевидно: надо применить алгоритм ортогонализации к произвольному базису E и затем нормировать векторы.

7.5. Ортогональное дополнение и его свойства. Две задачи о вычислении ортогонального дополнения в $\mathrm{R^n}$

Пусть E — произвольное евклидово пространство, L — линейное подпространство E.

Определение. *Ортогональным дополнением к подпространству L называется совокупность векторов E, каждый из которых ортогонален любому вектору из L:*

$$L^\perp := \{y \in E :\ \forall x \in L\ (y,x) = 0\} = \{y \in E :\ y \perp L\}.$$

Запись $y \perp A$ означает, что y ортогонален всем элементам $a \in A$.

Итак, L и $L^\perp$ связаны тем условием, что для любой пары $x \in L$, $y \in L^\perp$ выполнено $(x,y) = 0$, причём $L^\perp$ есть совокупность *всех* таких y.

Примеры. 1. Пусть L_1 — горизонтальная плоскость, L_2 — вертикальная прямая, рассматриваемые как совокупности векторов $E = \mathrm{V_3}$. Тогда $L_1^\perp = L_2,\ L_2 = L_1^\perp$. Геометрическое обоснование очевидно.

2. Пусть $L = \{x \in \mathrm{R^n} :\ x = (0, \xi_2, \ldots, \xi_n)\} \subset \mathrm{R^n}$; скалярное произведение в $\mathrm{R^n}$ выбрано обычным образом. Тогда $L^\perp = \{y = (\xi_1, 0, \ldots, 0)\}$.

Действительно, любой вектор $y = (\xi_1, 0, \ldots, 0)$ ортогонален каждому $x = (0, \xi_2, \ldots, \xi_n)$. Если же одна из последних $n-1$ компонент вектора y отлична от нуля, то найдётся $x \in L$ такой, что $(y,x) \neq 0$.

3. Основное определение охватывает и бесконечномерную ситуацию. Например, имеет смысл вопрос об описании ортогонального дополнения в пространстве $E = C[0,1]$ со скалярным произведением

$$(x,y) := \int_0^1 x(t)y(t)dt$$

к подпространству

$$L := \{x \in C[0,1] :\ \int_0^1 x(t)dt = 0\}\ .$$

В дальнейшем мы считаем, что E — конечномерное евклидово пространство размерности $n \geqslant 1$. Следует, однако, отметить, что доказательства многих свойств ортогонального дополнения подходят для общей ситуации.

Свойства ортогонального дополнения

1°. $L^\perp$ — линейное подпространство E.

2°. Пусть $e_1, \ldots, e_k$ — базис L. $y \in L^\perp \iff y \perp e_1, \ldots, e_k$.

3°. $L \oplus L^\perp = E$.

Тем самым, для любого $x \in E$ существует единственное представление $x = y+z$, где $y \in L,\ z \in L^\perp$. Вектор y называется *ортогональной проекцией x на L*, а вектор z — *ортогональной составляющей x*.

4°. Пусть $e_1, \ldots, e_k$ — ортогональный базис L, $e_{k+1}, \ldots, e_n$ — дополнение его до ортогонального базиса E. Тогда $e_{k+1}, \ldots, e_n$ — ортогональный базис $L^\perp$.

5°. $E^\perp = \{0\},\ \{0\}^\perp = E$.

6°. $(L^\perp)^\perp = L$.

7°. $(L_1 + L_2)^\perp = L_1^\perp \bigcap L_2^\perp$.

8°. $(L_1 \bigcap L_2)^\perp = L_1^\perp + L_2^\perp$.

Доказательство. 1°. Пусть $y_1, y_2 \in L^\perp,\ \lambda \in \mathrm{R}$. Тогда $(y_1, x) = (y_2, x) = 0$ для всех $x \in L$. Из свойств скалярного произведения получаем, что $(y_1 + y_2, x) = 0$ и $(\lambda y_1, x) = 0$. Поэтому $y_1 + y_2, \lambda y_1 \in L^\perp$.

2°. $\Longrightarrow$. Следует из определения $L^\perp$.

$\Longleftarrow$. Пусть $y \perp e_1, \ldots, e_k$. Если $x \in L$ — произвольный вектор, то x есть линейная комбинация $e_1, \ldots, e_k$. Применяя свойства скалярного произведения, получаем, что $y \perp x$.

3° – 4°. Сначала покажем, что сумма $L_1 + L_2$ является прямой. Достаточно убедиться, что $L \bigcap L^\perp = \{0\}$ (см. теорему о прямой сумме из пункта 6.3).

Пусть $x \in L \bigcap L^\perp$. Тогда одновременно $x \in L$ и $x \in L^\perp$. Это означает, что $(x, x) = 0$, то есть $x = 0$.

Покажем теперь, что $L_1 \oplus L_2$ совпадает со всем E. Достаточно убедиться, что $\dim(L \oplus L^\perp) = \dim E = n$.

Рассмотрим ситуацию $0 < k := \dim L < n$ (если $k = 0$ или $k = n$, надо воспользоваться простым свойством 5°).

Пусть $e_1, \ldots, e_k$ — ортогональный базис L, $e_{k+1}, \ldots, e_n$ — его дополнение до ортогонального базиса E. Последняя система есть базис $L^\perp$. Действительно, e_{k+1}, …, $e_n \in L^\perp$, в связи с чем $\dim L^\perp \geqslant n - k$. Однако если $\dim L^\perp > n - k$, то по той же теореме о прямой сумме

$$\dim(L \oplus L^\perp) = \dim L + \dim L^\perp > k + (n - k) = n,$$

что невозможно.

Таким образом, $\dim L^\perp = n-k$, и векторы $e_{k+1}, \ldots, e_n$ образуют базис $L^\perp$. Поэтому предыдущее соотношение обращается в равенство. Мы установили оба свойства 3° – 4°.

5°. Пусть $y \in E^\perp$. Тогда $(y, y) = 0$, и $y = 0$. Это означает, что $E^\perp = \{0\}$.

Равенство $\{0\}^\perp = E$ следует из того, что $(y, 0) = 0$ для всех $y \in E$.

6°. Ортогональный базис $L^\perp$ является дополнением ортогонального базиса L до базиса всего пространства (какая-то из этих систем может быть пустым множеством; тогда 6° совпадает с 5°.) Ясно, что базис L *также дополняет базис* $L^\perp$ до базиса E. Эта двойственность совпадает в конечномерной ситуации с равенством $(L^\perp)^\perp = L$.

7°. Пусть $y \in (L_1 + L_2)^\perp$. Тогда $(y, x_1 + x_2) = 0$ для всех $x_1 \in L_1$, $x_2 \in L_2$. Взяв поочерёдно $x_1 = 0$ и $x_2 = 0$, получим $(y, x_1) = (y, x_2) = 0$. Это означает, что одновременно $y \in L_1^\perp$ и $y \in L_2^\perp$, то есть $y \in L_1^\perp \bigcap L_2^\perp$.

Это даёт включение $(L_1 + L_2)^\perp \subset L_1^\perp \bigcap L_2^\perp$.

Установим противоположное включение. Если $y \in L_1^\perp \bigcap L_2^\perp$, то $(y, x_1) = (y, x_2) = 0$ для всех $x_1 \in L_1, x_2 \in L_2$. Простое сложение даёт $(y, x_1 + x_2) = 0$, то есть $y \in (L_1 + L_2)^\perp$.

Упражнение. Доказать 8°, *используя свойства* 6° – 7°.

Пусть теперь $E = \mathrm{R^n}$ с обычным скалярным произведением. Рассмотрим две важные задачи построения ортогонального дополнения к данному подпространству. В одной из них исходное подпространство есть линейная оболочка некоторых векторов, во второй — задаётся системой линейных однородных уравнений. Наши результаты означают, в частности, что эти способы задания подпространств являются в определённом смысле двойственными.

Пусть $L_1 := \mathrm{lin}(a^{(1)}, a^{(2)}, \ldots, a^{(m)})$, где

$$a^{(i)} = (a_{i1}, a_{i2}, \ldots, a_{in}), \quad i = 1, \ldots, m;$$

L_2 задаётся системой линейных однородных уравнений, коэффициенты которых являются компонентами векторов $a^{(i)}$:

$$a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n = 0, \quad i = 1, \ldots, m. \tag{18}$$

В этом фрагменте x_i обозначают компоненты n-мерного вектора $x = (x_1, \ldots, x_n)$.

Утверждение. *Имеют место равенства:*

$$L_1^\perp = L_2, \quad L_2^\perp = L_1.$$

Доказательство совершенно очевидно. Достаточно установить первое из соотношений; второе следует затем из двойственности 6°.

Пусть $x = (x_1, \ldots, x_n) \in L_1^\perp$. Тогда $(x, a^{(i)}) = 0$ для всех i, что в силу определения скалярного произведения эквивалентно (18); это означает, что $x \in L_2$.

Пусть, наоборот, $x \in L_2$. Запись (18) означает, что $(x, a^{(i)}) = 0$, $i = 1, \ldots, m$. Ясно, что тогда x ортогонален произвольной линейной комбинации векторов $a^{(i)}$. Поэтому $x \in L_1^\perp$.

Пример. Пусть $L \subset \mathrm{R}^4$ задаётся системой уравнений

$$\begin{aligned} 2x_1 + x_2 + 3x_3 - x_4 &= 0, \\ 3x_1 + 2x_2 \qquad - 2x_4 &= 0, \\ 3x_1 + x_2 + 9x_3 - x_4 &= 0. \end{aligned}$$

Тогда $L^\perp = \mathrm{lin}(a, b, c)$, где $a = (2, 1, 3, -1)$, $b = (3, 2, 0, -2)$, $c = (3, 1, 9, -1)$.

Более интересен вопрос о задании $L^\perp$ с помощью системы однородных уравнений. Чтобы выписать эти уравнения, зададим исходное подпространство L *как линейную оболочку*, а затем уже воспользуемся двойственностью.

Решая исходные уравнения, найдём общий вид элемента и базис L (фундаментальную систему решений):

$$x = (-6s, 9s + t, s, t), \quad s, t \in \mathrm{R},$$

$$f^{(1)} = (-6, 9, 1, 0), \qquad f^{(2)} = (0, 1, 0, 1).$$

Итак, $L = \lin(f^{(1)}, f^{(2)})$. Теперь применение последнего утверждения приводит к системе уравнений, задающих $L^\perp$:

$$-6x_1 + 9x_2 + x_3 = 0,$$

$$x_2 + x_4 = 0.$$

7.6. Расстояние в евклидовом пространстве. Расстояние от точки до подпространства. Два способа вычисления ортогональной проекции и ортогональной составляющей

Евклидовы пространства входят в более широкий класс так называемых *метрических линейных пространств*. Метрическое пространство — это произвольное множество, в котором определена *метрика, или расстояние*, то есть числовая функция $\mathrm{d}(x, y)$ двух аргументов, обладающая отмечаемыми ниже свойствами 1° – 3°.

Таким образом, в произвольном евклидовом пространстве можно решать различные метрические задачи, или задачи на расстояние.

Пусть E — евклидово пространство; его элементы, то есть векторы, в этом пункте мы будем называть также *точками*.

Определение 1. *Расстоянием между точками $x, y \in E$ называется величина*

$$\mathrm{d}(x, y) := |x - y| = \sqrt{(x - y, x - y)}. \tag{19}$$

Из свойств длины $|x|$ (см. пункт 7.2) сразу следуют основные свойства расстояния (x, y, z — произвольные элементы E):

1°. $\mathrm{d}(x, y) \geqslant 0$; $\mathrm{d}(x, y) = 0 \iff x = y$.

2°. $\mathrm{d}(x, y) = \mathrm{d}(y, x)$.

3°. $\mathrm{d}(x, y) \leqslant \mathrm{d}(x, z) + \mathrm{d}(z, y)$ (*неравенство треугольника*) .

Отметим также важные специфические свойства расстояния (19). Как отмечалось, определение метрики в произвольном метрическом пространстве содержит лишь условия 1° – 3°.

4°. $\mathrm{d}(x + a, y + a) = \mathrm{d}(x, y)$.

5°. $\mathrm{d}(\lambda x, \lambda y) = |\lambda| \mathrm{d}(x, y)$.

6°. Пусть $\dim E = n$. Если в некотором ортонормированном базисе $x = \{\alpha_1, \ldots, \alpha_n\}$, $y = \{\beta_1, \ldots, \beta_n\}$, то

$$\mathrm{d}(x, y) = \sqrt{(\alpha_1 - \beta_1)^2 + \ldots + (\alpha_n - \beta_n)^2}.$$

Упражнение 1. Доказать свойства 1° – 6°.

Определение 2. *Величина*

$$\mathrm{d}(x, B) := \inf_{y \in B} \mathrm{d}(x, y)$$

называется расстоянием между точкой $x \in E$ и множеством $B \subset E$. Число

$$\mathrm{d}(A, B) := \inf_{x \in A, y \in B} \mathrm{d}(x, y)$$

называется расстоянием между множествами $A, B \subset E$.

В ряде важных задач, но не всегда, inf можно заменить на min.

Отметим, что метрические задачи в евклидовых пространствах часто связывают с *методом наименьших квадратов*; это название объясняется свойством 6° и его аналогами в бесконечномерной ситуации.

Мы рассмотрим в этом пункте задачу вычисления расстояния $\mathrm{d}(x, L)$ от данной точки $x \in E$ до линейного подпространства $L \subset E$. Как мы покажем, эта задача допускает простое точное решение. Кроме того, мы остановимся на соответствующих алгоритмах.

Теорема. *Пусть $x = y + z,\ y \in L, z \in L^\perp$. Тогда $\mathrm{d}(x, L) = |z| = |x - y|$.*

Доказательство. Как было показано в пункте 7.5, для вектора x его ортогональная проекция y на L и ортогональная составляющая z определены единственным образом. Мы покажем, что y — *ближайший элемент* для x из L, то есть такой, для которого

$$\mathrm{d}(x, y) = \mathrm{d}(x, L) = \inf_{y_1 \in L} \mathrm{d}(x, y_1).$$

Таким образом, в предыдущей формуле inf может быть заменён на min — как говорят, *расстояние* $\mathrm{d}(x, L)$ *достигается на элементе* y.

Кроме того, мы установим, что ближайший элемент y является единственным.

Пусть y_1 — произвольный элемент L. Тогда $y - y_1 \in L$. Так как $z \in L^\perp$, то $z = x - y \perp y - y_1$. Применяя к векторам $x - y$ и $y - y_1$ теорему Пифагора для евклидовых пространств (см. пункт 7.2), получим

$$|y - y_1|^2 + |x - y|^2 = |x - y_1|^2.$$

Поэтому для любого $y_1 \in L$ выполняется неравенство

$$|x - y| \leqslant |x - y_1|, \tag{20}$$

равенство в котором имеет место лишь при $y_1 = y$.

Взятие в (20) inf по $y_1 \in L$ приводит в наших обозначениях к оценке $\mathrm{d}(x, y) \leqslant \mathrm{d}(x, L)$. Так как противоположная оценка очевидна из определения $\mathrm{d}(x, L)$, то справедливо равенство

$$\mathrm{d}(x, L) = \mathrm{d}(x, y) = |x - y|.$$

Теорема доказана.

Фактически мы доказали, что $\mathrm{d}(x, L) = \min_{y_1 \in L} \mathrm{d}(x, y_1)$, причём точка минимума $y_1 = y$ является единственной.

Замечание. Теорема допускает наглядную геометрическую иллюстрацию. Пусть $E = \mathrm{V}_3$, L — плоскость, $\vec{x}$ — вектор, не принадлежащий L. В этом случае доказательство имеет ясный геометрический смысл: единственная ближайшая точка плоскости получается ортогональным проектированием данной точки на эту плоскость.

Итак, для вычисления расстояния $\mathrm{d}(x, L)$ достаточно найти ортогональную проекцию y.

Мы остановимся на двух способах определения ортогональной проекции и ортогональной составляющей, имеющих и самостоятельное значение.

Первый способ. Пусть дан ортонормированный базис $e_1, \ldots, e_k$ подпространства L. Тогда следует положить

$$\alpha_i := (x, e_i), \quad y := \sum_{i=1}^{k} \alpha_i e_i, \quad z := x - y = x - \sum_{i=1}^{k} \alpha_i e_i. \tag{21}$$

Очевидно, $y \in \mathrm{lin}(e_1, \ldots, e_k) = L$. Далее, для всех $j = 1, \ldots, k$

$$(z, e_j) = (x - \sum_{i=1}^{k} \alpha_i e_i, e_j) = (x, e_j) - \sum_{i=1}^{k} \alpha_i (e_i, e_j) =$$
$$= (x, e_j) - (x, e_j) = 0.$$

Поэтому $z \perp e_1, \ldots, e_k$, то есть $z \in L^{\perp}$. Формулы (21) обоснованы.

Ясно, что

$$|y|^2 = (y, y) = (\sum_{i=1}^{k} \alpha_i e_i, \sum_{i=1}^{k} \alpha_i e_i) = \sum_{i=1}^{k} \alpha_i^2.$$

Так как $x - y = z \perp y$, то по теореме Пифагора для евклидовых пространств

$$|x - y|^2 = |x|^2 - |y|^2 = |x|^2 - \sum_{i=1}^{k} \alpha_i^2.$$

Поэтому в рассматриваемой ситуации имеет место равенство

$$\mathrm{d}(x, L) = |x - y| = \Big(|x|^2 - \sum_{i=1}^{k} (x, e_i)^2\Big)^{\frac{1}{2}}. \tag{22}$$

Второй способ. В приложениях чаще встречается ситуация, когда известен некоторый (не обязательно ортонормированный) базис $f_1, \ldots, f_k$ подпространства L.

В этой ситуации ортогональную проекцию y будем искать в виде

$$y = \lambda_1 f_1 + \ldots + \lambda_k f_k.$$

Неизвестные коэффициенты λ_i находятся из условий ортогональности $z = x - y \perp f_1, \ldots, f_k$. Равенства

$$(f_i, y - x) = 0, \quad i = 1, \ldots, k,$$

с учётом выражения для y приводятся к виду

$$\begin{aligned}
\lambda_1(f_1,f_1)+\lambda_2(f_1,f_2)+\ldots+\lambda_k(f_1,f_k)&=(f_1,x),\\
\lambda_1(f_2,f_1)+\lambda_2(f_2,f_2)+\ldots+\lambda_k(f_2,f_k)&=(f_2,x),\\
\ldots\quad\ldots\quad\ldots\quad\ldots&\\
\lambda_1(f_k,f_1)+\lambda_2(f_k,f_2)+\ldots+\lambda_k(f_k,f_k)&=(f_k,x).
\end{aligned}$$

Определитель последней системы линейных уравнений есть определитель Грама $Gr(f_1,\ldots,f_k)$. В силу линейной независимости $f_1,\ldots,f_k$ этот определитель отличен от нуля (см. пункт 7.3). Поэтому система имеет единственное решение $\lambda_1,\ldots,\lambda_k$.

После определения y можно найти $z=x-y$ и $\mathrm{d}(x,L)=|z|$.

Оказывается, что и в этой ситуации есть явная формула для расстояния, аналогичная (22). Эта формула имеет вид

$$\mathrm{d}(x,L)^2=\frac{Gr(f_1,\ldots,f_k,x)}{Gr(f_1,\ldots,f_k)}. \tag{23}$$

Для доказательства равенства (23) рассмотрим определитель Грама, стоящий в числителе:

$$Gr(f_1,\ldots,f_k,x)=\begin{vmatrix}
(f_1,f_1) & (f_1,f_2) & \ldots & (f_1,f_k) & (f_1,x)\\
(f_2,f_1) & (f_2,f_2) & \ldots & (f_2,f_k) & (f_2,x)\\
\vdots & \vdots & & \vdots & \vdots\\
(f_k,f_1) & (f_k,f_2) & \ldots & (f_k,f_k) & (f_k,x)\\
(x,f_1) & (x,f_2) & \ldots & (x,f_k) & (x,x)
\end{vmatrix}.$$

Пусть λ_i — числа, определённые выше. Из последнего столбца определителя вычтем предыдущие столбцы, умноженные соответственно на $\lambda_1,\ldots,\lambda_k$; при этом величина определителя останется прежней. Последний столбец, очевидно, изменится следующим образом: вместо второго множителя x во всех скалярных произведениях будет стоять $x-y$.

Напомним, что $(f_i,x-y)=0, i=1,\ldots,k$. Кроме того,

$$(x,x-y)=(x-y,x-y)=(z,z)=|z|^2.$$

Здесь используется ортогональность $z=x-y\perp y$. Поэтому $(k+1)$-й столбец преобразованного определителя имеет вид

$$\begin{pmatrix}0\\0\\\vdots\\0\\|z|^2\end{pmatrix}.$$

Разложение по этому столбцу даёт

$$Gr(f_1,\ldots,f_k,x)=|z|^2Gr(f_1,\ldots,f_k),$$

откуда и получается (23).

Упражнение 2. Убедиться, что для ортонормированного базиса формула (23) эквивалентна (22).

Часть 3

8. Линейные операторы

Линейные операторы составляют важный класс отображений одного линейного пространства в другое.

Основное определение означает, что линейный оператор довольно просто действует на линейных комбинациях — образ любой линейной комбинации векторов есть линейная комбинация образов этих векторов *с теми же коэффициентами*. Этому условию удовлетворяют многие важные отображения в различных линейных пространствах: поворот и проектирование в геометрических пространствах $\mathrm{V_n}, n = 1, 2, 3$, умножение на матрицу в $\mathrm{R^n}, n \in \mathrm{N}$, интегрирование и дифференцирование в функциональных пространствах и их модификации и обобщения.

В конечномерной ситуации изучение линейных операторов сводится к изучению *их матриц*: при переходе к координатам любой оператор действует как оператор умножения на некоторую матрицу.

Не следует думать, что все важные операторы и функционалы, встречающиеся в приложениях, являются линейными. Например, *оператор метрической проекции*, связанный с задачами наилучшего приближения, вообще говоря, не является линейным. Отметим также часто возникающие в математическом моделировании *нелинейные дифференциальные или разностные уравнения*.

В нелинейных задачах часто используют *линеаризацию*, то есть способ приближённой замены нелинейного оператора линейным. Кроме того, для численного решения задачи бесконечномерное пространство заменяется на конечномерное. Таким образом, возникает уже отмеченная ситуация.

Определение линейного оператора, данное в пункте 8.1, принадлежит итальянскому математику Джузеппе Пеано (G. Peano, 1888).

Теория линейных операторов получила мощное развитие в рамках алгебры, функционального анализа и многочисленных приложений. В этом тексте мы останавливаемся лишь на вводных основных понятиях и результатах.

8.1. Определение линейного оператора. Примеры линейных операторов и функционалов

Пусть L_1, L_2 — два действительных линейных пространства.

Определение. *Линейным оператором из L_1 в L_2 называется отображение $A : L_1 \to L_2$, для которого при всех $x, y \in L_1, \alpha \in \mathrm{R}$ выполняются равенства:*

$$1^\circ. \quad A(x+y) = A(x) + A(y) \qquad \textit{(аддитивность)}\ ;$$
$$2^\circ. \quad A(\alpha x) = \alpha A(x) \qquad \textit{(однородность)}\ .$$

В случае $L_1 = L_2 = L$ в литературе (но не в этом тексте) используется термин *линейное преобразование пространства* L. Если же $L_1 = L, L_2 = \mathrm{R}$, то A называется *линейным функционалом на* L (и чаще обозначается F или f).

Иногда мы будем использовать запись Ax вместо $A(x)$.

Условия $1^\circ - 2^\circ$ эквивалентны тому, что для любого $k \in \mathrm{N}$ и любых векторов $x_1, \ldots, x_k \in L_1$ и чисел $\alpha_1, \ldots, \alpha_k \in \mathrm{R}$

$$A(\sum_{i=1}^{k} \alpha_i x_i) = \sum_{i=1}^{k} \alpha_i A(x_i). \tag{1}$$

Определение означает, что линейный оператор переводит линейную комбинацию векторов в линейную комбинацию их образов с теми же коэффициентами — это и выражается равенством (1). Как правило, проверка условий линейности 1° – 2° в конкретной ситуации является весьма простой и использует известные факты.

Заметим, что из 2° легко следует, что $A(0) = 0$ (образ нуля L_1 есть нуль L_2). *Поэтому отображение* $A : L_1 \to L_2$ *такое, что* $A(0) \neq 0$, *заведомо не является линейным оператором.*

Основное определение естественным образом переносится на операторы, действующие из одного *комплексного* линейного пространства в другое — в этом случае $\alpha \in \mathrm{C}$. Свойства, доказываемые ниже, переносятся и на комплексный случай. При изложении материала в этом разделе мы ограничиваемся действительной ситуацией; в дальнейшем это не оговаривается специально.

Примеры линейных операторов

1. Пусть L — произвольное линейное пространство.

Оператор $A : L \to L$, для которого $A(x) := x, x \in L$, называется *единичным, или тождественным.* Единичный оператор обозначается в этом разделе через E (в разделе 11 используется другое стандартное обозначение I).

Пусть $A(x) := 0$ для всех $x \in L$. Такой оператор A называется *нулевым* и обозначается O.

Линейность этих операторов очевидна. Эти тривиальные примеры являются исключительно важными.

2. Пусть $A_\varphi : \mathrm{V}_2 \to \mathrm{V}_2$ — оператор поворота на угол φ против часовой стрелки, $0 \leqslant \varphi < 2\pi$. Выполнение равенств $1^\circ - 2^\circ$ геометрически очевидно.

3. Обозначим через $P = P_H$ оператор ортогонального проектирования в V_3 на фиксированную плоскость H (которую для наглядности будем представлять горизонтальной). Равенство $\vec{y} = P(\vec{x})$ означает, что $\vec{y} \in H$ и $\vec{x} - \vec{y} \perp H$.

Условия $1^\circ - 2^\circ$ очевидны. Например, равенство $P(\vec{x}+\vec{y}) = P(\vec{x}) + P(\vec{y})$ означает, что при ортогональном проектировании на плоскость параллелограмм переходит в параллелограмм. Поэтому $P : \mathrm{V}_3 \to \mathrm{V}_3$ — линейный оператор. Ясно также, что мы могли бы считать $P : \mathrm{V}_3 \to \mathrm{V}_2$.

Если $\vec{y} \in H$, то $P(\vec{y}) = \vec{y}$ — на подпространстве H оператор P совпадает с тождественным. Поэтому $P(P(\vec{x})) = P(\vec{x})$ для всех $\vec{x} \in \mathrm{V}_3$.

Замечание 1. Пусть L — произвольное линейное пространство. Линейный оператор $A : L \to L$ такой, что $A(A(x)) = A(x), x \in L$, в соответствии с геометрической аналогией называется *проекционным оператором*, или просто *проектором*.

Проекторы играют важную роль в ряде разделов математики; отметим теорию ортогональных рядов и теорию приближения. По поводу интерполяционного проектора см. ниже пример 8. Общий вид ортогонального проектора на конечномерное подпространство евклидова пространства дан в упражнении 2.

4. Зафиксируем матрицу $\mathbf{A} \in M_{m,n}$. Пусть $x = (x_1, \ldots, x_n) \in \mathrm{R}^{\mathrm{n}}$. Будем считать $A(x) = y = (y_1, \ldots, y_m) \in \mathrm{R}^{\mathrm{m}}$, если столбец компонент y получается из столбца компонент x умножением на матрицу $\mathbf{A}$:

$$y = A(x) \qquad \Longleftrightarrow \qquad \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \mathbf{A} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Оператор $A : \mathrm{R}^{\mathrm{n}} \to \mathrm{R}^{\mathrm{m}}$ называется *оператором умножения на матрицу*. Линейность A следует из свойств умножения матриц.

Этот пример является типичным для конечномерной ситуации. В частности, в пункте 8.3 мы покажем, что каждый линейный оператор $A : L \to L, \dim L = n$, *в координатном виде* есть оператор умножения на соответствующую ему матрицу порядка n.

5. Определим $A : \mathrm{R}^3 \to \mathrm{R}^3$ с помощью равенства

$$A(x) := (-x_1 + 2x_2 + 3x_3, 4x_1 + x_2 + 7x_3, -2x_1 + 5x_2 + 8x_3), \quad x = (x_1, x_2, x_3).$$

Этот оператор является линейным — он соответствует предыдущему примеру в ситуации $n = m = 3$ и

$$\mathbf{A} = \begin{pmatrix} -1 & 2 & 3 \\ 4 & 1 & 7 \\ -2 & 5 & 8 \end{pmatrix}.$$

Отображение $B : \mathrm{R}^3 \to \mathrm{R}^3$, задаваемое соотношением

$$B(x) := (|x_1|, x_2 + 7x_3, 5x_2 + 8x_3),$$

не является линейным оператором. Достаточно показать, что B не является аддитивным. Возьмём $u := (1, 0, 0), v := (-1, 0, 0)$, тогда

$$B(u + v) = (0, 0, 0) \neq (1, 0, 0) + (1, 0, 0) = B(u) + B(v).$$

Можно ограничиться установлением неоднородности B. В тех же обозначениях $B(-2u) \neq -2B(u)$.

Замечание 2. Нелинейность B связана с функционалом, выражающим первую компоненту $B(x)$, — функционал $F(x) := |x_1|$ не является линейным.

Ясно, что произвольное отображение $A : \mathrm{R}^{\mathrm{n}} \to \mathrm{R}^{\mathrm{m}}$ имеет вид

$$A(x) = (F_1(x), F_2(x), \ldots, F_m(x)), \qquad x \in \mathrm{R}^{\mathrm{n}}.$$

Здесь $F_j : \mathrm{R}^{\mathrm{n}} \to \mathrm{R}$ — функционалы, выражающие компоненты образа $A(x)$. Для линейности A необходима и достаточна линейность *всех* компонентных функционалов

$F_1, \ldots, F_m$. Как мы отметим ниже (см. пример 10), каждый линейный функционал на $\mathrm{R^n}$ имеет вид $F(x) = \sum d_i x_i$.

Поэтому в примере 4 дан так называемый *общий вид линейного оператора из* $\mathrm{R^n}$ *в* $\mathrm{R^m}$ — других линейных операторов $A : \mathrm{R^n} \to \mathrm{R^m}$ не существует. Этот факт следует также из общих рассуждений пункта 8.2.

6. Оператор дифференцирования D, сопоставляющий функции f её производную: $Df(t) := f'(t)$, определён в различных конечномерных и бесконечномерных пространствах. Можно считать, например, $D : P_n \to P_n$, $D : P_n \to P_{n-1} (n \geqslant 1)$ или $D : C^1[0,1] \to C[0,1]$. Здесь и далее $P_n := \mathrm{R_n}[t]$ — совокупность многочленов степени $\leqslant n$. Линейность D гарантируется известными свойствами производной.

Оператор $G : \mathrm{R}[t] \to \mathrm{R}[t]$, задаваемый равенством $Gf(t) := (f')^2$, не является линейным (отсутствует, например, однородность).

7. Пусть $K(s,t)$ — непрерывная на квадрате $[0,1]^2$ функция (так называемое *ядро интегрального оператора*). Определим оператор $A : C[0,1] \to C[0,1]$ равенством

$$Af(t) := \int_0^1 K(s,t) f(s) ds, \;\; f \in C[0,1].$$

Линейность оператора A следует из свойств интеграла. То, что $Af \in C[0,1]$, может быть установлено средствами математического анализа. Отметим ещё, что выбор $K(s,t) = h(t-s), h$ — функция одного переменного, соответствует важному *оператору свёртки* $Af = f * h$.

8. Зафиксируем на отрезке $[a,b]$ систему узлов $a \leqslant t_0 < t_1 < \ldots < t_n \leqslant b$. Рассмотрим оператор A, сопоставляющий каждой непрерывной функции f её интерполяционный многочлен p степени $\leqslant n$ по данной системе узлов, то есть такой, что $p(t_j) = f(t_j), j = 0, \ldots, n$.

В соответствии с интерполяционной формулой Лагранжа (см. пункт 4.6)

$$Af(t) := p(t) = \sum_{i=0}^{n} f(t_i) L_i(t), \;\; L_i(t) = \prod_{j \neq i} \frac{t - t_j}{t_i - t_j}.$$

Из этого равенства легко получается линейность оператора A. Можно считать, что $A : C[a,b] \to C[a,b]$ или $A : C[a,b] \to P_n$. Единственность решения интерполяционной задачи означает, что многочлену степени $\leqslant n$ соответствует он сам. Поэтому для каждой $f \in C[a,b]$ выполнено $A(Af) = f$; таким образом, оператор A является проектором на P_n. Этот оператор называется *интерполяционным проектором.*

Упражнение 1. Какое из следующих утверждений является справедливым: (i) каждый линейный оператор переводит любую линейно независимую систему в линейно независимую; (ii) каждый линейный оператор переводит любую линейно зависимую систему в линейно зависимую?

Упражнение 2. Пусть L — евклидово пространство размерности $\dim L \geqslant k$, L_1 — подпространство размерности k с ортонормированным базисом $e_1, \ldots, e_k$. Определим оператор $P : L \to L$ равенством $P(x) := y$, если y — ортогональная проекция x на L_1. Как следует из результатов пункта 7.6, $P(x)$ имеет вид

$$P(x) = \sum_{i=1}^{k} (x, e_i) e_i.$$

Показать, что P — линейный оператор, являющийся проектором (см. выше замечание 1).

Примеры линейных функционалов

Напомним, что линейным функционалом называется линейный оператор, действующий из некоторого пространства L в R.

9. $F(\vec{x}) := (\vec{a}, \vec{x})$, $\vec{a}$ — фиксированный вектор, есть линейный функционал на V_3. Другой пример: $F(\vec{x}) := \text{пр}_{\vec{a}}\, \vec{x}$ (скалярная проекция $\vec{x}$ на ось $\vec{a}$). Линейность этих функционалов следует из свойств проекций и скалярного произведения.

10. *Каждый линейный функционал F на R^n имеет вид*

$$F(x) = d_1 x_1 + \ldots + d_n x_n, \qquad d_i \in \mathrm{R}. \tag{2}$$

Легко видеть, что если $F(x)$ имеет вид (2), то функционал F — линейный. С другой стороны, условия линейности обеспечивают равенства

$$F(x) = F(x_1 e^{(1)} + \ldots + x_n e^{(n)}) = x_1 F(e^{(1)}) + \ldots + x_n F(e^{(n)}) =$$

$$= d_1 x_1 + \ldots + d_n x_n\ , \qquad d_i := F(e^{(i)}).$$

Здесь $e^{(1)}, \ldots, e^{(n)}$ — канонический базис R^n, $x = (x_1, \ldots, x_n)$. Одновременно мы выяснили смысл коэффициентов d_i из (2).

Равенство (2) даёт *общий вид линейного функционала на* R^n.

11. На других конечномерных пространствах линейные функционалы действуют по тому же типу. Например,

$$F(x) := 3a_0 + a_1 - a_2, \quad x(t) = a_0 + a_1 t + a_2 t^2,$$

— линейный функционал на $R_2[t]$;

$$F(\mathbf{A}) := -a_{11} + 2a_{12} + a_{22}, \qquad \mathbf{A} = (a_{ij}),$$

— линейный функционал на M_2, и т. д.

Функционал $F(\mathbf{A}) := \mathrm{tr}(\mathbf{A}) = \sum a_{ii}$ на каждом пространстве матриц $M_n, n \in \mathrm{N}$, является линейным. В то же время функционал $G(\mathbf{A}) := |\mathbf{A}|, \mathbf{A} \in M_n$, линеен лишь в случае $n = 1$ (почему?).

12. В приложениях играют важную роль линейные функционалы, заданные на бесконечномерных пространствах функций. Из основных отметим линейную комбинацию значений в фиксированных точках и линейную комбинацию интегралов по фиксированным областям. Так, каждый из функционалов на $C[0,1]$

$$F(x) := x(0), \qquad F(x) := -2x(0) + 5x(\frac{1}{2}) - 3x(1),$$

$$F(x) := \int_0^1 x(t)dt, \qquad F(x) := 3\int_0^{\frac{1}{2}} x(t)dt - 5\int_{\frac{1}{2}}^1 x(t)dt$$

является линейным. Здесь $x(\cdot) \in C[0,1]$.

Упражнение 3. Привести примеры нелинейных функционалов на пространстве $C[0,1]$.

В заключение этого пункта сделаем несколько замечаний о соотношении условий аддитивности и однородности $1^\circ - 2^\circ$ для функционалов $F : L \to \mathrm{R}$.

В случае $L = \mathrm{R}$ (F — обычная числовая функция, заданная на всей прямой) из однородности F следует аддитивность. Действительно, условие $F(\alpha x) = \alpha F(x)$, $\alpha, x \in \mathrm{R}$, даёт

$$F(x) = F(x \cdot 1) = xF(1) = cx, \ c := F(1).$$

В общей ситуации из аддитивности функционала $F : L \to \mathrm{R}$ следует равенство $F(rx) = rF(x)$ для рациональных множителей r , см. схему упражнения 4. Если дополнительно F является *непрерывным функционалом*, то это равенство распространяется на произвольные действительные множители. Таким образом, для непрерывных на L функционалов из аддитивности вытекает однородность. (Понятие непрерывности наиболее просто вводится в ситуации, когда L является *нормированным пространством*, см., например, [12].)

Для произвольного функционала $F : L \to \mathrm{R}$ из аддитивности не следует однородность. Достаточно взять $L = \mathrm{R}$. Известно, что среди решений функционального уравнения

$$F(x+y) = F(x) + F(y), \qquad f : \mathrm{R} \to \mathrm{R},$$

кроме непрерывных функций вида $F(x) = cx, c \in \mathrm{R}$, имеются и не непрерывные (и даже так называемые *неизмеримые*) функции. Последние заведомо не являются однородными (мы показали выше, что однородными на R являются лишь функции $F(x) = cx$).

Упражнение 4. Пусть $F : L \to \mathrm{R}$ *— аддитивный функционал. Установить последовательно равенства:*

$$(a) \quad F(0) = 0, \qquad (b) \quad F(-x) = -F(x),$$

$$(c) \quad F(kx) = kF(x), \ k \in \mathrm{N}, \qquad (d) \quad F(kx) = kF(x), \ k \in \mathrm{Z},$$

$$(e) \ F(rx) = rF(x), \quad r \in \mathrm{Q}.$$

Упражнение 5. Показать, что непрерывные решения функционального уравнения $F(x+y) = F(x) + F(y), \ F : \mathrm{R} \to \mathrm{R}, \ $ *есть функции вида* $F(x) = cx, \ c \in \mathrm{R}$.

8.2. Матрица линейного оператора. Применение матрицы оператора для нахождения координат образа вектора

Начиная с этого пункта мы рассматриваем только линейные операторы; слово *линейный* в этом сочетании часто опускается.

Перейдём к рассмотрению основной для нас ситуации, когда оператор действует в конечномерном пространстве L. Обозначим $\dim L = n$. Пусть $e_1, \ldots, e_n$ — фиксированный базис L.

Прежде всего покажем, что каждый оператор $A : L \to L$ однозначно определяется своим действием на базисных векторах. Равенство операторов $A, B : L \to L$ означает, что $A(x) = B(x)$ для всех $x \in L$.

Теорема 1. *Для произвольной системы $f_1, \ldots, f_n \in L$ существует единственный линейный оператор $A : L \to L$ такой, что*

$$A(e_1) = f_1, \ \ldots, \ A(e_n) = f_n.$$

Доказательство. *Существование.* Пусть $x = \{\xi_1, \ldots, \xi_n\}$ в базисе $e_1, \ldots, e_n$. Положим по определению

$$A(x) := \xi_1 f_1 + \ldots + \xi_n f_n.$$

Если $y = \{\eta_1, \ldots, \eta_n\}, \alpha \in \mathrm{R}$, то $x + y = \{\xi_1 + \eta_1, \ldots, \xi_n + \eta_n\}$, $\alpha x = \{\alpha\xi_1, \ldots, \alpha\xi_n\}$. Поэтому

$$A(x + y) = (\xi_1 + \eta_1)f_1 + \ldots + (\xi_n + \eta_n)f_n = A(x) + A(y),$$

$$A(\alpha x) = \alpha\xi_1 f_1 + \ldots + \alpha\xi_n f_n = \alpha A(x).$$

Очевидно, $A(e_j) = f_j$ для всех j.

Единственность. Пусть операторы $A, B : L \to L$ удовлетворяют условиям теоремы. Для любого $x \in L$ в предыдущих обозначениях

$$A(x) = A(\sum_{j=1}^{n} \xi_j e_j) = \sum_{j=1}^{n} \xi_j A(e_j) = \sum_{j=1}^{n} \xi_j f_j =$$

$$= \sum_{j=1}^{n} \xi_j B(e_j) = B(\sum_{j=1}^{n} \xi_j e_j) = B(x),$$

то есть $A = B$. Теорема доказана.

Таким образом, линейный оператор $A : L \to L$ однозначно определяется образами базисных векторов $A(e_1), \ldots, A(e_n)$, которые можно задать в координатном виде в том же базисе.

Определение. *Матрица $\mathbf{A} = (a_{ij}) \in M_n$, j-й столбец которой содержит координаты вектора $A(e_j)$ в базисе $e_1, \ldots, e_n$, называется матрицей линейного оператора $A : L \to L$ в базисе $e_1, \ldots, e_n$. Это означает, что для $j = 1, \ldots, n$*

$$A(e_j) = \sum_{i=1}^{n} a_{ij} e_i. \tag{3}$$

Следует особо выделить, что для составления $\mathbf{A}$ требуется не только определить образы базисных векторов $A(e_j)$, но и разложить их *по тому же базису* $e_1, \ldots, e_n$. Это часто приводит к решению систем линейных уравнений — в тех ситуациях, когда базис $e_1, \ldots, e_n$ не является стандартным.

Наши рассуждения означают, что соответствие между линейными операторами $A : L \to L$, $\dim L = n$, и $n \times n$-матрицами $\mathbf{A}$, осуществляемое по указанному правилу, *при фиксированном базисе является взаимно-однозначным.*

Матрицы одного и того же оператора в двух различных базисах, вообще говоря, различны. Связь между этими матрицами изучается в пункте 8.7.

Отметим, что матричная запись операторов является по сути выражением координатного подхода.

Примеры. 1. Матрица нулевого оператора O в любом базисе является нулевой. Матрица единичного оператора E в любом базисе является единичной.

2. Пусть оператор A действует на базисных векторах по правилу $A(e_j) = \lambda_j e_j, \lambda_j \in \mathrm{R}$. Тогда в базисе $e_1, \ldots, e_n$ матрица этого оператора будет *диагональной*:

$$\mathbf{A} = \mathrm{diag_n}(\lambda_1, \ldots, \lambda_n) := \begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & \lambda_n \end{pmatrix}.$$

Операторы такого типа называются *операторами простой структуры, или диагонализируемыми.*

3. Пусть $P : \mathrm{V}_3 \to \mathrm{V}_3$ — оператор ортогонального проектирования на плоскость H, см. пример 3 предыдущего пункта. Выберем в V_3 базис $\vec{e}_1, \vec{e}_2, \vec{e}_3$ так, чтобы $\vec{e}_1, \vec{e}_2 \in H, \vec{e}_3 \perp H$. Тогда $P(\vec{e}_1) = \vec{e}_1, P(\vec{e}_2) = \vec{e}_2, P(\vec{e}_3) = \vec{0}$. В этом базисе матрица оператора P имеет вид

$$\mathbf{P} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Пусть теперь базис $\vec{f}_1, \vec{f}_2, \vec{f}_3$ таков, что $\vec{f}_1, \vec{f}_2 \in H$, а результат проектирования $\vec{f}_3$ есть $\vec{f}_1$ (изобразите обе ситуации). Нетрудно понять, что в базисе $\vec{f}_1, \vec{f}_2, \vec{f}_3$ матрица оператора P будет иметь другой вид:

$$\mathbf{P_1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

4. Рассмотрим оператор $A : \mathrm{R}^3 \to \mathrm{R}^3$, действующий на векторе $x = (x_1, x_2, x_3)$ по правилу

$$A(x) := (2x_1 + x_2 - x_3, x_1 + x_2 + x_3, -4x_1 + 2x_2 + 2x_3).$$

Пусть $e^{(1)} = (1, 0, 0),\ e^{(2)} = (0, 1, 0),\ e^{(3)} = (0, 0, 1)$ — канонический базис R^3. Так как

$$A(e^{(1)}) = (2, 1, -4), \quad A(e^{(2)}) = (1, 1, 2), \quad A(e^{(3)}) = (-1, 1, 2),$$

а координаты разложения любого вектора по каноническому базису совпадают с его компонентами, то в базисе $e^{(1)}, e^{(2)}, e^{(3)}$ матрица оператора A будет иметь вид:

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

Возьмём теперь в качестве базиса $f^{(1)} = (1,0,0),\ f^{(2)} = (1,1,0), f^{(3)} = (1,1,1)$. Действие оператора на базисных векторах имеет вид

$$A(f^{(1)}) = (2,1,-4), \quad A(f^{(2)}) = (3,2,-2), \quad A(f^{(3)}) = (2,3,0).$$

Формальная запись компонент получившихся векторов по столбцам матрицы ведёт к ошибке! Чтобы составить матрицу оператора A в *неканоническом базисе* $f^{(1)}$, $f^{(2)}$, $f^{(3)}$, требуется найти координаты образов базисных векторов в этом базисе и именно эти последние координаты записать в столбцы.

Задача сводится к решению трёх систем линейных уравнений с матрицей коэффициентов, состоящей из компонент базисных векторов, записанных по столбцам. Столбцы свободных членов этих систем образованы компонентами $A(f^{(i)}), i = = 1,2,3$. Компактная запись всех трёх систем имеет вид:

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 2 & 3 & 2 \\ 0 & 1 & 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & -4 & -2 & 0 \end{array}\right).$$

Выполняя преобразования метода Гаусса, получим в левой части единичную матрицу (это возможно, так как каждая из систем имеет единственное решение). Справа, как нетрудно понять, получится именно матрица оператора A в базисе $f^{(1)}, f^{(2)}, f^{(3)}$. Обозначим эту матрицу $\mathbf{A}'$. Проверьте, что

$$\mathbf{A}' = \left(\begin{array}{ccc} 1 & 1 & -1 \\ 5 & 4 & 3 \\ -4 & -2 & 0 \end{array}\right).$$

Неопытному читателю рекомендуется хорошо разобраться в этом примере.

5. Матрица оператора дифференцирования $D : \mathrm{R_n}[t] \to \mathrm{R_n}[t],\ \ Df(t) := f'(t)$, в каноническом базисе $1, t, t^2, \ldots, t^n$ имеет вид

$$\mathbf{D} = \left(\begin{array}{cccccc} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 2 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & n \\ 0 & 0 & 0 & \ldots & 0 & 0 \end{array}\right).$$

Очевидно, $\mathbf{D} \in M_{n+1}$. Такой вид матрицы соответствует равенствам $D(1) = 0$; $D(t^j) = jt^{j-1}$, $j = 1, \ldots, n$.

Упражнение 1. Изменить базис $\mathrm{R_n}[t]$ *таким образом, чтобы ненулевые элементы матрицы оператора* D *в этом базисе были равны 1.*

Упражнение 2. Найти матрицу оператора дифференцирования $D : \mathrm{R_2}[t] \to \mathrm{R_2}[t]$ *в базисе* $f_1(t) = 1 + t$, $f_2(t) = 1 - t$, $f_3(t) = 1 + t^2$.

Покажем, что при переходе к координатам векторов оператор $A : L \to L$ действует как оператор умножения на некоторую матрицу, а именно на матрицу этого оператора в данном базисе.

Теорема 2. *Пусть* $\mathbf{A} = (a_{ij})$ *— матрица оператора* A *в базисе* $e_1, \ldots, e_n$, $x \in L$ *— произвольный вектор. Если* $x = \{\xi_1, \ldots, \xi_n\}$ *и* $A(x) = \{\eta_1, \ldots, \eta_n\}$ *в том же базисе, то*

$$\begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix} = \mathbf{A} \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}. \tag{4}$$

Доказательство. С одной стороны,

$$A(x) = \sum_{i=1}^{n} \eta_i e_i.$$

С другой стороны,

$$A(x) = A(\sum_{j=1}^{n} \xi_j e_j) = \sum_{j=1}^{n} \xi_j A(e_j) =$$

$$= \sum_{j=1}^{n} \xi_j \sum_{i=1}^{n} a_{ij} e_i = \sum_{i=1}^{n} (\sum_{j=1}^{n} a_{ij} \xi_j) e_i.$$

Мы использовали равенство (3) для $A(e_j)$. Единственность разложения вектора $A(x)$ по базису означает, что для всех $i = 1, \ldots, n$ имеют место равенства

$$\eta_i = \sum_{j=1}^{n} a_{ij} \xi_j,$$

что эквивалентно матричному равенству (4). Теорема доказана.

Результаты этого пункта естественным образом переносятся на линейные операторы $A : L_1 \to L_2$, $\dim L_1 = n, \dim L_2 = m$.

Матрица $\mathbf{A}$ такого оператора зависит от выбора двух базисов — $e_1, \ldots, e_n$ в пространстве L_1 и $f_1, \ldots, f_m$ в пространстве L_2. Столбцы $\mathbf{A}$ состоят из координат векторов $A(e_1), \ldots, A(e_n)$ в базисе $f_1, \ldots, f_m$. Итак, матрица $\mathbf{A} = (a_{ij}) \in M_{m,n}$ определяется равенствами

$$A(e_j) = \sum_{i=1}^{m} a_{ij} f_i.$$

При фиксированных базисах в L_1 и L_2 соответствие между линейными операторами $A : L_1 \to L_2$ и матрицами из $M_{m,n}$, устанавливаемое этим способом, является взаимно-однозначным. Справедлив также аналог теоремы 2, показывающий, что при переходе к координатам действие оператора описывается умножением на матрицу. Читателю предлагается самостоятельно сформулировать и доказать точный результат.

В дальнейшем мы будем рассматривать лишь основной случай $L_1 = L_2 = L$.

8.3. Действия с линейными операторами

С линейными операторами из L в L можно производить некоторые естественные действия, не выводящие за пределы этого множества отображений.

Пусть $A, B : L \to L$ — линейные операторы, $\lambda \in \mathrm{R}$.

Определение. *Суммой $A + B$, произведением на число λA и произведением (суперпозицией) операторов AB (или $A \cdot B$) называются операторы из L в L, действующие на векторе $x \in L$ по правилам:*

$$(A + B)(x) := A(x) + B(x),$$
$$(\lambda A)(x) := \lambda A(x),$$
$$AB(x) := A(B(x)).$$

Пусть $\dim L = n$; $e_1, \ldots, e_n$ — фиксированный базис L. Матрицы операторов $, B, C$ в этом базисе обозначаются через $\mathbf{A} = (a_{ij}), \mathbf{B} = (b_{ij}), \mathbf{C} = (c_{ij})$.

Теорема. *$A + B, \lambda A$ и AB есть линейные операторы из L в L, при этом их матрицы равны соответственно $\mathbf{A} + \mathbf{B}, \lambda\mathbf{A}$ и $\mathbf{AB}$.*

Доказательство. Линейность операторов следует из линейности A и B. Действительно, для $x, y \in L$, $\alpha, \beta \in \mathrm{R}$ выполняются равенства:

$$(A + B)(\alpha x + \beta y) = A(\alpha x + \beta y) + B(\alpha x + \beta y) =$$
$$= \alpha A(x) + \beta A(y) + \alpha B(x) + \beta B(y) = \alpha[A(x) + B(x)] +$$
$$+\beta[A(y) + B(y)] = \alpha(A + B)(x) + \beta(A + B)(y),$$

$$(\lambda A)(\alpha x + \beta y) = \lambda A(\alpha x + \beta y) =$$
$$= \lambda\alpha A(x) + \lambda\beta A(y) = \alpha(\lambda A)(x) + \beta(\lambda A)(y),$$

$$AB(\alpha x + \beta y) = A(B(\alpha x + \beta y) = A(\alpha B(x) + \beta B(y)) =$$
$$= \alpha A(B(x)) + \beta A(B(y)) = \alpha AB(x) + \beta AB(y).$$

Докажем вторую часть теоремы. Пусть сначала $C := A + B$. Тогда в соответствии с равенством (3)

$$C(e_j) = A(e_j) + B(e_j) = \sum_{i=1}^{n} a_{ij}e_i + \sum_{i=1}^{n} b_{ij}e_i = \sum_{i=1}^{n}(a_{ij} + b_{ij})e_i.$$

Если $\mathbf{C}$ — матрица оператора C, то должно быть одновременно

$$C(e_j) = \sum_{i=1}^{n} c_{ij}e_i,$$

поэтому (единственность разложения по базису) $\mathbf{C} = \mathbf{A} + \mathbf{B}$.

Пусть $C := \lambda A$. Тогда

$$C(e_j) = \sum_{i=1}^{n} (\lambda a_{ij}) e_i = \sum_{i=1}^{n} c_{ij} e_i,$$

что даёт $\mathbf{C} = \lambda \mathbf{A}$.

Положим, наконец, $C := AB$. Считаем, как и ранее, что оператору C соответствует матрица $\mathbf{C} = (c_{ij})$. Покажем, что $\mathbf{C} = \mathbf{AB}$.

В соответствии с определениями произведения операторов и матрицы оператора

$$C(e_j) = A(B(e_j)) = A(\sum_{i=1}^{n} b_{ij} e_i) = \sum_{i=1}^{n} b_{ij} A(e_i) =$$

$$= \sum_{i=1}^{n} b_{ij} (\sum_{k=1}^{n} a_{ki} e_k) = \sum_{i=1}^{n} \sum_{k=1}^{n} a_{ki} b_{ij} e_k = \sum_{k=1}^{n} (\sum_{i=1}^{n} a_{ki} b_{ij}) e_k.$$

С другой стороны,

$$C(e_j) = \sum_{k=1}^{n} c_{kj} e_k.$$

Сравнивая эти выражения, получим

$$c_{kj} = \sum_{i=1}^{n} a_{ki} b_{ij}, \qquad k, j = 1, \ldots, n.$$

Это означает, что $\mathbf{C} = \mathbf{AB}$.

Теорема доказана.

Замечание. Результат доказанной теоремы, касающийся матрицы произведения операторов, позволяет внести ясность в определение матричного умножения. Фактически, умножение двух $n \times n$-матриц — это такая операция, которая по известным матрицам операторов A и B в данном базисе позволяет построить матрицу оператора AB в том же базисе. Умножение операторов выглядит естественнее, чем умножение числовых матриц; однако это действие не может рассматриваться в самом начале курса.

Введённые операции обладают рядом свойств, аналогичным свойствам операций с матрицами. Например: $AB \neq BA$ (вообще говоря), $(AB)C = A(BC)$, $(A + B)C = AC + BC$, $C(A + B) = CA + CB$, $A(\lambda B) = \lambda(AB)$, и т. д.

Обоснование каждого из этих свойств можно провести непосредственно. В конечномерном случае альтернативная схема доказательства использует взаимную однозначность соответствия "оператор $A \longleftrightarrow$ матрица оператора $\mathbf{A}$" и доказанную выше теорему. Так как аналоги всех этих свойств выполняются для матриц порядка n, то они верны и для операторов — нужно лишь перейти к их матрицам.

Особо отметим, что совокупность $X(L)$ всех линейных операторов из L в L *образует линейное пространство относительно операций сложения и умножения на число.* Более того, $X(L)$ как линейное пространство изоморфно M_n :

$$X(L) \simeq M_n.$$

Отмеченное выше соответствие $A \longleftrightarrow \mathbf{A}$ является изоморфизмом. Так как изоморфными конечномерными пространствами могут быть лишь пространства одинаковой размерности, то $\dim X(L) = \dim M_n = n^2$.

Упражнение 1. Описать базис пространства $X(L)$.

Натуральная степень оператора $A : L \to L$ определяется равенством

$$A^k := \underbrace{A \cdot \ldots \cdot A}_{k}.$$

Если $A \neq O$, то полагают $A^0 := E$, E — тождественный оператор. Для так называемых обратимых операторов вводятся также целые отрицательные степени, см. пункт 8.5.

Оператор, удовлетворяющий условию $A^2 = A$, называется *проектором*. Примеры проекторов даны в пункте 8.1.

Интересно, что существуют операторы $A \neq O$, для которых $A^k = O$ при некотором $k > 1$. Такой оператор A называется *нильпотентным*, а минимальное значение k, при котором $A^k = O$ — *индексом нильпотентности* A.

Упражнение 2. Показать, что оператор дифференцирования $D : \mathrm{R_n}[t] \to \mathrm{R_n}[t]$ является нильпотентным, и найти его индекс нильпотентности.

В приложениях используются также *многочлены от операторов*.

Если $p(t) = a_0 + a_1 t + a_2 t^2 \ldots + a_k t^k,\ a_i \in \mathrm{R},$ — алгебраический многочлен, то для оператора $A : L \to L$ полагают

$$p(A) := a_0 E + a_1 A + a_2 A^2 + \ldots + a_k A^k.$$

Ясно, что $p(A)$ — линейный оператор из L в L, матрица которого равна $p(\mathbf{A})$.

Упражнение 3. Показать, что для всякого $A : L \to L,\ \dim L = n$, существует ненулевой аннулирующий многочлен $p(t)$, то есть такой, что $p(A) = O$.

8.4. Ядро и образ линейного оператора. Теорема о ранге и дефекте. Определение ранга и дефекта по матрице оператора

Определение. *Ядро и образ линейного оператора $A : L \to L$ определяются соответственно равенствами:*

$$\mathrm{Ker}A := \{x \in L :\ A(x) = 0\},$$

$$\mathrm{Im}A := \{y \in L : y = A(x) \text{ для некоторого } x \in L\}.$$

Обозначение связано с английскими словами *image* и *kernel*.

В рассматриваемой ситуации ядро и образ есть подмножества L. Более общее определение касается операторов $A : L_1 \to L_2$; тогда $\mathrm{Ker}A \subset L_1, \mathrm{Im}A \subset L_2$. В дальнейшем мы ограничиваемся случаем $L_1 = L_2 = L$.

Примеры. 1. Для нулевого и тождественного операторов $\mathrm{Ker}O = L$, $\mathrm{Im}O = \{0\}$ и $\mathrm{Ker}E = \{0\}, \mathrm{Im}E = L$.

2. Пусть $P : \mathrm{V_3} \to \mathrm{V_3}$ — оператор ортогонального проектирования на плоскость H. Тогда $\mathrm{Im}P = H,\ \mathrm{Ker}P = H^{\perp} = \{\vec{x} :\ x \perp H\}$.

3. Для оператора дифференцирования $D : \mathrm{R_n}[t] \to \mathrm{R_n}[t]$, $n \geqslant 1$, как нетрудно понять, $\mathrm{Ker}D = \mathrm{R_0}[t]$, $\mathrm{Im}D = \mathrm{R_{n-1}}[t]$. В частности, *каждый* многочлен степени $\leqslant n-1$ есть производная некоторого многочлена степени $\leqslant n$.

4. Определение касается и бесконечномерной ситуации. Зададим оператор $A : C[0,1] \to C[0,1]$ с помощью равенства

$$Ax(t) := \int_0^t x(s)ds, \quad x(\cdot) \in C[0,1].$$

Тогда $\mathrm{Ker}A = \{0\}$, $\mathrm{Im}A = \{x \in C^1[0,1] : x(0) = 0\}$.

Упражнение 1. Обосновать последние равенства.

Нетрудно показать, что *ядро и образ линейного оператора $A : L \to L$ являются линейными подпространствами L.*

Действительно, если $x_1, x_2 \in \mathrm{Ker}A$, то $A(x_1) = A(x_2) = 0$. Из линейности A следует, что $A(\alpha x_1 + \beta x_2) = 0$ при всех $\alpha, \beta \in \mathrm{R}$.

Если $y_1, y_2 \in \mathrm{Im}A$, то $y_1 = A(x_1), y_2 = A(x_2)$. Это означает, что $\alpha y_1 + \beta y_2 = = A(\alpha x_1 + \beta x_2) \in \mathrm{Im}A$.

В случае, когда ядро и образ конечномерны, их размерности $\dim \mathrm{Ker}A$ и $\dim \mathrm{Im}A$ называются соответственно *дефектом и рангом оператора A.*

Замечание. В приложениях важную роль играют так называемые *операторы конечного ранга*, то есть линейные операторы, заданные на бесконечномерном пространстве, образ которых имеет конечную размерность. Примером такого оператора является интерполяционный проектор, заданный на $C[a,b]$, см. пункт 8.1, пример 8.

Теорема 1. *Пусть* $\dim L = n$. *Для любого оператора $A : L \to L$*

$$\dim \mathrm{Ker}A + \dim \mathrm{Im}A = n. \tag{5}$$

Таким образом, в конечномерной ситуации сумма дефекта и ранга любого оператора равна размерности пространства.

Доказательство. Рассмотрим сначала случай $\dim \mathrm{Ker}A = 0$, то есть $\mathrm{Ker}A = = \{0\}$. Пусть $e_1, \ldots, e_n$ — произвольный базис L. Покажем, что образы базисных векторов $A(e_1), \ldots, A(e_n)$ линейно независимы. Это гарантирует равенство $\dim \mathrm{Im}A = = n$, то есть $\mathrm{Im}A = L$. Соотношение (5) в этом случае имеет вид $0 + n = n$.

Пусть линейная комбинация $A(e_i)$ с коэффициентами α_i равна 0. В силу линейности A

$$0 = \sum_{i=1}^n \alpha_i A(e_i) = A(\sum_{i=1}^n \alpha_i e_i),$$

то есть $z := \sum \alpha_i e_i \in \mathrm{Ker}L$. Так как ядро состоит из одного нуля, то $z = 0$. Это в силу линейной независимости e_i даёт $\alpha_1 = \ldots = \alpha_n = 0$.

Пусть $\dim \mathrm{Ker}A = n$, то есть $\mathrm{Ker}A = L$. В этом случае $A(x) = 0$ для всех $x \in L$. Это означает, что $\mathrm{Im}A = \{0\}$, так что $\dim \mathrm{Im}A = 0$, и (5) имеет вид $n + 0 = n$. Заметим, что в этой ситуации A совпадает с нулевым оператором O.

Наконец, считаем $1 \leqslant k := \dim \mathrm{Ker}A \leqslant n - 1$.

Пусть $e_1, \ldots, e_k$ — базис ядра. Дополним эту систему произвольным образом до базиса L векторами $f_{k+1}, \ldots, f_n$. Покажем, что образы этих векторов $A(f_{k+1})$, $\ldots$, $A(f_n)$ составляют базис $\mathrm{Im}A$.

Предположим, что

$$\beta_{k+1}A(f_{k+1}) + \ldots + \beta_n A(f_n) = 0.$$

Обозначим $z := \sum \beta_j f_j$. Из линейности A следует, что $A(z) = 0$, то есть $z \in \mathrm{Ker}A$. Вектор z, поэтому, есть линейная комбинация $e_1, \ldots, e_k$ — базиса ядра:

$$\beta_{k+1}f_{k+1} + \ldots + \beta_n f_n = \alpha_1 e_1 + \ldots + \alpha_k e_k.$$

Так как $e_1, \ldots, e_k, f_{k+1}, \ldots, f_n$ образуют базис L, то все коэффициенты в последнем равенстве равны 0. В частности, $\beta_{k+1} = \ldots = \beta_n = 0$.

Итак, векторы $A(f_{k+1}), \ldots, A(f_n)$ линейно независимы.

Покажем, что произвольный вектор $y \in \mathrm{Im}A$ есть их линейная комбинация. Для $x \in L$

$$y = A(x) = A(\sum_{i=1}^{k} \xi_i e_i + \sum_{i=k+1}^{n} \xi_i f_i) =$$

$$= \sum_{i=1}^{k} \xi_i A(e_i) + \sum_{i=k+1}^{n} \xi_i A(f_i) = \sum_{i=k+1}^{n} \xi_i A(f_i),$$

так как $e_i \in \mathrm{Ker}A$.

Мы показали, что $A(f_{k+1}), \ldots, A(f_n)$ образуют базис $\mathrm{Im}A$. Таким образом, $\dim \mathrm{Im}A = n - k$, и равенство (5) имеет вид $k + (n - k) = n$.

Теорема доказана.

Доказательство теоремы содержит простой алгоритм построения базисов ядра и образа. Проиллюстрируем его примерами операторов $A : \mathrm{R}^3 \to \mathrm{R}^3$. В этих примерах $x = (x_1, x_2, x_3) \in \mathrm{R}^3$, так что x_i обозначают компоненты вектора x.

Пример 5. Пусть

$$A(x) := (x_1 + 3x_2 + 5x_3, -x_1 + x_2 + x_3, 4x_1 + x_2 - 6x_3).$$

Ядро этого оператора задаётся системой уравнений

$$x_1 + 3x_2 + 5x_3 = 0,$$

$$-x_1 + x_2 + x_3 = 0,$$

$$4x_1 + x_2 - 6x_3 = 0,$$

единственное решение которой является нулевым: $x_1 = x_2 = x_3 = 0$. Это означает, что $\mathrm{Ker}A = \{(0, 0, 0)\}$. Дефект A равен нулю, следовательно, ранг A равен 3, то есть $\mathrm{Im}A = \mathrm{R}^3$. Базис $\mathrm{Im}A$ совпадает с базисом R^3. Можно взять, например, канонический базис $(1, 0, 0), (0, 1, 0), (0, 0, 1)$.

Пример 6. Рассмотрим оператор

$$A(x) := (2x_1 - x_2 - x_3, x_1 - 2x_2 + x_3, x_1 + x_2 - 2x_3).$$

Ядро состоит из тех x, для которых

$$2x_1 - x_2 - x_3 = 0,$$

$$x_1 - 2x_2 + x_3 = 0,$$

$$x_1 + x_2 - 2x_3 = 0.$$

Решая эту систему методом Гаусса, найдём общее решение в виде $x = (t, t, t), t \in \mathrm{R}$. Это есть общий вид элемента ядра. Базис $\mathrm{Ker}A$ совпадает с фундаментальной системой решений; в нашем случае можно взять $g^{(1)} := (1, 1, 1)$. Дефект оператора A равен 1.

В соответствии с (5) ранг оператора A равен $\dim \mathrm{Im}A = 3 - 1 = 2$. Для построения базиса образа сначала произвольным способом дополним $g^{(1)}$ до базиса R^3. Пусть, скажем, $g^{(2)} := (0, 1, 0), g^{(3)} := (0, 0, 1)$. Так как ранг системы $g^{(1)}, g^{(2)}, g^{(3)}$ равен 3, то эти векторы образуют базис R^3. Базис $\mathrm{Im}A$ составляют векторы

$$A(g^{(2)}) = (-1, -2, 1),\ A(g^{(3)}) = (-1, 1, -2).$$

В заключение отметим, что дефект и ранг оператора $A : L \to L,\ \dim L = n$, просто определяются по матрице этого оператора.

Теорема 2. *Пусть* $\mathbf{A}$ *— матрица оператора* A *в произвольном базисе. Тогда*

$$\dim \mathrm{Ker}A = n - \mathrm{rg}(\mathbf{A}), \quad \dim \mathrm{Im}A = \mathrm{rg}(\mathbf{A}). \tag{6}$$

Доказательство. В координатах, соответствующих тому базису, в котором задана матрица оператора, ядро задаётся системой линейных однородных уравнений с матрицей $\mathbf{A}$. Иначе говоря, $\mathrm{Ker}A$ изоморфно подпространству $W \subset \mathrm{R^n}$, состоящему из тех $(\xi_1, \ldots, \xi_n)$, для которых

$$\mathbf{A} \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Известно, что $\dim W = n - \mathrm{rg}(\mathbf{A})$, см. пункт 6.6. Так как $W \simeq \mathrm{Ker}A$, то $\dim \mathrm{Ker}A = \dim W$ (теорема об изоморфизме из пункта 5.5). Это обеспечивает левое равенство в (6). Правое получается затем из предыдущей теоремы.

Теорема 2 доказана.

Следствие. *Ранг матрицы оператора есть инвариант этого оператора, не зависящий от базиса. В частности, если матрица оператора является невырожденной в некотором базисе, то она является невырожденной и в любом другом базисе.*

Доказательство следствия сразу получается из (6): так как $\mathrm{rg}(\mathbf{A})$ совпадает с размерностью образа оператора, то это число не зависит от выбора базиса.

8.5. Обратный оператор, его линейность. Обратимость и невырожденность

Определение 1. *Оператор $A : L \to L$, для которого существует такой $A^{-1} : L \to L$, что $AA^{-1} = A^{-1}A = E$, называется обратимым. Оператор A^{-1} называется обратным к A.*

Для обратимого A из равенства $y = A(x)$ следует $x = A^{-1}(y)$, и наоборот. Это проясняет действие обратного оператора.

Легко понять, что не всякий оператор из L в L обратим. Не обратим, например, нулевой оператор O: для любого $B : L \to L$ выполняется $OB = BO = O \neq E$, поэтому O^{-1} не существует.

Из результатов этого пункта следует, что в случае $\dim L = n$ проверка обратимости линейного оператора сводится к проверке невырожденности (обратимости) его матрицы в произвольном базисе. Таким образом, и в этой тематике проявляется координатный подход.

Прежде всего заметим, что обращение — действие, не выводящее за пределы класса линейных операторов.

Теорема 1. *Пусть линейный оператор $A : L \to L$ обратим. Тогда оператор A^{-1} также является линейным.*

Доказательство. Для $x, y \in L$ и $\alpha, \beta \in \mathrm{R}$

$$\alpha x + \beta y = \alpha E(x) + \beta E(y) = \alpha A(A^{-1}(x)) + \beta A(A^{-1}(y)) =$$

$$= A(\alpha A^{-1}(x) + \beta A^{-1}(y)).$$

Мы воспользовались линейностью A. Применим к этому равенству оператор A^{-1}. С учётом определения 1 мы получим:

$$A^{-1}(\alpha x + \beta y) = \alpha A^{-1}(x) + \beta A^{-1}(y),$$

что и требовалось доказать.

Ниже мы считаем $\dim L = n$.

Определение 2. *Оператор $A : L \to L$, матрица которого в некотором базисе является невырожденной, называется невырожденным. Оператор, соответствующий вырожденной матрице, называется вырожденным.*

Как уже отмечалось, из невырожденности матрицы оператора в *некотором базисе* вытекает её невырожденность *в любом базисе* (см. следствие предыдущего пункта). Поэтому вместо первого выделенного курсивом фрагмента предыдущей фразы в определении 2 можно использовать второй; мы получим равносильное определение.

Теорема 2. *Невырожденность линейного оператора $A : L \to L$, $\dim L = n$, эквивалентна его обратимости. Матрицы операторов A и A^{-1} в любом базисе взаимно обратны.*

Доказательство. Пусть A — невырожденный оператор. В некотором базисе его матрица $\mathbf{A}$ является невырожденной, то есть обратимой. Рассмотрим тот оператор $B : L \to L$, матрица которого в том же базисе совпадает с $\mathbf{A}^{-1}$. В соответствии

с нашими предыдущими результатами матричное равенство $\mathbf{A}\mathbf{A}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{E}$ означает, что $AB = BA = E$, то есть $B = A^{-1}$. Итак, оператор A обратим.

Наоборот, существование обратного оператора A^{-1} гарантирует невырожденность матрицы оператора A в любом базисе.

Действительно, из операторного равенства $AA^{-1} = A^{-1}A = E$ следует $\mathbf{AB} = \mathbf{BA} = \mathbf{E}$. Здесь $\mathbf{B}$ — матрица оператора A^{-1} в базисе, которому соответствует матрица $\mathbf{A}$ оператора A. Поэтому в любом базисе $|\mathbf{A}| \neq 0$ и $\mathbf{B} = \mathbf{A}^{-1}$.

Теорема доказана.

Отметим простые свойства обратимых операторов, аналогичные соответствующим свойствам обратимых матриц.

Всегда

$$(A^{-1})^{-1} = A, \qquad (AB)^{-1} = B^{-1}A^{-1}. \tag{7}$$

Положим $A^{-j} := (A^{-1})^j,\ j \in \mathrm{N}$. Для всех целых k и l

$$(A^k)^{-1} = A^{-k}, \qquad A^{k+l} = A^k A^l. \tag{8}$$

Упражнение. Установить свойства (7) – (8).

8.6. Различные критерии невырожденности линейного оператора

Приведём утверждение о различных необходимых и достаточных условиях невырожденности линейного оператора $A : L \to L, \dim L = n$. Часть этих условий уже отмечалась.

Теорема. *Следующие условия эквивалентны (для любого оператора A они выполняются или не выполняются одновременно).*

1°. *Дефект A равен* 0.

2°. *Ранг A равен n .*

3°. $\mathrm{Ker}A = \{0\}$.

4°. $\mathrm{Im}A = L$ *, то есть A является сюръекцией.*

5°. *A является инъекцией, то есть для* $x_1 \neq x_2 \ \ A(x_1) \neq A(x_2)$.

6°. *A является биекцией (взаимно-однозначным отображением).*

7°. *A обратим, то есть существует* A^{-1}.

8°. *A переводит любую линейно независимую систему в линейно независимую (в частности, базис в базис).*

9°. *Матрица оператора A в некотором (а значит, и любом) базисе является невырожденной.*

Доказательство. Будем последовательно расширять набор равносильных условий, двигаясь сверху вниз.

Эквивалентность каждой пары условий $1° - 4°$ следует из теоремы о ранге и дефекте оператора, см. пункт 8.4, или является тривиальной (например, $1° \Longleftrightarrow 3°$).

$3° \Longrightarrow 5°$. Пусть $A(x_1) = A(x_2)$. Тогда $A(x_1 - x_2) = 0$, то есть $x_1 - x_2 \in \mathrm{Ker}A$. В силу 3° $x_1 = x_2$, то есть A является инъекцией.

$5^\circ \Longrightarrow 3^\circ$. Пусть A является инъекцией. Возьмём $x \in \mathrm{Ker}A$. Так как $A(x) = 0 = A(0)$, то обязательно $x = 0$. Значит, $\mathrm{Ker}A = \{0\}$.

Как известно, отображение $A : L \to L$ биективно тогда и только тогда, когда A одновременно является сюръекцией и инъекцией. Это обеспечивает импликации $4^\circ + 5^\circ \Longrightarrow 6^\circ$, $6^\circ \Longrightarrow 4^\circ$, $6^\circ \Longrightarrow 5^\circ$.

$6^\circ \Longleftrightarrow 7^\circ$ в силу общих результатов теории отображений: обратимыми являются лишь взаимно-однозначные отображения.

$3^\circ \Longrightarrow 8^\circ$. Пусть $e_1, \ldots, e_k$ — линейно независимая система. Рассмотрим равенство

$$\alpha_1 A(e_1) + \ldots + \alpha_k A(e_k) = 0.$$

Из линейности A следует, что $z := \sum \alpha_i e_i \in \mathrm{Ker}A$. Условие 3° даёт $z = 0$, поэтому $\alpha_1 = \ldots = \alpha_k = 0$.

$8^\circ \Longrightarrow 3^\circ$. Пусть $x \in \mathrm{Ker}A$. В случае выполнения 8° вектор x обязательно должен быть нулевым — иначе линейно независимая система x переходит в линейно зависимую систему $A(x) = 0$.

Наконец, результаты пунктов 8.4, 8.5 обеспечивают эквивалентность 9° и любого из условий $1^\circ - 4^\circ$, 7° .

Теорема доказана.

Замечание. Набор эквивалентных условий теоремы может быть дополнен ещё и следующим (оно обсуждается позднее в пункте 9.1):

10°. *A не имеет собственного значения $\lambda = 0$.*

Оператор, удовлетворяющий условию 9°, мы назвали невырожденным (см. определение 2 предыдущего пункта и замечание после него). Таким образом, $1^\circ - 8^\circ$ (и 10°) представляют собой различные, но эквивалентные *критерии невырожденности оператора.*

Интересно отметить, что для *линейных* отображений $A : L \to L$ требования сюръективности и инъективности равносильны.

Упражнение. Проверить выполнение каждого из условий теоремы для операторов: (i) поворота в V_2, *(ii) проектирования на плоскость в* V_3, *(iii) дифференцирования в* $\mathrm{R_n}[t]$.

8.7. Изменение матрицы линейного оператора при изменении базиса. Подобные матрицы

Простые примеры показывают, что матрицы одного и того же линейного оператора в двух различных базисах, вообще говоря, различны. Однако это изменение не может быть очень существенным: так, мы уже знаем, что ранги этих матриц обязательно совпадают (они равны размерности образа оператора).

В этом пункте мы получим явную формулу, связывающую матрицы оператора в двух базисах.

Пусть $e_1, \ldots, e_n$ и $f_1, \ldots, f_n$ — два базиса пространства L. Будем считать, что линейный оператор $A : L \to L$ имеет в этих базисах матрицы $\mathbf{A} = (a_{ij})$ и $\mathbf{B} = (b_{ij})$ соответственно.

Введём в рассмотрение матрицу перехода $\mathbf{C} = (c_{ij})$ от базиса $e_1, \ldots, e_n$ к базису $f_1, \ldots, f_n$. Напомним, что это невырожденная матрица, определяемая соотношениями

$$f_k = \sum_{i=1}^{n} c_{ik} e_i, \quad k = 1, \ldots, n. \tag{9}$$

Теорема. *Имеет место равенство*

$$\mathbf{B} = \mathbf{C}^{-1}\mathbf{A}\mathbf{C}. \tag{10}$$

Мы дадим два доказательства равенства (10). Первое доказательство использует понятие обратного оператора; второе базируется лишь на результатах пункта 8.2 и связи координат в различных базисах.

Доказательство 1. Введём в рассмотрение линейный оператор $C : L \to L$ такой, что $C(e_k) = f_k$, $k = 1, \ldots, n$. Существование и единственность такого оператора обоснованы в пункте 8.2. Ясно, что матрица оператора C в базисе $e_1, \ldots, e_n$ совпадает с $\mathbf{C}$, см. (9). Так как $\mathbf{C}$ является невырожденной, оператор C обратим, причём матрица обратного оператора в первом базисе совпадает с $\mathbf{C}^{-1}$ (пункт 8.5).

По определению матрицы линейного оператора

$$A(f_k) = \sum_{i=1}^{n} b_{ik} f_i.$$

Так как $f_k = C(e_k)$, то

$$A(C(e_k)) = \sum_{i=1}^{n} b_{ik} C(e_i).$$

Применим к последнему равенству оператор C^{-1} и воспользуемся его линейностью для преобразования правой части. Получим для $k = 1, \ldots, n$

$$C^{-1}AC(e_k) = \sum_{i=1}^{n} b_{ik} e_i.$$

Это означает, что матрица оператора $C^{-1}AC$ в базисе $e_1, \ldots, e_n$ совпадает с $\mathbf{B}$. Но, с другой стороны, она равна $\mathbf{C}^{-1}\mathbf{A}\mathbf{C}$, см. пункт 8.3. Тем самым соотношение (10) установлено.

Доказательство 2. Пусть $x \in L$ — произвольный вектор. Будем считать, что $x = \{\xi_1, \ldots, \xi_n\}$ в базисе $e_1, \ldots, e_n$ и $x = \{\eta_1, \ldots, \eta_n\}$ в базисе $f_1, \ldots, f_n$. Как известно, координаты одного и того же вектора в двух базисах связаны равенствами

$$\begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} = \mathbf{C} \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix}, \quad \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix} = \mathbf{C}^{-1} \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}.$$

Вектор $A(x)$ в базисе $e_1, \ldots, e_n$ имеет столбец координат

$$\mathbf{A}\begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix}.$$

Тот же вектор $A(x)$ в базисе $f_1,\ldots,f_n$ имеет столбец координат

$$\mathbf{B}\begin{pmatrix}\eta_1\\ \vdots\\ \eta_n\end{pmatrix}=\mathbf{B}\mathbf{C}^{-1}\begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix}.$$

Опять используя связь координат в различных базисах, получим матричное равенство

$$\mathbf{A}\begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix}=\mathbf{C}\mathbf{B}\mathbf{C}^{-1}\begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix}.$$

Последнее соотношение выполняется для всех $x=\{\xi_1,\ldots,\xi_n\}$. Взяв поочерёдно $x=e_1=\{1,\ldots,0\},\ldots,x=e_n=\{0,\ldots,1\}$, мы получим, что соответствующие столбцы матриц $\mathbf{A}$ и $\mathbf{C}\mathbf{B}\mathbf{C}^{-1}$ совпадают. Значит, $\mathbf{A}=\mathbf{C}\mathbf{B}\mathbf{C}^{-1}$, что эквивалентно (10). Доказательство закончено.

Матрицы $\mathbf{A},\mathbf{B}\in M_n$, для которых существует невырожденная матрица $\mathbf{C}\in M_n$ такая, что выполнено равенство (10), называются *подобными.*

Итак, *матрицы одного и того же линейного оператора $A: L\to L$ в двух базисах L подобны.*

Отметим некоторые свойства подобных матриц.

Пусть $\mathbf{B}=\mathbf{C}^{-1}\mathbf{A}\mathbf{C}$. Тогда

$$|\mathbf{B}|=|\mathbf{C}^{-1}\mathbf{A}\mathbf{C}|=|\mathbf{C}^{-1}||\mathbf{A}||\mathbf{C}|=|\mathbf{A}|$$

(мы применили теорему об определителе произведения матриц). В силу того, что $\mathbf{A}$ и $\mathbf{B}$ можно считать матрицами одного и того же оператора $A:\mathrm{R^n}\to\mathrm{R^n}$ в двух различных базисах, обязательно $\mathrm{rg}(\mathbf{B})=\mathrm{rg}(\mathbf{A})$ — это число равно $\dim\mathrm{Im}A$, то есть рангу оператора A. Таким образом, *подобные матрицы имеют одинаковые определители и ранги.*

Как мы покажем ниже (см. раздел 9), *совпадают и так называемые характеристические многочлены матриц* $\mathbf{B}$ *и* $\mathbf{A}$. Отсюда следует, что подобные матрицы имеют одинаковые собственные значения (они соответствуют действительным корням характеристического многочлена) и одинаковый след: $\mathrm{tr}(\mathbf{B})=\mathrm{tr}(\mathbf{A})$. Последнее связано с тем, что след матрицы с точностью до знака равен одному из коэффициентов её характеристического многочлена.

Нетрудно убедиться, что $\mathbf{B}^j=\mathbf{C}^{-1}\mathbf{A}^j\mathbf{C}$ для произвольного натурального j. Поэтому если $f(t)=\alpha_0+\alpha_1 t+\ldots+\alpha_k t^k$ — алгебраический многочлен, то

$$f(\mathbf{B})=\mathbf{C}^{-1}f(\mathbf{A})\mathbf{C}. \tag{11}$$

Это равенство распространяется также на *аналитические функции от матриц,* то есть такие функции, которые представляются сходящимися матричными степенными рядами:

$$f(\mathbf{A}) = \sum_{i=0}^{\infty} \alpha_i \mathbf{A}^i.$$

Тонкости и подробности этого подхода изложены в литературе по теории матриц (см., например, монографию Ф.Р. Гантмахера [5]).

Упражнение 1. Установить равенство (11) для многочлена f.

Наконец, отметим, что подобие является отношением эквивалентности на M_n. Это означает, что оно

(i) *рефлексивно*: $\mathbf{X} \sim \mathbf{X}$;

(ii) *симметрично*: $\mathbf{Y} \sim \mathbf{X}$ влечёт $\mathbf{X} \sim \mathbf{Y}$;

(iii) *транзитивно*: $\mathbf{Z} \sim \mathbf{Y}$ и $\mathbf{Y} \sim \mathbf{X}$ влечёт $\mathbf{Z} \sim \mathbf{X}$.

Здесь запись $\mathbf{Y} \sim \mathbf{X}$ означает, что матрица $\mathbf{Y}$ подобна матрице $\mathbf{X}$, то есть для некоторой $\mathbf{T} \in M_n$ (зависящей от исходной пары матриц) выполнено $\mathbf{Y} = \mathbf{T}^{-1}\mathbf{X}\mathbf{T}$.

Упражнение 2. Доказать, что отношение подобия обладает свойствами $(i)-(iii)$.

Как и любое отношение эквивалентности, отношение подобия разбивает множество M_n на непересекающиеся классы эквивалентности. Любой класс эквивалентности состоит из множества всех матриц, подобных любой заданной входящей в него матрице. Все матрицы из одного класса эквивалентности подобны, и никакие матрицы из двух разных классов не являются подобными.

Мы показали, что матрицы из одного класса эквивалентности обладают многими одинаковыми свойствами. Важнейшим и наиболее общим *инвариантом подобия* является *каноническая жорданова нормальная форма*, описание которой даётся в следующем разделе. Из инвариантности жордановой нормальной формы подобных матриц следует наличие у них всех тех инвариантов, о которых мы говорили выше.

8.8. Инвариантные подпространства линейного оператора

В заключение этого раздела обсудим следующее определение.

Определение. *Инвариантным подпространством оператора $A : L \to L$ называется подпространство $L_1 \subset L$, обладающее свойством: для каждого $x \in L_1$ его образ $A(x)$ также принадлежит L_1.*

Иначе говоря, L_1 является инвариантным для A, если имеет место включение $A(L_1) \subset L_1$. Здесь $A(L_1)$ обозначает *(полный) образ L_1 при отображении A*, то есть множество

$$A(L_1) := \{y \in L : \ y = A(x) \text{ для } x \in L_1\}.$$

Это включение может быть строгим, а может иметь форму равенства $A(L_1) = L_1$.

Если L_1 — инвариантное подпространство оператора A, то можно рассматривать оператор $A : L_1 \to L_1$, который называется *сужением, или следом оператора $A : L \to L$ на подпространство L_1*. Фактически это различные отображения, которые лишь для простоты обозначаются одной и той же буквой.

Ясно, что тривиальные линейные подпространства $\{0\}$ и всё L инвариантны для любого линейного оператора $A : L \to L$. Инвариантность первого из них связана с условием $A(0) = 0$.

В то же время, *не всякий линейный оператор, действующий в действительном пространстве L, имеет нетривиальное инвариантное подпространство.* Достаточно рассмотреть оператор $A : \mathrm{V}_2 \to \mathrm{V}_2$ поворота векторов на угол $\pi/2$; ясно, что $A(L_1) \not\subset L_1$ для любого подпространства L_1 размерности 1.

В следующих разделах мы покажем, что произвольный линейный оператор, действующий в *комплексном* линейном пространстве $L \neq \{0\}$, обязательно имеет *одномерное* инвариантное подпространство, а произвольный оператор, действующий в нетривиальном *действительном* линейном пространстве, имеет *одномерное или двумерное* инвариантное подпространство.

Отметим, что для любого оператора $A : L \to L$ его *ядро и образ являются инвариантными подпространствами.*

Действительно, если $x \in \mathrm{Ker}A$, то $A(x) = 0 \in \mathrm{Ker}A$. Условие $A(x) \in \mathrm{Im}A$ выполняется вообще для всех $x \in L$, а не только для $x \in \mathrm{Im}A$.

Примеры. 1. Для нулевого и тождественного операторов любое подпространство $L_1 \subset L$ является инвариантным.

2. Для оператора $P : \mathrm{V}_3 \to \mathrm{V}_3$ ортогонального проектирования на плоскость H инвариантными являются подпространства $L_1 = H$ и $L_2 := \{\vec{x} : \ \vec{x} \perp H\}$. Обратите внимание, что $\mathrm{V}_3 = L_1 \oplus L_2$.

3. Для оператора дифференцирования $D : \mathrm{R_n}[t] \to \mathrm{R_n}[t], n \in \mathrm{N}$, инвариантными являются все подпространства $\mathrm{R_k}[t], \ k = 0, \ldots, n-1$.

Упражнение 1. Показать, что других инвариантных подпространств, кроме тривиальных и указанных выше, в примерах 2 – 3 нет.

4. Пусть оператор $A : L \to L$ имеет в базисе e_1, e_2, e_3, e_4, e_5 матрицу

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

Тогда подпространства $L_1 := \mathrm{lin}(e_1, e_2)$ и $L_2 := \mathrm{lin}(e_1, e_2, e_3)$ инвариантны относительно оператора A.

Действительно, $A(e_1) = e_1 - e_2 \in L_1, \ A(e_2) = 2e_1 + e_2 \in L_1$. Значит, образ любого вектора $x = \alpha_1 e_1 + \alpha_2 e_2$ из L_1 также принадлежит L_1. Аналогично, если $x \in L_2$, то и $A(x) \in L_2$.

В этом примере L представляется в виде прямой суммы двух инвариантных подпространств: $L = L_1 \oplus L_2$, а матрица $\mathbf{A}$ содержит две ненулевые клетки, расположенные на главной диагонали.

5. Пусть $A : C[0,1] \to C[0,1]$ — оператор, задаваемый равенством

$$Ax(t) := \int_0^t x(s)ds, \quad t \in [0,1].$$

Для этого оператора $C^1[0,1]$ является нетривиальным инвариантным бесконечномерным подпространством.

Упражнение 2. Определить, имеет ли место равенство $A(W) = W$ или строгое включение $A(W) \subset W$ для каждого из перечисленных в примерах 1 – 5 инвариантных подпространств W.

Отметим, наконец, что разложение пространства L размерности n в прямую сумму инвариантных относительно оператора $A : L \to L$ подпространств:

$$L = L_1 \oplus L_2 \oplus \ldots \oplus L_k, \tag{12}$$

эквивалентно представлению матрицы оператора A в некотором базисе в *клеточном виде*:

$$\mathbf{A} = \begin{pmatrix} \mathbf{A_1} & & & 0 \\ & \mathbf{A_2} & & \\ & & \ddots & \\ 0 & & & \mathbf{A_k} \end{pmatrix}. \tag{13}$$

Все элементы матрицы $\mathbf{A}$ равны 0, кроме элементов квадратных подматриц $\mathbf{A_i}$, стоящих на главной диагонали.

Действительно, если имеет место разложение (12), то базис L может быть получен объединением базисов L_i. Так как каждое из L_i инвариантно относительно A, то базисные векторы каждой из k групп переходят под действием A в линейные комбинации векторов той же группы. Это означает, что в базисе L, полученном объединением этих совокупностей векторов, матрица оператора A будет иметь вид (13).

Наоборот, если в некотором базисе матрица оператора имеет клеточную форму (13), то группы векторов, соответствующие клеткам $\mathbf{A_i}$, порождают инвариантные подпространства L_i — линейные оболочки этих групп векторов (см. для иллюстрации пример 4). Сумма L_i является прямой, так как выполнено равенство $\sum \dim L_i = \dim L = n$, см. пункт 6.3. Поэтому имеет место (12).

9. Собственные векторы, собственные значения, диагонализируемость и каноническая форма матрицы линейного оператора

Если в линейном пространстве L имеются ненулевые векторы, на которых действие данного оператора сводится к умножению их на число, то они называются *собственными векторами* этого оператора.

Обнаружение собственных векторов и соответствующих им числовых множителей — *собственных значений* — позволяет получить важную информацию об операторе, которая может быть существенно использована в приложениях.

В ситуации, когда всё пространство представляется в виде прямой суммы собственных подпространств, оператор является *диагонализируемым* — существует базис, в котором матрица такого оператора диагональна.

Глубоким обобщением этого результата на произвольные операторы, действующие в комплексном линейном пространстве, является *теорема о канонической форме матрицы оператора.* Согласно этой теореме, матрица *любого* оператора может быть приведена к некоторому простейшему виду — так называемой *жордановой нормальной форме.*

Доказательство этой сложной теоремы читатель может найти, например, в учебнике А.И. Кострикина [14] или в книге И.М. Гельфанда [7]. В этом тексте мы ограничиваемся её формулировкой и подробными комментариями.

Одним из первых, кто рассматривал нормальную форму матрицы, был известный французский математик Камиль Жордан (C. Jordan, 1838 – 1922). Соответствующая работа Жордана опубликована в 1870 г.

9.1. Собственные векторы и собственные значения: определение и простейшие свойства

Пусть $A : L \to L$ — линейный оператор, действующий в действительном линейном пространстве L.

Определение. *Собственным вектором оператора A называется такой вектор $x \neq 0$, для которого при некотором $\lambda \in \mathrm{R}$ выполнено равенство*

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

Число λ из (1) называется соответствующим x собственным значением оператора A. Совокупность всех собственных значений оператора называется его спектром.

Геометрически (1) означает, что под действием оператора A собственный вектор переходит в коллинеарный себе.

Аналогично определяется собственный вектор и собственное значение оператора, действующего в комплексном линейном пространстве; в этом случае $\lambda \in \mathrm{C}$. Основные свойства справедливы и в комплексном варианте. Разница между действительной и комплексной ситуациями всегда специально отмечается.

Определение касается и операторов в бесконечномерных пространствах. Для них совокупность собственных значений называется *точечным спектром*, подробнее см. замечания в конце следующего пункта. Важные задачи, связанные с поиском собственных значений и *собственных функций* дифференциальных, интегральных и других операторов в функциональных пространствах, часто возникают на практике и являются предметом специального изучения прикладных разделов анализа.

За исключением простых примеров этого пункта и замечания 1 пункта 9.2 мы ограничиваемся конечномерной ситуацией.

Обратим особое внимание на ограничение $x \neq 0$ — собственный вектор по определению является ненулевым. В то же время собственное значение λ может равняться нулю. Если $\lambda = 0$, то $A(x) = 0$ для некоторого $x \neq 0$. Это эквивалентно условию $\mathrm{Ker}A \neq \{0\}$. В конечномерной ситуации такой оператор является вырожденным — его матрица $\mathbf{A}$ в любом базисе такова, что $|\mathbf{A}| = 0$.

Сказанное означает, что *оператор $A : L \to L$, $\dim L = n$, является невырожденным тогда и только тогда, когда A не имеет собственного значения $\lambda = 0$.* Мы отмечали это условие в замечании после доказательства теоремы пункта 8.6.

Примеры. 1. Для нулевого и тождественного операторов, действующих в пространстве $L \neq \{0\}$, каждый вектор $x \neq 0$ является собственным. Собственные значения равны 0 и 1 для O и E соответственно. Это сразу следует из равенств $O(x) = 0$ и $E(x) = x$.

2. Пусть $A_\varphi : \mathrm{V}_2 \to \mathrm{V}_2$ — оператор поворота на угол φ против часовой стрелки, $0 \leqslant \varphi < 2\pi$. Геометрически очевидно, что A_φ имеет собственные векторы лишь для $\varphi = 0$ или $\varphi = \pi$. В любой из ситуаций каждый $\vec{x} \neq \vec{0}$ является собственным. Собственные значения операторов равны соответственно 1 и -1.

3. Для оператора $P : \mathrm{V}_3 \to \mathrm{V}_3$ ортогонального проектирования на плоскость H нетрудно выделить два класса собственных векторов. Для $\vec{x} \in H$ собственное значение $\lambda_1 = 1$; для $\vec{x} \perp H \quad \lambda_2 = 0$. Ясно, что других собственных векторов и собственных значений нет.

Упражнение 1. Пусть $\dim L = n \geqslant 2, P : L \to L$ — ненулевой проектор на собственное подпространство L_1. Доказать, что P имеет собственные значения 1 и 0. Напомним, что проектор обладает свойством $P^2 = P$.

4. Для оператора дифференцирования $D : \mathrm{R_n}[t] \to \mathrm{R_n}[t]$, $n = 0, 1, \ldots$, собственными векторами являются лишь ненулевые многочлены из $\mathrm{R}_0[t]$ (константы); собственное значение $\lambda = 0$. Для многочленов ненулевой степени равенство $Df(t) = = f'(t) = \lambda f(t)$ невозможно (дифференцирование понижает степень).

5. Тот же оператор $Dx(t) := x'(t)$, действующий в бесконечномерном пространстве $C^1[0, 1]$, имеет бесконечное число собственных значений. Уравнение $x' = \lambda x$, $x(\cdot) \in C^1[0, 1]$, имеет ненулевые решения при *любом* $\lambda \in \mathrm{R}$, а именно $x(t) = Ce^{\lambda t}$, $C \neq 0$; они являются собственными функциями оператора D. Совокупность собственных значений совпадает со всем R.

6. Оператор $A : C[-1, 1] \to C[-1, 1]$, определяемый равенством $Ax(t) := x(-t)$,

имеет собственные значения $\lambda_1 = 1$, $\lambda_2 = -1$. Собственные функции являются соответственно чётными и нечётными и в этих пределах могут быть произвольными.

Действительно, $x(-t) = \lambda x(t), t \in [-1, 1]$, даёт после замены t на $-t$ тождество $x(t) \equiv \lambda^2 x(t)$. В силу $x(t) \not\equiv 0$ имеем $\lambda = \pm 1$.

7. Оператор $Ax(t) := tx(t)$ в пространстве $C[0, 1]$ не имеет собственных значений. Равенство $(\lambda - t)x(t) = 0, t \in [0, 1]$, при любом фиксированном $\lambda \in \mathrm{R}$ возможно лишь для $x(t) \equiv 0$.

Как мы увидим в следующем пункте, нахождение собственных значений оператора в конечномерном пространстве сводится к решению некоторого алгебраического уравнения, а нахождение собственных векторов — к решению системы линейных уравнений.

Отметим некоторые свойства собственных векторов и собственных значений.

Наличие собственного вектора оператора $A : L \to L$ эквивалентно наличию у A одномерного инвариантного подпространства L_1.

Действительно, если x — собственный вектор, соответствующий собственному значению λ, то $L_1 := \mathrm{lin}(x) = \{\mu x, \mu \in \mathrm{R}\}$ инвариантно относительно A:

$$A(\mu x) = \mu A(x) = \lambda \mu x \in L_1.$$

Наоборот, если $L_1 = \mathrm{lin}(x)$ инвариантно относительно A, то для базисного вектора $x \neq 0$ выполняется $A(x) \in L_1$, то есть $A(x) = \lambda x$ для некоторого λ.

Если $x_1, \ldots, x_k$ — собственные векторы оператора A, соответствующие одному и тому же собственному значению λ, то их любая линейная комбинация, не равная 0, является собственным вектором A с тем же λ :

$$A(\sum_{i=1}^{k} \tau_i x_i) = \sum_{i=1}^{k} \tau_i A(x_i) = \lambda \sum_{i=1}^{k} \tau_i x_i.$$

Наконец, отметим следующее утверждение.

Теорема. *Собственные векторы $e_1, \ldots, e_k$, соответствующие попарно различным собственным значениям $\lambda_1, \ldots, \lambda_k$ оператора A, линейно независимы.*

Доказательство (индукция по числу k векторов). При $k = 1$ утверждение очевидно, так как $e_1 \neq 0$.

Пусть утверждение верно для $e_1, \ldots, e_{k-1}$. Рассмотрим равенство

$$\alpha_1 e_1 + \ldots + \alpha_{k-1} e_{k-1} + \alpha_k e_k = 0. \tag{2}$$

Применим к (2) оператор A, воспользуемся его линейностью и равенствами $A(e_i) = = \lambda_i e_i$:

$$\alpha_1 \lambda_1 e_1 + \ldots + \alpha_{k-1} \lambda_{k-1} e_{k-1} + \alpha_k \lambda_k e_k = 0. \tag{3}$$

Умножим (2) на λ_k и затем вычтем (3):

$$\alpha_1 (\lambda_k - \lambda_1) e_1 + \ldots + \alpha_{k-1} (\lambda_k - \lambda_{k-1}) e_{k-1} = 0.$$

В силу предположения индукции $e_1, \ldots, e_{k-1}$ линейно независимы, то есть все коэффициенты в левой части равны 0. Так как $\lambda_k \neq \lambda_i, i = 1, \ldots, k-1$, то $\alpha_1 = = \ldots = \alpha_{k-1} = 0$. Равенство (2) гарантирует, что и $\alpha_k = 0$ (собственный вектор $e_k \neq 0$).

Таким образом, $e_1, \ldots, e_k$ линейно независимы.

Теорема доказана.

Упражнение 2. Доказать, что если x — собственный вектор оператора A, относящийся к собственному значению λ, то x является собственным вектором для операторов: (i) μA, (ii) $A^k, k \in \mathrm{N}$, (iii) $f(A)$, f — многочлен. Найти соответствующие собственные значения.

Упражнение 3. Верно ли утверждение: если x — собственный вектор оператора $f(A)$, f — некоторый многочлен, то x является собственным вектором оператора A?

Упражнение 4. Пусть оператор A обратим. Доказать, что A и A^{-1} имеют одно и то же множество собственных векторов.

9.2. Характеристический многочлен линейного оператора. Вычисление собственных значений и собственных векторов

Пусть $\dim L = n$, $A : L \to L$ — линейный оператор. Зафиксируем некоторый базис $e_1, \ldots, e_n$ и сопоставим оператору A его матрицу $\mathbf{A} = (a_{ij}) \in M_n$ в этом базисе.

Определение. *Характеристическим многочленом оператора A называется определитель матрицы $\mathbf{A} - \lambda\mathbf{E}$:*

$$p(\lambda) := |\mathbf{A} - \lambda\mathbf{E}| = \begin{vmatrix} a_{11} - \lambda & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} - \lambda & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} - \lambda \end{vmatrix}. \tag{4}$$

Очевидно, что $p(\lambda)$ является многочленом от λ степени n, коэффициенты которого определяются по элементам матрицы $\mathbf{A}$, то есть являются действительными или комплексными числами в зависимости от ситуации. Оба случая (действительного или комплексного L) мы будем рассматривать одновременно.

Многочлен $p(\lambda)$ удобно разложить по степеням $(-\lambda)^k$:

$$p(\lambda) = b_0 + b_1(-\lambda) + \ldots + b_{n-1}(-\lambda)^{n-1} + (-\lambda)^n.$$

В такой форме записи b_k *есть сумма всех главных миноров матрицы* $\mathbf{A}$ *порядка* $n - k$ (миноров, образованных строками и столбцами с одинаковыми номерами).

Действительно, произведение k выделенных диагональных элементов матрицы $\mathbf{A} - \lambda\mathbf{E}$ входит в $p(\lambda)$ с числовым множителем, равным главному минору матрицы $\mathbf{A}$, который получается из неё удалением k отмеченных строк и столбцов. Ясно, что b_k есть сумма всех таких множителей.

В частности, $b_0 = |\mathbf{A}|$ — определитель, $b_{n-1} = \mathrm{tr}(\mathbf{A}) = \sum a_{ii}$ — след матрицы $\mathbf{A}$.

В стандартном виде $p(\lambda) = p_0 + p_1\lambda + \ldots + p_{n-1}\lambda^{n-1} + p_n\lambda^n$ коэффициенты равны $p_k = (-1)^k b_k,\ k = 0, \ldots, n$.

Примеры. 1. Характеристические многочлены нулевого и тождественного операторов есть соответственно $f(\lambda) = (-\lambda)^n = (-1)^n\lambda^n$ и $g(\lambda) = (1-\lambda)^n$.

2. Характеристический многочлен оператора дифференцирования $D : \mathrm{R_n}[t] \to \mathrm{R_n}[t]$, вычисленный по её матрице $\mathbf{D}$ в базисе $1, t, \ldots, t^n$ (её ненулевые элементы имеют вид $d_{i+1,i} = i$), равен $p(\lambda) = (-1)^{n+1}\lambda^{n+1}$.

3. Пусть матрица $\mathbf{A}$ имеет верхний треугольный вид, то есть все её элементы ниже главной диагонали равны 0. Многочлен $p(\lambda)$, определяемый формулой (4), равен, очевидно,

$$p(\lambda) = (a_{11} - \lambda)(a_{22} - \lambda)\ldots(a_{nn} - \lambda).$$

4. Пусть $p(\lambda) = p_0 + p_1\lambda + p_2\lambda^2 + p_3\lambda^3 + \lambda^4$ — характеристический многочлен оператора с матрицей

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & -1 & 2 \\ 2 & 4 & 3 & -2 \\ -4 & -2 & 0 & 3 \\ 5 & 2 & -4 & -3 \end{pmatrix}.$$

В предыдущих обозначениях $p_0 = b_0 = |\mathbf{A}| = 108$,

$$p_1 = -b_1 = -\begin{vmatrix} 4 & 3 & -2 \\ -2 & 0 & 3 \\ 2 & -4 & -3 \end{vmatrix} - \begin{vmatrix} 1 & -1 & 2 \\ -4 & 0 & 3 \\ 5 & -4 & -3 \end{vmatrix} -$$

$$- \begin{vmatrix} 1 & 0 & 2 \\ 2 & 4 & -2 \\ 5 & 2 & -3 \end{vmatrix} - \begin{vmatrix} 1 & 0 & -1 \\ 2 & 4 & 3 \\ -4 & -2 & 0 \end{vmatrix} = -32 - 41 + 40 + 6 = -27,$$

$$p_2 = b_2 = \begin{vmatrix} 0 & 3 \\ -4 & -3 \end{vmatrix} + \begin{vmatrix} 4 & -2 \\ 2 & -3 \end{vmatrix} + \begin{vmatrix} 4 & 3 \\ -2 & 0 \end{vmatrix} +$$

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

$$= 12 - 8 + 6 - 13 - 4 + 4 = -3,$$

$$p_3 = -b_3 = -\mathrm{tr}(\mathbf{A}) = -(1 + 4 + 0 - 3) = -2.$$

Таким образом, $p(\lambda) = 108 - 27\lambda - 3\lambda^2 - 2\lambda^3 + \lambda^4$.

При вычислении характеристического многочлена оператора по формуле (4) может использоваться произвольный исходный базис L — результат будет одним и тем же.

Теорема 1. *Характеристический многочлен оператора не зависит от базиса, в котором записана его матрица.*

Доказательство. Пусть $\mathbf{A}$ и $\mathbf{B}$ — матрицы одного и того же оператора A в двух различных базисах. Тогда они связаны преобразованием подобия: $\mathbf{B} = \mathbf{C}^{-1}\mathbf{A}\mathbf{C}$.

Здесь $\mathbf{C}$ — невырожденная матрица перехода от одного базиса к другому, см. пункт 8.7. Но тогда по теореме об определителе произведения матриц

$$|\mathbf{B}-\lambda\mathbf{E}| = |\mathbf{C}^{-1}\mathbf{A}\mathbf{C}-\lambda\mathbf{E}| = |\mathbf{C}^{-1}\mathbf{A}\mathbf{C}-\mathbf{C}^{-1}(\lambda\mathbf{E})\mathbf{C}| =$$

$$= |\mathbf{C}^{-1}(\mathbf{A}-\lambda\mathbf{E})\mathbf{C}| = |\mathbf{C}^{-1}||\mathbf{A}-\lambda\mathbf{E}||\mathbf{C}| = |\mathbf{A}-\lambda\mathbf{E}|.$$

Мы использовали также свойства умножения матриц. Теорема доказана.

Итак, коэффициенты, а значит, и корни характеристического многочлена не зависят от выбора базиса — они являются инвариантами самого линейного оператора.

Основным результатом пункта является следующая теорема.

Теорема 2. *Число λ из основного поля является собственным значением оператора A тогда и только тогда, когда λ является корнем характеристического многочлена $p(\lambda)$.*

Доказательство. Собственный вектор x и собственное значение λ оператора A определяются условиями

$$(A-\lambda E)(x) = 0, \quad x \neq 0,$$

или в координатном виде

$$(\mathbf{A}-\lambda\mathbf{E})\begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix} = \begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}, \quad (\xi_1,\ldots,\xi_n) \neq (0,\ldots,0). \tag{5}$$

Здесь $x = \{\xi_1,\ldots,\xi_n\}$ в базисе, соответствующем матрице оператора $\mathbf{A}$. Число λ является собственным значением оператора тогда и только тогда, когда система линейных однородных уравнений из (5) имеет ненулевое решение $(\xi_1,\ldots,\xi_n)$. Это возможно тогда и только тогда, когда определитель матрицы системы $|\mathbf{A}-\lambda\mathbf{E}| = p(\lambda)$ равен 0, см. раздел 4.

Теорема доказана.

Таким образом, поиск собственных значений оператора связан с решением в основном поле алгебраического уравнения $p(\lambda) = 0$, называемого *характеристическим уравнением.* В действительной ситуации ищутся все *действительные* корни $p(\lambda)$, в комплексной — все *комплексные* корни. Для каждого найденного собственного значения λ соответствующие собственные векторы в координатном виде находятся затем из системы (5).

Следствие 1. *Каждый линейный оператор, действующий в комплексном линейном пространстве произвольной размерности $n \in \mathrm{N}$, имеет собственный вектор.*

Следствие 2. *Каждый линейный оператор, действующий в действительном линейном пространстве нечётной размерности $n = 2k+1$, имеет собственный вектор.*

Доказательство следствий очевидно. В комплексной ситуации $p(\lambda)$ — многочлен степени $n \geqslant 1$ с комплексными коэффициентами; такой многочлен обязательно имеет корень $\lambda_0 \in \mathrm{C}$ по *основной теореме алгебры многочленов,* см. пункт 14.4.

В действительной ситуации $p(\lambda)$ — многочлен с действительными коэффициентами. Если его степень n нечётна, то этот многочлен имеет *действительный* корень. Это связано с тем, что комплексные корни многочлена с действительными коэффициентами являются попарно сопряжёнными (кратности сопряжённых корней из одной пары одинаковы). Так как общее число корней с учётом кратностей нечётно, а именно равно n, то некоторый корень $\lambda_0 \in \mathrm{C}$ совпадает с сопряжённым себе; значит, $\lambda_0 \in \mathrm{R}$.

Наличие же собственного значения оператора эквивалентно наличию у него собственного вектора.

Упражнение 1. Используя характеристический многочлен, определить собственные значения для операторов из примеров 1 – 4 предыдущего пункта. Найти затем собственные векторы из системы (5).

Упражнение 2. Почему подобные матрицы имеют одинаковый след? Это свойство мы отмечали в пункте 8.7.

Упражнение 3. Показать, что след комплексной матрицы порядка n равен сумме её собственных значений λ_i с учётом их кратностей как корней $p(\lambda)$. Использовать каноническое разложение

$$p(\lambda) = (-1)^n(\lambda - \lambda_1)\dots(\lambda - \lambda_n).$$

Замечание. Дополним свойства характеристического многочлена, приведённые в этом пункте, формулировкой следующего утверждения, известного как *теорема Гамильтона – Кэли.*

Пусть $\mathbf{A} \in M_n$ и $p(\lambda) := |\mathbf{A} - \lambda\mathbf{E}|$. Тогда $p(\mathbf{A}) = \mathbf{0}$.

Доказательство см., например, в [14], [7]. Случай $n = 2$ проверяется прямым вычислением и предоставляется читателю. Эта теорема названа именами ирландца Уильяма Гамильтона (W. Hamilton, 1805 – 1856) и англичанина Артура Кэли (A. Cayley, 1821 – 1856).

Упражнение 4. Пусть $\mathbf{A} \in M_2$ и $\mathbf{A}^k = \mathbf{0}$ для некоторого $k > 2$. Доказать, что $\mathbf{A}^2 = \mathbf{0}$.

Мы не рассматриваем в этом пункте важные *вопросы о локализации собственных значений матрицы* $\mathbf{A}$. См. по этому поводу вторую часть пункта 14.7 или, более подробно, монографию [26].

В заключение сделаем ряд замечаний (необязательных для начинающих), касающихся операторов в бесконечномерных пространствах. Эта ситуация в настоящем разделе больше рассматриваться не будет.

Пусть $A : L \to L$. Если L конечномерно, то для каждого числа λ из основного поля существует две возможности:

1°. Уравнение $A(x) = \lambda x$ имеет ненулевое решение x, то есть λ есть собственное значение для A; при этом оператор $(A - \lambda E)^{-1}$ не существует.

2°. Уравнение $A(x) = \lambda x$ имеет лишь нулевое решение; оператор $(A - \lambda E)^{-1}$ определён на всём пространстве.

Но если L — бесконечномерное пространство, то добавляется ещё третья возможность:

3°. Уравнение $A(x) = \lambda x$ имеет лишь нулевое решение, но оператор $(A - \lambda E)^{-1}$ определён *не на всём пространстве* L.

Оператор $(A - \lambda E)^{-1}$, используемый в этом анализе, называется *резольвентой оператора* A. Числа λ, удовлетворяющие 2°, называются *регулярными.* Множество чисел λ, удовлетворяющих 3°, называется *непрерывным спектром оператора* — в отличие от *точечного спектра*, то есть собственных значений из условия 1°.

Возможность наличия у оператора непрерывного спектра — существенная особенность операторов в бесконечномерных пространствах.

Пример 5. Как отмечалось в пункте 9.1 (пример 7), оператор $A : C[0,1] \to C[0,1]$, задаваемый равенством $Ax(t) := tx(t)$, не имеет собственных значений. Резольвента имеет вид

$$(A - \lambda E)^{-1}x(t) = \frac{1}{t - \lambda}x(t).$$

Последний оператор при каждом $\lambda \in [0,1]$ определён не на всём $C[0,1]$ (почему?). В связи с этим оператор A имеет непустой непрерывный спектр, а именно отрезок $[0,1]$. Регулярные точки A составляют множество $\mathrm{R} \setminus [0,1]$.

Подробнее эти интересные вопросы изучаются в курсе функционального анализа, см., например, [13].

Всюду далее в этом разделе $\dim L = n, n \in \mathrm{N}$.

9.3. Собственное подпространство оператора. Алгебраическая и геометрическая кратности собственного значения, их соотношение

Пусть λ — собственное значение оператора $A : L \to L$.

Определение 1. *Совокупность всех $x \in L$, удовлетворяющих условию $A(x) = \lambda x$, называется собственным подпространством оператора A, соответствующим λ, и обозначается P_λ.*

Таким образом, P_λ есть множество всех собственных векторов, соответствующих λ, пополненное нулевым вектором. Очевидно также, что

$$P_\lambda = \{x \in L : \ (A - \lambda E)(x) = 0\} = \mathrm{Ker}(A - \lambda E). \tag{6}$$

В соответствии с (6) P_λ действительно является линейным подпространством (как ядро линейного оператора $A - \lambda E$). Этот факт легко следует также из свойств собственных векторов, отмеченных в пункте 9.1.

Упражнение 1. Показать, что каждое собственное подпространство оператора является для него инвариантным.

Определение 2. *Кратность собственного значения λ как корня характеристического многочлена называется его алгебраической кратностью и обозначается a_λ. Число $g_\lambda := \dim P_\lambda$ называется геометрической кратностью собственного значения λ.*

Установим соотношение между алгебраической и геометрической кратностями одного и того же собственного значения.

Теорема 1. *Для любого собственного значения λ_0*

$$1 \leqslant g_{\lambda_0} \leqslant a_{\lambda_0} \leqslant n. \tag{7}$$

Доказательство. Левое неравенство эквивалентно тому, что $P_{\lambda_0} \neq \{0\}$. Но так как λ_0 — собственное значение, то P_{λ_0} содержит ненулевой вектор (произвольный собственный вектор, соответствующий λ_0).

Правое неравенство в (7) следует из определения a_λ и основной теоремы алгебры многочленов (кратность любого корня характеристического многочлена $p(\lambda)$ не превосходит n).

Докажем среднее неравенство. Пусть $s := g_{\lambda_0}$. Дополним некоторый базис e_1, $\ldots$, e_s собственного подпространства P_{λ_0} векторами $e_{s+1}, \ldots, e_n$ до базиса всего L. Так как $e_1, \ldots, e_s \in P_{\lambda_0}$, то

$$A(e_j) = \lambda_0 e_j, \qquad j = 1, \ldots, s.$$

Поэтому в построенном базисе L матрица оператора A будет иметь вид:

$$\mathbf{A} = \begin{pmatrix} \lambda_0 & 0 & \ldots & 0 & a_{1,s+1} & \ldots & a_{1n} \\ 0 & \lambda_0 & \ldots & 0 & a_{2,s+1} & \ldots & a_{2n} \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & \lambda_0 & a_{s,s+1} & \ldots & a_{sn} \\ & & & & a_{s+1,s+1} & \ldots & a_{s+1,n} \\ & 0 & & & \vdots & & \vdots \\ & & & & a_{n,s+1} & \ldots & a_{nn} \end{pmatrix}.$$

Нетрудно видеть, что

$$p(\lambda) = |\mathbf{A} - \lambda \mathbf{E}| = (\lambda_0 - \lambda)^s q(\lambda),$$

где $q(\lambda)$ — многочлен степени $n - s$. Поэтому $a_{\lambda_0} \geqslant s = g_{\lambda_0}$.

Теорема доказана.

Полученное соотношение означает, что если $a_\lambda = 1$, то и $g_\lambda = 1$; если $g_\lambda = n$, то и $a_\lambda = n$. Возможны и некоторые другие простые варианты.

Пример. Пусть $A : \mathrm{R^n} \to \mathrm{R^n}$ — оператор, матрица которого в каноническом базисе $\mathrm{R^n}$ состоит из одних единиц. Условие $A(x) = \lambda x$, $x = (\xi_1, \ldots, \xi_n) \in \mathrm{R^n}$ сводится к системе уравнений

$$\xi_1 + \ldots + \xi_n = \lambda \xi_j, \ j = 1, \ldots, n.$$

Ненулевые решения системы соответствуют значениям $\lambda_1 = 0$ и $\lambda_2 = n$. Действительно, для λ, отличного от 0 и n, получаем последовательно $\xi_1 = \ldots = \xi_n = t$ и $nt = \lambda t$, то есть $t = 0$. Итак, оператор имеет два собственных подпространства:

$$P_1 = P_{\lambda_1} = \{x : \ \xi_1 + \ldots + \xi_n = 0\},$$
$$P_2 = P_{\lambda_2} = \{x : \ x = (t, \ldots, t), \ t \in \mathrm{R}\}.$$

Как нетрудно убедиться, $g_1 = g_{\lambda_1} = n - 1, \ g_2 = g_{\lambda_2} = 1$. Пусть $a_j = a_{\lambda_j}, \ j = 1, 2$. Так как $g_j \leqslant a_j$, то обязательно $a_1 = n - 1, a_2 = 1$ (иначе $a_1 + a_2 > n$).

Таким образом, $p(\lambda) = (-1)^n \lambda^{n-1}(\lambda - n)$. Трюк состоит в том, что мы определили характеристический многочлен косвенным путём.

Упражнение 2. Определить характеристический многочлен оператора из последнего примера прямым вычислением.

Установим также одно свойство собственных подпространств, используемое в следующем пункте.

Теорема 2. *Пусть $P_1, \ldots, P_k$ — собственные подпространства оператора A, соответствующие попарно различным собственным значениям $\lambda_1, \ldots, \lambda_k$. Тогда их сумма S является прямой:*

$$S := P_1 + \ldots + P_k = P_1 \oplus \ldots \oplus P_k \tag{8}$$

Доказательство. Достаточно показать, что соотношение $x_1 + \ldots + x_k = 0$, $x_j \in P_j$, возможно лишь в ситуации $x_1 = \ldots = x_k = 0$, см. пункт 6.3. Применяя к этому соотношению $k - 1$ раз оператор A и пользуясь тем, что $A(x_j) = \lambda_j x_j$, $j = 1, \ldots, k$, получим систему векторных равенств

$$\begin{gathered}
x_1 + \ldots + x_k = 0, \\
\lambda_1 x_1 + \ldots + \lambda_k x_k = 0, \\
\lambda_1^2 x_1 + \ldots + \lambda_k^2 x_k = 0, \\
\ldots \qquad \ldots \\
\lambda_1^{k-1} x_1 + \ldots + \lambda_k^{k-1} x_k = 0.
\end{gathered}$$

Перепишем эту систему в следующем обобщённом матричном виде:

$$\mathbf{V} \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{9}$$

В (9) обобщённый вектор-столбец, компоненты x_j которого есть элементы L, умножается на числовую матрицу $\mathbf{V}$ порядка k; результат умножения — столбец из k нулей L. Матрица $\mathbf{V}$ имеет структуру Вандермонда:

$$\mathbf{V} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \lambda_1 & \lambda_2 & \ldots & \lambda_k \\ \vdots & \vdots & & \vdots \\ \lambda_1^{k-1} & \lambda_2^{k-1} & \ldots & \lambda_k^{k-1} \end{pmatrix}.$$

Так как λ_j попарно различны, то $|\mathbf{V}| \neq 0$ (см. пункт 4.6 для действительной ситуации; комплексный вариант получается аналогично). Значит, существует обратная матрица $\mathbf{V}^{-1}$. После умножения (9) на $\mathbf{V}^{-1}$ мы получим, что столбец из векторов x_j совпадает со столбцом нулей. Итак, $x_1 = \ldots = x_k = 0$, и равенство (8) установлено.

Теорема доказана.

Следствие. *В обозначениях теоремы* $\dim S = \sum \dim P_j$.

Для доказательства достаточно учесть, что размерность прямой суммы k линейных подпространств равна сумме размерностей этих подпространств, как отмечалось в пункте 6.3.

9.4. Операторы простой структуры. Критерий диагонализируемости

При операциях с матрицами весьма существенна их *разреженность* (большая доля нулевых элементов) и упорядоченность их структуры. Насколько просто в этом смысле может выглядеть матрица данного оператора, если менять базис, в котором она записана? В 9.5 даётся исчерпывающий ответ для операторов в комплексном пространстве.

В этом пункте исследуются операторы, матрица которых может быть приведена к диагональному виду. Одновременно изучается вопрос о том, какие квадратные матрицы подобны диагональным.

Пусть L — n-мерное линейное пространство над полем F, $F = \mathrm{R}$ или C.

Определение. *Предположим, что для оператора $A : L \to L$ существует базис, в котором его матрица является диагональной. Такой оператор называется оператором простой структуры, или диагонализируемым.*

Если в базисе $e_1, \ldots, e_n$ матрица оператора A имеет диагональный вид:

$$\mathbf{A} = \mathrm{diag}_n(\mu_1, \ldots, \mu_n) = \begin{pmatrix} \mu_1 & & & 0 \\ & \mu_2 & & \\ & & \ddots & \\ 0 & & & \mu_n \end{pmatrix}, \tag{10}$$

то, очевидно, $A(e_j) = \mu_j e_j$, то есть e_j является собственным вектором, соответствующим собственному значению μ_j. Наоборот, если базис $e_1, \ldots, e_n$ состоит из собственных векторов оператора A, то выполнены равенства $A(e_j) = \mu_j e_j$, в связи с чем матрица оператора A в этом базисе имеет вид (10).

Поэтому *оператор A является оператором простой структуры тогда и только тогда, когда в L существует базис из собственных векторов A.*

Отметим сначала следующую простую ситуацию.

Утверждение. *Пусть оператор A имеет n различных собственных значений $\mu_1, \ldots, \mu_n$. Тогда A является диагонализируемым.*

Доказательство очевидно. В соответствии с теоремой пункта 9.1 собственные векторы, соответствующие попарно различным собственным значениям μ_j, линейно независимы, то есть образуют базис.

В общей диагональной форме (10) не все числа $\mu_j \in F$ обязательно различны. В связи с этим приводимый ниже *критерий диагонализируемости* формулируется сложнее.

Теорема. *Оператор A является диагонализируемым тогда и только тогда, когда одновременно выполнены условия:*

1°. *Все корни характеристического многочлена $p(\lambda)$ принадлежат основному полю F, то есть являются собственными значениями.*

2°. *Для каждого собственного значения λ^* $a_{\lambda^*} = g_{\lambda^*}$.*

Доказательство. Пусть A — оператор простой структуры с диагональной матрицей (10) в некотором базисе. Тогда его характеристический многочлен $p(\lambda) = (\mu_1 - \lambda) \dots (\mu_n - \lambda)$ имеет корни $\mu_1, \dots, \mu_n \in F$, и условие 1° выполнено.

Каждое собственное значение λ^* совпадает с одним из $\mu_1, \dots, \mu_n$. Пусть $a_{\lambda^*} = r$; это означает, что число λ^* встречается на диагонали $\mathbf{A}$ ровно r раз. Рассмотрим те базисные векторы, образы которых соответствуют столбцам с λ^* (всего их r). Все эти векторы принадлежат P_{λ^*}: для любого из них, скажем, e, выполнено $A() = \lambda^* e$. Это означает, что $g_{\lambda^*} = \dim P_{\lambda^*} \geqslant r = a_{\lambda^*}$.

В силу теоремы 1 предыдущего пункта выполнено и противоположное неравенство $g_{\lambda^*} \leqslant a_{\lambda^*}$. Тем самым условие 2° установлено.

Пусть теперь для некоторого $A : L \to L$ выполнены условия 1° – 2°. Обозначим через $\lambda_1, \dots, \lambda_k$ все *различные* собственные значения; $a_1, \dots, a_k$ и $g_1, \dots, g_k$ — их алгебраические и геометрические кратности; $P_1, \dots, P_k$ — соответствующие собственные подпространства.

Из 1° следует, что $a_1 + \dots + a_k = n$. Так как выполнено 2°, то и $g_1 + \dots + g_k = n$. В силу теоремы 2 предыдущего пункта сумма $S := P_1 + \dots + P_k$ является прямой. Следствие из этой теоремы даёт

$$\dim S = \sum_{j=1}^{k} \dim P_j = \sum_{j=1}^{k} g_j = n,$$

то есть $S = L$.

Итак, в рассматриваемой ситуации имеет место равенство

$$L = P_1 \oplus \dots \oplus P_k.$$

Выбирая в каждом из P_j базис и объединяя эти системы, мы получим базис L (характеристическое свойство прямой суммы, см. пункт 6.3). Очевидно, что в построенном базисе L матрица оператора A будет иметь диагональный вид (10) — каждый базисный вектор является собственным.

Теорема доказана.

Замечание 1. В случае $F = \mathrm{C}$ условие 1° выполнено для любого оператора A и его можно опустить.

Замечание 2. Как мы показали в пункте 8.7, матрицы одного и того же оператора в двух различных базисах связаны преобразованием подобия $\mathbf{B} = \mathbf{C}^{-1}\mathbf{A}\mathbf{C}$.

Таким образом, теорема описывает класс квадратных матриц, подобных диагональным. Например, в действительной ситуации в этот класс входят те и только те $\mathbf{A} \in M_n$, характеристический многочлен которых не имеет комплексных корней, а для каждого корня $\lambda \in \mathrm{R}$ выполняется $a_\lambda = g_\lambda$. Под g_λ здесь понимается размерность в $\mathrm{R^n}$ подпространства решений системы линейных однородных уравнений с матрицей $\mathbf{A} - \lambda\mathbf{E}$.

Упражнение. Получить из доказанного критерия утверждение о диагонализируемости оператора с n различными собственными значениями, см. начало пункта.

Примеры. 1. Рассмотрим оператор $A : \mathrm{R^n} \to \mathrm{R^n}$, матрица которого в каноническом базисе $\mathrm{R^n}$ состоит из одних единиц, см. пример предыдущего пункта. Собственные значения $\lambda_1 = 0$ и $\lambda_2 = n$ имеют кратности $a_1 = g_1 = n - 1$, $a_2 = g_2 = 1$. В связи с этим выполнены оба условия теоремы, и A имеет простую структуру.

Базис собственного подпространства

$$P_1 = \{x = (\xi_1, \ldots, \xi_{n-1}, -\xi_1 - \ldots - \xi_{n-1}),\ \xi_1, \ldots, \xi_{n-1} \in \mathrm{R}\}$$

составляют, например, векторы

$$f^{(1)} = (1, 0, \ldots, 0, -1),\ f^{(2)} = (0, 1, \ldots, 0, -1), \ldots, f^{(n-1)} = (0, 0, \ldots, 1, -1).$$

Базис собственного подпространства $P_2 = \{x = (t, t, \ldots, t),\ t \in \mathrm{R}\}$ образует вектор $f^{(n)} = (1, 1, \ldots, 1)$. В базисе $f^{(1)}, \ldots, f^{(n-1)}, f^{(n)}$ всего пространства $\mathrm{R^n}$ матрица оператора A имеет вид:

$$\mathbf{A}' = \mathrm{diag}_n(0, 0, \ldots, 0, n) = \begin{pmatrix} 0 & & & 0 \\ & 0 & & \\ & & \ddots & \\ 0 & & & n \end{pmatrix}.$$

2. Оператор дифференцирования $D : \mathrm{R_n}[t] \to \mathrm{R_n}[t], n \geqslant 1$, не является диагонализируемым. Характеристический многочлен $p(\lambda) = (-1)^{n+1}\lambda^{n+1}$ имеет единственный действительный корень $\lambda_1 = 0$ алгебраической кратности $a_1 = n+1 = \dim \mathrm{R_n}[t]$, так что условие 1° выполнено. Однако собственное подпространство $P_1 = \mathrm{R}_0[t]$ имеет размерность $g_1 = 1 \neq a_1$, и 2° не имеет места.

На языке матриц это означает, что матрица $\mathbf{A} = (a_{ij})$, у которой ненулевой является лишь одна диагональ — но не главная, а определяемая условием $j = i + 1$ — не является подобной диагональной.

3. Пусть оператор $A : \mathrm{R^3} \to \mathrm{R^3}$ имеет в каноническом базисе матрицу

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Характеристический многочлен $p(\lambda) = (\lambda^2 + 1)(1 - \lambda)$ имеет корни $\lambda_1 = 1, \lambda_{2,3} = \pm\mathbf{i}$. Так как $\lambda_{2,3} \in \mathrm{C}$, то условие 2° теоремы не выполнено, и оператор A не является диагонализируемым.

Однако если считать, что A действует из C^3 в C^3, то этот оператор имеет простую структуру — *A имеет три различных собственных значения.* Матрица оператора в некотором базисе C^3 (каком именно?) приводится к диагональному виду

$$\mathbf{A}' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \mathbf{i} & 0 \\ 0 & 0 & -\mathbf{i} \end{pmatrix}.$$

9.5. Теорема о жордановой нормальной форме матрицы линейного оператора. Комментарии

В этом пункте мы сформулируем и подробно прокомментируем одну из самых важных теорем линейной алгебры — о каноническом виде матрицы оператора, действующего в комплексном пространстве.

Известные доказательства этой теоремы являются достаточно сложными или длинными; лишь по этой причине ни одно из них в настоящем тексте целиком не приводится. Однако мы опишем основные этапы того доказательства, которое основано на свойствах корневых и циклических подпространств оператора.

Мы будем рассматривать операторы, действующие в комплексном линейном пространстве $L, \dim L = n$. Для операторов, действующих в действительном пространстве и имеющих n собственных значений (с учётом алгебраических кратностей) жорданова матрица является действительной.

Определение. *Жордановой клеткой порядка k, соответствующей $\lambda \in \mathrm{C}$, называется верхняя треугольная матрица размера $k \times k$, имеющая вид*

$$\mathbf{J}_k(\lambda) := \begin{pmatrix} \lambda & 1 & & & 0 \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ 0 & & & & \lambda \end{pmatrix}. \tag{11}$$

На главной диагонали матрицы (11) k раз повторяется число λ; над главной диагональю $k-1$ раз повторяется 1. *Все остальные элементы равны нулю. Кроме того, считаем* $\mathbf{J}_1(\lambda) := (\lambda)$.

Жордановой матрицей $\mathbf{J} \in M_n$ называется клеточная матрица

$$\mathbf{J} := \begin{pmatrix} \mathbf{J}_{n_1}(\lambda_1) & & & 0 \\ & \mathbf{J}_{n_2}(\lambda_2) & & \\ & & \ddots & \\ 0 & & & \mathbf{J}_{n_k}(\lambda_k) \end{pmatrix}, \tag{12}$$

$n_1 + n_2 + \ldots + n_k = n$. *Числа* λ_i *не все обязательно различны. Порядки каких-то клеток* n_i *также могут совпадать.*

Пример 1. Жорданова матрица размера 10×10, приведённая ниже, имеет пять клеток, порядки которых равны 2, 2, 2, 1 и 3. Три клетки порядка 2 соответствуют $\lambda_1 = \lambda_2 = 3$ и $\lambda_3 = 0$. Клетки порядков 1 и 3 соответствуют $\lambda_4 = \lambda_5 = 1$.

$$\begin{pmatrix} 3 & 1 & & & & & & & & \\ 0 & 3 & & & & & & 0 & & \\ & & 3 & 1 & & & & & & \\ & & 0 & 3 & & & & & & \\ & & & & 0 & 1 & & & & \\ & & & & 0 & 0 & & & & \\ & & & & & & 1 & & & \\ & & & & & & & 1 & 1 & 0 \\ & 0 & & & & & & 0 & 1 & 1 \\ & & & & & & & 0 & 0 & 1 \end{pmatrix}.$$

Если каждая жорданова клетка $\mathbf{J}_{n_i}(\lambda_i)$ в (12) имеет порядок 1, то есть $n_i = 1$ для всех i и $k = n$, то жорданова матрица $\mathbf{J}$ диагональна. Если же для какой-то клетки $\mathbf{J}_m(\lambda)$ $m > 1$, то $\mathbf{J}$ не только не диагональна, но даже не диагонализируема (то есть не является подобной никакой диагональной матрице).

Упражнение 1. Доказать, что жорданова клетка $\mathbf{J}_m(\lambda)$ *порядка* $m > 1$ *не является диагонализируемой.*

Упражнение 2. Для матрицы $\mathbf{Q} := \mathbf{J}_n(0)$ *(жорданова клетка порядка* n*, соответствующая числу* $\lambda = 0$*) определить степени* $\mathbf{Q}^j$, $j \in \mathrm{N}$.

Упражнение 3. Пусть $\mathbf{J}$ *имеет вид (12). Как выглядят матрицы*
(*i*) $\mathbf{J}^m$, $m \in \mathrm{N}$; (*ii*) $f(\mathbf{J})$, f *— многочлен?*

Сформулируем основной и самый интересный результат этого раздела.

Теорема о жордановой нормальной форме. *Пусть* $A : L \to L$ *— произвольный линейный оператор. Существует базис* L*, в котором матрица оператора* A *имеет вид (12). Жорданова матрица оператора является единственной с точностью до порядка клеток.*

Очевидно, что числа $\lambda_i \in \mathrm{C}$ из (12) являются собственными значениями A и исчерпывают множество всех собственных значений (как отмечалось выше, не все они обязательно различны).

Таким образом, каждая комплексная матрица подобна некоторой жордановой. Для действительной матрицы из M_n, которая имеет n собственных значений с учётом кратностей, соответствующая ей жорданова матрица является действительной. (В последнем случае матрица перехода и обратная к ней также являются действительными.)

Представление матрицы оператора A в виде (12) эквивалентно разложению пространства L в прямую сумму k подпространств, инвариантных относительно A (см. пункт 8.8). Это разложение осуществляется в два этапа.

На первом этапе L представляется в виде прямой суммы так называемых *корневых подпространств оператора* A :

$$L = K_{\lambda_1} \oplus \ldots \oplus K_{\lambda_s}. \tag{13}$$

Здесь и далее $\lambda_1, \ldots, \lambda_s$ — *все различные собственные значения* A. Обозначим алгебраическую и геометрическую кратности λ_i через a_i и g_i.

Корневое подпространство K_{λ_i} определяется как ядро оператора $(A - \lambda_i E)^{a_i}$:

$$K_{\lambda_i} := \mathrm{Ker}(A - \lambda_i E)^{a_i}.$$

Можно показать, что $\dim K_{\lambda_i} = a_i$ и сумма в (13) является прямой. Поэтому равенство (13) действительно имеет место.

Упражнение 4. Доказать, что K_{λ_i} *инвариантно относительно* A.

На втором этапе каждое корневое подпространство K_{λ_i} представляется в виде прямой суммы *циклических подпространств,* также инвариантных относительно A.

Пусть для определённости $i = 1$. Разложение для K_{λ_1} имеет вид

$$K_{\lambda_1} = W_1 \oplus \ldots \oplus W_j,$$

причём число слагаемых j равно g_{λ_1}.

Циклическое подпространство $W \subset K_{\lambda_1}$ размерности h есть оболочка линейно независимых векторов вида

$$e_h := f,\ e_{h-1} := (A - \lambda_1 E)(f),\ e_{h-1} := (A - \lambda_1 E)^2(f),\ \ldots,$$
$$e_1 := (A - \lambda_1 E)^{h-1}(f).$$

Линейная независимость такой *цепочки (или серии)* векторов достигается за счёт выбора $f \in K_{\lambda_1}$. Именно, вектор f выбирается так, чтобы было одновременно

$$(A - \lambda_1 E)^h(f) = 0, \quad (A - \lambda_1 E)^{h-1}(f) = e_1 \neq 0.$$

Поэтому вектор e_1 является собственным, соответствующим λ_1. Говорят, что f является *корневым вектором высоты* h.

Упражнение 5. Показать, что для корневого вектора f *высоты* h *система* $e_1, \ldots, e_h$ *является линейно независимой.*

По построению имеют место следующие равенства:

$$A(e_1) = \lambda_1 e_1; \quad A(e_l) = \lambda_1 e_l + e_{l-1},\ l = 2, \ldots, h. \tag{14}$$

Действительно, e_1 является собственным, а e_{l-1} при $l > 1$ удовлетворяет соотношению $e_{l-1} = (A - \lambda_1 E)(e_l)$. Тем самым, циклическое подпространство $W = \lin(e_1, \ldots, e_h)$ инвариантно относительно оператора A. Равенства (14) эквивалентны тому, что в базисе $e_1, \ldots, e_h$ оператор $A : W \to W$ имеет матрицу, совпадающую с жордановой клеткой порядка h, соответствующей λ_1.

Таким образом, каждой жордановой клетке в канонической форме (12) соответствует некоторое циклическое подпространство, размерность которого равна порядку этой клетки. Клетки с одним и тем же значением λ_1 соответствуют разложению K_{λ_1} в прямую сумму циклических подпространств.

Сказанное переносится и на корневые подпространства $K_{\lambda_2}, \ldots, K_{\lambda_s}$ по аналогии.

Подробности и полное обоснование этой схемы доказательства основной теоремы читатель может найти в книге И.М. Гельфанда [7].

Выделим отдельно ряд важных замечаний о жордановой матрице (12), полезных для её построения (см. [7], [26]).

З а м е ч а н и я

1. Число клеток матрицы $\mathbf{J}$, соответствующих данному собственному значению λ_i, равно $g_i = \dim P_{\lambda_i}$.

Число всех клеток матрицы $\mathbf{J}$ равно, таким образом, $k = \sum g_i$ — максимальному числу линейно независимых собственных векторов оператора A.

2. Оператор A диагонализируем тогда и только тогда, когда $k = \sum g_i = n$, то есть матрица (12) является диагональной. Это возможно лишь в ситуации $g_i = a_i$ для всех $i = 1, \ldots, s$, что соответствует теореме пункта 9.4 для комплексного L.

3. Сумма порядков всех клеток, соответствующих λ_i, равна a_i. Напомним, что алгебраическая кратность a_i оказывается равной размерности корневого подпространства K_{λ_i}.

4. Ранги операторов $(A - \lambda_i E)^j$, $j = 1, 2, \ldots$, или ранги матриц $(\mathbf{A} - \lambda_i \mathbf{E})^j$ монотонно убывают вплоть до некоторого значения j, после чего эта последовательность становится стационарной. Здесь $\mathbf{A}$ — матрица оператора A в любом исходном базисе. Именно эта матрица, как правило, и подвергается анализу.

Наименьшее натуральное j, минимизирующее ранг матрицы $(\mathbf{A} - \lambda_i \mathbf{E})^j$, называется *индексом* собственного значения λ_i и обозначается через m_i. Число m_i равно *максимальному порядку клетки, соответствующей* λ_i. Одновременно m_i есть максимальная высота корневого вектора из K_{λ_i}.

5. Знание всех собственных значений λ_i вместе с их алгебраическими и геометрическими кратностями a_i и g_i в общем случае не даёт полной информации о жордановой матрице — нужно ещё определить порядки клеток. Полная информация также получается из анализа последовательности $\operatorname{rg}(\mathbf{A} - \lambda_i \mathbf{E})^j$, $j = 1, 2, \ldots$.

Именно, число $N(\lambda_i, j)$ жордановых клеток порядка j, соответствующих λ_i, определяется по формуле:

$$N(\lambda_i, j) = \operatorname{rg}(\mathbf{B}^{j-1}) - 2\operatorname{rg}(\mathbf{B}^j) + \operatorname{rg}(\mathbf{B}^{j+1}), \quad \mathbf{B} := \mathbf{A} - \lambda_i \mathbf{E}. \tag{15}$$

Мы считаем $\mathbf{B}^0 := \mathbf{E}$. См. для иллюстрации пример 2.

6. Равенство (15) используют для построения жордановой матрицы без определения канонического базиса. Алгоритм нахождения канонического базиса L, то есть базиса, соответствующего жордановой матрице (12), описан, например, в задаче 1529 из сборника [23].

Пример 2. Пусть жорданова матрица оператора $A : L \to L, \dim L = 8$, есть

$$\mathbf{J} = \begin{pmatrix} 2 & 1 & 0 & & & & & \\ 0 & 2 & 1 & & & & 0 & \\ 0 & 0 & 2 & & & & & \\ & & & 2 & 1 & & & \\ & & & 0 & 2 & & & \\ & & & & & 2 & 1 & \\ & 0 & & & & 0 & 2 & \\ & & & & & & & 2 \end{pmatrix}$$

Единственное собственное значение $\lambda_1 = 2$ имеет алгебраическую кратность $a_1 = n = 8$ (сумма порядков всех клеток с λ_1; других клеток нет). В этой ситуации корневое подпространство K_{λ_1} совпадает со всем L. Вычислим последовательно

$$\mathbf{J} - 2\mathbf{E} = \begin{pmatrix} 0 & 1 & 0 & & & & & \\ 0 & 0 & 1 & & & & 0 & \\ 0 & 0 & 0 & & & & & \\ & & & 0 & 1 & & & \\ & & & 0 & 0 & & & \\ & & & & & 0 & 1 & \\ & 0 & & & & 0 & 0 & \\ & & & & & & & 0 \end{pmatrix},$$

$$(\mathbf{J} - 2\mathbf{E})^2 = \begin{pmatrix} 0 & 0 & 1 & & & & & \\ 0 & 0 & 0 & & & & 0 & \\ 0 & 0 & 0 & & & & & \\ & & & 0 & 0 & & & \\ & & & 0 & 0 & & & \\ & & & & & 0 & 0 & \\ & 0 & & & & 0 & 0 & \\ & & & & & & & 0 \end{pmatrix},$$

$(\mathbf{J} - 2\mathbf{E})^3 = \mathbf{0}$ (ср. с упражнением 2). Ранги этих матриц равны

$$r_1 = \operatorname{rg}(\mathbf{J} - 2\mathbf{E}) = 4,\ r_2 = \operatorname{rg}(\mathbf{J} - 2\mathbf{E})^2 = 1,\ r_3 = \operatorname{rg}(\mathbf{J} - 2\mathbf{E})^3 = 0.$$

Ясно, что все последующие степени $(\mathbf{J} - 2\mathbf{E})^j$ равны $\mathbf{0}$, и, начиная с $r_3 = 0$, последовательность $\{r_j\}$ рангов становится постоянной.

Это означает, что индекс собственного значения $\lambda_1 = 2$ равен $m_1 = 3$. Действительно, максимальный порядок клетки, соответствующей λ_1, равен 3. Одновременно получаем, что максимальная высота корневого вектора из K_{λ_1} равна 3.

Число клеток порядка 1

$$N(2,1) = \operatorname{rg}(\mathbf{E}) - 2r_1 + r_2 = 8 - 8 + 1 = 1.$$

Число клеток порядка 2

$$N(2,2) = r_1 - 2r_2 + r_3 = 4 - 2 + 0 = 2.$$

Имеется лишь одна клетка максимального порядка 3:

$$N(2,3) = r_2 - 2r_3 + r_4 = 1 - 0 + 0 = 1.$$

Далее в равенствах для $N(2,j),\ j \geqslant 4$, все слагаемые равны 0 — клеток большего порядка нет.

Собственное подпространство задаётся системой линейных однородных уравнений с матрицей $\mathbf{J}-2\mathbf{E}$, поэтому его размерность равна $g_1 = 8-\mathrm{rg}(\mathbf{J}-2\mathbf{E}) = 8-4 = 4$. Это есть общее число всех клеток, соответствующих $\lambda_1 = 2$.

Упражнение 6. Оператор A называется одноклеточным, если его жорданова матрица представляет собой единственную клетку порядка n. Доказать, что если A — одноклеточный оператор с собственным значением $\lambda_0 \neq 0$, то одноклеточными являются и операторы A^2; $A^r, r \in \mathrm{N}$; A^{-1}.

Доказать также, что если $\lambda_0 = 0$ и $n > 1$, то оператор A^2 уже не будет одноклеточным.

10. Билинейные и квадратичные формы

Билинейная форма в линейном пространстве L — это числовая функция двух аргументов $x, y \in L$, линейная по каждому из них. Если эта функция симметрична, то подстановка $y := x$ порождает *квадратичную форму* — функцию лишь одного аргумента $x \in L$.

Такие функции (или, лучше сказать, функционалы) возникают в различных разделах математики и приложениях, в связи с чем их определённый анализ осуществляется и в рамках настоящего курса. Особо отметим такие вопросы, как приведение квадратичной формы к каноническому виду и исследование её положительной определённости.

Фундаментальные результаты в этом направлении принадлежат английскому математику и педагогу профессору Джеймсу Джозефу Сильвестру (J.J. Sylvester, 1814 – 1897). Каждый прикладник знает *критерий Сильвестра положительной определённости квадратичной формы*, связанный с положительностью главных миноров её матрицы.

Открытый в 1852 г. также Сильвестром *закон инерции квадратичных форм* ранее был известен Якоби (C. Jacobi, 1804 – 1851) и Риману (B. Riemann, 1826 – 1866), но не опубликован ими.

10.1. Билинейные формы и их матрицы

Пусть L — действительное линейное пространство.

Определение 1. *Билинейной формой на L называется функционал $B : L \times \times L \to \mathrm{R}$, линейный по каждому из аргументов.*

Иначе говоря, билинейная форма B есть числовая функция двух аргументов из L, удовлетворяющая при всех $x, y, z \in L, \alpha \in \mathrm{R}$ равенствам:

$$1^\circ. \quad B(\alpha x, y) = \alpha B(x, y), \quad B(x + z, y) = B(x, y) + B(z, y).$$

$$2^\circ. \quad B(x, \alpha y) = \alpha B(x, y), \quad B(x, y + z) = B(x, y) + B(x, z).$$

Билинейная форма B называется *симметричной,* если при всех $x, y \in L$ выполнено $B(x, y) = B(y, x)$.

Условия $1^\circ - 2^\circ$ эквивалентны тому, что для произвольных натуральных k, m и любых векторов $x_1, \ldots, x_k, y_1, \ldots, y_m \in L$ имеет место равенство

$$B(\sum_{i=1}^{k} \alpha_i x_i, \sum_{j=1}^{m} \beta_j y_j) = \sum_{i=1}^{k} \sum_{j=1}^{m} \alpha_i \beta_j B(x_i, y_j). \tag{1}$$

На протяжении основного текста этого пункта считаем $\dim L = n$. (Примеры $3 - 4$ связаны с общей, а пример 5 — с бесконечномерной ситуациями.)

Определение 2. *Матрицей билинейной формы B в базисе $e_1, \ldots, e_n$ называется матрица $\mathbf{A} = (a_{ij}) \in M_n$, состоящая из чисел $a_{ij} := B(e_i, e_j)$.*

Матрица билинейной формы используется для вычисления значения $B(x,y)$ в координатах. Именно, пусть $x = \{\xi_1, \ldots, \xi_n\}, y = \{\eta_1, \ldots, \eta_n\}$ в том же базисе $e_1, \ldots, e_n$, в котором записана $\mathbf{A}$. Тогда с учётом (1)

$$B(x,y) = B(\sum_{i=1}^{n} \xi_i e_i, \sum_{j=1}^{n} \eta_j e_j) = \sum_{i,j=1}^{n} \xi_i \eta_j B(e_i, e_j) = \sum_{i,j=n}^{n} a_{ij} \xi_i \eta_j. \qquad (2)$$

Очевидно, что если билинейная форма B является симметричной, то её матрица $\mathbf{B}$ симметрична.

Упражнение 1. Показать, используя (2), что если матрица билинейной формы в некотором базисе является симметричной, то билинейная форма является симметричной (а значит, её матрица в любом базисе симметрична).

Таким образом, симметричность билинейной формы эквивалентна симметричности её матрицы в любом базисе.

Примеры.

1. Пусть $L = \mathrm{R^n}, \mathbf{A} = (a_{ij}) \in M_n$ — произвольная матрица. Для $x = (\xi_1, \ldots, \xi_n)$, $y = (\eta_1, \ldots, \eta_n) \in \mathrm{R^n}$ положим

$$B(x,y) := \sum_{i,j=1}^{n} a_{ij} \xi_i \eta_j.$$

Перепишем последнее равенство в виде

$$B(x,y) = d_1 \xi_1 + \ldots + d_n \xi_n, \;\; d_i = d_i(y) \in \mathrm{R}.$$

Оно означает, что $B(x,y)$ при каждом фиксированном $y \in L$ — линейный функционал по x. Мы воспользовались общим видом линейного функционала на $\mathrm{R^n}$ (см. по этому поводу пункт 8.1, пример 10).

Аналогично функционал $B(x,y)$ линеен по y при каждом фиксированном $x \in L$. Таким образом, B является билинейным функционалом, или в нашей терминологии билинейной формой на $\mathrm{R^n}$.

Нетрудно убедиться, что матрица билинейной формы B в каноническом базисе $e^{(1)} = (1,0,\ldots,0)$, $\ldots$, $e^{(n)} = (0,0,\ldots,1)$ совпадает с $\mathbf{A}$. Поэтому B является симметричной тогда и только тогда, когда $a_{ji} = a_{ij}$.

2. Конкретизируем предыдущий пример. Билинейная форма на $\mathrm{R^3}$, имеющая вид

$$B(x,y) := 2\xi_1\eta_1 + 3\xi_1\eta_2 - \xi_1\eta_3 + 4\xi_2\eta_1 + \xi_2\eta_3 - \xi_3\eta_2 + 5\xi_3\eta_3,$$

$$x = (\xi_1, \xi_2, \xi_3), \;\; y = (\eta_1, \eta_2, \eta_3),$$

соответствует матрице

$$\mathbf{A} = \begin{pmatrix} 2 & 3 & -1 \\ 4 & 0 & 1 \\ 0 & -1 & 5 \end{pmatrix}.$$

Она совпадает с матрицей билинейной формы B в базисе $e^{(1)} = (1,0,0)$, $e^{(2)} = (0,1,0)$, $e^{(3)} = (0,0,1)$. Так как $\mathbf{A}$ не является симметричной, то и билинейная форма B не является симметричной. Например, $B(e^{(1)}, e^{(2)}) = 3 \neq 4 = B(e^{(2)}, e^{(1)})$.

Найдём матрицу той же билинейной формы в базисе $f^{(1)} = (1,0,0)$, $f^{(2)} = (1,1,0)$, $f^{(3)} = (1,1,1)$. Для этого вычислим значения B на всевозможных парах базисных векторов.

$$b_{11} := B(f^{(1)}, f^{(1)}) = 2, \quad b_{12} := B(f^{(1)}, f^{(2)}) = 5,$$
$$b_{13} := B(f^{(1)}, f^{(3)}) = 4, \quad b_{21} := B(f^{(2)}, f^{(1)}) = 6,$$
$$b_{22} := B(f^{(2)}, f^{(2)}) = 9, \quad b_{23} := B(f^{(2)}, f^{(3)}) = 9,$$
$$b_{31} := B(f^{(3)}, f^{(1)}) = 6, \quad b_{32} := B(f^{(3)}, f^{(2)}) = 8,$$
$$b_{33} := B(f^{(3)}, f^{(3)}) = 13.$$

Матрица билинейной формы в базисе $f^{(1)}, f^{(2)}, f^{(3)}$ имеет вид

$$\mathbf{B} = (b_{ij}) = \begin{pmatrix} 2 & 5 & 4 \\ 6 & 9 & 9 \\ 6 & 8 & 13 \end{pmatrix}.$$

Другой способ определения матрицы $\mathbf{B}$ дан в примере 6.

3. Пусть F, G — линейные функционалы на L. Очевидно, что функционал $B(x,y) := F(x)G(y)$, $x, y \in L$, является билинейной формой на L. Проверка условий $1^\circ - 2^\circ$ использует линейность F и G.

4. Пусть L наделено структурой евклидова пространства, то есть в L определено скалярное произведение векторов (x,y), см. 7.1. Свойства скалярного произведения означают, что $B(x,y) := (x,y)$ есть симметричная билинейная форма. Этот общий пример порождает много частных.

5. Положим для функций $x, y \in C[0,1]$

$$B(x,y) := \int_0^1 \int_0^1 K(s,t)x(s)y(t)dsdt.$$

Здесь $K(s,t)$ — непрерывная функция двух переменных, заданная на квадрате $[0,1]^2$. Линейные свойства интеграла гарантируют, что B есть билинейная форма на $C[0,1]$. Если дополнительно $K(s,t) = K(t,s)$, то B является симметричной.

Пример 2 показывает, что в конечномерном пространстве матрица билинейной формы зависит от базиса L. Точный результат содержит следующее утверждение.

Теорема. *Пусть* $\mathbf{A}$ *и* $\mathbf{B}$ *— матрицы одной и той же билинейной формы* B *в базисах* $e_1, \ldots, e_n$ *и* $f_1, \ldots, f_n$ *соответственно;* $\mathbf{C}$ *— матрица перехода от первого базиса ко второму. Тогда*

$$\mathbf{B} = \mathbf{C}^T\mathbf{A}\mathbf{C}. \tag{3}$$

Доказательство. По определению матрицы перехода (см. пункт 5.6) $f_i = \{c_{1i}, \ldots, c_{ni}\}$, $f_k = \{c_{1k}, \ldots, c_{nk}\}$ в базисе $e_1, \ldots, e_n$. Поэтому в соответствии с (2) имеем:

$$b_{ik} = B(f_i, f_k) = \sum_{p,q=1}^{n} a_{pq} c_{pi} c_{qk} = \sum_{p,q=1}^{n} c'_{ip} a_{pq} c_{qk}.$$

Здесь $\mathbf{C}^T = (c'_{st})$; остальные обозначения стандартны. Нетрудно заметить, что система последних равенств для всех $i, k = 1, \ldots, n$ эквивалентна (3). Теорема доказана.

Пример 6. Матрица перехода от базиса $e^{(1)} = (1, 0, 0)$, $e^{(2)} = (0, 1, 0)$, $e^{(3)} = (0, 0, 1)$ к базису $f^{(1)} = (1, 0, 0)$, $f^{(2)} = (1, 1, 0)$, $f^{(3)} = (1, 1, 1)$ равна

$$\mathbf{C} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Поэтому матрица $\mathbf{B}$ билинейной формы из примера 2 в базисе $f^{(1)}$, $f^{(2)}$, $f^{(3)}$ может быть найдена по матрице $\mathbf{A}$ той же формы в каноническом базисе с помощью равенства

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & -1 \\ 4 & 0 & 1 \\ 0 & -1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 2 & 5 & 4 \\ 6 & 9 & 9 \\ 6 & 8 & 13 \end{pmatrix}$$

— тот же результат, что и в примере 2.

10.2. Квадратичные формы. Приведение квадратичной формы к каноническому виду

Определение. *Пусть B — симметричная билинейная форма на линейном пространстве L. Функционал Q, заданный равенством $Q(x) := B(x, x)$, называется квадратичной формой на L. Билинейная форма B называется полярной к порождаемой ею квадратичной форме Q.*

Полярная билинейная форма B однозначно определяется своей квадратичной формой Q. Это следует из легко проверяемого тождества

$$B(x, y) = \frac{1}{2}\Big[B(x + y, x + y) - B(x, x) - B(y, y)\Big] =$$

$$= \frac{1}{2}\Big[Q(x + y) - Q(x) - Q(y)\Big].$$

Таким образом, между симметричными билинейными формами B и квадратичными формами Q в евклидовом пространстве осуществляется *взаимно-однозначное*

соответствие, при котором имеет место равенство $Q(x) = B(x, x)$. Этот факт используется в дальнейшем.

В предыдущем пункте мы показали, что каждая билинейная форма в n-мерном пространстве может быть задана в координатном виде:

$$B(x, y) = \sum_{i,j=1}^{n} a_{ij}\xi_i\eta_j.$$

Здесь $x = \{\xi_1, \ldots, \xi_n\}, y = \{\eta_1, \ldots, \eta_n\}$ и $\mathbf{A} = (a_{ij})$ — матрица билинейной формы в одном и том же базисе. Если B является симметричной, то $a_{ji} = a_{ij}$.

Поэтому всякая квадратичная форма Q при заданном базисе $e_1, \ldots, e_n$ выражается формулой

$$Q(x) = \sum_{i,j=1}^{n} a_{ij}\xi_i\xi_j, \tag{4}$$

причём $a_{ji} = a_{ij}$. Матрица $\mathbf{A}$ называется *матрицей квадратичной формы* Q в базисе $e_1, \ldots, e_n$. Она является и матрицей полярной формы B в том же базисе.

При составлении матрицы квадратичной формы следует учитывать её симметричность (в обычной записи коэффициенты a_{ij} и $a_{ji}, i \neq j$, объединяются — они соответствуют сомножителю $\xi_i\xi_j$).

Пример 1. Пусть квадратичная форма $Q : L \to \mathrm{R}, \dim L = 3$, в некотором базисе e_1, e_2, e_3 выражается равенством

$$Q(x) = -2\xi_1^2 + 3\xi_2^2 - 5\xi_3^2 - 4\xi_1\xi_2 + 6\xi_1\xi_3 + 8\xi_2\xi_3.$$

Тогда её матрица в том же базисе имеет вид

$$\mathbf{A} = \begin{pmatrix} -2 & -2 & 3 \\ -2 & 3 & 4 \\ 3 & 4 & -5 \end{pmatrix}.$$

Говорят, что в базисе $f_1, f_2, \ldots, f_n$ квадратичная форма Q имеет *канонический вид,* если её матрица $\mathbf{A}'$ в этом базисе является диагональной:

$$\mathbf{A}' = \mathrm{diag}_n(\lambda_1, \lambda_2, \ldots, \lambda_n) = \begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}.$$

Это означает, что $Q(x)$ выражается равенством

$$Q(x) = \lambda_1\eta_1^2 + \lambda_2\eta_2^2 + \ldots + \lambda_n\eta_n^2. \tag{5}$$

Соответствующий базис $f_1, f_2, \ldots, f_n$ также называется *каноническим.*

Анализ квадратичной формы, имеющей канонический вид (5), осуществляется намного проще, чем в общей ситуации (4). Оказывается, что справедливо следующее утверждение, содержащее основной результат этого пункта.

Теорема 1. *Каждая квадратичная форма Q, заданная в исходном базисе равенством (4), может быть приведена к каноническому виду. Иными словами, в L может быть указан новый базис (канонический для Q), в котором будет иметь место равенство (5).*

Теорема 1 имеет ряд конструктивных доказательств — в каждом из них обосновывается некоторый способ приведения квадратичной формы к каноническому виду.

Отметим три таких способа: метод Лагранжа, метод Якоби и метод собственных значений. Первый из них является наиболее простым и общим. Второй способ совпадает с процессом ортогонализации (см. пункт 7.4), если заменить в последнем скалярное произведение на билинейную форму $B(x, y)$. Возможность его применения связана с некоторыми дополнительными ограничениями. Наконец, метод собственных значений, описываемый здесь лишь фрагментарно, обосновывается и иллюстрируется в следующем разделе, см. пункт 11.4.

10.2.1. Метод Лагранжа (или метод выделения полных квадратов)

Дадим конструктивное **доказательство теоремы 1** в приведённой выше общей формулировке.

Пусть квадратичная форма Q в исходном базисе имеет представление (4). Перейдём к каноническим координатам, последовательно дополняя до полных квадратов выражения в промежуточных координатах и вводя новые координаты как некоторые линейные комбинации старых. Число координат, входящих в $Q(x)$ только с квадратами, будет последовательно увеличиваться до тех пор, пока мы не придём к каноническому виду.

Каждому невырожденному линейному преобразованию координат (умножению столбца координат на невырожденную матрицу) соответствует некоторое преобразование базиса. Таким образом, вместе с конечным преобразованием координат может быть указан искомый канонический базис.

Опишем действия лишь на первом шаге; далее используется индукция. Для ненулевой Q возможны две ситуации.

1) При некотором $k, 1 \leqslant k \leqslant n$, диагональный коэффициент $a_{kk} \neq 0$. Положим тогда

$$Q(x) = \frac{1}{a_{kk}} \Big(\sum_{i=1}^{n} a_{ki} \xi_i \Big)^2 + Q_1(x).$$

Непосредственная проверка показывает, что квадратичная форма $Q_1(x)$ уже не содержит координаты ξ_k. Это выглядит как дополнение выражения с ξ_k до полного квадрата.

Введём новые координаты $\xi'_1, \ldots, \xi'_n$ по формулам

$$\xi'_k := \sum_{i=1}^{n} a_{ki} \xi_i \ ; \qquad \xi'_j := \xi_j, \ j \neq k.$$

Это преобразование можно записать следующим образом:

$$\begin{pmatrix} \xi'_1 \\ \vdots \\ \xi'_n \end{pmatrix} = \mathbf{M} \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}. \tag{6}$$

$\mathbf{M}$ получается из единичной матрицы заменой k-й строки на k-ю строку $\mathbf{A}$. Так как $a_{kk} \neq 0$, то $|\mathbf{M}| \neq 0$. Значит, преобразование (6) является невырожденным, и новые координаты соответствуют некоторому промежуточному базису. Ясно, что матрица перехода от исходного базиса к базису первого шага совпадает с $\mathbf{M^{-1}}$, см. пункт 5.6.

2) Пусть $a_{ii} = 0$ для всех $i = 1, \ldots, n$. Так как $Q(x) \not\equiv 0$, найдётся недиагональный коэффициент $a_{kl} \neq 0$. Считаем $1 \leqslant k < l \leqslant n$. Первое преобразование координат имеет вид:

$$\xi'_k := \xi_k - \xi_l,\ \xi'_l := \xi_k + \xi_l; \quad \xi'_i := \xi_i, \quad i \neq k, l.$$

При этом произведение $a_{kl}\xi_k\xi_l$ перейдёт в линейную комбинацию квадратов:

$$_{kl}\xi_k\xi_l = a_{kl} \cdot \frac{1}{2}(\xi'_k + \xi'_l) \cdot \frac{1}{2}(-\xi'_k + \xi'_l) = -\frac{1}{4}a_{kl}{\xi'_k}^2 + \frac{1}{4}a_{kl}{\xi'_l}^2.$$

Переход от $\xi_1, \ldots, \xi_n$ к $\xi'_1, \ldots, \xi'_n$ также имеет вид равенства (6). Матрица $\mathbf{M}$ получается из единичной матрицы $\mathbf{E} = (e_{ij})$ заменой элементов e_{kl} и e_{lk} на 1 и -1 соответственно. Применение теоремы Лапласа к k-й и l-й строкам даёт $|\mathbf{M}| = = 2 \neq 0$, поэтому преобразование (6) является невырожденным. Таким образом, ξ'_i соответствуют некоторому базису.

В новом выражении для $Q(x)$ коэффициенты при ${\xi'_k}^2$ и ${\xi'_l}^2$ отличны от нуля; таким образом, мы попадаем в ситуацию 1).

Пример 2. Приведём к каноническому виду квадратичную форму Q из примера 1 этого пункта. Так как $a_{11} \neq 0$, на первом шаге возьмём $k = 1$ (дополняем до квадрата сумму членов, содержащих ξ_1). Отметим, что в выборе k здесь и ниже имеется произвол.

$$Q(x) = -2\xi_1^2 + 3\xi_2^2 - 5\xi_3^2 - 4\xi_1\xi_2 + 6\xi_1\xi_3 + 8\xi_2\xi_3 =$$
$$= -2(\xi_1^2 + 2\xi_1\xi_2 - 3\xi_1\xi_3) + 3\xi_2^2 - 5\xi_3^2 + 8\xi_2\xi_3 =$$
$$= -2(\xi_1^2 + 2\xi_1\xi_2 - 3\xi_1\xi_3 + \xi_2^2 + \frac{9}{4}\xi_3^2 - 3\xi_2\xi_3) + 2\xi_2^2 + \frac{9}{2}\xi_3^2 - 6\xi_2\xi_3 +$$
$$+3\xi_2^2 - 5\xi_3^2 + 8\xi_2\xi_3 = -2(\xi_1 + \xi_2 - \frac{3}{2}\xi_3)^2 + 5\xi_2^2 - \frac{1}{2}\xi_3^2 + 2\xi_2\xi_3 =$$
$$= -2\psi_1^2 + 5\psi_2^2 - \frac{1}{2}\psi_3^2 + 2\psi_2\psi_3.$$

Мы положили

$$\begin{pmatrix} \psi_1 \\ \psi_2 \\ \psi_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & -\frac{3}{2} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{pmatrix}.$$

На втором шаге мы работаем с квадратичной формой $Q_1(x)$, содержащей три последних слагаемых. Возьмём $k = 3$.

$$Q(x) = -2\psi_1^2 + 5\psi_2^2 - \frac{1}{2}(\psi_3^2 - 4\psi_2\psi_3 + 4\psi_2^2) + 2\psi_2^2 =$$

$$= -2\psi_1^2 + 7\psi_2^2 - \frac{1}{2}(-2\psi_2 + \psi_3)^2 = -2\eta_1^2 + 7\eta_2^2 - \frac{1}{2}\eta_3^2.$$

Последнее выражение имеет требуемый вид. Переход к каноническим координатам η_1, η_2, η_3 от промежуточных ψ_1, ψ_2, ψ_3 выражается равенством

$$\begin{pmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} \begin{pmatrix} \psi_1 \\ \psi_2 \\ \psi_3 \end{pmatrix}.$$

Учитывая преобразование первого шага, нетрудно указать связь между исходными и каноническими координатами:

$$\begin{pmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & -\frac{3}{2} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 1 & -\frac{3}{2} \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{pmatrix} = \mathbf{M} \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{pmatrix}.$$

Матрица перехода $\mathbf{C}$ от исходного базиса e_1, e_2, e_3 к каноническому базису f_1, f_2, f_3, соответствующему координатам η_1, η_2, η_3, равна $\mathbf{M^{-1}}$. Вычисления по методу Гаусса дают

$$\mathbf{C} = \mathbf{M}^{-1} = \begin{pmatrix} 1 & 2 & \frac{3}{2} \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}.$$

Это означает, что новый базис связан с исходным базисом равенствами

$$f_1 = e_1, \quad f_2 = 2e_1 + e_2 + 2e_3, \quad f_3 = \frac{3}{2}e_1 + e_3.$$

10.2.2. Метод Якоби (или метод треугольного преобразования)

Этот метод применим лишь к квадратичным формам, удовлетворяющим некоторым ограничениям.

Пусть $Q(x)$ задаётся в исходном базисе $e_1, \ldots, e_n$ выражением (4). Обозначим через Δ_k, $k = 1, \ldots, n$, главный минор матрицы $\mathbf{A}$ порядка k, стоящий в k первых строках и столбцах $\mathbf{A}$.

Теорема 2. *Пусть все миноры Δ_k, $k = 1, \ldots, n$, отличны от 0. Существует базис $f_1, \ldots, f_n$ такой, что в соответствующих координатах $\eta_1, \ldots, \eta_n$ имеет место равенство*

$$Q(x) = \frac{1}{\Delta_1}\eta_1^2 + \frac{\Delta_1}{\Delta_2}\eta_2^2 + \ldots + \frac{\Delta_{n-1}}{\Delta_n}\eta_n^2. \tag{7}$$

Доказательство является конструктивным и составляет сущность метода Якоби.

Векторы $f_1, \ldots, f_n$ ищутся последовательно в виде:

$$f_1 = \alpha_{11}e_1,\ f_2 = \alpha_{21}e_1 + \alpha_{22}e_2,\ \ldots,\ f_n = \alpha_{n1}e_1 + \alpha_{n2}e_2 + \ldots + \alpha_{nn}e_n.$$

Коэффициенты вектора $f_k = \alpha_{k1}e_1 + \ldots + \alpha_{kk}e_k$ на k-м шаге находятся из условий

$$B(e_1, f_k) = \ldots = B(e_{k-1}, f_k) = 0, \quad B(e_k, f_k) = 1. \tag{8}$$

Здесь и далее B — билинейная форма, полярная к Q. В случае $k = 1$ (8) содержит лишь последнее равенство. Покажем, что задача (8) имеет единственное решение.

Ясно, что

$$\alpha_{11} = \frac{1}{B(e_1, e_1)} = \frac{1}{\Delta_1}.$$

Пусть $k > 1$. Подставим в (8) выражение f_k через e_j и используем линейность B по второму аргументу. Мы получим следующую систему уравнений относительно α_{kj} :

$$\begin{gathered}
\alpha_{k1}B(e_1, e_1) + \alpha_{k2}B(e_1, e_2) + \ldots + \alpha_{kk}B(e_1, e_k) = 0, \\
\alpha_{k1}B(e_2, e_1) + \alpha_{k2}B(e_2, e_2) + \ldots + \alpha_{kk}B(e_2, e_k) = 0, \\
\ldots \qquad \ldots \qquad \ldots \qquad \ldots \\
\alpha_{k1}B(e_{k-1}, e_1) + \alpha_{k2}B(e_{k-1}, e_2) + \ldots + \alpha_{kk}B(e_{k-1}, e_k) = 0, \\
\alpha_{k1}B(e_k, e_1) + \alpha_{k2}B(e_k, e_2) + \ldots + \alpha_{kk}B(e_k, e_k) = 1.
\end{gathered}$$

Система имеет единственное решение, так как её определитель $\Delta_k \neq 0$. Поэтому векторы f_j с указанными свойствами определены однозначно.

Заметим, что по правилу Крамера

$$\alpha_{kk} = \frac{\Delta_{k-1}}{\Delta_k}, \quad k > 1.$$

Это гарантирует, в частности, линейную независимость $f_1, \ldots, f_n$: столбцы координат f_j в базисе $e_1, \ldots, e_n$ образуют верхнюю треугольную матрицу с числами $\alpha_{kk} \neq 0$ на диагонали.

Остаётся показать, что в базисе $f_1, \ldots, f_n$ матрица $\mathbf{B} = (b_{ij})$ квадратичной формы является диагональной, причём

$$b_{11} = \frac{1}{\Delta_1},\ b_{22} = \frac{\Delta_1}{\Delta_2},\ \ldots,\ b_{nn} = \frac{\Delta_{n-1}}{\Delta_n}.$$

Это и будет означать выполнение равенства (7).

При $i < k$ в силу первых условий (8)

$$b_{ik} = B(f_i, f_k) = B(\alpha_{i1}e_1 + \ldots + \alpha_{ii}e_i, f_k) =$$
$$= \alpha_{i1}B(e_1, f_k) + \ldots + \alpha_{ii}B(e_i, f_k) = 0.$$

Так как $\mathbf{B}$ симметрична, то $b_{ik} = 0$ при всех $i \neq k$. Далее,

$$b_{11} = B(f_1, f_1) = B(\alpha_{11}e_1, f_1) = \alpha_{11}B(e_1, f_1) = \alpha_{11} = \frac{1}{\Delta_1},$$

а для $k > 1$

$$b_{kk} = B(f_k, f_k) = B(\alpha_{k1}e_1 + \ldots + \alpha_{k,k-1}e_{k-1} + \alpha_{kk}e_k, f_k) =$$
$$= \alpha_{k1}B(e_1, f_k) + \ldots + \alpha_{k,k-1}B(e_{k-1}, f_k) + \alpha_{kk}B(e_k, f_k) =$$
$$= \alpha_{kk} = \frac{\Delta_{k-1}}{\Delta_k}.$$

Теорема 2 доказана.

Упражнение. В стандартном базисе $e^{(1)} = (1, 0, 0), e^{(2)} = (0, 1, 0), e^{(3)} = (0, 0, 1)$ *квадратичная форма на* R^3 *имеет вид*

$$Q(x) = 2\xi_1^2 + 3\xi_1\xi_2 + 4\xi_1\xi_3 + \xi_2^2 + \xi_3^2.$$

Составить полярную билинейную форму B. *Убедившись, что условия теоремы выполнены, построить канонический для* Q *базис* R^3 *по методу Якоби.*

10.2.3. Метод собственных значений (приведение к главным осям)

Пусть L имеет структуру евклидова пространства, то есть в L задано скалярное произведение (x, y). Будем считать, что исходный базис $e_1, \ldots, e_n$, соответствующий (4), является ортонормированным.

Как мы покажем в следующем разделе, симметричная матрица $\mathbf{A}$ подобна некоторой действительной диагональной матрице $\mathbf{B}$:

$$\mathbf{B} = \mathbf{C}^{-1}\mathbf{A}\mathbf{C}, \quad \mathbf{B} = \mathrm{diag}_n(\lambda_1, \ldots, \lambda_n).$$

Числа λ_i являются, таким образом, собственными значениями матрицы $\mathbf{A}$, то есть корнями её характеристического многочлена. Их число с учётом кратностей обязательно равно n. Важно, что здесь матрица перехода $\mathbf{C}$ является *ортогональной,* то есть такой, что $\mathbf{C}\mathbf{C}^T = \mathbf{C}^T\mathbf{C} = \mathbf{E}$.

Это означает, что в L существует ортонормированный базис $f_1, \ldots, f_n$, в котором квадратичная форма Q имеет вид

$$Q(x) = \lambda_1\eta_1^2 + \ldots + \lambda_n\eta_n^2.$$

При этом коэффициенты λ_i *являются собственными значениями, а векторы* f_i *— собственными векторами исходной матрицы* $\mathbf{A}$. Последнее касается координатного вида f_i в старом базисе.

Эти интересные и важные результаты устанавливаются в пункте 11.4. Там же описываются и некоторые приложения.

10.3. Положительная определённость квадратичной формы. Критерий Сильвестра

В этом пункте рассматриваются квадратичные формы Q, сохраняющие один и тот же знак на всём пространстве L. Как и ранее, мы считаем $\dim L = n$. В этой ситуации вопрос о знаковой определённости Q может быть решён по её матрице *в любом исходном базисе.*

Эта тематика связана с важными приложениями в анализе и других разделах математики.

Определение. *Квадратичная форма Q на L называется положительно определённой, если $Q(x) > 0$ для всех $x \neq 0$. Если же $Q(x) < 0$ для $x \neq 0$, то Q называется отрицательно определённой.*

Q называется неотрицательно определённой, если $Q(x) \geqslant 0$ для всех $x \in L$, и неположительно определённой, если $Q(x) \leqslant 0$ для $x \in L$.

Ясно, что всегда $Q(0) = 0$. Положительно или отрицательно определённые формы принимают значения соответствующего знака на *всех* $x \neq 0$. Неотрицательно или неположительно определённые формы могут принимать нулевое значение и на некоторых $x \neq 0$. Заметим также, что вовсе не обязательно данная квадратичная форма Q принадлежит одному из этих четырёх классов — знаки $Q(x)$ могут чередоваться. В этом случае говорят, что Q является *знакопеременной.*

Пример 1. Пусть $\dim L = 3$. Рассмотрим квадратичные формы

$$Q_1(x) := \xi_1^2 + 4\xi_2^2 + 7\xi_3^2,\ Q_2(x) := -2\xi_1^2 - \xi_2^2 - 5\xi_3^2,$$

$$Q_3(x) := \xi_1^2 + \xi_3^2, \qquad Q_4(x) := -\xi_1^2 + \xi_2^2 + \xi_3^2.$$

Здесь $x = \{\xi_1, \xi_2, \xi_2\}$ в некотором базисе e_1, e_2, e_3. Нетрудно видеть, что Q_1, Q_2, Q_3 являются соответственно положительно, отрицательно и неотрицательно определёнными. При этом Q_3 не является положительно определённой: для $x^* := \{0, 1, 0\} \neq 0$ $Q(x^*) = 0$. Очевидно также, что $Q_4(x)$ меняет знак.

Пример 2. По каноническому виду Q столь же просто осуществляется анализ знаковой определённости в n-мерном пространстве L. Пусть

$$Q(x) = \lambda_1\xi_1^2 + \ldots + \lambda_n\xi_n^2.$$

Такая квадратичная форма принадлежит одному из четырёх введённых классов, тогда и только тогда, когда все коэффициенты λ_i удовлетворяют одному из четырёх неравенств $\lambda_i > 0$, $\lambda_i < 0$, $\lambda_i \geqslant 0$ или $\lambda_i \leqslant 0$ соответственно.

В частности, Q является положительно определённой тогда и только тогда, когда $\lambda_i > 0$ для всех $i = 1, \ldots, n$.

Упражнение 1. Доказать сформулированное утверждение для каждого из классов знаково-определённых форм.

Пример 3. Скалярное произведение в произвольном евклидовом пространстве L является примером симметричной билинейной формы, для которой соответствующая квадратичная форма положительно определена. Именно эти свойства выражают аксиомы скалярного произведения (x, y) (см. пункт 7.1):

$$(x, y) = (y, x);\ (\lambda x, y) = \lambda(x, y);\ (x + y, z) = (x, y) + (x, z);$$

$$(x,x) \geqslant 0;\ (x,x) = 0 \Longleftrightarrow x = 0.$$

Наоборот, если симметричная билинейная форма B на линейном пространстве L такова, что соответствующая ей квадратичная форма является положительно определённой, то равенство $(x,y) := B(x,y)$, $x, y \in L$, позволяет ввести на L структуру евклидова пространства, так как $B(x,y)$ удовлетворяет всем аксиомам скалярного произведения.

Основным вопросом в дальнейшем является задача о положительной определённости данной квадратичной формы Q. Эта задача является нетривиальной, если Q не приведена к каноническому виду. Следующий *критерий Сильвестра* связан с анализом матрицы $\mathbf{A} = (a_{ij})$ в любом (необязательно каноническом для Q) базисе $e_1, \ldots, e_n$.

Напомним, что для $x = \{\xi_1, \ldots, \xi_n\}$

$$Q(x) = \sum_{ij=1}^{n} a_{ij}\xi_i\xi_j, \quad a_{ij} := B(e_i, e_j).$$

Здесь B — полярная билинейная форма. Обозначим, как и ранее, через Δ_k главный минор $\mathbf{A}$ порядка k, стоящий в первых k строках и столбцах.

Теорема 1. *Квадратичная форма Q является положительно определённой тогда и только тогда, когда $\Delta_k > 0$ при всех $k = 1, \ldots, n$.*

Доказательство. Пусть Q является положительно определённой. Покажем прежде всего, что $\Delta_k \neq 0$ при любом k.

Предположим, что $\Delta_k = 0$ при некотором k. Тогда система линейных уравнений

$$\begin{aligned}
a_{11}\xi_1 + a_{12}\xi_2 + \ldots + a_{1k}\xi_k &= 0,\\
a_{21}\xi_1 + a_{22}\xi_2 + \ldots + a_{2k}\xi_k &= 0,\\
\ldots \qquad \ldots \qquad &\ldots\\
a_{k1}\xi_1 + a_{k2}\xi_2 + \ldots + a_{kk}\xi_k &= 0.
\end{aligned}$$

имеет ненулевое решение $(\xi_1, \ldots, \xi_k)$ — определитель этой системы $\Delta_k = 0$. Рассмотрим ненулевой вектор $x = \{\xi_1, \ldots, \xi_k, 0, \ldots, 0\}$. Умножим первое из равенств системы на ξ_1, второе — на ξ_2, и так далее. Складывая затем результаты, получим

$$\sum_{i,j=1}^{k} a_{ij}\xi_i\xi_j = 0.$$

Левая часть равна $Q(x)$. Получается, что для некоторого $x \neq 0$ выполнено $Q(x) = = 0$, то есть Q не является положительно определённой. Полученное противоречие означает, что $\Delta_k \neq 0$.

Так как $\Delta_1, \Delta_2, \ldots, \Delta_n \neq 0$, к квадратичной форме Q применима теорема 2 предыдущего пункта, связанная с методом Якоби. Существует базис L, в котором Q имеет канонический вид (7), то есть

$$Q(x) = \frac{1}{\Delta_1}\eta_1^2 + \frac{\Delta_1}{\Delta_2}\eta_2^2 + \ldots + \frac{\Delta_{n-1}}{\Delta_n}\eta_n^2.$$

В силу положительной определённости Q все коэффициенты в последнем равенстве должны быть положительными. Это даёт последовательно $\Delta_1 > 0$, $\Delta_2 > 0$, …, $\Delta_n > 0$.

Пусть теперь все миноры $\Delta_k > 0$. Применяя опять метод Якоби, получим для Q канонический вид (7). Положительность Δ_k означает, что все коэффициенты в этом каноническом виде также положительны. Это гарантирует положительную определённость Q.

Теорема доказана.

Замечание 1. Положительность миноров $\Delta_1, \ldots, \Delta_n$ симметричной матрицы $\mathbf{A}$ эквивалентна положительности вообще всех её главных миноров. Дадим обоснование этому факту.

Сначала заметим, что соответствующая квадратичная форма Q является положительно определённой. Значит, миноры, занимающие положение Δ_k, положительны для матрицы Q, записанной в любом базисе L.

Пусть теперь анализу подвергается главный минор $\mathbf{A}$, стоящий на пересечении строк и столбцов с номерами $i_1, \ldots, i_k$. Обозначим этот минор через D. Мы считаем, что $\mathbf{A}$ соответствует базису $e_1, \ldots, e_n$. Рассмотрим любую перестановку базисных векторов, в которой на первых k местах стоят $e_{i_1}, e_{i_2}, \ldots, e_{i_k}$. В матрице квадратичной формы Q, соответствующей этому новому базису, минор D будет стоять в первых k строках и столбцах. По предыдущей теореме $D > 0$.

Замечание 2. Из краткого описания метода собственных значений (см. конец предыдущего пункта) следует другой критерий положительной определённости квадратичной формы Q. Именно, *Q является положительно определённой тогда и только тогда, когда все собственные значения её симметричной матрицы положительны.* Обоснование этого результата откладывается до пункта 11.4.

Отметим здесь, что сравнение двух приведённых критериев приводит к такому утверждению: *для симметричной матрицы $\mathbf{A} \in M_n$ положительность миноров $\Delta_1, \ldots, \Delta_n$ эквивалентна положительности всех её собственных значений.*

Приведём теперь некоторые результаты для квадратичных форм из других классов знакоопределённости.

Отметим сначала, что условие

$$\Delta_1 \geqslant 0, \Delta_2 \geqslant 0, \ldots, \Delta_n \geqslant 0 \tag{9}$$

не обеспечивает неотрицательной определённости Q.

Пример 4. Квадратичная форма $Q(x) := -\xi_2^2$, заданная на двумерном L, очевидно, не является неотрицательно определённой. Но так как для неё $a_{11} = a_{12} = = a_{21} = 0$, то $\Delta_1 = \Delta_2 = 0$, и (9) выполнено.

Справедлива следующая теорема, которую мы приведём без доказательства (его можно найти, например, в [5, с. 261]).

Теорема 2. *Квадратичная форма Q является неотрицательно определённой тогда и только тогда, когда все главные миноры её матрицы $\mathbf{A}$ неотрицательны.*

В предыдущем примере один из главных миноров первого порядка, а именно $a_{22} = -1$ отрицателен.

Наконец, условия отрицательной и неположительной определённости Q получаются из теорем 1 и 2, если применить их к квадратичной форме $-Q$.

Теорема 3. *Квадратичная форма Q является отрицательно определённой тогда и только тогда, когда*

$$\Delta_1 < 0, \Delta_2 > 0, \ldots, \ (-1)^n \Delta_n > 0.$$

Теорема 4. *Квадратичная форма Q является неположительно определённой тогда и только тогда, когда для любого главного минора D матрицы $\mathbf{A}$ порядка k было выполнено неравенство $(-1)^k D \geqslant 0$.*

Упражнение 2. Доказать теоремы 3 и 4 по предложенной схеме.

Упражнение 3. Сформулировать критерии неотрицательной, отрицательной и неположительной определённости в терминах собственных значений $\mathbf{A}$, см. замечание 2.

10.4. Закон инерции квадратичных форм. Ранг квадратичной формы

Инерция квадратичной формы Q выражается свойством постоянства положительных и отрицательных коэффициентов в её каноническом виде *независимо от способа приведения к такому виду.* Точный результат выражается теоремой 1 этого пункта. Мы также покажем, что общее число ненулевых коэффициентов в каноническом виде совпадает с рангом матрицы квадратичной формы в произвольном базисе; последний, таким образом, также является инвариантом Q.

Определение 1. *Нормальным видом квадратичной формы Q называется такой её канонический вид, в котором каждый из коэффициентов равен одному из чисел $1, -1$ или 0, и матрица Q в соответствующем базисе равна*

$$\operatorname{diag}_n(1, \ldots, 1, -1, \ldots, -1, 0, \ldots, 0)$$

(с точностью до наличия любой из групп диагональных коэффициентов).

Иначе говоря, нормальный вид Q выражается равенством

$$Q(x) = \psi_1^2 + \ldots + \psi_p^2 - \psi_{p+1}^2 - \ldots - \psi_{p+q}^2. \tag{10}$$

Здесь p и q — число коэффициентов, равных 1 и -1 соответственно, $p \geqslant 0$, $q \geqslant 0$, $p + q \leqslant n = \dim L$. Число нулевых коэффициентов равно $n - p - q$.

Из канонического вида

$$Q(x) = \lambda_1 \xi_1^2 + \ldots + \lambda_n \xi_n^2$$

в базисе $e_1, \ldots, e_n$ легко получается нормальный вид (10): каждый коэффициент $\lambda_i \neq 0$ заменяется на $\operatorname{sign}(\lambda_i)$ и затем одинаковые коэффициенты объединяются в группы. Для построения базиса, соответствующего (10), нужно сначала перейти к векторам

$$f_i := \frac{1}{\sqrt{|\lambda_i|}} e_i, \quad \lambda_i \neq 0; \qquad f_i := e_i, \quad \lambda_i = 0.$$

В силу равенства

$$Q(f_i) = B(f_i, f_i) = \frac{1}{|\lambda_i|} B(e_i, e_i) = \frac{\lambda_i}{|\lambda_i|} = \operatorname{sign}(\lambda_i),\ \lambda_i \neq 0,$$

все коэффициенты $Q(x)$ в базисе f_i будут равны 1, -1 или 0. Знаки коэффициентов сохранятся. Остаётся лишь упорядочить базис по знаку этих коэффициентов.

Имеет место следующее утверждение, известное как *закон инерции квадратичных форм.*

Теорема 1. *Нормальный вид (10) квадратичной формы Q не зависит от способа приведения к этому виду, то есть является инвариантом Q.*

Иными словами, пусть Q двумя различными способами (то есть в двух различных базисах) приведена к каноническому виду. Тогда число положительных коэффициентов в первом варианте совпадает с их числом во втором варианте. То же имеет место отдельно для отрицательных и нулевых коэффициентов.

Доказательство. Пусть в базисе $f_1, \ldots, f_n$ выполняется (10), а в базисе $g_1, \ldots, g_n$ — равенство

$$Q(x) = \eta_1^2 + \ldots + \eta_s^2 - \eta_{s+1}^2 - \ldots - \eta_{s+t}^2. \tag{11}$$

Покажем сначала, что число положительных коэффициентов в (10) и (11) одно и то же, то есть $p = s$.

Пусть, например, $p > s$. Рассмотрим подпространства

$$L_1 := \operatorname{lin}(f_1, \ldots, f_p), \quad L_2 := \operatorname{lin}(g_{s+1}, \ldots, g_n).$$

По теореме о размерностях суммы и пересечения (пункт 6.2)

$$\dim L_1 \bigcap L_2 = \dim L_1 + \dim L_2 - \dim(L_1 + L_2) \geqslant$$

$$\geqslant \dim L_1 + \dim L_2 - n = p + (n - s) - n = p - s > 0.$$

Значит, $L_1 \bigcap L_2 \neq \{0\}$. Пусть $x \neq 0$ — некоторый вектор из $L_1 \bigcap L_2$. В базисе $f_1, \ldots, f_n$ $x = \{\psi_1, \ldots, \psi_p, 0, \ldots, 0\}$, поэтому по формуле (10) $Q(x) > 0$ (не все ψ_j равны нулю). В то же время в базисе $g_1, \ldots, g_n$ $x = \{0, \ldots, 0, \eta_{s+1}, \ldots, \eta_n\}$, и в соответствии с (11) $Q(x) < 0$. Противоречие означает, что неравенство $p > s$ невозможно. В силу симметрии невозможно и соотношение $p < s$. Тем самым, обязательно $p = s$.

По той же схеме может быть доказано равенство $q = t$ для числа отрицательных коэффициентов. Проще, однако, применить предыдущее рассуждение к квадратичной форме $-Q$. Очевидно, что q и t совпадают с числом *положительных* коэффициентов $-Q$ в базисе $f_1, \ldots, f_n$ и базисе $g_1, \ldots, g_n$ соответственно. По доказанному $q = t$.

Очевидно, что число нулевых коэффициентов в равенствах (10) и (11) также совпадает: если $p = s, q = t$, то и $n - (p + q) = n - (s + t)$. Мы доказали утверждение об инвариантности нормального вида.

Вторая часть утверждения сразу следует теперь из возможности перехода от канонического вида к нормальному, см. начало пункта.

Несовпадение числа коэффициентов одного знака для первого варианта канонического вида Q с соответствующим числом для второго варианта привело бы к

аналогичному несовпадению для двух вариантов нормального вида Q. Но, как мы показали выше, последнее невозможно.

Теорема доказана.

Определение 2. *Число ненулевых коэффициентов в каноническом виде Q называется рангом квадратичной формы Q. Число положительных (отрицательных) коэффициентов называется положительным (отрицательным) индексом инерции Q. Разность положительного и отрицательного индексов инерции называется сигнатурой Q.*

Из результатов предыдущих пунктов следуют такие свойства ранга r и сигнатуры σ.

1. Число r совпадает с рангом диагональной матрицы, соответствующей каноническому или нормальному виду Q.

2. Пусть для матрицы $\mathbf{A}$ квадратичной формы Q в некотором (необязательно каноническом базисе) выполнены условия $\Delta_k \neq 0$, $k = 1, \ldots, n$. Тогда положительный и отрицательный индексы Q равны соответственно числу V знакопостоянств и числу W знакоперемен в ряду

$$1,\ \Delta_1,\ \ldots,\ \Delta_n\ .$$

Поэтому $\sigma = V - W$. Это следует из теоремы Якоби пункта 10.2.

3. Неотрицательно определённая квадратичная форма Q характеризуется равенством $\sigma = r$. Действительно, это означает, что отрицательный индекс равен нулю.

Квадратичная форма является положительно определённой тогда и только тогда, когда $\sigma = n$. Это соответствует положительности всех коэффициентов в каноническом виде.

4. Все параметры могут быть найдены по собственным значениям λ_i симметричной матрицы $\mathbf{A}$, рассматриваемым с учётом кратностей. Именно, положительный (отрицательный) индекс равен числу положительных (отрицательных) λ_i. Ранг r равен сумме кратностей $\lambda_i \neq 0$, а сигнатура σ есть разность числа положительных и числа отрицательных λ_i.

Дополним этот список ещё одним важным свойством. Именно, мы покажем, что ранг квадратичной формы совпадает с рангом матрицы $\mathbf{A}$ *в любом базисе.* Предварительно дадим ещё одно определение.

Определение 3. *Нулевым подпространством билинейной формы B называется совокупность*

$$L_B := \{y \in L :\ B(x, y) = 0 \text{ для } \ x \in L\}.$$

Упражнение 1. Показать, что L_B есть линейное подпространство L.

Теорема 2. *Ранг матрицы $\mathbf{A}$ квадратичной формы Q в произвольном базисе равен* $\operatorname{rg}(\mathbf{A}) = n - \dim L_B$, *где B — полярная форма. Таким образом,* $\operatorname{rg}(\mathbf{A})$ *есть инвариант Q.*

Доказательство. Пусть $e_1, \ldots, e_n$ — базис, соответствующий $\mathbf{A}$. Заметим, что $y = \xi_1 e_1 + \ldots + \xi_n e_n \ \in L_B$ тогда и только тогда, когда

$$B(e_i, y) = 0, \quad i = 1, \ldots, n. \tag{12}$$

Подставим в (12) выражение для y и воспользуемся линейностью B по второму аргументу. Так как $B(e_i, e_j) = a_{ij}$, получается система уравнений относительно координат ξ_j :

$$\begin{gathered} a_{11}\xi_1 + a_{12}\xi_2 + \ldots + a_{1n}\xi_n = 0, \\ a_{21}\xi_1 + a_{22}\xi_2 + \ldots + a_{2n}\xi_n = 0, \\ \ldots \qquad \ldots \qquad \ldots \\ a_{n1}\xi_1 + a_{n2}\xi_2 + \ldots + a_{nn}\xi_n = 0. \end{gathered}$$

Таким образом, L_B изоморфно подпространству $X \subset \mathrm{R^n}$, задаваемому указанной системой линейных однородных уравнений. Как известно, $\dim X = n - \mathrm{rg}(\mathbf{A})$, см. пункт 6.6. Кроме того, $\dim L_B = \dim X$, см. 5.5. Отсюда и получается равенство $\mathrm{rg}(\mathbf{A}) = n - \dim L_B$.

Правая часть этого равенства не зависит от выбора базиса в L. Поэтому $\mathrm{rg}(\mathbf{A})$ есть инвариант Q.

Теорема доказана.

Ранг диагональной матрицы квадратичной формы в каноническом базисе равен рангу r самой квадратичной формы. Из теоремы 2 следует, что и в любом базисе $\mathrm{rg}(\mathbf{A}) = r$.

Итак, хотя матрица квадратичной формы Q меняется при изменении базиса, ранг этой матрицы остаётся неизменным — он численно равен числу ненулевых коэффициентов в каноническом виде Q.

Упражнение 2. Показать, что функционал $Q : M_n \to \mathrm{R}$, заданный равенством $Q(\mathbf{A}) := \mathrm{tr}(\mathbf{A}^2)$, является квадратичной формой. Найти положительный и отрицательный индексы инерции, ранг и сигнатуру Q. Рассмотреть случаи (i) $n = 2$, (ii) $n \in \mathrm{N}$.

11. Линейные операторы в евклидовом пространстве

Некоторые совокупности операторов в евклидовом пространстве определяются с помощью условий, в которых действие оператора согласуется со скалярным произведением. В конечномерной ситуации каждый вид операторов характеризуется также простыми свойствами их матриц в ортонормированном базисе.

Эта матричная характеризация выглядит следующим образом. Для каждого оператора A вводится *сопряжённый оператор* A^*, матрица которого получается из матрицы исходного оператора транспонированием.

Оператор, для которого сопряжённый совпадает с ним самим, называется *симметричным, или самосопряжённым.* Матрица такого оператора в любом ортонормированном базисе является симметричной.

Наконец, *ортогональный оператор* — это невырожденный оператор, матрица которого при транспонировании становится обратной себе.

В этом разделе устанавливаются свойства таких операторов и, в частности, каноническая форма их матриц. Особо отметим свойства симметричных операторов и матриц, имеющие многочисленные приложения. Ряд таких приложений приводится в тексте.

Действительное евклидово пространство, как и ранее, обозначается буквой E. Единичный оператор обозначается в настоящем разделе через I, а единичная матрица порядка n — через $\mathbf{I}$.

Задачу о *приведении к главным осям* поверхности второго порядка первым рассмотрел в 1826 г. великий Огюстен Коши (A.L. Cauchy, 1798 – 1857). Таким образом, именно Коши стоял у истоков *метода собственных значений.*

11.1. Инвариантные подпространства оператора в действительном линейном пространстве

Каждый линейный оператор A, действующий в *комплексном* линейном пространстве L размерности $n \geqslant 1$, обязательно имеет собственный вектор x. В связи с этим одномерное подпространство $L_1 := \lin(x)$ инвариантно относительно A.

Ситуация меняется, если L является *действительным.* В случае чётного n не каждый линейный оператор $A : L \to L$ имеет собственный вектор, а значит, и одномерное инвариантное подпространство (пример: оператор поворота в V_2 на угол $\pi/2$). По поводу определений и этих свойств см. пункты 9.1, 9.2.

В этом пункте мы докажем следующее утверждение, существенно используемое в дальнейшем.

Теорема. *Пусть L — действительное линейное пространство, $n = \dim L \geqslant 1$. Каждый линейный оператор $A : L \to L$ имеет одномерное или двумерное инвариантное подпространство L_1.*

Доказательство. Пусть $e_1, \ldots, e_n$ — базис L, $\mathbf{A}$ — матрица оператора A в этом базисе, $p(\lambda) := |\mathbf{A} - \lambda\mathbf{I}|$ — характеристический многочлен A. Из основной теоремы алгебры многочленов следует, что $p(\lambda_0) = 0$ для некоторого λ_0. Возможны две ситуации.

1. $\lambda_0 \in \mathrm{R}$. В этом случае λ_0 является собственным значением A. Существует собственный вектор x, соответствующий λ_0, то есть такой, что $A(x) = \lambda_0 x$ и $x \neq = 0$. Тогда $L_1 := \lim(x)$ является одномерным инвариантным подпространством оператора A, см. пункт 9.1.

2. $\lambda_0 \in \mathbf{C}$. Положим $\lambda_0 = \alpha + \beta\mathbf{i}$, $\alpha, \beta \in \mathrm{R}$. Рассмотрим следующую систему линейных уравнений с комплексными коэффициентами относительно неизвестных $z_1, \ldots, z_n \in \mathbf{C}$:

$$(\mathbf{A} - \lambda_0\mathbf{I}) \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{1}$$

Определитель этой системы $|\mathbf{A} - \lambda_0\mathbf{I}| = p(\lambda_0) = 0$. Поэтому (1) имеет ненулевое *комплексное* решение $z_1 = \xi_1 + \eta_1\mathbf{i}, \ldots, z_n = \xi_n + \eta_n\mathbf{i}$. Числа $\xi_i, \eta_j \in \mathrm{R}$ одновременно не равны 0. Запишем (1) в эквивалентном виде

$$\mathbf{A} \begin{pmatrix} \xi_1 + \eta_1\mathbf{i} \\ \vdots \\ \xi_n + \eta_n\mathbf{i} \end{pmatrix} = (\alpha + \beta\mathbf{i}) \begin{pmatrix} \xi_1 + \eta_1\mathbf{i} \\ \vdots \\ \xi_n + \eta_n\mathbf{i} \end{pmatrix}. \tag{2}$$

Выделим и приравняем действительные и мнимые части выражений, стоящих в (2). Мы получим два *действительных* матричных равенства:

$$\mathbf{A} \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} = \alpha \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} - \beta \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix}, \quad \mathbf{A} \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix} = \alpha \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix} + \beta \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}.$$

Введём в рассмотрение векторы $x := \{\xi_1, \ldots, \xi_n\}$, $y := \{\eta_1, \ldots, \eta_n\}$. Их координаты даны в том же базисе $e_1, \ldots, e_n$, в котором записана матрица $\mathbf{A}$. Среди этих векторов есть хотя бы один ненулевой. Последние матричные равенства равносильны соотношениям

$$A(x) = \alpha x - \beta y, \quad A(y) = \alpha y + \beta x. \tag{3}$$

Пусть теперь $L_1 := \lim(x, y)$. Тогда $1 \leqslant \dim L_1 \leqslant 2$. Соотношения (3) означают, что L_1 инвариантно относительно A.

Случай $\beta = 0$ соответствует $\lambda_0 = \alpha \in \mathrm{R}$ и относится к ситуации 1. В качестве L_1 мы можем взять $\lim(x)$ или $\lim(y)$; хотя бы одно из этих подпространств одномерно.

Теорема доказана.

Замечание 1. В случае $n = 2k+1$, $k = 0, 1, 2, \ldots$, оператор A *обязательно* имеет одномерное инвариантное подпространство, так как $p(\lambda)$ имеет нечётную степень и,

значит, хотя бы один корень $\lambda_0 \in \mathrm{R}$. С таким λ_0 мы попадаем в ситуацию 1 из доказательства теоремы. В случае $n = 2k$ одномерных инвариантных подпространств, как отмечалось, может не существовать.

Замечание 2. В дальнейшем мы используем тот факт, что комплексному корню $\lambda_0 = \alpha + \beta\mathbf{i}$ многочлена $p(\lambda)$ соответствуют векторы $x, y \in L$, одновременно не равные нулю, на которых оператор A действует по формулам (3).

11.2. Оператор, сопряжённый данному. Свойства сопряжения

Пусть E — действительное евклидово пространство со скалярным произведением (x, y), см. раздел 7.

Напомним, что имеют место следующие аксиомы скалярного произведения:

$$(x, y) = (y, x); \quad (x + y, z) = (x, z) + (y, z);$$

$$(\lambda x, y) = \lambda(x, y); \quad (x, x) \geqslant 0; \ (x, x) = 0 \iff x = 0.$$

Здесь $x, y, z \in E, \lambda \in \mathrm{R}$. Из этих свойств следует, что равенство $(x, y) = (x, z)$ для *любого* $x \in E$ гарантирует $y = z$ (пункт 7.1, упражнение 1). Мы будем часто применять этот простой результат без специальной ссылки.

Пусть $A : E \to E$ — линейный оператор. Для упрощения записи в выражениях со скалярным произведением $A(x)$ заменяется на Ax.

Теорема. *Оператор $B : E \to E$, удовлетворяющий равенству*

$$(Ax, y) = (x, By), \quad x, y \in E, \tag{4}$$

является единственным для A и линейным.

Если $\dim E = n \geqslant 1$, то матрицы операторов B и A в любом ортонормированном базисе связаны соотношением

$$\mathbf{B} = \mathbf{A}^T. \tag{5}$$

Наоборот, пусть операторы A и B таковы, что их матрицы в некотором ортонормированном базисе связаны соотношением (5). Тогда имеет место (4).

Доказательство. Пусть наряду с B существует оператор $C : E \to E$ такой, что $(Ax, y) = (x, Cy)$. Тогда $(x, Cy) = (x, By)$ для всех x и y. Поэтому $Cy = By$, $y \in E$, что означает $C = B$.

Для каждого $x \in E$ по свойствам скалярного произведения

$$(x, B(\alpha y_1 + \beta y_2)) = (Ax, \alpha y_1 + \beta y_2) = \alpha(Ax, y_1) + \beta(Ax, y_2) =$$

$$= \alpha(x, By_1) + \beta(x, By_2) = (x, \alpha By_1 + \beta By_2).$$

Отсюда $B(\alpha y_1 + \beta y_2) = \alpha By_1 + \beta By_2$, $y_1, y_2 \in E$, $\alpha, \beta \in \mathrm{R}$, то есть оператор B является линейным.

Докажем, что в конечномерной ситуации из (4) следует (5). Пусть $e_1, \ldots, e_n$ — ортонормированный базис E. Сопоставим операторам A и B их матрицы $\mathbf{A} = (a_{ij})$ и $\mathbf{B} = (b_{ij})$ в этом базисе. Для всех $i, j = 1, \ldots, n$ в силу (4)

$$(Ae_i, e_j) = (e_i, Be_j). \tag{6}$$

По определению матрицы линейного оператора $Ae_i = \{a_{1i}, a_{2i}, \ldots, a_{ni}\}$, $Be_j = \{b_{1j}, b_{2j} \ldots, b_{nj}\}$ в том же базисе. Применим правило вычисления скалярного произведения в координатах, соответствующих ортонормированному базису (пункт 7.4, теорема 1). Мы получим $(Ae_i, e_j) = a_{ji}$, $(e_i, Be_j) = b_{ij}$. Равенства (6) дают $a_{ji} = b_{ij}$, что эквивалентно (5).

Наконец, пусть для матриц операторов A и B в ортонормированном базисе $e_1, \ldots, e_n$ выполнено (5). Рассуждая, как выше, мы приходим к соотношению (6) для базисных векторов. Пусть $x = \{\xi_1, \ldots, \xi_n\}$, $y = \{\eta_1, \ldots, \eta_n\}$. Тогда

$$(Ax, y) = (A(\sum_{i=1}^{n} \xi_i e_i), \sum_{j=1}^{n} \eta_j e_j) = \sum_{i,j=1}^{n} \xi_i \eta_j (Ae_i, e_j) =$$

$$= \sum_{i,j}^{n} \xi_i \eta_j (e_i, Be_j) = (x, By).$$

В последнем равенстве использована линейность B. Итак, (4) установлено. Теорема полностью доказана.

Определение. *Линейный оператор $A^* : E \to E$, удовлетворяющий равенству $(Ax, y) = (x, A^*y)$, $x, y \in E$, называется сопряжённым к оператору $A : E \to E$.*

Как мы доказали выше, в конечномерной ситуации для каждого A существует единственный сопряжённый A^*. Таковым является оператор, матрица которого в данном ортонормированном базисе получается из матрицы оператора A транспонированием.

Отметим ряд свойств сопряжённых операторов, которые имеют место для произвольного (не обязательно конечномерного) E. Их обоснование в общей ситуации использует свойства скалярного произведения.

1°. $(A^*)^* = A$.

2°. $(AB)^* = B^*A^*$.

3°. $(A + B)^* = A^* + B^*$.

4°. $(\lambda A)^* = \lambda A^*$, $\lambda \in \mathrm{R}$.

5°. $O^* = O$.

6°. $I^* = I$.

Доказательство. 1° следует из равенства $(A^*y, x) = (y, Ax)$ и определения, применённого к оператору A^*.

2°. С одной стороны,

$$((AB)x, y) = (A(Bx), y) = (Bx, A^*y) = (x, B^*A^*y).$$

С другой стороны, $((AB)x, y) = (x, (AB)^* y)$. Остаётся использовать произвольность x, y.

3° и 4° получаются по той же схеме из равенств:

$$((A+B)x, y) = (Ax + Bx, y) = (Ax, y) + (Bx, y) =$$

$$= (x, A^*y) + (x, B^*y) = (x, A^*y + B^*y) = (x, (A^* + B^*)y),$$

$$((A+B)x, y) = (x, (A+B)^*y);$$

$$((\lambda A)x, y) = (\lambda Ax, y) = \lambda(Ax, y) =$$

$$= \lambda(x, A^*y) = (x, \lambda A^*y) = (x, (\lambda A^*)y),$$

$$((\lambda A)x, y) = (x, (\lambda A)^*y).$$

5°. При всех x, y выполнено $(x, O^*y) = (Ox, y) = (0, x) = 0$. Зафиксируем y и будем менять x. Нулевой вектор является единственным, ортогональным каждому $x \in E$. Поэтому $O^*y = 0$. Произвольность y означает, что $O^* = O$.

6°. Так как $(x, y) = (Ix, y) = (x, I^*y)$, то $y = I^*y$ для всех y. Это и означает $I^* = I$.

Свойства доказаны.

В *конечномерной* ситуации $1^\circ - 6^\circ$ легко устанавливаются и другим способом, а именно с учётом теоремы этого пункта. Зафиксируем произвольный ортонормированный базис E. Переход от A к A^* означает для матриц операторов переход от $\mathbf{A}$ к $\mathbf{A}^T$. Так как $1^\circ - 6^\circ$ справедливы для матриц порядка n (то есть при замене A на $\mathbf{A}$ и сопряжения на транспонирование), то они справедливы и в исходном операторном виде.

Упражнение. Дать аккуратное доказательство каждого из свойств $1^\circ - 6^\circ$ *по предложенной схеме.*

11.3. Симметричный (самосопряжённый) оператор и его свойства

Напомним, что SM_n обозначает совокупность действительных симметричных матриц порядка n. Каждая матрица $\mathbf{A} = (a_{ij}) \in SM_n$ удовлетворяет условию $\mathbf{A}^T = \mathbf{A}$, или $a_{ji} = a_{ij}$. Как отмечалось, SM_n есть линейное подпространство M_n, причём $\dim SM_n = (n^2 + n)/2$, см. пункт 6.3.

Мы установим важные свойства матриц из SM_n, часто используемые в приложениях. Как и ранее, наш подход связан с анализом некоторых операторов в евклидовом пространстве E.

Определение. *Линейный оператор $A : E \to E$, для которого $A^* = A$, называется симметричным, или самосопряжённым.*

Иначе говоря, симметричный оператор определяется равенством

$$(Ax, y) = (x, Ay), \ x, y \in E.$$

Пример 1. Рассмотрим в R^3 оператор умножения на матрицу

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

Образ $x = (x_1, x_2, x_3) \in \mathrm{R}^3$ есть $Ax = (x_1 - x_2 + 4x_3, -x_1 + 2x_2, 4x_1 + 3x_3)$. Считаем, что скалярное произведение в R^3 задано стандартным образом. Для $y = (y_1, y_2, y_3)$ легко получаются равенства:

$$(Ax, y) = (x_1 - x_2 + 4x_3)y_1 + (-x_1 + 2x_2)y_2 + (4x_1 + 3x_3)y_3 =$$

$$= x_1y_1 - x_1y_2 + 4x_1y_3 - x_2y_1 + 2x_2y_2 + 4x_3y_1 + 3x_3y_3 =$$

$$x_1(y_1 - y_2 + 4y_3) + x_2(-y_1 + 2y_2) + x_3(4y_1 + 3y_3) = (x, Ay).$$

Значит, A — симметричный оператор. Это обусловлено тем, что матрица оператора в ортонормированном базисе $e^{(1)} = (1, 0, 0), e^{(2)} = (0, 1, 0), e^{(3)} = (0, 0, 1)$, то есть $\mathbf{A}$, является симметричной. Общий факт выражается теоремой 1.

Упражнение 1. Показать по схеме примера 1, что оператор умножения в R^n *на матрицу* $\mathbf{A} \in SM_n$ *является симметричным.*

Пример 2. Определение действует и в бесконечномерной ситуации. Пусть функция двух переменных $K(s, t)$ непрерывна на квадрате $[0, 1]^2$ и такова, что $K(t, s) = = K(s, t)$. Определим оператор $A : C[0, 1] \to C[0, 1]$ равенством

$$Ax(t) := \int_0^1 K(s, t)x(s)ds, \quad t \in [0, 1].$$

Положим для $x(\cdot), y(\cdot) \in C[0, 1]$

$$(x, y) := \int_0^1 x(t)y(t)dt.$$

Тогда

$$(Ax, y) = \int_0^1 \Big(\int_0^1 K(s, t)x(s)ds\Big)y(t)dt = \int_0^1 \int_0^1 K(s, t)x(s)y(t)dsdt =$$

$$= \int_0^1 \int_0^1 K(t, s)x(s)y(t)dsdt = \int_0^1 \Big(\int_0^1 K(t, s)y(t)dt\Big)x(s)ds = (x, Ay).$$

Мы поменяли порядок интегрирования. Таким образом, оператор A является симметричным.

В дальнейшем считаем $\dim E = n, n \in \mathrm{N}$. Следующая теорема даёт *характеризацию симметричных операторов в конечномерных пространствах.*

Теорема 1. *Пусть A — симметричный оператор, $\mathbf{A}$ — матрица A в произвольном ортонормированном базисе. Тогда $\mathbf{A} \in SM_n$.*

Наоборот, линейный оператор, соответствующий в некотором ортонормированном базисе матрице $\mathbf{A} \in SM_n$, является симметричным.

Доказательство получается из результатов предыдущего пункта. Так как оператору A^* в ортонормированном базисе соответствует матрица $\mathbf{A}^T$, то равенство $A = A^*$ влечёт $\mathbf{A} = \mathbf{A}^T$.

Наоборот, если в некотором ортонормированном базисе матрица оператора A является симметричной, то для неё $\mathbf{A}^T = \mathbf{A}$. Переход к операторам даёт $A^* = A$. Таким образом, A является симметричным.

Замечание 1. Утверждение теоремы 1 эквивалентно следующему. Оператор $A : E \to E$ является симметричным тогда и только тогда, когда для векторов произвольного ортонормированного базиса $e_1, \ldots, e_n$ выполнено $(Ae_i, e_j) = (e_i, Ae_j)$. Последнее условие выглядит как равенство $a_{ji} = a_{ij}$ для элементов матрицы $\mathbf{A}$ оператора в том же базисе. Это условие *на базисных векторах* означает, что $(Ax, y) = (x, Ay)$ при *всех* $x, y \in E$. Подробнее см. доказательство теоремы предыдущего пункта для $B = A$.

Перейдём теперь к описанию свойств собственных значений и собственных векторов симметричного оператора.

Теорема 2. *Характеристический многочлен $p(\lambda)$ симметричного оператора A имеет только действительные корни.*

Иначе говоря, симметричный оператор, действующий в n-мерном E, имеет n собственных значений с учётом их алгебраических кратностей и всегда имеет собственный вектор.

Доказательство. Пусть $\lambda_0 = \alpha + \beta\mathbf{i}$ — комплексный корень $p(\lambda)$. Как отмечалось в пункте 11.1 (см. там равенства (3) и замечание 2), существуют $x, y \in E$, одновременно не равные нулю, для которых

$$Ax = \alpha x - \beta y, \quad Ay = \alpha y + \beta x.$$

Тогда

$$(Ax, y) = (\alpha x - \beta y, y) = \alpha(x, y) - \beta(y, y),$$
$$(x, Ay) = (x, \alpha y + \beta x) = \beta(x, x) + \alpha(x, y).$$

Оператор A — симметричный, поэтому последние величины равны. Вычитая из второго равенства первое, получим

$$\beta\Big[(x, x) + (y, y)\Big] = 0.$$

Так как x, y не равны нулю одновременно, то выражение в квадратных скобках отлично от 0. Это означает, что $\beta = 0$, то есть $\lambda_0 \in \mathrm{R}$. Это доказывает первую часть теоремы.

Вторая часть следует из основной теоремы алгебры многочленов и определения собственного вектора.

Теорема 3. *Собственные векторы симметричного оператора, соответствующие попарно различным собственным значениям, попарно ортогональны.*

Доказательство. Пусть собственные векторы e_1, e_2 симметричного оператора A соответствуют $\lambda_1 \neq \lambda_2$. Имеют место равенства:

$$(Ae_1, e_2) = (e_1, Ae_2), \quad Ae_1 = \lambda_1 e_1, \quad Ae_2 = \lambda_2 e_2.$$

Из них по свойствам скалярного произведения $(\lambda_1 - \lambda_2)(e_1, e_2) = 0$. Так как $\lambda_1 - \lambda_2 \neq 0$, то $(e_1, e_2) = 0$, что и требовалось доказать.

Теорема 4. *Пусть e — собственный вектор симметричного оператора A. Тогда совокупность $E' := \{x \in E : \ (x, e) = 0\}$ является инвариантным подпространством A размерности $n - 1$.*

Доказательство. По свойствам скалярного произведения, E' — линейное подпространство E. Очевидно, $\dim E' = n - 1$. Покажем, что E' инвариантно относительно A.

Пусть $Ae = \lambda e$. Возьмём $x \in E'$; тогда $(x, e) = 0$. Умножим последнее равенство на λ и воспользуемся симметричностью A:

$$0 = (x, \lambda e) = (x, Ae) = (Ax, e).$$

Это означает, что $Ax \in E'$. Теорема доказана.

Наконец, отметим центральный результат этого пункта.

Теорема 5. *Пусть $A : E \to E$ — симметричный оператор. Тогда в E существует ортонормированный базис, состоящий из собственных векторов A.*

Иначе говоря, каждый симметричный оператор является диагонализируемым (или оператором простой структуры), причём канонический базис для него может быть выбран ортонормированным.

Доказательство. Построим сначала ортогональный базис E, состоящий из собственных векторов оператора A.

В соответствии с теоремой 2 оператор $A : E \to E$ имеет собственный вектор f_1. Рассмотрим подпространство $E_1 := \{x \in E : \ (x, f_1) = 0\}$. Так как E_1 инвариантно относительно A (теорема 4), то можно считать $A : E_1 \to E_1$. Этот последний оператор, действующий в $E_1, \dim E_1 = n-1$, имеет собственный вектор $f_2 \in E_1$. Далее полагаем

$$E_2 := \{x \in E_1 : \ (x, f_2) = 0\} = \{x \in E : \ (x, f_1) = (x, f_2) = 0\}.$$

Симметричный оператор A, действующий в инвариантном подпространстве E_2, $\dim E_2 = n - 2$, имеет собственный вектор $f_3 \in E_2$, и так далее. Действуем таким образом до тех пор, пока не дойдём до инвариантного подпространства E_{n-1} размерности 1:

$$E_{n-1} := \{x \in E_{n-2} : \ (x, f_{n-1}) = 0\} = \{x \in E : (x, f_1) = \ldots = (x, f_{n-1}) = 0\}.$$

Оператор $A : E_{n-1} \to E_{n-1}$ имеет собственный вектор $f_n \in E_{n-1}$.

Собственные векторы $f_1, f_2, \ldots, f_n$ образуют ортогональный базис E. Действительно, каждый $f_j \neq 0$ как собственный вектор; по построению $(f_i, f_j) = 0, i \neq j$;

число векторов равно $n = \dim E$. Пусть $Af_j = \lambda_j f_j, j = 1, \ldots, n$. Заметим, что не все числа $\lambda_j \in \mathrm{R}$ обязательно различны.

Перейдём теперь к векторам

$$e_1 := \frac{1}{|f_1|} f_1, \ \ldots \ , \ e_n := \frac{1}{|f_n|} f_n.$$

Система $e_1, \ldots, e_n$ является ортонормированным базисом E, также состоящим из собственных векторов A. Именно, $Ae_j = \lambda_j e_j$ с теми же собственными значениями λ_j. Последние равенства означают, что в базисе $e_1, \ldots, e_n$ матрица оператора A будет диагональной, а именно

$$\mathbf{D} = \mathrm{diag}_n(\lambda_1, \ldots, \lambda_n).$$

Теорема доказана.

Замечание 2. Отдельно отметим свойства действительных симметричных матриц порядка n, вытекающие из теорем этого пункта.

Пусть $\mathbf{A} \in SM_n$. По теореме 2 характеристический многочлен $p(\lambda) = |\mathbf{A} - \lambda \mathbf{I}|$ имеет n действительных корней с учётом кратностей.

Теорема 5 означает, что $\mathbf{A}$ *ортогонально подобна некоторой диагональной матрице.* Именно, для неё существуют матрицы $\mathbf{D} = \mathrm{diag}_n(\lambda_1, \ \ldots, \ \lambda_n)$ и $\mathbf{C} \in M_n$, для которых

$$\mathbf{D} = \mathbf{C}^{-1}\mathbf{A}\mathbf{C}.$$

При этом столбцы $\mathbf{C}$ образуют в $\mathrm{R^n}$ ортонормированный базис относительно стандартного скалярного произведения. Такие матрицы $\mathbf{C}$ называются *ортогональными.* Для них $\mathbf{C}^{-1} = \mathbf{C}^T$, поэтому в дополнение к предыдущему

$$\mathbf{D} = \mathbf{C}^T\mathbf{A}\mathbf{C}.$$

Подробнее об ортогональных матрицах см. пункт 11.6.

Упражнение 2. Показать, что многочлен

$$f(t) = t^3 - (a^2 + b^2 + c^2)t - 2abc$$

имеет только действительные корни при всех $a, b, c \in \mathrm{R}$. *Связать* f *с характеристическим многочленом симметричной матрицы.*

Упражнение 3. Пусть собственные значения матриц $\mathbf{A}, \mathbf{B} \in SM_n$ *принадлежат отрезкам* $[a, b]$ *и* $[c, d]$ *соответственно. Доказать, что собственные значения матрицы* $\mathbf{A} + \mathbf{B}$ *принадлежат отрезку* $[a + c, b + d]$.

11.4. Приведение квадратичной формы к каноническому виду методом собственных значений

В начале пункта отмечается связь между симметричными операторами и билинейными формами в евклидовом пространстве. Выясняется, в частности, что

каждая квадратичная форма Q на E имеет вид $Q(x) = (Ax, x)$, где $A : E \to E$ — некоторый симметричный оператор.

Это даёт возможность использовать свойства A, установленные в предыдущем пункте, для приведения Q к каноническому виду. Соответствующий метод называется нами *методом собственных значений* ассоциированного с Q симметричного оператора A.

Докажем прежде всего следующее утверждение.

Теорема 1. *Равенство*

$$B(x, y) = (Ax, y) \tag{7}$$

устанавливает взаимно-однозначное соответствие между симметричными линейными операторами $A : E \to E$ и симметричными билинейными формами B на E.

Матрицы билинейной формы B и оператора A в любом ортонормированном базисе совпадают.

Доказательство. Пусть $A : E \to E$ — симметричный оператор. Тогда функция B, определяемая с помощью (7), является билинейной, то есть линейной по каждому аргументу $x, y \in E$. Это легко следует из линейности A и свойств скалярного произведения. Симметричность B связана с равенствами

$$B(y, x) = (Ay, x) = (y, Ax) = (Ax, y) = B(x, y).$$

Во втором из них используется то, что A — симметричный оператор. Ясно, что (7) гарантирует единственность B.

Пусть теперь B — симметричная билинейная форма на E. Сначала отметим, что оператор A, удовлетворяющий (7), является *единственным*. Если $B(x, y) = (Cx, y)$ для некоторого $C : E \to E$, то $(Cx, y) = (Ax, y)$ при всех $x, y \in E$. Это означает, что $C = A$.

Покажем теперь, что для каждой B симметричный оператор A *существует*. Зафиксируем ортонормированный базис $e_1, \ldots, e_n$. Пусть $\mathbf{A} = (a_{ij})$ — матрица B в этом базисе. Это означает, что $a_{ij} = B(e_i, e_j)$. Так как B является симметричной, то $\mathbf{A} \in SM_n$. Рассмотрим теперь линейный оператор, матрица которого в том же базисе совпадает с $\mathbf{A}$. В силу теоремы 1 этого пункта A является симметричным. Далее, пусть $x = \{\xi_1, \ldots, \xi_n\}, y = \{\eta_1, \ldots, \eta_n\}$ в том же базисе. Тогда

$$B(x, y) = \sum_{i,j}^{n} a_{ij}\xi_i\eta_j,$$

см.пункт 10.1, равенство (2). Для вычисления (Ax, y) воспользуемся правилом нахождения скалярного произведения в координатах для ортонормированного базиса. Так как

$$Ax = \{\sum_{j=1}^{n} a_{1j}\xi_j, \ldots, \sum_{j=1}^{n} a_{nj}\xi_j\},$$

и $a_{ij} = a_{ji}$, то

$$(Ax, y) = \sum_{i=1}^{n}\Big(\sum_{j=1}^{n} a_{ij}\xi_j\Big)\eta_i = \sum_{i,j=1}^{n} a_{ij}\xi_j\eta_i = \sum_{i,j=1}^{n} a_{ji}\xi_j\eta_i.$$

Сравнение полученных выражений даёт (7).

Наконец, (7) означает, что матрицы билинейной формы B и симметричного оператора A в любом ортонормированном базисе $e_1, \ldots, e_n$ совпадают. Обозначим эти матрицы временно $\mathbf{V}$ и $\mathbf{W}$. Применим (7) к базисным векторам. Мы получим по прежней схеме:

$$v_{ij} = B(e_i, e_j) = (Ae_i, e_j) = w_{ji} = w_{ij},$$

так как $\mathbf{W} \in SM_n$. Поэтому $\mathbf{V} = \mathbf{W}$.

Теорема доказана.

Следствие. *Каждая квадратичная форма Q на E имеет вид $Q(x) = (Ax, x)$, A — некоторый симметричный оператор. Матрицы квадратичной формы Q и оператора A в любом ортонормированном базисе совпадают.*

Наоборот, для любого симметричного оператора $A : E \to E$ функция $Q(x) := (Ax, x)$ является квадратичной формой.

Доказательство. Каждая квадратичная форма $Q(x)$ получается из полярной к ней симметричной билинейной формы $B(x, y)$ с помощью равенства $B(x, x) = Q(x)$. При этом полярная форма B восстанавливается по соответствующей Q однозначно, см. пункт 10.2. Пусть A — симметричный оператор, соответствующий полярной форме B в смысле (7). Для него будет выполнено $Q(x) = B(x, x) = (Ax, x)$. Матрица Q по определению есть матрица полярной формы B. По предыдущей теореме эта последняя в любом ортонормированном базисе совпадает с матрицей оператора A.

Вторая часть следствия получается из соответствия $Q \longleftrightarrow B \longleftrightarrow A$ при движении от A к Q.

Замечание 1. Отметим утверждение более общее, чем теорема 2. Именно, соотношение (7) устанавливает взаимно-однозначное соответствие между совокупностями *всех* линейных операторов $A : E \to E$ и *всех* билинейных форм B на E (без предположения симметричности тех и других). В случае выполнения (7) матрицы оператора A и билинейной формы B в любом ортонормированном базисе получаются одна из другой транспонированием.

Упражнение. Доказать утверждение из предыдущего замечания, модифицировав схему доказательства теоремы 2. Как из этого утверждения получается результат теоремы 2?

Перейдём к центральному утверждению этого пункта.

Теорема 2. *Пусть $Q(x) = (Ax, x)$ — квадратичная форма на E; $e_1, \ldots, e_n$ — ортонормированный базис E, составленный из собственных векторов ассоциированного симметричного оператора A. Обозначим через λ_i собственное значение, соответствующее e_i. Тогда в базисе $e_1, \ldots, e_n$ квадратичная форма имеет канонический вид*

$$Q(x) = \lambda_1 \xi_1^2 + \ldots + \lambda_n \xi_n^2. \tag{8}$$

Доказательство. Существование A и базиса $e_1, \ldots, e_n$ с отмеченными свойствами гарантировано предыдущим следствием и теоремой 5 пункта 11.3.

Пусть $x = \{\xi_1, \ldots, \xi_n\}$ в базисе $e_1, \ldots, e_n$. Справедлива следующая цепочка равенств:

$$Q(x) = (Ax, x) = (A \sum_{i=1}^{n} \xi_i e_i, \sum_{j=1}^{n} \xi_j e_j) = (\sum_{i=1}^{n} \xi_i A e_i, \sum_{j=1}^{n} \xi_j e_j) =$$

$$= (\sum_{i=1}^{n} \lambda_i \xi_i e_i, \sum_{j=1}^{n} \xi_j e_j) = \sum_{i,j=1}^{n} \lambda_i \xi_i \xi_j (e_i, e_j) = \sum_{i=1}^{n} \lambda_i \xi_i^2.$$

Мы использовали последовательно линейность оператора A, свойства скалярного произведения, затем равенства $Ae_i = \lambda_i e_i$ и, наконец, ортонормированность базиса $e_1, \ldots, e_n$.

Тем самым, равенство (8) установлено. Теорема доказана.

11.5. Приложения метода собственных значений

Ниже рассматриваются некоторые приложения метода, описанного в предыдущем пункте.

Во-первых, даётся простой критерий знакопостоянства квадратичной формы в терминах собственных значений её матрицы.

Во-вторых, излагается вопрос об *экстремальных свойствах собственных значений симметричного оператора.*

В-третьих, описывается решение задачи о приведении уравнений линий и поверхностей второго порядка к каноническому виду с использованием метода собственных значений. Обычно последняя задача обозначается как *приведение к главным осям.* Иногда это геометрическое название переносят на сам метод.

11.5.1. Положительная определённость квадратичной формы

Непосредственно из предыдущей теоремы получается простой критерий знакопостоянства квадратичной формы, дополняющий материал пункта 10.3.

Теорема 1. *Квадратичная форма Q является положительно (или: отрицательно, неотрицательно, неположительно) определённой тогда и только тогда, когда все собственные значения её матрицы* $\mathbf{A}$ *положительны (соответственно: отрицательны, неотрицательны, неположительны).*

Доказательство. Пусть $Q(x) = (Ax, x)$. Тогда матрицы формы Q и оператора A в ортонормированном базисе совпадают. Тем самым, числа λ_i из (8) есть собственные значения $\mathbf{A}$. Далее достаточно учесть анализ знакопостоянства Q по её каноническому виду.

Сравнение теоремы 1 с критерием Сильвестра, см. 10.3, позволяет дополнить свойства симметричных матриц. Именно, *если* $\mathbf{A} \in SM_n$, *то условия* $\lambda_i > 0$, $i = 1, \ldots, n$, *и* $\Delta_i > 0$, $i = 1, \ldots, n$, *эквивалентны.* Здесь λ_i — собственные значения, а Δ_i — главные миноры $\mathbf{A}$, стоящие в её первых строках и столбцах. Каждое из условий равносильно положительной определённости квадратичной формы, матрица которой совпадает с $\mathbf{A}$.

Пусть $\lambda_1 \leqslant \ldots \leqslant \lambda_n$ — собственные значения симметричного оператора $A : E \to E$. Обозначим через S *единичную сферу* E, то есть множество $S := \{x \in E : \ |x| = 1\}$. Как обычно, $|x| := \sqrt{(x,x)}$.

Покажем, что минимальное и максимальное собственные значения являются решениями некоторых экстремальных задач на сфере S.

Теорема 2. *Имеют место равенства*

$$\lambda_1 = \min_{x \neq 0} \frac{(Ax,x)}{(x,x)} = \min_{x \in S} (Ax,x), \quad \lambda_n = \max_{x \neq 0} \frac{(Ax,x)}{(x,x)} = \max_{x \in S} (Ax,x). \tag{9}$$

Векторы e_1 и e_n, на которых достигаются экстремумы в (9), являются собственными для A с собственными значениями λ_1 и λ_n.

Доказательство. Пусть $e_1, \ldots, e_n$ — базис из условия теоремы 2 предыдущего пункта, $x = \{\xi_1, \ldots, \xi_n\}$. Так как базис является ортонормированным, то $|x|^2 = (x,x) = \sum \xi_i^2$. Рассмотрим очевидное неравенство

$$\lambda_1 \sum_{i=1}^{n} \xi_i^2 \leqslant \sum_{i=1}^{n} \lambda_i \xi_i^2 \leqslant \lambda_n \sum_{i=1}^{n} \xi_i^2.$$

В силу (8) оно имеет вид

$$\lambda_1 (x,x) \leqslant (Ax,x) \leqslant \lambda_n (x,x). \tag{10}$$

Для $(x,x) = 1$, то есть $x \in S$, из (10) следует

$$\lambda_1 \leqslant (Ax,x) \leqslant \lambda_n.$$

Для всех $x \neq 0$ из того же неравенства (10)

$$\lambda_1 \leqslant \frac{(Ax,x)}{(x,x)} \leqslant \lambda_n.$$

Остаётся заметить, что при $x = e_1$ в этих соотношениях достигается левое, а при $x = e_n$ — правое равенство. Например,

$$(Ae_1, e_1) = (\lambda_1 e_1, e_1) = \lambda_1 (e_1, e_1) = \lambda_1.$$

Теорема доказана.

Замечание. Можно доказать, что не только минимальное и максимальное, но и все промежуточные собственные значения представляют собой решения некоторых экстремальных задач. Пусть, подробнее, $\lambda_1 \leqslant \lambda_2 \leqslant \lambda_3 \leqslant \ldots \leqslant \lambda_{n-2} \leqslant \lambda_{n-1} \leqslant \lambda_n$. Тогда

$$\lambda_1 = \min_{x \in S} (Ax,x), \quad \lambda_2 = \min_{x \in S : (x,e_1) = 0} (Ax,x),$$

$$\lambda_3 = \min_{x\in S:(x,e_1)=(x,e_2)=0} (Ax,x), \quad \ldots, \quad \lambda_n = \min_{x\in S:(x,e_1)=\ldots=(x,e_{n-1})=0} (Ax,x);$$

$$\lambda_n = \max_{x\in S}(Ax,x), \quad \lambda_{n-1} = \max_{x\in S:(x,e_n)=0}(Ax,x),$$

$$\lambda_{n-2} = \max_{x\in S:(x,e_n)=(x,e_{n-1})=0} (Ax,x), \quad \ldots, \quad \lambda_1 = \max_{x\in S:(x,e_n)=\ldots=(x,e_2)=0} (Ax,x).$$

Во всех вариантах экстремум λ_i достигается на соответствующем собственном векторе e_i.

Упражнение 1. Установить соотношения из последнего замечания.

Отношение $(Ax,x)/(x,x)$, стоящее в (9), называют *отношением Рэлея.* Рэлей (Rayleigh, 1842 – 1919) — английский физик, крупный учёный в области акустики, оптики, электричества, колебаний упругих тел и др., автор классической монографии "Теория звука"(1877 – 78). До получения титула лорда Рэлея носил фамилию Стратт (J.W. Strutt).

11.5.3. Приведение уравнений линий и поверхностей второго порядка к каноническому виду (приведение к главным осям)

Проиллюстрируем метод собственных значений на уравнении

$$ax^2 + 2bxy + cy^2 = 1. \tag{11}$$

Пусть на плоскости с декартовой системой координат Oxy задана линия второго порядка с уравнением (11). Считаем, что хотя бы один из коэффициентов a, b, c отличен от нуля. Если $b = 0$, то анализ (11) не представляет труда. В случае $b \neq 0$ удаётся ввести новую декартову систему координат $0uv$, получающуюся из Oxy некоторым поворотом и такую, в которой (11) приводится к виду

$$\lambda_1 u^2 + \lambda_2 v^2 = 1. \tag{12}$$

Обозначим орты исходного базиса через $\vec{i}, \vec{j}$. Рассмотрим тот линейный оператор $A : \mathrm{V}_2 \to \mathrm{V}_2$, матрица которого в базисе $\vec{i}, \vec{j}$ равна

$$\mathbf{A} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}.$$

В этом базисе A реализуется как оператор умножения столбца координат на матрицу $\mathbf{A}$. В связи с тем, что $\mathbf{A} \in SM_2$, оператор A является симметричным, и к нему можно применить подход этого пункта.

Построим ортонормированный правый базис из собственных векторов $\vec{e}_1, \vec{e}_2$ оператора A. Пусть новая система координат Ouv соответствует этим ортам $\vec{e}_1, \vec{e}_2$. Обозначим их собственные значения λ_1, λ_2.

Для вектора $\vec{r} = \{x, y\}$ легко получаем

$$(A\vec{r}, \vec{r}) = ax^2 + 2bxy + cy^2.$$

Это равенство соответствует следствию пункта 11.4. Так как (x, y) и (u, v) обозначают координаты одной и той же точки плоскости в двух системах Oxy и Ouv, то $\vec{r} = u\vec{e}_1 + v\vec{e}_2$. В связи с этим

$$ax^2 + 2bxy + cy^2 = (A\vec{r}, \vec{r}) = (uA\vec{e}_1 + vA\vec{e}_2, u\vec{e}_1 + v\vec{e}_2) =$$

$$= (u\lambda_1\vec{e}_1 + v\lambda_2\vec{e}_2, u\vec{e}_1 + v\vec{e}_2) = \lambda_1 u^2 + \lambda_2 v_2.$$

Так выглядит в этой ситуации доказательство теоремы 2 предыдущего пункта.

Тем самым, указанная система Ouv является искомой — в ней уравнение (11) имеет вид (12).

Если в исходном уравнении присутствуют линейные члены, то после поворота системы координат требуется выполнить ещё её некоторый параллельный перенос.

Пример. Исследуем линию с уравнением $3x^2 + 8xy - 3y^2 = 1$. Матрица соответствующей квадратичной формы есть

$$\mathbf{A} = \begin{pmatrix} 3 & 4 \\ 4 & -3 \end{pmatrix}.$$

Характеристический многочлен $p(\lambda) = \lambda^2 - \mathrm{tr}(\mathbf{A})\lambda + |\mathbf{A}| = \lambda^2 - 25$. Поэтому $\lambda_1 = 5, \lambda_2 = -5$. Собственные векторы $\vec{s} = \{x_1, x_2\}$ для $\lambda_1 = 5$ находятся из системы

$$-2x_1 + x_2 = 0,\ 4x_1 - 8x_2 = 0.$$

Их общий вид $\{2d, d\}, d \neq 0$. Возьмём $\vec{s} := \{2, 1\}$. Собственные векторы, соответствующие $\lambda_2 = -5$, есть $\{-d, 2d\}, d \neq 0$. Можно взять $\vec{t} := \{-1, 2\}$, так как двойка $\vec{s}, \vec{t}$ является правой:

$$\begin{vmatrix} 2 & 1 \\ -1 & 2 \end{vmatrix} = 5 > 0.$$

Нормируя $\vec{s}, \vec{t}$, находим

$$\vec{e}_1 := \{\frac{2}{\sqrt{5}}, \frac{1}{\sqrt{5}}\}, \qquad \vec{e}_2 := \{\frac{-1}{\sqrt{5}}, \frac{2}{\sqrt{5}}\}.$$

Введём в рассмотрение систему координат Ouv, соответствующую этим ортам. Матрица перехода от $\vec{i}, \vec{j}$ к $\vec{e}_1, \vec{e}_2$ имеет вид

$$\mathbf{C} = \frac{1}{\sqrt{5}} \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}.$$

Заметим, что $\mathbf{C}^{-1} = \mathbf{C}^T$, то есть $\mathbf{C}$ является ортогональной. Связь координат одной и той же точки плоскости в двух системах даётся матричными равенствами

$$\begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}, \quad \begin{pmatrix} u \\ v \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Оси новой системы координат Ou и Ov задаются векторами $\vec{s}$ и $\vec{t}$. Поэтому их уравнения в старой системе есть соответственно

$$\frac{x}{2} = \frac{y}{1}, \quad \frac{x}{-1} = \frac{y}{2}.$$

В системе координат Ouv уравнение линии преобразуется к виду $5u^2 - 5v^2 = 1$. Это гипербола, обе полуоси которой равны $\sqrt{0.2}$.

Коротко остановимся на преобразовании уравнений поверхностей второго порядка. Квадратичной форме уравнения поверхности в системе координат $Oxyz$, то есть выражению

$$H(x, y, z) = ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2fyz,$$

ставится в соответствие симметричный оператор $A : \mathrm{V}_3 \to \mathrm{V}_3$, матрица которого в исходном базисе $\vec{i}, \vec{j}, \vec{k}$ имеет вид

$$\mathbf{A} = \begin{pmatrix} a & d & e \\ d & b & f \\ e & f & c \end{pmatrix}.$$

Пусть $\vec{e}_1, \vec{e}_2, \vec{e}_3$ — ортонормированный базис V_3, состоящий из собственных векторов A, и $Ouvw$ — ассоциированная с ним декартова система координат. Тогда имеет место равенство

$$H(x, y, z) = \lambda_1 u^2 + \lambda_2 v^2 + \lambda_3 w^2.$$

Здесь λ_m есть собственное значение вектора $\vec{e}_m$, $m = 1, 2, 3$. Поэтому для упрощения уравнения следует перейти от $Oxyz$ к $Ouvw$.

Упражнение 2. Применить метод собственных значений к уравнению $z^2 = xy$.

11.6. Ортогональный оператор и его свойства

Среди операторов, действующих в евклидовом пространстве, особое место занимают операторы, которые сохраняют скалярное произведение.

Определение 1. *Линейный оператор $A : E \to E$, для которого при всех $x, y \in E$ выполнено*

$$(Ax, Ay) = (x, y), \tag{13}$$

называется ортогональным.

Так как A сохраняет скалярное произведение, то A сохраняет также длины векторов и углы между ними. Точнее, из (13) следует

$$|Ax| = \sqrt{(Ax, Ax)} = \sqrt{(x, x)} = |x|.$$

Если $x, y \neq 0$, то

$$\cos \overbrace{Ax, Ay} = \frac{(Ax, Ay)}{|Ax||Ay|} = \frac{(x, y)}{|x||y|} = \cos \overbrace{x, y}.$$

Здесь $\varphi = \widehat{a, b}$ обозначает такой угол между векторами $a, b \neq 0$, что $0 \leqslant \varphi \leqslant \pi$.

Из определения 1 вытекает ряд простых свойств ортогонального оператора. В дальнейшем, как обычно, $\dim E = n$.

Равенство $|Ax| = 0$ возможно лишь при $|x| = 0$, то есть $x = 0$. Это означает, что $\mathrm{Ker} A = \{0\}$. Таким образом, каждый ортогональный оператор является невырожденным, и для него выполнены все эквивалентные условия невырожденности, см. пункт 8.6. В частности, $\mathrm{Im} A = E$. Матрица A в любом базисе является невырожденной.

Пример. Оператор $A : \mathrm{V}_2 \to \mathrm{V}_2$ поворота на угол α является ортогональным. Геометрически очевидно, что A сохраняет длины и углы, а следовательно, и скалярное произведение. (Как обычно, в пространстве геометрических векторов длина и угол являются первичными понятиями. В абстрактном E они определяются через скалярное произведение.) Матрица оператора A в исходном ортонормированном базисе $\vec{i}, \vec{j}$ имеет вид

$$\mathbf{A} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}.$$

Нетрудно видеть, что $|\mathbf{A}| = 1$ и $\mathbf{A}^{-1} = \mathbf{A}^T$. Эта примечательная матрица возникает и в общей ситуации.

Упражнение 1. Дать простое операторное обоснование матричному равенству

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}^m = \begin{pmatrix} \cos m\alpha & -\sin m\alpha \\ \sin m\alpha & \cos m\alpha \end{pmatrix}$$

для (i) $m \in \mathrm{N}$, (ii) $m = -1$, (iii) $m \in \mathrm{Z}$.

Можно дать эквивалентное определение ортогонального оператора с использованием понятия сопряжённого, см. пункт 11.2. Предоставляем читателю убедиться в равносильности этих двух подходов в виде следующего полезного упражнения.

Упражнение 2. Доказать, что A является ортогональным тогда и только тогда, когда $A^{-1} = A^*$, то есть $AA^* = A^*A = I$.

Рассуждение не требует перехода к матрицам операторов, ср. с упражнением 5.

Следующее утверждение сводит проверку условия (13) к векторам ортонормированного базиса. Здесь и далее δ_{ij} — символ Кронекера.

Теорема 1. *Если A является ортогональным, то для векторов любого ортонормированного базиса $e_1, \ldots, e_n$*

$$(Ae_i, Ae_j) = (e_i, e_j) = \delta_{ij}. \tag{14}$$

Наоборот, если (14) выполнено для некоторого ортонормированного базиса, то оператор A является ортогональным.

Доказательство. Первая часть следует непосредственно из определения: надо применить (13) к $x = e_i,\ y = e_j$.

Пусть (14) выполнено для векторов некоторого ортонормированного базиса. Если в этом базисе $x = \{\xi_1, \ldots, \xi_n\}$, $y = \{\eta_1, \ldots, \eta_n\}$, то

$$(Ax, Ay) = (A\sum_{i=1}^{n} \xi_i e_i, A\sum_{j=1}^{n} \eta_j e_j) = \sum_{i,j=1}^{n} \xi_i \eta_j (Ae_i, Ae_j) =$$

$$= \sum_{i,j=1}^{n} \xi_i \eta_j (e_i, e_j) = \sum_{i,j=1}^{n} \xi_i \eta_j \delta_{ij} = \sum_{i=1}^{n} \xi_i \eta_i = (x, y).$$

Мы использовали правило вычисления скалярного произведения в координатах в ортонормированном базисе. Теорема доказана.

Дадим матричную характеризацию ортогональных операторов. Для этой цели сформулируем второе важное определение.

Определение 2. *Невырожденная матрица* $\mathbf{A} \in M_n$, *для которой* $\mathbf{A}^{-1} = \mathbf{A}^T$, *называется ортогональной.*

Таким образом, ортогональные матрицы и только они удовлетворяют соотношению

$$\mathbf{A}\mathbf{A}^T = \mathbf{I} = \mathbf{A}^T\mathbf{A}. \tag{15}$$

Справедливость одного из равенств (15) означает, что $\mathbf{A}^{-1} = \mathbf{A}^T$ и, значит, влечёт справедливость другого. Так как $|\mathbf{A}^T| = |\mathbf{A}|$, то определитель ортогональной матрицы равен 1 или -1.

Теорема 2. *Матрица ортогонального оператора в любом ортонормированном базисе является ортогональной. Наоборот, оператор, матрица которого в некотором ортонормированном базисе ортогональна, является ортогональным.*

Доказательство. Пусть $\mathbf{A} = (a_{ij})$ — матрица ортогонального оператора A в ортонормированном базисе $e_1, \ldots, e_n$. Тогда $Ae_i = \{a_{1i}, \ldots, a_{ni}\}$, $Ae_j = \{a_{1j}, \ldots, a_{nj}\}$. Поэтому

$$(Ae_i, Ae_j) = \sum_{k=1}^{n} a_{ki} a_{kj}.$$

Левая часть одновременно равна $(e_i, e_j) = \delta_{ij}$. Поэтому

$$\sum_{k=1}^{n} a_{ki} a_{kj} = \delta_{ij} \tag{16}$$

Нетрудно видеть, что (16) эквивалентно $\mathbf{A}^T\mathbf{A} = \mathbf{I}$. Из последнего условия следует невырожденность $\mathbf{A}$ и равенство $\mathbf{A}^{-1} = \mathbf{A}^T$. Таким образом, $\mathbf{A}$ является ортогональной.

Наоборот, пусть $\mathbf{A}$ есть матрица оператора A в ортонормированном базисе $e_1, \ldots, e_n$. Предположим, что $\mathbf{A}$ ортогональна. Тогда имеет место (16). Для базисных векторов это даёт

$$(Ae_i, Ae_j) = \delta_{ij} = (e_i, e_j).$$

По теореме 1 оператор A является ортогональным.

Теорема 2 доказана.

Как отмечалось в пункте 8.7, определитель матрицы оператора не зависит от базиса, в котором эта матрица записана. Ортогональный оператор A, для которого $|\mathbf{A}| = 1$, называется *собственным.* Если же $|\mathbf{A}| = -1$, то A называется *несобственным.*

Упражнение 3. Доказать, что произведение двух собственных ортогональных операторов является собственным, а произведение собственного на несобственный — несобственным ортогональным оператором.

Упражнение 4. Существуют ли такие ортогональные матрицы $\mathbf{A}, \mathbf{B} \in M_3$, *что* $\mathbf{ABA}^2\mathbf{B}^2\mathbf{A}^3\mathbf{B}^3 = -\mathbf{I}$?

Упражнение 5. Установить результат упражнения 2 с помощью матричного подхода.

Перейдём теперь к построению канонического вида матрицы ортогонального оператора.

Теорема 3. *Пусть* $E_1 \subset E$ *— инвариантное подпространство ортогонального оператора* A. *Тогда* $E_1^\perp$ *также инвариантно относительно* A.

Доказательство. Пусть $y \in E_1^\perp$. Покажем, что $Ay \in E_1^\perp$. Это и будет означать инвариантность $E_1^\perp$ относительно A.

Пусть $x \in E_1$. Тогда $x = Ax_1$ для некоторого $x_1 \in E_1$. Действительно, A действует из E_1 в E_1 и является невырожденным как ортогональный оператор. Это означает, в частности, что образ A как оператора из E_1 в E_1 совпадает со всем E_1.

В предыдущих обозначениях

$$(Ay, x) = (Ay, Ax_1) = (y, x_1) = 0.$$

Мы ещё раз использовали ортогональность A и то, что $y \in E_1^\perp$. В силу произвольности $x \in E_1$ это означает, что $Ay \in E_1^\perp$.

Теорема доказана.

Мы увидим в дальнейшем, что изучение ортогонального оператора в определённом смысле сводится к случаям $n = 1$ и $n = 2$. Действие оператора в одномерном и двумерном пространствах описывается следующим утверждением.

Теорема 4. *Пусть* $A : E \to E$ *— ортогональный оператор. Если* $\dim E = 1$, *то* $Ax = x$ *или* $Ax = -x$.

Если $\dim E = 2$ *и* A *— собственный, то в любом ортонормированном базисе* e_1, e_2 *матрица* A *имеет вид*

$$\mathbf{A} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}.$$

Если $\dim E = 2$ *и* A *— несобственный, то в некотором ортонормированном базисе его матрица имеет вид*

$$\mathbf{A}' = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Доказательство. Пусть сначала $\dim E = 1$. Тогда $E = \mathrm{lin}(e), e \neq 0$. Тогда $Ae \in \mathrm{lin}(e)$, то есть $Ae = \lambda e$ для некоторого $\lambda \in \mathrm{R}$. В этом случае действие A на произвольном $x = \mu e$ имеет вид

$$Ax = A(\mu e) = \mu Ae = \mu\lambda e = \lambda x.$$

Наконец, условие $(Ae, Ae) = (e, e)$ даёт $\lambda^2 = 1$, то есть $\lambda = \pm 1$. Таким образом, либо $Ax = x$ (собственный ортогональный оператор), либо $Ax = -x$ (несобственный ортогональный оператор).

Пусть теперь $\dim E = 2$. Считаем, что в исходном ортонормированном базисе e_1, e_2 оператор A имеет матрицу

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Если оператор A — собственный, то $|\mathbf{A}| = ad - bc = 1$. Равенство $\mathbf{A}^{-1} = \mathbf{A}^T$ означает

$$\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

После упрощений получим

$$\mathbf{A} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \qquad a^2 + b^2 = 1.$$

Полагая $a = \cos\alpha, -b = \sin\alpha, \alpha \in [0, 2\pi)$, приходим к матрице, указанной в условии. Геометрическая интерпретация такого оператора — поворот в плоскости e_1, e_2 на угол α.

Если же A — несобственный, то $|\mathbf{A}| = -1$. В этом случае корни $p(\lambda) = \lambda^2 - -(a+d)\lambda - 1$ являются действительными, поэтому A имеет собственный вектор e. Пусть $Ae = \lambda e$ и $|e| = 1$. Ортогональность A даёт $\lambda = \pm 1$.

Выберем f так, чтобы было $(f, e) = 0$, $|f| = 1$. Тогда f также является собственным для A. Действительно, $(Af, Ae) = (f, e) = 0$, но $Ae = \pm e$, поэтому $(Af, e) = 0$. Пусть $Af = \tau e + \mu f$. Скалярно умножив это равенство на e, получим $\tau = 0$. Значит, $Af = \mu f$. Из ортогональности A следует $\mu = \pm 1$.

Отметим, что рассуждение последнего абзаца эквивалентно применению теоремы 3 к $E_1 := \mathrm{lin}(e)$. Оператор A в исследуемой ситуации имеет два одномерных инвариантных подпространства.

Итак, $Ae = \pm e, Af = \pm f$. В ортонормированном базисе e, f матрица оператора A имеет вид

$$\mathbf{A}' = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}.$$

Так как $|\mathbf{A}'| = -1$, то из четырёх вариантов сочетания знаков возможны лишь два. Меняя, если нужно, порядок базисных векторов, получим матрицу, указанную в условии; мы сохраняем за ней обозначение $\mathbf{A}'$. Геометрический смысл соответствующего оператора — отражение относительно оси.

Теорема доказана.

Наконец, установим основной результат этого пункта.

Теорема 5. *Пусть $A : E \to E$ — ортогональный оператор, $\dim E = n$. Существует ортонормированный базис, в котором матрица оператора A имеет вид*

$$\mathbf{A} = \begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & & 0 & \\ & & 1 & & & & & & & & \\ & & & -1 & & & & & & & \\ & & & & \ddots & & & & & & \\ & & & & & -1 & & & & & \\ & & & & & & \cos\alpha_1 & -\sin\alpha_1 & & & \\ & & & & & & \sin\alpha_1 & \cos\alpha_1 & & & \\ & & & & & & & & \ddots & & \\ & & & & & & & & & \ddots & \\ & 0 & & & & & & & & \cos\alpha_r & -\sin\alpha_r \\ & & & & & & & & & \sin\alpha_r & \cos\alpha_r \end{pmatrix}.$$

Доказательство. Покажем, что всё пространство E представляется в виде прямой суммы одномерных G_i и двумерных H_j инвариантных для A подпространств:

$$E = G_1 \oplus \ldots \oplus G_q \oplus H_1 \oplus \ldots \oplus H_r. \tag{17}$$

При этом оператор A на каждом H_j является собственным.

В силу теоремы пункта 11.1 оператор $A : E \to E$ имеет одномерное или двумерное инвариантное подпространство M. Если $\dim M = 1$, положим $G_1 := M$. Пусть $\dim M = 2$. Если M содержит некоторое одномерное инвариантное M', положим $G_1 := M'$. В противном случае считаем $H_1 := M$. Тогда $A : M \to M$ является собственным: иначе A имеет одномерное инвариантное подпространство, см. доказательство теоремы 4.

Перейдём далее к $M^\perp$. По теореме 3 оно инвариантно относительно A. Применим наш метод к оператору $A : M^\perp \to M^\perp$. В приведённом рассуждении роль E будет играть $M^\perp$. Мы найдём очередное G_2 или H_2. Ортогональное к нему берётся уже в $M^\perp$, и так далее. Действуем подобным образом до тех пор, пока не будет выполнено

$$\sum_i \dim G_i + \sum_j \dim H_j = n.$$

В результате мы получим разложение (17). Одно из чисел q или r может быть нулём; это означает, что правая часть (17) не содержит соответствующих слагаемых.

На каждом G_i оператор A действует по правилу $Ax = x$ или $Ax = -x$, см. теорему 4. Упорядочим $G_1, \ldots, Gq$ так, чтобы на первых подпространствах было $Ax = x$, а на последних — $Ax = -x$.

Выберем теперь базис E как объединение ортонормированных базисов в G_1, $\ldots$, G_q, H_1, $\ldots$, H_r. По теореме 4 матрица оператора A в этом ортонормированном базисе будет совпадать с $\mathbf{A}$.

Теорема доказана.

Замечание 1. Нетрудно видеть, что матрица $\mathbf{A}$ из условия теоремы 5 представляется в виде произведения

$$\mathbf{A} = \mathbf{A_1} \dots \mathbf{A_q} \mathbf{B_1} \dots \mathbf{B_r}. \tag{18}$$

Матрицы правой части (18) получаются из единичной исправлением некоторых элементов последней. Именно, $\mathbf{A_i}$ получается заменой одного из диагональных элементов $\mathbf{I}$ на -1; $\mathbf{B_j}$ — заменой одной из клеток второго порядка, стоящих на главной диагонали $\mathbf{I}$, на клетку

$$\begin{pmatrix} \cos\alpha_j & -\sin\alpha_j \\ \sin\alpha_j & \cos\alpha_j \end{pmatrix}. \tag{19}$$

Число q равно количеству -1 на диагонали $\mathbf{A}$; число r — количеству блоков (19). Если $q = 0$ или $r = 0$, то соответствующих сомножителей в (18) нет.

Несобственный ортогональный оператор A_i, матрицей которого является $\mathbf{A_i}$, называется *простым отражением.* Собственный ортогональный оператор B_j с матрицей $\mathbf{B_j}$ называется *простым вращением.* Равенство (18) означает, что

$$A = A_1 \dots A_q B_1 \dots B_r.$$

Таким образом, каждый ортогональный оператор есть произведение некоторого числа простых отражений и некоторого числа простых вращений.

Замечание 2. Сформулируем полученные в этом пункте результаты в терминах матриц порядка n.

Пусть $\mathbf{B} \in M_n$ ортогональна, то есть $\mathbf{B}^{-1} = \mathbf{B}^T$. Тогда все собственные значения $\mathbf{B}$ (действительные корни $p(\lambda) := |\mathbf{B} - \lambda\mathbf{I}|$), если они существуют, равны 1 или -1.

Существуют невырожденная матрица $\mathbf{C}$ и матрица $\mathbf{A}$ из условия теоремы 5, для которых $\mathbf{B} = \mathbf{C}^{-1}\mathbf{A}\mathbf{C}$. При этом $\mathbf{C}$ также является ортогональной — как матрица перехода от одного ортонормированного базиса $\mathrm{R^n}$ к другому. Поэтому одновременно $\mathbf{B} = \mathbf{C}^T\mathbf{A}\mathbf{C}$. С учётом представления (18) получаем также, что

$$\mathbf{B} = \mathbf{C}^T \mathbf{A_1} \dots \mathbf{A_l} \mathbf{B_1} \dots \mathbf{B_k} \mathbf{C}. \tag{20}$$

Упражнение 6. Исследовать возможность экономичного вычисления степени $\mathbf{B}^m$ при большом $m \in \mathrm{N}$ для ортогональной $\mathbf{B}$ с использованием представления (20) и результата упражнения 1.

Часть 4

12. Группа, кольцо, поле

Группа, кольцо и поле относятся к классическим *алгебраическим системам, или структурам.* Терминология алгебраических систем — это язык современной математики и её приложений, относящийся к фундаменту науки. Главной задачей этого раздела является знакомство читателя с соответствующими понятиями и примерами, что сделает возможным дальнейшее изучение предмета.

Группа — алгебраическая система с одной *бинарной операцией*, обладающей набором простых свойств. В *кольце и поле* вводятся уже две операции, формально называемые сложением и умножением. Списку отдельных аксиом каждой из этих систем можно придать краткий вид общего описания структур сложения и умножения.

Уточнение свойств кольца касается лишь второй операции. Максимальные требования к мультипликативной структуре содержатся в определении поля. Таким образом, каждое поле является кольцом, но далеко не всякое кольцо является полем.

Важнейшей из трёх отмеченных является структура группы.

Абстрактное понятие группы введено в середине 19 века Артуром Кэли (A. Cayley, 1821 – 1895), Георгом Фробениусом (G. Frobenius, 1849 – 1917) и др. Однако идея группы оформлялась и прояснялась в течение предшествующих примерно ста лет.

Исторические источники понятия группы — решение алгебраических уравнений в радикалах, потребности геометрии и теория чисел. Не претендуя на полноту, отметим здесь некоторые имена.

С первым направлением связывают работы Жозефа Луи Лагранжа (J.L. Lagrange, 1736 – 1813), Паоло Руффини (P. Ruffini, 1765 – 1822), Нильса Хенрика Абеля (N.H. Abel, 1802 – 1829) и, в особенности, Эвариста Галуа (E. Galois, 1811 – 1832). Галуа ввёл в употребление сам термин *группа.* (В современной терминологии его результат выглядит следующим образом: *алгебраическое уравнение* $f(x) = 0$ *разрешимо в радикалах* $\Longleftrightarrow$ *группа Галуа многочлена* f *является разрешимой.*)

Второе направление связано с именем немецкого математика Феликса Клейна (F. Klein, 1849 – 1925), положившего в основу классификации геометрий понятие группы преобразований (1872).

Наконец, теоретико-числовые основы понятия группы заложены в работах великих Леонарда Эйлера (L. Euler, 1707 – 1783) и Карла Фридриха Гаусса (C.F. Gauss, 1777 – 1855).

На развитие теории групп в России большое влияние оказала книга О.Ю. Шмидта (1891 – 1956) "Абстрактная теория групп"(1916).

Для первоначального знакомства с основными алгебраическими системами могут использоваться учебники А.Г. Куроша [16] и А.И. Кострикина [13]. Дальнейшие сведения по алгебраическим системам и, в частности, по теории групп, читатель может найти в учебнике [14]. В этой книге и, например, монографии [12] имеются списки дополнительной литературы. Отметим здесь ставшую классической монографию [17].

Обширная литература посвящена приложениям алгебраических структур к прикладным задачам.

Конечные поля Галуа $GF(p^k)$ служат блестящей иллюстрацией того, что деление математики на фундаментальную и прикладную является во многом условным. Отметим приложения конечных структур к *теории кодирования* и задачам *цифровой обработки сигналов* — вариантам дискретного преобразования Фурье и др.

Для первого чтения по теории кодирования подойдёт, например, учебное пособие Л.С. Казарина [10]. Подготовленный читатель может ознакомиться с предметной областью указанных приложений по книгам [4] и [18]. Монография [8] содержит весьма подробную библиографию по цифровой обработке сигналов.

Следует обратить внимание и на ряд книг по *компьютерной алгебре*, изданных в последнее время; см., например, [1]. Особо отметим русский перевод [20] прекрасной книги П. Нодена и К. Китте, целиком посвящённой *алгебраической алгоритмике* (с многочисленными упражнениями и подробным списком литературы).

12.1. Бинарная операция, полугруппа и группа. Примеры

Пусть G — произвольное непустое множество. Обозначим через $G^2 = G \times G$, как обычно, *прямое, или декартово, произведение* G на себя, то есть совокупность упорядоченных пар $(a, b),\ a, b \in G$.

Определение 1. *Бинарной операцией* $*$, *заданной на* G, *называется некоторое отображение* $* : G^2 \to G$. *Запись* $c = a*b$ *означает, что* $(a, b) \mapsto c$. *Таким образом,* $c = a * b \in G$ *есть результат операции на паре элементов* $a, b \in G$.

Говорят, что эта операция определяет на G *алгебраическую структуру.* Множество G вместе с заданной на нём бинарной операцией $*$ называется *алгебраической системой* и обозначается $(G; *)$.

В случае, когда G конечно, алгебраическая система называется *конечной,* а число $|G|$ — её *порядком.* Здесь и далее $|G|$ обозначает число элементов конечного множества G.

Если $|G| = n$, то $G = \{a_1, a_2, \ldots, a_n\}, a_i \neq a_j$. В этой ситуации действие операции $*$ на G может быть описано квадратной таблицей из n^2 клеток, содержащей все возможные результаты операции на упорядоченных парах элементов G. Результат операции $a_i * a_j$ записывается на пересечение i-й строки и j-го столбца. Такая таблица называется *таблицей Кэли* — по имени одного из основоположников абстрактной теории групп англичанина Артура Кэли (A. Cayley).

Пусть $(G; *)$ — некоторая алгебраическая система. В дальнейшем обсуждаются следующие условия, не все из которых обязательно выполнены одновременно.

$$1^\circ. \quad (a * b) * c = a * (b * c).$$

$$2^\circ. \quad \exists e \in G \ : \quad a * e = e * a = a.$$
$$3^\circ. \quad \exists \hat{a} \in G \ : \quad a * \hat{a} = \hat{a} * a = e.$$
$$4^\circ. \quad a * b = b * a.$$

В $1^\circ - 4^\circ$ a, b, c — произвольные элементы G. Операция, для которой выполнено 1°, называется *ассоциативной.* Если же имеет место 4°, то $*$ называется *коммутативной.*

Отметим сразу, что эти важные свойства операции в общей ситуации никак не связаны. Например, умножение матриц порядка n ассоциативно, но не коммутативно. В то же время бинарная операция на R, определённая равенством $x * y := x^2 y^2$, очевидно, коммутативна, но ассоциативной не является.

Элемент e из 2° называется *нейтральным.* Условие 3° означает существование для произвольного элемента a *обратного к нему* $\hat{a}$.

Определение 2. *Алгебраическая система* $(G; *)$, *для которой выполняется* 1°, *называется полугруппой. Система, для которой имеют место условия* $1^\circ - -2^\circ$, *называется полугруппой с нейтральным элементом, или моноидом. Наконец, алгебраическая система* $(G; *)$, *для которой выполняются условия* $1^\circ - 3^\circ$, *называется группой. Если же дополнительно выполняется* 4°, *то группа называется коммутативной, или абелевой.*

Итак, группой называется непустое множество G с заданной на нём бинарной ассоциативной операцией, такое, что в G существует нейтральный элемент и для каждого элемента G существует обратный. В случае же, когда рассматриваемая операция является коммутативной, группа G называется коммутативной (абелевой).

Последний термин хранит память о норвежском математике Нильсе Хенрике Абеле (N.H. Abel).

Отметим сначала простейшие свойства группы $(G; *)$.

1). Значение выражения $a_1 * a_2 * \ldots * a_n$ не зависит от способа расстановки скобок, обозначающих порядок выполнения операций.

2). Нейтральный элемент e является единственным.

3). Для каждого $a \in G$ обратный $\hat{a}$ является единственным.

4). $\hat{\hat{a}} = a, \quad \hat{e} = e.$

5). В G однозначно разрешимо каждое из уравнений $a * x = b, \ \ x * a = b.$

6). Обратный к $a * b$ есть $\hat{b} * \hat{a}$.

Доказательство свойств. 1). Получается из ассоциативности 1° индукцией по n. Подробное обоснование предлагается читателю.

2). Сразу следует из элегантного равенства $e_1 = e_1 * e_2 = e_2$ для *двух* нейтральных элементов.

3). Пусть для некоторого $a \in G$ существуют *два* обратных b и c. Для них $a * b = = a * c$. Тогда $\hat{a}(a * b) = \hat{a}(a * c)$, откуда $b = c$.

4). Получается из условий $2^\circ - 3^\circ$.

5) Единственность решений получается из свойства 3). Если $a * x = b$, то, очевидно, $x = \hat{a} * b$. Если же $x * a = b$, то $x = b * \hat{a}$.

6). Следует из равенств $(\hat{b} * \hat{a}) * (a * b) = (a * b) * (\hat{b} * \hat{a}) = e$ с учётом первого свойства и аксиом группы.

Предложенные выше обозначения и названия часто заменяются на более привычные. Так, в частности, обстоит дело для аддитивных и мультипликативных групп. Остановимся подробнее на этой терминологии.

В *аддитивной группе* бинарная операция $*$ называется *сложением* и обозначается знаком $+$ (но это не всегда обычное сложение чисел). Нейтральный элемент называется *нулевым, или нулём,* и обозначается 0 (это не обязательно число). Элемент $\hat{a}$ называется *противоположным* и имеет обозначение $-a$. Кроме того, для $a \in G$ и $n \in N$ полагают

$$na := \underbrace{a + \ldots + a}_{n}.$$

В *мультипликативной группе* операция называется *умножением* и обозначается точкой. Результат умножения чаще записывают в виде ab и называют *произведением* (но это не всегда обычное числовое произведение). Нейтральный элемент называется *единичным, или единицей,* и часто обозначается 1 (это не обязательно число). За элементом $\hat{a}$ сохраняется название *обратного*; в этой ситуации он обозначается a^{-1}. Каждый элемент группы является *обратимым.* Для $a \in G$ и $n \in N$ полагают

$$a^n := \underbrace{a \cdot \ldots \cdot a}_{n}. \tag{1}$$

В дальнейшем в этом и следующем пунктах мы будем придерживаться терминологии мультипликативных групп, сохранив за единичным элементом обозначение e. Итак, группа $(G; \cdot)$ определяется одновременным выполнением условий:

$$1^\circ. \qquad (ab)c = a(bc).$$

$$2^\circ. \qquad \exists e \in G \ : \quad ae = ea = a.$$

$$3^\circ. \qquad \exists a^{-1} \ : \quad aa^{-1} = a^{-1}a = e.$$

Для коммутативной G дополнительно $ab = ba$.

Упражнение 1. Записать аксиомы группы в терминологии аддитивных групп. Сформулировать двумя способами свойства 1) – 6).

Пусть $a \in G$ и $n \in \mathrm{N}$. Положим

$$a^0 := e, \qquad a^{-n} := (a^n)^{-1}. \tag{2}$$

Можно принять $a^{-n} := (a^{-1})^n$. Действительно, $(a^{-1})^n a^n = e$, поэтому $(a^n)^{-1} = (a^{-1})^n$.

Равенства (1) – (2) определяют степень с произвольным целым показателем.

Упражнение 2. Показать, что в группе G при всех $k, m \in \mathrm{Z}$

$$a^{m+k} = a^m a^k, \qquad (a^m)^k = a^{mk}.$$

Прежде чем перейти к примерам, дадим ещё два определения.

Определение 3. *Пусть при некотором $k \in \mathrm{N}$ для $a \in G$ выполняется $a^k = e$. Минимальное натуральное n, для которого $a^n = e$, называется порядком элемента a. В случае $a^k \neq e,\ k \in \mathrm{N}$, говорят, что a имеет бесконечный порядок.*

Группа G, каждый элемент которой имеет конечный порядок, называется *периодической.* Группа, в которой каждый элемент имеет бесконечный порядок, называется *группой без кручения.*

Определение 4. *Две группы $(G;\cdot)$ и $(G';\circ)$ называются изоморфными, если существует такое биективное отображение $\varphi : G \to G'$, для которого*

$$\varphi(ab) = \varphi(a) \circ \varphi(b), \qquad a, b \in G.$$

Биекция φ с этим свойством называется изоморфизмом. Для изоморфных групп используется запись $G \simeq G'$.

Упражнение 3. Доказать, что изоморфизм $\varphi : G \to G'$ обладает свойствами $\varphi(e) = e',\ \varphi(a^{-1}) = (\varphi(a))^{-1}$.

Здесь $a \in G$; e' — единица G'. Правая часть второго равенства содержит обращение в G'.

Упражнение 4. Показать, что две конечные группы G и G' изоморфны тогда и только тогда, когда одновременно $|G| = |G'|$ и эти группы имеют изоморфные таблицы Кэли.

Последнее условие означает, что таблицы Кэли для G и G' могут быть получены одна из другой перестановкой строк и столбцов. Мы считаем, что клетки таблиц содержат лишь номера элементов.

Упражнение 5. Показать, что таблица Кэли для конечной группы G в каждом из случаев $|G| = 1, 2, 3$ заполняется единственным способом (с точностью до выбора порядка элементов).

Таким образом, для каждого $k = 1, 2, 3$ существует единственная с точностью до изоморфизма группа порядка k.

Упражнение 6. Существует ли некоммутативная группа порядка 2? порядка 3?

Для фиксированного $n \in \mathrm{N}$ далее используются обозначения

$$\mathrm{nZ} := \{a = nk :\ k \in \mathrm{Z}\}, \qquad \mathrm{Z_n} := \{0, 1, 2, \ldots, n-1\}.$$

Таким образом, nZ есть множество целых чисел, кратных n. Например, 2Z — множество чётных чисел. $\mathrm{Z_n}$ есть совокупность всех возможных остатков (вычетов) по модулю n; ясно, что $|\mathrm{Z_n}| = n$.

Запись $m \equiv k \pmod n$ означает, что $m - k$ делится нацело на n.

П р и м е р ы

1. Каждая из числовых систем $(\mathrm{Z};+)$, $(\mathrm{nZ};+)$, $(\mathrm{Q};+)$, $(\mathrm{R};+)$, $(;+)$, очевидно, является группой относительно обычного сложения (то есть аддитивной группой).

2. Множество Z не является группой относительно обычного умножения (нет обратимости). Очевидно, $(\mathrm{Z};\cdot)$ — полугруппа с единицей, или моноид. Пример полугруппы без единицы даёт система $(2\mathrm{Z};\cdot)$.

3. Не являются группами относительно умножения совокупности *всех* рациональных, действительных или комплексных чисел. В каждой из них имеется необратимый элемент — число 0. Однако каждая из систем $\bigl(\mathrm{Q}\setminus\{0\};\cdot\bigr)$, $\bigl(\mathrm{R}\setminus\{0\};\cdot\bigr)$, $\bigl(\mathrm{C}\setminus\{0\};\cdot\bigr)$ является (мультипликативной) группой.

Заметим, что $\bigl(\{-1,1\};\cdot\bigr)$ — группа порядка 2.

4. Мультипликативная группа $(\mathrm{R}_+;\cdot)$ положительных действительных чисел изоморфна аддитивной группе $(\mathrm{R};+)$. Изоморфизм $\varphi:\mathrm{R}_+\to\mathrm{R}$ устанавливается равенством $\varphi(x):=\ln x$. Указанные в определении 4 условия изоморфизма обеспечиваются биективностью функции $\ln x$ и свойством $\ln xy=\ln x+\ln y$, $x,y>0$.

5. *Существуют конечные группы любого натурального порядка.*

Пусть $n\in\mathrm{N}$; $\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{n-1}$ — совокупность всех комплексных корней из 1 степени n :

$$\varepsilon_k:=\cos\frac{2k\pi}{n}+\mathbf{i}\sin\frac{2k\pi}{n},\qquad k=0,1,\ldots,n-1.$$

$G=\{\varepsilon_0,\ldots,\varepsilon_{n-1}\}$ есть мультипликативная группа порядка n с единицей $\varepsilon_0=1$. Случай $n=1$ соответствует $G=\{1\}$; при $n=2\quad G=\{-1,1\}$. Если $n>2$, группа G содержит не только действительные числа.

При более внимательном подходе замечаем, что $\varepsilon_k\varepsilon_l=\varepsilon_m$, где m таково, что $k+l\equiv m\pmod n$. Возникает возможность сопоставить совокупности G множество $\mathrm{Z_n}$ с операцией $\oplus$ сложения по модулю n. Для $k,l\in\mathrm{Z_n}$ полагаем $k\oplus l:=m$. Очевидно, $(\mathrm{Z_n};\oplus)$ также является группой порядка n.

Введём отображение $\varphi:G\to\mathrm{Z_n}$ равенством $\varphi(\varepsilon_k):=k$. Сказанное означает, что биекция φ обладает свойством

$$\varphi(\varepsilon_k\varepsilon_l)=\varphi(\varepsilon_k)\oplus\varphi(\varepsilon_l)$$

— обе части равны m. Таким образом, φ является изоморфизмом и $G\simeq\mathrm{Z_n}$.

6. *Группа движений квадрата.* Пусть $ABCD$ — фиксированный квадрат плоскости. Рассмотрим совокупность G всех движений плоскости, отображающих квадрат в себя. (Под *движением* понимается взаимно-однозначное преобразование плоскости, сохраняющее расстояние между точками.) В данном случае G имеет вид

$$G=\{e,\ p_1,\ p_2,\ p_3,\ s_1,\ s_2,\ s_3,\ s_4\}.$$

Здесь p_i — поворот вокруг центра квадрата на угол $i\pi/2$; s_j — симметрия относительно одной из четырёх осей квадрата; e — тождественное преобразование. Введём операцию $x\circ y$, состоящую в выполнении движений y и x последовательно. Система $(G;\circ)$ является группой порядка 8. Детали предоставляются читателю.

Обратите внимание на значительное многообразие примеров, построенных по такой схеме.

7. Пусть L — действительное или комплексное линейное пространство, см. пункт 5.1. Тогда $(L;+)$ есть коммутативная группа.

Попутно заметим, что умножение на число является бинарной операцией лишь в ситуации $L=\mathrm{R}$ или C (почему?).

8. Совокупность M_n действительных матриц порядка n относительно умножения матриц является полугруппой с единицей (это единичная матрица), но не является группой. Однако совокупность $\tilde{M}_n$ всех *невырожденных* матриц порядка n образует группу.

Интересно заметить, что группа $(\tilde{M}_n; \times)$, в отличие от предыдущих примеров, *не является коммутативной*. Эти простые заключения следуют из результатов разделов 2 и 4.

9. Пусть X — произвольное непустое множество. Обозначим через $B(X)$ совокупность всех биекций $f : X \to X$. Введём на $B(X)$ бинарную операцию *суперпозиции, или произведения отображений,* положив $f \circ g(x) := f(g(x)), x \in X$.

Алгебраическая система $\Big(B(X); \circ\Big)$ является группой, вообще говоря, некоммутативной. Единичный элемент есть тождественное отображение $e : X \to X$, определённое равенством $e(x) := x, x \in X$. Эта группа является конечной лишь для конечного X. Если $|X| = n$, то $|B(X)| = n!$.

Читателю предлагается убедиться в справедливости этих положений.

10. Конкретизируем последний пример, выбрав $X := \{1, 2, \ldots, n\}$. Группа $B(X)$ предыдущего примера обозначается в этом случае S_n и называется *группой подстановок.* Эта группа возникает, например, при введении определителя порядка n прямым методом, см. пункт 4.1.

Элемент α из S_n, называемый подстановкой порядка n, есть взаимно-однозначное отображение множества X на себя. Подстановка α изображается в виде таблицы

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}.$$

Считаем, что $j \mapsto \alpha_j$, или $\alpha_j := \alpha(j)$.

Группы S_1, S_2 являются коммутативными. Начиная с $n = 3$, группа $(S_n; \circ)$ не является коммутативной. Например, для

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

имеем:

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Замечание. Фундаментальную роль S_n в теории конечных групп иллюстрирует следующая *теорема Кэли. Любая конечная группа порядка n изоморфна некоторой подгруппе группы S_n.* Доказательство см., например, в [13]. Определение подгруппы даётся чуть ниже в пункте 12.2.

Упражнение 7. Применить к группам примеров 1 – 10 терминологию определения 3.

12.2. Подгруппа. Теорема Лагранжа. Факторгруппа

Пусть $(G;\cdot)$ — некоторая группа. В этом пункте мы считаем групповую операцию фиксированной и помечаем группу одним символом G.

Определение 1. *Подгруппой называется такое непустое подмножество $A \subset G$, для которого выполнены условия:*

$$1^\circ. \qquad a, b \in A \implies ab \in A.$$

$$2^\circ. \qquad a \in A \implies a^{-1} \in A.$$

Из 1° – 2° следует, что $e \in A$. Таким образом, подгруппа — это такое подмножество $A \subset G$, которое является группой относительно той же операции. То, что A — подгруппа G, будем записывать в виде $A \prec G$.

Примеры. 1. Множество $\{e\}$ и вся группа G — тривиальные примеры подгрупп. Эти подгруппы называются *несобственными.*

2. *Пересечение любого числа подгрупп также является подгруппой.*

Этот простой результат, обоснование которого предоставляется читателю, может использоваться в различных ситуациях. Так, $2\mathrm{Z}$ и $3\mathrm{Z}$ — подгруппы $(\mathrm{Z};+)$. Поэтому их пересечение $6\mathrm{Z} = 2\mathrm{Z} \bigcap 3\mathrm{Z}$ также является подгруппой Z. Впрочем, последний факт очевиден непосредственно.

3. Совокупность матриц порядка n, определитель которых равен ± 1, есть подгруппа в группе всех невырожденных матриц порядка n (операция — умножение матриц).

Пусть G — произвольная группа, $a \in G$. Обозначим через $\langle a \rangle$ совокупность всех степеней a :

$$\langle a \rangle := \{a^m \ : \ m \in \mathrm{Z}\}.$$

Из свойств степеней следует, что $\langle a \rangle$ — подгруппа G. В случае $a \neq e$ эта подгруппа не совпадает с $\{e\}$, но может совпадать со всей G.

Определение 2. *Множество $\langle a \rangle$ называется циклической подгруппой, порождённой элементом a. Группа G, совпадающая с одной из своих циклических подгрупп, называется циклической.*

Если a — элемент порядка n, то, очевидно, $|\langle a \rangle| = n$. В этом случае

$$\langle a \rangle = \{e = a^0, a^1, \ldots, a^{n-1}\}. \tag{3}$$

Дело в том, что $a^n = e, a^{n+1} = a, \ldots, a^{2n} = e, \ldots$ Отрицательные степени равны $a^{-1} = a^{n-1}, a^{-2} = a^{n-2}, \ldots, a^{-n} = e$, и т.д..

Наоборот, если $|\langle a \rangle| = n$, то выполнено равенство (3). Каждая из степеней $a^0, a^1, \ldots, a^{n-1}$ принадлежит $\langle a \rangle$ и все они попарно различны (иначе порядок этой подгруппы меньше n). В то же время они исчерпывают совокупность вообще всех степеней (иначе порядок $\langle a \rangle$ больше n.) Равенство (3) гарантирует, что $|a| = n$. Действительно, если $a^n = a^k, 0 < k < n$, то $a^{n-k} = a^0 = e$, что невозможно.

Итак, для элементов a конечного порядка $|\langle a \rangle| = |a|$. Для элементов бесконечного порядка (и только в этом случае) подгруппа $\langle a \rangle$ бесконечна.

Упражнение 1. Пусть $|G| = n$. Элемент $a \in G$ порядка n называется первообразным, или примитивным. Показать, что a является первообразным тогда и только тогда, когда $G = \{e, a, \ldots, a^{n-1}\}$.

Пусть $A \prec G$, x — фиксированный элемент G. Множества

$$xA := \{xa : a \in A\}, \qquad Ax := \{ax : a \in A\}$$

называются соответственно *левым и правым классом смежности по подгруппе* A.

Отметим некоторые свойства левых классов смежности; их аналоги верны и для правых классов.

Так как $e \in A$, то всегда $x \in xA$. Ясно, что $eA = A$.

Теорема 1. *Два класса смежности* xA *и* yA *либо совпадают, либо не пересекаются. При этом* $yA = xA$ *тогда и только тогда, когда* $y \in xA$.

Доказательство. Покажем сначала, что если $y \in xA$, то $yA = xA$. Действительно, $y = xa_0, a_0 \in A$. Поэтому $x = ya_0{}^{-1}$. Это даёт

$$xA = (ya_0{}^{-1})A \subset yA = (xa_0)A \subset xA.$$

Поэтому, если $z \in xA$ и $z \in yA$, то $zA = xA$, $zA = yA$. Значит, $yA = xA$.

Пусть теперь $yA = xA$. Тогда $ye = y \in xA$, так как $e \in A$.

Теорема доказана.

Замечание. Взяв в условии теоремы $x = e$, получим, что $yA = A$ лишь в случае $\in A$.

Из теоремы 1 вытекает ряд важных утверждений.

Следствие 1. *Группа* G *может быть представлена в виде объединения непересекающихся (левых) классов смежности по подгруппе* A.

Пример 4. Рассмотрим группу $G = \mathrm{Z}$ относительно сложения. В этом случае естественно использовать запись $x + A$ вместо xA, и т.д. Возьмём

$$A = 3\mathrm{Z} = \{3z : z \in \mathrm{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}.$$

Пусть $x_0, x_1, x_2 \in \mathrm{Z}$ таковы, что $x_j \equiv j \pmod 3$. Например, можно взять $x_0 = 0, x_1 = 1, x_2 = 2$. (Это не единственный вариант — подойдёт, скажем, и набор $x_0 = 24, x_1 = -5, x_2 = 5$.) Тогда $x_0 + A = A = \{3z\}$, $x_1 + A = \{1 + 3z : z \in \mathrm{Z}\}$, $x_2 + A = \{2 + 3z : z \in \mathrm{Z}\}$. Представление (или разложение) следствия 1 имеет вид

$$\mathrm{Z} = (0 + A) \bigcup (1 + A) \bigcup (2 + A) = \{3z\} \bigcup \{1 + 3z\} \bigcup \{2 + 3z\}.$$

Заметим, что другой выбор x_j с условиями $x_j \equiv j \pmod 3$ приводит к тому же разложению Z. Например, $24 + A = 0 + A = A = \{3z\}$, $-5 + A = 1 + A = \{1 + 3z\}$, $5 + A = 2 + A = \{2 + 3z\}$, и т.д..

Упражнение 2. Как выглядит представление следствия 1 в ситуациях $A = \{e\}$ *и* $A = G$?

Упражнение 3. Найти класс смежности xA *по подгруппе* $A \prec G$ *в следующих вариантах.*

(*a*) $G = \mathrm{R} \setminus \{0\}$ относительно умножения, $A = \{a : a > 0\}$, $x = -7$;

(*b*) $G = \mathrm{R} \setminus \{0\}$ относительно умножения, $A = \{-1, 1\}$, $x = 5$;

(*c*) $G = \mathrm{Z}$ относительно сложения, $A = 6\mathrm{Z}$, $x = -7$;

(*d*) G — совокупность невырожденных матриц второго порядка, A — совокупность матриц с определителем 1, $x = \begin{pmatrix} 1 & 2 \\ 2 & 6 \end{pmatrix}$;

(*e*) G и x те же, что и в (*d*), $A = \{\lambda \mathbf{E} : \lambda > 0\}$;

(*f*) G — группа подстановок S_4, $A := \{\alpha \in S_4 : \alpha(1) = 1\}$, $x(1) = 2$, $x(2) = 3$, $x(3) = 4$, $x(4) = 1$.

Число различных классов смежности xA по подгруппе A называется *индексом подгруппы* A и обозначается $j(A)$.

Так, в последнем примере $j(A) = 3$.

Следствие 2 (теорема Лагранжа). *Во всякой конечной группе порядок любой подгруппы есть делитель порядка группы. В частности, если $|G| = p$ — простое, то в G есть лишь тривиальные подгруппы.*

Доказательство. Для любого $x \in G$ класс смежности xA содержит столько же элементов, сколько A. Действительно, равенство $xa_1 = xa_2$ эквивалентно $a_1 = a_2$, поэтому при умножении x на различные $a \in A$ получаются различные элементы xA.

Итак, $|xA| = |A|$. Применяя следствие 1, в силу конечности G получаем

$$|G| = j(A)|A|.$$

Отсюда следует, что оба числа $|A|$ и $j(A)$ есть делители $|G|$. Следствие 2 доказано.

Теорема Лагранжа имеет многочисленные приложения. Одно из них (так называемая *малая теорема Ферма*) отмечается в пункте 12.4.

Следствие 3. *В конечной группе порядок любого элемента есть делитель порядка группы.*

Достаточно вспомнить, что $|a| = |\langle a \rangle|, a \in G$, и применить следствие 1 к циклической подгруппе $\langle a \rangle$.

Следствие 4. *Всякая конечная группа, порядок которой есть простое число, является циклической.*

Действительно, такая группа G должна совпадать с подгруппой $\langle a \rangle, a \in G$, $a \neq e$.

Упражнение 4. Показать, что для любого простого p существует единственная с точностью до изоморфизма конечная группа порядка p.

Ясно, что для коммутативных групп $xA = Ax$. В общей ситуации это может не выполняться. Подгруппа A, для которой $xA = Ax$ при всех $x \in G$, называется *нормальным делителем* G. На протяжении оставшейся части этого пункта мы рассматриваем лишь такие подгруппы.

Зафиксируем нормальный делитель $A \prec G$. Обозначим через G/A совокупность всех классов смежности xA. На множестве G/A зададим бинарную операцию $\circ$, положив

$$(xA) \circ (yA) := (xy)A.$$

Это равенство означает, что произведением классов xA и yA считается тот класс смежности, который содержит элемент xy.

Важно отметить, что результат операции не зависит от выбора элементов $x \in xA$, $y \in yA$ (как говорят, *представителей* этих классов).

Действительно, пусть есть ещё $x_1 \in xA$, $y_1 \in yA$. В этом случае $x_1 = xa$, $y_1 = yb$; $a, b \in A$. Тогда

$$x_1 y_1 = xayb = x(ay)b = x(ya_1)b = (xy)(ab) \in (xy)A.$$

Мы использовали здесь, что $ay = ya_1$ для некоторого $a_1 \in A$. Это связано с тем, что A — нормальный делитель, для неё $Ay = yA$. Итак, мы получили, что $x_1 y_1 \in (xy)A$. По теореме 1 $(x_1 y_1)A = (xy)A$.

Определение 3. *Пусть A — нормальный делитель G. Алгебраическая система $\Big(G/A; \circ\Big)$ называется факторгруппой группы G по подгруппе A.*

Имеет место следующее утверждение, поясняющее выбор термина *факторгруппа*.

Теорема 2. *Факторгруппа $\Big(G/A; \circ\Big)$ является группой.*

Доказательство. Ассоциативность $\circ$ следует из ассоциативности умножения в G. Действительно,

$$(xA \circ yA) \circ zA = (xy)A \circ zA = (xy)zA = x(yz)A = xA \circ (yz)A.$$

Нейтральным элементом (единицей) G/A является подгруппа A, являющаяся одним из классов смежности: $A \in G/A$, так как $A = eA$. Имея в виду то же равенство, получаем

$$xA \circ A = xA \circ eA = (xe)A = xA, \;\; A \circ xA = eA \circ xA = (ex)A = xA.$$

Наконец, обратным для xA является $x^{-1}A$:

$$xA \circ x^{-1}A = (xx^{-1})A = eA = A.$$

Аналогично,

$$x^{-1}A \circ xA = (x^{-1}x)A = eA = A.$$

Теорема доказана.

Пример 5. Зафиксируем целое $n > 1$. Подгруппа $A = \mathrm{nZ}$ является нормальным делителем аддитивной группы Z (см. пример 4 для $n = 3$). Классы смежности имеют вид

$$A_0 = A = \{nz\}, A_1 = \{1 + nz\}, \ldots, A_n = \{n - 1 + nz\}.$$

В этой записи $z \in \mathrm{Z}$. Таким образом, A_j есть совокупность целых чисел, дающих при делении на n остаток j, $\quad j = 0, 1, \ldots, n-1$. Порядок факторгруппы $\mathrm{Z/nZ}$ равен n. Действия с элементами этой факторгруппы, то есть классами A_j, как нетрудно понять, осуществляются по правилу:

$$A_i \circ A_j := A_m, \qquad i \oplus j = m.$$

Здесь $\oplus$ обозначает сложение по модулю n, заданное на множестве

$$\mathrm{Z_n} := \{0, 1, \ldots, n - 1\}.$$

Тем самым, факторгруппа $\left(\mathrm{Z}/\mathrm{nZ};\circ\right)$ изоморфна группе $(\mathrm{Z_n};\oplus)$:

$$\mathrm{Z}/\mathrm{nZ}\simeq\mathrm{Z_n}.$$

Изоморфизм $\varphi:\mathrm{Z}/\mathrm{nZ}\to\mathrm{Z_n}$ устанавливается простой формулой $\varphi(A_j):=j,\quad j==0,1,\ldots,n-1$.

Упражнение 5. Показать, что в случае $A=\{e\}$ имеет место изоморфизм $G/A\simeq G$, а в случае $A=G$ — изоморфизм $G/A\simeq\{e\}$.

Упражнение 6. Показать, что если G — коммутативная, то и G/A коммутативная. Если G — циклическая, то и G/A циклическая.

Упражнение 7. Пусть G — конечная группа. Почему $|G|$ делится нацело на $|G/A|$?

12.3. Кольцо. Определение, свойства и примеры. Кольцо вычетов

Кольцо и поле — это алгебраические системы *с двумя бинарными операциями,* называемыми сложением и умножением. Разумеется, это не всегда обычные числовые сложение и умножение, но могут таковыми быть.

Для нас особый интерес представляют некоторые свойства этих систем, которые не проявляются в их важнейших реализациях (кольцо целых и поле действительных чисел и др.). Вместе с тем мы выделяем общие черты вообще всех колец и полей.

Определение 1. *Кольцом $(R;+,\cdot)$ называется алгебраическая система с двумя бинарными операциями — сложением и умножением, обладающая свойствами:*

$$1^\circ.\quad (R;+)\ -\ \textit{коммутативная группа ;}$$
$$2^\circ.\quad (a+b)c=ac+bc,\quad a(b+c)=ab+ac.$$

Здесь a,b,c — произвольные элементы R. Условие 2° выражает *дистрибутивность* умножения относительно сложения.

Развёрнутое определение содержит расшифровку термина *алгебраическая система с двумя бинарными операциями*, а также подробную запись аксиом аддитивной группы кольца, и является весьма пространным. Мы предоставляем читателю дать такое определение в качестве упражнения.

Нейтральные элементы относительно сложения и умножения обозначаются соответственно через 0 и 1. Это вовсе не обязательно числа, хотя могут и быть таковыми.

Условие $1\in R$ в определение кольца не входит. От сложения в общем определении кольца требуется гораздо больше, чем от умножения. Поэтому дальнейшие уточнения и термины касаются мультипликативной структуры кольца, то есть описания свойств системы $(R;\cdot)$.

Определение 2. *Ассоциативным (коммутативным) кольцом называется кольцо $(R;+,\cdot)$, в котором умножение является ассоциативным (соответственно*

коммутативным). Кольцо с единицей, или унитарное, — это кольцо R, для которого $1 \in R$.

Упражнение 1. Записать все аксиомы ассоциативного коммутативного кольца с единицей, разделив их на две группы. Какое условие на систему $(R;+)$ не имеет аналога в группе аксиом умножения?

Отметим важнейшие свойства кольца $(R;+,\cdot)$, связывающие его аддитивную и мультипликативную системы. Ниже a, b — произвольные элементы R.

1). $a \cdot 0 = 0 \cdot a = 0$.

2). Пусть R — кольцо с единицей, содержащее более одного элемента. Тогда $1 \neq 0$.

3). $(-a)b = a(-b) = -(ab)$.

4). $(ka)b = k(ab) = a(kb), \quad k \in \mathrm{Z}$.

5). Для $a_i, b_j \in R,\ m, n \in \mathrm{N}$

$$(\sum_{i=1}^{m} a_i)(\sum_{j=1}^{n} b_j) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j.$$

6). Пусть R — коммутативное кольцо. Тогда

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Доказательство свойств. 1). Так как $a + 0 = a$, то $a^2 = a(a+0) = a^2 + a \cdot 0$. Поэтому $a \cdot 0 = 0$. Аналогично $0 \cdot a = 0$.

2). Так как R содержит более одного элемента, то найдётся $a \neq 0$. Предположим, что $0 = 1$. Для этого $a \neq 0$ в соответствии с предыдущим свойством $0 = a \cdot 0 = a \cdot \cdot 1 = a$. Противоречие.

3). $ab + (-a)b = (a + (-a))b = 0 \cdot b = 0$. Аналогично $ab + a(-b) = 0$. Мы использовали первое свойство.

4). Для $k \in \mathrm{N}$ следует из дистрибутивности индукцией по k. Применим это двойное соотношение с $k > 0$ к элементам $-a, b$ и проанализируем первое равенство $(k(-a))b = k((-a)b)$.

Так как $k(-a) = (-k)a$, то слева стоит $((-k)a)b$. Далее, $(-a)b = -ab$, в связи с чем правая часть есть $k((-a)b) = k(-ab) = (-k)(ab)$. Поэтому исследуемое равенство принимает вид $((-k)a)b = (-k)(ab)$.

По той же схеме получается $a((-k)b) = (-k)(ab)$. Тем самым, $((-k)a)b = (-\ -k)(ab) = a((-k)b)$, что соответствует доказываемому соотношению при $k < 0$.

В случае $k = 0$ равенство следует из первого свойства.

5). Получается из дистрибутивности индукцией по n при фиксированном m. База рассуждения — случай $n = 1$ — использует индукцию по m. Возможна и обратная схема.

6). Доказывается индукцией по n.

Упражнение 2. Восполнить пробелы в доказательстве свойств.

Упражнение 3. Верно ли, что в любом кольце $0 \neq 1$? *Сравнить со свойством 2).*

Приведём ещё одно важное определение.

Определение 3. *Элементы* $a, b \in R$, *для которых*

$$ab = 0, \qquad a \neq 0,\ b \neq 0, \tag{4}$$

называются делителями нуля. Кольцо, содержащее такие элементы, называется кольцом с делителями нуля. Наконец, целостным кольцом, или областью целостности, называется ассоциативное коммутативное кольцо с единицей, в котором нет делителей нуля.

То, что определение 3 является существенным, отмечается в примерах 2 и 6 — *кольца с делителями нуля существуют.* Свойство некоторых колец содержать элементы с условием (4) является новым и, вероятно, непривычным для неопытного читателя. Как мы увидим в дальнейшем, это свойство ряда колец является их специфическим атрибутом по сравнению с полями — любое поле не содержит делителей нуля.

Отметим, что если два кольца R_1, R_2 с одними и теми же операциями связаны включением $R_1 \subset R_2$, то R_1 называется *подкольцом* R_2, а R_2 — *расширением* R_1.

П р и м е р ы к о л е ц

1. Любая из числовых систем $(\mathrm{nZ}; +, \cdot), n > 1$ — фиксировано, $(\mathrm{Z}; +, \cdot)$, $(\mathrm{Q}; +, \cdot)$, $(\mathrm{R}; +, \cdot)$, $(; +, \cdot)$ является кольцом относительно числовых операций сложения и умножения. Каждое кольцо в этой цепочке есть расширение предыдущего. Но наиболее типичным в некотором смысле является лишь кольцо целых чисел Z — здесь это единственное *целостное кольцо, не являющееся полем.*

Уточним это высказывание. Каждое из множеств является ассоциативным коммутативным кольцом без делителей нуля. Однако, в отличие от остальных, nZ *не является кольцом с единицей* (возьмите $n = 2$). С другой стороны, кольца Q, R и C содержат обратные для своих ненулевых элементов, то есть являются *полями*, см. пункт 12.4. Совокупность же Z этим свойством не обладает.

2. Совокупность $\mathrm{R}[t]$ многочленов произвольной степени от переменного t с действительными коэффициентами — целостное кольцо относительно операций сложения и умножения многочленов (не являющееся полем).

Интересно заметить, что относительно сложения многочленов и умножения их на число $\mathrm{R}[t]$ образует другой алгебраический объект, а именно *действительное линейное пространство.*

3. Пусть $n > 1$. Система $(M_n; +, \times)$ с операциями сложения и умножения матриц есть ассоциативное, но не коммутативное кольцо с единицей (единичной матрицей). Интересно, что в отличие от примеров 1 – 2 это кольцо *содержит делители нуля.* Например, при $n = 2$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

4. Совокупность функций $f : \mathrm{R} \to \mathrm{R}$ с операциями поточечного сложения и умножения — ассоциативное коммутативное кольцо с единицей, не являющееся целостным. Делителями нуля являются, например, функции

$$f(t) := \begin{cases} 1-t & , \quad t \in [0,1] \\ 0 & , \quad t \notin [0,1] \end{cases}, \quad g(t) := \begin{cases} 0 & , \quad t \leqslant 2 \\ t-2 & , \quad t > 2 \end{cases},$$

и вообще такие $f(t) \not\equiv 0$ и $g(t) \not\equiv 0$, для которых $f(t)g(t) \equiv 0$.

Спецификация свойств функций приводит к большому многообразию примеров *функциональных колец.*

5. *Существуют конечные кольца любого натурального порядка.*

Пусть $n \in \mathrm{N}$. Обозначим через $\oplus$ и $\odot$ операции сложения и умножения положительных целых чисел по модулю n. Их результаты $a \oplus b$ и $a \odot b$ есть остатки от деления чисел $a + b$ и ab на n. Рассмотрим эти операции на множестве

$$\mathrm{Z_n} = \{0, 1, \ldots, n-1\}.$$

Теорема. *Система* $(\mathrm{Z_n}; \oplus, \odot)$ *является ассоциативным коммутативным кольцом с единицей.*

Это кольцо называется *кольцом вычетов по модулю* n.

Доказательство. Сложение и умножение по модулю n являются бинарными операциями на $\mathrm{Z_n}$. Обе они ассоциативны и коммутативны. Нейтральные элементы 0 и 1 содержатся в $\mathrm{Z_n}$. Каждый элемент $a \in \mathrm{Z_n}$ обладает противоположным — таковым является $n-a$. Действительно, $a \oplus (n-a) = (n-a) \oplus a = 0$. Остальные свойства — ассоциативность $\oplus$, ассоциативность $\odot$ и дистрибутивность — обосновываются по одной и той же схеме. Покажем, например, что всегда

$$(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c). \tag{5}$$

Пусть $a, b \in \mathrm{Z_n}$. Обозначим левую и правую части (5) через v и w. Нетрудно понять, что v отличается на целое кратное n от $(a+b)c$. (В последней записи операции обычные.) Аналогично, w отличается на целое кратное n от $ac + bc$. Но $(a + b)c = ac + bc$. Поэтому v и w отличаются друг от друга на некоторое число, кратное n. В силу того, что $v, w \in \mathrm{Z_n}$, получаем, что $v = w$. Равенство (5) установлено.

Теорема доказана.

Замечание. Кольцо $(\mathrm{Z_n}; \oplus, \odot)$ не всегда является целостным. Именно, если n — составное число, то $\mathrm{Z_n}$ содержит делители нуля. Действительно, пусть $n = st$, $1 < s, t < n$. Тогда $s \odot t = 0$.

Например, делителями нуля в $\mathrm{Z_6}$ являются 2 и 3: при умножении по модулю 6 получается $2 \odot 3 = 0$.

Упражнение 4. Построить таблицы Кэли для операций в кольцах $\mathrm{Z_4}$ *и* $\mathrm{Z_5}$. *Постарайтесь найти особенность таблицы для* $\odot$ *в* $\mathrm{Z_5}$ *по сравнению с* $\mathrm{Z_4}$.

Упражнение 5. Пусть $\mathrm{Z}[\sqrt{-5}]$ — *подмножество* C, *определяемое равенством* $\mathrm{Z}[\sqrt{-5}] := \{a + b\sqrt{5}\mathbf{i},\ a, b \in \mathrm{Z}\}$. *Это наименьшее множество, содержащее суммы и произведения всех чисел вида* $a\sqrt{5}\mathbf{i},\ a \in \mathrm{Z}$.

Квалифицировать систему $\left(\mathrm{Z}[\sqrt{-5}]; +, \cdot\right)$.

12.4. Поле. Определение, свойства и примеры. Поле вычетов. Другие конечные поля

Резюме этого пункта — *каждое поле является кольцом, но далеко не каждое кольцо является полем.* Это означает, что аксиомы поля существенно дополняют аксиомы кольца.

Определение 1. *Полем называется алгебраическая система* $(F;+,\cdot)$ *с двумя бинарными операциями, обладающая свойствами:*

1°. $(F;+)$ — *коммутативная группа .*

2°. $\big(F\setminus\{0\};\cdot\big)$ — *коммутативная группа .*

3°. $(a+b)c=ac+bc$.

Группы $(F;+)$ и $\big(F\setminus\{0\};+\big)$ называются соответственно *аддитивной и мультипликативной группами поля* F. Для сокращения записи часто используют обозначение $F^*:=F\setminus\{0\}$.

Приведём развёрнутый список аксиом поля. Мы учитываем коммутативность операций, поэтому, например, вместо $a\cdot 1=1\cdot a=a$ пишем лишь $a\cdot 1=a$.

1° $(a+b)+c=a+(b+c)$;

$\exists 0\in F\ :\quad a+0=a$;

$\exists(-a):\quad a+(-a)=0$;

$a+b=b+a$.

2°. $(ab)c=a(bc)$;

$\exists 1\in F\ :\quad a\cdot 1=a$;

$a\neq 0\implies \exists a^{-1}\ :\quad aa^{-1}=1$;

$ab=ba$.

3°. $(a+b)c=ac+bc$.

Так как каждое поле является кольцом, то для полей справедливы все свойства колец из предыдущего пункта. Отметим здесь специфические свойства поля, которые, вообще говоря, не относятся к произвольному кольцу.

1). В поле определено не только *вычитание* (действие, обратное сложению), но и *деление на* $a\neq 0$ (действие, обратное умножению). Именно, если $ax=b, a\neq 0$, то $x=a^{-1}b$.

2). В поле определены степени a^m, m — отрицательное целое, для любого $a\neq 0$.

3). Поле не имеет делителей нуля.

Все свойства очевидны. Установим, например, важное третье свойство. Если $ab=0$ и $a\neq 0$, то $b=a^{-1}\cdot 0=0$.

Замечание 1. Пусть $(F;+,\cdot)$ — поле, и для некоторого $k \in N$ выполнено

$$k1 = \underbrace{1+\ldots+1}_{k} = 0. \tag{6}$$

Минимальное k, удовлетворяющее (6), называется *характеристикой поля* F. Если же все натуральные кратные элемента 1 отличны от 0, то F называют *полем характеристики 0.*

Из свойства 3) получается, что если F — поле характеристики $p \neq 0$, то p — простое число. Действительно, предположение $p = st, \quad s,t < p$, даёт $0 = p1 = st1 = (s1)\cdot(t1)$. Так как F не имеет делителей нуля, то одно из кратных $s1$ или $p1$ есть 0. Это противоречит определению p.

Упражнение 1. Почему в предыдущем рассуждении $st1 = (s1)\cdot(t1)$?

Упражнение 2. Пусть F *— поле характеристики* p*. Доказать, что* $(a+b)^p = a^p + b^p$ *для любых* $a, b \in F$.

Определение 2. *Два кольца* $(R;+,\cdot)$ *и* $(R';\oplus,\odot)$ *называются изоморфными, если существует такое биективное отображение* $\varphi : R \to R'$*, для которого при всех* $a, b \in R$

$$\varphi(a+b) = \varphi(a) \oplus \varphi(b),$$
$$\varphi(ab) = \varphi(a) \odot \varphi(b).$$

Биекция φ *с этим свойством называется изоморфизмом. Для изоморфных колец используется запись* $R \simeq R'$.

Два поля называются изоморфными, если они изоморфны как кольца.

Если F_1 и F_2 — два поля с одними и теми же операциями и $F_1 \subset F_2$, то F_1 называется *подполем* F_2, а F_2 — *расширением* F_1.

П р и м е р ы п о л е й

1. Любая из систем $(\mathrm{Q};+,\cdot)$, $(\mathrm{R};+,\cdot)$, $(;+,\cdot)$, является полем относительно числовых операций сложения и умножения. Каждое поле в этой цепочке есть расширение предыдущего.

2. Рассмотрим совокупность M всех матриц вида

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

В этом примере $a, b \in \mathrm{R}$.

Система $(M;+,\times)$ с операциями сложения и умножения матриц является полем. Действительно,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}, \; x = a+c, y = b+d;$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}, \; x = ac-bd, y = ad+bc.$$

Поэтому сложение и умножение являются бинарными операциями на M. Ясно, что нуль и единица, то есть нулевая и единичная матрицы, содержатся в M. Имеют место коммутативность сложения и ассоциативность обеих операций. Коммутативность умножения в M получается из симметричного вида произведения относительно сомножителей. Если $\mathbf{A} \in M$, то, очевидно, $-\mathbf{A} \in M$. Остаётся заметить, что каждая ненулевая матрица из M обладает обратной. Действительно, если $a^2+b^2 \neq$ $= 0$, то

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in M.$$

Рассмотрим теперь поле C коплексных чисел с операциями (в алгебраической форме)

$$(a+b\mathbf{i}) + (c+d\mathbf{i}) := (a+c) + (b+d)\mathbf{i},\ (a+b\mathbf{i}) \cdot (c+d\mathbf{i}) := (ac-bd) + (ad+bc)\mathbf{i}.$$

Соответствие $\varphi : \mathrm{C} \to M$, осуществляемое по правилу

$$a+b\mathbf{i} \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

является изоморфизмом, что следует из формул для операций в C и M.

Таким образом, $\mathrm{C} \simeq M$.

3. Система $\Big(\mathrm{Q}[\sqrt{2}]; +, \cdot\Big)$ с обычным сложением и умножением является полем. Здесь

$$\mathrm{Q}[\sqrt{2}] := \mathrm{Q} + \sqrt{2}\mathrm{Q} := \{a + b\sqrt{2},\ a, b \in \mathrm{Q}\}$$

— наименьшее множество, содержащее не только числа $q\sqrt{2}, q \in \mathrm{Q}$, но и все их произведения и суммы.

Упражнение 3. Проверить аксиомы поля $\mathrm{Q}[\sqrt{2}]$. *Изоморфны ли поля* $\mathrm{Q}[\sqrt{2}]$ *и* $\mathrm{Q}[\sqrt{3}]$?

4. *Существует бесконечное семейство конечных полей.* Установим здесь следующий важный факт.

Теорема. *Кольцо вычетов* $(\mathrm{Z_n}; \oplus, \odot)$ *по модулю* $n \in \mathrm{N}$ *является полем тогда и только тогда, когда* $n = p$ *— простое.*

Доказательство. Пусть $\mathrm{Z_n}$ — поле. Допустим, n — составное, $n = st$, $1 \leqslant s, t \leqslant n-1$. Тогда $s \odot t = 0$. Но это невозможно, так как поле не имеет делителей нуля. Значит, $n = p$ — простое.

Пусть p — простое число. Докажем, что в этом случае $(\mathrm{Z_p}; \oplus, \odot)$ является полем.

Как было показано в пункте 12.3, $\mathrm{Z_p}$ — ассоциативное коммутативное кольцо с единицей. В связи с этим достаточно установить обратимость каждого ненулевого элемента $\mathrm{Z_p}$.

Заметим прежде всего, что $\mathrm{Z_p}$ не содержит делителей нуля. Действительно, в силу простоты p обычное произведение st для $s, t \in \mathrm{Z_p}$, $s, t \neq 0$, не содержит множителя p. Поэтому $s \odot t \neq 0$.

Возьмём теперь $k \in \mathrm{Z_p}, k \neq 0$. Рассмотрим набор из $p-1$ элементов

$$k \odot 1,\ k \odot 2,\ \ldots,\ k \odot (p-1). \tag{7}$$

Все они различны: если при $i > j$ выполнено $k \odot i = k \odot j$, то $k \odot (i-j) = 0$; последнее невозможно по предыдущему. Итак, элементы (7) попарно различны и

каждый отличен от 0. Так как их ровно $p-1$, то они исчерпывают множество $\{1, 2, \ldots, p-1\}$. Поэтому $k \odot l = 1$ для некоторого $l \in \mathrm{Z_p}$. Тем самым, $l = k^{-1}$ существует.

Теорема доказана.

Отметим, что $\mathrm{Z_p}$ имеет характеристику p.

Как иллюстрацию, приведём известный результат теории чисел — так называемую *малую теорему Ферма.*

Следствие. *Пусть m — целое, не делящееся на простое p. Тогда $m^{p-1} \equiv 1 \pmod{p}$.*

Доказательство. Порядок мультипликативной группы $\mathrm{Z_p}^*$ равен $p-1$. По теореме Лагранжа (пункт 12.2) порядок любого элемента из $\mathrm{Z_p}^*$ делит $p-1$. Возьмём $\bar{m} \in \mathrm{Z_p}^*$ таким, что $m \equiv \bar{m} \pmod{p}$. Тогда $\bar{m}^{p-1} \equiv 1 \pmod{p}$. Остаётся учесть, что $m^d \equiv \bar{m}^d \pmod{p}$ для любого d.

Существуют ли конечные поля, неизоморфные $\mathrm{Z_p}$? Оказывается, да. Именно, *для каждого простого p и $n \in \mathrm{N}$ существует единственное с точностью до изоморфизма поле, содержащее p^n элементов.*

Это поле называется *полем Галуа* и обозначается $GF(p^n)$ *(Galois Field).* Других конечных полей нет.

Поле $GF(p)$ изоморфно $\mathrm{Z_p}$ и, значит, может быть реализовано как поле вычетов. В случае $n > 1$ поле $GF(p^n)$ уже не допускает такой конструкции. Произвольное поле Галуа может быть некоторым образом реализовано с помощью многочленов. Здесь мы не будем подробно обсуждать этот интересный вопрос.

Упражнение 4. Является ли истинным высказывание: существуют конечные поля порядка 2, 4, 6, 9, 12, 25, 26, 27 ? Укажите причину.

Упражнение 5. Ассоциативное кольцо $(R; +, \cdot)$ с единицей $1 \neq 0$, в котором каждый $a \neq 0$ обратим, называется телом.

Привести пример тела, не являющегося полем.

Остаётся отметить, что конечные кольца и поля являются важным *прикладным* средством исследования и прекрасно иллюстрируют невозможность строгого деления математики на фундаментальную и прикладную. Из приложений отметим теорию и практику *кодирования, цифровой обработки сигналов* (например, изображений,) и вообще задачи *компьютерной алгебры* или, как теперь говорят, *алгебраической алгоритмики.*

Некоторые ссылки на соответствующую литературу даются во введении к настоящему разделу.

13. Комплексные числа

Комплексные числа — важный инструмент и язык современной математики. Их алгебраическая природа состоит в том, что поле C является *расширением* поля действительных чисел R, получающегося алгебраическим присоединением к R корня $\mathbf{i}$ многочлена $f(x) = x^2 + 1$.

Наиболее важное свойство поля C состоит в его *алгебраической замкнутости*: любой многочлен степени $n \geqslant 1$ с коэффициентами из C имеет по крайней мере один комплексный корень. Это так называемая *основная теорема алгебры (многочленов)*, называемая также *теоремой Д'Аламбера – Гаусса*. Каждое поле, содержащее подполе, изоморфное R, обязательно содержит и подполе, изоморфное C — так выглядит свойство *минимальности* C по отношению к его подполю R.

В настоящем разделе содержатся основные сведения по комплексным числам.

Комплексные числа имеют свою длительную историю. Впервые мнимые величины появились в работах итальянских математиков 16 в. Кардано, Бомбелли и др. для получения действительных корней уравнений 3 степени. Дж. Кардано (G. Cardano, 1545) счёл их непригодными к употреблению. Пользу мнимых величин при решении кубического уравнения (когда действительные корни выражаются через кубические корни из мнимых величин) впервые оценил Р. Бомбелли (R. Bombelli, 1572). Он же дал некоторые простейшие правила действий с комплексными числами. Как пример одного из самых древних, приведём *тождество Бомбелли*:

$$\sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} = 4.$$

Выражения вида $a + b\sqrt{-1}, b \neq 0$, появляющиеся при решении квадратных и кубических уравнений, стали называть *мнимыми*. Термин *imaginaire (мнимый, воображаемый)* впервые употребил Р. Декарт (R. Descartes,1637). Начиная со второй половины 17 в., математики всё более уверенно пользовались символом $\sqrt{-1}$, причём не только в алгебраических тождествах, но и в аналитических формулах для функций. К этому времени А. Де Муавром (A. de Moivre, 1707, 1724) и Р. Котесом (R. Cotes, 1722) была решена задача извлечения корня n-й степени из комплексного числа. Формулы для умножения в тригонометрической форме и извлечения корня с тех пор называют *формулами Муавра* (чаще это название относится к первой из них). В 1748 г. Л. Эйлер (L. Euler) вывел свою знаменитую формулу

$$e^{\mathbf{i}\varphi} = \cos\varphi + \mathbf{i}\sin\varphi,$$

носящую теперь его имя. Это тождество лежит в основе перехода к так называемой *показательной форме комплексного числа* $z = re^{\mathbf{i}\varphi}$. В случае $\varphi = \pi$ получаем знаменитое равенство $e^{\mathbf{i}\pi} = -1$, в котором заняты пять замечательных символов $0, 1, e, \pi, \mathbf{i}$ (так как $-1 = 0 - 1$). Эйлер же предложил использовать $\mathbf{i}$ вместо $\sqrt{-1}$ (1771).

Первые мемуары о геометрическом представлении комплексных чисел принадлежат К. Весселю (1797) и Р. Аргану (1806). Второй из них ввёл в употребление

термин *модуль*; современное обозначение $|z|$ предложил позднее К. Вейерштрасс (K. Weirstraass). Название *комплексное число* впервые встречается у К. Гаусса (C. Gauss, 1831).

Чисто арифметическая теория комплексных чисел как пар действительных чисел была построена У. Гамильтоном (W. Hamilton, 1837). Ему же принадлежит обобщение комплексных чисел — *кватернионы Гамильтона* $q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, $a, b, c, d \in \mathrm{R}$, в умножении которых используются равенства

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1,\ \mathbf{ij} = \mathbf{k} = -\mathbf{ji},\ \mathbf{jk} = \mathbf{i} = -\mathbf{kj},\ \mathbf{ki} = \mathbf{j} = -\mathbf{ik}$$

(так что $\mathbf{ijk} = \mathbf{jki} = \mathbf{kij} = -1$). Совокупность кватернионов образует некоммутативное *тело*, содержащее С в качестве подполя. Позднее А. Кэли (A. Cayley), отбросив требование ассоциативности умножения, построил обобщение кватернионов — *октавы Кэли,* наборы, состоящие из восьми компонент. К концу 19 в. появилось много работ, посвящённых более широким системам чисел, названных *гиперкомплексными*; теперь такие системы называют *алгебрами конечного ранга.*

Дальнейшее развитие представлений о комплексных числах проходило в рамках *теории функций комплексного переменного* — своеобразной и очень интересной области анализа. Проблематику этой науки изложил Гаусс в своём письме к Бесселю (1811). Основоположником ТФКП является О. Коши (A. Cauchy), а подлинными творцами — Б. Риман (B. Riemann) и К. Вейерштрасс.

Кроме алгебры, теории чисел и ТФКП, комплексные числа играют существенную роль в длинном перечне разделов математики. Лишь для примера отметим здесь анализ и его приложения (*дифференциальные и интегральные уравнения; спектральная теория; преобразование Фурье; аппроксимация в комплексной области; интерполяция линейных операторов и др.*) и математическое моделирование (*задачи математической физики; цифровая обработка сигналов и др.*).

13.1. Определение комплексных чисел и переход к алгебраической форме

Определение 1. *Комплексным числом называется упорядоченная пара* $z = (a, b)$ *чисел* $a, b \in \mathrm{R}$. *Если* $z_1 = (a_1, b_1)$, $z_2 = (a_2, b_2)$, *то* $z_1 = z_2$ *тогда и только тогда, когда* $a_1 = a_2$ *и* $b_1 = b_2$. *Сложение и умножение двух комплексных чисел вводятся по формулам:*

$$(a_1, b_1) + (a_2, b_2) := (a_1 + a_2, b_1 + b_2), \tag{1}$$

$$(a_1, b_1) \cdot (a_2, b_2) := (a_1 a_2 - b_1 b_2, a_1 b_2 + b_1 a_2). \tag{2}$$

Компоненты a и b называются соответственно *действительной и мнимой частями комплексного числа* $z = (a, b)$. Их обозначения $\mathrm{Re}z := a, \mathrm{Im}z := b$. Равенство $z_1 = z_2$ двух комплексных чисел по определению означает, что одновременно $\mathrm{Re}z_1 = \mathrm{Re}z_2$ и $\mathrm{Im}z_1 = \mathrm{Im}z_2$. В связи с этим

$$\mathrm{Re}(z_1 + z_2) = \mathrm{Re}z_1 + \mathrm{Re}z_2,\ \mathrm{Im}(z_1 + z_2) = \mathrm{Im}z_1 + \mathrm{Im}z_2,$$

$$\mathrm{Re}(z_1z_2) = \mathrm{Re}z_1\mathrm{Re}z_2 - \mathrm{Im}z_1\mathrm{Im}z_2,\ \mathrm{Im}(z_1z_2) = \mathrm{Re}z_1\mathrm{Im}z_2 + \mathrm{Im}z_1\mathrm{Re}z_2.$$

Совокупность всех комплексных чисел z обозначается через $\mathbf{C}$.

Операции (1) – (2) порождают на C так называемую алгебраическую структуру (мы пользуемся терминологией раздела 12). Как отмечалось в разделе 12, *алгебраическая система* $(\mathrm{C}; +, \cdot)$ *является полем.* Напомним здесь, что это означает выполнение следующих свойств.

$$\begin{aligned}
&1^\circ. \quad (z_1 + z_2) + z_3 = z_1 + (z_2 + z_3),\\
&2^\circ. \quad z + \mathbf{0} = z,\\
&3^\circ. \quad \exists(-z)\ : z + (-z) = \mathbf{0},\\
&4^\circ. \quad z_1 + z_2 = z_2 + z_1,\\
&5^\circ. \quad (z_1z_2)z_3 = z_1(z_2z_3),\\
&6^\circ. \quad z \cdot \mathbf{1} = z,\\
&7^\circ. \quad z \neq \mathbf{0} \implies \exists z^{-1}\ : zz^{-1} = \mathbf{1},\\
&8^\circ. \quad z_1z_2 = z_2z_1,\\
&9^\circ. \quad (z_1 + z_2)z_3 = z_1z_3 + z_2z_3.
\end{aligned}$$

Здесь $z, z_1, z_2, z_3 \in \mathrm{C}$; $\mathbf{0}$ и $\mathbf{1}$ обозначают пары $\mathbf{0} := (0,0), \mathbf{1} := (1,0)$ — нейтральные элементы относительно сложения и умножения (за ними чуть ниже мы установим привычные обозначения 0 и 1).

Проверка этих свойств не составляет труда. Установим, например, дистрибутивность 9°. Пусть $z_k = (a_k, b_k), k = 1, 2, 3$. Тогда левая часть 9° равна

$$(z_1 + z_2)z_3 = (a_1 + a_2, b_1 + b_2) \cdot (a_3, b_3) =$$

$$\Big((a_1 + a_2)a_3 - (b_1 + b_2)b_3, (a_1 + a_2)b_3 + (b_1 + b_2)a_3\Big) =$$

$$= (a_1a_3 + a_2a_3 - b_1b_3 - b_2b_3, a_1b_3 + a_2b_3 + b_1a_3 + b_2a_3).$$

Правая часть есть

$$z_1z_3 + z_2z_3 = (a_1a_3 - b_1b_3, a_1b_3 + b_1a_3) + (a_2a_3 - b_2b_3, a_2b_3 + b_2a_3) =$$

$$= (a_1a_3 - b_1b_3 + a_2a_3 - b_2b_3, a_1b_3 + b_1a_3 + a_2b_3 + b_2a_3).$$

Сравнение результатов даёт 9°. В справедливости остальных свойств убедитесь самостоятельно.

Как и во всяком поле, в C можно ввести действия, обратные сложению и умножению, — а именно, *вычитание* и *деление.* Для произвольных $z_1 = (a_1, b_1)$, $z_2 = (a_2, b_2)$ полагают

$$z_1 - z_2 := z_1 + (-z_2) = (a_1 - a_2, b_1 - b_2).$$

Пусть $z_2 \neq \mathbf{0}$, то есть $a_2^2 + b_2^2 \neq 0$. Нетрудно видеть, что

$$z_2^{-1} = \Big(\frac{a_2}{a_2^2 + b_2^2}, \frac{-b_2}{a_2^2 + b_2^2}\Big)$$

— это число удовлетворяет равенству $z_2 z_2^{-1} = \mathbf{1} = (1,0)$. Положим

$$\frac{z_1}{z_2} := z_1 z_2^{-1} = (a_1, b_1) \cdot \left(\frac{a_2}{a_2^2 + b_2^2}, \frac{-b_2}{a_2^2 + b_2^2}\right)$$

$$= \left(\frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2}, \frac{-a_1 b_2 + b_1 a_2}{a_2^2 + b_2^2}\right). \tag{3}$$

Простой способ нахождения частного, не требующий автоматического запоминания формулы (3), будет указан ниже. Для разности и частного выполнено

$$z_2 + (z_1 - z_2) = z_1, \qquad z_2 \cdot \frac{z_1}{z_2} = z_1.$$

Обычным образом определяются *степени* с нулевым, натуральным и целым показателями. Для $z \in \mathbf{C}$ и $n \in \mathrm{N}$

$$z^0 := \mathbf{1}, \qquad z^n := \underbrace{z \cdot \ldots \cdot z}_{n}, \qquad z^{-n} := (z^n)^{-1}.$$

В последнем равенстве $z \neq \mathbf{0}$. Можно взять и $z^{-n} := (z^{-1})^n$, так как, очевидно, $(z^{-1})^n = (z^n)^{-1}$.

Наконец, *корнем натуральной степени* n из комплексного числа z называется такое число $\omega \in \mathrm{C}$, для которого выполнено

$$\omega^n = z. \tag{4}$$

Как мы покажем в пункте 13.3, если $z \neq \mathbf{0}$, то существует ровно n различных значений ω, удовлетворяющих (4).

Пример 1. Уравнение $x^2 + 1 = 0$ неразрешимо в R. Его аналогом в C является уравнение $z^2 + \mathbf{1} = \mathbf{0}$, то есть

$$z^2 + (1,0) = (0,0). \tag{5}$$

Покажем, что (5) имеет два различных комплексных решения.

Пусть $z = (a, b)$. Тогда

$$z^2 + (1,0) = (a,b) \cdot (a,b) + (1,0) = (a^2 - b^2 + 1, 2ab).$$

Из определения равенства комплексных чисел получаем систему

$$a^2 - b^2 + 1 = 0,$$

$$2ab = 0.$$

Её решения $a = 0, b = \pm 1$. Поэтому $z = (0, \pm 1)$.

Комплексное число $\mathbf{i} := (0,1)$ обладает свойством $\mathbf{i}^2 = (-1,0)$; оно называется иногда *мнимой единицей.*

Важным этапом изучения комплексных чисел является осуществление перехода от вида $z = (a,b)$ к так называемой алгебраической форме.

Замечание 1. В ряде текстов начинают именно с записи $z = a + b\mathbf{i}$, отмечая при этом, что мнимая единица $\mathbf{i}$ есть не что иное, как $\sqrt{-1}$. Это вызывает обоснованное удивление неискушённого читателя (ибо квадратный корень из отрицательного

числа извлечь нельзя!). Наш подход лишён этой трудности: из двух определений $\mathbf{i} := (0,1)$ и $\mathbf{i} := \sqrt{-1}$ мы предпочитаем первое; второе же пока вообще лишено смысла.

Обозначим через U подмножество C, состоящее из комплексных чисел вида $(a,0), a \in \mathrm{R}$. Нетрудно видеть, что U есть *подполе* C (здесь и ниже мы используем терминологию пункта 12.4). Действия с элементами U как с комплексными числами производятся подобно обычным сложению и умножению действительных чисел. Именно, из формул (1) – (2) легко следует, что

$$(a,0)+(b,0)=(a+b,0), \qquad (a,0)\cdot(b,0)=(ab,0).$$

Поэтому соответствие $(a,0) \mapsto a$ осуществляет *изоморфизм* между совокупностью U всех пар отмеченного вида (с операциями над комплексными числами) и множеством R (с обычными сложением и умножением); мы пишем $U \simeq \mathrm{R}$. Соответствующие элементы этих двух структур отождествляют, формально полагая $(a,0)=a$. Однако это равенство является необычным — в нём содержатся объекты различной природы. Понимать его следует как иную форму записи соответствия $(a,0) \longleftrightarrow a$. С этого момента мы считаем, в частности, $(1,0)=1$ и $(0,0)=0$.

Итак, поле C *можно считать расширением поля* R. Более точно, C содержит подполе U такое, что $U \simeq \mathrm{R}$.

Замечание 2. Можно показать, что C является в некотором смысле *минимальным* расширением R, в котором разрешимо уравнение $x^2+1=0$. Одновременно поле C является *алгебраически замкнутым.* Последнее означает, что *любой многочлен степени* $n \geqslant 1$ *с коэффициентами из* C *имеет по крайней мере один комплексный корень.*

Полное доказательство этой *основной теоремы алгебры (многочленов)* было дано Гауссом (C.F. Gauss, 1799).

Для $z \in \mathrm{C}$, как нетрудно видеть, справедливо

$$z=(a,b)=(a,0)+(0,b)=(a,0)+(b,0)\cdot(0,1). \tag{6}$$

Приняв во внимание отождествление пар $(a,0)$, $(b,0)$ с действительными числами a, b и определение $\mathbf{i}$, равенство (6) переписывают в виде

$$z=a+b\mathbf{i}.$$

Это и есть *алгебраическая форма комплексного числа* z. В случае $\mathrm{Im}z=b=0$ комплексное число z считается *действительным.* Число z, для которого $a=\mathrm{Re}z=0$, называется *чисто мнимым.*

Основные действия с комплексными числами в алгебраической форме выглядят следующим образом:

$$(a_1+b_1\mathbf{i})+(a_2+b_2\mathbf{i})=(a_1+a_2)+(b_1+b_2)\mathbf{i},$$

$$(a_1+b_1\mathbf{i})(a_2+b_2\mathbf{i})=(a_1a_2-b_1b_2)+(a_1b_2+b_1a_2)\mathbf{i}.$$

Это просто другой вид равенств (1) – (2). В таком же варианте можно описать вычитание и деление (сделайте это самостоятельно).

При умножении комплексных чисел в алгебраической форме можно автоматически действовать с ними как с двучленами, учитывая то, что $\mathbf{i}^2 = -1$. Чётные степени $\mathbf{i}$ дают вклад в действительную часть, а нечётные — в мнимую, например:

$$\mathbf{i}^3 = \mathbf{i}^2 \cdot \mathbf{i} = -\mathbf{i},\ \mathbf{i}^4 = 1,\ \mathbf{i}^5 = \mathbf{i},$$

и т.д. Отрицательные степени равны

$$\mathbf{i}^{-1} = -\mathbf{i},\ \mathbf{i}^{-2} = -1,\ \mathbf{i}^{-3} = \mathbf{i},\ \mathbf{i}^{-4} = 1.$$

В этой цепочке совсем нетрудно увидеть закономерность, а именно последовательное чередование значений $1, \mathbf{i}, -1, -\mathbf{i}$ при возрастании показателя степени. Неискушённому читателю рекомендуется освоить действия в алгебраической форме в первую очередь — именно такая запись комплексных чисел является основной.

Пример 2. $(-1 + 2\mathbf{i})(2 + 5\mathbf{i}) = -2 + 4\mathbf{i} - 5\mathbf{i} + 10\mathbf{i^2} = -12 - \mathbf{i}$,

$$(1 + 2\mathbf{i})^6 = \sum_{k=0}^{6} \binom{6}{k} 1^k (2\mathbf{i})^{6-k} =$$

$$= -64 + 192\mathbf{i} + 240 - 160\mathbf{i} - 60 + 12\mathbf{i} + 1 = 117 + 44\mathbf{i}.$$

Упражнение 1. Вычислить в алгебраической форме $\sqrt{3 - 4\mathbf{i}}$.

Упражнение 2. Решить квадратное уравнение $(2 + \mathbf{i})z^2 - (5 - \mathbf{i})z + (2 - 2\mathbf{i}) = 0$, *применив формулу для его корней.*

Определение 2. *Пусть* $z = a + b\mathbf{i}$. *Действительное число* $|z| := \sqrt{a^2 + b^2}$ *называется модулем* z. *Комплексное число* $\overline{z} := a - b\mathbf{i}$ *называется сопряжённым к* z.

Другими словами, модуль определяется равенством $|z| = \sqrt{(\mathrm{Re}z)^2 + (\mathrm{Im}z)^2}$, а сопряжённое число — условиями $\mathrm{Re}\overline{z} := \mathrm{Re}z,\ \mathrm{Im}\overline{z} := -\mathrm{Im}z$.

Операция сопряжения (то есть переход к сопряжённому комплексному числу) обладает рядом очевидных, но очень важных свойств.

$1^\circ.$ $\quad \overline{\overline{z}} = z,$

$2^\circ.$ $\quad \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2},$

$3^\circ.$ $\quad \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2},$

$4^\circ.$ $\quad (\overline{z})^k = \overline{z^k},$

$5^\circ.$ $\quad z + \overline{z} = 2\mathrm{Re}z = 2a,$

$6^\circ.$ $\quad z - \overline{z} = 2\mathrm{Im}z \cdot \mathbf{i} = 2b\mathbf{i},$

$7^\circ.$ $\quad |\overline{z}| = |z|,$

$8^\circ.$ $\quad z \cdot \overline{z} = |z|^2.$

В 5° и 6°, как обычно, $z = a + b\mathbf{i}$. Обратим особое внимание на то, что сумма и произведение попарно сопряжённых чисел есть действительное, а разность — чисто мнимое числа. Свойства 2° и 3° по индукции переносятся на любое число слагаемых и сомножителей.

Установим для иллюстрации 3°. Пусть $z_1 = a_1 + b_1\mathbf{i}, z_2 = a_2 + b_2\mathbf{i}$. Тогда

$$z_1 \cdot z_2 = (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)\mathbf{i},$$

$$\overline{z_1 \cdot z_2} = (a_1a_2 - b_1b_2) - (a_1b_2 + b_1a_2)\mathbf{i}.$$

С другой стороны,

$$\overline{z_1} \cdot \overline{z_2} = (a_1 - b_1\mathbf{i}) \cdot (a_2 - b_2\mathbf{i}) = (a_1a_2 - b_1b_2) - (a_1b_2 + b_1a_2)\mathbf{i},$$

что и гарантирует 3°.

Упражнение 3. Доказать остальные свойства.

Упражнение 4. Пусть $\mathbf{A} = (a_{kl})$ *— матрица порядка* n *с комплексными элементами,* Δ *— её определитель. Доказать, что определитель матрицы* $\mathbf{B} = (\overline{a_{kl}})$ *равен* $\overline{\Delta}$.

Сопряжение эффективно применяется при делении комплексных чисел. Пусть $z_1 = a_1 + b_1\mathbf{i}, z_2 = a_2 + b_2\mathbf{i} \neq 0$.

$$\frac{z_1}{z_2} = \frac{z_1\overline{z_2}}{z_2\overline{z_2}} = \frac{z_1\overline{z_2}}{|z_2|^2} = \frac{a_1a_2 + b_1b_2 + (-a_1b_2 + b_1a_2)\mathbf{i}}{a_2^2 + b_2^2} =$$

$$= \frac{a_1a_2 + b_1b_2}{a_2^2 + b_2^2} + \frac{-a_1b_2 + b_1a_2}{a_2^2 + b_2^2}\mathbf{i}. \qquad (7)$$

Мы получили формулу, аналогичную (3). Существенно то, что $z_2\overline{z_2}$ — действительное число.

Пример 3. В конкретном случае обычно повторяют весь процесс — это проще, чем запоминать явное выражение (7).

$$\frac{-1 + 2\mathbf{i}}{2 + 5\mathbf{i}} = \frac{(-1 + 2\mathbf{i})(2 - 5\mathbf{i})}{(2 + 5\mathbf{i})(2 - 5\mathbf{i})} = \frac{-12 - \mathbf{i}}{29} = -\frac{12}{29} - \frac{1}{29}\mathbf{i}.$$

Основные свойства модуля мы рассмотрим в следующем пункте; выше мы отметили лишь те из них, которые связаны с сопряжением.

Термины, введённые в этом пункте, относятся к фундаменту математики и могут использоваться в самых разных задачах и моделях.

Пример 4. Решим уравнение $\mathrm{Im}z + |\overline{z} - 2z| \cdot \mathbf{i} = 2\mathbf{i}$.

Мы следуем стандартной схеме для задач такого сорта. Пусть $z = a + b\mathbf{i}$. Тогда $\overline{z} = a - b\mathbf{i}$, $\mathrm{Im}z = b$,

$$|\overline{z} - 2z| = |a - b\mathbf{i} - 2a - 2b\mathbf{i}| = |-a - 3b\mathbf{i}| =$$

$$= \sqrt{(-a)^2 + (-3b)^2} = \sqrt{a^2 + 9b^2}.$$

Подставляя в уравнение, получим

$$b + \sqrt{a^2 + 9b^2} \cdot \mathbf{i} = 2\mathbf{i}.$$

Сравнение действительной и мнимой частей даёт $b = 0, \quad \sqrt{a^2 + 9b^2} = 2$. Это означает, что $a = \pm 2, b = 0$. Итак, $z = \pm 2$.

Упражнение 5. В пункте 12.4 было показано, что поле C *изоморфно совокупности* M *матриц второго порядка вида*

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \qquad a, b \in \mathrm{R},$$

с операциями сложения и умножения матриц. Изучите вопрос о возможности эффективного вычисления произведения двух комплексных чисел, используя их связь с матрицами и идеи алгоритма Штрассена, см. пункт 2.3.

13.2. Изображение на плоскости. Модуль, аргумент и тригонометрическая форма комплексного числа. Свойства модуля

На плоскости с декартовой системой координат комплексное число $z+b\mathbf{i}$ изображается точкой Q с координатами (a, b). Соответствие точек плоскости и комплексных чисел, осуществляемое по правилу $Q(a, b) \longleftrightarrow z = a + b\mathbf{i}$, является взаимнооднозначным. Поэтому декартову плоскость часто называют *комплексной плоскостью,* отождествляя её точки с числами $z \in$ C. Оси координат, по которым откладываются величины $a = \mathrm{Re}z$ и $b = \mathrm{Im}z$, называются соответственно *действительной и мнимой осями.* Их уравнения $\mathrm{Im}z = 0,\ \mathrm{Re}z = 0$.

При таком подходе легко понять геометрический смысл операций $z_1 + z_2$, $z_1 - z_2$, $\overline{z}$ — они описываются простыми действиями с векторами (какими именно?).

Комплексному числу $z = a + b\mathbf{i}$ можно сопоставить также и *полярные координаты* точки $Q(a, b)$ — числа $r \geqslant 0$ и $\varphi \in$ R. Мы считаем, что полярная система координат обычным образом ассоциирована с декартовой: полюс совпадает с началом декартовой системы — точкой O, а направление полярного луча совпадает с направлением оси абсцисс. Поэтому r представляет собой длину вектора $\overline{Q}$, а φ — угол, образованный $\overline{OQ}$ и направлением действительной оси. Считаем далее, что $\varphi \in [0, 2\pi)$.

Очевидно, r является модулем числа z :

$$r = |\overline{OM}| = \sqrt{a^2 + b^2} = |z|,$$

см. определение 2 предыдущего пункта. Число φ называется *аргументом* z:

$$\arg z := \varphi \in [0, 2\pi).$$

(Точнее, это так называемое *главное значение аргумента.* Ясно, что угол φ определён с точностью до слагаемого $2\pi k, k \in$ Z, поэтому аргумент необязательно фиксировать в указанных пределах.) Для точки $z = 0$ значение $\arg z$ не определено.

Очевидно, в наших обозначениях $a = \cos\varphi,\ b = \sin\varphi$, поэтому

$$z = a + b\mathbf{i} = r(\cos\varphi + \mathbf{i}\sin\varphi).$$

Последняя форма записи комплексного числа называется *тригонометрической.*

Чтобы перевести комплексное число z из алгебраической формы в тригонометрическую, требуется найти $r = |z|$ и $\varphi = \arg z$. Для нахождения аргумента часто полезно изобразить z на комплексной плоскости.

Пример 1. Пусть $z = 1$. Так как $a = \mathrm{Re} z = 1, b = \mathrm{Im} z = 0$, то $|z| = \sqrt{1^2 + 0} = 1$, $\varphi = \arg z = 0$. Поэтому $1 = 1(\cos 0 + \mathbf{i} \sin 0)$. Аналогично

$$-1 = 1(\cos \pi + \mathbf{i} \sin \pi), \quad 1 - \mathbf{i} = \sqrt{2}(\cos \frac{7\pi}{4} + i \sin \frac{7\pi}{4}),$$

$$3 + 4\mathbf{i} = 5(\cos \alpha + \mathbf{i} \sin \alpha).$$

В последнем равенстве α — угол первой четверти, для которого $\cos \alpha = 3/5$.

Приведём в этом пункте ряд свойств модуля комплексного числа. Прежде всего отметим свойства, означающие, что $|\cdot|$ является так называемой *нормой* на $\mathbf{C}$.

$$1^\circ. \quad |z| \geqslant 0; \ |z| = 0 \Longleftrightarrow z = 0.$$

$$2^\circ. \quad |\lambda z| = |\lambda||z|, \qquad \lambda \in \mathrm{R}.$$

$$3^\circ. \quad |z_1 + z_2| \leqslant |z_1| + |z_2|.$$

Свойства 1° – 2° очевидны. Соотношение, стоящее в 3°, называется *неравенством треугольника.* Его геометрическое обоснование совершенно ясно. В алгебраической форме 3° имеет вид

$$\sqrt{(a_1 + a_2)^2 + (b_1 + b_2)^2} \leqslant \sqrt{a_1^2 + b_1^2} + \sqrt{a_2^2 + b_2^2}, \quad a_j, b_j \in \mathrm{R}.$$

После простых преобразований оно приводится к эквивалентному неравенству $0 \leqslant (a_1 b_2 - a_2 b_1)^2$, справедливость которого также очевидна.

Упражнение 1. Доказать 3°, *используя тригонометрическую форму.*

Из 3° получаются некоторые другие соотношения:

$$|z_1 - z_2| \leqslant |z_1| + |z_2|,$$

$$|z_1 - z_2| \geqslant \Big||z_1| - |z_2|\Big|, \qquad |z_1 + z_2| \geqslant \Big||z_1| - |z_2|\Big|.$$

По свойствам сопряжения из пункта 13.1,

$$|z_1 \cdot z_2 \ldots \cdot z_n|^2 = z_1 \cdot z_2 \cdot \ldots \cdot z_n \cdot \overline{z_1 \cdot z_2 \ldots \cdot z_n} =$$

$$= z_1 \cdot z_2 \ldots \cdot z_n \cdot \overline{z_1} \cdot \overline{z_2} \cdot \ldots \cdot \overline{z_n} = |z_1|^2 \cdot |z_2|^2 \cdot \ldots \cdot |z_n|^2,$$

поэтому

$$|z_1 \cdot z_2 \cdot \ldots \cdot z_n| = |z_1| \cdot |z_2| \cdot \ldots \cdot |z_n|. \tag{8}$$

Итак, *модуль произведения комплексных чисел равен произведению их модулей.* Важное равенство (8) может быть получено и с использованием тригонометрической формы (см. следующий пункт). Ясно, что оно обобщает свойство 2°, где $\lambda \in \mathrm{R}$.

Из (8) при $n = 2, z_1 = z \neq 0, z_2 = z^{-1}$ получаем

$$1 = |z \cdot z^{-1}| = |z| \cdot |z^{-1}|,$$

в связи с чем

$$|\frac{1}{z}| = |z^{-1}| = \frac{1}{|z|}, \quad z \neq 0.$$

Опять применяя (8), приходим к равенству:

$$|\frac{z_1}{z_2}| = |z_1 \cdot \frac{1}{z_2}| = |z_1| \cdot |\frac{1}{z_2}| = \frac{|z_1|}{|z_2|}, \quad z_2 \neq 0.$$

Укажем также оценки

$$-|z| \leqslant \mathrm{Re} z \leqslant |z|, \quad -|z| \leqslant \mathrm{Im} z \leqslant |z|,$$

$$-\sqrt{2}|z| \leqslant \mathrm{Re} z + \mathrm{Im} z \leqslant \sqrt{2}|z|.$$

Последняя следует из соотношения

$$|a+b| \leqslant \sqrt{2}\sqrt{a^2+b^2}, \qquad a, b \in \mathrm{R}.$$

Отмеченные соотношения эффективно применяются в самых различных задачах.

Пример 2. Докажем, что если $|z| < 1/2$, то $|(1+\mathbf{i})z^3 + \mathbf{i}z| < 3/4$.

Доказательство содержится в цепочке оценок:

$$|(1+\mathbf{i})z^3 + \mathbf{i}z| \leqslant |(1+\mathbf{i})z^3| + |\mathbf{i}z| = |1+\mathbf{i}| \cdot |z|^3 + 1 \cdot |z| <$$

$$< \sqrt{2} \cdot \frac{1}{8} + \frac{1}{2} = \frac{\sqrt{2}+4}{8} < \frac{6}{8} = \frac{3}{4}.$$

Геометрический смысл величины $|z_1 - z_2|$ — расстояние между точками z_1, z_2. Действительно, в стандартных обозначениях

$$|z_1 - z_2| = |(a_1 - a_2) + (b_1 - b_2)\mathbf{i}| = \sqrt{(a_1-a_2)^2 + (b_1-b_2)^2}.$$

Отсюда сразу следует, что при фиксированных $z_0 \in \mathrm{C}, R \geqslant 0$ множество

$$G = \{z \in \mathrm{C} \ : \ |z - z_0| \leqslant R\}$$

изображается кругом (с границей) радиуса R с центром в z_0. Граница Γ этого круга (окружность) задаётся равенством $|z - z_0| = R$, внешность круга (без границы) — неравенством $|z - z_0| > R$. Если $R = 0$, то $G = \Gamma = \{z_0\}$. В связи с этим

$$G' = \{z \in \mathrm{C} \ : \ r \leqslant |z - z_0| \leqslant R\}, \quad 0 < r < R,$$

представляет собой кольцо, ограниченное концентрическими окружностями с радиусами r, R и центрами в z_0.

Исходя из определения $\arg z$, получаем, что множество

$$H = \{z \in \mathrm{C} \ : \ \arg z = s\}, \qquad 0 \leqslant s < 2\pi,$$

есть луч (без начала координат), образующий с действительной осью угол s,

$$H' = \{z \in \mathrm{C} \ : s_1 \leqslant \arg z \leqslant s_2\}, \qquad 0 \leqslant s_1 < s_2 \leqslant 2\pi,$$

— внутренность углового сектора, образованного лучами $\arg z = s_1, \arg z_2 = s_2$ (с границей за исключением точки $z = 0$).

Наконец, уравнения

$$|z - z_1| + |z - z_2| = 2q, \qquad 2c = |z_1 - z_2| < 2q,$$

$$\Big||z - z_1| - |z - z_2|\Big| = 2q, \qquad 2c = |z_1 - z_2| > 2q > 0$$

при фиксированных z_1, z_2 задают на комплексной плоскости соответственно эллипс и гиперболу с фокусами в точках z_1, z_2 и полуосью q.

Упражнение 2. Изобразить множества точек $z \in \mathrm{C}$, для которых

$$(a)\ \mathrm{Im}z + \mathrm{Re}z \leqslant 3,\ 1 \leqslant \arg z \leqslant \frac{\pi}{2}; \quad (b)\ 1 \leqslant |z + 5| \leqslant 2,\ |\mathrm{Re}z| < 5;$$

$$(c)\ |z - \overline{z}| \leqslant 1; \quad (d)\ |z - 2\overline{z}| = 1; \quad (e)\ z = \frac{1 + t\mathbf{i}}{1 - t\mathbf{i}},\ t \in \mathrm{R}.$$

Упражнение 3. Найти $A = \min_{z \in D} f(z)$, где

$$f(z) = |3 + 2\mathbf{i} - z|, \qquad D = \{z \in \mathrm{C} :\ |z| \leqslant 1\}.$$

Упражнение 4. Доказать для $z_1, z_2 \in \mathrm{C}$ неравенство

$$|z_1 - z_2| \leqslant \Big||z_1| - |z_2|\Big| + \max\{|z_1|, |z_2|\} \cdot |\arg z_1 - \arg z_2|.$$

Упражнение 5. Точка z движется против часовой стрелки по контуру квадрата $\max\{|\mathrm{Re}z|, |\mathrm{Im}z|\} = 1$. Изобразить траекторию движения точки $\omega = z^{-1}$.

13.3. Действия в тригонометрической форме (умножение, деление, возведение в степень, извлечение корня)

Сложение и вычитание комплексных чисел очень просто выполняются в алгебраической форме. Результаты этого пункта означают, что умножение, деление, возведение в степень и извлечение корня удобнее производить в тригонометрической форме.

Теорема 1. *Пусть $z_1 = r_1(\cos\varphi_1 + \mathbf{i}\sin\varphi_1),\ z_2 = r_2(\cos\varphi_2 + \mathbf{i}\sin\varphi_2)$. Тогда*

$$z_1 z_2 = r_1 r_2\Big(\cos(\varphi_1 + \varphi_2) + \mathbf{i}\sin(\varphi_1 + \varphi_2)\Big). \tag{9}$$

Если $z_2 \neq 0$, то

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}\Big(\cos(\varphi_1 - \varphi_2) + \mathbf{i}\sin(\varphi_1 - \varphi_2)\Big). \tag{10}$$

Доказательство. Воспользуемся формулами тригонометрии для суммы и разности углов. Сначала получим (9).

$$z_1 z_2 = r_1 r_2\Big(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 + \mathbf{i}(\sin\varphi_1\cos\varphi_2 + \cos\varphi_1\sin\varphi_2)\Big) =$$

$$= r_1 r_2 \Big(\cos(\varphi_1 + \varphi_2) + \mathbf{i} \sin(\varphi_1 + \varphi_2) \Big).$$

Пусть дополнительно $z_2 \neq 0$. Тогда

$$\frac{z_1}{z_2} = \frac{z_1 \overline{z_2}}{z_2 \overline{z_2}} = \frac{z_1 \overline{z_2}}{|z_2|^2} = \frac{r_1(\cos\varphi_1 + \mathbf{i}\sin\varphi_1) \cdot r_2(\cos\varphi_2 - \mathbf{i}\sin\varphi_2)}{r_2^2} =$$
$$= \frac{r_1}{r_2} \Big(\cos\varphi_1 \cos\varphi_2 + \sin\varphi_1 \sin\varphi_2 + \mathbf{i}(\sin\varphi_1 \cos\varphi_2 - \cos\varphi_1 \sin\varphi_2) \Big) =$$
$$= \frac{r_1}{r_2} \Big(\cos(\varphi_1 - \varphi_2) + \mathbf{i} \sin(\varphi_1 - \varphi_2) \Big).$$

Формулы (9) – (10) доказаны.

Следствие. *Пусть* $z = r(\cos\varphi + \mathbf{i}\sin\varphi)$. *Тогда*

$$z^n = r^n(\cos n\varphi + \mathbf{i}\sin n\varphi). \tag{11}$$

Равенство (11) получается из (9). Надо взять сначала $z_1 = z_2 = z$ и затем использовать индукцию по n.

Соотношение (11) называется *формулой Муавра* по имени английского математика Авраама Де Муавра (A. de Moivre, 1667 – 1754), известного также своими результатами в теории вероятностей. Под таким названием (11) впервые появилась в 1748 г. во "Введении"Леонарда Эйлера (L. Euler, 1707 – 1783). Приводимую ниже теорему 2 также связывают с именем Де Муавра.

Теорема 2. *Существует ровно* n *различных значений корня* n*-й степени из комплексного числа* z.

Если $z = r(\cos\varphi + \mathbf{i}\sin\varphi)$, *то эти значения* $\sqrt[n]{z}$ *имеют вид:*

$$\omega_k = \sqrt[n]{r} \Big(\cos\frac{\varphi + 2\pi k}{n} + \mathbf{i}\sin\frac{\varphi_+ 2\pi k}{n} \Big), \quad k = 0, 1, \ldots, n-1. \tag{12}$$

Доказательство. Пусть ω_k определяются с помощью (12). Тогда обязательно $\omega_s \neq \omega_t$ при $0 \leqslant s < t \leqslant n-1$. Действительно, разность их аргументов $\arg\omega_t - \arg\omega_s = 2\pi(t-s)/n$ не является кратной 2π. Покажем, что $\omega_k^n = z$ для всех $k = 0, 1, \ldots, n-1$. Это будет означать, что существует не менее n значений корня $\sqrt[n]{z}$.

Воспользуемся формулой Муавра (11):

$$\omega_k^n = (\sqrt[n]{r})^n \Big(\cos n \cdot \frac{\varphi + 2\pi k}{n} + \mathbf{i}\sin n \cdot \frac{\varphi_+ 2\pi k}{n} \Big) =$$
$$= r\Big(\cos(\varphi + 2\pi k) + \mathbf{i}\sin(\varphi + 2\pi k) \Big) = r(\cos\varphi + \mathbf{i}\sin\varphi) = z.$$

Теперь установим, что других значений корня, отличных от (12), нет. Пусть $u = \varrho(\cos\gamma + \mathbf{i}\sin\gamma) = \sqrt[n]{z}$. Тогда $u^n = z$, и опять по формуле (11)

$$\varrho^n = r; \qquad n\gamma = \varphi + 2\pi m, \quad m \in \mathrm{Z}.$$

(Если $\sin\alpha = \sin\beta, \cos\alpha = \cos\beta$, то α и β различаются на угол $2\pi m$.) В связи с этим обязательно

$$\varrho = \sqrt[n]{r}, \quad \gamma = \frac{\varphi + 2\pi m}{n}.$$

Остаётся понять, что число u, соответствующее этому целому m, обязательно совпадает с некоторым ω_k из набора (12). Пусть k таково, что $m-k$ делится нацело на n; тогда $u=\omega_k$. Действительно,

$$\cos\gamma=\cos\frac{\varphi+2\pi m}{n}=\cos\frac{\varphi+2\pi k}{n},\ \sin\gamma=\sin\frac{\varphi+2\pi m}{n}=\sin\frac{\varphi+2\pi k}{n},$$

так как аргументы отличаются на целое кратное 2π. Заметим, что такое k найдётся для любого $m\in\mathrm{Z}$, так как совокупность $\{0,1,\ldots,n-1\}$ есть в точности множество всех остатков по модулю n.

Теорема 2 доказана.

Замечание. Формула (12) показывает, что значения корня n-й степени из комплексного z лежат на окружности радиуса $\varrho=\sqrt[n]{z}$ с центром в начале координат и делят её на n равных дуг, то есть изображаются вершинами правильного n-угольника, вписанного в эту окружность.

Примеры. 1. Вычислим $(1+\mathbf{i})^{25}$ с использованием (11). Для этого переведём $z:=1+\mathbf{i}$ в тригонометрическую форму. Так как $|z|=\sqrt{2}$, $\arg z=\pi/4$, то

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

Применение (11) с $n=25$ даёт

$$z^{25}=(\sqrt{2})^{25}\Big(\cos\frac{25\pi}{4}+\mathbf{i}\sin\frac{25\pi}{4}\Big)=2^{12}\sqrt{2}\Big(\cos\frac{\pi}{4}+\mathbf{i}\sin\frac{\pi}{4}\Big)=$$

$$=2^{12}\sqrt{2}\Big(\frac{\sqrt{2}}{2}+\mathbf{i}\frac{\sqrt{2}}{2}\Big)=2^{12}(1+\mathbf{i}).$$

2. Пусть требуется найти все значения корня

$$\sqrt[6]{\frac{1-\mathbf{i}}{\sqrt{3}+\mathbf{i}}}.$$

Сначала переведём числитель и знаменатель в тригонометрическую форму, затем выполним деление по формуле (10) и, наконец, применим (12). Такой порядок действий является самым экономичным.

$$z_1:=1-\mathbf{i}=\sqrt{2}\Big(\cos\frac{7\pi}{4}+\mathbf{i}\sin\frac{7\pi}{4}\Big),\quad z_2:=\sqrt{3}+\mathbf{i}=2\Big(\cos\frac{\pi}{6}+\mathbf{i}\sin\frac{\pi}{6}\Big),$$

$$z:=\frac{z_1}{z_2}=\frac{\sqrt{2}\Big(\cos\frac{7\pi}{4}+\mathbf{i}\sin\frac{7\pi}{4}\Big)}{2\Big(\cos\frac{\pi}{6}+\mathbf{i}\sin\frac{\pi}{6}\Big)}=\frac{1}{\sqrt{2}}\Big(\cos(\frac{7\pi}{4}-\frac{\pi}{6})+\mathbf{i}\sin(\frac{7\pi}{4}-\frac{\pi}{6})\Big)=$$

$$=\frac{1}{\sqrt{2}}\Big(\cos\frac{19\pi}{12}+\mathbf{i}\sin(\frac{19\pi}{12})\Big).$$

Применение формулы (12) с $n=6$ даёт:

$$\omega_k=\frac{1}{\sqrt[12]{2}}\left(\cos\frac{\frac{19\pi}{12}+2k\pi}{6}+\mathbf{i}\sin\frac{\frac{19\pi}{12}+2k\pi}{6}\right)=$$

$$=\frac{1}{\sqrt[12]{2}}\Big(\cos\frac{19\pi+24k\pi}{72}+\mathbf{i}\sin\frac{19\pi+24k\pi}{72}\Big).$$

Все значения ω_k корня $\sqrt[6]{z}$ получаются, если взять последовательно $k=0,1,2,3,4,5$.

13.4. Корни из 1, их свойства

В этом пункте мы рассмотрим свойства значений корня n-й степени из 1 для фиксированного натурального n. Вместо *значение корня* для краткости будем говорить просто *корень.*

Корни n-й степени из 1 — это комплексные числа

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

Они получаются из формулы (12), если взять $z = 1 = \cos 0 + \mathbf{i}\sin 0$.

Ясно, что $\varepsilon_k \in \mathrm{R}$ при $k = 0$ и $k = n/2$, если n чётно, и лишь при $k = 0$, если n нечётно. Числа ε_k изображаются на комплексной плоскости точками единичной окружности, которые расположены в вершинах правильного n-угольника. Одно из этих чисел, а именно ε_0, равно 1. Заметим, что для любого корня ε_k выполнены равенства

$$\varepsilon_k = (\varepsilon_1)^k, \qquad \varepsilon_k^{-1} = \overline{\varepsilon_k}.$$

Первое следует из формулы Муавра (11), второе проверяется простым вычислением. (Вообще $z^{-1} = \overline{z} \Longleftrightarrow |z| = 1$.)

Теорема 1. (A) *Пусть ε и δ — корни n-й степени из 1. Тогда $\overline{\varepsilon}$, ε^m при любом $m \in \mathrm{Z}$ и $\varepsilon\delta$ также есть корни из 1 той же степени. В частности, таковым является ε^{-1}.*

(B) *Все значения корня n-й степени из $z \in \mathrm{C}$ имеют вид $\varepsilon_0\omega$, $\varepsilon_1\omega$, …, $\varepsilon_{n-1}\omega$, где ω — какое-то фиксированное значение $\sqrt[n]{z}$.*

Доказательство. (A). Следует из равенств:

$$\overline{\varepsilon}^n = \overline{\varepsilon^n} = \overline{1} = 1, \quad (\varepsilon^m)^n = \varepsilon^{mn} = 1, \quad (\varepsilon\delta)^n = \varepsilon^n \cdot \delta^n = 1 \cdot 1 = 1.$$

(B). Все указанные значения $\varepsilon_j\omega$ попарно различны, так как $\varepsilon_j \neq \varepsilon_k$ при $j \neq k$. Кроме того, $(\varepsilon_j\omega)^n = \varepsilon^n \cdot \omega^n = 1 \cdot z = z$. Поэтому набор чисел $\varepsilon_j\omega$ исчерпывает всю совокупность значений корня из 1 степени n.

Теорема доказана.

Из части (A) следует, что совокупность $\{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}\}$ образует *мультипликативную группу G порядка n*. Очевидно, что $\varepsilon_k\varepsilon_l = \varepsilon_m$, где m таково, что $k+l \equiv m \pmod n$. Так как $\varepsilon_k = \varepsilon_1^k$, то G — *циклическая группа,* порождённая элементом ε_1, то есть $G = \langle\varepsilon_1\rangle$.

Группа G *изоморфна* группе вычетов $\mathrm{Z_n} = \{0, 1, \ldots, n-1\}$ с операцией сложения по модулю n. Здесь и далее мы используем терминологию и некоторые простые результаты пунктов 12.1 и 12.2.

Определение. *Корень n-й степени из 1, который не является корнем из 1 никакой меньшей степени, называется первообразным, или примитивным.*

Первообразными являются, например, ε_1 и ε_{n-1}. Нетрудно получить следующий результат.

Теорема 2. *Корень ε_k является первообразным тогда и только тогда, когда степени $\varepsilon_k^0, \varepsilon_k^1, \ldots, \varepsilon_k^{n-1}$ различны, то есть исчерпывают совокупность всех значений корня n-й степени из 1.*

Доказательство. Пусть корень ε_k — первообразный. В этом случае равенство $\varepsilon_k^l = \varepsilon_k^m$ при $1 \leqslant l < m \leqslant n$ невозможно, так как тогда $\varepsilon_k^{m-l} = 1$ при $0 < m - l < n$.

Если же все степени попарно различны, то $\varepsilon_k^m \neq \varepsilon_k^0 = 1$ ни при каком натуральном $m < n$. Это по определению означает, что ε_k — первообразный корень степени n, что и требовалось доказать.

Теорема 2 означает, что для первообразных корней ε_k и только для них $G = \langle \varepsilon_k \rangle$.

Оказывается, что есть более простой способ нахождения первообразных корней для данного n. Обозначим через (k, n) наибольший общий делитель чисел k и n.

Теорема 3. *Число ε_k является первообразным корнем из 1 степени n тогда и только тогда, когда $(k, n) = 1$.*

Доказательство. Корень ε_1 является первообразным, что соответствует утверждению для $k = 1$. Считаем далее, что $k > 1$.

Пусть $1 < d =: (k, n) < n$. Тогда $m = n/d$ меньше n и в то же время

$$\varepsilon_k^m = (\varepsilon_1^k)^m = \varepsilon_1^{km} = \varepsilon_1^{qn} = 1.$$

Здесь $q := k/d$. По теореме 2 ε_k не является первообразным. Поэтому, если ε_k является первообразным, то обязательно $d = 1$.

Пусть теперь $d = (k, n) = 1$ и в то же время ε_k не является первообразным. По теореме 2 это означает, что для некоторого $m < n$ будет $\varepsilon_k^m = 1$. Тогда число km не делится нацело на n, но для него $\varepsilon_1^{km} = \varepsilon_k^m = 1$. Это невозможно в силу первообразности ε_1. Противоречие означает, что в случае $d = 1$ корень ε_k обязательно является первообразным.

Теорема 3 доказана.

Обозначим через $\Phi(n)$ количество чисел, взаимно простых с n и меньших n (включая единицу). Так определённая функция $\Phi(n)$ называется *функцией Эйлера.* Результат теоремы 3 означает, что общее число первообразных корней степени n из 1 совпадает с $\Phi(n)$.

Функция Эйлера возникает в теории чисел. Не вдаваясь в подробности, укажем, что при любом n

$$\Phi(n) = n\Big(1 - \frac{1}{p_1}\Big) \cdot \ldots \cdot \Big(1 - \frac{1}{p_s}\Big).$$

Здесь $p_1, \ldots p_s$ — все различные простые делители n.

Упражнение 1. Используя последнюю формулу, показать, что функция Эйлера является мультипликативной, то есть $\Phi(mn) = \Phi(m)\Phi(n)$, если $(m, n) = 1$.

Порядком корня ε_k называется наименьшее целое m такое, что $\varepsilon_k^m = 1$.

Иначе говоря, m есть порядок подгруппы $\langle \varepsilon_k \rangle$. По теореме Лагранжа (см. пункт 12.2), в конечной группе порядок любой подгруппы делит порядок группы. Поэтому порядок ε_k совпадает с одним из делителей числа n. Именно, *порядок ε_k равен $m = n/d$, где $d = (k, n)$.* Заметим, что если ε_k — первообразный, то $d = 1$ и $m = n$. Это соответствует теоремам 2 – 3.

Упражнение 2. Показать, что порядок ε_k равен $n/d, d = (k, n)$. См. доказательство теоремы 3.

Пример. Первообразными корнями из 1 степени 12 будут $\varepsilon_1, \varepsilon_5, \varepsilon_7, \varepsilon_{11}$, так как 1, 5, 7, 11 — это все взаимно простые с 12 числа, меньшие 12. Число первообразных корней совпадает со значением

$$\Phi(12) = 12\Big(1 - \frac{1}{2}\Big)\Big(1 - \frac{1}{3}\Big) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4.$$

Мы использовали, что $12 = 2^2 \cdot 3$.

Найдём порядок m корня ε_8. Так как $d = (8, 12) = 4$, то $m = 12/4 = 3$. Действительно, $\varepsilon_8 \cdot \varepsilon_8 = \varepsilon_4$, $\varepsilon_4 \cdot \varepsilon_8 = \varepsilon_0$, и поэтому $\langle \varepsilon_8 \rangle = \{\varepsilon_8, \varepsilon_4, \varepsilon_0\}$.

Упражнение 3. Найти и изобразить значения корня из 1 степени n для $n = 3, 4, 5, 6$.

Упражнение 4. Чему равно число первообразных корней из 1 степени 120? степени 1000?

Упражнение 5. Пусть $n = 60$. Найти порядки корней $\varepsilon_7, \varepsilon_9, \varepsilon_{18}$. Какой из них является первообразным?

Упражнение 6. Доказать, что для любого натурального q, не являющегося кратным n, имеет место равенство

$$1 + \varepsilon_1^q + \varepsilon_1^{2k} + \ldots + \varepsilon_1^{(n-1)q} = 0.$$

13.5. Дополнение. Понятие о теории функций комплексного переменного

Систематическое изложение *теории функций комплексного переменного (ТФКП)* осуществляется в рамках отдельного курса или соответствующего раздела курса анализа. Не претендуя на полную точность, мы дадим лишь некоторое понятие о проблематике этой науки и её исторических корнях. Разумеется, этот пункт не является обязательным для читателя.

В широком смысле слова ТФКП изучает функции одного или многих комплексных переменных. В узком смысле предметом исследования являются лишь так называемые *аналитические функции* комплексных переменных. Всюду далее мы ограничимся последней темой, рассматривая, кроме того, комплекснозначные функции *одного* комплексного переменного.

Как самостоятельная дисциплина ТФКП оформилась примерно к середине 19 века. Основополагающими здесь были работы Огюстена Коши (A. Cauchy, 1789 – 1857), Карла Вейерштрасса (K. Weirstraass, 1815 – 1897) и Бернхарда Римана (B. Riemann, 1826 – 1866), которые подходили к развитию этой науки с различных позиций. Классический курс ТФКП объединяет черты этих подходов и рассматривает взаимосвязь соответствующих понятий и свойств.

Исходным пунктом является введение *топологии* на так называемой *расширенной комплексной плоскости,* то есть совокупности C, пополненной идеальной бесконечно удалённой точкой $z = \infty$. Топология задаётся с помощью системы окрестностей, то есть множеств вида

$$V(z_0, \delta) := \{z : |z - z_0| < \delta\}, \quad V(\infty, \delta) := \{z : |z| > \delta\}; \quad z_0 \in \mathrm{C},\ \delta > 0.$$

На этой основе вводятся понятия *открытых и замкнутых множеств, внутренних и граничных точек, замыкания и компактности.* Под *областью D* понимается обычно открытое связное множество (то есть множество $D \subset \mathrm{C}$, все точки которого входят в D с некоторой окрестностью, и любые две точки которого можно соединить ломаной, целиком лежащей в D).

Даётся определение *сходимости* числовых последовательностей и рядов с комплексными элементами. Далее описываются такие свойства функций комплексного переменного, как *непрерывность, равномерная непрерывность,* и свойства *сходимости функциональных последовательностей и рядов.* Особую роль, как и в классическом анализе, играют *степенные ряды,* частичные суммы которых являются алгебраическими многочленами. С помощью степенных рядов вводятся некоторые элементарные функции, например

$$e^z := \sum_{k=0}^{\infty} \frac{z^k}{k!}, \quad \cos z := \sum_{k=0}^{\infty} (-1)^k \frac{z^{2k}}{(2k)!}, \quad \sin z := \sum_{k=0}^{\infty} (-1)^k \frac{z^{2k+1}}{(2k+1)!}.$$

Основное определение — аналитической функции — можно сформулировать поразному в рамках каждого из подходов.

Коши в своём построении теории аналитических функций исходил из понятия моногенности. Функцию f называют *моногенной* в точке z, если она имеет в z *производную.* Пусть $f(z) = u(x,y) + v(x,y)\mathbf{i}$ для $z = x + y\mathbf{i}$. Действительная и мнимая части моногенной функции обязательно удовлетворяют условиям Коши – Римана:

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \qquad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}. \tag{13}$$

Наоборот, выполнение условий (13) в точке z при условии существования полных дифференциалов функций u и v является достаточным для моногенности f в этой точке. Функция называется *аналитической в области* D, если она моногенна всюду в D.

Коши развил теорию интегрирования непрерывных функций; в частности, он показал (1825), что интеграл с комплексными пределами не зависит от выбора пути интегрирования. (В комплексной ситуации интеграл берётся по некоторой непрерывной кривой — так называемой *кривой Жордана*). Таким образом, для произвольной аналитической в односвязной области D функции f и любой замкнутой кривой $\Gamma \subset D$

$$\int_{\Gamma} f(z)dz = 0.$$

Отсюда получается, что при некоторых условиях

$$\frac{1}{2\pi\mathbf{i}} \int_{\Gamma} \frac{f(t)dt}{t-z} = f(z). \tag{14}$$

Здесь Γ — граница D и $z \in D$. Если же z принадлежит дополнению к замыканию D, то интеграл в левой части (14) равен 0. Свойства этого *интеграла Коши* приводят к интересному результату, не имеющему аналога в действительном анализе: аналитическая в области D функция f в каждой точке этой области имеет производные любого порядка.

Таким образом, *в комплексном анализе однократная дифференцируемость влечёт бесконечную дифференцируемость.*

По Вейерштрассу, функция f является аналитической в области D, если в окрестности каждой точки $z_0 \in D$ она разлагается в степенной ряд

$$w = f(z) = \sum_{k=0}^{\infty} a_k (z - z_0)^k. \tag{15}$$

Для определения аналитических (в этом смысле) функций достаточно даже, чтобы сходящийся ряд (15) был задан в окрестности одной-единственной точки z_0, ибо значения f в других точках z_1 и соответствующие ряды могут быть определены в процессе так называемого *аналитического продолжения* вдоль различных путей, соединяющих z_0 и z_1.

В этом процессе могут встретиться *особые точки,* аналитическое продолжение в которые невозможно. Это ведёт к тому, что продолжение f вдоль различных путей Γ_1 и Γ_2 от z_0 к z_1 может привести к различным значениям $f(z_1)$.

Таким образом, *полная аналитическая функция* $w = f(z)$, полученная аналитическими продолжениями ряда (15) по всевозможным путям, может оказаться *многозначной.* Таковы, например, функции $w = \sqrt[n]{z}$ и $w = \log z$. Способ превращения многозначной аналитической функции в *однозначную* состоит в том, что её следует рассматривать не как функцию точки $z \in \mathbb{C}$, а как функцию точки *римановой поверхности*, состоящей из нескольких листов, накрывающих комплексную плоскость и соединённых некоторым образом между собой. Так, риманова поверхность для функции $w = \sqrt[n]{z}$ состоит из n листов, а для $w = \log z$ является бесконечнолистной.

Наконец, для Римана главным был геометрический подход, состоящий в анализе свойств отображений, осуществляемых аналитическими функциями. Если f является аналитической в смысле Коши (в частности, удовлетворяет условиям Коши – Римана), то при некоторых условиях f осуществляет так называемое *конформное отображение.* При таком отображении имеет место консерватизм углов и постоянство искажения масштаба по всем направлениям, выходящим из точки z_0.

Риманом установлены *основные принципы теории конформных отображений.* Им, в частности, доказана следующая знаменитая теорема, носящая его имя.

Для каждой односвязной однолистной области, граница которой состоит более чем из одной точки, существует единственная однолистная аналитическая функция, осуществляющая конформное отображение этой области на внутренность единичного круга.

Итак, существенной и исторически обусловленной частью ТФКП является сравнение следующих условий и связанных с ними свойств функции:

1. f является моногенной в D и, следовательно, имеет в D производные любого порядка;

2. f разлагается в окрестности точек D в степенные ряды;

3. f осуществляет конформное отображение.

К тематике ТФКП относятся и другие важные вопросы (*изучение свойств конкретных функций, ряд Лорана, вычеты и их приложения, классификация изолированных особых точек и др.,* см., например, [22]).

В заключение сформулируем ряд упражнений, которые касаются функций вида

$$f(z) = \frac{az+b}{cz+d}\ ; \qquad a,b,c,d \in \mathrm{C},\ ad \neq bc. \tag{16}$$

Такие функции называются *дробно-линейными.*

Упражнение 1. Установить, что каждая функция (16) является однолистной, то есть $f(z_1) \neq f(z_2)$ *при* $z_1 \neq z_2$.

Упражнение 2. Показать, что совокупность всех дробно-линейных функций (16) образует группу относительно операции суперпозиции.

Упражнение 3. Доказать, что каждая функция (16) отображает любую окружность или прямую в окружность или прямую. Воспользоваться тем, что произвольная окружность или прямая на комплексной плоскости может быть задана уравнением вида

$$\frac{|z-z_1|}{|z-z_2|} = \lambda \tag{17}$$

с подходящими $z_1, z_2 \in \mathrm{C}$ *и* $\lambda > 0$ *(окружность Аполлония).*

Упражнение 4. Проверить, что уравнение (17) задаёт на плоскости C *окружность или прямую.*

14. Многочлены

Многочлены, или полиномы, — важные объекты, играющие фундаментальную роль во всех областях математики.

Конечно, чаще всего многочлены понимаются как функции некоторого простого вида, обладающие целым рядом полезных свойств. Сумма, разность, произведение и даже суперпозиция двух многочленов есть снова многочлен. Область определения многочлена $f(x)$ является максимально широкой. Значение $f(x_0)$ в данной точке x_0 может быть вычислено по сравнительно простой схеме. Многочлен — это гладкая функция (существуют производные f любого порядка). Хорошо изучены свойства нулей $f(x)$. Если к этому добавить, что различные функции эффективно *аппроксимируются* многочленами и функциями, получающимися из них с помощью некоторых простых операций (*рациональными и кусочно-полиномиальными функциями, или сплайнами*), то это во многом объяснит роль многочленов в анализе и приложениях.

Следует, однако, сказать, что многочлены возникают и в задачах теории чисел, дискретной математики, науки о вычислениях и др. Вообще, многие их приложения возникают на стыке различных разделов математики. В качестве примера приведём задачу об эффективном выборе узлов для полиномиальной интерполяции функций нескольких переменных; это анализ, алгебра и геометрия одновременно. Некоторые классические монографии о многочленах служат выразительной иллюстрацией единства математики. Так, прекрасная книга Т. Ривлина (T. Rivlin [27]) о *многочленах Чебышёва* $T_n(x) := \cos(n \arccos x)$ имеет впечатляющий подзаголовок *From Approximation Theory to Algebra and Number Theory.*

Отвлекаясь от этой интересной тематики, поясним, что в настоящем тексте совокупности многочленов рассматриваются как *алгебраические системы,* а именно *кольца.* В кольце многочленов определяются такие важные понятия, как *делимость, наибольший общий делитель, неприводимость и т.д.,* не требующие функционального подхода. Начиная с пункта 14.2, мы будем записывать многочлен в привычном виде

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

понимая, однако, что идентификация и действия с такими объектами осуществляются через их коэффициенты a_i. Иначе говоря, многочлены трактуются как бесконечные наборы чисел $(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$, равных 0, начиная с некоторой позиции. В последних пунктах раздела мы будем смотреть на многочлены и как на функции.

Ниже рассматриваются прежде всего многочлены с действительными или комплексными коэффициентами; их совокупности имеют единое обозначение $F[x]$, где $F = \mathrm{R}$ или $F = \mathrm{C}$. Замечания указывают на справедливость основных свойств и в более общей ситуации — для многочленов над кольцом K.

Для знакомства с многочленами рекомендуются учебники А.Г. Куроша [16] и А.И. Кострикина [13]. Отметим также книгу П. Нодена, К. Китте [20], содержащую многие важные алгоритмы. Некоторые другие ссылки даются в основном тексте.

14.1. Совокупности многочленов как алгебраические системы

Пусть F — поле действительных чисел R или комплексных чисел C.

Определение 1. *Многочленом над F называется выражение вида*

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n, \qquad a_i \in F. \tag{1}$$

Числа a_i называются коэффициентами $f(x)$. Максимальное k, для которого $a_k \neq 0$, называется степенью $f(x)$ и обозначается $\deg f$. *Два многочлена $f(x)$ и $g(x)$ называются равными, если равны все их соответствующие коэффициенты.*

Совокупность всех таких многочленов (с различными $n = 0, 1, 2, \ldots$ и $a_i \in F$) обозначается через $F[x]$.

Нулевым многочленом, или нуль–многочленом, обозначаемым просто 0, называется многочлен, все коэффициенты которого равны 0. Степень такого многочлена полагается равной $-\infty$. (Часто, впрочем, считают $\deg 0 = 0$.)

Вместо $f(x)$ мы будем обычно писать просто f. Следует хорошо понять, что в $F[x]$ равенство $f = 0$ или, подробнее, $f(x) = 0$ означает, что все коэффициенты f равны 0, а вовсе не является уравнением относительно x. Наоборот, $f \neq 0$ тогда и только тогда, когда f имеет хотя бы один ненулевой коэффициент a_i.

При сравнении коэффициентов f и g в случае $\deg f \neq \deg g$ возникает необходимость пополнять совокупность коэффициентов одного из них нулями. Так как основные действия с многочленами вводятся в дальнейшем также *покоэффициентно,* то более точным является следующий подход.

Определение 2. *Многочленом называется бесконечный набор*

$$f = (a_0, a_1, \ldots, a_i, \ldots) \tag{2}$$

чисел $a_i \in F$, в котором все a_i, начиная с некоторого, равны 0. Два набора, у которых все соответствующие компоненты совпадают, называются равными. В частности, $f = 0$ тогда и только тогда, когда все $a_i = 0$.

Соответствие между записями (1) и (2) очевидно:

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \longleftrightarrow (a_0, a_1, \ldots, a_n, 0, 0, \ldots).$$

В этом пункте мы будем использовать более точное определение 2, свободное от функционального вида многочлена. Но в дальнейшем мы перейдём к более привычной записи (1).

Сложение и умножение двух многочленов $f = (a_0, a_1, \ldots)$ и $g = (b_0, b_1, \ldots)$ вводятся по правилам:

1. $f + g := (a_0 + b_0, a_1 + b_1, \ldots)$.
2. $fg := (c_0, c_1, \ldots,)$, где $c_k = \sum\limits_{i+j=k} a_ib_j$.

Нетрудно понять, что произведение fg вычисляется по привычной схеме, если использовать для сомножителей форму (2). Заметим также, что

$$(a_0, 0, 0, \ldots) + (b_0, 0, 0, \ldots) = (a_0 + b_0, 0, 0, \ldots),$$

$$(a_0,0,0,\ldots)\cdot(b_0,0,0,\ldots)=(a_0b_0,0,0,\ldots),$$

$$(0,1,0,\ldots)\cdot(0,1,0,\ldots)=(0,0,1,0,\ldots),$$

$$(0,1,0,\ldots)\cdot(0,0,1,0,\ldots)=(0,0,0,1,0,\ldots),$$

и т.д. Отождествим набор $(a,0,\ldots)$ с числом $a\in F$ и обозначим $x:=(0,1,0,\ldots)$. Тогда

$$(a_0,a_1,a_2,\ldots,a_n,0,\ldots)=$$

$$=(a_0,0,\ldots)+(0,a_1,0,\ldots)+(0,0,a_2,\ldots)+(0,0,0,\ldots,a_n,0)=$$

$$=a_0+a_1x+a_2x^2+\ldots+a_nx^n.$$

В такой трактовке (2) просто совпадает с (1). Этот процесс является аналогом перехода от записи комплексных чисел в виде пар (a,b) к их алгебраической форме $a+b\mathbf{i}$, см. пункт 13.1.

Наконец, обратим внимание на то, что умножение $(\lambda,0,\ldots)$ на f имеет вид $(\lambda,0,\ldots)\cdot(a_0,a_1,\ldots,a_n,0,\ldots)=(\lambda a_0,\lambda a_1,\ldots,\lambda a_n,0,\ldots)$, то есть соответствует умножению $f\in F[x]$ на число $\lambda\in F$.

Можно показать, что относительно операций сложения многочленов и умножения многочлена на $\lambda\in F$ совокупность $F[x]$ образует *линейное пространство,* см. пункт 5.1.

Здесь же нас будут интересовать свойства алгебраической системы $F[x]$ относительно операций 1 – 2. Ниже мы используем терминологию раздела 12.

Теорема 1. *Совокупность $F[x]$ относительно операций 1 – 2 образует ассоциативное коммутативное кольцо с единицей, не имеющее делителей нуля, то есть целостное кольцо.*

Доказательство. Коммутативность сложения и умножения в $F[x]$ следует из симметричного вида $f+g$ и fg относительно f и g. Нулевой элемент $F[x]$ — это нульмногочлен $0=(0,0,\ldots)$. Очевидно, для $f=(a_0,a_1,\ldots)$ противоположным является $-f:=(-a_0,-a_1,\ldots)$. Единицей в $F[x]$ будет многочлен $(1,0,0,\ldots)$, обозначаемый просто 1. Ясно, что $1\cdot f=f$.

Ассоциативность сложения, ассоциативность умножения и дистрибутивность вытекают из следующих числовых равенств:

$$(a_r+b_r)+c_r=a_r+(b_r+c_r),\tag{3}$$

$$\sum_{k+l=r}\Big(\sum_{i+j=k}a_ib_j\Big)c_l=\sum_{i+j+l=r}a_ib_jc_l=\sum_{i+k=r}a_i\Big(\sum_{j+l=k}b_jc_l\Big),\tag{4}$$

$$\sum_{i+k=r}(a_i+b_i)c_k=\sum_{i+k=r}a_ic_k+\sum_{i+k=r}b_ic_k.\tag{5}$$

Обозначим $f=(a_0,a_1,\ldots),g=(b_0,b_1,\ldots),h=(c_0,c_1,\ldots)$. Соотношение (3) означает, что совпадают r-е компоненты многочленов $(f+g)+h$ и $f+(g+h)$ при произвольном r; поэтому $(f+g)+h=f+(g+h)$. Аналогично, (4) и (5) эквивалентны соответственно $(fg)h=f(gh)$ и $(f+g)h=fh+gh$.

Покажем, наконец, что $F[x]$ не имеет делителей нуля, то есть таких многочленов f и g, одновременно не равных 0, что $fg = 0$. Пусть $f \neq 0, g \neq 0$; a_s и b_r — первые ненулевые компоненты f и g. Тогда

$$fg = (0, \ldots, 0, a_r, \ldots) \cdot (0, \ldots, 0, b_s, \ldots) = (0, \ldots, 0, a_r b_s, \ldots) \neq 0.$$

В правом наборе $a_r b_s$ есть компонента с номером $r + s$. Это означает, что если $fg = 0$, то обязательно $f = 0$ или $g = 0$.

Теорема доказана.

Степени суммы и произведения многочленов удовлетворяют следующим естественным условиям.(Мы считаем, что $\deg 0 := -\infty$ и для произвольного конечного n имеет место $-\infty + n = -\infty$.)

Теорема 2. *Для любых* $f, g \in F[x]$

$$\deg(f + g) \leqslant \max\{\deg f, \deg g\}, \quad \deg fg = \deg f + \deg g. \tag{6}$$

Если $\lambda \in F, \lambda \neq 0$, *то* $\deg \lambda f = \deg f$.

Доказательство сразу получается из определения операций 1 – 2.

Упражнение 1. Привести примеры двух многочленов из $\mathrm{R}[x]$, *для которых левое соотношение в (6) обращается* (i) *в строгое неравенство;* (ii) *в равенство.*

Замечание. Теоремы 1 – 2 допускают обобщение на совокупность $K[x]$ многочленов с компонентами из произвольного кольца K (быть может, поля). $K[x]$ определяется аналогично $F[x], F = \mathrm{R}$ или C, с заменой числовых компонент на элементы K. Операции сложения и умножения таких многочленов в $K[x]$ осуществляются в компонентах через сложение и умножение в основном кольце K.

Аналог теоремы 1 в этой ситуации утверждает, что совокупность $K[x]$ является кольцом, которое *наследует* такие свойства K, как ассоциативность и коммутативность, наличие единицы, отсутствие или наличие делителей нуля. Так, в случае, когда K обладает делителями нуля, $K[x]$ также ими обладает.

Многие равенства в $K[x], K \neq \mathrm{R}, \mathrm{C}$, могут быть весьма непривычными для неискушённого читателя. Например, если K есть поле Z_2 (с операциями по модулю 2), то в $K[x]$ выполнено $(x + 1)^2 = x^2 + 1$ (почему?).

Упражнение 2. В кольце $K[x], K = \mathrm{Z}_4$, *привести примеры делителей нуля* (i) *нулевой степени;* (ii) *ненулевой степени.*

Упражнение 3. Пусть K *— поле характеристики* p. *Показать, что в* $K[x]$ *выполнено* $(1 + x)^p = 1 + x^p$.

14.2. Делимость многочленов. Теорема о делении с остатком

В этом пункте мы установим некоторые свойства *делимости* многочленов из $F[x]$, аналогичные свойствам целых чисел. Как и ранее, в основном тексте мы считаем, что $F = \mathrm{R}$ или C.

Определение 1. *Будем говорить, что* $g \in F[x]$ *делит* $f \in F[x]$, *и записывать это в виде* $g \mid f$, *если для некоторого* $h \in F[x]$ *имеет место* $f = gh$.

Обратим внимание на следующие свойства, которые будут использоваться в дальнейшем.

1°. $g \mid f,\ f \mid h \implies g \mid h$.

2°. $g \mid f,\ g \mid h \implies g \mid f \pm h$.

3°. $g \mid f \implies \forall h \quad g \mid hf$.

4°. $\deg g = 0 \implies \forall f \quad g \mid f$.

5°. $g \mid f,\ \lambda \neq 0 \implies \lambda g \mid h$.

6°. $g \mid f,\ \deg g = \deg f \implies \exists \lambda \neq 0 \ :\ g = \lambda f$.

7°. $g \mid f,\ f \mid g \implies \exists \lambda \neq 0 \ :\ g = \lambda f$.

Здесь $f, g, h \in F[x], \lambda \in F$. Покажем, например, как получаются импликации 3° и 6°. Пусть $g \mid f$, тогда для некоторого $u \in F[x]$ имеет место $f = gu$. Тогда $hf = hgu$, то есть $g \mid hf$. Это даёт 3°.

Пусть $g \mid f, \deg g = \deg f$. Так как $f = gu$, то по теореме 2 предыдущего пункта $\deg f = \deg g + \deg u$, откуда $\deg u = 0$. Поэтому $u(x) = \lambda \in F \setminus \{0\}$ и $f = \lambda g$. Это соответствует 6°.

Упражнение 1. Установить остальные свойства.

Ясно, что для данной пары многочленов f, g вовсе не всегда будет $g \mid f$. Следующая важная теорема говорит о том, что при условии $g \neq 0$ для всех пар f, g определено так называемое *деление с остатком.*

Теорема. *Пусть $f, g \in F[x]$ и дополнительно $g \neq 0$. Существует единственный $q \in F[x]$ и единственный $r \in F[x]$ такие, что*

$$f(x) = g(x)q(x) + r(x), \qquad \deg r < \deg g. \tag{7}$$

Доказательство. Сначала установим *существование* q и r.

Пусть $\deg f = n, \deg g = m$ и эти многочлены имеют вид

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n, \quad g(x) = b_0 + b_1 x + \ldots + b_m x^m.$$

Если $f = 0$, возьмём $q = r = 0$. В этом случае (7) имеет вид $0 = 0 \cdot g + 0$. В случае $f \neq 0$, то есть $n \geqslant 0$, проведём индукцию по n.

База индукции — вариант $n = 0$. Если при этом $m > 0$, возьмём $q = 0, r = f$, что соответствует представлению $f = 0 \cdot g + f$. Если же $m = n = 0$, то положим $q = a_0 b_0^{-1}, r = 0$; равенство $f = a_0 b_0^{-1} g + 0$ имеет вид $a_0 = a_0$.

Предположим теперь, что утверждение справедливо для всех многочленов степени $< n$, где n — данное положительное число, и докажем, что оно имеет место для многочленов f степени n. Если $m > n$, можно взять $q = 0, r = f$. Поэтому считаем $m \leqslant n$.

Введём в рассмотрение многочлен $\tilde{f}$, для которого

$$f(x) = a_n b_m^{-1} x^{n-m} \cdot g(x) + \tilde{f}(x).$$

Простой анализ показывает, что $\deg \tilde{f} < n$. Значит, по предположению индукции, существуют многочлены $\tilde{q}$ и r, для которых $\tilde{f} = \tilde{q}g + r$, причём $\deg r < \deg g$. Таким образом,

$$f(x) = a_n b_m^{-1} x^{n-m} \cdot g(x) + \tilde{q}(x)g(x) + r(x) = q(x)g(x) + r(x).$$

Мы положили $q(x) = a_n b_m^{-1} x^{n-m} + \tilde{q}(x)$.

Существование многочленов q, r со свойствами (7) доказано. Перейдём к обоснованию *единственности* этих многочленов.

Предположим, что наряду с (7) для пары q_1, r_1 выполнено $f = q_1 g + r_1, \deg r_1 < \deg g$. Тогда $qg + r = q_1 g + r_1$, то есть $r - r_1 = (q_1 - q)g$. По теореме 2 пункта 14.1 мы приходим к равенству

$$\deg(r - r_1) = \deg(q_1 - q) + \deg g. \tag{8}$$

Соотношение (8) выполняется лишь в ситуации $r = r_1, q = q_1$ — тогда оно имеет вид $-\infty = -\infty + m$. Если же $r \neq r_1$ или $q \neq q_1$, то (8) неверно, так как $\deg(r - - r_1) < \deg g$. Это устанавливает единственность q и r.

Теорема полностью доказана.

Определение 2. *Многочлены q и r, для которых имеют место соотношения (7), называются соответственно частным и остатком при делении f на g.*

Ясно, что случай $r = 0$ соответствует ситуации $g \mid f$.

Упражнение 2. Выполнить деление с остатком $f(x) = 2x^4 - x^3 + x^2 + 2x - 1$ на $g(x) = x^3 + 1$ в кольце $\mathrm{R}[x]$.

Замечание. Внимательное рассмотрение доказательства показывает, что теорема о делении с остатком обобщается на многочлены из кольца $K[x]$ над произвольным целостным кольцом K. Именно, *пусть K — целостное кольцо и старший коэффициент многочлена $g \in K[x]$ обратим в K. Тогда для каждого $f \in K[x]$ существует единственная пара $q, r \in K[x]$ такая, для которой выполнены оба условия (7).*

По поводу кольца $K[x]$ см. замечание предыдущего пункта. Так как каждое поле F является одновременно и целостным кольцом, то приведённое утверждение является обощением теоремы этого пункта.

14.3. Наибольший общий делитель и алгоритм Евклида

Пусть f, g — произвольные многочлены из $F[x], F = \mathrm{R}$ или C.

Определение 1. *Пусть $h \in F[x]$ — многочлен, для которого выполнены одновременно следующие два условия:*

1. $h \mid f,\ h \mid g.$
2. *Если* $h_1 \mid f,\ h_1 \mid g,$ *то* $h_1 \mid h.$

Такой многочлен h называется наибольшим общим делителем (НОД) f и g. Мы применяем обозначение $h = (f, g)$.

Условие 1 означает, что h является *общим делителем* f и g; условие 2 требует, чтобы h был *наибольшим* из всех общих делителей этих многочленов.

Обратим внимание читателя, что в определении 1 термин *наибольший* реализуется через делимость, а не через старшинство степени h (из всех общих делителей). Впрочем, последний подход приводит к эквивалентному определению.

Упражнение 1. Показать, используя свойства делимости, что если условие 2 заменить на следующее:

$2'$. *Если* $h_1 \mid f,\ h_1 \mid g$, *то* $\deg h_1 \leqslant \deg h$,

то получится эквивалентное определение.

Прежде всего мы остановимся на единственности НОД, то есть корректности применения записи $h = (f, g)$.

Очевидно, что если $h = (f, g)$, то и $\lambda h = (f, g)$ для любого $\lambda \in F$, отличного от 0. Это связано с тем, что $\lambda h \mid h$ и $h \mid \lambda h$. Таким образом, если НОД двух многочленов существует (а мы покажем, что это действительно так), то он определён с точностью до числового множителя. Поэтому запись $h = (f, g)$ в смысле определения 1 фиксирует h именно в этих пределах и не является однозначной. Например, справедливо одновременно $2x^2 = (x^2, x^4)$ и $10x^2 = (x^2, x^4)$. Впрочем, если иметь в виду эту неоднозначность, она вполне применима.

Для того, чтобы обеспечить единственность НОД, его следует определённым образом *нормировать.* Из многих возможных способов нормировки мы выберем самый простой — будем считать, что *у нормированного многочлена старший коэффициент равняется 1.*

Ясно, что переход от $h \in F[x]$, $h \neq 0$, к нормированному h^* осуществляется посредством равенства $h^* := \lambda^{-1} h$, где $\lambda \neq 0$ — старший коэффициент многочлена h.

Теорема 1. *Пусть НОД многочленов f и g существует. Тогда нормированный НОД этих многочленов является единственным.*

Иначе говоря, если в определение 1 добавить условие нормированности h, то запись $h = (f, g)$ становится однозначной.

Доказательство. Если φ, ψ — два нормированных НОД f и g. Тогда по определению $\psi \mid \varphi$ и $\varphi \mid \psi$. По свойству 7° предыдущего пункта $\varphi = \lambda\psi, \lambda \in F$. Так как старшие коэффициенты φ и ψ равны 1, то $\lambda = 1$, то есть $\varphi = \psi$, что и требовалось доказать.

Отметим теперь некоторые свойства НОД. Ниже $f, g, h \in F[x]$ — произвольные многочлены, $\lambda \in F$ — ненулевое число.

$1°$. $(f, g) = (g, f)$.

$2°$. $(f, g + hf) = (f, g)$.

$3°$. $(f, 0) = f$.

$4°$. $(f, g) = (f, \lambda g)$.

Свойства 1° и 3° очевидны. Установим 4°.

Пусть $\varphi = (f, g)$. Тогда $\varphi \mid f, \varphi \mid g$. Ясно, что имеет место и $\varphi \mid \lambda g$. Поэтому φ — общий делитель f и λg. Итак, $(f, g) \mid (f, \lambda g)$. Теперь заметим, что $g = \lambda^{-1}(\lambda g)$ и по уже доказанному $(f, \lambda g) \mid (f, g)$. Считая эти НОД нормированными, мы приходим к 4°.

Упражнение 2. Доказать свойство 2°.

Центральным результатом этого пункта является существование НОД.

Теорема 2. *Для любых двух ненулевых многочленов $f, g \in F[x]$ их НОД $h = (f, g)$ существует.*

Доказательство является конструктивным и имеет форму алгоритма. Пусть $\deg f \geqslant \deg g$. Построим конечные последовательности многочленов r_i и q_i по сле-

дующему правилу:

$r_{-1} := f,\ r_0 := g;$ если $r_i \neq 0$, то q_i и r_{i+1} есть соответственно частное и остаток при делении r_{i-1} на r_i, $i = 0, 1, \ldots$.

Иными словами,

$$r_{i-1} := r_i q_i + r_{i+1}, \quad \deg r_{i+1} < \deg r_i, \quad i = 0, 1, \ldots . \tag{9}$$

Покажем, что этот процесс обрывается на некотором шаге, когда очередное новое значение остатка принимает значение $r_{n+1} = 0$. По построению $\deg r_{-1} \geqslant \deg r_0 > \deg r_1 > \deg r_2 > \ldots$. Так как степени остатков строго убывают, то на некотором шаге равенство (9) соответствует делению нацело — в крайнем случае мы дойдём до ситуации $\deg r_n = 0$, тогда очередной остаток r_{n+1} равен нулю.

Пусть r_n — последний не равный нулю остаток. Тогда r_n является наибольшим общим делителем f и g.

Для обоснования рассмотрим подробную запись алгоритма.

$$\begin{gathered} f = r_{-1} = gq_1 + r_1, \\ g = r_0 = r_1 q_2 + r_2, \\ r_1 = r_2 q_3 + r_3, \\ \ldots \quad \ldots \quad \ldots \\ r_{n-3} = r_{n-2} q_n + r_{n-1}, \\ r_{n-2} = r_{n-1} q_n + r_n, \\ r_{n-1} = r_n q_{n+1}. \end{gathered} \tag{10}$$

Поднимаясь снизу вверх, мы получаем последовательно, что $r_n \mid r_{n-1}$, $r_n \mid r_{n-2}$, $r_n \mid r_{n-3}$, $\ldots$, $r_n \mid r_1$, $r_n \mid g$, $r_n \mid f$, то есть r_n является общим делителем f, g.

Пусть теперь некоторый многочлен φ делит f и g. Тогда, опускаясь в (10) сверху вниз (до предпоследнего соотношения), имеем: $\varphi \mid r_1$, $\varphi \mid r_2$, $\varphi \mid r_3$, $\ldots$, $\varphi \mid r_{n-1}$, $\varphi \mid r_n$. Таким образом, r_n есть наибольший из всех общих делителей f, g. При обосновании мы воспользовались простым свойством делимости: если два элемента равенства (10) делятся на некоторый многочлен, то на него делится и третий элемент.

Итак, $r_n = (f, g)$. Фактически мы доказали последовательность соотношений $(f, g) = (g, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = r_n$.

Теорема доказана.

Приведённый в доказательстве теоремы 2 алгоритм широко известен — он называется *алгоритмом Евклида.* Конечно, Евклид (365 – ок. 300 г. до н.э.), живший 23 века назад, изобрёл его для целых положительных чисел (и в таком виде его проще всего иллюстрировать). Но описанный метод применим также и для многих совокупностей многочленов, см. замечание 1 в конце этого пункта.

Отметим некоторые следствия из алгоритма Евклида.

Следствие 1. *Для любых ненулевых $f, g \in F[x]$ существуют $u, v \in F[x]$ такие, что*

$$(f, g) = fu + gv. \tag{11}$$

Если дополнительно $\deg f, \deg g > 0$, *то многочлены* u, v *можно выбрать так, чтобы было* $\deg u < \deg g, \deg v < \deg f$.

Доказательство. Из предпоследнего соотношения цепочки (10) следует, что

$$(f, g) = r_n = r_{n-2} - r_{n-1}q_n = r_{n-2}u_1 + r_{n-1}v_1;$$

мы положили $u_1 := 1, v_1 := -q_n$ (в обозначениях из доказательства теоремы 2). Выражая из предыдущего равенства (10) r_{n-1} через r_{n-2} и r_{n-3}, получим

$$r_n = r_{n-3}u_2 + r_{n-2}v_2,$$

$u_2 := v_1, v_2 := u_1 - v_1q_{n-1}$, и т.д. В конце концов мы придём к представлению

$$r_n = r_{-1}u + r_0v = fu + gv,$$

совпадающему с (11).

Более тонкое рассуждение показывает, что можно выбрать u, v так, чтобы было одновременно $\deg u < \deg g, \deg v < \deg f$. Пусть, например, многочлен u из (11) таков, что $\deg u > \deg g$. Укажем новое соотношение вида (11), удовлетворяющее всем условиям. Пусть

$$u = gq + r, \qquad \deg r < \deg g.$$

Подставим это соотношение в (11).

$$(f, g) = fr + g(v + fq). \tag{12}$$

Анализ равенства (12) показывает, что это и есть нужное представление. Действительно, в нём $\deg r < \deg g$ и обязательно $\deg(v + fq) < \deg f$. Дело в том, что если последнее неравенство неверно, то степень правой части (12) совпадает со степенью второго слагаемого. В этой ситуации левая и правая части (12) содержали бы многочлены разных степеней: $\deg(f, g) \leqslant \min\{\deg f, \deg g\}$, $\deg g(v + fq) = \deg g + \deg(v + fq) > \deg g + \deg f$. Мы учитываем, что $\deg f, \deg g > 0$.

Следствие доказано.

Пример 1. Пусть $f(x) = x^4+4x^3+2x^2-4x-3$, $g(x) = x^3+3x^2-x-3$ — многочлены из $\mathrm{R}[x]$. Получим для них представление (11) с помощью метода из доказательства следствия 1. Прежде всего выполняем все шаги алгоритма Евклида.

$$\begin{aligned}
&f = gq_1 + r_1, \qquad && q_1(x) = x + 4, && r_1(x) = 5x^2 + 6x - 11;\\
&g = r_1q_2 + r_2, \qquad && q_2(x) = 1/5x - 6/25, && r_2(x) = 16/25x - 16/25;\\
&r_1 = r_2q_3; && (f, g) = r_2(x) = 16/25x - 16/25.
\end{aligned}$$

Пока мы избегаем нормировки. Последовательно получаем:

$$r_2 = g - r_1q_2 = g - (f - gq_1)q_2 = f(-q_2) + g(q_1q_2 + 1);$$
$$(f, g) = r_2 = fu + gv, \qquad u = -q_2,\ v = q_1q_2 + 1.$$

В числах это выглядит так:

$$\frac{16}{25}x - \frac{16}{25} = f(x)\left(-\frac{1}{5}x + \frac{6}{25}\right) + g(x)\left(\frac{1}{5}x^2 + \frac{14}{25}x + \frac{1}{25}\right).$$

После умножения на $25/16$ равенство принимает окончательный вид с нормированным НОД в левой части:

$$x-1=f(x)\left(-\frac{5}{16}x+\frac{3}{8}\right)+g(x)\left(\frac{5}{16}x^2+\frac{7}{8}x+\frac{1}{16}\right).$$

Пример 2. Многочлены u и v можно найти и с помощью *метода неопределённых коэффициентов*. Пусть f и g такие же, как в примере 1. Предположим, что из каких-то соображений известно, что нормированный НОД $(f,g)=x-1$. Так как $\deg u<\deg g=3, \deg v<\deg f=4$, полагаем $v(x)=Ax^2+Bx+C,\ \ u(x)=Dx^3+Ex^2+Fx+G$. Для неизвестных (или, как говорят, неопределённых) коэффициентов A,B,C,D,E,F,G,H выполняется равенство:

$$x-1=(x^4+4x^3+2x^2-4x-3)(Ax^2+Bx+C)+(x^3-3x+2)(Dx^3+Ex^2+Fx+G).$$

Это одно равенство в $\mathrm{R}[x]$ эквивалентно системе из семи линейных уравнений, выражающих совпадение коэффициентов при $x^6, x^5, x^4, x^3, x^2, x, 1$ в левой и правой частях.

$$A+D=0,\qquad 4A+B+E=0,\qquad 2A+4B+C-3D+F=0,$$

$$-4A+2B+4C+2D-3E+G=0,\quad -3A-4B+2C+2E-3F=0,$$

$$-3B-4C+2F-3G=1,\qquad -3C+2G=-1,$$

В матричной форме система имеет вид

$$\left(\begin{array}{ccccccc|c}
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
4 & 1 & 0 & 0 & 1 & 0 & 0 & 0\\
2 & 4 & 1 & -3 & 0 & 1 & 0 & 0\\
-4 & 2 & 4 & 2 & -3 & 0 & 1 & 0\\
-3 & -4 & 2 & 0 & 2 & -3 & 0 & 0\\
0 & -3 & -4 & 0 & 0 & 2 & -3 & 1\\
0 & 0 & -3 & 0 & 0 & 0 & 2 & -1
\end{array}\right).$$

Демонстрируя известное упорство, можно найти

$$A=0,\quad B=-\frac{5}{16},\quad C=\frac{3}{8},\quad D=0,\quad E=\frac{5}{16},\quad F=\frac{7}{8},\quad G=\frac{1}{16}.$$

Этот пример показывает, что даже при не очень больших значениях степеней f и g второй метод менее эффективен, чем использование результатов алгоритма Евклида.

Упражнение 3. Получить представление (11) для $f(x)=x^3-1, g(x)=x^2-1$ двумя способами, описанными в примерах 1 – 2.

Определение 2. *Многочлены $f,g\in F[x]$, для которых $(f,g)=1$, называются взаимно простыми.*

Следствие 2. *Многочлены $f,g\in F[x]$ являются взаимно простыми тогда и только тогда, когда существуют многочлены $u,v\in F[x]$, для которых $fu+gv=1$.*

Доказательство. Пусть f,g взаимно просты. Тогда $(f,g)=1$, и по первому следствию $1=fu+gv$ для некоторых $u,v\in F[x]$.

Пусть, наоборот, имеет место $fu + gv = 1$. Тогда $\varphi := (f, g)$ делит 1, то есть является многочленом нулевой степени. Если φ нормирован, то $\varphi = 1$.

В случае $F = \mathrm{R}$ это представление для взаимно простых многочленов доказано Э. Безу (E. Bezout, 1730 – 1783). Из следствия 2 получаются некоторые важные свойства, которые мы объединим в одно утверждение.

Следствие 3. (*i*) *Если* $(f, \varphi) = (f, \psi) = 1$, *то* $(f, \varphi\psi) = 1$.

(*ii*) *Если* $\varphi \mid fg$ *и* $(f, \varphi) = 1$, *то* $\varphi \mid g$.

(*iii*) *Если* $(\varphi, \psi) = 1$, $\varphi \mid f$, $\psi \mid f$, *то* $\varphi\psi \mid f$.

Доказательство. (*i*). По предыдущему следствию, для некоторых u, v имеет место $fu + \varphi v = 1$. Умножим это равенство на ψ :

$$\psi f u + \psi\varphi v = \psi.$$

Каждый общий делитель f и $\psi\varphi$ является и делителем ψ, то есть общим делителем для f и ψ. Так как $(f, \psi) = 1$, то таковых последних, отличных от многочленов нулевой степени, нет. Поэтому $(f, \psi\varphi) = 1$.

(*ii*). Умножим равенство $fu + \varphi v = 1$ на g :

$$fgu + \varphi g v = g.$$

Так как φ делит оба слагаемых левой части, то φ делит и правую часть.

(*iii*). По условию, $f = \varphi h = \psi h_1$. Поэтому $\psi \mid \varphi h$. Так как $(\varphi, \psi) = 1$, то по предыдущему свойству $\psi \mid h$. Тогда $\varphi\psi \mid f$.

Следствие 3 доказано.

Замечание 1. Результаты этого пункта являются справедливыми для так называемых *евклидовых колец многочленов,* то есть целостных колец, в которых определено деление с остатком. В частности, к таковым относится $K[x]$, где K — произвольное поле. Ситуация $K = F$ соответствует основному тексту пункта. Подробности см. в [13, с. 194].

Замечание 2. Алгоритмические вопросы, связанные с процессом деления с остатком и вычисления НОД в кольцах чисел и многочленов, подробно обсуждаются во второй главе книги [20], которую мы рекомендуем заинтересованному читателю.

14.4. Корни многочлена. Основная теорема алгебры многочленов

В этом пункте мы рассматриваем многочлен $f \in F[x]$ как функцию $f : F \to F$ аргумента x. Ставится вопрос о *нулях* этой функции, называемых корнями многочлена.

Ситуации $F = \mathrm{R}$ и $F = \mathrm{C}$, которые сначала изучаются параллельно, имеют каждая свою специфику. Именно, далеко не каждый многочлен $f \in \mathrm{R}[x]$ степени $\geqslant 1$ имеет *действительный* корень (простейший пример: $f(x) = x^2 + 1$.) В то же время, любой многочлен $f \in \mathrm{C}[x], \deg f \geqslant 1$, обязательно имеет *комплексный* корень. Однако целый ряд вопросов решается одинаково как в действительном, так и комплексном случае.

Итак, сначала считаем, что F есть R или C.

Определение 1. *Пусть $f \in F[x]$. Число $c \in F$, для которого $f(c) = 0$, называется корнем многочлена f.*

Таким образом, корень c многочлена $f(x) = a_0 + a_1x + \ldots + a_nx^n, a_i \in F$, определяется с помощью равенства

$$f(c) = a_0 + a_1c + \ldots + a_nc^n = 0, \qquad c \in F.$$

Для многочлена f с действительными коэффициентами правомерен вопрос и о его комплексных корнях; в этом последнем случае мы неизбежно рассматриваем f как элемент $\mathrm{C}[x]$. Очень часто в различных текстах эта тонкость специально не оговаривается.

Определение 1 допускает характеризацию в терминах делимости многочленов, то есть в рамках подхода предыдущих пунктов.

Теорема 1. *Остаток от деления многочлена $f \in F[x]$ на двучлен $x - c$ равен $f(c)$. Таким образом, $x - c$ делит f тогда и только тогда, когда c — корень f.*

Доказательство. По теореме о делении с остатком из пункта 14.2, $f(x) = (x - c)q(x) + r(x)$, $\deg r < \deg(\cdot - c) = 1$. Поэтому $r(x)$ есть число из F, которое может быть найдено путём подстановки $x = c$. В связи с этим получается $f(x) = (x - c)q(x) + f(c)$. Теорема доказана.

Замечание 1. Вторая часть утверждения ($x - c \mid f \iff f(c) = 0$) называется *теоремой Безу.* Кроме этого результата и представления для взаимно простых многочленов из $\mathrm{R}[x]$ (см. следствие 2 пункта 14.3 в ситуации $F = \mathrm{R}$) широко известна и его теорема о точках пересечения алгебраических кривых. Именно, Безу (E. Bezout, 1779) показал, что *две плоские алгебраические кривые порядков m и n имеют максимально $m \cdot n$ общих точек.*

Деление многочлена $f(x)$ на линейный двучлен $x - c$, а значит, и вычисление значения $f(c)$ — остатка при таком делении, может быть выполнено по так называемой *схеме Горнера.*

Пусть $f(x) = (x-c)q(x)+r$, где $f(x) = a_0+a_1x+\ldots+a_nx^n$ — данный многочлен степени n; $r = f(c)$. Тогда $\deg q = n - 1$. Положим $q(x) = b_0 + b_1x + \ldots + b_{n-1}x^n$, тогда

$$a_0 + a_1x + \ldots + a_nx^n = (x - c)(b_0 + b_1x + \ldots + b_{n-1}x^{n-1}) + r.$$

Приравнивая коэффициенты при $x^n, x^{n-1}, \ldots, x, 1$ в обеих частях последнего равенства, получим соотношения:

$$a_n = b_{n-1}, \quad a_{n-1} = b_{n-2} - cb_{n-1}, \quad a_{n-2} = b_{n-3} - cb_{n-2},$$

$$\ldots\ , \quad a_1 = b_0 - cb_1, \quad a_0 = r - cb_0.$$

Перепишем эти равенства таким образом, чтобы иметь возможность последовательно выразить неизвестные коэффициенты $b_{n-1}, b_{n-2}, \ldots, b_0$ и остаток $r = f(c)$ через $a_n, \ldots, a_0, c$.

$$b_{n-1} = a_n, \quad b_{n-2} = a_{n-1} + cb_{n-1}, \quad b_{n-3} = a_{n-2} + cb_{n-2},$$

$$\ldots\ , \quad b_{n-2} = a_1 + cb_1, \quad r = a_0 + cb_0.$$

Вычисления проводят в том порядке, который мы указали. Обычно процесс оформляется в виде двустрочной таблицы, первая строка которой содержит известные числа $a_n, a_{n-1}, \ldots, a_1, a_0$, а вторая — вычисляемые слева направо значения b_{n-1}, b_{n-2}, $\ldots$, b_0, r :

$$\begin{array}{c|cccccc|} & a_n & a_{n-1} & \ldots & a_1 & a_0 \\ c & b_{n-1}=a_n & b_{n-2}=a_{n-1}+cb_{n-1} & \ldots & b_0=a_1+cb_1 & r=a_0+cb_0 \end{array}$$

Пример 1. Выполним деление $f(x) = 2x^5 - x^4 - 3x^3 + 4x^2 - 5x + 1$ на $x + 1$ и найдём, тем самым, $f(-1)$. Предыдущая таблица соответствует $c = -1$ и имеет вид

$$\begin{array}{c|cccccc|} & 2 & -1 & -3 & 4 & -5 & 1 \\ -1 & 2 & -3 & 0 & 4 & -9 & 10 \end{array}$$

Поэтому $f(x) = (x+1)(2x^4 - 3x^3 + 4x - 9) + 10$ и $f(-1) = 10$. Схема Горнера может применяться при решении и ряда других задач.

Замечание 2. Описанный способ по существу совпадает с методом Тянь–юань, применявшимся в средневековом Китае. В начале 19 века он был заново открыт итальянцем П. Руффини (P. Ruffini, 1802) и англичанином У. Горнером (W.G. Horner, 1819), а затем получил имя второго математика.

Характеризация теоремы 1 мотивирует следующее определение.

Определение 2. *Пусть $k \in \mathrm{N}$. Корнем кратности k многочлена $f \in F[x]$ называется такой его корень c, для которого $(x-c)^k \mid f$, но $(x-c)^{k+1}$ не делит f. Корень кратности $k = 1$ называется простым, а кратности $k > 1$ — кратным.*

Для корней кратностей 2 и 3 иногда используют термины *двойной* и *тройной.*

Таким образом, кратность корня c есть максимальный показатель степени двучлена $x - c$, которая делит f.

Очень важно, что кратные корни допускают описание в терминах производных f. Так как мы не располагаем понятием предела, то обычное в анализе определение производной мы заменяем более простым.

Определение 3. *Производной f' многочлена $f(x) = a_0 + a_1x + a_2 + \ldots + a_nx^n$ называется многочлен $f'(x) = a_1 + 2a_2x + \ldots + na_nx^{n-1}$.*

Дифференцирование (переход к производной) в $F[x]$ обладает рядом привычных свойств, легко проверяемых непосредственно.

$$1^\circ.\quad (f+g)' = f' + g'.$$

$$2^\circ.\quad (\lambda f)' = \lambda f',\ \lambda \in F.$$

$$3^\circ.\quad (f \cdot g)' = f' \cdot g + f \cdot g'.$$

$$4^\circ.\quad f' = 0 \iff f \in F.$$

$$5^\circ.\quad f(x) = x \implies f' = 1.$$

Заметим, что f' совпадает с производной f в смысле действительного ($F = \mathrm{R}$) или комплексного ($F = \mathrm{C}$) анализа. Старшие производные многочлена определяются по индукции; мы сохраняем за ними стандартное обозначение.

Упражнение 1. Доказать свойства 1° – 5°.

Упражнение 2. Проверить, что для произвольного многочлена $f \in F[x]$ степени $\leqslant n$ и любого $a \in F$ имеет место равенство

$$f(x) = \sum_{i=0}^{n} \frac{f^{(i)}(a)}{i!}(x-a)^i. \tag{13}$$

Для этого формально продифференцировать $1, 2, \ldots, n$ раз по x равенство $f(x) = \sum b_j(x-a)^j$, полагая затем $x = a$.

Равенство (13) называется *формулой Тейлора* для многочленов — по имени английского математика Брука Тейлора (B. Taylor, 1685 – 1731). Многочисленные и глубокие обобщения этой формулы на классы дифференцируемых функций играют важную роль в анализе.

Теорема 2. *Пусть c является корнем кратности k многочлена f. Тогда c является корнем кратности $k-1$ производной f'.*

Доказательство. По условию,

$$f(x) = (x-c)^k g(x), \qquad g(c) \neq 0.$$

Тогда по свойствам дифференцирования

$$f'(x) = k(x-c)^{k-1}g(x) + (x-c)^k g'(x) =$$

$$= (x-c)^{k-1}\Big(kg(x) + (x-c)g'(x)\Big) = (x-c)^{k-1}h(x).$$

Кроме того, $h(c) = kg(c) \neq 0$. Поэтому c есть корень кратности $k-1$ для f'. Теорема доказана.

Следствие. *Пусть c — корень кратности k многочлена f. Тогда*

$$f(c) = f'(c) = f''(c) = \ldots = f^{(k-1)}(c) = 0, \quad f^k(c) \neq 0. \tag{14}$$

Соотношения (14) получаются после последовательного применения теоремы 2 к многочленам $f, f', f'', \ldots, f^{(k-1)}, f^{(k)}$.

Другое доказательство следствия позволяет дать формула Тейлора (13), см. упражнение 2. Кроме того, (13) гарантирует и справедливость обратного утверждения. *Именно, если выполнены условия (14), то c является корнем кратности k многочлена f в смысле исходного определения 2.* Несложные подробности предоставляются читателю.

Итак, есть два эквивалентных подхода к описанию кратных корней многочлена — через делимость и через производные. Разумное комбинирование этих подходов позволяет получить короткие решения некоторых задач.

Пример 2. Многочлен $f(x) = (x-1)^3(x+1) = x^4 - 2x^3 + 2x - 1$ имеет число $c = 1$ тройным корнем. Действительно, максимальная степень $(x-1)^k$, которая делит f, равна $k = 3$. С другой стороны,

$$f'(x) = 4x^3 - 6x^2 + 2, \quad f''(x) = 12x^2 - 12x, \quad f'''(x) = 24x - 12,$$

$$f(1) = f'(1) = f''(1) = 0, \qquad f'''(1) = 12 \neq 0.$$

Пример 3. Пусть требуется определить $a, b \in \mathrm{R}$ так, чтобы многочлен $f(x) = 2x^3 - ax^2 + b$ делился на $g(x) = (x-2)^2$. Как и в предыдущем примере, $F = \mathrm{R}$.

Можно разделить f на g и приравнять коэффициенты остатка к 0. Вместо этого заметим, что по условию задачи число $c = 1$ является корнем многочлена f кратности не ниже второй. Поэтому должно быть выполнено $f(2) = f'(2) = 0$. Это даёт систему равенств $16 - 4a + b = 0,\ 24 - 4a = 0$, откуда $a = 6, b = 8$.

Рассмотрим теперь вопрос об отделении кратных корней многочлена $f \in F[x]$, имеющий практический интерес. Дело в том, что кратные нули функции являются причиной неэффективной работы ряда вычислительных алгоритмов.

Теорема 3. *Пусть $f \in F[x]$ и $f_1 := (f, f')$. Число c является корнем f кратности $k > 1$ тогда и только тогда, когда c — корень f_1 кратности $k - 1$.*

Доказательство. Из предыдущего следует, что c есть корень f кратности k тогда и только тогда, когда одновременно $(x-c)^{k-1} \mid f'$ и $(x-c)^k$ не делит f'. Последнее эквивалентно тому, что c есть корень кратности $k-1$ для НОД (f, f').

На этой теореме основан метод определения кратностей корней многочлена. Пусть f — данный многочлен, корни которого подвергаются анализу. Составляем ряд многочленов

$$f, \quad f_1 := (f, f'), \quad f_2 := (f_1, f_1'), \quad \ldots\ , \ f_{j+1} := (f_j, f_j') = 1. \tag{15}$$

Из теоремы 2 получаем: f_{j+1} вообще не имеет корней; корни f_j являются простыми; все они являются корнями кратности 2 для f_{j-1} (который имеет, быть может, и другие корни), и т.д. Все *различные* корни f являются корнями многочлена h, являющегося частным от деления f на f_1.

Пример 4. Пусть $f(x) = (x-1)^3(x-2)^2(x-3)$. Тогда

$$f'(x) = 3(x-1)^2(x-2)^2(x-3) + 2(x-1)^3(x-2)(x-3) + (x-1)^3(x-2)^2,$$

$$f_1 = (f, f') = (x-1)^2(x-2), \quad f_1' = 2(x-1)(x-2) + (x-1)^2,$$

$$f_2 = (f_1, f_1') = x - 1, \qquad f_2' = 1, \qquad f_3 = (f_2, f_2') = 1.$$

Поэтому ряд (15) имеет вид

$$f(x), \quad (x-1)^2(x-2), \quad x - 1, \quad 1.$$

Частное от деления f на f_1 есть $h(x) = (x-1)(x-2)(x-3)$. Отсюда $c_1 = 1$, $c_2 = 2$, $c_3 = 3$ — все различные корни f. При этом $c_1 = 1$ — общий для f, f_1, f_2 — имеет кратность 3 как корень f; $c_2 = 2$ — общий для f и f_1, но не являющийся корнем f_2, — имеет кратность 2; наконец, $c_3 = 3$ — простой корень f.

Во второй части этого пункта приведём формулировку теоремы, гарантирующей наличие корня у многочлена $f \in \mathrm{C}[x]$, и ряд следствий этого выдающегося результата.

Теорема 4. *Каждый многочлен $f \in \mathrm{C}[x]$, степень которого $n \geqslant 1$, имеет хотя бы один корень $c \in \mathrm{C}$.*

Это утверждение исторически получило название *основной теоремы алгебры.* Его полное обоснование впервые дал великий Гаусс (C.F. Gauss, 1777 – 1855), который, начиная с 1799 г., опубликовал четыре различных доказательства.

Самое короткое из известных ныне доказательств теоремы 4 использует понятия и результаты теории аналитических функций комплексного переменного (и является самым предпочтительным, если иметь в виду краткость). Более элементарные доказательства базируются на подходе математического анализа, см., например, [13] и [16]. В [13] приведено также алгебраическое доказательство. Мы ограничимся лишь формулировкой этого результата.

Надо отметить, что теорема 4 касается, в первую очередь, структуры поля C комплексных чисел. Именно, она гарантирует, что поле C является *алгебраически замкнутым* в том смысле, что *всякий многочлен степени* $\geqslant 1$ *из соответствующего кольца* $\mathrm{C}[x]$ *разлагается на линейные множители.* Действительно, из теоремы 4 и результатов этого пункта сразу получается следующее важное утверждение.

Теорема 5. *Каждый многочлен* f *из* $\mathrm{C}[x]$ *степени* $n \geqslant 1$ *представляется в виде*

$$f(x) = A(x - c_1)(x - c_2)\dots(x - c_n), \quad A, c_1, c_2, \dots, c_n \in \mathrm{C}, \tag{16}$$

причём среди чисел c_j *могут быть и одинаковые. Разложение (16) является единственным для* f *с точностью до порядка сомножителей.*

Иначе говоря, каждый многочлен из $\mathrm{C}[x]$ *степени* $n \geqslant 1$ *имеет ровно* n *(комплексных) корней с учётом их кратностей.*

Доказательство. По теореме 4, многочлен f имеет комплексный корень c_1. Теорема 1 позволяет записать $f(x) = (x - c_1)g_1(x)$. Если $\deg g \geqslant 1$, то опять по теореме 4 g_1 имеет корень c_2, возможно, совпадающий с c_1; тогда $g_1(x) = (x - c_2)g_3$, и т.д. В конце концов, придём к многочлену $A = g_{n+1}$ степени 0. Собирая все представления вместе, получим разложение (16). Тем самым установлено существование (16). Ясно, что числа $c_1, \dots, c_n$ являются корнями f.

Покажем, что разложение (16) является единственным. Пусть наряду с (16) есть ещё

$$f(x) = B(x - d_1)(x - d_2)\dots(x - d_n), \quad B, d_1, d_2, \dots, d_n \in \mathrm{C}.$$

Тогда в $\mathrm{C}[x]$ имеет место равенство

$$A(x - c_1)(x - c_2)\dots(x - c_n) = B(x - d_1)(x - d_2)\dots(x - d_n).$$

Сравнивая старшие коэффициенты в обеих частях, сразу имеем $A = B$. Далее, для каждого c_i найдётся d_j такое, что $c_i = d_j$, так как если два многочлена равны как элементы $\mathrm{C}[x]$, то они имеют одинаковые значения при всех x и, в частности, одинаковые корни — их нули как функций. Наконец, число множителей $x - c_i$ с одним и тем же c_i слева и справа совпадает — иначе, поделив многочлены на произведение общих множителей, мы пришли бы к равенству двух новых многочленов с различными корнями. Таким образом, рассматриваемые разложения совпадают с точностью до порядка линейных множителей.

Теорема 5 доказана.

Следствие 1. *Каждый многочлен степени* $n \geqslant 1$ *с действительными коэффициентами имеет не более* n *действительных корней (с учётом кратностей).*

Доказательство. Достаточно рассмотреть такой многочлен f как элемент $\mathrm{C}[x]$. У него по теореме 5 ровно n комплексных корней (с учётом кратностей). Ясно, что не все из них должны быть действительными. Поэтому число действительных корней не более n.

Следствие 2. *Два многочлена f, g равны как элементы $F[x]$ тогда и только тогда, когда они совпадают как функции, то есть $f(x) = g(x)$ при всех $x \in F$. Здесь $F = \mathrm{R}$ или C.*

Доказательство. Ясно, что если $f = g$ в кольце $F[x]$, то $f(x) = g(x), x \in F$ (все коэффициенты f и g, а значит, и их значения совпадают). Пусть $f(x) = g(x)$ при всех x. Тогда $f(x) - g(x) = 0, x \in F$, то есть многочлен $f - g \in F[x]$ имеет бесконечное число корней. По теореме 5 число корней любого ненулевого многочлена ограничено его степенью. Поэтому обязательно $f - g = 0$ в $F[x]$.

Упражнение 3. Пусть $f(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + x^n$ — многочлен со старшим коэффициентом 1. Доказать, используя (16), следующие формулы Виета, выражающие коэффициенты f через его корни $c_1, c_2, \ldots, c_n$:

$$
\begin{aligned}
&a_{n-1} = -(c_1 + c_2 + \ldots + c_n),\\
&a_{n-2} = c_1c_2 + c_1c_3 + \ldots + c_1c_n + c_2c_3 + \ldots + c_{n-1}c_n,\\
&a_{n-3} = -(c_1c_2c_3 + c_1c_2c_4 + \ldots + c_{n-2}c_{n-1}c_n),\\
&\ldots \quad \ldots \quad \ldots \quad \ldots\\
&a_1 = (-1)^{n-1}(c_1c_2\ldots c_{n-1} + c_1c_2\ldots c_{n-2}c_n + \ldots + c_2c_3\ldots c_n),\\
&a_0 = (-1)^n c_1c_2\ldots c_n.
\end{aligned}
$$

Эти формулы названы именем Франсуа Виета (F. Viete, 1540 –1603).

Упражнение 4. Написать формулы Виета для $n = 2, 3$ и 4.

Равенство (16) записывают чаще в свёрнутом виде:

$$f(x) = A(x - c_1)^{k_1}(x - c_2)^{k_2}\ldots(x - c_m)^{k_m}. \tag{17}$$

В (17) m — число всех *различных* корней многочлена f, которые мы обозначили $c_1, \ldots, c_m$. Натуральные числа k_j обозначают кратности c_j; очевидно, $\sum k_j = n$. Представление (17) получается из (16) после переобозначения корней и объединения одинаковых множителей.

Разложение (17) является единственным с точностью до порядка множителей. Это также следует из теоремы 5.

Замечание 3. Теоремы 1 – 3 этого пункта допускают обобщение на кольцо многочленов $K[x]$, где K — произвольное поле (в аналоге теоремы 3 поле K имеет бесконечную характеристику).

14.5. Неприводимые многочлены

В этом пункте сначала мы опять считаем $F = \mathrm{R}$ или C, но затем будем рассматривать эти две ситуации отдельно; каждая из них имеет особенности.

Роль неприводимых многочленов в кольце $F[x]$ аналогична роли простых чисел в кольце Z.

Определение. *Неприводимым называется многочлен $f \in F[x]$ положительной степени, который не представляется в виде*

$$f = g \cdot h, \qquad 0 < \deg g < \deg f, \quad 0 < \deg h < \deg f.$$

Примеры. 1. Многочлены вида $f(x) = ax + b, a \neq 0$, неприводимы в $F[x]$. Это следует непосредственно из определения.

2. Многочлен $f(x) = x^2 + 1$ не является неприводимым в $\mathrm{C}[x]$ (или, как ещё говорят, над полем C). Действительно, $x^2 + 1 = (x + \mathbf{i})(x - \mathbf{i})$.

3. Тот же многочлен является неприводимым в $\mathrm{R}[x]$ (или, как говорят, над полем R). Если бы было $(ax + b)(cx + d) = x^2 + 1$, то обязательно $ac = bd = 1, bc = -ad$. После простых преобразований получаем $-a^2d = b^2d$, откуда либо $d = 0$, либо $-a^2 = b^2$, то есть $a = b = 0$. Оба эти варианта, как нетрудно понять, неприемлемы.

Можно заметить также, что $f(x) = x^2+1$ не имеет действительных корней, в то время, как $\varphi(x) = (ax+b)(cx+d)$ имеет корни $-b/a, -d/c$. В связи с этим равенство $f = \varphi$ в $\mathrm{R}[x]$ невозможно.

Немного позднее мы отметим простые критерии неприводимости над R и над C.

Теорема 1. *Пусть $f \in F[x]$ — неприводимый и $g \in F[x]$ — произвольный многочлены. Тогда $f \mid g$ или $(f, g) = 1$, причём эти варианты не осуществляются одновременно.*

Доказательство. Покажем, что случай $f \mid g, (f, g) = 1$ невозможен. Если $f \mid g$, то $(f, g) = f$. Но, так как f — неприводимый, то $\deg f > 0$. Это противоречит условию $(f, g) = 1$. Что и требовалось доказать.

Напомним, что *нормированным* мы называем многочлен, старший коэффициент которого равен 1.

Теорема 2. *Для каждого многочлена $f \in F[x]$, $\deg f > 0$, существуют такие натуральные числа k, $\alpha_1, \ldots, \alpha_k$, число $c \in F$ и неприводимые нормированные многочлены $p_1, \ldots, p_k$, что*

$$f(x) = cp_1(x)^{\alpha_1} \cdot \ldots \cdot p_k(x)^{\alpha_k}. \tag{18}$$

Разложение (18) является единственным для f с точностью до порядка сомножителей.

Доказательство. Существование разложения (18) устанавливается индукцией по степени $n = \deg f$. В случае $n = 1$ (18) имеет вид $f = cp$. Здесь c — старший коэффициент f; многочлен p получен нормировкой из f. Число сомножителей $k = = 1$.

Пусть существование (18) обосновано для всех многочленов степени $0 < \deg f < n$, где $n > 1$. Докажем, что (18) справедливо для многочленов степени n. Пусть f — произвольный такой многочлен. Если f является неприводимым, то (18) опять имеет вид $f = cp$, отмеченный выше. Если же f не является неприводимым, то $f = gh$, причём $\deg g, \deg h < n$. По предположению индукции, разложения вида (18) для g и h существуют. Совмещая их и объединяя, если нужно, одинаковые множители, мы получим представление (18) для f.

Докажем единственность (18). Пусть

$$cp_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} = dq_1^{\beta_1} \cdot \ldots \cdot q_m^{\beta_m} \tag{19}$$

для неприводимых нормированных $q_1, \ldots, q_m$ и натуральных $\beta_1, \ldots, \beta_m$. Равенство $c = d$ следует из сравнения старших коэффициентов в обеих частях (19).

Покажем, что для любого i найдётся j такое, что $p_i = q_j, \alpha_i = \beta_j$. Возьмём $i = 1$. Заметим, что p_1 — неприводимый многочлен, который делит правую часть (19). Равенства $(p_1, q_1) = \ldots = (p_1, q_m) = 1$ не могут выполняться одновременно, так как тогда p_1 был бы взаимно простым со всей правой частью (следствие 3 из пункта 14.3). Значит, для некоторого j выполнено $(p_1, q_j) \neq 1$. Привлекая теорему 1 этого пункта, получаем, что $p_1 \mid q_j$. Неприводимость и нормированность q_j дают теперь $p_1 = q_j$. Поэтому

$$cp_1^{\alpha_1} \cdot \prod_{s=2}^{k} p_s^{\alpha_s} = cp_1^{\beta_j} \cdot \prod_{s \neq j}^{m} q_s^{\beta_s}.$$

Предположим, что $\alpha_1 < \beta_j$. Тогда

$$cp_1^{\alpha_1} \Big(\prod_{s=2}^{k} p_s^{\alpha_s} - p_1^{\beta_1 - \alpha_1} \cdot \prod_{s \neq j}^{m} q_s^{\beta_s} \Big) = 0.$$

Так как $p_1 \neq 0$, то

$$\prod_{s=2}^{k} p_s^{\alpha_s} = p_1^{\beta_1 - \alpha_1} \cdot \prod_{s \neq j}^{m} q_s^{\beta_s}.$$

В связи с последним равенством p_1 делит его левую часть. Но многочлен p_1 взаимно прост с $p_2, \ldots, p_k$, поэтому он взаимно прост и с их произведением. Тем самым, последнее равенство не может иметь места. Мы показали, что неравенство $\alpha_1 < \beta_j$ ведёт к противоречию. Аналогично, невозможным является и соотношение $\alpha_1 > \beta_j$. Поэтому для рассматриваемого j выполнено $\alpha_1 = \beta_j$.

Теперь от (19) мы переходим к равенству произведений, содержащих $k - 1$ и $m - 1$ сомножителей, не включающих p_1. Если бы выполнялось $m \neq k$, то, действуя подобным образом, мы пришли бы к невозможному равенству, в котором произведение многочленов ненулевой степени равнялось бы 1. Таким образом, $m = k$. Тогда описанный процесс позволяет установить идентичность каждого из p_i с некоторым q_s и равенство соответствующих степеней.

Теорема доказана.

Дадим теперь характеризацию неприводимых многочленов из $\mathrm{C}[x]$ и $\mathrm{R}[x]$. Здесь имеется некоторая разница, не касающаяся, однако, того факта, что многообразие степеней неприводимых многочленов в обоих случаях весьма невелико.

Приводимый ниже результат следует из основной теоремы алгебры (пункт 14.4, теорема 4).

Теорема 3. *Пусть f — неприводимый многочлен из $F[x]$. Если $F = \mathrm{C}$, то $\deg f = 1$. Если $F = \mathrm{R}$, то $\deg f \leqslant 2$, причём в случае $\deg f = 2$ квадратичный многочлен f не имеет действительных корней (имеет отрицательный дискриминант).*

Наоборот, все многочлены степени 1 неприводимы над C и над R. Кроме линейных, неприводимыми над R являются все квадратичные многочлены отмеченного вида.

Доказательство. Пусть $F = \mathrm{C}$. Так как $\deg f \geqslant 1$, то по теореме 5 предыдущего пункта f разлагается в произведение многочленов первой степени, см. (16) и (17). Тем самым, в случае $\deg f > 1$ многочлен f не является неприводимым. В то же время, каждый многочлен степени 1 является неприводимым по определению.

Пусть $F = \mathrm{R}$. По основной теореме алгебры (см. пункт 14.4, теорема 4), так как $\deg f \geqslant 1$, существует $\lambda \in \mathrm{C}$ такое, что $f(\lambda) = 0$. Возможны две ситуации: $\lambda \in \mathrm{C}$ и $\lambda \in \mathrm{C} \setminus \mathrm{R}$.

Предположим сначала, что $\lambda \in \mathrm{R}$. Тогда $x - \lambda \mid f(x)$, то есть $f(x) = (x - \lambda)g(x), g \in \mathrm{R}[x]$ (теорема 1 из пункта 14.4). Так как f — неприводимый, то $\deg g = 0$. Это означает, что $f(x) = \alpha(x - \lambda), \alpha \neq 0$, и $\deg f = 1$. С другой стороны, по определению, любой многочлен первой степени является неприводимым над R.

Пусть теперь $\lambda \in \mathrm{C} \setminus \mathrm{R}$. Прежде всего, заметим, что число $\overline{\lambda}$, комплексно сопряжённое с λ, также является корнем f. Это следует из равенств

$$f(\overline{\lambda}) = \overline{f(\lambda)} = \overline{0} = 0.$$

Самое левое из них связано с тем, что f — многочлен с действительными коэффициентами (совпадающими с сопряжёнными себе).

Рассмотрим в этом месте f как элемент $\mathrm{C}[x]$. Оба линейных многочлена $x - \lambda$ и $x - \overline{\lambda}$ делят f в этом кольце. Так как они взаимно просты, то и их произведение $h(x) = (x - \lambda)(x - \overline{\lambda})$ также делит f (следствие 3 из пункта 14.3). Итак, в $\mathrm{C}[x]$ выполнено $f(x) = h(x)\varphi(x)$. Коэффициенты многочлена h являются действительными:

$$h(x) = (x - \lambda)(x - \overline{\lambda}) = x^2 - (\lambda + \overline{\lambda})x + \lambda \cdot \overline{\lambda} = x^2 - (2\mathrm{Re}\lambda)x + |\lambda|^2.$$

Отсюда следует, что φ — также многочлен с действительными коэффициентами. (Достаточно выполнить деление с остатком f на h в кольце $\mathrm{R}[x]$ и сравнить этот результат с аналогичным делением в $\mathrm{C}[x]$, которое даёт остаток $r = 0$; однозначность результата гарантирует $\varphi \in \mathrm{R}[x]$.)

Итак, в $\mathrm{R}[x]$ имеет место $f = h\varphi$, $\deg h = 2$. Так как f — неприводимый, то $\deg \varphi = 0$, и f — многочлен степени 2. Как было сказано, h, а значит, и f не имеют действительных корней.

Для завершения доказательства остаётся заметить, что каждый квадратичный многочлен без действительных корней является неприводимым, так как не раскладывается на множители степени 1 над R.

Теорема 3 полностью доказана.

Замечание. Приведённое выше доказательство теоремы 2 не привлекает основной теоремы алгебры о существовании корня многочлена из $\mathrm{C}[x]$, а доказательство теоремы 3 существенно использует этот результат.

Теорему 2 (о разложении в произведение неприводимых) мы фактически доказали ещё в предыдущем пункте, см. разложения (16) – (17), применив основную теорему алгебры. В конце пункта 14.4 был рассмотрен комплексный вариант. Разложение над R может быть получено из (16) объединением линейных множителей с попарно сопряжёнными комплексными корнями многочлена $f \in \mathrm{R}[x]$. При этом получаются квадратичные множители, не имеющие действительных корней, как при доказательстве теоремы 3 этого пункта.

Причина, по которой выше было дано иное обоснование теоремы 2, независимое от основной теоремы алгебры, заключается в степени общности этого доказательства.

Именно, *как определение неприводимых, так и аналог теоремы 2 о разложении в их произведение переносятся на кольцо многочленов $K[x]$ над произвольным полем K*. Уточнения здесь самые минимальные — схема доказательства работает именно в этом общем случае.

Теорема 3 гарантирует, что *степени многочленов, неприводимых над* R *или над* C, *ограничены*. Использование в этом месте вместо R или C произвольного поля K недопустимо — тогда утверждение перестаёт быть верным. Так, над любым *конечным* полем (например, полем вычетов $\mathrm{Z_p}, p$ — простое) существуют неприводимые многочлены *сколь угодно большой степени*. Несложное доказательство этого факта дано в [13, с. 198].

Отметим также, что с неприводимыми многочленами из $K[x]$, где поле K не совпадает с C или R и, в частности, является конечным, связан ряд разделов *прикладной*, или как теперь говорят, *компьютерной алгебры*, см. по этому поводу, например, [1], [10], [18], [20] и библиографию в этих книгах.

14.6. Интерполяция многочленами. Формулы Лагранжа и Ньютона

Задача полиномиальной интерполяции уже рассматривалась в пункте 4.6 в связи с определителем Вандермонда. Здесь, тем не менее, мы повторим её постановку и опишем основные методы её решения.

Постановка задачи интерполяции заключается в следующем. Как и ранее, $F = \mathrm{R}$ или $F = \mathrm{C}$. Наиболее употребителен первый случай.

Пусть $x_0, x_1, \ldots, x_n \in F$ — попарно различные *узлы интерполяции*, $b_0, b_1, \ldots, b_n \in F$ — произвольные числа. Требуется найти многочлен $f \in F[x]$ степени $\leqslant n$ такой, что

$$f(x_k) = b_k, \quad k = 0, 1, \ldots, n. \tag{20}$$

Требование $\deg f \leqslant n$ обеспечивает единственность решения. В сформулированном виде задача интерполяции является вполне корректной. Именно, *существует единственный многочлен f степени $\leqslant n$ такой, что выполнены равенства (20).*

Эта теорема была доказана в пункте 4.6 с помощью перехода к системе линейных уравнений относительно неизвестных коэффициентов f. Так как определитель этой системы является определителем Вандермонда для попарно различных узлов $x_0, x_1, \ldots, x_n$, то он отличен от нуля, что обеспечивает существование и единственность решения.

Здесь мы дадим иное обоснование этого факта. Именно, единственность решения задачи интерполяции следует из основной теоремы алгебры. Пусть f и g — два многочлена степени $\leqslant n$, для которых $f(x_k) = g(x_k) = 0$ при всех k. Тогда $f - g$ обращается в нуль в $(n+1)$-й точке x_k. Но ненулевой многочлен степени n имеет не более n корней (в комплексной ситуации — ровно n корней, см. пункт 14.4). В связи с этим обязательно $f = g$.

Итак, если задача интерполяции имеет решение, то это решение единственно. Существование следует из явной формулы, называемой *интерполяционной формулой Лагранжа* (J.L. Lagrange, 1795):

$$f(x) = \sum_{i=0}^{n} b_i L_i(x) \ ; \quad L_i(x) := \prod_{j \neq i} \frac{x - x_j}{x_i - x_j} \ , \ i = 0, 1, \ldots, n. \tag{21}$$

Многочлены Лагранжа $L_i \in F[x]$ обладают важными свойствами

$$\deg L_i = n, \qquad L_i(x_k) = \delta_{ik},$$

δ_{ik} — символ Кронекера. Поэтому, если $f(x)$ имеет вид (21), то $f \in F[x]$, $\deg f \leqslant n$ и

$$f(x_k) = \sum_{i=0}^{n} b_i L_i(x_k) = \sum_{i=0}^{n} b_i \delta_{ik} = b_k.$$

Укажем ещё один способ построения интерполяционного многочлена, основанный на *формуле Ньютона.* Она имеет следующий вид (I. Newton, опубликовано в 1736 г.):

$$f(x) = u_0 + u_1(x - x_0) + u_2(x - x_0)(x - x_1) + \ldots + \\ + u_n(x - x_0) \cdot \ldots \cdot (x - x_{n-1}). \tag{22}$$

Коэффициенты $u_0, u_1, \ldots, u_n$ представляют собой так называемые *разделённые разности,* построенные по наборам (b_j) и (x_j). Более элементарным является способ последовательного нахождения u_j в процессе подстановки в (22) значений $x = x_j$. Нетрудно понять, что в этом случае получается система

$$f(x_0) = b_0 = u_0,$$
$$f(x_1) = b_1 = u_0 + u_1(x_1 - x_0),$$
$$f(x_2) = b_2 = u_0 + u_1(x_2 - x_0) + u_2(x_2 - x_0)(x_2 - x_1),$$
$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$
$$f(x_n) = b_n = u_0 + u_1(x_n - x_0) + \ldots + u_n(x_n - x_0) \cdot \ldots \cdot (x_n - x_{n-1}),$$

из которой и находятся неизвестные множители $u_0, u_1, \ldots, u_n$.

Пример 1. Пусть $F = \mathrm{R}$. Рассмотрим интерполяционную задачу

$$f(-1) = -6, f(1) = 4, f(2) = 9, f(3) = 22, \quad \deg f \leqslant 3.$$

Она соответствует узлам $x_0 = -1, x_1 = 1, x_2 = 2, x_3 = 3$ и значениям $b_0 = -6$, $b_1 = 4$, $b_2 = 9$, $b_3 = 22$. Для нахождения f применим формулу Лагранжа.

$$L_0(x) = \frac{(x - x_1)(x - x_2)(x - x_3)}{(x_0 - x_1)(x_0 - x_2)(x_0 - x_3)} = \\ = \frac{(x-1)(x-2)(x-3)}{(-1-1)\cdot(-1-2)\cdot(-1-3)} = -\frac{(x-1)(x-2)(x-3)}{24},$$

$$L_1(x) = \frac{(x-x_0)(x-x_2)(x-x_3)}{(x_1-x_0)(x_1-x_2)(x_1-x_3)} =$$
$$= \frac{(x+1)(x-2)(x-3)}{(1-(-1))\cdot(1-2)\cdot(1-3)} = \frac{(x+1)(x-2)(x-3)}{4},$$

$$L_2(x) = \frac{(x-x_0)(x-x_1)(x-x_3)}{(x_2-x_0)(x_2-x_1)(x_2-x_3)} =$$
$$= -\frac{(x+1)(x-1)(x-3)}{(2-(-1))\cdot(2-1)\cdot(2-3)} = -\frac{(x+1)(x-1)(x-3)}{3},$$

$$L_3(x) = \frac{(x-x_0)(x-x_1)(x-x_2)}{(x_3-x_0)(x_3-x_1)(x_3-x_2)} =$$
$$= \frac{(x+1)(x-1)(x-2)}{(3-(-1))\cdot(3-1)\cdot(3-2)} = \frac{(x+1)(x-1)(x-2)}{8}.$$

В соответствии с (21)

$$f(x) = -6L_0(x) + 4L_1(x) + 9L_2(x) + 22L_3(x) =$$
$$= \frac{1}{4}(x-1)(x-2)(x-3) + (x+1)(x-2)(x-3) -$$
$$-3(x+1)(x-1)(x-3) + \frac{11}{4}(x+1)(x-1)(x-2) =$$
$$= x^3 - 2x^2 + 4x + 1.$$

Пример 2. Решим ту же задачу с использованием формулы Ньютона (22). Неизвестный многочлен ищется в виде

$$f(x) = u_0 + u_1(x+1) + u_2(x+1)(x-1) + u_3(x+1)(x-1)(x-2).$$

Полагая последовательно $x = -1, x = 1, x = 2, x = 3$, получим систему уравнений:

$$-6 = u_0,$$
$$4 = u_0 + 2u_1,$$
$$9 = u_0 + 3u_1 + 3u_2,$$
$$22 = u_0 + 4u_1 + 8u_2 + 8u_3.$$

Её решение $u_0 = -6, u_1 = 5, u_2 = 0, u_3 = 1$. Поэтому

$$f(x) = -6 + 5(x+1) + (x+1)(x-1)(x-2) = x^3 - 2x^2 + 4x + 1.$$

В специальных разделах анализа и его приложений рассматриваются *вопросы аппроксимации функций с помощью интерполяционных многочленов*, см., например, [19]. Здесь мы не будем останавливаться на этой тематике.

14.7. Локализация корней многочлена

Проблема локализации корней многочлена связана с указанием областей на действительной прямой или комплексной плоскости, содержащих те или иные (а чаще всего — все) корни данного многочлена f. Естественно, ответ должен быть дан в терминах коэффициентов f. Задачи такого типа весьма многообразны, и ниже описываются лишь некоторые из них.

Наше изложение имеет обзорный характер; мы ограничиваемся лишь формулировкой результатов, примерами и некоторыми упражнениями.

В первой части пункта рассматривается вопрос о локализации действительных корней многочлена $f \in \mathrm{R}[x]$.

Во второй части приводятся результаты о локализации собственных значений действительной или комплексной матрицы порядка n, то есть корней её характеристического многочлена. Этот частный случай общей задачи имеет очень важные приложения.

Пусть $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathrm{R}[x],\ a_n \neq 0$. Положим $A := \max\{|a_0|, \ldots, |a_{n-1}|\}$. Нетрудно показать, что все действительные корни f принадлежат области

$$U := \{x \in \mathrm{R} :\ |x| \leqslant \frac{A}{|a_n|} + 1\ \}. \tag{23}$$

Упражнение 1. Доказать, что все корни многочлена f принадлежат области (23).

Пусть теперь $a_n > 0$. Обозначим через m наибольший индекс, для которого $a_m < 0$, через B — максимальное значение модуля неотрицательных коэффициентов f. Каждый *положительный* корень c многочлена f удовлетворяет соотношению

$$c \leqslant 1 + \sqrt[n-m]{\frac{B}{a_n}} \tag{24}$$

По поводу доказательства см. [16, с. 244].

Упражнение 2. Показать, что верхние границы C_1, C_2, C_3 для положительных корней многочленов

$$\varphi_1(x) := x^n f(\frac{1}{x}), \quad \varphi_2(x) := f(-x), \quad \varphi_3(x) := x^n f(-\frac{1}{x})$$

могут быть использованы для получения нижней оценки положительных корней, а также нижней и верхней оценок для отрицательных корней многочлена f. Именно, проверить, что $1/C_1$ будет нижней границей положительных корней, а $-C_2$ и $-1/C_3$ — соответственно нижней и верхней границами отрицательных корней f.

Пример 1. Пусть

$$f(x) = (x+1)(x-1)(x-2)(x-3) = x^4 - 5x^3 + 5x^2 + 5x - 6.$$

Точные значения корней f равны $-1, 1, 2, 3$. Для этого многочлена $n = 4$, $a_4 = = 1$, $A = \max\{|a_0|, |a_1|, |a_2|, |a_3|\} = 6$. Таким образом, область U локализации всех корней f, см. (23), задаётся неравенством $|x| < 7$.

Число m из (24) равно 3. Поэтому оценка для положительных корней f имеет вид $c < 1 + 6/1 = 7$.

Получим оценки для отрицательных корней многочлена f по методу упражнения 2. Сначала найдём

$$\varphi_2(x) := f(-x) = x^4 + 5x^3 + 5x^2 - 5x - 6,$$

$$\varphi_3(x) := -x^4 f(-\frac{1}{x}) = 6x^4 + 5x^3 - x^2 - 5x - 1.$$

Верхние границы для положительных корней многочленов φ_2 и φ_3, получаемые с помощью (24), равны

$$C_2 = 1 + \sqrt[3]{\frac{6}{1}} = 1 + \sqrt[3]{6}, \quad C_3 = 1 + \sqrt{\frac{5}{6}}.$$

Поэтому отрицательные корни f лежат в пределах

$$-2.8172 \approx -C_2 < x < -\frac{1}{C_3} \approx -0.5228.$$

Немаловажным является вопрос о количестве корней многочлена, принадлежащих данной области. Оценки сверху для числа отрицательных и положительных действительных корней получаются из соображений, подмеченных ещё Декартом (R. Descartes, 1637).

Определение. *Пусть*

$$a_n,\ a_{i_1},\ a_{i_2},\ \ldots\ ,\ a_{i_q} \tag{25}$$

— все ненулевые коэффициенты многочлена $f \in \mathrm{R}[x]$, $n > i_1 > \ldots > i_q \geqslant 0$. *Если* $a_{i_k} a_{i_{k+1}} < 0$, *будем говорить, что на* $(k+1)$*-м коэффициенте в (25) имеет место перемена знака. Общее число перемен знака в последовательности (25) обозначается* $L(f)$.

Ясно, что всегда $0 \leqslant L(f) \leqslant \deg f$. Если $L(f) = 0$, то, очевидно, f не имеет положительных корней. С другой стороны, f может не иметь положительных корней даже в ситуации $L(f) = \deg f$ (пример: $f(x) = x^2 - x + 1$). Однако величина $L(f)$ имеет прямое отношение к количеству положительных корней f. Следующий результат называют *правилом знаков Декарта*.

Теорема 1. *Число* N *положительных корней многочлена* $f \in \mathrm{R}[x]$ *совпадает с числом* $L(f)$ *или меньше последнего на чётное число. Таким образом, всегда* $N \leqslant L(f)$.

В случае, когда есть дополнительная информация о корнях f, это утверждение может быть существенно уточнено. Мы сохраняем обозначения теоремы 1.

Теорема 2. *Пусть все корни* f *являются действительными. Тогда имеет место равенство* $N = L(f)$.

Наконец, отметим важное утверждение о числе корней многочлена f в фиксированном интервале (a, b). Оно является частным случаем так называемой *теоремы Бюдана – Фурье*.

Теорема 3. *Пусть все корни* f *действительны. Тогда число* M *корней, принадлежащих интервалу* (a, b), *равно* $M = L(f_a) - L(f_b)$, *где*

$$f_a(x) := f(x+a) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!} x^k, \quad f_b(x) := f(x+b) = \sum_{k=0}^{n} \frac{f^{(k)}(b)}{k!} x^k.$$

Таким образом, $M = W - V$, где W есть число перемен знака в ряду

$$f(a), \quad f'(a), \quad \dots \quad , \quad f^{(n)}(a),$$

а V — число перемен знака в ряду

$$f(b), \quad f'(b), \quad \dots \quad , \quad f^{(n)}(b).$$

Доказательства теорем 2 – 3 даются, например, в учебнике [13].

Пример 2. Опять рассмотрим многочлен $f(x) = (x+1)(x-1)(x-2)(x-3) = x^4 - 5x^3 + 5x^2 + 5x - 6$. Число $L(f)$ перемен знака в ряду его коэффициентов $1, -5, 5, 5, -6$ равно 3. Поэтому f имеет три положительных корня, что соответствует теореме 2.

Определим число M корней, принадлежащих интервалу $(0, 4)$, располагая информацией о том, что все корни f действительны. Для этого вычислим последовательно $f(0) = -6, \quad f(4) = 30;$

$$f'(x) = 4x^3 - 15x^2 + 10x + 5, \qquad f'(0) = 5, \quad f'(4) = 61;$$

$$f''(x) = 12x^2 - 30x + 10, \qquad f''(0) = 10, \quad f''(4) = 82;$$

$$f'''(x) = 24x - 30, \qquad f'''(0) = -30, \quad f'''(4) = 66;$$

$$f^{(4)}(x) = 24, \qquad f^{(4)}(0) = 24, \quad f^{(4)}(4) = 24.$$

Число V перемен знака в ряду $-6, 5, 10, -30, 24$ равно 3. (Так как $a = 0$, то для определения V можно было взять и набор коэффициентов f.) Число W перемен знака в ряду $30, 61, 82, 66, 24$ равно 0. Поэтому $M = 3 - 0 = 3$. Это соответствует точным значениям корней $1, 2, 3$.

Во второй части этого пункта мы дадим обзор некоторых результатов о локализации комплексных корней многочлена f, который является *характеристическим многочленом* некоторой действительной или комплексной матрицы $\mathbf{A} \in M_n$. Это означает, что $f(\lambda) = |\mathbf{A} - \lambda\mathbf{E}|$, $\mathbf{E}$ — единичная матрица порядка n.

Тем самым, мы одновременно рассматриваем *вопрос о локализации собственных значений* данной матрицы $\mathbf{A} = (a_{ij})$, которые и являются корнями её характеристического многочлена. Для них мы используем привычное обозначение λ. По поводу определения и свойств характеристического многочлена см. пункт 9.2.

Доказательства теорем 4 – 7 содержатся, например, в монографии Р. Хорна, Ч. Джонсона [26]. Из этой же книги взяты предлагаемые ниже упражнения 2 – 5.

Прежде всего отметим теорему о так называемых *кругах Гершгорина.* Этот результат получен С. Гершгорином (S. Geršgorin, 1931).

Теорема 4. *Пусть* $\mathbf{A} \in M_n$ *и*

$$R_i := \sum_{j=1, j\neq i}^{n} |a_{ij}|, \qquad 1 \leqslant i \leqslant n.$$

Все собственные значения $\mathbf{A}$ *заключены в объединении кругов*

$$G(\mathbf{A}) := \bigcup_{i=1}^{n} \{z \in \mathrm{C} : \ |z - a_{ii}| \leqslant R_i(\mathbf{A})\}.$$

Кроме того, если объединение k из этих кругов есть связная область, не пересекающаяся с остальными $n-k$ кругами, то в ней находятся ровно k собственных значений матрицы $\mathbf{A}$.

Поскольку $\mathbf{A}$ и $\mathbf{A}^T$ имеют одни и те же собственные значения, то справедлив и следующий столбцовый вариант теоремы 4.

Теорема 5. *Пусть* $\mathbf{A} \in M_n$ *и*

$$Q_j := \sum_{i=1, i\neq j}^{n} |a_{ij}|, \qquad 1 \leqslant j \leqslant n.$$

Все собственные значения $\mathbf{A}$ *заключены в объединении кругов*

$$G(\mathbf{A}^T) := \bigcup_{j=1}^{n} \{z \in \mathrm{C} : \ |z - a_{jj}| \leqslant Q_j\}.$$

Кроме того, если объединение k из этих кругов есть связная область, не пересекающаяся с остальными $n-k$ кругами, то в ней находятся ровно k собственных значений матрицы $\mathbf{A}$.

Упражнение 3. Из теорем 4 – 5 получается, что все собственные значения $\mathbf{A}$ *принадлежат пересечению* $G(\mathbf{A}) \bigcap G(\mathbf{A}^T)$. *Проиллюстрировать это на примере матрицы порядка 3 с элементами* $a_{ij} := i/j$.

Обозначим через $\varrho(\mathbf{A})$) *спектральный радиус* $\mathbf{A}$, то есть максимальное значение $|\lambda|$, λ — собственное значение $\mathbf{A}$. Из теорем Гершгорина следует, что

$$\varrho(\mathbf{A}) \leqslant \min\Big\{\max_i \sum_{j=1}^{n} |a_{ij}|, \max_j \sum_{i=1}^{n} |a_{ij}|\Big\}. \tag{26}$$

Эти оценки могут быть улучшены из следующих соображений. Пусть $\mathbf{D} = \mathrm{diag_n}(p_1, \ldots, p_n), p_i > 0$. Известно, что матрицы $\mathbf{A}$ и $\mathbf{D}^{-1}\mathbf{A}\mathbf{D}$ имеют одни и те же собственные значения. Так как $\mathbf{D}^{-1}\mathbf{A}\mathbf{D} = (p_j a_{ij}/p_i)$ (убедитесь в этом самостоятельно), то из (26) получаются также неравенства:

$$\varrho(\mathbf{A}) \leqslant \min_{p_1,\ldots,p_n>0} \max_i \frac{1}{p_i} \sum_{j=1}^{n} p_j |a_{ij}|,$$

$$\varrho(\mathbf{A}) \leqslant \min_{p_1,\ldots,p_n>0} \max_j p_j \sum_{i=1}^{n} \frac{1}{p_i} |a_{ij}|.$$

Упражнение 4. Для матрицы

$$\mathbf{A} = \begin{pmatrix} 7 & -16 & 8 \\ -16 & 7 & -8 \\ 8 & -8 & -5 \end{pmatrix}$$

извлечь из теорем 4 – 5 максимум информации о расположении собственных значений и величине $\varrho(\mathbf{A})$. *Затем рассмотреть матрицы вида* $\mathbf{D}^{-1}\mathbf{A}\mathbf{D}$, *где* $\mathbf{D} = \mathrm{diag_3}(p_1, p_2, p_3)$, *и выяснить, можно ли улучшить результаты локализации. Наконец, вычислить точно собственные значения* $\mathbf{A}$. *Прокомментировать результаты.*

Сформулируем ещё два обобщения теорем 4 – 5. Теорема 6 принадлежит Островскому (A. Ostrowski), теорема 7 — Брауэру (A. Brauer). Мы пользуемся предыдущими обозначениями.

Теорема 6. *Пусть* $\mathbf{A} \in M_n$ *и* $\alpha \in [0,1]$. *Все собственные значения* $\mathbf{A}$ *принадлежат объединению* n *кругов*

$$\bigcup_{i=1}^{n} \{z \in \mathrm{C} : \ |z - a_{ii}| \leqslant R_i^{\alpha} Q_i^{1-\alpha}\}.$$

Упражнение 5. Для $\mathbf{A} = \begin{pmatrix} 1 & 4 \\ 1 & 6 \end{pmatrix}$ *сравнить области теорем 4, 5 и теоремы 6, взяв* $\alpha = 1/2$.

Упражнение 6. Получить оценку для $\varrho(\mathbf{A})$ *с помощью теоремы Островского и сравнить её с (26).*

Теорема 7. *Все собственные значения* $\mathbf{A}$ *принадлежат следующему объединению* $n(n-1)/2$ *множеств, называемых овалами Кассини:*

$$\bigcup_{i,j=1}^{n} \{z \in \mathrm{C} : \ |z - a_{ii}||z - a_{jj}| \leqslant R_i R_j\}.$$

Упражнение 7. Провести численное сравнение приведённых оценок для локализации собственных значений с помощью компьютера.

14.8. Дополнение. О роли многочленов в теории приближения

В силу своего простого строения, многочлены играют исключительно важную роль в длинном ряде разделов математики, в частности, в анализе и его многочисленных приложениях. Эта тема является поистине необъятной; поэтому мы ограничимся лишь той областью анализа, которая называется *теорией приближения, или теорией аппроксимации.* Это в полной мере соответствует вкусам автора. Однако и здесь мы рассмотрим лишь отдельные примеры.

Материал этого пункта является дополнительным и предназначается для заинтересованных читателей.

В определённом смысле теория аппроксимации занимается приближённым представлением функций и закономерностями, связанными с таким представлением. Многочлены (от одного и нескольких переменных) играют фундаментальную роль в этой науке, с одной стороны, как самостоятельный аппарат приближения и, с другой стороны, как база для построения более совершенных средств — рациональных функций, кусочно-полиномиальных функций и сплайнов.

Фундаментальную роль многочленов в теории приближения иллюстрирует следующая теорема Вейерштрасса (K. Weirstraass, 1885). *Каждая непрерывная на конечном отрезке функция может быть с любой точностью равномерно приближена алгебраическими многочленами.* Более точно, для непрерывной $f : [a,b] \to \mathrm{R}$ и $\varepsilon > 0$ существует такой многочлен P, для которого

$$\|f - P\|_{C[a,b]} := \max_{a \leqslant x \leqslant b} |f(x) - P(x)| < \varepsilon.$$

Первоначальное доказательство Вейерштрасса и целый ряд других основаны на идее *сглаживания* функции f. На этом пути f сначала приближается с помощью гладкой функции φ, для которой строится, например, *многочлен Тейлора* P (отрезок её *ряда Тейлора*). Окончательно считается $f \approx P$. В некоторых вариантах вместо φ сразу получается P (как результат *свёртки* f с некоторым ядром).

Отметим элегантное доказательство теоремы Вейерштрасса, принадлежащее А. Лебегу (H. Lebesgue, 1898). Идеи Лебега можно выразить тремя фразами: (1) каждая непрерывная функция равномерно приближаема ломаными; (2) любая ломаная есть линейная комбинация функций вида $u(x) = |x - \gamma|$; (3) функция $v(x) = |x|$ раскладывается на $[-1, 1]$ в равномерно сходящийся степенной ряд, частичные суммы которого есть многочлены.

Конструктивное доказательство теоремы Вейерштрасса, основанное на соображениях теории вероятностей, принадлежит С.Н. Бернштейну (1912). В нём вводится явный аппарат приближения — *многочлены Бернштейна,* которые для непрерывной на $[0, 1]$ функции f имеют вид

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} f\Big(\frac{k}{n}\Big) x^k (1 - x)^{n-k}.$$

Бернштейн показал, что

$$\|f - B_n\|_{C[0,1]} \to 0, \qquad n \to \infty.$$

Основы *теории равномерного приближения функций многочленами* заложены П.Л. Чебышёвым (1821 – 1894) в его знаменитом мемуаре "Теория механизмов, известных под названием параллелограммов"(1853). В этой работе поставлена задача наилучшего равномерного приближения непрерывной функции многочленами степени $\leqslant n$ и сформулирована *теорема об альтернансе,* характеризующая так называемый *многочлен наилучшего приближения.*

В этой же работе поставлена и решена задача о *многочленах, наименее уклоняющихся от нуля* в метрике пространства $C[-1, 1]$. В ходе решения этой экстремальной задачи возникли *многочлены Чебышёва* $T_n(x) := \cos(n \arccos x)$, имеющие много разнообразных и удивительных свойств. Остановимся на них подробнее.

Экстремальное свойство многочленов T_n, открытое Чебышёвым, заключается в следующем. Среди всех многочленов степени $\leqslant n$ со старшим коэффициентом 1 нормированный многочлен Чебышёва $\tilde{T}_n = 1/2^{n-1} T_n$ имеет минимальную $C[-1, 1]$-норму, равную $1/2^{n-1}$. Несмотря на непривычную форму записи, $T_n(x)$ есть алгебраический многочлен от x. Действительно, $T_0(x) = 1$, $T_1(x) = x$. Каждый из остальных T_n может быть получен из *рекуррентного соотношения*

$$T_{n+1}(x) = 2x T_n(x) - T_{n-1}(x), \qquad n \geqslant 1. \tag{27}$$

Из (27) получается

$$T_2(x) = 2x^2 - 1,$$

$$
\begin{aligned}
&T_3(x) = 4x^3 - 3x,\\
&T_4(x) = 8x^4 - 8x^2 + 1,\\
&T_5(x) = 16x^5 - 20x^3 + 5x,\\
&T_6(x) = 32x^6 - 48x^4 + 18x^2 - 1,\\
&T_7(x) = 64x^7 - 112x^5 + 56x^3 - 7x,\\
&T_8(x) = 128x^8 - 256x^6 + 160x^4 - 32x^2 + 1,\\
&T_9(x) = 256x^9 - 576x^7 + 432x^5 - 120x^3 + 9x,\\
&T_{10}(x) = 512x^{10} - 1280x^8 + 1120x^6 - 400x^4 + 50x^2 - 1,\\
&\dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots
\end{aligned}
$$

Старший коэффициент T_n равен 2^{n-1}. Функции T_n являются чётными или нечётными в зависимости от чётности n. При $-1 \leqslant x \leqslant 1$ всегда $-1 \leqslant T_n(x) \leqslant 1$, что следует из первоначальной записи (применимой лишь для $|x| \leqslant 1$).

Корни многочлена T_n при любом $n > 0$ действительны, различны и принадлежат отрезку $[-1, 1]$. Они могут быть получены в результате следующей геометрической процедуры. Над отрезком $[-1, 1]$ строится полуокружность и делится на n равных дуг. Затем середина каждой дуги проектируется на $[-1, 1]$. Точки проекций и есть корни T_n.

Многочлены Чебышёва являются примером так называемых *ортогональных многочленов,* разные варианты которых плодотворно используются в анализе. Именно, семейство $\{T_n\}$ является ортогональным на $[-1, 1]$ с весом $w(x) = (1 - x^2)^{-1/2}$. Простое вычисление даёт

$$
\int_{-1}^{1} T_m(x) T_n(x) \frac{1}{\sqrt{1-x^2}} dx = \begin{cases} 0, & m \neq n \\ \pi/2, & m = n \neq 0 \\ \pi, & m = n = 0 \end{cases} . \tag{28}
$$

Это позволяет раскладывать функции $f : [-1, 1] \to \mathrm{R}$ в *ряды по многочленам Чебышёва*

$$
f(x) = \sum_{k=0}^{\infty} a_k T_k(x), \quad a_k = \gamma \int_{-1}^{1} f(x) T_k(x) w(x) dx. \tag{29}
$$

Ряды (29) часто сходятся быстрее рядов Тейлора; их частичные суммы являются хорошей полиномиальной аппроксимацией f. Многочлены Чебышёва находят своё приложение и в *интерполяционных процессах,* см. подробнее [21], [19].

Из других свойств T_n отметим следующие. Многочлены Чебышёва коммутируют относительно операции суперпозиции:

$$
T_n \circ T_m = T_m \circ T_n = T_{mn}. \tag{30}
$$

Если p — нечётное простое, $x \in \mathrm{N}$, то

$$
T_p(x) \equiv T_1(x) \pmod{p}.
$$

Последнее равенство по форме аналогично записи теоремы Ферма $a^p \equiv a \pmod{p}$ для целого a.

Наконец, если в квадрате $[-1,1]^2$ построить графики всех $T_0, T_1, \ldots, T_n$ при достаточно большом n, то окажется, что границы областей, не содержащих этих графиков, образуют некоторые интересные линии.

Многочлены и ряды Чебышёва применяются в целом ряде практически важных алгоритмов, см. [21]. Из монографий о многочленах Чебышёва отметим также менее доступную, но очень хорошую книгу [27].

Упражнение 1. Доказать соотношения (27), (28), (30).

Упражнение 2. Исследовать с помощью компьютера поведение графиков T_n.

Более эффективными (но и более сложными) методами аппроксимации является *рациональная и сплайн-аппроксимация.*

Рациональная функция r есть отношение двух многочленов. Алгебраические свойства таких функций изложены в [16]. Естественные классы функций r не являются линейными пространствами, в связи с чем рациональная аппроксимация является *нелинейной. Сплайн* s (англ. *spline*) — это так называемая кусочно-полиномиальная функция, которая на отдельных участках области определения имеет вид многочлена. Обычно сплайн обладает некоторой гладкостью, то есть s имеет производные в узлах. Следует сказать также, что узлы сплайнов могут быть фиксированными, а могут и меняться — то есть быть *свободными, или плавающими.* Сплайн-аппроксимация со свободными узлами, как и рациональная, относится к нелинейным методам приближения и служит примером *адаптивной аппроксимации.*

Построение рациональных и сплайн-функций, приближающих данную функцию f, осуществляется многими важными способами (интерполяция, среднеквадратическая аппроксимация и т.д.). Опишем здесь метод рациональных аппроксимаций Паде, имеющий явное алгебраическое основание (действия с формальными многочленами и степенными рядами). Эти рациональные функции являлись темой диссертации Паде (H. Pade, 1892), однако они изучались и ранее в работах Якоби (C. Jacobi, 1846) и Фробениуса (G. Frobenius, 1881).

Аппроксимация Паде $r = [L/M]$ — это рациональная функция

$$r(z) = [L/M](z) = \frac{a_0 + a_1 z + \ldots + a_L z^L}{b_0 + b_1 z + \ldots + b_M z^M},$$

приближающая функцию f с заданным степенным рядом

$$f(z) = \sum_{k=0}^{\infty} c_k z^k$$

или даже просто формальный степенной ряд. Условие на r выглядит следующим образом:

$$f(z) - r(z) = \gamma_1 z^{L+M+1} + \gamma_2 z^{L+M+2} + \ldots = O(z^{L+M+1}).$$

Умножение на знаменатель даёт

$$(c_0 + c_1 z + c_2 z^2 + \ldots)(b_0 + b_1 z + \ldots + b_M z^M) - (a_0 + a_1 z + \ldots + a_L z^L) =$$

$$= O(z^{L+M+1}).$$

Сравнивая коэффициенты при $1, z, \ldots, z^{L+M}$, получаем систему линейных уравнений относительно неизвестных коэффициентов числителя и знаменателя a_i, b_j.

Так как их значения определяются с точностью до пропорциональности, полагают $b_0 = 1$.

Аппроксимации Паде и их модификации являются эффективным средством приближения и применяются во многих интересных алгоритмах. Читатель может ознакомиться с их приложениями по замечательной книге Дж. Бейкера, П. Грейвс-Морриса [2].

Упражнение 3. Найти аппроксимации Паде $[2/0], [1/1]$ *и* $[0/2]$ *для функции* $f(z) = e^z$.

В заключение скажем несколько слов о многочленах от нескольких переменных $x_1, \ldots, x_n$. Как функции, они определены на пространстве $\mathrm{R^n}$ (или $\mathrm{C^n}$). Многочлен от $x_1, \ldots, x_n$ имеет вид

$$g(x) = g(x_1, \ldots, x_n) = \sum a_{\alpha_1, \ldots, \alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}, \tag{31}$$

где суммирование распространено на конечное множество целых неотрицательных α_j. Буквами a обозначены действительные (комплексные) коэффициенты.

Здесь естественно возникают два конечномерных линейных пространства многочленов — P_k и $P_{\vec{k}}$. В первом варианте $k = 0, 1, 2, \ldots$; P_k содержит те многочлены g, общая степень которых не превосходит k. Это означает, что суммирование в (31) осуществляется по множеству $0 \leqslant \alpha_1 + \ldots + \alpha_n \leqslant k$. Например, в случае $n = 2$ $P_1 = \{ax_1 + bx_2 + c\}$.

Во втором варианте $\vec{k}$ есть n-мерный вектор $\vec{k} = (k_1, \ldots, k_n)$ с целыми неотрицательными компонентами. Совокупность $P_{\vec{k}}$ содержит те многочлены, степень которых по x_i не превосходит k_i. Для функций $g \in P_{\vec{k}}$ суммирование в (31) осуществляется по множеству индексов $0 \leqslant \alpha_1 \leqslant k_1, \ldots, 0 \leqslant \alpha_n \leqslant k_n$. Например, $P_{(1,1)} = \{ax_1x_2 + bx_1 + cx_2 + d\}$.

Упражнение 4. Доказать, что

$$\dim P_k(\mathrm{R}^n) = \dim P_n(\mathrm{R}^k) = \binom{n+k}{k}.$$

Таким образом, влияние степени k *и размерности основного пространства* n *на величину* $\dim P_k(\mathrm{R}^n)$ *одинаково.*

Для таких многочленов изучаются многие вопросы, поставленные в ситуации $n = 1$ (интерполяция, наилучшее приближение, рациональная и сплайн-аппроксимация и др.). Следует отметить, что, как правило, задачи для $P_{\vec{k}}$ решаются проще — они в некотором смысле сводятся к одномерным аналогам. См., например, [19] по поводу интерполяции функций двух переменных.

В многомерной ситуации возникают проблемы, решение которых при $n = 1$ не вызывает большого труда. Рамки этого краткого обзора являются слишком узкими для их описания.

Литература

Многие ссылки в тексте соответствуют дополнительному материалу или приложениям. Поэтому не все книги относятся к учебной литературе по алгебре.

1. *Акритас А.* Основы компьютерной алгебры с приложениями. М.: Мир, 1994. 544 с.

2. *Бейкер Д., Грейвс-Моррис П.* Аппроксимации Паде. М.: Мир, 1986. 502 с.

3. *Беллман Р.* Введение в теорию матриц. М.: Наука, 1969. 368 с.

4. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986. 576 с.

5. *Гантмахер Ф.Р.* Теория матриц. 4-е изд. М.: Наука, 1988. 552 с.

6. *Гарднер М.* Путешествие во времени. М.: Мир, 1990. 341 с.

7. *Гельфанд И.М.* Лекции по линейной алгебре. 4-е изд. М.: Наука, 1971. 272 с.

8. *Залманзон Л.А.* Преобразования Фурье, Уолша, Хаара и их применение в управлении, связи и других областях. М.: Наука, 1989. 496 с.

9. *Ильин В.А., Позняк Э.Г.* Линейная алгебра. 3-е изд. М.: Наука, 1984. 295 с.

10. *Казарин Л.С.* Теория кодирования. Ярославль, 1987. 62 с.

11. *Каргаполов М.И., Мерзляков Ю.И.* Основы теории групп. 3-е изд. М.: Наука, 1982. 288 с.

12. *Колмогоров А.Н., Фомин С.В.* Элементы теории функций и функционального анализа. 4-е изд. М.: Наука, 1976. 544 с.

13. *Кострикин А.И.* Введение в алгебру. Часть 1. Основы алгебры. М.: Физматлит, 2000. 272 с.

14 *Кострикин А.И.* Введение в алгебру. Часть 2. Линейная алгебра. М.: Физматлит, 2000. 368 с.

15 *Кострикин А.И.* Введение в алгебру. Часть 3. Основные структуры алгебры. М.: Физматлит, 2001. 272 с.

16. *Курош А.Г.* Курс высшей алгебры. 10-е изд. М.: Наука, 1971. 432 с.

17. *Курош А.Г.* Теория групп. 3-е изд. М.: Наука, 1967. 648 с.

18. *Макклеллан Дж.Г., Рейдер Ч.М.* Применение теории чисел в цифровой обработке сигналов. М.: Радио и связь, 1983. 264 с.

19. *Невский М.В., Иродова И.П.* Некоторые вопросы теории приближения функций. Ярославль, 1999. 92 с.

20. *Ноден П., Китте К.* Алгебраическая алгоритмика. М.: Мир, 1999. 720 с.

21. *Пашковский С.* Вычислительные применения многочленов и рядов Чебышева. М.: Наука, 1983. 384 с.

22. *Привалов И.И.* Введение в теорию функций комплексного переменного. 14-е изд. М.: Высш. шк., 1999. 432 с.

23. *Проскуряков И.В.* Сборник задач по линейной алгебре. 3-е изд. М.: Наука, 1967. 384 с.

24. *Стренг Г.* Линейная алгебра и её применения. М.: Мир, 1980. 455 с.

25. *Схрейвер А.* Теория линейного и целочисленного программирования. Т. 1. М.: Мир, 1991. 360 с.

26. *Хорн Р., Джонсон Ч.* Матричный анализ. М.: Мир, 1989. 655 с.

27. *Rivlin T.* Chebyshev polynomials. John Wiley & sons. New York etc. 1990. 249 p.

Приложение

ПРОГРАММА

дисциплины "Геометрия и алгебра"для специальности "010200 — Прикладная математика и информатика"

Приведённая ниже программа составлена в соответствии с требованиями государственного образовательного стандарта и с Примерной программой дисциплины "Геометрия и алгебра утверждённой Министерством образования Российской Федерации в 2000 г.

Программа содержит как алгебраические, так и геометрические разделы дисциплины "Геометрия и алгебра"; они расположены в порядке изложения (и изучения) курса. Настоящее пособие содержит не весь, а только алгебраический материал, который разбит на четырнадцать разделов. Названия восьми разделов программы, относящихся к аналитической геометрии и не вошедших в пособие, выделены курсивом.

Введение. Предмет и метод дисциплины "Геометрия и алгебра". Краткие исторические сведения. "Геометрия и алгебра"для математика-прикладника.

Системы линейных уравнений и их решение методом Гаусса. Общий вид системы линейных уравнений. Классификация. Элементарные преобразования. Ступенчатые и специальные ступенчатые матрицы. Анализ системы уравнений, имеющей ступенчатый вид. Решение систем методом Гаусса. Трудоёмкость метода Гаусса. Понятие о других методах решения линейных систем. Вычислительные особенности решения линейных систем.

Пространство $\mathrm{R^n}$. Матрицы и действия с ними. Пространство $\mathrm{R^n}$. Действия с n-мерными векторами. Пространство матриц $M_{m,n}$. Простейшие операции с матрицами. Умножение матриц. Многочлен от матрицы. Важнейшие классы матриц.

Пространство геометрических векторов $\mathrm{V_n}, n = 1, 2, 3$. Понятие геометрического вектора. Коллинеарность и компланарность. Пространство $\mathrm{V_n}$. Линейная зависимость векторов из $\mathrm{V_n}, n = 1, 2, 3$, и $\mathrm{R^n}, n \in \mathrm{N}$. Свойства линейной зависимости. Решение задачи о линейной зависимости в $\mathrm{R^n}$. Базис $\mathrm{V_n}$. Характеризация базисов $\mathrm{V_1}, \mathrm{V_2}, \mathrm{V_3}$. Размерность. Координаты вектора. Действия в координатах. Изоморфизм $\mathrm{V_n}$ и $\mathrm{R^n}, n = 1, 2, 3$.

Системы координат, проекции, произведения векторов. Аффинная и декартова системы координат на прямой, на плоскости и в пространстве. Полярная система координат на плоскости. Другие системы координат. Векторная и скалярная проекции вектора на ось и их свойства. Геометрический смысл декартовых координат. Скалярное, векторное и смешанное произведения векторов, их свойства. Вычисление площадей и объёмов с помощью определителей 2 – 3 порядка.

Преобразования координат. Уравнения линий и поверхностей. Преобразования аффинных координат на прямой, на плоскости и в пространстве. Преобразования декартовых координат. Поворот и перенос. Различные виды уравнений линии и поверхности. Алгебраические линии и поверхности, независимость их порядка от выбора аффинной системы координат.

Прямая на плоскости. Различные виды уравнений — векторное, каноническое, параметрические, общее. Неполные уравнения. Уравнение в отрезках. Уравнение с угловым коэффициентом. Переход от одних уравнений к другим. Угол между двумя прямыми. Параллельность и перпендикулярность двух прямых. Нормальное уравнение. Отклонение точки от прямой. Расстояние от точки до прямой. Основные типы задач.

Плоскость и прямая в пространстве. Уравнение плоскости в векторной форме. Параметрические и общее уравнения. Неполные уравнения плоскости, уравнение в отрезках. Переход от одних уравнений к другим. Нормальное уравнение плоскости. Отклонение точки от плоскости. Расстояние от точки до плоскости. Различные виды уравнений прямой в пространстве. Углы между прямыми и плоскостями. Задачи на взаимное расположение точек, прямых и плоскостей.

Полуплоскость и полупространство. Системы линейных неравенств. Выпуклые множества.

Линии второго порядка. Происхождение. Конические сечения. Исторические сведения. Определение, каноническое уравнение, характеристики и свойства эллипса, гиперболы, параболы. Директрисы линий второго порядка, их свойство.

Приведение уравнений линий второго порядка к каноническому виду при помощи поворота и переноса декартовой системы координат. Собственные векторы и собственные значения матриц второго порядка. Приведение к главным осям методом собственных значений. Простейшие уравнения второго порядка и их геометрические образы.

Поверхности второго порядка. Общее уравнение поверхности второго порядка. Классификация поверхностей. Понятие о методе собственных значений при приведении к главным осям. Эллипсоид. Гиперболоиды. Параболоиды. Конус и цилиндры второго порядка. Канонические уравнения, основные свойства. Метод сечений.

Понятие о группе, кольце, поле. Бинарная операция, алгебраическая система. Полугруппа и группа. Терминология. Подгруппа. Теорема Лагранжа. Кольцо и поле, их разновидности. Примеры и свойства. Конечные структуры. Кольцо и поле вычетов. Другие конечные поля.

Комплексные числа и действия с ними. Определение и характеристики комплексных чисел. Действия в алгебраической и тригонометрической форме. Геометрическая интерпретация комплексных чисел. Корни из 1, их свойства.

Многочлены. Многочлены над R и над C. Другие кольца многочленов. Делимость. Теорема о делении с остатком. Наибольший общий делитель, алгоритм Евклида. Неприводимые многочлены. Разложение в произведение неприводимых. Корни многочлена. Кратные корни и дифференцирование. Основная теорема ал-

гебры многочленов. Интерполяция многочленами. Формулы Лагранжа и Ньютона.

Определители. Перестановки и инверсии. Определитель порядка n. Свойства определителей. Вычисление методом Гаусса. Приложение к решению линейных систем. Критерий определённости, правило Крамера. Разложение определителя по строке (столбцу). Теорема Лапласа. Определитель произведения двух матриц. Определитель Вандермонда и задача интерполяции многочленами. Обратная матрица и способы её вычисления. Обратимость и невырожденность матриц.

Линейные пространства. Определение и примеры линейных пространств. Линейная зависимость, её свойства. Конечномерные и бесконечномерные пространства. Примеры. Базис, размерность, координаты. Изоморфизм линейных пространств.

Линейные подпространства и ранг. Подпространства. Линейная оболочка. Ранг и база системы векторов. Сумма и пересечение подпространств. Прямая сумма. Ранг матрицы. Теорема о ранге. Методы вычисления ранга матрицы. Теорема Кронекера – Капелли. Размерность и базис подпространства R^{n}, задаваемого системой линейных однородных уравнений. Фундаментальная система решений.

Линейные операторы и действия с ними. Определение и примеры линейных операторов в основных пространствах. Матрица линейного оператора. Действия с линейными операторами. Ядро и образ. Определение ранга и дефекта по матрице оператора. Обратимость и невырожденность. Изменение матрицы оператора при изменении базиса. Подобные матрицы. Инвариантные подпространства оператора.

Собственные векторы и собственные значения линейного оператора.
Определение, свойства и вычисление. Характеристический многочлен оператора. Собственные подпространства. Диагонализируемость. Каноническая форма матрицы линейного оператора.

Билинейные и квадратичные формы в линейном пространстве. Матрица билинейной формы. Приведение квадратичной формы к каноническому виду методами Лагранжа и Якоби. Положительная определённость, критерий Сильвестра. Закон инерции квадратичных форм.

Евклидово пространство. Определение и примеры. Определитель Грама. Длина и угол в евклидовом пространстве. Неравенство Коши – Буняковского и его частные виды. Ортогонализация Грама – Шмидта. Ортогональное дополнение к подпространству. Расстояние от точки до подпространства.

Линейные операторы в евклидовом пространстве. Сопряжённый оператор. Симметричные операторы и их свойства. Диагонализируемость симметричного оператора. Ортогональные операторы и их свойства. Каноническая форма матрицы ортогонального оператора.

Билинейные и квадратичные формы в евклидовом пространстве. Приведение квадратичной формы к каноническому виду с использованием свойств симметричного оператора (метод собственных значений).

Михаил Викторович Невский

ЛЕКЦИИ ПО АЛГЕБРЕ

Редактор, корректор А.А. Аладьева.
Компьютерный набор, вёрстка М.В. Невского.

Лицензия ЛР N 020319 от 30.12.96.

Подписано в печать 20.02.2002. Формат $60 \times 88^1/_8$. Печать офсетная.
Усл. печ. л. 30,8. Уч.-изд. л. 16,0. Тираж 200 экз.

Оригинал-макет подготовлен в редакционно-издательском отделе
Ярославского государственного университета.

Ярославский государственный университет им. П.Г. Демидова.
150000 Ярославль, ул. Советская, 14.

Отпечатано на ризографе.
ООО "Рио-Гранд".
150000 Ярославль, ул. Свердлова, 18.
Офис 34. Тел. 30-75-98.