

**А. В. ВАСИЛЬЕВ**

**Д. В. ЛЫТКИНА**

**В. Д. МАЗУРОВ**

# **Высшая алгебра**

**конспект лекций**

**ИЗДАТЕЛЬСТВО  
ИНСТИТУТА МАТЕМАТИКИ**

А. В. Васильев, Д. В. Лыткина, В. Д. Мазуров

**ВЫСШАЯ АЛГЕБРА**  
**конспект лекций**

**Новосибирск**

**Издательство Института Математики**

**2020**

УДК 512  
ББК В15я73  
В 191

Васильев А. В., Лыткина Д. В., Мазуров В. Д. Высшая алгебра: конспект лекций / Новосибирск: Издательство Института математики, 2020. — 252 с.

ISBN 978-5-86134-173-8

В основе предлагаемого читателю учебного пособия лежит содержание двух семестров курса «Высшая алгебра», который авторы читали на первом курсе механико-математического факультета Новосибирского государственного университета. В курсе на основе понятия алгебраической системы определяются основные алгебраические структуры: группы, кольца, поля, векторные пространства, алгебры. В дальнейшем рассматриваются примеры этих структур: группы подстановок, кольца матриц и многочленов, поле комплексных чисел, конечномерные векторные пространства и алгебры. В рамках этого подхода изучаются классические алгебраические объекты: определители и системы линейных уравнений. Большое внимание уделено теории линейных операторов, как в произвольных векторных пространствах, так и в пространствах со скалярным произведением, а также теории квадратичных форм. Последний параграф посвящен основам абстрактной теории групп. Часть этого материала уже выходила в виде пособия в издательстве НГУ.

УДК 512  
ББК В15я73  
В 191

Рецензент  
д-р физ.-мат. наук П. С. Колесников

ISBN 978-5-86134-173-8

© Васильев А. В., Лыткина Д. В.,  
Мазуров В. Д., 2020

# Содержание

<b>Предисловие</b>	<b>5</b>
<b>Глава 1. Введение</b>	<b>6</b>
§ 1.1. Множества и отображения . . . . .	6
§ 1.2. Алгебраические системы . . . . .	10
§ 1.3. Изоморфизм алгебраических систем . . . . .	16
<b>Глава 2. Группы, кольца, поля</b>	<b>19</b>
§ 2.1. Определения основных алгебраических структур . . . . .	19
§ 2.2. Группа подстановок . . . . .	27
§ 2.3. Кольцо квадратных матриц . . . . .	35
§ 2.4. Определитель . . . . .	47
§ 2.5. Поле комплексных чисел . . . . .	61
<b>Глава 3. Векторные пространства</b>	<b>67</b>
§ 3.1. Определение векторного пространства . . . . .	67
§ 3.2. Базис и размерность векторного пространства . . . . .	70
§ 3.3. Взаимное расположение подпространств . . . . .	80
<b>Глава 4. Системы линейных уравнений</b>	<b>86</b>
§ 4.1. Ранг матрицы . . . . .	86
§ 4.2. Совместность системы линейных уравнений . . . . .	92
§ 4.3. Однородные системы линейных уравнений . . . . .	96
<b>Глава 5. Кольцо многочленов</b>	<b>100</b>
§ 5.1. Кольцо многочленов от одной переменной . . . . .	100
§ 5.2. Делимость в кольце многочленов . . . . .	102
§ 5.3. Значения и корни многочленов . . . . .	108
§ 5.4. Симметрические многочлены . . . . .	115
§ 5.5. Алгебраическая замкнутость поля комплексных чисел . . . . .	118
§ 5.6. Разложимость над полем рациональных чисел . . . . .	127
<b>Глава 6. Линейные преобразования</b>	<b>133</b>
§ 6.1. Линейное преобразование и его матрица . . . . .	133
§ 6.2. Ядро и образ линейного преобразования . . . . .	142
§ 6.3. Инвариантные подпространства и собственные векторы . . . . .	146
§ 6.4. Корневые подпространства и корневое разложение . . . . .	152

---

§ 6.5. Нильпотентные преобразования . . . . .	157
§ 6.6. Жорданова форма матрицы линейного преобразования . . . . .	163
§ 6.7. Многочлены и функции от линейных преобразований . . . . .	166
<b>Глава 7. Евклидовы и унитарные пространства</b>	<b>175</b>
§ 7.1. Скалярное произведение на векторном пространстве . . . . .	175
§ 7.2. Преобразования евклидовых и унитарных пространств . . . . .	181
§ 7.3. Ортогональные и унитарные преобразования . . . . .	188
§ 7.4. Самосопряжённые и косоэрмитовы преобразования . . . . .	193
§ 7.5. Сингулярные числа, полярное и сингулярное разложения	196
<b>Глава 8. Квадратичные формы</b>	<b>202</b>
§ 8.1. Квадратичная форма и её матрица . . . . .	202
§ 8.2. Диагонализация квадратичных форм . . . . .	204
§ 8.3. Положительно определённые квадратичные формы . . . . .	209
<b>Глава 9. Начала теории групп</b>	<b>214</b>
§ 9.1. Группы и их подгруппы . . . . .	214
§ 9.2. Порождающее множество и циклическая подгруппа . . . . .	216
§ 9.3. Смежные классы по подгруппе . . . . .	218
§ 9.4. Гомоморфизмы групп . . . . .	222
§ 9.5. Прямое произведение групп . . . . .	225
§ 9.6. Действие группы на множестве . . . . .	228
<b>Предметный указатель</b>	<b>235</b>
<b>Указатель обозначений</b>	<b>242</b>
<b>Приложение</b>	<b>244</b>
<b>Список литературы</b>	<b>248</b>

## Предисловие

В основе предлагаемого читателю учебного пособия лежит содержание двух семестров курса «Высшая алгебра», который авторы читали на первом курсе механико-математического факультета Новосибирского государственного университета. Часть этого материала уже выходила в виде пособия в издательстве НГУ [4].

Нумерация определений, теорем, предложений и упражнений, принятая в пособии, соответствует его разбиению на главы и параграфы. Например, теорема 2.3.1 — это первая теорема из третьего параграфа второй главы. Нумерация вынесенных формул начинается заново внутри каждого параграфа. Упражнения, сопровождающие изложение, призваны помочь усвоению материала. Наиболее трудные из них помечены звёздочкой. Мы также рекомендуем использовать классические задачки [11, 18, 20], а также менее известные сборники задач [1, 22]. Отметим, что список литературы, приведённый в конце пособия, не претендует на полноту, его основная цель — предоставить читателю дополнительную возможность ознакомиться с затрагиваемыми в курсе понятиями и идеями. Для удобства в приложении приводится программа курса «Высшая алгебра» на 2016–17 учебный год. Ссылки на соответствующие места из книг, указанных в списке литературы, находятся в этой программе. Пособие снабжено предметным указателем и указателем обозначений.

Мы благодарны всем нашим коллегам, общение с которыми оказало влияние на наши представления о преподавании алгебры студентам-математикам. Мы выражаем глубокую признательность сотрудникам кафедры алгебры и математической логики ММФ НГУ, и особенно Марии Александровне Гречкосеевой, чью помощь невозможно переоценить.

# Глава 1

## Введение

### § 1.1. Множества и отображения

Под *множеством* понимается неупорядоченная совокупность мыслимых вместе объектов произвольной природы, которые мы умеем различать между собой. Объекты, составляющие множество, называются его *элементами*. Обычно мы будем обозначать множества заглавными, а элементы — строчными латинскими буквами. Свойство объекта быть элементом некоторого множества выражается словами *элемент  $a$  принадлежит множеству  $A$*  и записывается так:  $a \in A$ . Если элемент  $a$  не принадлежит множеству  $A$ , пишем  $a \notin A$ . Два множества *равны*, если они состоят из одних и тех же элементов. Множество можно задать перечислением всех его элементов или указанием некоторого свойства, которому элементы, его составляющие, должны удовлетворять. В последнем случае, если обозначить соответствующее свойство через  $P$ , запись того факта, что множество  $A$  состоит из тех и только тех элементов, которые обладают свойством  $P$ , выглядит следующим образом:  $A = \{x \mid x \text{ обладает свойством } P\}$  или кратко  $A = \{x \mid P(x)\}$ . Мы также будем иногда использовать кванторы  $\forall$  и  $\exists$ , заменяя ими выражения *для любого* и *существует* соответственно. Например, запись  $\forall a \in A : P(a)$  означает, что для любого элемента  $a \in A$  выполняется свойство  $P$ , а запись  $\exists a \in A : P(a)$  означает, что найдётся хотя бы один элемент  $a \in A$ , обладающий свойством  $P$ .

Читателю уже известны основные числовые множества:  $\mathbb{N} = \{1, 2, 3, \dots\}$  — множество натуральных чисел,  $\mathbb{Z}$  — множество целых чисел,  $\mathbb{Q}$  — множество рациональных чисел и  $\mathbb{R}$  — множество действительных чисел.

Множество  $B$  называется *подмножеством* множества  $A$ , если каждый элемент множества  $B$  принадлежит множеству  $A$ . Мы будем обозначать этот факт так:  $B \subseteq A$ . В случае, если найдётся хотя бы один элемент множества  $A$ , который не принадлежит подмножеству  $B$ , множество  $B$  называется *собственным* подмножеством множества  $A$ , что можно подчеркнуть, используя следующее обозначение:  $B \subset A$ . Единственным множеством, не имеющим собственных подмножеств, является

ся *пустое* множество  $\emptyset$ , которое по определению не содержит ни одного элемента. Множество всех подмножеств данного множества  $A$  обозначается через  $P(A)$  или  $2^A$ .

Из двух и более множеств можно образовать новые множества. Если заданы множества  $A_1, A_2, \dots, A_n$ , то множество  $A_1 \cap A_2 \cap \dots \cap A_n = \{x \mid x \in A_1 \text{ и } x \in A_2 \text{ и } \dots \text{ и } x \in A_n\}$  называется *пересечением*, а множество  $A_1 \cup A_2 \cup \dots \cup A_n = \{x \mid x \in A_1 \text{ или } x \in A_2 \text{ или } \dots \text{ или } x \in A_n\}$  — *объединением* множеств  $A_1, A_2, \dots, A_n$ . Под *разностью* множеств  $A$  и  $B$  мы будем понимать множество  $A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}$ . Если при этом множество  $B$  является подмножеством множества  $A$ , то мы будем называть множество  $A \setminus B$  *дополнением* множества  $B$  в множестве  $A$ . Если множество  $A$  фиксировано, то дополнение в  $A$  его подмножества  $B$  мы будем также обозначать через  $\bar{B}$ .

Напомним, что порядок элементов при записи множества не играет роли. Так, множества  $\{a, b\}$  и  $\{b, a\}$  равны, поскольку состоят из одних и тех же элементов. С другой стороны, в математике, как и в жизни, часто приходится рассматривать упорядоченные совокупности объектов. Упорядоченный набор из  $n$  элементов  $a_1, a_2, \dots, a_n$  мы будем обозначать как  $(a_1, a_2, \dots, a_n)$  и называть  *$n$ -кой*. В случае двух объектов будем употреблять термин *упорядоченная пара*. Две  $n$ -ки  $(a_1, a_2, \dots, a_n)$  и  $(b_1, b_2, \dots, b_n)$  равны тогда и только тогда, когда  $a_1 = b_1, a_2 = b_2, \dots, a_n = b_n$ .

**УПРАЖНЕНИЕ 1.1.1.** Доказать, что множества  $\{\{a\}, \{a, b\}\}$  и  $\{\{c\}, \{c, d\}\}$  равны тогда и только тогда, когда  $a = c$  и  $b = d$ .

**Определение 1.1.1.** Если заданы множества  $A_1, A_2, \dots, A_n$ , то их *декартовым произведением* называется множество

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}.$$

*Декартовой  $n$ -ой степенью* множества  $A$  называется множество

$$A^n = \{(a_1, a_2, \dots, a_n) \mid a_1 \in A, a_2 \in A, \dots, a_n \in A\}.$$

В случае когда  $n = 2$ , мы будем говорить о *декартовом квадрате* множества  $A$ .

Пусть заданы два множества  $X$  и  $Y$ . Правило  $f$ , по которому *каждому* элементу множества  $X$  сопоставляется *однозначно определённый* элемент множества  $Y$ , принято называть *функцией* или *отображением* из множества  $X$  в множество  $Y$  (обозначение:  $f : X \rightarrow Y$ ). Мы будем в основном использовать термин *отображение*.



Тот факт, что элемент  $y$  множества  $Y$  является образом элемента  $x$  множества  $X$  при отображении  $f$ , можно записать разными способами:  $f(x) = y$ ,  $xf = y$ ,  $x^f = y$ . Мы будем в основном использовать обозначения, при которых символ отображения располагается справа от символа элемента, т. е. предпочитать обозначение  $xf$  обозначению  $f(x)$ . Если  $Z \subseteq X$ , обозначим через  $Zf$  множество  $\{y \in Y \mid \exists x \in Z : xf = y\}$ , которое называется образом  $Z$  в  $Y$ . Если  $Z = X$ , то образ  $Xf$  мы будем также обозначать через  $\text{Im } f$ .

Рассмотрим два отображения:  $f : X \rightarrow Y$  и  $g : Y \rightarrow Z$ . *Композицией* (или *произведением*) отображений  $f$  и  $g$  называется отображение  $f * g : X \rightarrow Z$ , определяемое для любого  $x \in X$  равенством  $x(f * g) = (xf)g$ . Таким образом, отображение  $f * g$  — это результат последовательного выполнения сначала отображения  $f$ , а затем отображения  $g$ . Иногда по аналогии с умножением чисел мы будем опускать символ  $*$  и писать просто  $fg$  вместо  $f * g$ .

**ЗАМЕЧАНИЕ.** При расположении символа отображения слева от символа элемента запись  $f * g$  композиции отображений  $f$  и  $g$  уже означала бы, что сначала выполняется отображение  $g$ , а потом  $f$ :  $(f * g)x = f(g(x))$ . Таким образом, нам пришлось бы читать запись  $f * g$  справа налево, что не слишком удобно. Это одна из причин, почему мы отдаём предпочтение правостороннему расположению символа отображения. Отметим, что при этом имеются достаточно веские причины и для использования левосторонней записи.

Вернёмся к определению отображения. Оно требует, чтобы *каждый* элемент  $x$  множества  $X$  имел образ  $y = xf$  в  $Y$ . Обратное верно не всегда: могут существовать элементы множества  $Y$ , которые не имеют прообразов в  $X$ . Те отображения, для которых таких элементов в  $Y$  нет, носят специальное название.

**Определение 1.1.2.** Отображение  $f : X \rightarrow Y$  называется отображением множества  $X$  на множество  $Y$  или *сюръекцией*, если для каждого элемента  $y \in Y$  существует элемент  $x \in X$ , такой, что  $y = xf$ . Соответствующее обозначение:  $f : X \xrightarrow{\text{на}} Y$ .

Определение отображения также требует, чтобы каждый элемент множества  $X$  имел *ровно один* образ в  $Y$ . Иными словами, если  $xf = y_1$  и  $xf = y_2$ , то  $y_1 = y_2$ . Обратное снова в общем случае неверно: у одного элемента из  $Y$  может быть несколько прообразов в  $X$ . Например, если рассмотреть отображение  $f : \mathbb{R} \rightarrow \mathbb{R}$ , действующее по правилу  $xf = x^2$ , то число 4 имеет два прообраза: 2 и  $-2$ . Мы опять выделим отображения, для которых такая ситуация невозможна.

**Определение 1.1.3.** Отображение  $f : X \rightarrow Y$  называется *взаимно однозначным* отображением из множества  $X$  в множество  $Y$  или *инъекцией*, если для любых элементов  $x_1, x_2 \in X$  из равенства  $x_1 f = x_2 f$  следует равенство  $x_1 = x_2$ . Соответствующее обозначение:  $f : X \xrightarrow{1-1} Y$ .

Отображения, которые удовлетворяют определениям 1.1.2 и 1.1.3 одновременно, также имеют специальное название.

**Определение 1.1.4.** Отображение  $f : X \rightarrow Y$  называется *взаимно однозначным* отображением множества  $X$  на множество  $Y$  или *биекцией*, если оно является сюръекцией и инъекцией одновременно. Соответствующее обозначение:  $f : X \xrightarrow[\text{на}]{1-1} Y$ .

Если отображение  $f : X \rightarrow Y$  является биекцией, то, как следует из определения отображения, существует *обратное* к нему отображение  $f^{-1} : Y \rightarrow X$ , действующее по правилу:  $x = y f^{-1}$  тогда и только тогда, когда  $y = x f$ . Обратное отображение снова является биекцией. Множества  $X$  и  $Y$ , между которыми можно установить биекцию, принято называть *равномощными*.

УПРАЖНЕНИЕ 1.1.2. Привести пример отображения, которое:

- 1) не является ни сюръекцией, ни инъекцией;
- 2) является сюръекцией, но не является инъекцией;
- 3) является инъекцией, но не является сюръекцией;
- 4) является биекцией.

УПРАЖНЕНИЕ 1.1.3. Доказать, что композиция двух биекций снова является биекцией.

УПРАЖНЕНИЕ 1.1.4. Пусть  $m, n \in \mathbb{N}$ , множество  $X$  состоит из  $m$  элементов, а множество  $Y$  — из  $n$  элементов. Доказать, что следующие утверждения эквивалентны.

1. Существует биекция  $\varphi : X \rightarrow Y$ .
2. Выполняется равенство  $m = n$ .

Из утверждения, приведённого в упражнении, в частности следует, что если множество  $X$  конечно (состоит из конечного числа элементов), то между ним и любым его собственным подмножеством установить биекцию не удастся. Это неверно в случае, когда множество  $X$  бесконечно, как показывает следующее упражнение.

УПРАЖНЕНИЕ 1.1.5. Пусть множество  $X$  бесконечно. Тогда найдётся по крайней мере одно собственное подмножество  $Y$  множества  $X$ , такое, что существует биекция  $\varphi : X \rightarrow Y$ . Более точно, выполняются

следующие утверждения.

1. Для любого конечного подмножества  $Z$  множества  $X$  существует биекция  $\varphi : X \rightarrow Y$ , где  $Y = X \setminus Z$ .

2. Найдётся бесконечное число бесконечных подмножеств  $Z$  множества  $X$ , таких, что существует биекция  $\varphi : X \rightarrow Y$ , где  $Y = X \setminus Z$ .

ЗАМЕЧАНИЕ. Как следует из утверждений упражнений 1.1.4 и 1.1.5, множество  $X$  конечно тогда и только тогда, когда оно не содержит собственных подмножеств, равномоощных  $X$ . Любопытно, что интуитивно ясное понятие конечного множества удаётся формализовать в рамках теории множеств, положив в качестве определения именно указанный выше критерий.

## § 1.2. Алгебраические системы

Алгебра, как известно из опыта, имеет дело с операциями на множествах. Например, если рассмотреть множество  $\mathbb{N}$  натуральных чисел, то для любых двух чисел  $m$  и  $n$  можно определить их сумму и произведение, которые в свою очередь являются натуральными числами. Не проводя вычислений, мы способны предсказать, что сумма  $n + m$  совпадёт с суммой  $m + n$ . Если  $m < n$ , то можно найти единственное натуральное число  $x$ , удовлетворяющее уравнению  $x + m = n$ , и т. д. В течение долгого времени именно решение уравнений (или систем уравнений) считалось основным предметом алгебры.

Решению уравнений (в том числе квадратных) был посвящён и труд «Китаб аль-джебр валь-мукабала» арабского математика Эль Хорезми (Хорезми Мухаммед бен Муса), жившего около 800 г. н. э., в котором впервые появился термин *аль-джебр*, давший в латинизированном варианте название всей математической дисциплине. Однако полезно помнить, что этим термином Эль Хорезми называл не конкретное уравнение, а одно из двух основных преобразований, используемых им при решении уравнений. Иными словами, свойство операции, заданной на множестве (в данном случае, числовом).

Взгляд на алгебру как на науку, изучающую свойства операций на множествах, возобладавший с развитием математики, оказался весьма плодотворным. Оказалось, что полезно рассматривать не только различные числовые множества, но и множества функций, преобразований (в том числе преобразований геометрических объектов) и даже множества произвольной природы. В соответствии с этим взглядом расширилось и понятие алгебраической операции. Например, если рассмотреть

множество *движений* плоскости, т. е. множество биекций плоскости на себя, сохраняющих расстояние между точками, то композиция, т. е. последовательное выполнение двух движений, результатом которой снова является движение, также может быть рассмотрена как естественная *алгебраическая операция* на множестве всех движений плоскости.

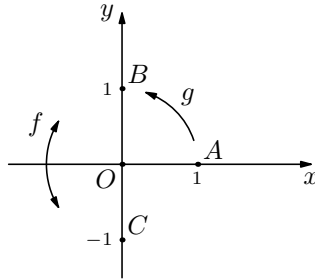
Наша первая задача — сформулировать по возможности наиболее общее определение алгебраической операции. С этой целью мы рассмотрим несколько примеров и попытаемся выделить то главное, что их объединяет.

**ПРИМЕРЫ. 1.** Операция сложения на множестве  $\mathbb{N}$  натуральных чисел сопоставляет каждой паре натуральных чисел  $m$  и  $n$  однозначно определённое натуральное число  $k = m + n$ , которое называется суммой чисел  $m$  и  $n$ . Вспомним определение отображения. Несложно сообразить, что сложение можно рассматривать как отображение множества  $\mathbb{N}^2$  в множество  $\mathbb{N}$  (или  $+: \mathbb{N}^2 \rightarrow \mathbb{N}$ ). Правда, тогда, следуя нашим обозначениям для отображений, логичнее было бы писать  $(m, n)+ = k$  вместо привычного  $m + n = k$ , но суть дела от этого не меняется.

Более существенным выглядит другой вопрос: стоит ли считать, что пара элементов (в нашем случае это числа  $m$  и  $n$ ), к которой мы применяем операцию, упорядочена? Ведь, как мы хорошо знаем, сложение натуральных чисел обладает тем свойством, что  $m + n = n + m$ , а значит, результат данной операции не зависит от порядка слагаемых. Но не стоит забывать, что мы стремимся к тому, чтобы дать по возможности общее определение алгебраической операции. Скажем, если мы зададим операцию  $f: \mathbb{N}^2 \rightarrow \mathbb{N}$  по правилу  $(m, n)f = m^n$  (возведение  $m$  в степень  $n$ ), то при перемене мест аргументов результат, очевидно, изменится, поскольку  $m^n$ , вообще говоря, не равно  $n^m$ . То же самое мы увидим и в следующем примере.

**2.** Рассмотрим множество  $S$  всех отображений непустого множества  $A$  в себя. Мы будем называть такие отображения *преобразованиями* множества  $A$ . Поскольку композиция  $f * g$  двух преобразований  $f: A \rightarrow A$  и  $g: A \rightarrow A$  снова является преобразованием множества  $A$ , отображение  $*$ :  $S^2 \rightarrow S$ , ставящее в соответствие паре преобразований их композицию, можно рассматривать как естественную алгебраическую операцию на множестве  $S$ . Легко заметить, что эта операция может оказаться некоммутативной ( $f * g \neq g * f$ ). Рассмотрим, к примеру, следующие преобразования координатной плоскости  $\mathbb{R}^2$ . Пусть  $f$  — осевая симметрия плоскости относительно оси абсцисс, а  $g$  — поворот на угол  $90^\circ$  относительно начала координат. Композиция двух данных

преобразований, взятых в любом порядке, снова является преобразованием плоскости, однако результат зависит от порядка, в котором мы производим преобразования.



Действительно, образ точки  $A$  с координатами  $(1, 0)$  под действием преобразования  $f * g$  есть точка  $B$  с координатами  $(0, 1)$ :

$$A(f * g) = (Af)g = Ag = B.$$

С другой стороны, образ точки  $A$  под действием преобразования  $g * f$  есть точка  $C$  с координатами  $(0, -1)$ :

$$A(g * f) = (Ag)f = Bf = C.$$

Таким образом, преобразования  $f * g$  и  $g * f$  различны.

Первые два примера приводят нас к определению операции на множестве  $A$  (вообще говоря, произвольной природы) как произвольного отображения из  $A^2$  в  $A$ . Однако естественное желание продолжить обобщение приводит нас к мысли, что можно рассматривать операции от иного количества аргументов.

3. Операция вычитания на множестве  $\mathbb{Z}$  целых чисел может быть успешно определена через операцию сложения, если мы предварительно введём операцию  $f$  *взятия противоположного элемента*. А именно, положим, что для любого  $x \in \mathbb{Z}$  выполняется  $xf = -x$ . Тогда правило  $x - y = (x, y)- = (x, yf)+ = x + (-y)$  определяет вычитание для любых  $x, y \in \mathbb{Z}$ . Операция  $f$  *взятия противоположного элемента* зависит от одного, а не от двух аргументов, как это было в предыдущих примерах. Мы будем называть такие операции *унарными*, а операции, зависящие от двух аргументов, — *бинарными*.

4. В физике часто рассматривается центр масс системы тел. Пусть в пространстве  $V$  заданы три произвольные материальные точки  $A, B,$

$C$  одинаковой массы. Задача состоит в том, чтобы определить точку  $D$  пространства, которая является центром масс данной системы. Эта задача решается достаточно просто. Скажем, если точки  $A, B, C$  не лежат на одной прямой, то  $D$  — точка пересечения медиан треугольника  $ABC$ . Отображение  $f : V^3 \rightarrow V$ , ставящее в соответствие набору из трёх точек пространства точку, которая является центром масс указанной системы, можно рассматривать как алгебраическую операцию на множестве  $V$ . Естественно, можно рассмотреть аналогичную систему, состоящую из  $n$  материальных точек, что приведёт нас к операции от  $n$  аргументов.

Рассмотренные примеры приводят нас к следующему общему определению алгебраической операции.

**Определение 1.2.1.** Пусть  $A$  — непустое множество. Отображение  $f : A^n \rightarrow A$  называется  $n$ -арной (или  $n$ -местной) алгебраической операцией на множестве  $A$ . Иными словами,  $n$ -арная алгебраическая операция, заданная на множестве  $A$ , ставит в соответствие каждому упорядоченному набору из  $n$  элементов множества  $A$  некоторый однозначно определённый элемент множества  $A$ . Число  $n$  называется *арностью* или *местностью* операции  $f$ .

Теперь мы готовы определить основной объект алгебры.

**Определение 1.2.2.** Алгебраической системой называется объект  $\mathfrak{A} = \langle A, f_1, f_2, \dots, f_k, \dots \rangle$ , являющийся совокупностью непустого множества  $A$  и непустого набора алгебраических операций  $f_1, f_2, \dots, f_k, \dots$ , заданных на этом множестве. Множество  $A$  называется *носителем* или *основным множеством* системы  $\mathfrak{A}$ , а его элементы — *элементами системы*  $\mathfrak{A}$ .

Используя данное определение, можно сказать, что предметом алгебры является изучение алгебраических систем.

**ПРИМЕРЫ.** 1.  $\mathfrak{A} = \langle \mathbb{Z}, +, \cdot, f \rangle$ , где  $+$ ,  $\cdot$  — это обычные операции сложения и умножения целых чисел, а  $f$  — унарная операция взятия противоположного элемента.

2.  $\mathfrak{A} = \langle S, * \rangle$ , где  $S$  — множество всех преобразований непустого множества  $A$ , а  $*$  — композиция двух преобразований.

3.  $\mathfrak{A} = \langle \mathbb{R}[x], +, \cdot \rangle$ , где  $\mathbb{R}[x]$  — множество всех многочленов от одной переменной с коэффициентами из множества  $\mathbb{R}$  действительных чисел, а сложение и умножение заданы естественным образом.

4.  $\mathfrak{A} = \langle F, +, * \rangle$ , где  $F$  — множество всех функций из  $\mathbb{R}$  в  $\mathbb{R}$ ,  $*$  — композиция двух функций, а операция сложения определяется правилом

$$x(f + g) = xf + xg.$$

5.  $\mathfrak{A} = \langle P(A), \cap, \cup, \setminus, \neg \rangle$ , где  $P(A)$  — множество всех подмножеств некоторого непустого множества  $A$ , а операции пересечения, объединения, разности и взятия дополнения определяются в соответствии с нашими определениями из предыдущего параграфа. При этом  $\cap, \cup, \setminus$  — бинарные операции, а операция  $\neg$  взятия дополнения унарна.

6. Следующие объекты нельзя рассматривать как алгебраические системы:  $\langle \mathbb{N}, - \rangle, \langle \mathbb{Z}, : \rangle$ , так как результат операции не лежит в соответствующем множестве. Отметим, что даже на множестве  $\mathbb{Q}$  не удаётся корректно определить операцию деления, поскольку на 0 делить нельзя. Однако если мы обозначим через  $\mathbb{Q}^*$  множество  $\mathbb{Q} \setminus \{0\}$  ненулевых рациональных чисел, то  $\langle \mathbb{Q}^*, : \rangle$  — алгебраическая система. То же самое верно и для множества действительных чисел.

**УПРАЖНЕНИЕ 1.2.1.** Являются ли алгебраическими системами следующие объекты?

1. Множество  $\mathbb{Z}$  целых чисел.

2.  $\langle \mathbb{Q}^+, \sqrt{\phantom{x}} \rangle$ , где  $\mathbb{Q}^+$  — множество положительных рациональных чисел, а  $\sqrt{\phantom{x}}$  — унарная операция извлечения арифметического корня. Тот же вопрос, если в качестве носителя выбрано множество  $\mathbb{R}^+$  положительных действительных чисел.

3.  $\langle \mathbb{N}, f \rangle$ , где  $f : \mathbb{N}^2 \rightarrow \mathbb{N}$  — операция нахождения наибольшего общего делителя чисел:  $(m, n)f = \text{Н.О.Д.}(m, n)$ .

**Определение 1.2.3.** Пусть на множестве  $A$  задана  $n$ -арная алгебраическая операция  $f$ . Если непустое подмножество  $B$  множества  $A$  таково, что  $B^n f \subseteq B$  (т.е. результат операции  $f$ , произведённой над произвольными элементами множества  $B$ , снова принадлежит  $B$ ), то  $B$  называется *замкнутым* относительно операции  $f$ . При этом на множестве  $B$  определена  $n$ -арная алгебраическая операция  $f|_B : B^n \rightarrow B$ , действующая по правилу  $(b_1, b_2, \dots, b_n)f|_B = (b_1, b_2, \dots, b_n)f$ , которую мы назовём *сужением* (или *ограничением*)  $f$  на  $B$ .

**ЗАМЕЧАНИЕ.** Если подмножество  $B$  множества  $A$  замкнуто относительно операции  $f$ , то в случаях, не вызывающих недоразумений, будем использовать для сужения  $f$  на  $B$  то же самое обозначение  $f$ , что и для операции на основном множестве  $A$ .

**ПРИМЕРЫ.** 1. Подмножества  $\mathbb{Q}, \mathbb{Z}, \mathbb{N}$  множества  $\mathbb{R}$  замкнуты относительно операции сложения  $+$ , заданной на  $\mathbb{R}$ . С другой стороны, первые два из упомянутых подмножеств замкнуты относительно операции вычитания  $-$ , заданной на том же множестве, а третье — множество  $\mathbb{N}$

натуральных чисел — нет.

2. Как следует из упражнения 1.1.3, подмножество всех биекций множества всех преобразований непустого множества  $A$  замкнуто относительно операции композиции.

**УПРАЖНЕНИЕ 1.2.2.** Обозначим через  $2\mathbb{Z}$  и  $2\mathbb{Z} + 1$  множества чётных и нечётных целых чисел соответственно. Относительно каких операций, заданных на множестве  $\mathbb{Z}$  целых чисел, замкнуты эти множества? Рассмотреть бинарные операции: сложение, умножение, вычитание, деление, взятие наибольшего общего делителя; а также унарные операции: взятие противоположного элемента, удвоение, утроение. Под удвоением (утроением) понимается операция, сопоставляющая каждому целому числу  $n$  число  $2n$  ( $3n$  соответственно).

**УПРАЖНЕНИЕ 1.2.3.** Даны два взаимно простых натуральных числа  $a$  и  $b$ . Пусть подмножество  $M$  множества  $\mathbb{Z}$  целых чисел таково, что  $a, b \in M$  и  $M$  замкнуто относительно операций сложения и взятия противоположного элемента. Доказать, что  $M = \mathbb{Z}$ .

**Определение 1.2.4.** Непустое подмножество  $B$  основного множества  $A$  системы  $\mathfrak{A} = \langle A, f_1, f_2, \dots, f_k, \dots \rangle$  называется *замкнутым* в системе  $\mathfrak{A}$ , если оно замкнуто относительно каждой алгебраической операции системы  $\mathfrak{A}$ . Система  $\mathfrak{B} = \langle B, f_1|_B, f_2|_B, \dots, f_k|_B, \dots \rangle$  называется *подсистемой* системы  $\mathfrak{A}$ .

**ПРИМЕРЫ.** 1. Система  $\mathfrak{B} = \langle \mathbb{N}, +, \cdot, \rangle$  является подсистемой системы  $\mathfrak{A} = \langle \mathbb{Z}, +, \cdot, \rangle$ . Но если в  $\mathfrak{A}$  добавить операцию вычитания (или взятия противоположного элемента), то образовать подсистему, используя в качестве носителя множество  $\mathbb{N}$ , уже не удастся.

2. Пусть  $\mathfrak{A} = \langle F, +, * \rangle$ , где  $F$  — множество всех функций из  $\mathbb{R}$  в  $\mathbb{R}$ ,  $*$  — композиция двух функций, а операция сложения определяется правилом  $x(f + g) = xf + xg$ . Пусть  $\widehat{F}$  — подмножество всех возрастающих функций множества  $F$ . Тогда  $\mathfrak{B} = \langle \widehat{F}, +, * \rangle$  — подсистема системы  $\mathfrak{A}$ .

**УПРАЖНЕНИЕ 1.2.4.** Определить все конечные подсистемы (т. е. подсистемы с носителями, содержащими конечное число элементов) следующих алгебраических систем:

- 1)  $\langle \mathbb{Z}, f \rangle$ , где  $f$  — операция удвоения;
- 2)  $\langle \mathbb{Z}, \cdot \rangle$ ;
- 3)  $\langle P, f \rangle$ , где  $P$  — множество точек плоскости, а  $f$  — 3-арная (тернарная) операция, сопоставляющая трём точкам пространства их центр масс.



### § 1.3. Изоморфизм алгебраических систем

В математике очень важно иметь возможность выяснить, когда две на первый взгляд различные задачи по существу совпадают. В алгебре нас занимают только те свойства алгебраических систем и их основных множеств, которые могут быть выражены в терминах заданных операций. Если две алгебраические системы имеют одни и те же алгебраические свойства, то с точки зрения алгебраиста их можно рассматривать как идентичные. Этот подход приводит нас к понятию *изоморфизма* — биективного отображения носителя одной алгебраической системы на носитель другой, *сохраняющего* заданные операции.

**Определение 1.3.1.** Пусть заданы две алгебраические системы  $\mathfrak{A} = \langle A, f_1, f_2, \dots, f_k, \dots \rangle$  и  $\mathfrak{B} = \langle B, g_1, g_2, \dots, g_k, \dots \rangle$  с одним и тем же числом алгебраических операций, причём операции  $f_i$  и  $g_i$  с одним и тем же индексом имеют одинаковую ариность  $n_i$ . Системы  $\mathfrak{A}$  и  $\mathfrak{B}$  называются *изоморфными* (запись  $\mathfrak{A} \simeq \mathfrak{B}$ ), если существует биекция  $\varphi : A \rightarrow B$ , такая, что для любого индекса  $i$  и любого упорядоченного набора элементов  $(a_1, a_2, \dots, a_{n_i}) \in A^{n_i}$  выполняется равенство

$$((a_1, a_2, \dots, a_{n_i})f_i)\varphi = (a_1\varphi, a_2\varphi, \dots, a_{n_i}\varphi)g_i.$$

Биекция  $\varphi$ , удовлетворяющая указанному свойству, называется *изоморфизмом системы  $\mathfrak{A}$  на систему  $\mathfrak{B}$* .

**ЗАМЕЧАНИЕ.** Поскольку изоморфизм  $\varphi$  системы  $\mathfrak{A}$  на систему  $\mathfrak{B}$  является биекцией их носителей  $A$  и  $B$ , корректно определено обратное отображение  $\varphi^{-1} : B \rightarrow A$ , которое также является биекцией. Нетрудно проверить, что это отображение тоже сохраняет операции, а значит, является изоморфизмом системы  $\mathfrak{B}$  на систему  $\mathfrak{A}$ . Таким образом, если система  $\mathfrak{A}$  изоморфна системе  $\mathfrak{B}$ , то и система  $\mathfrak{B}$  изоморфна системе  $\mathfrak{A}$ , т. е. понятие изоморфизма *симметрично* относительно  $\mathfrak{A}$  и  $\mathfrak{B}$ .

**ПРИМЕРЫ.** 1. Пусть  $\mathfrak{A} = \langle \mathbb{R}, + \rangle$ ,  $\mathfrak{B} = \langle \mathbb{R}^+, \cdot \rangle$ ; здесь  $\mathbb{R}^+$  — множество положительных действительных чисел. Рассмотрим отображение  $\varphi : \mathbb{R} \rightarrow \mathbb{R}^+$ , заданное правилом  $x\varphi = 2^x$ . Докажем, что  $\varphi$  — изоморфизм  $\mathfrak{A}$  на  $\mathfrak{B}$ . Тот факт, что  $\varphi$  — биекция множества  $\mathbb{R}$  на множество  $\mathbb{R}^+$ , известен из школьного курса математики. С другой стороны, для любых  $x, y \in \mathbb{R}$  имеем

$$(x + y)\varphi = 2^{x+y} = 2^x \cdot 2^y = (x\varphi) \cdot (y\varphi),$$

откуда следует, что  $\varphi$  сохраняет операцию, а следовательно, является изоморфизмом. Аналогично обратное отображение, действующее по

правилу  $x\varphi^{-1} = \log_2(x)$ , есть изоморфизм  $\mathfrak{B}$  на  $\mathfrak{A}$ .

2. Пусть  $\mathfrak{A} = \langle \mathbb{Z}, + \rangle$ ,  $\mathfrak{B} = \langle 2\mathbb{Z}, + \rangle$ ; здесь, как и в предыдущем параграфе,  $2\mathbb{Z}$  — множество всех чётных чисел. Рассмотрим отображение  $\varphi : \mathbb{Z} \rightarrow 2\mathbb{Z}$ , заданное правилом  $x\varphi = 2x$ . Это отображение, очевидно, является биекцией, а цепочка равенств  $(x + y)\varphi = 2(x + y) = 2x + 2y = x\varphi + y\varphi$  показывает, что оно к тому же сохраняет операцию. Следовательно,  $\mathfrak{A} \simeq \mathfrak{B}$ .

Подчеркнём ещё раз, что изоморфизм систем влечёт полное совпадение их алгебраических свойств. Иными словами, любое утверждение, которое можно записать в терминах алгебраических операций, заданных на одной из изоморфных систем, будет верно и для второй системы (естественно, в терминах соответствующих операций второй системы).

Предположим теперь, что две алгебраические системы  $\mathfrak{A}$  и  $\mathfrak{B}$  не изоморфны. Вопрос состоит в том, как это доказать. Если носители  $A$  и  $B$  этих систем не равномощны, то всё очевидно, так как между ними не удастся установить биекцию. Однако если множества  $A$  и  $B$  равномощны, то проблема сложнее, поскольку проверка того факта, что некоторая биекция не сохраняет операции, не даёт права утверждать, что системы не изоморфны. Требуется проверить все биекции, а их может быть очень много. Например, если равномощные множества  $A$  и  $B$  бесконечны, то и биекций между ними бесконечно много. Тем не менее обращение к сути понятия изоморфизма подсказывает способ доказательства неизоморфности систем. Напомним, что изоморфизм систем влечёт полное совпадение их алгебраических свойств. Следовательно, если мы укажем свойство операции (операций) одной системы, которое не имеет места для соответствующей операции (операций) второй системы, то отсюда будет вытекать неизоморфность этих систем. Поясним сказанное на простом примере.

ПРИМЕР. Пусть  $\mathfrak{A} = \langle \mathbb{Z}, \cdot \rangle$ ,  $\mathfrak{B} = \langle 2\mathbb{Z}, \cdot \rangle$ . В множестве  $\mathbb{Z}$  есть элемент 1, который обладает тем свойством, что для любого  $x \in \mathbb{Z}$  имеет место равенство  $1 \cdot x = x$ . В множестве  $2\mathbb{Z}$  элемента с таким свойством нет. Воспользуемся этим для доказательства того факта, что системы  $\mathfrak{A}$  и  $\mathfrak{B}$  не изоморфны. Предположим противное, и пусть  $\varphi$  — биекция, устанавливающая изоморфизм. Положим  $1\varphi = 2k$ ,  $2\varphi = 2n$ , где  $k, n$  — некоторые целые числа. Поскольку  $\varphi$  должна сохранять операцию, выполняется цепочка равенств:  $4kn = (2k) \cdot (2n) = 1\varphi \cdot 2\varphi = (1 \cdot 2)\varphi = 2\varphi = 2n$ . Если  $n \neq 0$ , то  $2k = 1$ , что невозможно. Если же предположить, что  $2\varphi = 0$ , то можно записать аналогичную цепочку равенств для элементов  $1\varphi$  и  $3\varphi = 2m$ , последний из которых в данном случае не может быть ра-

вен 0, поскольку  $\varphi$  — взаимно однозначное отображение и  $3\varphi \neq 2\varphi = 0$ . Имеем  $4kt = (2k) \cdot (2m) = 1\varphi \cdot 3\varphi = (1 \cdot 3)\varphi = 3\varphi = 2m$ . Отсюда снова  $2k = 1$ ; противоречие. Таким образом, никакая биекция не сохраняет операцию, а значит, системы  $\mathfrak{A}$  и  $\mathfrak{B}$  не изоморфны.

УПРАЖНЕНИЕ 1.3.1. *Изоморфны ли следующие алгебраические системы:*

- 1)  $\langle \mathbb{Z}, + \rangle$  и  $\langle \mathbb{Z}, \cdot \rangle$ ;
- 2)  $\langle P(A), \cap \rangle$  и  $\langle P(A), \cup \rangle$ , здесь  $A$  — произвольное непустое множество;
- 3)  $\langle \mathbb{Q}, + \rangle$  и  $\langle \mathbb{Q}^+, \cdot \rangle$ , здесь  $\mathbb{Q}^+$  — множество положительных рациональных чисел (сравните с примером 1 к определению изоморфизма);
- 4)  $\langle \mathbb{N}, f \rangle$  и  $\langle \mathbb{N}, g \rangle$ , здесь  $f$  и  $g$  — унарные операции удвоения и утроения?

УПРАЖНЕНИЕ 1.3.2 \*. Пусть  $a, b$  — два произвольных действительных числа. Обозначим через  $\mathfrak{A}_{ab}$  алгебраическую систему  $\langle \mathbb{R}, f \rangle$  с одной унарной операцией  $f$ , действующей по правилу  $xf = ax + b$ . Сколько попарно неизоморфных алгебраических систем в множестве  $\{\mathfrak{A}_{ab} \mid a, b \in \mathbb{R}\}$ ?

# Глава 2

## Группы, кольца, поля

### § 2.1. Определения основных алгебраических структур

В силу общности определений алгебраической операции и алгебраической системы можно придумать массу примеров алгебраических систем. Далеко не все из них будут представлять реальный интерес. В этом параграфе мы определим наиболее важные классы алгебраических систем: группы, кольца и поля. Мы сделаем это, выделив естественные алгебраические свойства, которыми системы из этих классов должны обладать. Поэтому сначала мы обсудим, какие свойства можно считать наиболее существенными. Рассмотрим следующее выражение:  $(x + y) - x$ . Одного взгляда на него достаточно, чтобы уверенно заявить, что оно равно  $y$  (предполагается, что  $x$  и  $y$  — числа). Однако та лёгкость, с которой был сделан вывод, основана на хорошем знакомстве со свойствами сложения чисел. Попробуем вспомнить эти свойства, выписав подробно все шаги, которые мы совершили при преобразовании выражения:

$$(x + y) - x = (x + y) + (-x), \quad (1)$$

$$(x + y) + (-x) = (y + x) + (-x), \quad (2)$$

$$(y + x) + (-x) = y + (x + (-x)), \quad (3)$$

$$y + (x + (-x)) = y + 0, \quad (4)$$

$$y + 0 = y. \quad (5)$$

Шаг (1) соответствует определению операции вычитания через сложение с противоположным элементом. В свою очередь, определение *противоположного* элемента:  $x + (-x) = 0$  — явным образом использовалось на шаге (4). Основное свойство 0, или, как говорят в алгебре, *нейтрального элемента* по сложению, — основа шага (5). Шаг (2) — знакомый с первого класса переместительный закон сложения. Его общеупотребительное алгебраическое название — закон *коммутативности*. Наконец, шаг (3) основан на законе *ассоциативности* сложения (в элементарной математике его называют сочетательным законом). Если

добавить к указанным свойствам аналогичные свойства операции умножения, а также связывающий между собой сложение и умножение распределительный закон (свойство *дистрибутивности*), то мы получим набор базовых свойств основных операций на числовых множествах. Разумно определённые алгебраические системы (необязательно числовые) также обладают аналогичными свойствами (или некоторыми из них). Сначала мы займёмся алгебраическими системами с одной бинарной операцией. Наиболее важный класс таких систем — *группы*.

**Определение 2.1.1.** Алгебраическая система  $\mathfrak{G} = \langle G, * \rangle$  с одной бинарной операцией называется *группой*, если выполняются следующие условия (*аксиомы группы*):

1. Для любых элементов  $a, b, c \in G$  выполняется  $(a * b) * c = a * (b * c)$  (аксиома ассоциативности).
2. Существует элемент  $e \in G$ , такой, что для любого элемента  $a \in G$  выполняется  $a * e = e * a = a$  (аксиома нейтрального элемента).
3. Для любого  $a \in G$  существует элемент  $a^{-1} \in G$ , такой, что выполняется  $a * a^{-1} = a^{-1} * a = e$  (аксиома обратного элемента).

**ЗАМЕЧАНИЕ.** Подчеркнём, что термин *группа* — это не название конкретной алгебраической системы. Любая алгебраическая система с одной бинарной операцией, удовлетворяющей перечисленным аксиомам, является группой. Таким образом, с помощью термина “группа” мы выделяем целый класс алгебраических систем.

**ПРИМЕРЫ.** 1.  $\mathfrak{G} = \langle \mathbb{Z}, + \rangle$ . В данном случае групповая операция — сложение. Нейтральным элементом является число 0, а обратным элементом к целому числу  $a$ , очевидно, будет число с противоположным знаком. Группами также являются следующие числовые алгебраические системы:  $\langle \mathbb{Q}, + \rangle$ ,  $\langle \mathbb{R}, + \rangle$ ,  $\langle \mathbb{Q} \setminus \{0\}, \cdot \rangle$ ,  $\langle \mathbb{R} \setminus \{0\}, \cdot \rangle$ .

2. Если  $S$  — множество всех движений плоскости, а  $*$  — операция композиции, заданная на этом множестве, то система  $\mathfrak{G} = \langle S, * \rangle$  является группой. Относительно той же операции композиции группы образуют и множество всех параллельных переносов, и множество всех поворотов плоскости относительно заданной точки.

Несложно заметить, что все числовые алгебраические системы из примера 1 помимо аксиом группы обладают свойством коммутативности:  $a * b = b * a$ . С другой стороны, группа движений плоскости из примера 2 этим свойством не обладает (см. пример с композицией поворота и осевой симметрии из § 1.2).

**Определение 2.1.2.** Группа  $\mathfrak{G} = \langle G, * \rangle$  называется *абелевой* (или

коммутативной), если для любых двух элементов  $a, b \in G$  выполняется равенство  $a * b = b * a$  (аксиома коммутативности).

ЗАМЕЧАНИЕ. Обычно операцию в группе называют *умножением* и вместо  $a * b$  пишут просто  $ab$ . Стоит однако помнить, что носитель группы может не являться числовым множеством, а групповая операция может не иметь никакого отношения к обычному умножению чисел. Иногда, если речь идет о коммутативной группе, в качестве символа операции используют знак  $+$ , операцию называют *сложением*, нейтральный элемент называют нулём и обозначают  $0$ , а обратный элемент к элементу  $a$  называют противоположным и обозначают  $-a$ . В зависимости от обозначения групповой операции говорят о *мультипликативной* (операция — умножение) или *аддитивной* (операция — сложение) группе. В тех ситуациях, когда групповая операция заранее известна, обозначение группы отождествляют с обозначением основного множества, на котором она задана, т. е. вместо записи *группа*  $\mathfrak{G} = \langle G, * \rangle$  пишут просто *группа*  $G$ .

УПРАЖНЕНИЕ 2.1.1. Пусть  $G$  — мультипликативная группа (группа с операцией умножения),  $g$  — некоторый элемент этой группы. Доказать, что отображение  $\varphi_g : G \rightarrow G$ , действующее по правилу  $x\varphi_g = xg$  для любого элемента  $x \in G$ , является биекцией множества  $G$  на себя.

УПРАЖНЕНИЕ 2.1.2. Пусть  $G$  — группа. Доказать, что нейтральный элемент группы, определённый аксиомой 2, единствен. Доказать, что для каждого элемента  $g \in G$  его обратный элемент, определённый аксиомой 3, единствен.

Пусть  $g_1, g_2, \dots, g_n$  — элементы группы  $G$ . Определим

$$\prod_{i=1}^n g_i = (\dots (g_1 \cdot g_2) \cdot \dots) \cdot g_n.$$

УПРАЖНЕНИЕ 2.1.3. Доказать, что

$$\prod_{i=1}^n g_i = \prod_{i=1}^k g_i \cdot \prod_{i=k+1}^n g_i.$$

Указание. Воспользоваться индукцией по  $n$  с базой  $n = 3$ .

ЗАМЕЧАНИЕ. Вывод, который следует из утверждения упражнения 2.1.3, можно сформулировать так: произведение элементов группы не зависит от расстановки скобок в этом произведении (*обобщённый ассоциативный закон*).

При определении абелевой группы мы добавили к аксиомам группы дополнительную аксиому коммутативности. С другой стороны, иногда бывает полезно рассматривать алгебраические системы с одной бинарной операцией, в которых выполняются только некоторые из аксиом группы.

**Определение 2.1.3.** Алгебраическая система  $\mathfrak{G} = \langle G, * \rangle$  с одной бинарной операцией называется *полугруппой*, если она удовлетворяет аксиоме ассоциативности. Полугруппа называется *моноидом*, если в ней есть нейтральный элемент.

**ПРИМЕР.** Примером полугруппы служит множество  $\mathbb{N}$  натуральных чисел с операцией сложения (или умножения), а моноидом является множество всех преобразований произвольного непустого множества, если в качестве операции взять композицию двух преобразований (подробнее об этом позже).

**УПРАЖНЕНИЕ 2.1.4.** Пусть  $A$  — непустое множество. Доказать, что система  $\langle P(A), \cap \rangle$  — полугруппа. Является ли она моноидом?

Используя определение 2.1.3, можно определить понятие группы следующим образом: группа — это моноид, в котором каждый элемент обратим.

**Определение 2.1.4.** Пусть алгебраическая система  $\mathfrak{G} = \langle G, * \rangle$  является группой. Её подсистема  $\mathfrak{H} = \langle H, *|_H \rangle$  называется *подгруппой*, если она является группой относительно сужения  $*|_H$  групповой операции  $*$  на множество  $H$ .

**ЗАМЕЧАНИЕ.** Отметим, что не каждая подсистема группы является подгруппой. Например,  $\langle \mathbb{N}, + \rangle$  является подсистемой группы  $\langle \mathbb{Z}, + \rangle$ , но не является её подгруппой, поскольку в ней не выполняются аксиомы нейтрального элемента и обратного элемента.

Как и в случае с группой, мы будем отождествлять обозначение подгруппы  $\mathfrak{H} = \langle H, *|_H \rangle$  с обозначением её основного множества  $H$ . В частности, тот факт, что  $H$  — подгруппа группы  $G$ , мы будем кратко записывать следующим образом:  $H \leq G$ .

**ПРИМЕРЫ. 1.** В любой группе  $G$  подгруппами являются сама  $G$  и *единичная* (или *тривиальная*) *подгруппа*  $1 = \{e\}$ , состоящая из нейтрального элемента  $e$  группы  $G$ .

2. Для данного натурального числа  $n$  множество  $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$  всех целых чисел, кратных  $n$ , является подгруппой группы  $\mathbb{Z}$  целых чисел с операцией сложения.

УПРАЖНЕНИЕ 2.1.5. Пусть  $G$  — группа. Доказать, что непустое подмножество  $H$  является подгруппой группы  $G$ , если  $\forall a, b \in H$  выполняются свойства:

- 1)  $ab \in H$ ; 2)  $a^{-1} \in H$ .

Порядком группы  $G$  называется количество элементов множества  $G$ . Мы будем обозначать порядок группы через  $|G|$ . Аналогично определяется порядок подгруппы. Пусть  $g$  — элемент мультипликативной группы  $G$ . Если  $n$  — натуральное число, то через  $g^n$  мы обозначим элемент группы  $G$ , который получается в результате умножения  $g$  на себя  $n$  раз:

$$g^n = \underbrace{g \cdot g \cdot \dots \cdot g}_{n \text{ раз}}$$

Порядком элемента  $g$  группы  $G$  называется наименьшее натуральное число  $n$ , такое, что  $g^n = e$ , где  $e$  — нейтральный элемент группы  $G$ , если такое число  $n$  существует. В противном случае мы говорим, что элемент  $g$  имеет бесконечный порядок. Порядок элемента  $g$  обозначается через  $|g|$ .

УПРАЖНЕНИЕ 2.1.6. Доказать, что в конечной группе каждый элемент имеет конечный порядок.

Для удобства мы также положим, что  $g^0 = e$  и  $g^{-n} = (g^{-1})^n$ , где  $n$  — натуральное число, определив таким образом любую целую степень элемента группы.

УПРАЖНЕНИЕ 2.1.7. Пусть  $h$  — произвольный элемент группы  $G$ . Доказать, что множество  $H = \{h^n \mid n \in \mathbb{Z}\}$  является подгруппой группы  $G$ .

Теперь мы определим два важнейших класса алгебраических систем с двумя бинарными операциями. Мы будем называть эти операции сложением и умножением и обозначать через  $+$  и  $\cdot$ , не забывая о том, что они могут существенно отличаться от сложения и умножения чисел в обычном смысле.

**Определение 2.1.5.** Алгебраическая система  $\mathfrak{R} = \langle R, +, \cdot \rangle$  с двумя бинарными операциями — сложением и умножением — называется *кольцом*, если выполняются следующие условия:

1. Множество  $R$  является абелевой группой относительно сложения.
2. Для любых  $a, b, c \in R$  выполняются равенства  $(a + b)c = ac + bc$  (*правый закон дистрибутивности*) и  $c(a + b) = ca + cb$  (*левый закон дистрибутивности*).



ЗАМЕЧАНИЕ. Как и в случае с группой, мы будем зачастую использовать обозначение носителя  $R$  для самого кольца  $\mathfrak{R}$ .

Кольцо называется *ассоциативным*, если операция умножения, заданная в кольце, ассоциативна. Поскольку в нашем курсе алгебры мы будем иметь дело только с ассоциативными кольцами, договоримся, что под термином *кольцо* мы будем всегда понимать именно ассоциативное кольцо.

Кольцо называется *коммутативным*, если операция умножения, заданная в кольце, коммутативна. Кольцо называется *кольцом с единицей*, если в нём существует нейтральный по умножению элемент, который мы будем записывать как  $1$ . Отметим, что мы всегда полагаем, что в кольце с единицей  $1 \neq 0$ , в частности, кольцо с единицей содержит по крайней мере два различных элемента. Элемент кольца называется *обратимым*, если для него существует обратный по умножению элемент. Множество всех обратимых элементов кольца  $R$  обозначим через  $R^*$ .

**Определение 2.1.6.** Алгебраическая система  $\mathfrak{F} = \langle F, +, \cdot \rangle$  с двумя бинарными операциями — сложением и умножением — называется *полем*, если она является коммутативным (и, по нашей договорённости, ассоциативным) кольцом с единицей, в котором каждый ненулевой элемент обратим.

Перед тем как перейти к примерам, приведём для удобства полный список аксиом кольца и поля.

1.  $\forall a, b, c: (a + b) + c = a + (b + c)$  — ассоциативность сложения.
2.  $\forall a, b: a + b = b + a$  — коммутативность сложения.
3.  $\exists 0 \forall a: a + 0 = 0 + a = a$  — существование нуля.
4.  $\forall a \exists(-a): a + (-a) = (-a) + a = 0$  — существование противоположного элемента.
5.  $\forall a, b, c: (a + b)c = ac + bc$  — правая дистрибутивность.
6.  $\forall a, b, c: c(a + b) = ca + cb$  — левая дистрибутивность.
7.  $\forall a, b, c: (ab)c = a(bc)$  — ассоциативность умножения.
8.  $\forall a, b: ab = ba$  — коммутативность умножения.
9.  $\exists 1 \forall a: a \cdot 1 = 1 \cdot a = a$  — существование единицы.

10.  $\forall a \neq 0 \exists a^{-1}: aa^{-1} = a^{-1}a = 1$  — существование обратного элемента.

Таким образом, алгебраическая система с операциями сложения и умножения, удовлетворяющая аксиомам 1–7 (или 1–6, если не предполагать, что кольцо ассоциативно), является кольцом, а система, удовлетворяющая аксиомам 1–10, является полем.

ПРИМЕРЫ. 1. Числовые алгебраические системы  $\langle \mathbb{Z}, +, \cdot \rangle$ ,  $\langle \mathbb{Q}, +, \cdot \rangle$ ,  $\langle \mathbb{R}, +, \cdot \rangle$  являются кольцами. Первая из них является коммутативным кольцом с единицей, но не является полем. Вторая и третья системы являются полями.

2. Определим на множестве  $P(A)$  всех подмножеств непустого множества  $A$  операцию *симметрической разности*  $\Delta$  по правилу:  $\forall B, C \subseteq A$  имеем  $B \Delta C = (B \setminus C) \cup (C \setminus B)$ . Система  $\langle P(A), \Delta, \cap \rangle$  является коммутативным кольцом с единицей.

3. Множество всех векторов трёхмерного пространства относительно операций сложения и векторного произведения образует неассоциативное (и некоммутативное) кольцо.

Как и в случае с группой, *подкольцо (подполе)* определяется как подсистема кольца (поля), которая сама является кольцом (полем) относительно сужений операций сложения и умножения, заданных в кольце (в поле).

ПРИМЕР. Подмножество  $n\mathbb{Z}$  образует подкольцо кольца целых чисел относительно обычных операций сложения и умножения. Поле рациональных чисел, очевидно, является подполем поля действительных чисел.

Как и в случае с группой, под *порядком* кольца (поля) мы понимаем количество элементов в его носителе.

ПРИМЕР. Поле из двух элементов можно определить, записав для его элементов, а это по необходимости 0 и 1 (не путать с числами!), таблицы сложения и умножения:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Это поле, которое мы обозначим через  $\mathbb{Z}_2$ , — частный пример кольца  $\mathbb{Z}_n$  вычетов по модулю  $n$  (см. упражнения в конце этого параграфа).

Если взглянуть на таблицу умножения поля  $\mathbb{Z}_2$ , обнаруживается, что для любого элемента  $a \in \mathbb{Z}_2$  выполняется  $a \cdot 0 = 0 \cdot a = 0$ . Это же

свойство, как известно, присуще и числовым кольцам (см. примеры). Сейчас мы докажем, что это свойство имеет место в любом кольце (в том числе и неассоциативном).

**Предложение 2.1.1.** Пусть  $R$  — кольцо. Для любого элемента  $a \in R$  имеет место равенство  $a \cdot 0 = 0 \cdot a = 0$ .

**ДОКАЗАТЕЛЬСТВО.** Мы докажем только равенство  $a0 = 0$ , поскольку второе доказывается аналогично. Пусть  $a0 = b$ . Тогда

$$b + b = a0 + a0 = a(0 + 0) = a0 = b.$$

Прибавляя к обеим частям равенства  $b + b = b$  противоположный к  $b$  элемент, получаем  $(b + b) + (-b) = b + (-b)$ . Откуда  $b + (b + (-b)) = 0$ , а значит,  $b + 0 = 0$ , и окончательно  $b = 0$ .  $\square$

Отметим, что в произвольном кольце из равенства  $ab = 0$ , вообще говоря, не следует, что  $a = 0$  или  $b = 0$ . Ненулевые элементы кольца, для которых имеет место равенство  $ab = 0$ , называют *делителями нуля*. Кольцо, в котором таких делителей нет, называют *кольцом без делителей нуля*. Примером кольца без делителей нуля может служить произвольное поле.

**Предложение 2.1.2.** В поле нет делителей нуля.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $F$  — поле и элементы  $a, b \in F$  таковы, что  $ab = 0$ , но  $a \neq 0$  и  $b \neq 0$ . Умножим каждую часть равенства  $ab = 0$  справа на элемент  $b^{-1}$ , обратный к элементу  $b$  (его существование следует из аксиомы 10). Имеем  $(ab)b^{-1} = 0b^{-1}$ . Левая часть этого равенства в силу ассоциативности умножения равна  $a(bb^{-1})$ , а значит, в силу аксиом 9 и 10 она равна  $a$ . Правая часть равенства в силу предложения 2.1.1 равна 0. Полученное противоречие доказывает наше утверждение.  $\square$

Утверждение предложения 2.1.1 выполняется для любой алгебраической системы, являющейся кольцом, а утверждение предложения 2.1.2 — для любой алгебраической системы, являющейся полем. Поэтому, доказав эти предложения, мы получили результаты, касающиеся не одной конкретной системы, а целого класса алгебраических систем. В этом состоит значение абстрактного подхода к алгебре.

**УПРАЖНЕНИЕ 2.1.8.** Зафиксируем натуральное число  $n$ . Для произвольного целого числа  $k$  обозначим через  $\bar{k}$  множество всех целых чисел, сравнимых с  $k$  по модулю  $n$ . Пусть  $\mathbb{Z}_n = \{\bar{k} \mid k \in \mathbb{Z}\}$ . Показать, что операции сложения и умножения, заданные формулами:  $\bar{i} + \bar{j} = \overline{i + j}$ ,  $\bar{i} \cdot \bar{j} = \overline{i \cdot j}$ , корректно определены на  $\mathbb{Z}_n$ , и доказать, что относительно

указанных операций множество  $\mathbb{Z}_n$  образует кольцо. Это кольцо называется кольцом вычетов по модулю  $n$ .

УПРАЖНЕНИЕ 2.1.9. Доказать, что кольцо  $\mathbb{Z}_n$  является полем тогда и только тогда, когда  $n$  — простое число.

УПРАЖНЕНИЕ 2.1.10. Сформулировать определение изоморфизма для колец и доказать, что любой изоморфизм кольца целых чисел на себя является тождественным.

## § 2.2. Группа подстановок

**Определение 2.2.1.** Биективное преобразование  $\pi$  непустого множества  $M$ , т. е. взаимно однозначное отображение  $M$  на себя, называется *подстановкой* множества  $M$ .

ПРИМЕРЫ. 1. Преобразование  $\pi$  множества  $\mathbb{N}$  натуральных чисел, определённое правилом

$$n\pi = \begin{cases} 2k - 1, & \text{при } n = 2k, \\ 2k, & \text{при } n = 2k - 1, \end{cases}$$

является подстановкой, а преобразование  $\chi$  того же множества по правилу  $n\chi = 2n$  — нет, поскольку это отображение — инъекция, но не сюръекция.

2. Преобразование  $\pi$  множества  $M = \{1, 2, 3\}$  по правилу  $1\pi = 2$ ,  $2\pi = 3$ ,  $3\pi = 1$ , будет подстановкой, а преобразование  $\chi$  того же множества  $M$  по правилу  $1\chi = 2$ ,  $2\chi = 3$ ,  $3\chi = 2$ , — нет.

В случае, когда множество  $M$  конечно, подстановку удобно записывать в виде таблицы из двух строк. Например, подстановка  $\pi$  из примера 2 при такой форме записи будет выглядеть следующим образом:

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

При этом в первой строке перечисляются все элементы множества, а затем под каждый из них *подставляется* его образ при отображении  $\pi$ . Термин *подстановка* появился именно из-за этой формы записи. Отметим, что элементы в первой строке подстановки могут располагаться в любом порядке. В частности,

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

**Теорема 2.2.1.** *Множество  $S(M)$  всех подстановок непустого множества  $M$  образует группу относительно операции композиции.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\pi, \sigma$  — две подстановки множества  $S(M)$ . Докажем, во-первых, что их композиция  $\pi * \sigma$  тоже является подстановкой. Заметим, что  $\pi * \sigma$  — преобразование множества  $M$ . Поэтому нам остаётся показать, что  $\pi * \sigma$  — биективное преобразование. Для любых  $x, y \in M$  из равенства  $x(\pi * \sigma) = y(\pi * \sigma)$  следует равенство  $(x\pi)\sigma = (y\pi)\sigma$ . Поскольку  $\sigma$  — биекция, имеем  $x\pi = y\pi$ . Но  $\pi$  — тоже биекция, откуда  $x = y$ . Следовательно,  $\pi * \sigma$  — инъекция. С другой стороны, подстановки  $\pi$  и  $\sigma$  как биекции имеют обратные отображения  $\pi^{-1}$  и  $\sigma^{-1}$ , которые тоже являются биекциями, а значит, подстановками. Для произвольного элемента  $x \in M$  элемент  $y = (x\sigma^{-1})\pi^{-1} \in M$  обладает тем свойством, что  $y(\pi * \sigma) = ((x\sigma^{-1})\pi^{-1})(\pi * \sigma) = ((x\sigma^{-1})(\pi^{-1} * \pi))\sigma = (x\sigma^{-1})\sigma = x$ . А значит,  $\pi * \sigma$  — сюръекция. Поэтому  $\pi * \sigma$  — подстановка. Таким образом,  $\langle S(M), * \rangle$  — алгебраическая система.

Проверим теперь, что эта система является группой. Нейтральным элементом этой системы является тождественная подстановка  $\varepsilon$ , действующая на каждом элементе  $x \in M$  по правилу  $x\varepsilon = x$ . С другой стороны, для каждой подстановки  $\pi$  существует обратное преобразование  $\pi^{-1}$ , которое тоже является биекцией, а значит, подстановкой. Поэтому аксиомы 2 и 3 группы выполнены. Осталось доказать, что операция композиции подстановок ассоциативна. Мы докажем более общее утверждение:

**Предложение 2.2.1.** *Пусть  $f : X \rightarrow Y, g : Y \rightarrow U, h : U \rightarrow W$  — произвольные отображения, тогда  $(f * g) * h = f * (g * h)$ .*

**ДОКАЗАТЕЛЬСТВО ПРЕДЛОЖЕНИЯ.** Пусть  $x$  — произвольный элемент множества  $X$ . Утверждение предложения следует из следующей цепочки равенств:

$$x((f * g) * h) = (x(f * g))h = ((xf)g)h = (xf)(g * h) = x(f * (g * h)).$$

Поскольку подстановка — частный случай отображения, ассоциативность композиции подстановок следует из предложения 2.2.1.  $\square$

Поскольку  $S(M)$  — группа, мы будем называть композицию подстановок  $\pi$  и  $\sigma$  *произведением*, операцию композиции — *умножением* подстановок и писать  $\pi \cdot \sigma$  или  $\pi\sigma$  вместо  $\pi * \sigma$ .

ПРИМЕР. Пусть  $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ ,  $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ . Тогда

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

#### УПРАЖНЕНИЕ 2.2.1.

1. Перемножить подстановки  $\pi$  и  $\sigma$  из примера в обратном порядке и убедиться, что  $\pi\sigma \neq \sigma\pi$ .
2. Найти порядки подстановок  $\pi$  и  $\sigma$  как элементов группы.
3. Найти подстановки  $\pi^{100}$  и  $\sigma^{100}$ .
4. Найти подстановки  $\pi^{-1}$  и  $\sigma^{-1}$ , обратные к подстановкам  $\pi$  и  $\sigma$ .

**Определение 2.2.2.** Группа  $S(M)$  всех подстановок множества  $M$  называется *симметрической группой подстановок* множества  $M$  (иногда она также обозначается как  $\text{Sym}(M)$ ). Произвольную подгруппу этой группы будем называть *группой подстановок* множества  $M$ .

Поскольку свойства группы подстановок множества  $M$  не зависят от природы элементов из  $M$ , симметрические группы подстановок равномогущих множеств изоморфны. В случае, когда множество  $M$  конечно и состоит из  $n$  элементов, будем обозначать симметрическую группу подстановок множества  $M$  через  $S_n$  (*симметрическая группа степени  $n$* ) и полагать, что  $M = \{1, 2, \dots, n\}$ . Элементы множества  $M$  будем называть *символами*. В нашем курсе мы будем иметь дело прежде всего с группами подстановок, заданных на конечных множествах.

УПРАЖНЕНИЕ 2.2.2. Доказать, что  $|S_n| = n!$ . Выписать все подстановки из группы  $S_3$ . Составить таблицу умножения для группы  $S_3$ . Найти все подгруппы группы  $S_3$ .

Будем записывать произвольную подстановку  $\pi$  группы  $S_n$  как

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix},$$

подразумевая, что  $\{i_1, i_2, \dots, i_n\} = \{1, 2, \dots, n\}$  и  $1\pi = i_1, 2\pi = i_2, \dots, n\pi = i_n$ . Иногда мы будем нарушать порядок элементов в первой строке и записывать произвольную подстановку как

$$\pi = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix},$$

где  $i_k \pi = j_k$ . В частности, подстановка  $\pi^{-1}$  может быть записана следующим образом:

$$\pi^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Теперь мы рассмотрим вопрос о структуре множества символов  $M = \{1, 2, \dots, n\}$  относительно действия на нём некоторой подстановки  $\pi \in S_n$ . Пусть  $i$  — произвольный символ из  $M$ . Если  $i\pi = i$ , т. е.  $i$  остаётся на месте под действием подстановки  $\pi$ , то мы будем называть  $i$  *неподвижным символом* относительно  $\pi$ . Если  $i\pi \neq i$ , то будем говорить, что  $i$  — *перемещаемый символ*. Множество всех перемещаемых подстановкой  $\pi$  символов обозначим через  $\text{supp}(\pi)$  и назовём *носителем* или *суппортом* подстановки  $\pi$ . Таким образом, подстановка

$$\pi = \begin{pmatrix} i_1 & i_2 & \dots & i_s & k_1 & \dots & k_t \\ j_1 & j_2 & \dots & j_s & k_1 & \dots & k_t \end{pmatrix},$$

где  $i_l \neq j_l$  для любого  $l \in \{1, 2, \dots, s\}$ , имеет носитель  $\text{supp}(\pi) = \{i_1, i_2, \dots, i_s\}$ . Несложно заметить, что образ  $\text{supp}(\pi)\pi = \{j_1, j_2, \dots, j_s\}$  носителя  $\text{supp}(\pi)$  под действием  $\pi$  совпадает с самим носителем, т. е.  $\text{supp}(\pi)\pi = \text{supp}(\pi)$ . Кроме того,  $\text{supp}(\varepsilon) = \emptyset$  и  $\text{supp}(\pi^{-1}) = \text{supp}(\pi)$ , где  $\varepsilon$  — тождественная, а  $\pi^{-1}$  — обратная к  $\pi$  подстановки.

Пусть  $i_1 \in \text{supp}(\pi)$  и  $i_1\pi = i_2$ ,  $i_2\pi = i_3$  и т. д., а  $s$  — наименьшее натуральное число, такое, что  $i_s\pi \in \{i_1, i_2, \dots, i_s\}$ . Указанное число  $s$  существует из-за конечности множества  $M$ , а значит, и множества  $\text{supp}(\pi)$ . Несложно заметить, что  $i_s\pi = i_1$ , поскольку элементы  $i_2, \dots, i_s$  уже имеют прообразы  $i_1, \dots, i_{s-1}$ . Множество  $\{i_1, i_2, \dots, i_s\}$  называется *нетривиальной орбитой* подстановки  $\pi$  длины  $s$  (*тривиальная орбита* состоит из неподвижного элемента). Каждая нетривиальная орбита имеет циклическое строение: все символы, входящие в орбиту, могут быть получены из произвольного символа орбиты путём последовательного действия подстановкой  $\pi$ . Следовательно, две орбиты подстановки либо не пересекаются, либо совпадают, и каждый символ из  $M$  принадлежит некоторой орбите (тривиальной или нетривиальной). Таким образом, множество  $M$  относительно подстановки  $\pi$  распадается в объединение непересекающихся орбит, а носитель  $\text{supp}(\pi)$  — в объединение непересекающихся нетривиальных орбит.

ПРИМЕР. Пусть

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

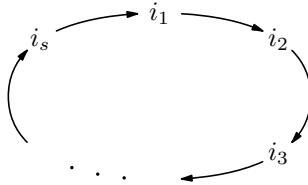
Тогда  $\{1, 6, 4\}$ ,  $\{2, 3\}$ ,  $\{5\}$  — орбиты подстановки  $\pi$  на множестве  $M$ , первые две из них нетривиальны. Имеем  $M = \{1, 6, 4\} \cup \{2, 3\} \cup \{5\}$  и  $\text{supp}(\pi) = \{1, 6, 4\} \cup \{2, 3\}$ .

В соответствие с разбиением множества  $\text{supp}(\pi)$  в объединение непесекающихся орбит существует удобная форма представления подстановки в виде произведения независимых циклов, которую мы сейчас и рассмотрим.

**Определение 2.2.3.** Подстановка  $\pi \in S_n$  вида

$$\left( \begin{array}{cccccccc} i_1 & i_2 & \dots & i_{s-1} & i_s & k_1 & \dots & k_t \\ i_2 & i_3 & \dots & i_s & i_1 & k_1 & \dots & k_t \end{array} \right),$$

где  $\{i_1, i_2, \dots, i_s, k_1, \dots, k_t\} = \{1, 2, \dots, n\}$  и  $s \geq 2$ , называется *циклом* длины  $s$  и обозначается как  $(i_1, i_2, \dots, i_s)$ .



Иными словами, подстановка является циклом тогда и только тогда, когда её носитель состоит ровно из одной нетривиальной орбиты.

**ПРИМЕРЫ.** 1. Следующая подстановка является циклом длины три:

$$\left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{array} \right) = \left( \begin{array}{cccc} 1 & 2 & 4 & 3 \\ 2 & 4 & 1 & 3 \end{array} \right) = (1, 2, 4) = (2, 4, 1) = (4, 1, 2).$$

2. Подстановка  $\left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{array} \right)$  циклом не является.

**Предложение 2.2.2.** Порядок  $|\alpha|$  цикла  $\alpha$  длины  $s$  (как элемента группы  $S_n$ ) равен  $s$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\alpha = (i_1, i_2, \dots, i_s)$ . Наименьшее натуральное число  $k$ , такое, что  $i_1 \pi^k = i_1$ , равно  $s$ . Но тогда  $i_l \pi^s = i_l$  для любого  $l = 1, 2, \dots, s$ . □

**Определение 2.2.4.** Циклы  $\alpha$  и  $\beta$  из  $S_n$  называются *независимыми*, если  $\text{supp}(\alpha) \cap \text{supp}(\beta) = \emptyset$ .

**Предложение 2.2.3.** Если циклы  $\alpha$  и  $\beta$  независимы, то  $\alpha\beta = \beta\alpha$ .



ДОКАЗАТЕЛЬСТВО. Пусть  $i$  — произвольный символ из  $M$ . Разберём последовательно три возможных случая.

1.  $i \notin \text{supp}(\alpha) \cup \text{supp}(\beta)$ . Тогда  $i\alpha\beta = i = i\beta\alpha$ .
2.  $i \in \text{supp}(\alpha)$ . Тогда  $i\alpha\beta = i\alpha = i\beta\alpha$ .
3.  $i \in \text{supp}(\beta)$ . Тогда  $i\alpha\beta = i\beta = i\beta\alpha$ . □

**Следствие.** Если  $\alpha_1, \alpha_2, \dots, \alpha_k$  — попарно независимые циклы, то порядок подстановки  $\alpha_1\alpha_2 \dots \alpha_k$  равен наименьшему общему кратному длин циклов  $\alpha_1, \alpha_2, \dots, \alpha_k$ .

УПРАЖНЕНИЕ 2.2.3. Доказать следствие из предложения 2.2.3.

**Теорема 2.2.2.** Пусть  $\pi$  — нетождественная подстановка из  $S_n$ . Тогда  $\pi = \sigma_1\sigma_2 \dots \sigma_k$  есть произведение попарно независимых циклов  $\sigma_1, \sigma_2, \dots, \sigma_k$ . Это разложение единственно с точностью до порядка сомножителей.

ДОКАЗАТЕЛЬСТВО. Проведём доказательство индукцией по числу нетривиальных орбит, на которые множество  $M = \{1, 2, \dots, n\}$  распадается под действием подстановки  $\pi$ . Поскольку  $\pi$  не тождественна, по крайней мере одна такая орбита  $\{i_1, i_2, \dots, i_s\}$  существует. Пусть  $\sigma_1 = (i_1, i_2, \dots, i_s)$  — соответствующий этой орбите цикл. Если других нетривиальных орбит нет, то  $\pi = \sigma_1$  — цикл, и теорема доказана.

Предположим, что  $\text{supp}(\sigma_1) \subset \text{supp}(\pi)$ , и рассмотрим подстановку  $\pi_1 = \sigma_1^{-1}\pi$ . Если  $i \in \text{supp}(\sigma_1)$ , т. е.  $i = i_l$  для некоторого  $l \in \{1, 2, \dots, s\}$ , то  $i\pi_1 = i_l\pi_1 = i_l(\sigma_1^{-1}\pi) = (i_l\sigma_1^{-1})\pi = i_{l-1}\pi = i_l = i$ . Поэтому все символы из  $\text{supp}(\sigma_1)$  неподвижны относительно действия подстановки  $\pi_1$ . С другой стороны, если  $i \notin \text{supp}(\sigma_1)$ , то  $i\pi_1 = i(\sigma_1^{-1}\pi) = (i\sigma_1^{-1})\pi = i\pi$ . Иными словами, на всех остальных символах действие подстановки  $\pi_1$  совпадает с действием подстановки  $\pi$ . Таким образом, подстановка  $\pi_1$  имеет носитель  $\text{supp}(\pi_1) = \text{supp}(\pi) \setminus \text{supp}(\sigma_1)$ , и он распадается на нетривиальные орбиты, число которых на единицу меньше, чем у носителя  $\text{supp}(\pi)$  исходной подстановки. Следовательно, по предположению индукции  $\pi_1 = \sigma_2 \dots \sigma_k$  есть произведение независимых циклов  $\sigma_2, \dots, \sigma_k$ , причём это разложение единственно с точностью до порядка сомножителей. Поскольку  $\pi = \sigma_1\pi_1$  и  $\text{supp}(\sigma_1) \cap \text{supp}(\pi_1) = \emptyset$ , разложение  $\pi = \sigma_1\sigma_2 \dots \sigma_k$  является искомым.

Предположим, что  $\pi = \tau_1\tau_2 \dots \tau_m$  — другое разложение  $\pi$  в произведение независимых циклов. Поскольку  $i_1 \in \text{supp}(\pi)$ , найдётся цикл  $\tau_l$  из этого разложения, такой, что  $i_1 \in \text{supp}(\tau_l)$ . Так как циклы  $\tau_1, \tau_2, \dots, \tau_m$  независимы, то они перестановочны, и можно считать, что

$i_1 \in \text{supp}(\tau_1)$ . Тогда выполняются равенства

$$i_1\tau_1 = i_1\pi = i_1\sigma_1 = i_2, i_2\tau_1 = i_2\pi = i_2\sigma_1 = i_3, \dots, i_s\tau_1 = i_s\pi = i_s\sigma_1 = i_1.$$

Отсюда  $\tau_1 = \sigma_1$  и  $\pi = \tau_1\pi_1 = \sigma_1\pi_1$ , а однозначность разложения  $\pi_1$  вытекает из предположения индукции.  $\square$

**ЗАМЕЧАНИЕ.** Иногда удобно считать, что неподвижный символ  $i$  относительно подстановки  $\pi$  образует цикл единичной длины, и записывать этот цикл как  $(i)$ .

**ПРИМЕР.** Для подстановки

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 1 & 5 & 4 \end{pmatrix}$$

имеет место разложение  $\pi = (1, 6, 4)(2, 3)$  или, если необходимо упомянуть неподвижные символы,  $\pi = (1, 6, 4)(2, 3)(5)$ .

Таким образом, имеется взаимно однозначное соответствие между орбитами, на которые разбивается множество  $M$  относительно подстановки  $\pi$ , и циклами, в произведение которых  $\pi$  раскладывается. Причём это верно как в случае, когда мы учитываем только нетривиальные орбиты и неединичные циклы, так и в общем случае.

Имеется ещё один существенный для нас способ разложить подстановку в произведение циклов специального вида, так называемых *транспозиций*.

**Определение 2.2.5.** Цикл длины 2 называется *транспозицией*.

**Предложение 2.2.4.** Каждая подстановка  $\pi \in S_n$  разлагается в произведение транспозиций.

**ДОКАЗАТЕЛЬСТВО.** В силу теоремы 2.2.2 достаточно представить в виде произведения транспозиций произвольный цикл. Пусть  $\sigma = (i_1, i_2, \dots, i_s)$  — цикл длины  $s$ . Непосредственно проверяется, что  $\sigma = (i_1, i_2)(i_1, i_3) \dots (i_1, i_s)$  — искомое разложение.  $\square$

Представление произвольной подстановки в виде произведения транспозиций в отличие от её представления в виде произведения независимых циклов уже не является однозначным. В частности, число транспозиций в различных разложениях одной и той же подстановки может быть различным.

**ПРИМЕР.**  $(1, 2)(1, 3)(1, 2) = (2, 3)$ .

Тем не менее чётность этого числа не зависит от способа разложения. Доказательству этого важного факта мы и посвятим остаток параграфа.

**Определение 2.2.6.** Пусть подстановка  $\pi \in S_n$ , множество  $\text{supp}(\pi)$  перемещаемых символов которой состоит из  $m$  элементов, разлагается в произведение  $k$  независимых циклов. *Декрементом*  $d(\pi)$  подстановки  $\pi$  называется разность  $m - k$ . *Знаком* подстановки  $\pi$  называется число  $\text{sgn}(\pi) = (-1)^{d(\pi)}$ . Подстановка называется *чётной*, если  $\text{sgn}(\pi) = 1$ , и *нечётной*, если  $\text{sgn}(\pi) = -1$ .

**ПРИМЕР.** Для подстановки  $\pi$  из предыдущего примера имеем  $d(\pi) = 5 - 2 = 3$ ,  $\text{sgn}(\pi) = (-1)^3 = -1$ , т. е. подстановка  $\pi$  нечётна.

**ЗАМЕЧАНИЕ.** Декремент подстановки  $\pi$  множества  $M$  можно также определить как разность между общим числом символов в  $M$  и общим числом циклов (включая единичные).

**Теорема 2.2.3.** *Умножение на транспозицию меняет знак подстановки на противоположный.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\pi$  — подстановка, а  $\tau = (i, j)$  — транспозиция из  $S_n$ . На самом деле мы докажем более сильное утверждение, чем в формулировке теоремы. А именно, покажем, что  $d(\pi\tau) = d(\pi) \pm 1$ . Пусть  $\pi = \sigma_1\sigma_2 \dots \sigma_k$  — разложение подстановки в произведение циклов (в том числе и единичных). Для удобства договоримся считать, что  $\text{supp}(\sigma) = \{i\}$  в случае единичного цикла  $\sigma = (i)$ . Символы  $i$  и  $j$ , перемещаемые транспозицией  $\tau$ , либо лежат в одной орбите относительно действия  $\pi$ , либо в двух разных орбитах. Разберём обе эти возможности.

Пусть сначала  $i, j$  лежат в одной орбите  $\{k_1, k_2, \dots, k_s\}$ , т. е. найдётся цикл  $\sigma = (k_1, k_2, \dots, k_s)$  в разложении  $\pi$  на независимые циклы, такой, что  $i, j \in \text{supp}(\sigma)$ . Пусть для определённости  $i = k_1, j = k_m$  (напомним, что цикл можно начинать с любого символа). Тогда непосредственно проверяется, что  $(k_1, \dots, k_m, \dots, k_s)(i, j) = (k_1, \dots, k_{m-1})(k_m, \dots, k_s)$ . Таким образом, в разложении подстановки вместо одного из независимых циклов появляются два новых независимых цикла (циклы, носитель которых не содержит  $i, j$ , очевидно, не изменятся). Следовательно, в этом случае  $d(\pi\tau) = d(\pi) - 1$ .

Пусть теперь  $i$  лежит в орбите  $\{i_1, i_2, \dots, i_s\}$  и  $i = i_1$ , а  $j$  лежит в орбите  $\{j_1, j_2, \dots, j_t\}$  и  $j = j_1$  (подчёркнём, что орбиты могут в этом случае быть и тривиальными). Этим орбитам в разложении  $\pi$  соответствуют независимые циклы  $(i_1, i_2, \dots, i_s)$  и  $(j_1, j_2, \dots, j_t)$ . Равенство  $(i_1, i_2, \dots, i_s)(j_1, j_2, \dots, j_t)(i, j) = (i_1, i_2, \dots, i_s, j_1, \dots, j_t)$  показывает, что в рассматриваемом нами случае два независимых цикла в разложении  $\pi$  превращаются в один цикл в разложении  $\pi\tau$ . Таким образом,  $d(\pi\tau) = d(\pi) + 1$ .  $\square$

**ЗАМЕЧАНИЕ.** При доказательстве теоремы мы умножали подстановку на транспозицию справа. Несложно понять, что аналогичные рассуждения проходят при умножении на транспозицию слева.

**Следствие 1.** Чётность числа транспозиций, в произведение которых разлагается подстановка  $\pi$ , не зависит от способа разложения и совпадает с чётностью декремента  $d(\pi)$ .

**ДОКАЗАТЕЛЬСТВО.** Начнём с того, что декремент тождественной подстановки  $\varepsilon$  равен нулю, а значит,  $\text{sgn}(\varepsilon) = 1$ . Пусть  $\pi = \tau_1 \tau_2 \dots \tau_k$  — произвольное разложение подстановки  $\pi$  в произведение транспозиций. По теореме 2.2.3 имеем  $\text{sgn}(\tau_1) = \text{sgn}(\varepsilon \tau_1) = (-1)^1$ . Аналогично  $\text{sgn}(\tau_1 \tau_2) = (-1)^2$  и т. д. Таким образом,  $\text{sgn}(\pi) = (-1)^{d(\pi)} = (-1)^k$ .  $\square$

**УПРАЖНЕНИЕ 2.2.4.** Доказать, что наименьшее возможное число транспозиций, в произведение которых можно разложить произвольную подстановку  $\pi$ , равно её декременту  $d(\pi)$ .

Отметим ещё одно полезное следствие из только что доказанной теоремы.

**Следствие 2.** Пусть  $\pi, \sigma$  — произвольные подстановки из  $S_n$ . Тогда  $\text{sgn}(\pi\sigma) = \text{sgn}(\pi) \text{sgn}(\sigma)$ .

**УПРАЖНЕНИЕ 2.2.5.** Доказать следствие 2 из теоремы 2.2.3.

**УПРАЖНЕНИЕ 2.2.6. 1.** Доказать, что число чётных подстановок множества  $M$  равно числу нечётных подстановок того же множества.

2. Доказать, что подмножество  $A_n$  всех чётных подстановок из группы  $S_n$  является подгруппой в  $S_n$ .

3. Доказать, что при  $n \geq 3$  каждый элемент из группы  $A_n$  разлагается в произведение циклов длины 3.

Группа  $A_n$  из упражнения 2.2.6 называется *знакопеременной группой подстановок*.

**УПРАЖНЕНИЕ 2.2.7\*.** Доказать, что каждый элемент из  $S_n$  представим в виде произведения двух элементов порядка 2.

## § 2.3. Кольцо квадратных матриц

**Определение 2.3.1.** Пусть задано непустое множество  $S$ . Матрицей над  $S$  размера  $m$  на  $n$  (или  $(m \times n)$ -матрицей) называется прямо-

угольная таблица вида

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

где  $a_{ij} \in S$ ,  $i \in \{1, 2, \dots, m\}$  — номер строки,  $j \in \{1, 2, \dots, n\}$  — номер столбца таблицы. В случае когда число строк матрицы совпадает с числом столбцов, т. е.  $m = n$ , будем называть матрицу *квадратной*, а число  $n$  — *размерностью* матрицы. Множество всех матриц размера  $m$  на  $n$  над  $S$  обозначается через  $M_{m \times n}(S)$ , а множество всех квадратных  $(n \times n)$ -матриц — через  $M_n(S)$ .

Мы будем обозначать матрицу заглавной буквой и использовать ту же строчную букву для обозначения её элементов. Например, будем писать  $A = (a_{ij})$  или  $A = (a_{ij})_{m \times n}$ , если хотим подчеркнуть её размер. Две матрицы  $A$  и  $B$  *равны*, если они имеют один и тот же размер и их элементы, стоящие на одних и тех же местах, равны: если  $A = (a_{ij})_{m \times n}$ ,  $B = (b_{ij})_{m \times n}$ , то  $A = B \Leftrightarrow a_{ij} = b_{ij} \forall i = 1 \dots m, \forall j = 1 \dots n$ .

ПРИМЕРЫ.

1.  $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$  — матрица размера  $2 \times 3$  над множеством  $\{1\}$ .
2.  $(1 \ 2 \ 3 \ 4 \ 5)$  — матрица размера  $1 \times 5$  над множеством  $\mathbb{N}$ .
3.  $\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}$  — матрица размера  $4 \times 1$  над множеством  $\mathbb{N}$ .

Иногда мы будем называть матрицы размера  $1 \times n$  *строками* длины  $n$ , а матрицы размера  $m \times 1$  — *столбцами* высоты  $m$ . В этой терминологии матрица из примера 2 — строка длины 5, а матрица из примера 3 — столбец высоты 4.

ЗАМЕЧАНИЕ. Назвав матрицу прямоугольной таблицей, мы, конечно, пожертвовали математической строгостью в угоду интуитивной ясности. Недостаток строгости в определении матрицы можно исправить следующим образом. Очевидно, что множество всех строк длины  $n$  над множеством  $S$  может быть отождествлено с множеством всех упорядоченных  $n$ -ок элементов из  $S$ , т. е. с декартовой  $n$ -ой степенью  $S^n$  множества  $S$ . Тогда множество  $M_{m \times n}(S)$  всех матриц размера  $m$  на  $n$  над  $S$

можно рассматривать как множество всех упорядоченных  $m$ -ок, элементами которых являются упорядоченные  $n$ -ки элементов из  $S$ , или, иными словами, как декартову  $m$ -ую степень  $(S^n)^m$  множества  $S^n$ .

Ещё один вариант состоит в том, чтобы дать определение матрицы на языке отображений. Пусть  $I = \{(i, j) \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ . Произвольная матрица  $A = (a_{ij})$  из множества  $M_{m \times n}(S)$  может быть определена как отображение из множества  $I$  в множество  $S$ , сопоставляющее каждой паре индексов  $(i, j)$  элемент  $a_{ij} \in S$ , а само множество  $M_{m \times n}(S)$  — как множество всех таких отображений.

Пусть на множестве  $S$  задана операция сложения  $+$ . Тогда матрицы одного и того же размера будем складывать по следующему правилу:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1n} \\ b_{21} & \dots & b_{2n} \\ \dots & \dots & \dots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & \dots & a_{2n} + b_{2n} \\ \dots & \dots & \dots \\ a_{m1} + b_{m1} & \dots & a_{mn} + b_{mn} \end{pmatrix}.$$

Дадим точное определение.

**Определение 2.3.2.** Пусть  $A = (a_{ij})_{m \times n}$ ,  $B = (b_{ij})_{m \times n}$  — матрицы одного и того же размера над множеством  $S$  с операцией сложения. Суммой матриц  $A$  и  $B$  называется матрица  $C = (c_{ij})_{m \times n} = A + B$  над  $S$  того же размера, для которой  $c_{ij} = a_{ij} + b_{ij}$ .

Если на  $S$  помимо ассоциативной и коммутативной операции сложения задана операция умножения, то на матрицах согласованных размеров можно определить операцию умножения следующим образом.

**Определение 2.3.3.** Пусть  $A = (a_{ik})_{m \times s}$  и  $B = (b_{kj})_{s \times n}$  — две матрицы над  $S$ , такие, что число столбцов первой матрицы равно числу строк второй матрицы. Пусть на  $S$  заданы операции сложения и умножения. Произведением матриц  $A$  и  $B$  называется матрица  $C = (c_{ij})_{m \times n} = AB$  над  $S$  размера  $m$  на  $n$ , для которой

$$c_{ij} = \sum_{k=1}^s a_{ik} b_{kj} = a_{i1} b_{1j} + a_{i2} b_{2j} + \dots + a_{is} b_{sj}.$$

Иными словами, чтобы получить элемент, стоящий в  $i$ -ой строке и  $j$ -ом столбце произведения двух матриц, нужно элементы  $i$ -ой строки первой матрицы умножить на соответствующие элементы  $j$ -ого столбца второй матрицы и полученные произведения сложить.

ПРИМЕР. Пусть  $S = \mathbb{Z}$  — кольцо целых чисел.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 2 & 3 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 + 2 \cdot 2 + 3 \cdot 4 & 1 \cdot 1 + 2 \cdot 3 + 3 \cdot 5 \\ 4 \cdot 0 + 5 \cdot 2 + 0 \cdot 4 & 4 \cdot 1 + 5 \cdot 3 + 0 \cdot 5 \end{pmatrix} = \begin{pmatrix} 16 & 22 \\ 10 & 19 \end{pmatrix}.$$

Заметим, что если  $A$  и  $B$  — квадратные матрицы одной и той же размерности, то их можно и складывать, и умножать.

**Теорема 2.3.1.** Пусть  $\langle R, +, \cdot \rangle$  — кольцо,  $n$  — произвольное натуральное число. Тогда  $M_n(R)$  — кольцо относительно операций сложения и умножения матриц.

ДОКАЗАТЕЛЬСТВО. Мы разобьём доказательство теоремы на ряд последовательных лемм, в каждой из которых будет рассматриваться ситуация несколько более общая, чем в формулировке самой теоремы.

**Лемма 1.** Если  $\langle R, + \rangle$  — абелева группа, то  $\langle M_{m \times n}(R), + \rangle$  — абелева группа.

ДОКАЗАТЕЛЬСТВО. Пусть  $A = (a_{ij})$ ,  $B = (b_{ij})$ ,  $C = (c_{ij}) \in M_{m \times n}(R)$ . Поскольку  $R$  — кольцо, для всех  $i, j$  имеют место равенства  $a_{ij} + b_{ij} = b_{ij} + a_{ij}$  и  $(a_{ij} + b_{ij}) + c_{ij} = a_{ij} + (b_{ij} + c_{ij})$ . Следовательно,  $A + B = B + A$  и  $(A + B) + C = A + (B + C)$ . Нейтральным по сложению элементом, очевидно, является матрица, каждый элемент которой — нуль кольца  $R$ . Кроме того, матрица  $-A = (-a_{ij})$  является противоположным элементом к матрице  $A = (a_{ij})$ . Таким образом,  $M_{m \times n}(R)$  — абелева группа относительно операции сложения.  $\square$

**Лемма 2.** Пусть  $A = (a_{ij})$ ,  $B = (b_{ij}) \in M_{m \times s}(R)$  и  $C = (c_{ij}) \in M_{s \times n}(R)$ . Тогда  $(A + B)C = AC + BC$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $D = (d_{ij}) = (A + B)C$ , а  $F = (f_{ij}) = AC + BC$ . Для любых  $i, j$  имеем

$$d_{ij} = \sum_{k=1}^n (a_{ik} + b_{ik})c_{kj} = \sum_{k=1}^n (a_{ik}c_{kj} + b_{ik}c_{kj}) = \sum_{k=1}^n a_{ik}c_{kj} + \sum_{k=1}^n b_{ik}c_{kj} = f_{ij}.$$

Следовательно,  $D = F$ , и правая дистрибутивность доказана.  $\square$

Закон левой дистрибутивности  $A(B + C) = AB + AC$  для матриц соответствующих размеров, в том числе квадратных, проверяется аналогично.

Нам осталось проверить аксиому ассоциативности умножения матриц. Сформулируем сначала некоторое вспомогательное утверждение о перемене порядка суммирования, так называемую *лемму бухгалтера*.

**Предложение 2.3.1** (лемма бухгалтера). Пусть  $\langle S, + \rangle$  — коммутативная полугруппа и  $X = (x_{ij})_{m \times n}$  — матрица над  $S$ . Тогда

$$\sum_{i=1}^m \sum_{j=1}^n x_{ij} = \sum_{j=1}^n \sum_{i=1}^m x_{ij}.$$

**ДОКАЗАТЕЛЬСТВО.** Поскольку операция сложения на  $S$  коммутативна и ассоциативна, элементы матрицы можно складывать в любом порядке. Осталось заметить, что в левой и правой части доказываемого равенства стоит сумма всех элементов матрицы  $X$ .  $\square$

**Лемма 3.** Если  $A = (a_{ij}) \in M_{m \times s}(R)$ ,  $B = (b_{ij}) \in M_{s \times t}(R)$  и  $C = (c_{ij}) \in M_{t \times n}(R)$ , то  $(AB)C = A(BC)$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $D = AB$ ,  $F = BC$  и  $G = (AB)C = DC$ ,  $H = A(BC) = AF$ . Нам надо доказать, что  $G = H$ . Заметим, во-первых, что  $G$  и  $H$  — матрицы одного и того же размера  $m$  на  $n$ . Кроме того, для любых  $i \in \{1 \dots m\}$  и  $j \in \{1 \dots n\}$  выполняется

$$\begin{aligned} g_{ij} &= \sum_{k=1}^t d_{ik} c_{kj} = \sum_{k=1}^t \left( \sum_{l=1}^s a_{il} b_{lk} \right) c_{kj} = \sum_{k=1}^t \sum_{l=1}^s (a_{il} b_{lk}) c_{kj} = \\ &= \sum_{l=1}^s \sum_{k=1}^t a_{il} (b_{lk} c_{kj}) = \sum_{l=1}^s a_{il} \left( \sum_{k=1}^t (b_{lk} c_{kj}) \right) = \sum_{l=1}^s a_{il} f_{lj} = h_{ij}. \end{aligned}$$

$\square$

Поскольку утверждения лемм 1–3 верны, в частности, для квадратных матриц, алгебраическая система  $M_n(R)$  — кольцо. Теорема доказана.  $\square$

Рассмотрим теперь вопрос о том, переносятся ли остальные свойства умножения с кольца  $R$  (если  $R$  ими обладает) на кольцо  $M_n(R)$ . Во-первых, если  $n = 1$ , то отображение  $\varphi : R \rightarrow M_1(R)$ , действующее по правилу  $a\varphi = (a)_{1 \times 1}$ , очевидно, является изоморфизмом. Поэтому любое алгебраическое свойство кольца  $R$  выполняется и для  $M_1(R)$ . В частности, если  $R$  — поле, то  $M_1(R)$  тоже является полем.

Во-вторых, если  $R$  — кольцо с единицей, то  $M_n(R)$  — кольцо с единицей для любого  $n \in \mathbb{N}$ . Действительно, матрица

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



у которой  $e_{ij} = 1$  при  $i = j$  и  $e_{ij} = 0$  в остальных случаях, является, как несложно проверить непосредственно, единицей кольца  $M_n(R)$ . Мы будем называть  $E$  *единичной матрицей*.

С другой стороны, если  $n > 1$ , то свойства коммутативности умножения и существования обратного элемента не переносятся с  $R$  на  $M_n(R)$ . Пусть, например,  $F$  — произвольное поле, 0 и 1 — его нейтральные элементы по сложению и умножению соответственно. Рассмотрим матрицы из  $M_2(F)$ :

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ и } B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Имеем

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

Следовательно, кольцо  $M_2(F)$  некоммутативно. Кроме того, поскольку

$$A^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0,$$

матрица  $A$  не имеет обратной. Действительно, если бы существовала матрица  $A^{-1}$ , для которой  $A^{-1}A = E$ , то, умножая равенство  $A^2 = 0$  слева на  $A^{-1}$ , мы бы получили неверное равенство  $A = 0$ .

В дальнейшем предполагается, что множество  $F$ , над которым задана матрица, является полем относительно операций сложения и умножения. Мы будем называть поле  $F$  *полем определения* матрицы, а его элементы — *скалярами*.

Как и в случае с подстановками, мы научимся представлять каждую квадратную матрицу в виде произведения матриц специального (и достаточно простого) вида.

**Определение 2.3.4.** *Диагональная матрица*  $D(\alpha_1, \alpha_2, \dots, \alpha_n)$  — это квадратная матрица вида

$$D = (d_{ij})_{n \times n} = \begin{pmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_n \end{pmatrix},$$

где  $d_{ii} = \alpha_i$  и  $d_{ij} = 0$  при  $i \neq j$ . Диагональная матрица  $D(\alpha_1, \alpha_2, \dots, \alpha_n)$  называется *скалярной*, если  $\alpha_1 = \alpha_2 = \dots = \alpha_n = \alpha$ .

В частности, единичная и нулевая матрицы являются диагональными и даже скалярными:  $E = D(1, 1, \dots, 1)$ ,  $0 = D(0, 0, \dots, 0)$ .

Совокупность элементов  $\{a_{ii} \mid i = 1, \dots, n\}$  квадратной матрицы  $A = (a_{ij})_{n \times n}$ , стоящих на пересечении строк и столбцов с одинаковыми номерами, принято называть *главной диагональю* матрицы  $A$ . Используя этот термин, можно определить диагональную матрицу как квадратную матрицу, все элементы которой вне главной диагонали равны 0.

Посмотрим, что произойдёт с произвольной матрицей  $A = (a_{ij}) \in M_{m \times n}(F)$  при умножении её слева (а потом справа) на некоторую диагональную матрицу  $D$ .

$$\begin{aligned} D(\alpha_1, \alpha_2, \dots, \alpha_m) \cdot A &= \begin{pmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_m \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \\ &= \begin{pmatrix} \alpha_1 a_{11} & \alpha_1 a_{12} & \dots & \alpha_1 a_{1n} \\ \alpha_2 a_{21} & \alpha_2 a_{22} & \dots & \alpha_2 a_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_n a_{m1} & \alpha_n a_{m2} & \dots & \alpha_n a_{mn} \end{pmatrix} = (\alpha_i a_{ij})_{m \times n}. \end{aligned}$$

Таким образом, при умножении матрицы  $A = (a_{ij})_{m \times n}$  слева на диагональную матрицу  $D(\alpha_1, \alpha_2, \dots, \alpha_m)$  все элементы  $i$ -ой строки матрицы  $A$  умножаются на  $\alpha_i$  для каждого  $i = 1, \dots, m$ .

С другой стороны,

$$\begin{aligned} A \cdot D(\alpha_1, \alpha_2, \dots, \alpha_n) &= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_n \end{pmatrix} = \\ &= \begin{pmatrix} \alpha_1 a_{11} & \alpha_2 a_{12} & \dots & \alpha_n a_{1n} \\ \alpha_1 a_{21} & \alpha_2 a_{22} & \dots & \alpha_n a_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_1 a_{m1} & \alpha_2 a_{m2} & \dots & \alpha_n a_{mn} \end{pmatrix} = (\alpha_j a_{ij})_{m \times n}, \end{aligned}$$

т. е. при умножении матрицы  $A = (a_{ij})_{m \times n}$  справа на диагональную матрицу  $D(\alpha_1, \alpha_2, \dots, \alpha_n)$  все элементы  $j$ -ого столбца матрицы  $A$  умножаются на  $\alpha_j$  для каждого  $j = 1, \dots, n$ .

**УПРАЖНЕНИЕ 2.3.1.** Доказать, что для любых двух диагональных матриц  $D_1, D_2 \in M_n(F)$  матрица  $D_1 D_2$  является диагональной и имеет место равенство  $D_1 D_2 = D_2 D_1$ .

Если диагональная матрица является скалярной:  $D = D(\alpha, \alpha, \dots, \alpha)$ , то для любой квадратной матрицы  $A = (a_{ij})$  имеет место равенство  $DA = AD = (\alpha a_{ij})$ . Иными словами, при умножении на скалярную матрицу (с любой стороны) все элементы матрицы  $A$  умножаются на скаляр  $\alpha$ . Матрицу, которая получилась в результате, будем записывать как  $\alpha A$ . В частности, саму скалярную матрицу  $D(\alpha, \alpha, \dots, \alpha)$  можно записать как  $\alpha E$ , где  $E$  — единичная матрица соответствующего размера.

**УПРАЖНЕНИЕ 2.3.2.** Доказать, что множество всех скалярных матриц из  $M_n(F)$  является полем относительно сложения и умножения матриц, а отображение  $\varphi$  из  $F$  на множество всех скалярных матриц из  $M_n(F)$ , действующее по правилу  $\alpha\varphi = \alpha E$ , является изоморфизмом полей.

**УПРАЖНЕНИЕ 2.3.3.** Доказать, что матрица  $A \in M_n(F)$  перестановочна (коммутирует) по умножению со всеми матрицами из  $M_n(F)$  тогда и только тогда, когда  $A$  — скалярная матрица.

**Определение 2.3.5.** Клеточно диагональная матрица  $A$  — это квадратная матрица размера  $n \times n$  вида

$$\begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_s \end{pmatrix},$$

где для каждого  $i = 1, \dots, s$  матрица  $A_i$  — квадратная матрица размера  $n_i \times n_i$ ,  $\sum_{i=1}^s n_i = n$ , объединение главных диагоналей матриц  $A_i$  является главной диагональю матрицы  $A$  и все элементы матрицы  $A$ , не попавшие ни в одну матрицу  $A_i$ , равны 0.

**Предложение 2.3.2.** Пусть

$$A = \begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_s \end{pmatrix} \text{ и } B = \begin{pmatrix} B_1 & & & 0 \\ & B_2 & & \\ & & \ddots & \\ 0 & & & B_s \end{pmatrix} -$$

две клеточно диагональные матрицы, причём размеры клеток  $A_i$  и  $B_i$

совпадают для каждого  $i = 1, \dots, s$ . Тогда их произведение

$$AB = \begin{pmatrix} A_1B_1 & & & 0 \\ & A_2B_2 & & \\ & & \ddots & \\ 0 & & & A_sB_s \end{pmatrix}.$$

УПРАЖНЕНИЕ 2.3.4. Доказать предложение 2.3.2.

**Определение 2.3.6.** Пусть  $\alpha \in F$ ,  $r$  и  $s$  — два числа из множества  $\{1, 2, \dots, n\}$ , причём  $r \neq s$ . Элементарная матрица  $E_{rs}(\alpha)$  — это квадратная матрица вида

$$E_{rs}(\alpha) = (t_{ij})_{n \times n} = \begin{matrix} & & & & & & & s \\ & & & & & & & | \\ & & & & & & & \vdots \\ & & & & & & & \vdots \\ & & & & & & & \vdots \\ r - & & & & & & & \dots & 1 & \dots & \alpha & \dots & \\ & & & & & & & & & & \vdots & & \\ & & & & & & & & & & 1 & & \\ & & & & & & & & & & \vdots & \ddots & \\ & & & & & & & & & & \vdots & & \\ & & & & & & & & & & \vdots & & 1 \end{matrix},$$

где  $t_{rs} = \alpha$ ,  $t_{ii} = 1$  и  $t_{ij} = 0$  в остальных случаях. Элементарные матрицы называют также *трансекциями*.

Заметим, что единичную матрицу можно считать элементарной, поскольку  $E = E_{rs}(0)$ .

Посмотрим теперь, что происходит с произвольной матрицей  $A$  при

её умножении на элементарную матрицу. Имеем:

$$\begin{aligned}
 E_{rs}(\alpha)A &= \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & \alpha & & \\ & & & \ddots & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ & \cdots & \cdots & \\ a_{r1} & a_{r2} & \cdots & a_{rn} \\ & \cdots & \cdots & \\ a_{s1} & a_{s2} & \cdots & a_{sn} \\ & \cdots & \cdots & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} = \\
 &= \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r1} + \alpha a_{s1} & a_{r2} + \alpha a_{s2} & \cdots & a_{rn} + \alpha a_{sn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{s1} & a_{s2} & \cdots & a_{sn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.
 \end{aligned}$$

Таким образом, при умножении матрицы  $A$  слева на элементарную матрицу  $E_{rs}(\alpha)$  к  $r$ -ой строке матрицы  $A$  прибавляется  $s$ -ая строка, умноженная на  $\alpha$ .

С другой стороны,

$$\begin{aligned}
 AE_{rs}(\alpha) &= \begin{pmatrix} a_{11} & \cdots & a_{1r} & \cdots & a_{1s} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2r} & \cdots & a_{2s} & \cdots & a_{2n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{m1} & \cdots & a_{mr} & \cdots & a_{ms} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} 1 & & & & & & \\ & \ddots & & \alpha & & & \\ & & 1 & & & & \\ & & & \ddots & & & \\ & & & & \ddots & & \\ & & & & & 1 & \end{pmatrix} = \\
 &= \begin{pmatrix} a_{11} & \cdots & a_{1r} & \cdots & a_{1s} + \alpha a_{1r} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2r} & \cdots & a_{2s} + \alpha a_{2r} & \cdots & a_{2n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{m1} & \cdots & a_{mr} & \cdots & a_{ms} + \alpha a_{mr} & \cdots & a_{mn} \end{pmatrix}.
 \end{aligned}$$

Иными словами, при умножении матрицы  $A$  справа на элементарную матрицу  $E_{rs}(\alpha)$  к  $s$ -ому столбцу матрицы  $A$  прибавляется  $r$ -й столбец, умноженный на  $\alpha$ .

**Предложение 2.3.3.** Матрица  $E_{rs}(-\alpha)$  является обратным элементом по умножению к матрице  $E_{rs}(\alpha)$ , т. е.  $E_{rs}(\alpha) \cdot E_{rs}(-\alpha) = E$ .

УПРАЖНЕНИЕ 2.3.5. Доказать предложение 2.3.3.

Преобразования строк и столбцов матрицы, описанные выше, при которых к одной из строк (одному из столбцов) матрицы прибавляется другая строка (другой столбец), умноженная на некоторый скаляр из поля определения, принято называть *элементарными преобразованиями*. Таким образом, элементарным преобразованиям строк соответствует умножение слева на элементарную матрицу, а элементарным преобразованиям столбцов — умножение справа на элементарную матрицу.

**Теорема 2.3.2.** Пусть  $A \in M_n(F)$  — квадратная матрица над полем  $F$ . Тогда найдутся элементарные матрицы  $E_1, \dots, E_k, E_{k+1}, \dots, E_s \in M_n(F)$  и диагональная матрица  $D \in M_n(F)$ , такие, что  $A = E_1 \dots E_k D E_{k+1} \dots E_s$ .

**ДОКАЗАТЕЛЬСТВО.** Проведём доказательство индукцией по размерности  $n$  матрицы  $A$ .

При  $n = 1$  имеем  $A = (a_{11}) = D(a_{11})$ , и утверждение доказано.

Предположим, что утверждение теоремы верно для любой матрицы  $\tilde{A} \in M_{n-1}(F)$ , и докажем его для матрицы  $A \in M_n(F)$ . Разобьём доказательство на три этапа.

Этап 1.

$$A = \left( \begin{array}{ccc|c} a_{11} & \dots & a_{1,n-1} & 0 \\ \dots & \dots & \dots & \vdots \\ a_{n-1,1} & \dots & a_{n-1,n-1} & 0 \\ \hline 0 & \dots & 0 & a_{nn} \end{array} \right) = \left( \begin{array}{c|c} \tilde{A} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \hline 0 \dots 0 & a_{nn} \end{array} \right).$$

Заметим, что матрица

$$\tilde{A} = \left( \begin{array}{ccc} a_{11} & \dots & a_{1,n-1} \\ \dots & \dots & \dots \\ a_{n-1,1} & \dots & a_{n-1,n-1} \end{array} \right)$$

лежит в  $M_{n-1}(F)$ . Следовательно, по предположению индукции найдутся элементарные матрицы  $\tilde{E}_1, \dots, \tilde{E}_k, \tilde{E}_{k+1}, \dots, \tilde{E}_s \in M_{n-1}(F)$  и диагональная матрица  $\tilde{D} \in M_{n-1}(F)$ , такие, что  $\tilde{A} = \tilde{E}_1 \dots \tilde{E}_k \tilde{D} \tilde{E}_{k+1} \dots \tilde{E}_s$ .

Пусть для каждого  $i = 1, \dots, s$

$$E_i = \left( \begin{array}{ccc|c} & & & 0 \\ & \tilde{E}_i & & \vdots \\ & & & 0 \\ \hline 0 & \dots & 0 & 1 \end{array} \right) \text{ и } D = \left( \begin{array}{ccc|c} & & & 0 \\ & \tilde{D} & & \vdots \\ & & & 0 \\ \hline 0 & \dots & 0 & a_{nn} \end{array} \right).$$

Тогда матрицы  $E_i$  — элементарные матрицы, а  $D$  — диагональная матрица из  $M_n(F)$ . В силу предложения 2.3.2 имеем  $E_1 \dots E_k D E_{k+1} \dots E_s =$

$$= \left( \begin{array}{cccc|c} \tilde{E}_1 \dots \tilde{E}_k \tilde{D} \tilde{E}_{k+1} \dots \tilde{E}_s & & & & 0 \\ & & & & \vdots \\ & & & & 0 \\ \hline 0 & \dots & 0 & a_{nn} \end{array} \right) = \left( \begin{array}{ccc|c} \tilde{A} & & & 0 \\ & & & \vdots \\ & & & 0 \\ \hline 0 & \dots & 0 & a_{nn} \end{array} \right) = A.$$

Первый этап доказательства завершён. Отметим, что на этом этапе мы не делали никаких предположений относительно элемента  $a_{nn}$  матрицы  $A$ , в частности, могло оказаться, что  $a_{nn} = 0$ .

Этап 2. На этом этапе  $A$  — произвольная матрица из  $M_n(F)$  с единственным условием:  $a_{nn} \neq 0$ . Пусть матрица  $\tilde{A} \in M_{n-1}(F)$  такова, что

$$A = \left( \begin{array}{ccc|c} & & & a_{1n} \\ & \tilde{A} & & \vdots \\ & & & a_{n-1,n} \\ \hline a_{n1} & \dots & a_{n,n-1} & a_{nn} \end{array} \right).$$

Совершим элементарное преобразование матрицы  $A$ , прибавив к её первой строке последнюю, умноженную на  $\alpha = -a_{1n}a_{nn}^{-1}$  (обратный элемент к  $a_{nn}$  существует, поскольку по нашему предположению  $a_{nn} \neq 0$ ). Обозначим полученную в результате этого преобразования матрицу через  $A_1$ . Тогда

$$A_1 = E_{1n}(\alpha)A = \left( \begin{array}{ccc|c} & & & 0 \\ & & & a_{2n} \\ & \tilde{A}_1 & & \vdots \\ & & & a_{n-1,n} \\ \hline a_{n1} & \dots & a_{n,n-1} & a_{nn} \end{array} \right),$$

где  $\tilde{A}_1$  — некоторая матрица из  $M_{n-1}(F)$ . Отметим, что в матрице  $A_1$  на месте  $(1, n)$  стоит 0. В силу предложения 2.3.3 матрица

$A = E_{1n}(a_{1n}/a_{nn})A_1$ , где  $a_{1n}/a_{nn} = -\alpha = -(-a_{1n}a_{nn}^{-1})$ . Если мы умножим матрицу  $A_1$  слева на элементарную матрицу  $E_{2n}(-a_{2n}/a_{nn})$ , то в получившейся матрице  $A_2$  на пересечении второй строки и  $n$ -го столбца появится 0. Кроме того,  $A = E_{1n}(a_{1n}/a_{nn})E_{2n}(a_{2n}/a_{nn})A_2$ . Продолжая этот процесс, занулим все элементы последнего столбца матрицы  $A$ , кроме элемента  $a_{nn}$ . Проведя аналогичные преобразования со столбцами матрицы  $A$ , занулим все элементы последней строки матрицы  $A$  (за исключением  $a_{nn}$ ). В результате получим, что  $A = E_{1n}(a_{1n}/a_{nn}) \dots \dots E_{n-1,n}(a_{n-1,n}/a_{nn})BE_{n,n-1}(a_{n,n-1}/a_{nn}) \dots E_{n1}(a_{n1}/a_{nn})$ , где  $B$  — матрица вида, для которого мы уже провели доказательство на первом этапе. Заменяя в нашем равенстве  $B$  на соответствующее ей разложение, получим искомое разложение для матрицы  $A$ . Этап 2 завершён.

Этап 3. Пусть теперь матрица  $A \in M_n(F)$  произвольна. Если  $a_{nn} \neq 0$ , то мы действуем, как на втором этапе. Следовательно, можно полагать, что  $a_{nn} = 0$ . Если все элементы последней строки и последнего столбца матрицы  $A$  равны 0, то мы действуем, как на первом этапе доказательства. Значит, можно считать, что либо в последней строке, либо в последнем столбце найдётся элемент, отличный от нуля. Не теряя общности, можно считать, что  $a_{1n} \neq 0$ . Прибавим к последней строке матрицы  $A$  её первую строку, умножив  $A$  слева на элементарную матрицу  $E_{n1}(1)$ . В получившейся матрице  $B = E_{n1}(1)A$  элемент, стоящий на месте  $(n, n)$ , не равен 0. Поэтому для  $B$  существует разложение  $B = E_1 \dots E_l D E_{l+1} \dots E_t$  в произведение элементарных и диагональной матрицы. Тогда  $A = E_{n1}(-1)E_1 \dots E_l D E_{l+1} \dots E_t$  — искомое разложение для матрицы  $A$ , и теорема доказана.

УПРАЖНЕНИЕ 2.3.6. Пользуясь методом, изложенным при доказательстве теоремы, разложить в произведение элементарных и диагональной матриц матрицу

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & -1 \\ -2 & 1 & 0 \end{pmatrix}.$$

## § 2.4. Определитель

В этом параграфе мы продолжим заниматься квадратными матрицами, заданными над некоторым полем. Мы определим и изучим очень важную скалярную характеристику матрицы, которую называют *определителем* или *детерминантом* матрицы.



**Определение 2.4.1.** Пусть  $n$  — натуральное число,  $S_n$  — симметрическая группа подстановок множества  $\{1, \dots, n\}$ ,  $F$  — поле,  $A = (a_{ij})_{n \times n}$  — квадратная матрица из  $M_n(F)$ . *Определителем* (или *детерминантом*) матрицы  $A$  называется элемент поля  $F$ , который обозначается как  $\det(A)$  или  $|A|$  и определяется следующим образом:

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot a_{11\sigma} a_{22\sigma} \dots a_{nn\sigma}.$$

**ЗАМЕЧАНИЕ.** В формуле определителя сумма берётся по всем подстановкам  $\sigma$  из  $S_n$ , а под  $a_{ii\sigma}$  понимается элемент матрицы  $A$ , стоящий на пересечении  $i$ -ой строки и  $(i\sigma)$ -ого столбца, где  $i\sigma$  — образ  $i$  под действием подстановки  $\sigma$ .

**ПРИМЕРЫ.** 1. Пусть  $n = 1$ . Тогда  $S_1 = \{\varepsilon\}$ ,  $A = (a_{11})$  и  $\det(A) = a_{11}$ .

2. Пусть  $n = 2$ . Имеем  $S_2 = \{\varepsilon, (1, 2)\}$ , где  $\operatorname{sgn} \varepsilon = 1$  и  $\operatorname{sgn}(1, 2) = -1$ . Пусть

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

Тогда

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

Определитель  $(2 \times 2)$ -матрицы возникает естественным образом в следующих ситуациях.

Пусть дана система

$$\begin{cases} a_{11}x_1 + a_{12}x_2 = b_1, \\ a_{21}x_1 + a_{22}x_2 = b_2 \end{cases}$$

из двух линейных уравнений с двумя неизвестными. Тогда она имеет единственное решение

$$x_1 = \frac{b_1a_{22} - b_2a_{12}}{a_{11}a_{22} - a_{12}a_{21}}, \quad x_2 = \frac{b_2a_{11} - b_1a_{21}}{a_{11}a_{22} - a_{12}a_{21}}$$

в том и только том случае, когда  $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0$ . Заметим, что в случае, когда определитель равен 0, система может либо не иметь решения, либо иметь бесконечно много решений.

**Геометрический пример.** Пусть на плоскости задана прямоугольная система координат и векторы  $x$  и  $y$  имеют в этой системе координаты

$(x_1, x_2)$  и  $(y_1, y_2)$  соответственно. Тогда площадь  $S$  параллелограмма, натянутого на векторы  $x$  и  $y$ , равна модулю определителя  $\begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}$ . В частности, векторы  $x$  и  $y$  коллинеарны тогда и только тогда, когда этот определитель равен 0.

**УПРАЖНЕНИЕ 2.4.1.** Доказать утверждение о площади параллелограмма, сформулированное в предыдущем абзаце.

3. Пусть  $n = 3$ . Тогда  $S_n = \{\varepsilon, (1, 2, 3), (1, 3, 2), (1, 2), (1, 3), (2, 3)\}$ , а  $A_n = \{\varepsilon, (1, 2, 3), (1, 3, 2)\}$ . Следовательно,

$$\text{если } A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}, \text{ то } \det(A) = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} =$$

$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32}.$$

Оказывается, что выписанная выше формула вновь позволяет ответить на вопросы о существовании единственного решения системы линейных уравнений (трёх уравнений от трёх неизвестных), а также вычислить объём параллелепипеда и сформулировать критерий копланарности векторов в пространстве. Более того, и для системы из  $n$  линейных уравнений от  $n$  неизвестных критерий существования единственного решения выглядит, как в случаях  $n = 1, 2, 3$ , — решение единственно в том и только том случае, когда определитель так называемой матрицы коэффициентов системы не равен 0 (подробнее об этом в главе 4). И в пространствах размерности  $n > 3$  имеет место формула *объёма* фигуры, натянутой на  $n$  векторов, а также критерий линейной зависимости  $n$  векторов. Мы вернёмся к вопросу о приложениях определителя позднее, а пока изучим его основные свойства.

**Предложение 2.4.1.** Пусть  $A = (a_{ij})$ ,  $B = (b_{ij}) \in M_n(F)$ ,  $\alpha \in F$ ,  $r$  — некоторое натуральное число из множества  $\{1, 2, \dots, n\}$ . Пусть для каждого  $j = 1, \dots, n$  имеют место равенства  $b_{rj} = \alpha a_{rj}$  и  $b_{ij} = a_{ij}$  при  $i \neq r$ . Тогда  $\det(B) = \alpha \det(A)$ .

Иными словами, при умножении некоторой строки матрицы на скаляр  $\alpha$  определитель полученной матрицы равен произведению определителя исходной матрицы на скаляр  $\alpha$ .

**ДОКАЗАТЕЛЬСТВО.** Требуемое вытекает из равенств  $\det(B) = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma b_{11\sigma} \dots b_{rr\sigma} \dots b_{nn\sigma} = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma a_{11\sigma} \dots (\alpha a_{rr\sigma}) \dots a_{nn\sigma} = \alpha \sum_{\sigma \in S_n} \operatorname{sgn} \sigma a_{11\sigma} \dots a_{rr\sigma} \dots a_{nn\sigma} = \alpha \det(A)$ .  $\square$

**Следствие.** Если одна из строк матрицы  $A$  нулевая (все элементы этой строки равны 0), то  $\det(A) = 0$ .

УПРАЖНЕНИЕ 2.4.2. Пусть  $A \in M_n(F)$ ,  $\alpha \in F$ . Выразить  $\det(\alpha A)$  через  $\det(A)$ .

**Предложение 2.4.2.** Пусть  $A = (a_{ij})$ ,  $B = (b_{ij})$ ,  $C = (c_{ij}) \in M_n(F)$ ,  $r$  — некоторое натуральное число из множества  $\{1, 2, \dots, n\}$ . Пусть для каждого  $j = 1, \dots, n$  имеют место равенства  $c_{rj} = a_{rj} + b_{rj}$  и  $c_{ij} = a_{ij} = b_{ij}$  при  $i \neq r$ . Тогда  $\det(C) = \det(A) + \det(B)$ .

Иными словами, если две матрицы различаются лишь по  $r$ -ой строке, то матрица, полученная сложением  $r$ -х строк этих матриц с сохранением остальных строк неизменными, имеет определитель, равный сумме определителей исходных матриц.

ДОКАЗАТЕЛЬСТВО. Требуемое вытекает из равенств  $\det(C) =$

$$\begin{aligned} &= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma c_{11\sigma} \cdots c_{rr\sigma} \cdots c_{nn\sigma} = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma c_{11\sigma} \cdots (a_{rr\sigma} + b_{rr\sigma}) \cdots c_{nn\sigma} = \\ &= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma c_{11\sigma} \cdots a_{rr\sigma} \cdots c_{nn\sigma} + \sum_{\sigma \in S_n} \operatorname{sgn} \sigma c_{11\sigma} \cdots b_{rr\sigma} \cdots c_{nn\sigma} = \\ &= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma a_{11\sigma} \cdots a_{rr\sigma} \cdots a_{nn\sigma} + \sum_{\sigma \in S_n} \operatorname{sgn} \sigma b_{11\sigma} \cdots b_{rr\sigma} \cdots b_{nn\sigma} = \\ &= \det(A) + \det(B). \quad \square \end{aligned}$$

**Предложение 2.4.3.** Пусть  $A = (a_{ij}) \in M_n(F)$ ,  $r, s$  — два различных натуральных числа из множества  $\{1, 2, \dots, n\}$ . Если для каждого  $j = 1, \dots, n$  выполняются равенства  $a_{rj} = a_{sj}$ , то  $\det(A) = 0$ .

Иными словами, если в матрице две строки совпадают, то её определитель равен 0.

ДОКАЗАТЕЛЬСТВО. Обозначим через  $\tau$  транспозицию  $(r, s) \in S_n$ . В силу утверждения упражнения 2.1.1 отображение  $\varphi_\tau : \sigma \mapsto \tau\sigma$  является биекцией множества  $S_n$  на себя. Поэтому если  $\sigma$  пробегает всё множество  $S_n$ , то и  $\pi = \tau\sigma$  тоже пробегает всё  $S_n$ . С другой стороны, поскольку  $\operatorname{sgn} \pi = \operatorname{sgn}(\tau\sigma) = -\operatorname{sgn} \sigma$ , когда  $\sigma$  пробегает множество всех чётных подстановок  $A_n$ , подстановка  $\pi$  пробегает множество всех нечётных подстановок  $S_n \setminus A_n$ . Поэтому

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma a_{11\sigma} \cdots a_{rr\sigma} \cdots a_{ss\sigma} \cdots a_{nn\sigma} =$$

$$\begin{aligned}
 &= \sum_{\sigma \in A_n} a_{11\sigma} \dots a_{rr\sigma} \dots a_{ss\sigma} \dots a_{nn\sigma} - \sum_{\pi \in S_n \setminus A_n} a_{11\pi} \dots a_{rr\pi} \dots a_{ss\pi} \dots a_{nn\pi} = \\
 &= \sum_{\sigma \in A_n} a_{11\sigma} \dots a_{rr\sigma} \dots a_{ss\sigma} \dots a_{nn\sigma} - \sum_{\sigma \in A_n} a_{11\tau\sigma} \dots a_{rr\tau\sigma} \dots a_{ss\tau\sigma} \dots a_{nn\tau\sigma} = \\
 &= \sum_{\sigma \in A_n} (a_{11\sigma} \dots a_{rr\sigma} \dots a_{ss\sigma} \dots a_{nn\sigma} - a_{11\sigma} \dots a_{rs\sigma} \dots a_{sr\sigma} \dots a_{nn\sigma}) = \\
 &= \sum_{\sigma \in A_n} (a_{11\sigma} \dots a_{rr\sigma} \dots a_{ss\sigma} \dots a_{nn\sigma} - a_{11\sigma} \dots a_{rr\sigma} \dots a_{ss\sigma} \dots a_{nn\sigma}) = 0.
 \end{aligned}$$

**Следствие.** Пусть  $A = (a_{ij}), B = (b_{ij}) \in M_n(F)$ ,  $r, s$  — некоторые натуральные числа из множества  $\{1, 2, \dots, n\}$ . Пусть для каждого  $j = 1, \dots, n$  имеют место равенства  $a_{rj} = b_{sj}, a_{sj} = b_{rj}$  и  $a_{ij} = b_{ij}$  при  $r \neq i \neq s$ . Тогда  $\det(A) + \det(B) = 0$ .

Иными словами, при перестановке местами двух строк матрицы её определитель меняет знак на противоположный.

ДОКАЗАТЕЛЬСТВО. Используя предложения 2.4.2 и 2.4.3, получаем следующую цепочку равенств:

$$\begin{aligned}
 &\left| \begin{array}{c} \vdots \\ \dots a_{rj} \dots \\ \vdots \\ \dots a_{sj} \dots \\ \vdots \end{array} \right| + \left| \begin{array}{c} \vdots \\ \dots b_{rj} \dots \\ \vdots \\ \dots b_{sj} \dots \\ \vdots \end{array} \right| = \left| \begin{array}{c} \vdots \\ \dots a_{rj} \dots \\ \vdots \\ \dots a_{sj} \dots \\ \vdots \end{array} \right| + \left| \begin{array}{c} \vdots \\ \dots a_{sj} \dots \\ \vdots \\ \dots a_{rj} \dots \\ \vdots \end{array} \right| = \\
 &= \left| \begin{array}{c} \vdots \\ \dots a_{rj} \dots \\ \vdots \\ \dots a_{sj} \dots \\ \vdots \end{array} \right| + \left| \begin{array}{c} \vdots \\ \dots a_{rj} \dots \\ \vdots \\ \dots a_{rj} \dots \\ \vdots \end{array} \right| + \left| \begin{array}{c} \vdots \\ \dots a_{sj} \dots \\ \vdots \\ \dots a_{rj} \dots \\ \vdots \end{array} \right| + \left| \begin{array}{c} \vdots \\ \dots a_{sj} \dots \\ \vdots \\ \dots a_{sj} \dots \\ \vdots \end{array} \right| = \\
 &= \left| \begin{array}{c} \vdots \\ \dots a_{rj} \dots \\ \vdots \\ \dots a_{rj} + a_{sj} \dots \\ \vdots \end{array} \right| + \left| \begin{array}{c} \vdots \\ \dots a_{sj} \dots \\ \vdots \\ \dots a_{rj} + a_{sj} \dots \\ \vdots \end{array} \right| = \left| \begin{array}{c} \vdots \\ \dots a_{rj} + a_{sj} \dots \\ \vdots \\ \dots a_{rj} + a_{sj} \dots \\ \vdots \end{array} \right| = 0.
 \end{aligned}$$

**Предложение 2.4.4.** Пусть  $A = (a_{ij})$ ,  $B = (b_{ij}) \in M_n(F)$ ,  $\alpha \in F$ ,  $r, s$  — некоторые натуральные числа из множества  $\{1, 2, \dots, n\}$ . Пусть для каждого  $j = 1, \dots, n$  имеет место  $b_{rj} = a_{rj} + \alpha a_{sj}$ , и  $a_{ij} = b_{ij}$  при  $i \neq r$ . Тогда  $\det(B) = \det(A)$ .

Иными словами, при элементарных преобразованиях строк матрицы её определитель не меняется.

**ДОКАЗАТЕЛЬСТВО.** Обозначим через  $C = (c_{ij})$  и  $D = (d_{ij})$  матрицы из  $M_n(F)$ , такие, что для каждого  $j = 1, \dots, n$  имеют место равенства  $c_{rj} = \alpha a_{sj}$ ,  $d_{rj} = a_{sj}$  и  $c_{ij} = d_{ij} = a_{ij}$  при  $i \neq r$ . Тогда по предложению 2.4.3 определитель матрицы  $D$  равен нулю (её  $r$ -ая и  $s$ -ая строки совпадают). В силу предложения 2.4.1 имеет место равенство  $\det(C) = \alpha \det(D) = 0$ . Наконец, из предложения 2.4.2 следует, что  $\det(B) = \det(A) + \det(C) = \det(A)$ .  $\square$

**Определение 2.4.2.** Верхнетреугольная матрица  $A = (a_{ij})$  — это квадратная ( $n \times n$ )-матрица, в которой для любых  $i, j \in \{1, \dots, n\}$  с условием  $i > j$  имеет место равенство  $a_{ij} = 0$ . Иными словами, все элементы матрицы, расположенные под главной диагональю, равны 0. Квадратная матрица называется нижнетреугольной, если все её элементы, расположенные над главной диагональю, равны 0. Квадратная матрица называется треугольной, если она либо верхнетреугольная, либо нижнетреугольная.

**Предложение 2.4.5.** Пусть  $A = (a_{ij}) \in M_n(F)$  — треугольная матрица. Тогда её определитель равен произведению элементов, стоящих на главной диагонали, т. е.  $\det(A) = a_{11}a_{22} \dots a_{nn}$ .

**ДОКАЗАТЕЛЬСТВО.** Мы проведём доказательство, предполагая, что  $A$  — верхнетреугольная матрица. Случай нижнетреугольных матриц разбирается аналогично.

Предположим, что подстановка  $\sigma \in S_n$  обладает следующим свойством: для каждого  $i = 1, \dots, n$  выполняется  $i \leq i\sigma$ . Тогда  $n\sigma = n$ , поскольку иначе требуемое неравенство не имеет места. Далее,  $(n-1)\sigma = n-1$ , так как  $n$  уже является образом элемента  $n$ . Продолжая рассуждение, получаем, что  $(n-2)\sigma = n-2, \dots, 2\sigma = 2, 1\sigma = 1$ . Следовательно,  $\sigma$  — тождественная подстановка. Таким образом, для каждой нетождественной подстановки  $\sigma \in S_n$  найдётся такой  $i \in \{1, \dots, n\}$ , что  $i > i\sigma$ .

Пусть  $A$  — верхнетреугольная матрица. Тогда для каждой нетождественной подстановки  $\sigma$  произведение  $a_{11\sigma}a_{22\sigma} \dots a_{nn\sigma}$  равно 0. Поэтому  $\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma a_{11\sigma}a_{22\sigma} \dots a_{nn\sigma} = a_{11}a_{12} \dots a_{1n}$ .  $\square$

**Следствие.** Пусть  $D = D(\alpha_1, \dots, \alpha_n)$  — диагональная матрица,  $T = E_{rs}(\alpha)$  — элементарная матрица. Тогда  $\det(D) = \alpha_1 \dots \alpha_n$ ,  $\det(T) = 1$ . В частности, определитель единичной матрицы равен единице.

**Теорема 2.4.1.** Пусть  $A, B \in M_n(F)$ . Тогда  $|AB| = |A| \cdot |B|$ .

**ДОКАЗАТЕЛЬСТВО.** Предположим сначала, что  $A = D(\alpha_1, \dots, \alpha_n)$  — диагональная матрица. При умножении матрицы  $B$  слева на  $A$  для каждого  $i \in \{1, 2, \dots, n\}$   $i$ -ая строка матрицы  $B$  умножается на  $\alpha_i$ . Следовательно, по предложению 2.4.1 имеет место равенство  $|AB| = \alpha_1 \dots \alpha_n |B| = |A||B|$ .

Если  $A = E_{rs}(\alpha)$  — элементарная матрица, то её определитель равен 1. С другой стороны, при умножении на элементарную матрицу слева происходит элементарное преобразование строк. По предложению 2.4.4 в этом случае тоже выполняется  $|AB| = |B| = 1|B| = |A||B|$ .

Пусть теперь  $A$  — произвольная квадратная матрица. По теореме 2.3.2 найдутся элементарные матрицы  $E_1, \dots, E_k, E_{k+1}, \dots, E_s$  и диагональная матрица  $D$  из  $M_n(F)$ , такие, что  $A = E_1 \dots E_k D E_{k+1} \dots E_s$ . Тогда  $|A| = |E_1(E_2 \dots E_k D E_{k+1} \dots E_s)| = |E_2 \dots E_k D E_{k+1} \dots E_s| = \dots = |D(E_{k+1} \dots E_s)| = |D||E_{k+1} \dots E_s| = |D|$ . Наконец,  $|AB| = |E_1 \dots E_k D E_{k+1} \dots E_s B| = |D(E_{k+1} \dots E_s B)| = |D||E_{k+1} \dots E_s B| = |D||B| = |A||B|$ .  $\square$

**УПРАЖНЕНИЕ 2.4.3.** Рассмотрим клеточно диагональную матрицу

$$A = \begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_s \end{pmatrix}.$$

Доказать, что  $|A| = |A_1||A_2| \dots |A_s|$ .

**Определение 2.4.3.** Пусть  $A = (a_{ij})$  —  $(m \times n)$ -матрица над множеством  $S$ . Матрица  $B = (b_{ij})$  размера  $n$  на  $m$  над  $S$  называется транспонированной к матрице  $A$ , если  $b_{ij} = a_{ji}$  для каждого  $i = 1, \dots, n$  и каждого  $j = 1, \dots, m$ . Мы будем обозначать матрицу, транспонированную к матрице  $A$ , через  $A'$  или  $A^\top$ .

Сформулируем в виде упражнения свойства транспонирования матриц.

УПРАЖНЕНИЕ 2.4.4. Для прямоугольных матриц  $A$  и  $B$  согласованных размеров доказать следующие утверждения:

- 1)  $A'' = (A')' = A$ ;
- 2)  $(A + B)' = A' + B'$ ;
- 3)  $(AB)' = B'A'$ .

ЗАМЕЧАНИЕ. Несложно заметить также, что если  $D$  — диагональная матрица, а  $E_{rs}(\alpha)$  — элементарная матрица, то  $D' = D$  и  $E_{rs}(\alpha)' = E_{sr}(\alpha)$ .

**Предложение 2.4.6.** Пусть  $A \in M_n(F)$ . Тогда  $\det(A') = \det(A)$ .

ДОКАЗАТЕЛЬСТВО. Заметим, во-первых, что из утверждения 3 упражнения 2.4.4 несложно вывести по индукции следующее правило транспонирования произведения нескольких матриц:  $(A_1 A_2 \dots A_s)' = A'_s \dots A'_2 A'_1$ . Как мы знаем,  $A = E_1 \dots E_k D E_{k+1} \dots E_s$ , где  $E_1, \dots, E_k, E_{k+1}, \dots, E_s$  — элементарные матрицы, а  $D$  — диагональная матрица, причём  $|A| = |D|$ . Поэтому  $A' = E'_s \dots E'_{k+1} D' E'_k \dots E'_1$  и  $|A'| = |D'| = |D| = |A|$ .  $\square$

**Следствие.** Если в каждом доказанном нами утверждении о свойствах определителя заменить слово «строка» на слово «столбец», то утверждение останется верным.

УПРАЖНЕНИЕ 2.4.5. Сформулируйте и обоснуйте указанные утверждения для столбцов матрицы.

Следующая наша задача — доказать утверждение, которое позволит вычислять определитель матрицы размера  $n$  через определители матриц меньшего размера.

**Определение 2.4.4.** Пусть  $A = (a_{ij}) \in M_n(F)$ . Минором, дополнительным к элементу  $a_{rs}$  матрицы  $A$ , называется матрица  $M_{rs}(A)$  из  $M_{n-1}(F)$ , полученная из матрицы  $A$  вычеркиванием  $r$ -ой строки и  $s$ -го столбца.

ПРИМЕР.

$$\text{Для } A = \begin{pmatrix} 1 & 2 & 5 \\ 3 & 4 & 6 \\ 7 & 8 & 9 \end{pmatrix} \text{ минор } M_{23}(A) = \begin{pmatrix} 1 & 2 \\ 7 & 8 \end{pmatrix}.$$

**Определение 2.4.5.** Пусть  $A = (a_{ij}) \in M_n(F)$ . Алгебраическое дополнение в  $A$  к элементу  $a_{rs}$  — это скаляр  $A_{rs} = (-1)^{r+s} |M_{rs}(A)|$ .

Иными словами, алгебраическое дополнение к элементу матрицы с номером  $(r, s)$  — это определитель минора, дополнительного к данному

элементу, взятый со знаком плюс, если сумма  $r + s$  чётна, и знаком минус, если эта сумма нечётна.

**ПРИМЕР.** Для элемента  $a_{23}$  матрицы  $A$  из предыдущего примера выполняется

$$A_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 2 \\ 7 & 8 \end{vmatrix} = (-1) \cdot (1 \cdot 8 - 2 \cdot 7) = 6.$$

**Теорема 2.4.2** (о разложении определителя по строке). Пусть  $A = (a_{ij}) \in M_n(F)$ . Тогда для любых  $i, k \in \{1, \dots, n\}$  имеет место равенство

$$\sum_{j=1}^n a_{ij} A_{kj} = \begin{cases} |A|, & \text{если } k = i, \\ 0, & \text{если } k \neq i. \end{cases}$$

**ЗАМЕЧАНИЕ.** Формула разложения определителя по  $i$ -ой строке:

$$|A| = \sum_{j=1}^n a_{ij} A_{ij},$$

выполняющаяся для каждого  $i = 1, \dots, n$ , является частным случаем теоремы при  $k = i$ .

**ДОКАЗАТЕЛЬСТВО.** Сначала мы докажем теорему в случае когда  $i = k$ , т.е. докажем, что  $|A| = \sum_{j=1}^n a_{ij} A_{ij}$  для каждого  $i = 1, \dots, n$ . Разобьём это доказательство на четыре этапа.

**Этап 1.** Пусть  $i = n$ ,  $a_{n1} = a_{n2} = \dots = a_{n,n-1} = 0$ . Матрица  $A$  имеет вид

$$\left( \begin{array}{ccc|c} & & & * \\ & & & \vdots \\ & & & * \\ \hline 0 & \dots & 0 & a_{nn} \end{array} \right),$$

где  $M_{nn} = M_{nn}(A)$  — минор, дополнительный к элементу  $a_{nn}$  в матрице  $A$ , а  $*$  обозначает произвольный скаляр.

Для подстановки  $\sigma = \begin{pmatrix} 1 & \dots & n-1 & n \\ i_1 & \dots & i_{n-1} & n \end{pmatrix} \in S_n$  положим  $\sigma' = \begin{pmatrix} 1 & \dots & n-1 \\ i_1 & \dots & i_{n-1} \end{pmatrix} \in S_{n-1}$ . Имеем  $|A| =$

$$= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma a_{11\sigma} \dots a_{n-1,(n-1)\sigma} a_{nn\sigma} = \sum_{\substack{\sigma \in S_n \\ n\sigma = n}} \operatorname{sgn} \sigma a_{11\sigma} \dots a_{n-1,(n-1)\sigma} a_{nn} =$$



$$\begin{aligned}
&= a_{nn} \cdot \sum_{\sigma' \in S_{n-1}} \operatorname{sgn} \sigma' a_{11\sigma'} \dots a_{n-1,(n-1)\sigma'} = a_{nn} |M_{nn}| = a_{nn} (-1)^{n+n} |M_{nn}| = \\
&= a_{nn} A_{nn} = 0 \cdot A_{n1} + \dots + 0 \cdot A_{n,n-1} + a_{nn} A_{nn} = \sum_{j=1}^n a_{nj} A_{nj}.
\end{aligned}$$

Этап 2. Пусть  $i = n$ ,  $a_{nj} = 0$ , кроме, быть может, одного элемента  $a_{ns}$ .

Если  $s = n$ , то мы получаем матрицу из первого этапа доказательства. Пусть  $s < n$ . Пусть матрица  $A_1$  получена из матрицы  $A$  перестановкой  $s$ -го и  $(s+1)$ -го столбца. Тогда в силу следствия из предложения 2.4.3 и следствия из предложения 2.4.6 имеет место равенство  $|A| = -|A_1|$ .

Если  $s = n-1$ , то полученная матрица имеет вид, как у матрицы на первом этапе доказательства, а минор  $M_{nn}(A_1) = M_{n,n-1}(A)$ . Следовательно,  $|A| = -|A_1| = -a_{n,n-1} |M_{n,n-1}| = a_{n,n-1} A_{n,n-1}$ , что и требовалось.

Если  $s < n-1$ , то мы продолжаем указанный процесс, меняя  $(s+1)$ -ый столбец матрицы  $A_1$  (т.е.  $s$ -ый столбец матрицы  $A$ ) с  $(s+2)$ -ым столбцом, и так далее, пока не поставим  $s$ -ый столбец матрицы  $A$  на место  $n$ -го столбца. Всего нам потребуется  $n-s$  перестановок. Получившаяся в результате матрица  $B$  имеет вид

$$\left( \begin{array}{ccc|c} & & & * \\ & & & \vdots \\ & M_{ns}(A) & & * \\ \hline 0 & \dots & 0 & a_{ns} \end{array} \right).$$

Поэтому  $|A| = (-1)^{n-s} |B| = (-1)^{n-s+2s} a_{ns} |M_{ns}(A)| = a_{ns} A_{ns} = \sum_{j=1}^n a_{nj} A_{nj}$ , что и требовалось. Отметим, что наше рассуждение существенно использует последовательную перестановку соседних столбцов матрицы  $A$ . Если мы, к примеру, сразу поменяем между собой  $s$ -ый и  $n$ -ый столбцы, то в левом верхнем углу получившейся матрицы не будет минора  $M_{ns}(A)$  и предложенное рассуждение будет неверным.

Этап 3. Пусть  $i = n$ . Обозначим через  $A_j$  матрицу того же размера  $n$ , что и  $A$ , у которой первые  $n-1$  строк совпадают с соответствующими строками матрицы  $A$ , в последней строке на месте  $(n, j)$  стоит элемент  $a_{nj}$  матрицы  $A$ , а остальные элементы последней строки равны нулю. По предложению 2.4.2 имеем  $|A| = |A_1| + |A_2| + \dots + |A_n| = \sum_{j=1}^n a_{nj} A_{nj}$ .

Этап 4. Пусть номер строки произволен. Если  $i = n$ , то утверждение доказано. Пусть  $i < n$ . Поменяем местами  $i$ -ую и  $(i+1)$ -ую строки

матрицы  $A$  так же, как на втором этапе мы меняли местами соседние столбцы. Затем  $(i+1)$ -ую и  $(i+2)$ -ую строки получившейся матрицы, и так далее, продолжая процесс до тех пор, пока  $i$ -ая строка матрицы  $A$  не переместится на место  $n$ -ой строки. Обозначим полученную в результате всех этих перестановок матрицу через  $B$ . В силу следствия из предложения 2.4.3 имеем  $|A| = (-1)^{n-i}|B|$ .

Если для краткости обозначить  $k$ -ые строки матриц  $A$  и  $B$  через  $a_k$  и  $b_k$  соответственно, то для них будут иметь место равенства:  $b_k = a_k$  при  $1 \leq k < i$ ,  $b_k = a_{k+1}$  при  $i \leq k < n$  и  $b_n = a_i$ . В частности,  $M_{nj}(B) = M_{ij}(A)$  для каждого  $j = 1, \dots, n$ . Поэтому  $|A| =$

$$\begin{aligned} &= (-1)^{n-i}|B| = (-1)^{n-i} \sum_{j=1}^n b_{nj} B_{nj} = (-1)^{n-i} \sum_{j=1}^n b_{nj} (-1)^{n+j} |M_{nj}(B)| = \\ &= \sum_{j=1}^n a_{ij} (-1)^{n+j+n-i} |M_{ij}(A)| = \sum_{j=1}^n a_{ij} (-1)^{i+j+2(n-i)} |M_{ij}(A)| = \sum_{j=1}^n a_{ij} A_{ij}. \end{aligned}$$

Таким образом, формула разложения определителя по строке доказана.

Докажем оставшуюся часть теоремы.  $A$  именно, покажем, что при  $i \neq k$  имеет место равенство  $\sum_{j=1}^n a_{ij} A_{kj} = 0$ . Определим матрицу  $B$  той же размерности  $n$ , что и матрица  $A$ , следующим образом: все строки матрицы  $B$ , кроме  $k$ -ой строки, совпадают с соответствующими строками матрицы  $A$ , а на месте  $k$ -ой строки стоит  $i$ -я строка матрицы  $A$ . Поскольку  $i$ -ая и  $k$ -ая строки матрицы  $B$  равны между собой (обе равны  $i$ -ой строке матрицы  $A$ ), по предложению 2.4.3 определитель матрицы  $B$  равен нулю. С другой стороны, раскладывая определитель матрицы  $B$  по  $k$ -ой строке, получаем

$$|B| = \sum_{j=1}^n b_{kj} B_{kj} = \sum_{j=1}^n a_{ij} A_{kj},$$

так как миноры  $M_{kj}$  матриц  $A$  и  $B$  совпадают (единственная строка, различная в матрицах  $A$  и  $B$ , — строка под номером  $k$  — вычеркивается при вычислении этих миноров).  $\square$

**Следствие** (о разложении определителя по столбцу). Пусть  $A = (a_{ij}) \in M_n(F)$ . Тогда для любых  $j, k \in \{1, \dots, n\}$  имеет место равенство

$$\sum_{i=1}^n a_{ij} A_{ik} = \begin{cases} |A|, & \text{если } j = k, \\ 0, & \text{если } j \neq k. \end{cases}$$

**ДОКАЗАТЕЛЬСТВО.** Доказательство дословно повторяет доказательство теоремы с заменой слова «строка» на слово «столбец» и обратно. Кроме того, следствие можно доказать, применив теорему о разложении по строке к транспонированной матрице  $A'$ .  $\square$

**УПРАЖНЕНИЕ 2.4.6.** Вычислить определитель матрицы  $A$  из примера после определения 2.4.4 двумя способами: разложив его сначала по второй строке, а затем по третьему столбцу.

Имеется одна полезная переформулировка только что доказанной нами теоремы, так называемая *матричная форма* теоремы о разложении по строке, для которой нам понадобится следующее определение.

**Определение 2.4.6.** Пусть  $A = (a_{ij}) \in M_n(F)$ . Матрица  $\hat{A} = (\hat{a}_{ij}) \in M_n(F)$ , для которой  $\hat{a}_{ij} = A_{ji}$  при всех  $i, j \in \{1, \dots, n\}$ , называется *присоединённой* к матрице  $A$ .

Иными словами, *присоединённая матрица* — это транспонированная матрица алгебраических дополнений.

Теперь теорема 2.4.2 может быть сформулирована следующим образом.

**Теорема 2.4.2'** (матричная форма теоремы о разложении по строке). Пусть  $A$  — квадратная матрица из  $M_n(F)$ , а  $\hat{A}$  — присоединённая к ней матрица. Тогда

$$A\hat{A} = \hat{A}A = |A|E = \begin{pmatrix} |A| & 0 & \dots & 0 \\ 0 & |A| & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & |A| \end{pmatrix}.$$

**ДОКАЗАТЕЛЬСТВО.** Обозначим через  $B$  матрицу  $A\hat{A}$ . Тогда

$$b_{ij} = \sum_{k=1}^n a_{ik}\hat{a}_{kj} = \sum_{k=1}^n a_{ik}A_{jk} = \begin{cases} |A|, & \text{если } i = j, \\ 0, & \text{если } i \neq j. \end{cases}$$

Для матрицы  $\hat{A}A$  результат получается аналогично.  $\square$

Используя матричную форму теоремы, несложно доказать критерий обратимости матрицы.

**Определение 2.4.7.** Квадратная матрица  $A$  называется *вырожденной*, если  $\det(A) = 0$ , и *невырожденной* в противном случае.

**Определение 2.4.8.** Пусть  $A$  — квадратная матрица из  $M_n(F)$ . Матрица  $A^{-1}$  называется *обратной* к матрице  $A$ , если  $AA^{-1} = A^{-1}A = E$ .

**Теорема 2.4.3** (об обратной матрице). Пусть  $A \in M_n(F)$  и  $\widehat{A}$  — присоединённая к ней матрица. Матрица  $A$  обратима (имеет обратную матрицу) тогда и только тогда, когда она невырождена. Обратная матрица вычисляется по следующей формуле:

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

**ДОКАЗАТЕЛЬСТВО.** Пусть сначала  $|A| = 0$ . Предположим, что для матрицы  $A$  существует обратная матрица  $A^{-1}$ . Тогда по теореме об определителе произведения матриц  $1 = |E| = |AA^{-1}| = |A||A^{-1}| = 0$ ; противоречие.

Если же матрица  $A$  невырождена, то матрица  $\frac{1}{|A|} \widehat{A}$  всегда существует. Напомним, что для скаляра  $\alpha$  и матрицы  $A = (a_{ij})$  матрица  $\alpha A$  — это матрица  $(\alpha a_{ij})$ . Кроме того,  $\alpha E$  — это скалярная матрица с элементом  $\alpha$  по главной диагонали. В частности, в силу упражнения 2.3.3 выполняется  $\alpha A = \alpha EA = A(\alpha E)$ .

По теореме 2.4.2' имеют место равенства

$$A \left( \frac{1}{|A|} \widehat{A} \right) = A \left( \frac{1}{|A|} E \widehat{A} \right) = \frac{1}{|A|} E (A \widehat{A}) = \frac{1}{|A|} E |A| E = E$$

$$\text{и } \left( \frac{1}{|A|} \widehat{A} \right) A = \frac{1}{|A|} |A| E = E.$$

**УПРАЖНЕНИЕ 2.4.7.** Для матрицы  $A$  из примера после определения 2.4.4 вычислить присоединённую матрицу. Проверить, что полученная из неё делением на определитель матрица удовлетворяет определению обратной матрицы.

**УПРАЖНЕНИЕ 2.4.8.** Пусть  $GL_n(F) = \{A \in M_n(F) \mid \det(A) \neq 0\}$ . Доказать, что  $GL_n(F)$  — группа относительно операции умножения матриц.

**Определение 2.4.9.** Группа  $GL_n(F)$ , определённая в упражнении 2.4.8, называется *общей линейной группой матриц над полем  $F$* , а любая её подгруппа — *линейной группой матриц над полем  $F$* .

Заметим, что теорема об обратной матрице влечёт, что для данных матриц  $A$  и  $B$  линейные матричные уравнения  $A X = B$  и  $Y A = B$  имеют единственное решение в том и только том случае, когда матрица  $A$  невырождена (предполагается, что матрицы  $A, B, X, Y$  — квадратные матрицы одной размерности). Решениями уравнений будут матрицы  $X = A^{-1}B$  и  $Y = B A^{-1}$  соответственно.

Рассмотрим теперь ещё один способ вычисления обратной матрицы, а также решения линейных матричных уравнений, основанный на разложении квадратной матрицы в произведение элементарной и диагональной матриц. Мы изложим его в виде серии упражнений.

**УПРАЖНЕНИЕ 2.4.9.** Доказать, что если матрица  $A$  невырождена, то её можно разложить в произведение диагональной и элементарных матриц так, чтобы диагональная матрица оказалась в произведении последней справа (слева). Иными словами, требуется доказать, что невырожденную матрицу можно привести к диагональному виду, пользуясь только элементарными преобразованиями строк (или только столбцов).

**УПРАЖНЕНИЕ 2.4.10.** Пусть  $A, B \in M_n(F)$  и  $|A| \neq 0$ . Преобразование строки (столбца) прямоугольной матрицы, при котором все элементы строки (столбца) умножаются на ненулевой скаляр  $\alpha$ , будем так же, как и прибавление к строке (столбцу) другой строки (другого столбца), умноженной на скаляр, называть элементарным преобразованием строки (столбца). Доказать, что прямоугольную  $(n \times 2n)$ -матрицу  $(A \mid B)$ , составленную из матриц  $A$  и  $B$ , можно элементарными преобразованиями строк привести к виду  $(E \mid X)$ , где  $E$  — единичная матрица, а  $X$  — матрица  $A^{-1}B$ , т. е. решение матричного уравнения  $A X = B$ . В частности, если положить  $B = E$ , то  $X = A^{-1}$ . Доказать, что элементарными преобразованиями столбцов  $(2n \times n)$ -матрицу  $\begin{pmatrix} A \\ B \end{pmatrix}$  можно привести к виду  $\begin{pmatrix} E \\ Y \end{pmatrix}$ , где  $Y$  — решение уравнения  $Y A = B$ .

**ЗАМЕЧАНИЕ.** Существует ещё два способа ввести понятие определителя: аксиоматический и индуктивный. В первом случае мы определяем  $\det$  как функцию из  $M_n(F)$  в  $F$ , удовлетворяющую свойствам, указанным в предложениях 2.4.1–2.4.3, и принимающую значение 1 на единичной матрице. Во втором случае мы полагаем, что для матрицы  $A = (a) \in M_1(F)$  её определитель равен  $a$ , а для матрицы  $A \in M_n(F)$  определяем  $\det(A)$  по индукции через определители матриц размерности  $n - 1$ , используя формулу разложения по строке (см. теорему 2.4.2).

**УПРАЖНЕНИЕ 2.4.11 \*** Показать, что три предложенных определения определителя (включая данное нами в этом курсе) эквивалентны.

## § 2.5. Поле комплексных чисел

**Определение 2.5.1.** *Поле комплексных чисел* называется поле  $\mathbb{C}$ , удовлетворяющее следующим условиям.

1. Поле  $\mathbb{C}$  содержит в качестве подполя поле  $R$ , изоморфное полю  $\mathbb{R}$  действительных чисел.

2. Поле  $\mathbb{C}$  содержит элемент  $i$ , такой, что  $i^2 = -1$ , где  $-1$  — это элемент, противоположный к единице поля  $\mathbb{C}$ , а значит, и его подполя  $R$ .

3. Каждый элемент  $z$  поля  $\mathbb{C}$  однозначно представляется в виде  $a+bi$ , где  $a, b \in R$ , подполе  $R$  определено в п. 1, а  $i$  — в п. 2.

**Теорема 2.5.1.** *Поле  $\mathbb{C}$  комплексных чисел существует и единственно с точностью до изоморфизма.*

**ДОКАЗАТЕЛЬСТВО.** Обозначим через  $\mathbb{C}$  множество квадратных матриц вида

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \text{ где } a, b \in \mathbb{R}.$$

В силу равенств

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

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} \quad (2)$$

множество  $\mathbb{C}$  замкнуто относительно операций сложения и умножения матриц.

Докажем, что  $\mathbb{C}$  является полем относительно этих операций. Поскольку нулевая и единичная матрицы из  $M_2(\mathbb{R})$  лежат в  $\mathbb{C}$ , а само  $M_2(\mathbb{R})$  является кольцом с единицей, нам остаётся проверить лишь коммутативность умножения матриц из  $\mathbb{C}$ , а также существование противоположного и обратного элемента для произвольного

$$z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{C}.$$

Выполнив умножение матриц из равенства (2) в обратном порядке, получим

$$\begin{pmatrix} c & -d \\ d & c \end{pmatrix} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix}.$$

Следовательно, умножение элементов из  $\mathbb{C}$  коммутативно. Поскольку матрица

$$\begin{pmatrix} -a & -(-b) \\ -b & -a \end{pmatrix}$$

лежит в  $\mathbb{C}$ , имеет место и аксиома существования противоположного элемента.

Нам осталось показать, что любой ненулевой элемент  $z \in \mathbb{C}$  имеет обратный в  $\mathbb{C}$ . Воспользуемся теоремой 2.4.3 об обратной матрице. Во-первых,

$$\begin{vmatrix} a & -b \\ b & a \end{vmatrix} = a^2 + b^2 \neq 0,$$

кроме случая  $a = b = 0$ , в котором элемент  $z$  — это нулевая матрица. Во-вторых,

$$z^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbb{C}.$$

Таким образом,  $\mathbb{C}$  — поле. Покажем, что  $\mathbb{C}$  удовлетворяет условиям 1–3 из определения 2.5.1 и, следовательно, является полем комплексных чисел.

Пусть

$$R = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R} \right\}.$$

Очевидно, что  $R$  — подмножество множества  $\mathbb{C}$ . С другой стороны, в силу утверждения упражнения 2.3.2 множество  $R$  как множество всех скалярных матриц из  $M_2(\mathbb{R})$  есть поле, изоморфное полю  $\mathbb{R}$  действительных чисел. В качестве изоморфизма здесь выступает отображение  $\varphi$ , действующее по правилу  $(aE)\varphi = a \in \mathbb{R}$ .

Обозначим через  $i$  элемент поля  $\mathbb{C}$ , равный

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

Несложно проверить, что

$$i^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Элемент, полученный в результате этого умножения, является противоположным к единичной матрице и переходит в  $-1$  при отображении  $\varphi$  из  $R$  в  $\mathbb{R}$ .

Для произвольного элемента  $z \in \mathbb{C}$ , записываемого в виде матрицы

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

положим

$$a = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \text{ и } b = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}.$$

Тогда

$$z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = a + bi.$$

Предположим, что элемент  $z$  имеет два представления:  $z = a + bi = c + di$ ,  $a, b, c, d \in R$ . Тогда  $a - c = (d - b)i$ . Возводя последнее равенство в квадрат, получаем  $(a - c)^2 = -(d - b)^2 \in R$ . Поскольку поля  $\mathbb{R}$  и  $R$  изоморфны,  $a, b, c, d$  можно считать действительными числами, поэтому имеет место  $a - c = d - b = 0$ . Отсюда  $a = c$  и  $b = d$ , а значит, представление  $z = a + bi$  единственно. Таким образом,  $\mathbb{C}$  — поле комплексных чисел.

Пусть  $C$  — ещё одно поле, удовлетворяющее определению комплексных чисел. Обозначим через  $i'$  элемент этого поля со свойством  $(i')^2 = -1$ . Тогда в силу свойства 3 любой элемент поля  $C$  однозначно представим в виде  $a + bi'$ , где элементы  $a$  и  $b$  в силу свойства 1 можно считать действительными числами. Поэтому отображение  $\psi : \mathbb{C} \rightarrow C$ , действующее по правилу  $(a + bi)\psi = a + bi'$ , является биекцией. Кроме того, равенства  $(a + bi') + (c + di') = (a + c) + (b + d)i'$  и  $(a + bi')(c + di') = (ac - bd) + (ad + bc)i'$  вместе с равенствами (1) и (2) показывают, что  $\psi$  — изоморфизм.  $\square$

**ЗАМЕЧАНИЕ.** В дальнейшем мы будем называть элементы поля  $\mathbb{C}$  *комплексными числами* и, как правило, обозначать их через  $a + bi$ . Кроме того, если договориться, что элементы вида  $a + 0i = a$  — это действительные числа, то можно считать, что  $\mathbb{R}$  является подполем поля  $\mathbb{C}$ . Поскольку поле  $\mathbb{Q}$  рациональных чисел является подполем поля  $\mathbb{R}$ , его также можно рассматривать как подполе поля  $\mathbb{C}$ . Мы будем называть *числовым полем* любое подполе поля комплексных чисел.

**Определение 2.5.2.** Действительные числа  $a$  и  $b$  называются *действительной* и *мнимой частью* комплексного числа  $z = a + bi$  и обозначаются как  $a = \operatorname{Re} z$  и  $b = \operatorname{Im} z$  соответственно. Число  $i$  со свойством  $i^2 = -1$  из определения поля комплексных чисел называется *мнимой единицей*.



В поле  $\mathbb{C}$  есть два элемента, которые в квадрате дают  $-1$ . Если один из них обозначен через  $i$ , то второй равен  $-i$ . Как легко проверить, решая уравнение  $(a + bi)^2 = -1 + 0i$ , других элементов с таким свойством в  $\mathbb{C}$  нет. Если в доказательстве единственности поля комплексных чисел положить  $i' = -i$ , то мы получим, что отображение  $z = a + bi \rightarrow \bar{z} = a - bi$  есть изоморфизм поля комплексных чисел на себя. Этот изоморфизм называется *комплексным сопряжением*, а числа  $z$  и  $\bar{z}$  — *комплексно сопряжёнными*. Поскольку комплексное сопряжение — изоморфизм, для любых комплексных чисел  $z$  и  $u$  выполняются следующие равенства:  $\overline{z + u} = \bar{z} + \bar{u}$  и  $\overline{zu} = \bar{z} \cdot \bar{u}$ . Кроме того, очевидно, что  $\overline{\bar{z}} = z$ .

**УПРАЖНЕНИЕ 2.5.1 \***. Доказать, что любой изоморфизм поля действительных чисел на себя является тождественным, а изоморфизмов поля комплексных чисел на себя ровно два: тождественный и комплексное сопряжение.

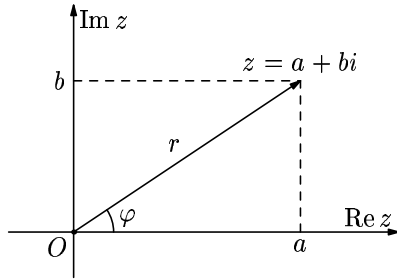
*Указание.* Используя упражнение 2.1.10, доказать, что любой изоморфизм поля рациональных чисел на себя является тождественным. Затем использовать определение действительных чисел, а также следующее соображение: для действительного числа  $a$  выполняется  $a \geq 0 \Leftrightarrow \Leftrightarrow \exists b \in \mathbb{R} : b^2 = a$ .

В силу определения поля  $\mathbb{C}$  два комплексных числа  $z$  и  $u$  равны тогда и только тогда, когда  $\operatorname{Re} z = \operatorname{Re} u$  и  $\operatorname{Im} z = \operatorname{Im} u$ . Поэтому существует биекция множества  $\mathbb{C}$  на множество пар действительных чисел  $\mathbb{R}^2$ , которое в свою очередь можно отождествить с множеством всех точек плоскости (или множеством всех векторов плоскости). Таким образом, комплексное число  $z = a + bi$  изображается точкой с координатами  $(a, b)$ . Координатную плоскость в этом случае называют *комплексной плоскостью*, ось абсцисс — *действительной осью*, а ось ординат — *мнимой осью*.

При векторном представлении комплексному числу  $z = a + bi$  ставится в соответствие вектор  $\vec{z}$  с координатами  $(a, b)$ . При таком представлении сложению комплексных чисел соответствует сложение соответствующих векторов по правилу параллелограмма. Для того чтобы естественным образом указать вектор, соответствующий произведению двух комплексных чисел, удобнее перейти к терминологии, связанной с полярными координатами.

**Определение 2.5.3.** Пусть  $z = a + bi \in \mathbb{C}$ . *Модулем* комплексного числа  $z = a + bi$  называется неотрицательное действительное число  $r = \sqrt{a^2 + b^2}$ , равное длине вектора  $\vec{z}$  с координатами  $(a, b)$ . Модуль

комплексного числа  $z$  обозначается через  $|z|$ .



**ЗАМЕЧАНИЕ.** При таком определении модуль произвольного действительного числа  $z = a + 0i$ , понимаемого как комплексное число с нулевой мнимой частью, равен  $\sqrt{a^2 + 0^2}$  и совпадает обычным определением модуля действительного числа.

**Определение 2.5.4.** *Аргументом* ненулевого комплексного числа  $z = a + bi$  называется величина угла, образуемого соответствующим вектором  $\vec{z}(a, b)$  с положительным направлением действительной оси комплексной плоскости. Аргумент определяется с точностью до прибавления целого кратного числа  $2\pi$ . Аргумент числа 0 не определён. Аргумент числа  $z$  обозначается через  $\arg z$ .

**ЗАМЕЧАНИЕ.** Хотя для числа 0 аргумент не определён, проблем не возникает, поскольку число 0 однозначно определяется своим модулем.

Пусть  $r$  и  $\varphi$  — модуль и аргумент комплексного числа  $z = a + bi$ . Несложно понять, что  $a = r \cos \varphi$  и  $b = r \sin \varphi$ . Поэтому

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

Это представление комплексного числа называется его *тригонометрической формой*.

Из данных нами определений следует, что два комплексных числа  $z = r(\cos \varphi + i \sin \varphi)$  и  $u = s(\cos \psi + i \sin \psi)$ , записанных в тригонометрической форме, равны тогда и только тогда, когда  $r = s$  и  $\varphi = \psi + 2k\pi$ ,  $k \in \mathbb{Z}$ .

**Предложение 2.5.1.** *Пусть заданы два комплексных числа  $z = r(\cos \varphi + i \sin \varphi)$  и  $u = s(\cos \psi + i \sin \psi)$ . Тогда их произведение  $zu = rs(\cos(\varphi + \psi) + i \sin(\varphi + \psi))$ .*

Иными словами, при умножении двух комплексных чисел их модули перемножаются, а аргументы складываются.

**ДОКАЗАТЕЛЬСТВО.** Формула умножения комплексных чисел легко выводится с использованием тригонометрических формул косинуса и синуса суммы двух углов.  $\square$

**Следствие** (формула Муавра). Пусть  $z = r(\cos \varphi + i \sin \varphi)$ . Тогда  $z^n = r^n(\cos n\varphi + i \sin n\varphi)$ .

Корнем  $n$ -ой степени из комплексного числа  $z$  мы назовём комплексное число  $u$ , такое, что  $u^n = z$ . Используя формулу Муавра, мы докажем следующую теорему о корнях  $n$ -ой степени из комплексного числа.

**Теорема 2.5.2.** Пусть  $z = r(\cos \varphi + i \sin \varphi)$  — ненулевое комплексное число. Тогда уравнение  $x^n = z$  имеет ровно  $n$  различных решений  $x_0, x_1, \dots, x_{n-1}$  в поле комплексных чисел. Причём для  $k = 0, 1, \dots, n-1$

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

**ДОКАЗАТЕЛЬСТВО.** Пусть комплексное число  $u = s(\cos \psi + i \sin \psi)$  — решение уравнения  $x^n = z$ . По формуле Муавра  $s^n = r$  и  $n\psi = \varphi + 2k\pi$  ( $k \in \mathbb{Z}$ ). Следовательно,  $s = \sqrt[n]{r}$  (арифметический корень) и  $\psi = \frac{\varphi + 2k\pi}{n}$ . Заметим, что для  $k, m \in \{0, 1, \dots, n-1\}$  значения косинуса и синуса от чисел  $\frac{\varphi + 2k\pi}{n}$  и  $\frac{\varphi + 2m\pi}{n}$  совпадают только в том случае, когда  $k = m$ . С другой стороны, при  $m = k + nj$  ( $j \in \mathbb{Z}$ ) аргументы  $\frac{\varphi + 2k\pi}{n}$  и  $\frac{\varphi + 2m\pi}{n} = \frac{\varphi + 2k\pi}{n} + 2j\pi$  различаются лишь на целое кратное  $2\pi$ . Следовательно, множество различных решений данного уравнения есть

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

Отметим в качестве упражнения некоторые полезные свойства корней  $n$ -ой степени из единицы.

**УПРАЖНЕНИЕ 2.5.2.** Доказать следующие утверждения:

1. Множество  $\mathbb{C}_n = \{\varepsilon_k \mid k = 0, 1, \dots, n-1\}$ , где  $\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$ , есть множество всех решений уравнения  $x^n = 1$ .

2. Если  $x_0$  — некоторое решение уравнения  $x^n = z$ , то множество  $\{x_k = x_0 \varepsilon_k \mid k = 0, 1, \dots, n-1\}$  — это множество всех решений уравнения  $x^n = z$ .

3. Множество  $\mathbb{C}_n$  относительно операции умножения комплексных чисел образует абелеву группу. При этом  $\langle \mathbb{C}_n, \cdot \rangle \simeq \langle \mathbb{Z}_n, + \rangle$  (см. упражнение 2.1.8).

# Глава 3

## Векторные пространства

### § 3.1. Определение векторного пространства

Использование алгебраических методов в геометрии неразрывно связано с понятием вектора. В этой главе мы изучим класс алгебраических систем, возникающих как обобщение геометрических векторов и связанных с ними операций. Напомним, что в элементарной геометрии рассматриваются следующие операции с векторами: сложение двух векторов и умножение вектора на число. Отметим, что умножение вектора на число нельзя рассматривать в качестве бинарной операции, так как множители берутся из разных множеств. Однако для каждого числа  $\alpha \in \mathbb{R}$  умножение на  $\alpha$  можно рассматривать как унарную операцию  $f_\alpha$ , сопоставляющую вектору  $v$  вектор  $\alpha v$ .

**Определение 3.1.1.** Пусть  $F$  — поле. *Векторное* (или *линейное*) *пространство* над полем  $F$  — это множество  $V$  (его элементы называются *векторами*), на котором определена бинарная операция  $+$  (*сложение векторов*) и по одной унарной операции  $v \mapsto \alpha v$  (*умножение вектора на скаляр*) для каждого скаляра  $\alpha$  из поля  $F$ , обладающие следующими свойствами.

1.  $\langle V, + \rangle$  — абелева группа.
2. Для любых  $\alpha \in F$  и  $u, v \in V$  выполняется  $\alpha(u + v) = \alpha u + \alpha v$ .
3. Для любых  $\alpha, \beta \in F$  и  $v \in V$  выполняется  $(\alpha + \beta)v = \alpha v + \beta v$ .
4. Для любых  $\alpha, \beta \in F$  и  $v \in V$  выполняется  $(\alpha\beta)v = \alpha(\beta v)$ .
5. Для любого  $v \in V$  и единицы  $1$  поля  $F$  выполняется  $1v = v$ .

Укажем в качестве упражнения некоторые элементарные свойства операций, заданных на векторном пространстве.

**УПРАЖНЕНИЕ 3.1.1.** Пусть  $V$  — векторное пространство над полем  $F$ ;  $\alpha, \beta \in F$ ;  $u, v \in V$ ;  $0$  — ноль поля  $F$ ,  $1$  — единица поля  $F$ , а  $\bar{0}$  — нейтральный по сложению вектор из  $V$  (его называют нуль-вектором). Тогда

- 1)  $\alpha\bar{0} = \bar{0}$ ;
- 2)  $\alpha(-v) = -\alpha v$ ;
- 3)  $\alpha(u - v) = \alpha u - \alpha v$ ;

- 4)  $0v = \bar{0}$ ;
- 5)  $(-1)v = -v$ ;
- 6)  $(\alpha - \beta)v = \alpha v - \beta v$ .

ЗАМЕЧАНИЕ. В дальнейшем, если не возникает путаницы с нулём поля  $F$ , мы будем обозначать нулевой вектор просто через  $0$ .

ПРИМЕРЫ. 1. Пусть  $F$  — некоторое поле. Зададим на множестве  $F^n = \{(\alpha_1, \alpha_2, \dots, \alpha_n) \mid \alpha_i \in F\}$  всех упорядоченных  $n$ -ок из элементов поля  $F$  операции сложения и умножения на скаляр  $\alpha \in F$  по правилам:

- 1)  $(\alpha_1, \alpha_2, \dots, \alpha_n) + (\beta_1, \beta_2, \dots, \beta_n) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots, \alpha_n + \beta_n)$ ;
- 2)  $\alpha(\alpha_1, \alpha_2, \dots, \alpha_n) = (\alpha\alpha_1, \alpha\alpha_2, \dots, \alpha\alpha_n)$ .

Тогда  $F^n$  относительно указанных операций образует векторное пространство над полем  $F$ . Это пространство называется *арифметическим векторным пространством*.

Заметим, что если ввести на плоскости (или в пространстве) систему координат и отождествить геометрические векторы плоскости (пространства) с их координатами в этой системе, то мы получим арифметическое векторное пространство  $\mathbb{R}^2$  ( $\mathbb{R}^3$ ).

2. Пусть  $F$  — подполе поля  $K$ . Тогда  $K$  можно рассматривать как векторное пространство над полем  $F$  относительно операции сложения элементов поля  $K$  и умножения элемента поля  $K$  на скаляр из  $F$ , понимаемого как обычное умножение элементов поля  $K$  (напомним, что  $F \subseteq K$ ). Так, поле  $\mathbb{R}$  действительных чисел можно рассматривать как векторное пространство над полем  $\mathbb{Q}$  рациональных чисел, а поле  $\mathbb{C}$  комплексных чисел — как векторное пространство над полем  $\mathbb{R}$ .

3. Множество  $F(X, K)$  всех функций из множества  $X$  в поле  $K$  является векторным пространством относительно обычных операций: сложения функций  $(f+g)(x) = f(x)+g(x)$  и умножения функции на скаляр  $(\alpha f)(x) = \alpha f(x)$ .

4. Векторным пространством является множество  $F[x]$  всех многочленов от переменной  $x$  над полем  $F$  относительно тех же операций, что и в предыдущем примере.

5. Множество  $M$  всех матриц размера  $m \times n$  над полем  $F$  является векторным пространством относительно операций сложения матриц и умножения матрицы на скаляр  $\alpha \in F$  по правилу  $A \mapsto \alpha A$ , где через  $\alpha A$ , как обычно, обозначена матрица, полученная из матрицы  $A$  умножением каждого её элемента на  $\alpha$ .

В частности, векторным пространством над полем  $F$  будет множество  $M_n(F)$  квадратных матриц. Напомним, что  $M_n(F)$  является также

кольцом относительно операций сложения и умножения матриц. Алгебраические системы, которые являются одновременно и кольцом, и векторным пространством, принято называть *алгебрами*.

**Определение 3.1.2.** *Алгеброй* над полем  $F$  называется множество  $A$  с двумя бинарными операциями: сложением и умножением, а также унарными операциями умножения на скаляр для каждого скаляра из поля  $F$ , если выполняется:

- 1)  $A$  — кольцо относительно операций сложения и умножения;
- 2)  $A$  — векторное пространство относительно сложения и умножения на скаляр;
- 3) для любых  $\alpha \in F$  и  $a, b \in A$  выполняется  $\alpha(ab) = (\alpha a)b = a(\alpha b)$ .

#### УПРАЖНЕНИЕ 3.1.2.

1. Проверить, что  $M_n(F)$  является алгеброй над  $F$ .
2. Используя приведённые примеры векторных пространств, привести примеры алгебр.

**Определение 3.1.3.** Пусть  $V$  — векторное пространство над полем  $F$ . Непустое подмножество  $U$  множества  $V$  называется *подпространством* пространства  $V$ , если оно замкнуто относительно операций, заданных на  $V$ , т.е. для любых  $u, v \in U$  и  $\alpha \in F$  выполняется  $u + v \in U$  и  $\alpha u \in U$ .

**ЗАМЕЧАНИЕ.** Заметим, что подпространство  $U$  пространства  $V$  над полем  $F$  само является векторным пространством над  $F$ . Действительно, ассоциативность и коммутативность сложения, а также все свойства, связывающие между собой операции сложения и умножения на скаляр, имеют место для векторов из  $U$ , поскольку векторы из  $U$  одновременно являются векторами из  $V$ . С другой стороны, в силу утверждения 5 упражнения 3.1.1 для любого элемента  $u \in U$  противоположный к нему элемент  $-u = (-1)u$  снова лежит в  $U$ , а значит, там лежит и нуль-вектор как их сумма.

**Определение 3.1.4.** Пусть  $A$  — алгебра над полем  $F$ . Непустое подмножество  $B$  множества  $A$  называется *подалгеброй* алгебры  $A$ , если оно замкнуто относительно операций, заданных на  $A$ , т.е. для любых  $a, b \in B$  и  $\alpha \in F$  выполняется  $a + b \in B$ ,  $ab \in B$  и  $\alpha a \in B$ .

**ПРИМЕРЫ.** 1. Любое пространство  $V$  всегда содержит два подпространства: *нулевое подпространство*  $0 = \{0\}$  и само пространство  $V$ . Всякое подпространство, отличное от нулевого, мы будем называть *нетривиальным*, а всякое подпространство, отличное от самого про-

пространства, — *собственным*. Аналогичные понятия можно определить и для произвольной алгебры  $A$ .

2. Множество  $\mathbb{R}$  действительных чисел можно рассматривать как подпространство (подалгебру) пространства (алгебры)  $\mathbb{C}$  над полем  $\mathbb{R}$ .

УПРАЖНЕНИЕ 3.1.3. Доказать следующие утверждения:

1. Подмножество  $\{(\alpha_1, \dots, \alpha_n) \mid \alpha_1 + \dots + \alpha_n = 0\}$  векторов арифметического пространства  $F^n$  над полем  $F$  является подпространством.

2. Подмножество  $F_n[x]$  многочленов от переменной  $x$ , степень которых не превосходит  $n$ , является подпространством пространства  $F[x]$  всех многочленов от переменной  $x$  над полем  $F$ . Однако если рассматривать  $F[x]$  как алгебру над  $F$ , то  $F_n[x]$  уже не является её подалгеброй.

3. Множество всех симметрических матриц из  $M_n(F)$ , т.е. матриц  $A \in M_n(F)$ , для которых  $A' = A$ , является подпространством пространства  $M_n(F)$  над полем  $F$ . Является ли это множество подалгеброй в алгебре  $M_n(F)$ ?

### § 3.2. Базис и размерность векторного пространства

Пусть  $V$  — векторное пространство над полем  $F$ . Под *набором* векторов  $a_1, a_2, \dots, a_s$  (не обязательно различных между собой!) мы будем понимать их упорядоченную совокупность.

**Определение 3.2.1.** *Линейной комбинацией* векторов (набора векторов)  $a_1, a_2, \dots, a_s$  векторного пространства  $V$  над полем  $F$  с коэффициентами  $\alpha_1, \alpha_2, \dots, \alpha_s$  из поля  $F$  называется выражение вида  $\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_s a_s$ , а также вектор, получающийся в результате выполнения операций в этом выражении. Линейная комбинация называется *тривиальной*, если  $\alpha_1 = \alpha_2 = \dots = \alpha_s = 0$ , и *нетривиальной* в противном случае.

ЗАМЕЧАНИЕ. Из свойств операций, заданных на  $V$ , следует, что тривиальная линейная комбинация любого набора векторов всегда равна 0.

**Определение 3.2.2.** Набор векторов  $a_1, a_2, \dots, a_s$  называется *линейно зависимым*, если существует нетривиальная линейная комбинация векторов этого набора, равная 0. В противном случае набор называется *линейно независимым*.

Иными словами, набор векторов  $a_1, a_2, \dots, a_s$  называется *линейно независимым*, если из равенства  $\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_s a_s = 0$  следует, что  $\alpha_1 = \alpha_2 = \dots = \alpha_s = 0$ .

**Определение 3.2.3.** Вектор  $a$  линейно выражается через набор векторов  $a_1, a_2, \dots, a_s$ , если существует линейная комбинация векторов этого набора, равная вектору  $a$ .

ПРИМЕРЫ. 1. Набор векторов

$$\begin{aligned} a_1 &= (1, 0, \dots, 0) \\ a_2 &= (0, 1, \dots, 0) \\ &\dots \\ a_n &= (0, 0, \dots, 1) \end{aligned}$$

из  $\mathbb{R}^n$ , векторы которого составляют строки единичной матрицы, является линейно независимым, поскольку из равенства  $\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n = (\alpha_1, \alpha_2, \dots, \alpha_n) = (0, 0, \dots, 0) = 0$  следует, что  $\alpha_1 = \alpha_2 = \dots = \alpha_n = 0$ .

2. Напротив, набор векторов  $a_1 = (1, 1, 1)$ ,  $a_2 = (0, 1, 2)$ ,  $a_3 = (1, 2, 3)$  из  $\mathbb{R}^3$  является линейно зависимым, так как  $1a_1 + 1a_2 + (-1)a_3 = 0$ . Заметим, что в этом случае вектор  $a_3$  линейно выражается через векторы  $a_1$  и  $a_2$ :  $a_3 = 1a_1 + 1a_2$ . Линейно зависимым, очевидно, является и любой набор, содержащий нуль-вектор.

Последнее замечание обобщается следующим образом.

**Предложение 3.2.1** (критерий линейной зависимости). *Набор векторов  $a_1, a_2, \dots, a_s$  линейно зависим тогда и только тогда, когда один из этих векторов линейно выражается через предыдущие, т. е. найдётся  $i \in \{1, \dots, s\}$ , такое, что  $a_i = \beta_1 a_1 + \dots + \beta_{i-1} a_{i-1}$ .*

ЗАМЕЧАНИЕ. Для удобства мы будем считать, что нулевой вектор и только он один линейно выражается через пустой набор векторов.

ДОКАЗАТЕЛЬСТВО. Из указанной договорённости следует, что наше утверждение верно для набора, состоящего из одного вектора. Поэтому в дальнейшем мы полагаем, что в нашем наборе есть по крайней мере два вектора.

Докажем необходимость. Пусть имеется нетривиальная комбинация  $\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_s a_s = 0$ . Тогда существует такое  $i \in \{1, \dots, s\}$ , что  $\alpha_i \neq 0$  и  $\alpha_{i+1} = \dots = \alpha_s = 0$  (возможно, что  $i = s$ ). Отсюда  $\alpha_1 a_1 + \dots + \alpha_{i-1} a_{i-1} + \alpha_i a_i = 0$ . Тогда

$$a_i = -\alpha_i^{-1}(\alpha_1 a_1 + \dots + \alpha_{i-1} a_{i-1}) = \left(-\frac{\alpha_1}{\alpha_i}\right)a_1 + \dots + \left(-\frac{\alpha_{i-1}}{\alpha_i}\right)a_{i-1},$$

и необходимость доказана.

Пусть теперь существует такое  $i$ , что  $a_i = \beta_1 a_1 + \dots + \beta_{i-1} a_{i-1}$ . Тогда линейная комбинация  $\beta_1 a_1 + \dots + \beta_{i-1} a_{i-1} + (-1)a_i + 0a_{i+1} + \dots + 0a_s$



равна 0 и нетривиальна, поскольку коэффициент при  $a_i = -1$  не равен 0.  $\square$

**Определение 3.2.4.** Пусть  $A$  и  $B$  — наборы векторов. Набор  $A$  линейно выражается через набор  $B$ , если каждый вектор набора  $A$  линейно выражается через векторы набора  $B$ . Наборы  $A$  и  $B$  эквивалентны, если  $A$  линейно выражается через  $B$ , а  $B$  линейно выражается через  $A$ .

**Определение 3.2.5.** Линейной оболочкой набора  $A$  векторов  $a_1, a_2, \dots, a_s$  называется множество всех векторов, являющихся линейными комбинациями векторов набора  $A$ . Линейная оболочка набора  $A$  обозначается через  $L(A)$  или  $\langle A \rangle$ .

Таким образом,

$$L(A) = \langle a_1, a_2, \dots, a_s \rangle = \{ \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_s a_s \mid \alpha_i \in F, i = 1, 2, \dots, s \}.$$

Договоримся считать, что линейной оболочкой пустого набора векторов является нулевое подпространство, т. е. множество векторов, состоящее только из нуль-вектора.

УПРАЖНЕНИЕ 3.2.1. Доказать следующие утверждения.

1. Линейная оболочка  $L(A)$  произвольного набора векторов  $A$  векторного пространства  $V$  является его подпространством.

2. Набор  $A$  линейно выражается через набор  $B$  тогда и только тогда, когда  $L(A) \subseteq L(B)$ . В частности, наборы  $A$  и  $B$  эквивалентны тогда и только тогда, когда  $L(A) = L(B)$ .

3. Если набор  $B$  получен из набора  $A$  перестановкой векторов, то  $L(A) = L(B)$ .

Теперь мы готовы сформулировать и доказать основное техническое утверждение этого параграфа, так называемую теорему о замене.

**Теорема 3.2.1** (о замене). Пусть  $A$  и  $B$  — наборы векторов  $a_1, a_2, \dots, a_r$  и  $b_1, b_2, \dots, b_s$  соответственно, причём набор  $A$  линейно независим и линейно выражается через набор  $B$ . Тогда  $r \leq s$  и существует такая перенумерация набора векторов  $B$ , что после неё набор  $B$  эквивалентен набору векторов  $a_1, \dots, a_r, b_{r+1}, \dots, b_s$ .

Иными словами, если условия теоремы выполнены, то найдётся  $r$  векторов набора  $B$  при замене которых на векторы набора  $A$  получится набор, эквивалентный исходному набору  $B$ .

**ДОКАЗАТЕЛЬСТВО.** Утверждение теоремы очевидно при  $r = 0$ . Предположим, что мы доказали теорему в случае, когда  $A$  состоит из  $r - 1$

вектора, и докажем её для  $r$  векторов. Обозначим через  $A'$  поднабор набора  $A$ , состоящий из векторов  $a_1, a_2, \dots, a_{r-1}$ . Очевидно, что  $A'$  линейно выражается через  $B$ . Кроме того, из определения линейной независимости несложно вывести, что  $A'$  линейно независим как поднабор линейно независимого набора  $A$ . Таким образом, наборы  $A'$  и  $B$  удовлетворяют условиям теоремы, а значит, по нашему предположению,  $r - 1 \leq s$  и существует перенумерация векторов набора  $B$ , такая, что набор  $B'$ , состоящий из векторов  $a_1, \dots, a_{r-1}, b_r, \dots, b_s$ , эквивалентен набору  $B$ , т. е.  $L(B') = L(B)$ .

По условию теоремы  $a_r \in L(B) = L(B')$ . Следовательно, вектор  $a_r$  линейно выражается через векторы набора  $B'$ :

$$a_r = \alpha_1 a_1 + \dots + \alpha_{r-1} a_{r-1} + \beta_r b_r + \dots + \beta_s b_s. \quad (1)$$

Если  $r - 1 = s$  или  $\beta_r = \dots = \beta_s = 0$ , то  $a_r = \alpha_1 a_1 + \dots + \alpha_{r-1} a_{r-1}$  и  $a_r$  линейно выражается через предыдущие векторы набора  $A$ , что в силу предложения 3.2.1 противоречит линейной независимости набора  $A$ . Таким образом,  $r \leq s$  и среди коэффициентов  $\beta_r, \dots, \beta_s$  есть хотя бы один ненулевой. Перенумеруем векторы  $b_r, \dots, b_s$  так, чтобы  $\beta_r \neq 0$ . Обозначим через  $B''$  набор  $a_1, \dots, a_r, b_{r+1}, \dots, b_s$ . Если мы докажем, что  $B''$  эквивалентен набору  $B'$ , то из равенств  $L(B'') = L(B') = L(B)$  будет следовать утверждение теоремы.

Поскольку векторы  $a_1, \dots, a_r, b_{r+1}, \dots, b_s$  принадлежат как набору  $B''$ , так и набору  $B'$ , нам нужно лишь показать, что  $a_r \in L(B')$  и  $b_r \in L(B'')$ . Первое сразу следует из равенства (1). С другой стороны, поскольку  $\beta_r \neq 0$ , из (1) следует, что вектор  $b_r$  равен

$$\left(-\frac{\alpha_1}{\beta_r}\right) a_1 + \dots + \left(-\frac{\alpha_{r-1}}{\beta_r}\right) a_{r-1} + \frac{1}{\beta_r} a_r + \left(-\frac{\beta_{r+1}}{\beta_r}\right) b_{r+1} + \dots + \left(-\frac{\beta_s}{\beta_r}\right) b_s.$$

Таким образом,  $b_r \in L(B'')$ . Поэтому наборы  $B'$  и  $B''$ , а значит, и наборы  $B$  и  $B''$  эквивалентны.  $\square$

**Следствие.** Если два линейно независимых набора эквивалентны, то они состоят из одного и того же числа векторов.

**Определение 3.2.6.** Векторное пространство  $V$  над полем  $F$  называется *конечномерным*, если в  $V$  существует конечный набор векторов  $v_1, v_2, \dots, v_s$ , линейная оболочка которого совпадает со всем пространством, т. е.  $\langle v_1, v_2, \dots, v_s \rangle = V$ .

**Определение 3.2.7.** *Базисом* (или *базой*) векторного пространства  $V$  над полем  $F$  называется линейно независимый набор векторов

пространства  $V$ , линейная оболочка которого совпадает с  $V$ .

**Теорема 3.2.2** (о базисе). Пусть  $V$  — конечномерное векторное пространство над полем  $F$ . Тогда верны следующие утверждения.

1.  $V$  обладает базисом.
2. Два базиса пространства  $V$  состоят из одного и того же числа векторов.
3. Если выбран базис пространства  $V$ , то каждый вектор пространства однозначно представляется в виде линейной комбинации векторов этого базиса.
4. Если  $A$  — линейно независимый набор векторов  $a_1, a_2, \dots, a_r$  пространства  $V$ , то существует базис пространства  $V$ , содержащий  $A$  в качестве поднабора.

**ДОКАЗАТЕЛЬСТВО.** 1. Пусть  $v_1, v_2, \dots, v_s$  — набор векторов пространства  $V$ , линейная оболочка которого совпадает с  $V$ . Исключим последовательно (начиная с первого) из него все векторы, которые выражаются через предыдущие. Заметим, что первый вектор требуется исключить только в том случае, если он нулевой. Обозначим получившийся в результате набор векторов через  $B$ . В силу предложения 3.2.1 набор  $B$  линейно независим. С другой стороны, поскольку любой вектор исходного набора линейно выражается через векторы из  $B$ , любой вектор пространства  $V$  также линейно выражается через векторы из  $B$ . Следовательно,  $L(B) = V$ , что и требовалось.

2. Пусть  $B$  и  $B'$  — два базиса пространства  $V$ . Поскольку  $L(B) = L(B') = V$ , наборы  $B$  и  $B'$  эквивалентны. По следствию из теоремы о замене получаем, что число векторов в этих наборах одно и то же.

3. Пусть  $B$  — базис пространства  $V$ , состоящий из векторов  $b_1, b_2, \dots, b_n$ . Предположим, что некоторый вектор  $v \in V$  имеет два представления через векторы базиса:

$$v = \alpha_1 b_1 + \alpha_2 b_2 + \dots + \alpha_n b_n = \beta_1 b_1 + \beta_2 b_2 + \dots + \beta_n b_n.$$

Тогда линейная комбинация  $(\alpha_1 - \beta_1)b_1 + (\alpha_2 - \beta_2)b_2 + \dots + (\alpha_n - \beta_n)b_n$  равна 0. Поскольку векторы из  $B$  линейно независимы, эта комбинация должна быть тривиальной. Следовательно,  $\alpha_1 = \beta_1, \dots, \alpha_n = \beta_n$  и представление вектора  $v$  однозначно.

4. Пусть  $B$  — базис пространства  $V$ , состоящий из векторов  $b_1, b_2, \dots, b_n$ . Набор  $A$  линейно независим и линейно выражается через набор  $B$ . Следовательно, по теореме о замене существует эквивалентный набору  $B$  набор  $B'$ , состоящий из  $n$  векторов и содержащий набор  $A$  в качестве поднабора. Поскольку  $B'$  эквивалентен  $B$ , выполняется  $L(B') = L(B) =$

$V$ . С другой стороны, если  $B'$  линейно зависим, то, исключая из него лишние векторы, как при доказательстве п. 1, мы получим его поднабор из меньшего числа векторов, который является базисом пространства, что противоречит п. 2. Таким образом,  $B'$  — базис пространства  $V$ , содержащий  $A$  в качестве поднабора.  $\square$

**Определение 3.2.8.** Число векторов в базисе векторного пространства  $V$  называется *размерностью* пространства и обозначается через  $\dim V$ .

**ЗАМЕЧАНИЕ.** В силу п. 2 теоремы о базисе определение размерности пространства корректно, поскольку любые два базиса состоят из одного и того же числа векторов.

**Следствие.** Пусть  $V$  — векторное пространство размерности  $n$  над полем  $F$ . Имеют место следующие утверждения.

1. При  $m > n$  любые  $m$  векторов из  $V$  линейно зависимы. Любые  $n$  линейно независимых векторов образуют базис пространства  $V$ .

2. При  $m < n$  линейная оболочка любого набора  $A$  из  $m$  векторов не совпадает с  $V$ . Любой набор  $B$  из  $n$  векторов, для которого  $L(B) = V$ , образует базис пространства  $V$ .

**УПРАЖНЕНИЕ 3.2.2.** Доказать следствие из теоремы о базисе.

**ПРИМЕРЫ.** 1. Пусть  $V = F^n$  — арифметическое векторное пространство над полем  $F$ . Тогда  $V$  конечномерно,  $\dim V = n$ , а в качестве базиса можно взять, например, набор

$$\begin{aligned} a_1 &= (1, 0, \dots, 0), \\ a_2 &= (0, 1, \dots, 0), \\ &\dots \\ a_n &= (0, 0, \dots, 1) \end{aligned}$$

из  $F^n$ , векторы которого составляют строки единичной матрицы из  $M_n(F)$ .

2. Если мы обозначим через  $E^2$  ( $E^3$ ) пространство геометрических векторов плоскости (пространства), то любые два неколлинеарных (три некопланарных) вектора этого пространства образуют базис. В частности,  $\dim E^2 = 2$  и  $\dim E^3 = 3$ .

3. Поле  $\mathbb{C}$  комплексных чисел, рассматриваемое как векторное пространство над полем  $\mathbb{R}$  действительных чисел, имеет размерность 2. Базисом этого пространства является, в частности, набор, состоящий из 1 и  $i$ , поскольку любое комплексное число однозначно представимо в виде  $a + bi$ , где  $a, b \in \mathbb{R}$ .

4. Векторное пространство  $V = \mathbb{R}[x]$  многочленов от одной переменной над полем  $\mathbb{R}$  действительных чисел не является конечномерным. Докажем это. Предположим, что  $V$  имеет конечный базис, состоящий из многочленов  $f_1, \dots, f_n$ . Обозначим через  $m$  наибольшую степень многочленов из этого базиса (степенью многочлена называется максимальная степень входящего в него одночлена с ненулевым коэффициентом). Тогда степень любого многочлена, являющегося линейной комбинацией многочленов  $f_1, \dots, f_n$ , не превосходит  $m$ . В частности, многочлен  $x^{m+1}$  не выражается через  $f_1, \dots, f_n$ . Полученное противоречие показывает, что  $V$  не конечномерно.

**УПРАЖНЕНИЕ 3.2.3.** Доказать, что набор векторов  $b_1, b_2, \dots, b_n$  арифметического пространства  $F^n$  является базисом этого пространства тогда и только тогда, когда матрица, строками которой являются упорядоченные  $n$ -ки  $b_1, b_2, \dots, b_n$ , невырождена.

**УПРАЖНЕНИЕ 3.2.4.** Доказать, что пространство  $M_{m \times n}(F)$  матриц конечномерно. Найдите базис и размерность этого пространства.

**УПРАЖНЕНИЕ 3.2.5.** Доказать, что пространство  $F(X, K)$  всех функций из множества  $X$  в поле  $K$  конечномерно тогда и только тогда, когда множество  $X$  конечно. Найти размерность этого пространства в случае, когда  $|X| = n$ .

**Указание.** Рассмотреть набор функций  $\varphi_a$  (здесь  $a$  пробегает всё множество  $X$ ), каждая из которых действует по правилу:

$$\varphi_a(x) = \begin{cases} 1, & \text{если } x = a, \\ 0, & \text{если } x \neq a. \end{cases}$$

Мы определили базис векторного пространства как набор векторов, который с одной стороны линейно независим, а с другой — обладает тем свойством, что каждый вектор пространства линейно выражается через векторы этого набора. Следующее утверждение показывает, что базис можно определить, используя каждое из этих свойств по отдельности.

**Предложение 3.2.2.** Пусть  $B$  — набор векторов конечномерного векторного пространства  $V$ . Следующие утверждения эквивалентны.

1.  $B$  — базис пространства  $V$ .
2.  $B$  — максимальный линейно независимый набор векторов пространства  $V$ .
3.  $B$  — минимальный набор векторов пространства, линейная оболочка которого совпадает со всем пространством  $V$ .

**ЗАМЕЧАНИЕ.** Максимальность (минимальность) набора с заданным свойством означает, что если мы добавим к набору (исключим из набора) произвольный вектор, то набор перестанет обладать указанным свойством.

**ДОКАЗАТЕЛЬСТВО.** (1  $\Rightarrow$  2) Поскольку каждый вектор  $v$  пространства  $V$  выражается через векторы базиса  $B$ , добавление  $v$  к  $B$  приведёт к тому, что полученный набор перестанет быть линейно независимым.

(2  $\Rightarrow$  1) Из максимальной  $B$  следует, что любой вектор, не входящий в  $B$ , линейно выражается через векторы из  $B$ . Следовательно,  $L(B) = V$  и  $B$  — базис.

(1  $\Rightarrow$  3) Пусть базис  $B$  не является минимальным набором с условием  $L(B) = V$ . Тогда в  $B$  найдётся вектор  $v$ , который линейно выражается через остальные векторы из  $B$ . Это противоречит линейной независимости набора  $B$ .

(3  $\Rightarrow$  1) Из минимальности  $B$  следует, что ни один из векторов набора  $B$  не выражается через остальные. Следовательно, набор  $B$  линейно независим.  $\square$

**Определение 3.2.9.** Пусть  $V$  — векторное пространство над полем  $F$  и  $\dim V = n$ . Зафиксируем некоторый базис  $B$  пространства  $V$ , состоящий из векторов  $b_1, b_2, \dots, b_n$ . Каждый вектор  $v \in V$  единственным образом записывается в виде линейной комбинации  $v = \beta_1 b_1 + \beta_2 b_2 + \dots + \beta_n b_n$  векторов базиса. Упорядоченная  $n$ -ка  $[v]_B = (\beta_1, \beta_2, \dots, \beta_n)$  называется *строкой координат* вектора  $v$  в базисе  $B$ .

**Теорема 3.2.3.** *Векторное пространство  $V$  размерности  $n$  над полем  $F$  изоморфно арифметическому векторному пространству  $F^n$ . Изоморфизмом является отображение  $\varphi : V \rightarrow F^n$ , действующее по правилу  $v\varphi = [v]_B$  для некоторого фиксированного базиса  $B$  пространства  $V$ .*

**ДОКАЗАТЕЛЬСТВО.** Поскольку базис  $B$  предполагается фиксированным, обозначим строку координат  $[v]_B$  вектора  $v$  через  $[v]$ . Тогда  $v\varphi = [v]$ . Каждый вектор пространства  $V$  единственным образом представляется в виде линейной комбинации векторов базиса, а значит, равенство  $[u] = [v]$  влечёт равенство  $u = v$ . Следовательно, отображение  $\varphi$  взаимно однозначно. Поскольку для любой упорядоченной  $n$ -ки  $(\beta_1, \beta_2, \dots, \beta_n)$  из  $F^n$  вектор  $v = \beta_1 b_1 + \beta_2 b_2 + \dots + \beta_n b_n$  лежит в  $V$ , отображение  $\varphi$  — сюръекция. Таким образом,  $\varphi$  — биекция.

Пусть  $[u] = (\alpha_1, \alpha_2, \dots, \alpha_n)$ ,  $[v] = (\beta_1, \beta_2, \dots, \beta_n)$ . Тогда  $u\varphi + v\varphi =$

$[u] + [v] = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots, \alpha_n + \beta_n) = [u + v] = (u + v)\varphi$ . Аналогично для каждого скаляра  $\alpha$  имеем  $\alpha(v\varphi) = \alpha[v] = [\alpha v] = (\alpha v)\varphi$ . Таким образом,  $\varphi$  сохраняет операции, заданные на  $V$ , и следовательно, является изоморфизмом.  $\square$

**Следствие.** *Два конечномерных векторных пространства одной и той же размерности над одним и тем же полем изоморфны.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $V$  и  $U$  — векторные пространства над полем  $F$  и  $\dim V = \dim U = n$ . Пространства  $V$  и  $U$  изоморфны  $F^n$ , а значит, изоморфны между собой.  $\square$

Рассмотрим теперь вопрос о том, как изменится запись вектора в виде строки координат при переходе от одного базиса пространства к другому.

Пусть  $V$  — векторное пространство размерности  $n$  над полем  $F$ . Пусть  $A$  и  $B$  — два базиса пространства  $V$ , состоящие из векторов  $a_1, \dots, a_n$  и  $b_1, \dots, b_n$  соответственно. Поскольку  $A$  — базис, для каждого  $i = 1, \dots, n$  вектор  $b_i$  из  $B$  линейно выражается через векторы  $A$ :

$$b_i = t_{i1}a_1 + \dots + t_{in}a_n. \quad (2)$$

Обозначим через  $a$  и  $b$  столбцы высоты  $n$ , элементами которых являются векторы базисов  $A$  и  $B$ . Иными словами,

$$a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \text{ и } b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

Тогда равенства (2) можно записать в матричном виде:

$$b = Ta, \text{ где } T = \begin{pmatrix} t_{11} & \dots & t_{1n} \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ t_{n1} & \dots & t_{nn} \end{pmatrix}.$$

Матрица  $T$  называется *матрицей перехода* от базиса  $A$  к базису  $B$ .

Докажем небольшое вспомогательное утверждение.

**Предложение 3.2.3.** *Пусть  $X = (x_{ij})$ ,  $Y = (y_{ij})$  —  $(m \times n)$ -матрицы. Пусть  $a$  — столбец высоты  $n$ , элементы которого — линейно независимые векторы  $a_1, \dots, a_n$ . Тогда из равенства  $Xa = Ya$  следует равенство  $X = Y$ .*

ДОКАЗАТЕЛЬСТВО. Из равенства  $Xa = Ya$  следует, что для каждого  $i = 1, \dots, m$  имеет место равенство  $x_{i1}a_1 + \dots + x_{in}a_n = y_{i1}a_1 + \dots + y_{in}a_n$ . Отсюда  $(x_{i1} - y_{i1})a_1 + \dots + (x_{in} - y_{in})a_n = 0$ . Из линейной независимости векторов  $a_1, \dots, a_n$  следует, что для каждого  $i = 1, \dots, m$  и каждого  $j = 1, \dots, n$  имеет место равенство  $x_{ij} = y_{ij}$ , т. е.  $X = Y$ .  $\square$

Пусть  $v$  — произвольный вектор пространства  $V$  и  $[v]_A, [v]_B$  — строки координат вектора  $v$  в базисах  $A$  и  $B$  соответственно. Используя матричную форму записи, вектор  $v$  можно записать так:  $v = [v]_A a = [v]_B b$ . С другой стороны,  $[v]_B b = [v]_B (Ta) = ([v]_B T)a$  (последнее равенство следует из ассоциативности умножения матриц согласованных размеров). В силу предложения 3.2.3 из равенства  $[v]_A a = ([v]_B T)a$  получаем равенство  $[v]_A = [v]_B T$ . Полученный нами результат можно сформулировать следующим образом.

*Если  $T$  — матрица перехода от базиса  $A$  к базису  $B$ , то строка координат вектора  $v$  в базисе  $A$  получается в результате умножения строки координат вектора  $v$  в базисе  $B$  на матрицу перехода  $T$ .*

Пусть  $A, B, C$  — базисы пространства  $V$ , а  $a, b, c$  — столбцы, составленные из векторов этих базисов. Пусть  $T$  — матрица перехода от базиса  $A$  к базису  $B$ ,  $S$  — матрица перехода от базиса  $B$  к базису  $C$ , а  $P$  — матрица перехода от базиса  $A$  к базису  $C$ . Из равенств  $c = Sb = S(Ta) = (ST)a$  и предложения 3.2.3 следует, что матрица перехода  $P$  от базиса  $A$  к базису  $C$  равна  $ST$ . В частности,  $[v]_A = [v]_C P = [v]_C (ST)$ .

УПРАЖНЕНИЕ 3.2.6. Пусть  $T$  — матрица перехода от базиса  $A$  к базису  $B$ . Доказать, что матрица  $T$  обратима, обратная к ней матрица  $T^{-1}$  есть матрица перехода от базиса  $B$  к базису  $A$  и для любого вектора  $v$  имеет место равенство  $[v]_B = [v]_A T^{-1}$ .

Указание. В предшествующем рассуждении нужно положить  $A = C$  и заметить, что матрица перехода от базиса  $A$  к базису  $A$  является единичной.

УПРАЖНЕНИЕ 3.2.7 \*. Установить биекцию между всеми базисами пространства  $V$  размерности  $n$  над полем  $F$  и множеством  $GL_n(F)$  всех невырожденных квадратных  $(n \times n)$ -матриц над полем  $F$ . В случае, когда поле  $F$  имеет конечный порядок  $q$ , найти порядок группы  $GL_n(F)$ .

ЗАМЕЧАНИЕ. Принятый нами способ записи вектора в виде строки координат называется *система вектор-строка*. В некоторых случаях удобнее использовать запись вектора  $v$  в некотором базисе  $B$  в виде столбца координат (*система вектор-столбец*). Используя принятые на-



ми обозначения и операцию транспонирования матриц, эту запись можно отобразить следующим образом:  $v = b'[v]'_B$ . Если  $A$  — ещё один базис пространства и  $v = a'[a]'_A$ , то матрица перехода  $\tilde{T}$  от базиса  $A$  к базису  $B$  в системе вектор-столбец есть транспонированная матрица перехода в принятой нами системе вектор-строка. Действительно, из равенства  $b = Ta$  после транспонирования получим  $b' = a'T' = a'\tilde{T}$ . Аналогично в системе вектор-столбец столбец координат вектора  $v$  в базе  $A$  выражается следующим образом:  $[v]'_A = \tilde{T}[v]'_B$ .

### § 3.3. Взаимное расположение подпространств

Начнём этот параграф с ещё одного определения понятия подпространства.

**Определение 3.3.1.** Пусть  $V$  — векторное пространство над полем  $F$ . Подмножество  $U$  множества  $V$  называется *подпространством*, если каждая линейная комбинация векторов из  $U$  снова лежит в  $U$ .

ЗАМЕЧАНИЕ. В этом определении, которое, очевидно, эквивалентно определению, данному в § 3.1, нам уже не нужно заранее предполагать, что множество  $U$  непусто, поскольку нулевой вектор, будучи линейной комбинацией пустого набора векторов, лежит в  $U$ .

**Теорема 3.3.1.** Пусть  $U$  — подпространство векторного пространства  $V$  размерности  $n$  над полем  $F$ . Тогда выполняются следующие утверждения.

1.  $U$  — конечномерное векторное пространство, и  $\dim U \leq n$ .
2. Каждый базис пространства  $U$  может быть дополнен до базиса пространства  $V$ .
3. Если  $\dim U = n$ , то  $U = V$ .

ДОКАЗАТЕЛЬСТВО. 1. Если  $U = 0 = \{\bar{0}\}$ , то  $U$  конечномерно (его базис — пустой набор векторов, а размерность равна 0).

Если  $U \neq 0$ , то найдётся ненулевой вектор  $u_1 \in U$ . Если  $L(u_1) = U$ , то  $\dim U = 1$ , и утверждение доказано (заметим, что  $u_1 \in V$ , а значит,  $\dim V \geq \dim U = 1$ ).

Пусть  $U \neq L(u_1)$ . Тогда найдётся вектор  $u_2 \in U$ , такой, что набор  $u_1, u_2$  линейно независим. Если  $L(u_1, u_2) = U$ , то снова утверждение доказано. Если же  $L(u_1, u_2) \neq U$ , то опять выбираем вектор  $u_3 \in U \setminus L(u_1, u_2)$ . Поскольку  $u_3$  нельзя линейно выразить через  $u_1, u_2$ , набор векторов  $u_1, u_2, u_3$  линейно независим. Продолжаем этот процесс, получая на каждом шаге линейно независимый набор векторов из  $U$ .

Поскольку пространство  $V$  имеет размерность  $n$ , число векторов в этом наборе не может превосходить  $n$  (см. утверждение 1 из следствия теоремы 3.2.2 о базисе). Значит, наш процесс оборвётся через конечное число шагов. Следовательно, для некоторого неотрицательного целого числа  $k$ , не превосходящего  $n$ , выполняется  $L(u_1, \dots, u_k) = U$ . Отсюда  $\dim U = k$ .

2. Поскольку любой базис  $U$  является линейно независимым набором векторов из  $V$ , утверждение сразу следует из п. 4 теоремы 3.2.2 о базисе.

3. Если  $\dim U = n$ , то базис  $B$  пространства  $U$  состоит из  $n$  линейно независимых векторов пространства  $V$ . В силу п. 1 следствия из теоремы 3.2.2 о базисе  $B$  является базисом пространства  $V$ .  $\square$

**Определение 3.3.2.** Базис пространства  $V$ , который содержит некоторый базис пространства  $U$  в качестве поднабора, называется *согласованным* с подпространством  $U$ .

В силу п. 2 теоремы 3.3.1 для каждого подпространства пространства  $V$  найдётся базис, согласованный с этим подпространством. Далее мы докажем, что даже для двух произвольных подпространств всегда найдётся базис пространства, одновременно согласованный с каждым из них.

**Определение 3.3.3.** Пусть  $U_1, U_2, \dots, U_s$  — подпространства векторного пространства  $V$  над полем  $F$ . *Суммой* подпространств  $U_1, U_2, \dots, U_s$  называется множество

$$U_1 + U_2 + \dots + U_s = \sum_{i=1}^s U_i = \{u_1 + u_2 + \dots + u_s \mid u_i \in U_i, i = 1, 2, \dots, s\}.$$

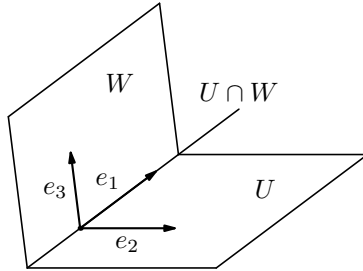
**УПРАЖНЕНИЕ 3.3.1.** Пусть  $U, W$  — подпространства пространства  $V$ . Доказать следующие утверждения.

1.  $U \cap W, U + W$  — подпространства пространства  $V$ .
2.  $U + W$  есть пересечение всех подпространств, содержащих и  $U$ , и  $W$ .
3.  $U \cup W$  — подпространство тогда и только тогда, когда  $U \subseteq W$  или  $W \subseteq U$ .

**ЗАМЕЧАНИЕ.** В утверждениях упражнения пересечение и объединение понимаются в теоретико-множественном смысле. Используя индукцию по  $s$ , несложно проверить, что сумма и пересечение подпространств  $U_1, U_2, \dots, U_s$  являются подпространствами пространства  $V$ .

**Теорема 3.3.2.** Пусть  $U, W$  — подпространства конечномерного пространства  $V$  над полем  $F$ . Найдётся базис пространства  $V$ , согласованный с каждым из подпространств.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $v_1, \dots, v_r$  — базис пересечения  $U \cap W$  (возможно, пустой). Пусть  $v_1, \dots, v_r, u_{r+1}, \dots, u_s$  — базис пространства  $U$ , а  $v_1, \dots, v_r, w_{r+1}, \dots, w_t$  — базис пространства  $W$ . Заметим, что оба эти базиса согласованы с  $U \cap W$ .



Если мы докажем, что набор векторов  $v_1, \dots, v_r, u_{r+1}, \dots, u_s, w_{r+1}, \dots, w_t$  линейно независим, то, дополнив его до базиса всего пространства, получим требуемое. Предположим, что линейная комбинация векторов данного набора равна нулю:

$$\alpha_1 v_1 + \dots + \alpha_r v_r + \alpha_{r+1} u_{r+1} + \dots + \alpha_s u_s + \beta_{r+1} w_{r+1} + \dots + \beta_t w_t = 0.$$

Отсюда

$$\alpha_1 v_1 + \dots + \alpha_r v_r + \alpha_{r+1} u_{r+1} + \dots + \alpha_s u_s = -(\beta_{r+1} w_{r+1} + \dots + \beta_t w_t).$$

Вектор, стоящий в левой части последнего равенства, лежит в  $U$ , а вектор, стоящий в его правой части, лежит в  $W$ . Поскольку левая и правая части равны, вектор  $z$ , равный левой (или правой) части равенства, лежит в  $U \cap W$ . Поскольку  $v_1, \dots, v_r$  — базис  $U \cap W$ , выполняется

$$z = \gamma_1 v_1 + \dots + \gamma_r v_r = -(\beta_{r+1} w_{r+1} + \dots + \beta_t w_t).$$

Следовательно,

$$\gamma_1 v_1 + \dots + \gamma_r v_r + \beta_{r+1} w_{r+1} + \dots + \beta_t w_t = 0.$$

В силу того, что  $v_1, \dots, v_r, w_{r+1}, \dots, w_t$  — базис пространства  $W$ , имеем  $\gamma_1 = \dots = \gamma_r = \beta_{r+1} = \dots = \beta_t = 0$ . Отсюда  $z = 0$ . Следовательно,  $\alpha_1 v_1 + \dots + \alpha_r v_r + \alpha_{r+1} u_{r+1} + \dots + \alpha_s u_s = 0$ . Поскольку

$v_1, \dots, v_r, u_{r+1}, \dots, u_s$  — базис пространства  $U$ , выполняется  $\alpha_1 = \dots = \alpha_s = 0$ , что и требовалось доказать.  $\square$

**Следствие.** Если  $U, W$  — подпространства конечномерного пространства  $V$ , то  $\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$ .

**ДОКАЗАТЕЛЬСТВО.** Из определения суммы следует, что  $U$  и  $W$  — подпространства пространства  $U + W$ . Сохраняя обозначения теоремы, докажем, что  $U + W = \langle v_1, \dots, v_r, u_{r+1}, \dots, u_s, w_{r+1}, \dots, w_t \rangle$ . Для любого  $v \in U + W$  имеем

$$\begin{aligned} v &= u + w = (\alpha_1 v_1 + \dots + \alpha_r v_r + \alpha_{r+1} u_{r+1} + \dots + \alpha_s u_s) + \\ &\quad + (\beta_1 v_1 + \dots + \beta_r v_r + \beta_{r+1} w_{r+1} + \dots + \beta_t w_t) = \\ &= (\alpha_1 + \beta_1) v_1 + \dots + (\alpha_r + \beta_r) v_r + \alpha_{r+1} u_{r+1} + \dots + \alpha_s u_s + \beta_{r+1} w_{r+1} + \dots + \beta_t w_t. \end{aligned}$$

Таким образом,  $v_1, \dots, v_r, u_{r+1}, \dots, u_s, w_{r+1}, \dots, w_t$  — базис пространства  $U + W$ . Поэтому

$$\dim(U + W) = s + (t - r) = \dim U + \dim W - \dim(U \cap W).$$

**УПРАЖНЕНИЕ 3.3.2.** Пусть  $U_1, U_2, \dots, U_s$  — подпространства векторного пространства  $V$  и  $S$  — сумма этих подпространств. Доказать, что  $\dim S \leq \sum_{i=1}^s \dim U_i$ .

**Указание.** Используя следствие из теоремы 3.3.2, провести рассуждение индукцией по  $s$ .

**Определение 3.3.4.** Пусть  $U_1, U_2, \dots, U_s$  — подпространства векторного пространства  $V$  над полем  $F$ . Сумма  $U_1 + U_2 + \dots + U_s$  этих подпространств называется *прямой суммой*, если из равенства  $u_1 + u_2 + \dots + u_s = 0$ , где  $u_i \in U_i, i = 1, 2, \dots, s$ , следует  $u_1 = u_2 = \dots = u_s = 0$ . Прямая сумма подпространств  $U_1, U_2, \dots, U_s$  обозначается как

$$U_1 \oplus U_2 \oplus \dots \oplus U_s \text{ или } \bigoplus_{i=1}^s U_i.$$

**Теорема 3.3.3.** Пусть  $U_1, U_2, \dots, U_s$  — подпространства конечномерного векторного пространства  $V$  над полем  $F$  и  $S = U_1 + U_2 + \dots + U_s$  — сумма этих подпространств. Следующие утверждения эквивалентны.

1.  $S$  — прямая сумма.

2. Каждый вектор  $v \in S$  единственным образом записывается в виде суммы  $v = u_1 + u_2 + \dots + u_s$ , где  $u_i \in U_i$ ,  $i = 1, 2, \dots, s$ .

3. Набор векторов, составленный из базисов подпространств  $U_1, U_2, \dots, U_s$ , есть базис пространства  $S$ .

4.  $\dim S = \sum_{i=1}^s \dim U_i$ .

5. Пусть  $S_j = U_1 + \dots + U_{j-1} + U_{j+1} + \dots + U_s$ . Для каждого  $j \in \{1, 2, \dots, s\}$  имеет место  $U_j \cap S_j = 0$ .

ДОКАЗАТЕЛЬСТВО. (1  $\Rightarrow$  2) Пусть для некоторого  $v \in S$  выполняется  $v = u_1 + u_2 + \dots + u_s = w_1 + w_2 + \dots + w_s$ , где  $u_i, w_i \in U_i$ . Тогда  $(u_1 - w_1) + (u_2 - w_2) + \dots + (u_s - w_s) = 0$ , а значит,  $u_1 = w_1$ ,  $u_2 = w_2$ ,  $\dots$ ,  $u_s = w_s$ .

(2  $\Rightarrow$  3) Пусть для каждого  $i = 1, 2, \dots, s$  набор  $B_i$  векторов  $b_{i1}, \dots, b_{it_i}$  — базис пространства  $U_i$ . Нам нужно показать, что набор  $B$ , составленный из наборов  $B_1, B_2, \dots, B_s$ , является базисом пространства  $S$ . Поскольку  $S = \sum_{i=1}^s U_i$ , выполняется  $L(B) = S$ . Остаётся показать, что набор  $B$  линейно независим. Предположим, что

$$\sum_{i=1}^s \sum_{j=1}^{t_i} \alpha_{ij} b_{ij} = 0. \quad (1)$$

Для  $i = 1, 2, \dots, s$  положим  $u_i = \sum_{j=1}^{t_i} \alpha_{ij} b_{ij}$ . Тогда  $\sum_{i=1}^s u_i = 0$ . Поскольку нуль-вектор единственным образом записывается в сумму  $u_i$ , для каждого  $i = 1, 2, \dots, s$  имеем  $u_i = 0$ . Из линейной независимости наборов  $B_i$  следует, что все коэффициенты  $\alpha_{ij}$  в равенстве (1) равны 0.

(3  $\Rightarrow$  4) Очевидно.

(4  $\Rightarrow$  5) Заметим, что для каждого  $j \in \{1, 2, \dots, s\}$  выполняется  $S = U_j + S_j$ . По условию  $\dim S = \sum_{i=1}^s \dim U_i$ . С другой стороны, в силу следствия из теоремы 3.3.2 имеем  $\dim S = \dim U_j + \dim S_j - \dim(U_j \cap S_j)$ . Отсюда  $\sum_{i=1, i \neq j}^s \dim U_i = \dim S_j - \dim(U_j \cap S_j)$ . Поскольку из утверждения упражнения 3.3.2 следует, что  $\dim S_j \leq \sum_{i=1, i \neq j}^s \dim U_i$ , получаем  $\dim(U_j \cap S_j) = 0$ . Следовательно,  $U_j \cap S_j = 0$ .

(5  $\Rightarrow$  1) Пусть  $\sum_{i=1}^s u_i = 0$  и существует  $j \in \{1, 2, \dots, s\}$ , такое, что  $u_j \neq 0$ . Тогда из равенства  $u_j = -u_1 + \dots + (-u_{j-1}) + (-u_{j+1}) + \dots + (-u_s)$  следует, что  $u_j \in U_j \cap S_j$ ; противоречие.  $\square$

ЗАМЕЧАНИЕ. Из п. 5 теоремы следует, что сумма  $U + W$  двух подпространств  $U$  и  $W$  является прямой тогда и только тогда, когда  $U \cap W = 0$ .

УПРАЖНЕНИЕ 3.3.3. Привести пример трёх подпространств, все попарные пересечения которых равны нулю, а их сумма не является прямой.

**Определение 3.3.5.** Пусть  $V = U \oplus W$ . Тогда каждый вектор  $v \in V$  однозначно представляется в виде  $v = u + w$ , где  $u \in U$ ,  $w \in W$ . Вектор  $u$  называется *проекцией* вектора  $v$  на подпространство  $U$  параллельно подпространству  $W$ .

**ЗАМЕЧАНИЕ.** Определение проекции  $u$  вектора  $v$  зависит как от выбора подпространства  $U$ , так и выбора подпространства  $W$  (поскольку такой выбор не определяется однозначно выбором  $U$ ).

Определение проекции несложно перенести на случай прямой суммы нескольких подпространств. В этом случае проектирование на одно из них происходит параллельно прямой сумме остальных.

**ПРИМЕРЫ.** 1. Пусть набор  $B$  векторов  $b_1, b_2, \dots, b_n$  — базис пространства  $V$  над полем  $F$ . Тогда  $V = \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \dots \oplus \langle b_n \rangle$  является прямой суммой  $n$  одномерных подпространств. Проекция вектора  $v \in V$  на  $\langle b_i \rangle$  есть вектор  $\alpha_i b_i$ , где  $\alpha_i$  — это  $i$ -я координата вектора  $v$  в базисе  $B$ .

2. Рассмотрим пространство  $V = F(\mathbb{R}, \mathbb{R})$  всех функций на вещественной прямой. Обозначим через  $V_+$ ,  $V_-$  подмножества множества  $V$  всех чётных и всех нечётных функций соответственно. Несложно проверить, что  $V_+$  и  $V_-$  — подпространства пространства  $V$ . Пусть  $f \in F[\mathbb{R}, \mathbb{R}]$ . Зададим функции  $f_+$  и  $f_-$  следующим образом:  $f_+(x) = \frac{1}{2}(f(x) + f(-x))$  и  $f_-(x) = \frac{1}{2}(f(x) - f(-x))$ . Тогда  $f_+$  — чётная функция,  $f_-$  — нечётная функция и  $f = f_+ + f_-$ . Следовательно,  $V = V_+ + V_-$ . С другой стороны,  $V_+ \cap V_- = 0$ . Поэтому  $V = V_+ \oplus V_-$ . Отметим, что в этом примере и само пространство, и два подпространства, в прямую сумму которых оно разлагается, бесконечномерны.

Напомним, что квадратная матрица  $A$  называется *симметрической*, если  $A' = A$ . Квадратная матрица  $A$  называется *кососимметрической*, если  $A' = -A$ . В силу утверждения (3) упражнения 3.1.3 подмножество всех симметрических матриц пространства  $M_n(F)$  является подпространством.

**УПРАЖНЕНИЕ 3.3.4.** Проверить, что подмножество всех кососимметрических матриц пространства  $M_n(F)$  квадратных матриц является подпространством. Доказать, что векторное пространство  $M_n(F)$  есть прямая сумма подпространств симметрических и кососимметрических матриц.

# Глава 4

## Системы линейных уравнений

### § 4.1. Ранг матрицы

Эта глава посвящена системам линейных уравнений. Однако в первом параграфе мы введём и обсудим понятие ранга матрицы. Используя это понятие, в следующем параграфе мы сформулируем критерий совместности системы линейных уравнений.

**Определение 4.1.1.** Пусть  $A$  — набор векторов  $a_1, a_2, \dots, a_s$  векторного пространства  $V$  над полем  $F$ . *Рангом набора  $A$*  называется размерность его линейной оболочки  $L(A)$ . Ранг набора  $A$  обозначается через  $r(A)$ .

Пусть ранг набора  $A$  равен  $r$ . Отметим, что, рассуждая, как при доказательстве п. 1 теоремы 3.2.2 о базисе, несложно выбрать  $r$  векторов набора  $A$ , составляющих базис  $L(A)$ . Иногда, допуская некоторую вольность речи, мы будем называть выбранные таким образом векторы *базисом набора*.

**Определение 4.1.2.** Пусть  $A$  —  $(m \times n)$ -матрица над полем  $F$ . Обозначим через  $a_1, \dots, a_m$  строки, а через  $\tilde{a}_1, \dots, \tilde{a}_n$  — столбцы матрицы  $A$ . Строки матрицы  $A$  можно рассматривать как векторы пространства  $F^m$ , а её столбцы — как векторы пространства  $F^n$ . *Строчный ранг* матрицы  $A$  — это ранг набора  $a_1, \dots, a_m$ . *Столбцовый ранг* матрицы  $A$  — это ранг набора  $\tilde{a}_1, \dots, \tilde{a}_n$ .

Оказывается, для любой матрицы её строчный и столбцовый ранги совпадают. Мы докажем это утверждение, называемое теоремой о ранге матрицы, показав, что оба указанных числа равны третьему, так называемому *минорному рангу*. В § 2.3 было введено понятие минора, дополнительного к элементу матрицы. Теперь нам потребуется более общий термин.

**Определение 4.1.3.** Пусть  $A = (a_{ij})$  —  $(m \times n)$ -матрица над полем  $F$  и  $r$  — некоторое натуральное число, такое, что  $r \leq \min\{m, n\}$ . Пусть выбраны некоторые  $r$  строк и  $r$  столбцов матрицы  $A$ . Квадратная матрица  $M$ , составленная из элементов матрицы  $A$ , стоящих на

пересечении данных  $r$  строк и  $r$  столбцов, взятых в соответствующем расположении, называется *минором* размерности  $r$  матрицы  $A$ . Более точно, если выбраны строки с номерами  $i_1, \dots, i_r$  и столбцы с номерами  $j_1, \dots, j_r$ , то элемент  $m_{kl}$  минора  $M$  равен  $a_{i_k, j_l}$ .

**ЗАМЕЧАНИЕ.** Следуя традиции, было бы точнее назвать минором определитель матрицы, которую мы назвали минором. Тем не менее мы фиксируем определение минора как матрицы, а не как её определителя, считая его более удобным.

**ПРИМЕР.** Пусть

$$A = \begin{pmatrix} 1 & 2 & 1 & 0 \\ 2 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \text{ Тогда } M = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix} \text{ — минор размерности } 2,$$

составленный из элементов матрицы  $A$ , стоящих на пересечении первой, второй строки и первого, третьего столбцов.

**УПРАЖНЕНИЕ 4.1.1.** Если  $C_k^r = \frac{k!}{r!(k-r)!}$  — число сочетаний из  $k$  предметов по  $r$ , то число миноров размерности  $r$  в  $(m \times n)$ -матрице равно  $C_m^r \cdot C_n^r$ .

**Определение 4.1.4.** *Минорным рангом* матрицы  $A$  называется наибольшая размерность её невырожденного минора. Иными словами, минорный ранг матрицы равен  $r$ , если в ней есть хотя бы один невырожденный минор размерности  $r$  и нет невырожденных миноров размерности  $r + 1$ .

**ПРИМЕР.** В предыдущем примере ранг матрицы  $A$  равен 2. Невырожденным минором размерности 2 является минор  $M$ .

**Теорема 4.1.1** (о ранге матрицы). Пусть  $A = (a_{ij})$  —  $(m \times n)$ -матрица над полем  $F$ . Строчный, столбцовый и минорный ранги матрицы  $A$  совпадают.

**ДОКАЗАТЕЛЬСТВО.** Мы докажем, что строчный ранг равен минорному. Доказательство того факта, что столбцовый ранг совпадает с минорным, а значит, и со строчным, проводится аналогично с одновременной заменой слова «строка» на слово «столбец» и наоборот.

Пусть минорный ранг матрицы  $A$  равен  $r$ . Это означает, что можно выбрать  $r$  строк и  $r$  столбцов матрицы  $A$  так, чтобы на их пересечении стоял минор  $M$  размерности  $r$ , определитель которого не равен 0. Кроме того, все миноры размерности  $r + 1$  матрицы  $A$  (если такие миноры вообще существуют) вырождены. Не теряя общности, мы можем



считать, что невырожденный минор  $M$  стоит на пересечении первых  $r$  строк и первых  $r$  столбцов. Действительно, это предположение просто позволяет нам вместо номеров  $i_1, i_2, \dots, i_r$  использовать номера  $1, 2, \dots, r$  для обозначения соответствующих строк. То же верно и для обозначений столбцов. Итак, пусть  $M = (a_{ij})$ , где  $i, j \in \{1, 2, \dots, r\}$ .

Обозначим  $i$ -ю строку матрицы  $A$  через  $a_i$ , а  $i$ -ю строку минора  $M$  — через  $\bar{a}_i$ . Тогда для  $i \in \{1, 2, \dots, r\}$  строка  $\bar{a}_i$  — подстрока строки  $a_i$ , состоящая из первых её  $r$  элементов. Предположим, что строки  $a_1, a_2, \dots, a_r$  линейно зависимы как векторы арифметического пространства  $F^n$ , т. е. найдётся нетривиальная линейная комбинация этих строк, равная нулю. Тогда линейная комбинация с теми же самыми коэффициентами строк  $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_r$  как векторов пространства  $F^r$  тоже, очевидно, равна нулю. Следовательно, они линейно зависимы. Но тогда в силу утверждения упражнения 3.2.3 имеем  $\det M = 0$ ; противоречие. Итак, строки  $a_1, a_2, \dots, a_r$  матрицы  $A$  линейно независимы, т. е. её строчный ранг больше либо равен  $r$ .

Если  $m = r$ , то теорема доказана. Поэтому мы можем считать, что  $m > r$ . Докажем, что строки матрицы  $A$  с номером, большим  $r$ , линейно выражаются через первые  $r$  строк. Очевидно, что достаточно доказать это для какой-то одной строки. Например, для  $(r+1)$ -ой. Пусть  $\bar{a}_{r+1} = (a_{r+1,1}, a_{r+1,2}, \dots, a_{r+1,r})$ . Поскольку  $r$  строк  $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_r$  пространства  $F^r$  линейно независимы, они образуют базис в этом пространстве. Следовательно, строка  $\bar{a}_{r+1}$  является их линейной комбинацией:  $\bar{a}_{r+1} = \alpha_1 \bar{a}_1 + \alpha_2 \bar{a}_2 + \dots + \alpha_r \bar{a}_r$ . Обозначим через  $b$  строку пространства  $F^n$ , равную  $a_{r+1} - (\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_r a_r)$ . Если мы докажем, что  $b = (\beta_1, \beta_2, \dots, \beta_n) = \bar{0}$ , то получим требуемое. Отметим, что в силу выбора коэффициентов  $\alpha_1, \alpha_2, \dots, \alpha_r$  первые  $r$  элементов строки  $b$  уже равны нулю. Пусть найдётся такой элемент  $\beta_i$  ( $i > r$ ), что  $\beta_i \neq 0$ . Снова без потери общности можно считать, что  $i = r+1$ . Рассмотрим минор  $M^*$  размерности  $r+1$  матрицы  $A$ , составленный из первых  $r+1$  строк и первых  $r+1$  столбцов.

$$\left( \begin{array}{ccc|c} a_{11} & \dots & a_{1r} & a_{1,r+1} \\ \vdots & M & \vdots & \vdots \\ a_{r1} & \dots & a_{rr} & a_{r,r+1} \\ \hline a_{r+1,1} & \dots & a_{r+1,r} & a_{r+1,r+1} \end{array} \right) \rightarrow \left( \begin{array}{ccc|c} a_{11} & \dots & a_{1r} & a_{1,r+1} \\ \vdots & M & \vdots & \vdots \\ a_{r1} & \dots & a_{rr} & a_{r,r+1} \\ \hline 0 & \dots & 0 & \beta_{r+1} \end{array} \right)$$

По условию  $\det M^* = 0$ . Вычтем из последней строки минора  $M^*$

последовательно первую строку, умноженную на  $\alpha_1$ , вторую строку, умноженную на  $\alpha_2, \dots, r$ -ю строку, умноженную на  $\alpha_r$ . Полученная в результате матрица  $M^{**}$  будет иметь определитель, равный определителю матрицы  $M^*$ . С другой стороны, все элементы её  $r + 1$ -ой строки, а это  $\beta_1, \beta_2, \dots, \beta_{r+1}$ , кроме, быть может, последнего, равны нулю. Разложив определитель матрицы  $M^{**}$  по последней строке, получим  $0 = \det M^* = \det M^{**} = \beta_{r+1} \det M$ . Поскольку  $\det M \neq 0$ , выполняется равенство  $\beta_{r+1} = 0$ , что противоречит выбору  $\beta_{r+1}$ . Таким образом,  $b = 0$  и  $a_{r+1} = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_r a_r$ .  $\square$

**Определение 4.1.5.** Строчный (столбцевой, минорный) ранг матрицы  $A$  называется её *рангом* и обозначается через  $r(A)$ .

**Следствие.** Ранг квадратной  $(n \times n)$ -матрицы  $A$  равен  $n$  тогда и только тогда, когда  $\det A \neq 0$ .

ЗАМЕЧАНИЕ. Минор  $M^*$  размерности  $r + 1$ , полученный из минора  $M$  размерности  $r$  в результате добавления некоторой строки и некоторого столбца, принято называть минором, *окаймляющим* минор  $M$ . Изучив доказательство теоремы о ранге, обоснуйте следующее утверждение.

УПРАЖНЕНИЕ 4.1.2. Если все окаймляющие миноры невырожденного минора размерности  $r$  матрицы  $A$  равны нулю или их вообще нет, то ранг матрицы  $A$  равен  $r$ .

Утверждение, сформулированное в упражнении, указывает способ вычисления ранга матрицы (в данном случае минорного). Однако на практике проще найти строчный ранг матрицы, используя её приведение к так называемому ступенчатому виду. Ступенчатая матрица — это матрица вида

$$\left( \begin{array}{cccc} \boxed{a_{1j_1}} & \dots & \dots & \dots \\ & \boxed{a_{2j_2}} & \dots & \dots \\ & & \dots & \dots \\ & & & \dots \\ & & & \boxed{a_{rj_r}} \dots \\ & 0 & & \dots \end{array} \right). \tag{1}$$

Дадим точное определение.

**Определение 4.1.6.** Назовём *ведущим* элементом ненулевой строки матрицы её первый слева ненулевой элемент. Матрица называется *ступенчатой*, если выполнены следующие условия:

1) номера столбцов ведущих элементов ненулевых строк матрицы образуют строго возрастающую последовательность;

2) нулевые строки, если они есть, стоят в конце.

Несложно заметить, что ранг ступенчатой матрицы равен числу ненулевых строк. В частности, у представленной матрицы невырожденным является минор, стоящий на пересечении первых  $r$  строк и столбцов с номерами  $j_1, j_2, \dots, j_r$ , а невырожденных миноров размерности  $(r + 1)$ , очевидно, нет.

Напомним, что мы назвали *элементарными* следующие преобразования строк (столбцов) матрицы:

1) прибавление к строке (столбцу) другой строки (другого столбца), умноженной на скаляр;

2) умножение строки (столбца) на ненулевой скаляр.

Добавим к этим преобразованиям ещё один тип преобразований:

3) перестановка двух строк (столбцов) местами.

Отметим, что любое преобразование третьего типа можно представить в виде цепочки последовательных преобразований первого и второго типов, и в этом смысле его введение является *избыточным*. Причина его добавления — удобство при применении.

Практическое определение ранга матрицы основано на двух следующих утверждениях.

**Предложение 4.1.1.** *При элементарных преобразованиях строк (столбцов) матрицы  $A$  её ранг не меняется.*

**ДОКАЗАТЕЛЬСТВО.** Достаточно заметить, что строки  $a_i, a_j$  линейно выражаются через строки  $a_i + \alpha a_j$  и  $a_j$ , а строка  $a_i$  — через строку  $\alpha a_i$ , если  $\alpha \neq 0$ .  $\square$

**Предложение 4.1.2.** *Каждая матрица приводится элементарными преобразованиями строк к ступенчатому виду.*

**ДОКАЗАТЕЛЬСТВО.** Утверждение доказывается индукцией по числу  $m$  строк матрицы  $A = (a_{ij})_{m \times n}$ . Пусть  $j_1$  — наименьший номер столбца матрицы  $A$ , содержащего ненулевой элемент. Переставив при необходимости строки местами, получим матрицу, в которой элемент, стоящий на месте  $(1, j_1)$ , не равен нулю. Используя элементарные преобразования первого типа, занулим с помощью этого элемента все остальные

элементы  $j_1$ -го столбца. В результате получится матрица вида

$$\left( \begin{array}{ccc|c|ccc} 0 & \dots & 0 & a_{1j_1} & * & \dots & * \\ \hline & & & 0 & & & \\ & & & \vdots & & & \\ & 0 & & 0 & & A_1 & \end{array} \right).$$

В силу предположения индукции матрицу  $A_1$  можно привести элементарными преобразованиями к ступенчатому виду. В результате вся матрица  $A$  будет приведена к виду (1).  $\square$

Мы завершаем этот параграф утверждением о ранге суммы и произведения матриц.

### Предложение 4.1.3.

1. Пусть  $A = (a_{ij})_{m \times n}$ ,  $B = (b_{ij})_{m \times n}$  — матрицы над полем  $F$ . Тогда  $r(A + B) \leq r(A) + r(B)$ .

2. Пусть  $A = (a_{ij})_{m \times s}$ ,  $B = (b_{ij})_{s \times n}$  — матрицы над полем  $F$ . Тогда  $r(AB) \leq r(A)$  и  $r(AB) \leq r(B)$ .

ДОКАЗАТЕЛЬСТВО. 1. Пусть  $C = (c_{ij})_{m \times n} = A + B$ . Рассмотрим матрицы  $A, B, C$  как наборы векторов арифметического пространства  $F^n$ , состоящие из строк этих матриц. Поскольку для каждого  $i = 1, 2, \dots, m$  выполняется  $c_i = a_i + b_i$ , имеем  $L(C) \subseteq L(A) + L(B)$ . Следовательно,  $r(C) = \dim L(C) \leq \dim(L(A) + L(B)) \leq \dim L(A) + \dim L(B) = r(A) + r(B)$ .

2. Пусть  $C = (c_{ij})_{m \times n} = AB$ . Докажем сначала, что  $r(C) \leq r(B)$ . Рассмотрим матрицы  $B, C$  как наборы векторов арифметического пространства  $F^n$ , состоящие из строк этих матриц. Поскольку для каждого  $i = 1, 2, \dots, m$  выполняется  $c_i = (c_{i1}, \dots, c_{in}) =$

$$= \left( \sum_{k=1}^s a_{ik}b_{k1}, \dots, \sum_{k=1}^s a_{ik}b_{kn} \right) = \sum_{k=1}^s a_{ik}(b_{k1}, \dots, b_{kn}) = \sum_{k=1}^s a_{ik}b_k,$$

набор  $C$  линейно выражается через набор  $B$ . Отсюда  $L(C) \subseteq L(B)$  и  $r(C) \leq r(B)$ .

Доказательство неравенства  $r(C) \leq r(A)$  проводится аналогично. Нужно лишь рассмотреть наборы столбцов матриц  $A$  и  $C$ .  $\square$



**Теорема 4.2.1** (критерий совместности системы линейных уравнений). Система (1) совместна тогда и только тогда, когда ранг матрицы  $A$  системы (1) равен рангу расширенной матрицы этой системы, т. е.  $r(A) = r(\tilde{A})$ .

**ДОКАЗАТЕЛЬСТВО.** Воспользуемся векторной формой (2) записи системы (1). Заметим, что строка  $x^0 = (x_1^0, x_2^0, \dots, x_n^0)$  есть решение системы (1) тогда и только тогда, когда  $b = x_1^0 a_1 + x_2^0 a_2 + \dots + x_n^0 a_n$ , т. е. вектор  $b$  — линейная комбинация векторов  $a_1, a_2, \dots, a_n$  с коэффициентами  $x_1^0, x_2^0, \dots, x_n^0$ . Следовательно, совместность системы (1) равносильна равенству линейных оболочек  $\langle a_1, a_2, \dots, a_n \rangle = \langle a_1, a_2, \dots, a_n, b \rangle$ , а значит, и равенству  $r(A) = r(\tilde{A})$ .  $\square$

**ЗАМЕЧАНИЕ.** Этот критерий также называют теоремой Кронекера — Капелли.

На практике проверить, совместна ли система линейных уравнений, можно следующим образом. Приведём элементарными преобразованиями строк расширенную матрицу  $\tilde{A}$  к ступенчатому виду. При этом к ступенчатому виду будет приведена и матрица  $A$  как подматрица матрицы  $\tilde{A}$ . Если в полученной ступенчатой матрице есть строка с ведущим элементом, стоящим в последнем столбце, то система несовместна. В противном случае  $r(A) = r(\tilde{A})$  и система совместна.

Для решения совместной системы уравнений вида (1) можно использовать так называемый *метод Гаусса*, основанный на справедливости следующего утверждения.

**Предложение 4.2.1.** При элементарных преобразованиях уравнений системы (1), соответствующих элементарным преобразованиям строк расширенной матрицы её коэффициентов, множество решений системы не изменяется.

**ДОКАЗАТЕЛЬСТВО.** Прямая проверка, как в доказательстве предложения 4.1.1.  $\square$

Изложению метода Гаусса мы и посвятим остаток параграфа.

**Определение 4.2.3.** Ступенчатая матрица  $A$  называется *унифицированной* (или *редуцированной*), если выполнены следующие условия:

- 1) ведущие элементы её ненулевых строк равны 1;
- 2) все элементы любого столбца, содержащего ведущий элемент, кроме самого ведущего элемента, равны 0.

**УПРАЖНЕНИЕ 4.2.1.** Каждая матрица приводится элементарными преобразованиями строк к унифицированному ступенчатому виду.

Пусть система линейных уравнений (1) совместна. Приведём расширенную матрицу  $\tilde{A} = (A \mid b)$  её коэффициентов элементарными преобразованиями строк к унифицированному ступенчатому виду. Обозначим получившуюся матрицу, из которой мы убрали все нулевые строки, через  $\tilde{C} = (C \mid d)$ . Тогда система

$$Cx' = d \quad (4)$$

равносильна исходной системе  $Ax' = b$ . Предположим, что

$$r(\tilde{A}) = r(A) = r.$$

Тогда  $\tilde{C} - (r \times (n + 1))$ -матрица, строки которой линейно независимы. Пусть подстановка

$$\begin{pmatrix} 1 & \dots & r & \dots & n \\ j_1 & \dots & j_r & \dots & j_n \end{pmatrix}$$

выбрана так, что  $c_{1j_1} = c_{2j_2} = \dots = c_{rj_r} = 1$  — ведущие элементы строк матрицы  $\tilde{C}$ . Назовём неизвестные  $x_{j_1}, \dots, x_{j_r}$  *связанными*, а неизвестные  $x_{j_{r+1}}, \dots, x_{j_n}$  — *свободными*. Перенесём все свободные неизвестные системы (4) вместе со стоящими перед ними коэффициентами в правую часть каждого из уравнений системы. В результате получится система вида

$$\begin{cases} x_{j_1} = -c_{1j_{r+1}}x_{j_{r+1}} - \dots - c_{1j_n}x_{j_n} + d_1, \\ x_{j_2} = -c_{2j_{r+1}}x_{j_{r+1}} - \dots - c_{2j_n}x_{j_n} + d_2, \\ \dots \\ x_{j_r} = -c_{rj_{r+1}}x_{j_{r+1}} - \dots - c_{rj_n}x_{j_n} + d_r, \end{cases} \quad (5)$$

равносильная системе (4), а значит, и системе (1).

Пусть  $t_1, t_2, \dots, t_{n-r}$  — произвольный упорядоченный набор из  $n - r$  элементов поля  $F$ . Определим элементы строки  $x^0$  пространства  $F^n$  следующим образом:  $x_i^0 = f_i(t_1, t_2, \dots, t_{n-r})$  для  $i = 1, \dots, n$ , где  $f_{j_i}(t_1, t_2, \dots, t_{n-r}) = -c_{ij_{r+1}}t_1 - \dots - c_{ij_n}t_{n-r} + d_i$  при  $i = 1, \dots, r$  и  $f_{j_i}(t_1, t_2, \dots, t_{n-r}) = t_{i-r}$  при  $i = r + 1, \dots, n$ . Тогда  $x^0$  — решение системы (5). С другой стороны, если  $x^0 = (x_1^0, x_2^0, \dots, x_n^0)$  — произвольное решение системы (5), то, положив  $t_1 = x_{j_{r+1}}^0, \dots, t_{n-r} = x_{j_n}^0$ , получим, что любое решение системы (5) может быть записано в виде  $x^0 = (f_1(t_1, \dots, t_{n-r}), \dots, f_n(t_1, \dots, t_{n-r}))$ . Поскольку системы (1) и (5) эквивалентны, мы получили общее решение системы (1). Уточним полученный результат следующим образом.

**Определение 4.2.4.** Пусть  $F$  — поле. Упорядоченная  $n$ -ка функций  $(f_1(t_1, \dots, t_s), \dots, f_n(t_1, \dots, t_s))$ , где  $f_i : F^s \rightarrow F$ , называется *общим решением системы (1)*, если множество решений системы (1) равно множеству

$$\{(f_1(t_1, \dots, t_s), \dots, f_n(t_1, \dots, t_s)) \mid (t_1, \dots, t_s) \in F^s\}.$$

Выше мы фактически доказали следующее утверждение.

**Теорема 4.2.2.** Пусть система (1) совместна и ранг её матрицы коэффициентов равен  $r$ . Тогда существует  $n$  функций  $f_i : F^{n-r} \rightarrow F$  вида  $f_i(t_1, \dots, t_{n-r}) = \alpha_{i1}t_1 + \dots + \alpha_{i,n-r}t_{n-r} + \beta_i$ , где  $i = 1, 2, \dots, n$ , от  $n - r$  переменных, упорядоченная  $n$ -ка которых является общим решением системы (1).

Как следует из утверждения теоремы, каждое частное решение системы получается из общего решения подстановкой на место переменных некоторого набора из  $n - r$  элементов поля  $F$ . Подчёркнём, что из нашего анализа следует, что, хотя общее решение системы может быть записано различными способами, число переменных, от которых зависят функции, составляющие общее решение системы, является инвариантом системы (1). Это число равно разности между числом неизвестных и рангом матрицы коэффициентов системы.

Иногда общим решением системы (1) называют просто систему (5).

УПРАЖНЕНИЕ 4.2.2. Для системы

$$\begin{cases} x_1 + 2x_2 + x_3 = 2, \\ x_1 + 3x_2 + 2x_3 - x_4 = 4, \\ 2x_1 + x_2 - x_3 + 3x_4 = -2, \\ 2x_1 - 2x_3 + 4x_4 = -4 \end{cases} \quad (6)$$

записать её векторную и матричную формы. Привести расширенную матрицу системы к ступенчатому виду и проверить, что система совместна. Привести полученную матрицу к унифицированному ступенчатому виду и найти общее решение системы.

Для решения систем уравнений, в которых количество независимых уравнений (ранг матрицы коэффициентов системы) равно количеству неизвестных, применяют также *метод Крамера*, основанный на вычислении определителей специального вида. И хотя для практического разыскания решения системы метод Гаусса удобнее, мы докажем в заключение этого параграфа утверждение, на котором основан метод Крамера, поскольку он имеет существенное теоретическое значение.





**ДОКАЗАТЕЛЬСТВО.** Запишем однородную систему (1) в матричном виде  $Ax' = 0$ . Пусть  $x^1, x^2$  — два решения этой системы (не обязательно различные). Тогда  $A((x^1)' + (x^2)') = A(x^1)' + A(x^2)' = 0 + 0 = 0$ . Следовательно, строка  $x^0 = x^1 + x^2$  — снова решение системы. Аналогично доказывается, что строка  $\alpha x^0$  является решением системы, если строка  $x^0$  — решение, а  $\alpha$  — произвольный скаляр.

Пусть упорядоченная  $n$ -ка функций  $f_i(t_1, \dots, t_{n-r})$ , где  $i = 1, \dots, n$ , есть общее решение системы (1), существующее в силу теоремы 4.2.2. Для  $k = 1, \dots, n - r$  и  $i = 1, \dots, n$  положим  $x_i^k = f_i(0, \dots, 0, 1, 0, \dots, 0)$ , где 1 стоит на  $k$ -ом месте. Рассмотрим набор из  $n - r$  строк  $x^k = (x_1^k, \dots, x_n^k) \in F^n$ . Во-первых, для каждого  $k = 1, \dots, n - r$  строка  $x^k$  — решение системы (1). Во-вторых, эти строки линейно независимы, поскольку составленная из них матрица содержит минор размерности  $n - r$ , равный единичной матрице. В-третьих, любое решение системы можно выразить в виде линейной комбинации строк этого набора. Действительно, произвольное решение можно записать в виде  $x^0 = (f_1(\alpha_1, \dots, \alpha_{n-r}), \dots, f_n(\alpha_1, \dots, \alpha_{n-r})) = \alpha_1 x^1 + \dots + \alpha_{n-r} x^{n-r}$ . Таким образом, набор  $x^1, \dots, x^{n-r}$  — базис пространства  $X$ .  $\square$

**Определение 4.3.2.** Базис пространства решений однородной системы линейных уравнений называется *фундаментальным набором решений* системы.

**Следствие.** Пусть  $V = F^n$  — арифметическое векторное пространство размерности  $n$  над полем  $F$ , а  $U$  — подпространство размерности  $k$  пространства  $V$ . Тогда существует однородная система линейных уравнений от  $n$  неизвестных над полем  $F$ , пространство решений которой совпадает с  $U$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть набор векторов  $u_i = (\beta_{i1}, \dots, \beta_{in})$ , где  $i = 1, \dots, k$ , является базисом подпространства  $U$ . Рассмотрим однородную систему  $Bu' = 0$ , матрица коэффициентов которой  $B = (\beta_{ij})_{k \times n}$  состоит из записанных построчно коэффициентов этого базиса. Поскольку ранг матрицы  $B$  равен  $k$ , по теореме 4.3.1 пространство решений системы  $Bu' = 0$  имеет размерность  $n - k$ . Выберем некоторый фундаментальный набор решений этой системы:  $a_i = (\alpha_{i1}, \dots, \alpha_{in})$ , где  $i = 1, \dots, n - k$ . Пусть  $A = (\alpha_{ij})_{(n-k) \times n}$  — матрица, строки которой являются элементами этого фундаментального набора. Поскольку  $\alpha_{i1}\beta_{j1} + \dots + \alpha_{in}\beta_{jn} = 0$  для каждого  $i = 1, \dots, n - k$  и  $j = 1, \dots, k$ , строка  $u_j$  является решением однородной системы  $Ax' = 0$  для каждого  $j = 1, \dots, k$ . Поэтому  $U$  лежит в пространстве  $X$  решений системы

$Ax' = 0$ . С другой стороны, ранг матрицы  $A$  равен  $n - k$ , а значит, размерность пространства  $X$  равна  $n - (n - k) = k$ . Следовательно,  $U = X$ .  $\square$

**Теорема 4.3.2.** Пусть совместная система линейных уравнений  $Ax' = b$  имеет матрицу коэффициентов  $A$  и  $Ax' = 0$  — однородная система с той же матрицей коэффициентов. Пусть  $x^0$  — одно из решений системы  $Ax' = b$ ,  $X$  — множество всех решений системы  $Ax' = b$ , а  $Z$  — множество всех решений системы  $Ax' = 0$ . Тогда  $X = x^0 + Z = \{x^0 + z \mid z \in Z\}$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $z^0$  — решение однородной системы. Тогда  $A(x^0 + z^0)' = A(x^0)' + A(z^0)' = b + 0 = b$ . Следовательно,  $x^0 + Z \subseteq X$ . С другой стороны, если  $x$  — произвольное решение исходной неоднородной системы, то  $A(x - x^0)' = Ax' - A(x^0)' = b - b = 0$ . Следовательно,  $z = x - x^0$  — решение однородной системы. Поэтому  $X \subseteq x^0 + Z$ .  $\square$

**Следствие.** Если система  $Ax' = b$  совместна, то она имеет единственное решение тогда и только тогда, когда система  $Ax' = 0$  имеет только тривиальное решение.

Ещё одно утверждение о связи между однородной и неоднородной системами уравнений называют теоремой Фредгольма.

**Теорема 4.3.3** (Фредгольм). Пусть даны система линейных уравнений  $Ax' = b$  и однородная система  $A'y' = 0$ , матрица коэффициентов которой есть транспонированная матрица коэффициентов неоднородной системы. Система  $Ax' = b$  совместна тогда и только тогда, когда для любого решения  $y$  системы  $A'y' = 0$  выполняется равенство  $yb = 0$ .

**ДОКАЗАТЕЛЬСТВО.** Предположим, что система  $Ax' = b$  совместна и строка  $x^0$  — некоторое её решение. Тогда выполняется матричное равенство  $A(x^0)' = b$ . Заметим, что равенство  $A'y' = 0$  равносильно равенству  $yA = 0$  (одно получается из другого с помощью транспонирования). Следовательно, для каждого  $y$ , удовлетворяющего условию  $A'y' = 0$ , выполняется  $yb = y(A(x^0)') = (yA)(x^0) = 0$ .

Пусть для каждого  $y$ , такого, что  $A'y' = 0$ , выполняется  $yb = 0$ , а значит, и  $b'y' = 0$ . Тогда пространство решений системы

$$\left(\begin{array}{c} A' \\ b' \end{array}\right) y' = 0$$

совпадает с пространством решений системы  $A'y' = 0$ . Следовательно,

имеет место равенство рангов

$$r(A') = r\left(\frac{A'}{b'}\right),$$

которое после транспонирования матриц превращается в равенство  $r(A) = r(A | b)$ . Отсюда и из теоремы Кронекера — Капелли вытекает совместность системы  $Ax' = b$ .  $\square$

**УПРАЖНЕНИЕ 4.3.1.** Рассмотреть однородную систему линейных уравнений с той же матрицей коэффициентов, что и неоднородная система из упражнения 4.2.2. Найти общее решение этой системы и её фундаментальный набор решений. Проверить справедливость утверждений теорем 4.3.2 и 4.3.3 на этом примере.

Отметим, что мы строили теорию систем линейных уравнений над произвольным полем (в том числе и произвольным конечным полем).

**УПРАЖНЕНИЕ 4.3.2.** Пусть  $F = \mathbb{Z}_2$  — поле вычетов по модулю 2 и система

$$\begin{cases} x_2 + x_3 + x_5 = 1, \\ x_1 + x_2 = 1, \\ x_2 + x_3 + x_4 + x_5 = 0, \\ x_1 + x_2 + x_4 = 0 \end{cases}$$

задана над этим полем. Найти все решения данной системы и соответствующей ей однородной системы.

## Глава 5

### Кольцо многочленов

#### § 5.1. Кольцо многочленов от одной переменной

Эта глава посвящена многочленам. Под многочленом (от одной переменной) с действительными коэффициентами обычно понимается функция  $f : \mathbb{R} \rightarrow \mathbb{R}$  вида  $f(x) = a_0 + a_1x + \dots + a_nx^n$ , где  $a_i \in \mathbb{R}$ . Однако если рассматривать многочлены над произвольным полем (или даже кольцом), то в случае конечного поля (кольца) определение многочлена как отображения не слишком удачно. Действительно, многочлены  $x$  и  $x^2$  над полем  $F = \mathbb{Z}_2$  порядка 2, очевидно, совпадают как отображения, так как  $0^2 = 0$  и  $1^2 = 1$ . Поскольку удобнее считать их различными, мы дадим более абстрактное определение многочлена, а потом покажем, что в случае бесконечного поля данное нами определение не отличается от определения многочлена как функции. Для краткости обозначим через  $\mathbb{N}_0$  множество  $\mathbb{N} \cup \{0\}$  целых неотрицательных чисел.

**Определение 5.1.1.** Пусть  $k \in \mathbb{N}_0$ . *Многочленом* (или *полиномом*)  $f$  от переменной  $x$  над кольцом  $R$  называется выражение

$$f(x) = \sum_{k=0}^{\infty} a_k x^k = a_0 x^0 + a_1 x^1 + \dots + a_k x^k + \dots,$$

где коэффициенты  $a_k$  лежат в кольце  $R$  и лишь конечное их число отлично от 0. Ненулевой коэффициент многочлена  $f$  с наибольшим индексом называется *старшим коэффициентом* многочлена, а сам этот индекс называется *степенью* многочлена  $f$  и обозначается через  $\deg f$ . Коэффициент многочлена с индексом нуль называется *свободным* коэффициентом. Множество всех многочленов от переменной  $x$  над кольцом  $R$  обозначается через  $R[x]$ .

**ЗАМЕЧАНИЕ.** Если договориться, что одночлены, т.е. выражения вида  $a_k x^k$ , с нулевыми коэффициентами при записи многочлена могут быть опущены, то многочлен степени  $n$  можно записать в виде  $f(x) = a_0 x^0 + a_1 x^1 + \dots + a_n x^n$ . Кроме того, многочлены нулевой степени естественным образом отождествляются с элементами кольца  $R$  ( $a_0 x^0 = a_0$ ). Используя это отождествление, мы приходим к привычной

форме записи многочлена  $f(x) = a_0 + a_1x + \dots + a_nx^n$ . Отметим также, что нулевой многочлен  $0 = \sum_{k=0}^{\infty} 0x^k$  не является многочленом степени 0. Его степень считается неопределённой. Иногда для удобства (об этом ниже) полагают, что  $\deg 0 = -\infty$ .

**Определение 5.1.2.** Многочлены  $f(x) = \sum_{k=0}^{\infty} a_kx^k$  и  $g(x) = \sum_{k=0}^{\infty} b_kx^k$  равны, если для любого  $k \in \mathbb{N}_0$  имеет место равенство  $a_k = b_k$ .

ЗАМЕЧАНИЕ. В силу данного определения многочлены  $x$  и  $x^2$  над полем  $\mathbb{Z}_2$  должны рассматриваться как различные.

**Определение 5.1.3.** Пусть  $R$  — кольцо и многочлены

$$f(x) = \sum_{k=0}^{\infty} a_kx^k, \quad g(x) = \sum_{k=0}^{\infty} b_kx^k \in R[x].$$

Многочлены

$$h(x) = \sum_{k=0}^{\infty} c_kx^k \quad \text{и} \quad p(x) = \sum_{k=0}^{\infty} d_kx^k \in R[x]$$

называются соответственно *суммой* и *произведением* многочленов  $f$  и  $g$ , если для любого  $k \in \mathbb{N}_0$  выполняется  $c_k = a_k + b_k$  и  $d_k = \sum_{i+j=k} a_ib_j$  (указанные равенства формализуют хорошо знакомые читателю раскрытие скобок и приведение подобных). Обозначения:  $h = f+g$  и  $p = fg$ .

ЗАМЕЧАНИЕ. Данное определение корректно, поскольку  $h = f+g$  и  $p = fg$  имеют лишь конечное число отличных от нуля коэффициентов, а значит, являются многочленами.

**Теорема 5.1.1.** Пусть  $R$  — кольцо. Тогда имеют место следующие утверждения.

1.  $R[x]$  — кольцо относительно операций сложения и умножения многочленов.
2. Если  $R$  — коммутативное кольцо, то  $R[x]$  — коммутативное кольцо.
3. Если  $R$  — кольцо с единицей, то  $R[x]$  — кольцо с единицей.

ДОКАЗАТЕЛЬСТВО. Доказательство теоремы представляет собой последовательную проверку аксиом кольца, а также свойств коммутативности и существования единицы. Например, если  $f(x) = \sum_{k=0}^{\infty} a_kx^k$ ,  $g(x) = \sum_{k=0}^{\infty} b_kx^k$ ,  $h(x) = \sum_{k=0}^{\infty} c_kx^k$ , то закон правой дистрибутивности  $fh + gh = (f+g)h$  следует из равенств

$$\sum_{i+j=k} a_ic_j + \sum_{i+j=k} b_ic_j = \sum_{i+j=k} (a_i + b_i)c_j \quad \text{для } k \in \mathbb{N}_0,$$

которые, в свою очередь, легко выводятся из соответствующих аксиом кольца  $R$ .  $\square$

**ЗАМЕЧАНИЕ.** Отождествление элементов кольца  $R$  с многочленами нулевой степени в  $R[x]$  (и нуля с нулевым многочленом) позволяет считать, что  $R$  — подкольцо кольца  $R[x]$ .

**УПРАЖНЕНИЕ 5.1.1.** Доказать теорему 5.1.1 полностью.

**Предложение 5.1.1.** Пусть  $R$  — кольцо и  $f, g \in R[x]$ ,  $f, g \neq 0$ . Тогда имеют место следующие утверждения.

1.  $\deg(f + g) \leq \max\{\deg f, \deg g\}$ .
2.  $\deg fg \leq \deg f + \deg g$ , причём если  $R$  — кольцо без делителей нуля, то  $\deg fg = \deg f + \deg g$  и  $R[x]$  — кольцо без делителей нуля.

**ЗАМЕЧАНИЕ.** Отметим, что если один из многочленов в формулировке предложения нулевой, то утверждение п. 2 предложения остаётся в силе, если считать, что  $\deg 0 = -\infty$ .

**Следствие.** Если  $R$  — поле, то множество  $R[x]^*$  всех обратимых элементов кольца  $R[x]$  — это множество всех многочленов нулевой степени.

**УПРАЖНЕНИЕ 5.1.2.** Доказать предложение 5.1.1 и следствие из него. Привести пример кольца  $R$ , для многочленов над которым формула  $\deg fg = \deg f + \deg g$  неверна.

В дальнейшем мы будем рассматривать многочлены над некоторым полем  $F$ . Как уже отмечалось, множество многочленов  $F[x]$  относительно операций сложения и умножения на скаляр образует векторное пространство. Следовательно,  $F[x]$  — алгебра над полем  $F$ . Отметим, что эта алгебра всегда бесконечномерна.

## § 5.2. Делимость в кольце многочленов

В силу следствия из предложения 5.1.1 многочлен ненулевой степени не имеет обратного по умножению в кольце  $F[x]$ . Поэтому деление в привычном смысле в кольце многочленов невозможно. Однако, как и в кольце целых чисел, в кольце многочленов можно естественным образом определить деление с остатком.

**Теорема 5.2.1** (о делении с остатком). Пусть  $f, g$  — многочлены из  $F[x]$  и  $g \neq 0$ . Тогда существуют многочлены  $q, r \in F[x]$ , такие, что  $f = qg + r$  и либо  $r = 0$ , либо  $\deg r < \deg g$ . Многочлены  $q$  и  $r$ , удовлетворяющие этим условиям, определены однозначно.

**ДОКАЗАТЕЛЬСТВО.** Начнём с доказательства существования. Если  $\deg f < \deg g$ , то, полагая  $q = 0$ ,  $r = f$ , получим требуемое. Таким образом, мы можем считать, что  $\deg f = n \geq \deg g = m$ . Пусть  $f(x) = a_n x^n + \dots + a_1 x + a_0$  и  $b(x) = b_m x^m + \dots + b_1 x + b_0$ . Используем индукцию по  $n$ . Поскольку для  $n = 0$  утверждение очевидно (речь идет о делении в поле  $F$ ), база индукции установлена. Следовательно, мы можем полагать, что  $n > 0$  и для всех многочленов степени, меньшей  $n$ , утверждение уже доказано. Рассмотрим многочлен  $f_1 = f - \frac{a_n}{b_m} x^{n-m} g$ . Его степень меньше  $n$ , следовательно, существуют такие многочлены  $q_1$  и  $r$ , что  $f_1 = q_1 g + r$  и либо  $r = 0$ , либо  $\deg r < \deg g$ . Тогда  $f = \frac{a_n}{b_m} x^{n-m} g + f_1 = (\frac{a_n}{b_m} x^{n-m} + q_1) g + r$ , и многочлены  $q = \frac{a_n}{b_m} x^{n-m} + q_1$  и  $r$  — искомые.

Пусть  $f = qg + r = q'g + r'$ . Тогда  $r - r' = (q' - q)g$ . Если  $q' - q$  — ненулевой многочлен, то в силу п. 2 предложения 5.1.1 степень многочлена, стоящего в правой части равенства, больше или равна  $\deg g$ . С другой стороны, степень многочлена, стоящего в левой части, в силу п. 1 того же предложения и условия на степени многочленов  $r, r'$  меньше  $\deg g$ . Полученное противоречие показывает, что  $q' = q$ , а значит, и  $r = r'$ .  $\square$

**Определение 5.2.1.** Многочлены  $q$  и  $r$ , определённые в теореме, называются соответственно (*неполным*) *частным* и *остатком* при делении  $f$  на  $g$ .

**Определение 5.2.2.** Многочлен  $g \neq 0$  делит многочлен  $f$ , если найдётся многочлен  $q$ , такой, что  $f = qg$ . В этом случае  $g$  называется *делителем* многочлена  $f$ , а  $f$  — *кратным* многочлена  $g$ . Запись  $g \mid f$  означает, что  $g$  делит  $f$ , а запись  $f \dot{=} g$  означает, что  $f$  делится на  $g$ .

**ЗАМЕЧАНИЕ.** Тот факт, что  $g$  не делит  $f$ , будем кратко обозначать так:  $g \nmid f$ .

**Предложение 5.2.1** (свойства делимости многочленов). В кольце  $F[x]$  выполняются следующие утверждения.

1. Если  $g \mid f$  и  $g \mid h$ , то  $g \mid (f + h)$ .
2. Если  $g \mid f$ , то для каждого  $h \in F[x]$  выполняется  $g \mid (fh)$ .
3. Если  $\deg g = 0$ , то для каждого  $h \in F[x]$  выполняется  $g \mid h$ .
4. Если  $\deg h = 0$  и  $g \mid f$ , то  $(hg) \mid f$ .

**УПРАЖНЕНИЕ 5.2.1.** Доказать предложение 5.2.1, используя определение делимости.

**Определение 5.2.3.** Пусть  $f, g \in F[x]$ . Наибольшим общим дели-



теlem многочленов  $f$  и  $g$  называется многочлен  $d \in F[x]$ , удовлетворяющий следующим условиям:

- 1)  $d \mid f$  и  $d \mid g$ ;
- 2) если  $d' \in F[x]$  таков, что  $d' \mid f$  и  $d' \mid g$ , то  $d' \mid d$ .

Обозначение:  $d = (f, g)$ .

**ЗАМЕЧАНИЕ.** Из свойств 2 и 4 делимости многочленов следует, что если  $d$  — наибольший общий делитель многочленов  $f$  и  $g$ , то многочлен  $w$  также является наибольшим общим делителем многочленов  $f$  и  $g$  тогда и только тогда, когда  $w = ud$ , где  $u$  — многочлен нулевой степени. Иными словами, наибольший общий делитель определяется с точностью до скаляра из поля  $F$ . Поэтому запись вида  $(f, g) = (u, v)$  ниже означает, что наибольшие делители соответствующих многочленов равны с точностью до ненулевого скаляра.

**Теорема 5.2.2** (алгоритм Евклида). Пусть  $f, g \in F[x]$  и  $g \neq 0$ . Тогда существует наибольший общий делитель этих многочленов  $d = (f, g)$ , и он может быть представлен в виде  $d = fu + gv$ , где  $u, v \in F[x]$ . Более того, если степени  $f$  и  $g$  больше 0, то многочлены  $u$  и  $v$  можно выбрать так, чтобы выполнялось  $\deg u < \deg g$  и  $\deg v < \deg f$ .

**ДОКАЗАТЕЛЬСТВО.** Доказательство теоремы основано на следующем несложном утверждении.

**Лемма.** Пусть  $r$  — остаток от деления  $f$  на  $g$ . Тогда множество общих делителей многочленов  $f$  и  $g$  совпадает с множеством общих делителей многочленов  $g$  и  $r$ . В частности,  $(f, g) = (g, r)$ .

**ДОКАЗАТЕЛЬСТВО ЛЕММЫ.** Если  $h \mid g$  и  $h \mid r$ , то в силу свойств 1 и 2 делимости многочленов  $h$  делит  $f = qg + r$ . Обратно, если  $h \mid f$  и  $h \mid g$ , то  $h \mid r$ , так как  $r = f - qg$ . Таким образом, множества общих делителей совпадают, а значит, совпадают и наибольшие по делимости элементы этих множеств.  $\square$

Вернёмся к доказательству теоремы. Если  $f$  делится на  $g$ , то  $d = g = f \cdot 0 + g \cdot 1$ , и теорема доказана. В противном случае разделим с остатком  $f$  на  $g$ , затем  $g$  — на полученный остаток, затем первый остаток — на второй, и т. д. Поскольку степени остатков убывают, на некотором шаге произойдёт деление без остатка. Получим цепочку равенств:

$$f = q_1g + r_1,$$

$$\begin{aligned}
 g &= q_2 r_1 + r_2, \\
 &\dots\dots\dots \\
 r_{n-2} &= q_n r_{n-1} + r_n, \\
 r_{n-1} &= q_{n+1} r_n,
 \end{aligned}
 \tag{1}$$

где  $r_i \neq 0$  для каждого  $i = 1, \dots, n$ .

Имеем  $r_n = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \dots = (r_1, r_2) = (g, r_1) = (f, g)$ . Таким образом, наибольшим общим делителем многочленов  $f$  и  $g$  оказывается многочлен  $r_n$  — последний ненулевой остаток в этой цепочке.

Проходя по цепочке сверху вниз, мы последовательно получаем, что

$$\begin{aligned}
 r_1 &= f u_1 + g v_1, \\
 r_2 &= f u_2 + g v_2, \\
 &\dots\dots\dots \\
 r_{n-1} &= f u_{n-1} + g v_{n-1} \\
 r_n &= f u_n + g v_n,
 \end{aligned}
 \tag{2}$$

где  $u_i, v_i$  ( $i = 1, \dots, n$ ) — некоторые многочлены из  $F[x]$  (например,  $u_1 = 1, v_1 = -q_1$ ). Таким образом,  $d = r_n$  можно представить в виде суммы  $f u + g v$ .

Пусть в представлении  $d = f u + g v$  степень  $u$  больше или равна степени  $g$ . Поделим с остатком  $u$  на  $g$ :  $u = qg + r$ . Подставляя в исходное равенство, имеем  $d = f(qg + r) + gv = fr + gv'$ . В получившемся новом представлении  $\deg r < \deg g$ . Если  $\deg f \leq \deg v'$ , то  $\deg fr < \deg gv'$ . Кроме того, поскольку в случае, когда  $g$  делит  $f$ , теорема уже доказана, мы можем полагать, что  $\deg d < \deg g \leq \deg gv'$ . С другой стороны,  $gv' = d - fr$ , следовательно,  $\deg gv' = \deg(d - fr) \leq \max\{\deg d, \deg fr\}$ ; противоречие. Таким образом,  $\deg v' < \deg f$ .  $\square$

**ЗАМЕЧАНИЕ.** Практический метод поиска наибольшего общего делителя основан на цепочке равенств (1). Его принято называть *алгоритмом Евклида*. Мы договоримся считать, что старший коэффициент наибольшего общего делителя  $(f, g)$  многочленов  $f$  и  $g$  равен единице. Тогда  $(f, g)$  уже единственным образом определяется по  $f$  и  $g$ .

**Определение 5.2.4.** Многочлены  $f, g \in F[x]$  называются *взаимно простыми*, если  $(f, g) = 1$ .

**Теорема 5.2.3** (критерий взаимной простоты многочленов). *Многочлены  $f, g \in F[x]$  взаимно просты тогда и только тогда, когда существуют многочлены  $u, v \in F[x]$ , такие, что  $1 = fu + gv$ .*

**ДОКАЗАТЕЛЬСТВО.** Если  $(f, g) = 1$ , то  $u, v$ , удовлетворяющие условию, существуют по теореме 5.2.2. Обратно, если существуют многочлены  $u, v$ , такие, что  $1 = fu + gv$ , то любой общий делитель  $d$  многочленов  $f, g$  делит  $fu + gv = 1$ . Следовательно,  $d$  — многочлен нулевой степени.  $\square$

**Предложение 5.2.2** (свойства взаимно простых многочленов). Пусть  $f, g, h \in F[x]$ . Тогда выполняются следующие утверждения.

1. Если  $(f, g) = (f, h) = 1$ , то  $(f, gh) = 1$ .
2. Если  $(f, g) = 1$  и  $f \mid (gh)$ , то  $f \mid h$ .
3. Если  $(f, g) = 1$ ,  $f \mid h$  и  $g \mid h$ , то  $(fg) \mid h$ .

**ДОКАЗАТЕЛЬСТВО.** Докажем первое утверждение. Поскольку  $(f, g) = 1$ , существуют  $a, b \in F[x]$  такие, что  $fa + gb = 1$ . Тогда  $h = h(fa) + h(gb)$ . Кроме того, существуют  $c, d \in F[x]$ , такие, что  $fc + hd = 1$ . Подставим в последнее равенство выражение для  $h$ . Получим  $fc + (hfa + hgb)d = f(c + had) + (gh)cd = 1$ . Полагая  $u = c + ha$  и  $v = cd$ , имеем  $fu + (gh)v = 1$ . Следовательно, по теореме 5.2.3 многочлены  $f$  и  $gh$  взаимно просты.

Второй и третий пункты предложения доказываются схожим образом с использованием критерия взаимной простоты.  $\square$

**УПРАЖНЕНИЕ 5.2.2.** Доказать пп. 2 и 3 предложения 5.2.2.

Аналогия между кольцом многочленов и кольцом целых чисел, которую мы имеем в виду на протяжении этого параграфа, приводит к понятию *неразложимого* многочлена, соответствующего понятию простого числа.

**Определение 5.2.5.** Многочлен  $f \in F[x]$  степени, большей нуля, называется *неразложимым*, если из равенства  $f = uv$ , где  $u, v \in F[x]$ , следует, что либо  $\deg u = 0$ , либо  $\deg v = 0$ . В противном случае многочлен  $f$  *разложим*.

**ЗАМЕЧАНИЕ.** К многочленам нулевой степени понятие разложимости не применяется, так же как в случае кольца целых чисел единица не считается ни простым, ни составным числом. Кроме того, очевидно, что многочлен первой степени всегда неразложим.

**ПРИМЕР.** Многочлен  $x^2 + 1$  неразложим в  $\mathbb{Q}[x]$  и  $\mathbb{R}[x]$ , но разложим в  $\mathbb{C}[x]$ :  $x^2 + 1 = (x + i)(x - i)$ . Многочлен  $x^2 - 2$  неразложим в  $\mathbb{Q}[x]$ , но разложим в  $\mathbb{R}[x]$ :  $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ . Таким образом, ответ на вопрос о разложимости многочлена зависит от того, над каким полем задан многочлен.

**Предложение 5.2.3.** Пусть  $f \in F[x]$  неразложим. Тогда выполняются следующие утверждения.

1. Многочлен  $af$  неразложим тогда и только тогда, когда  $a$  — многочлен нулевой степени.
2. Для каждого  $g \in F[x]$  либо  $f \mid g$ , либо  $(f, g) = 1$ .
3. Если  $g \in F[x]$  таков, что  $g \neq 0$  и  $\deg g < \deg f$ , то  $(f, g) = 1$ .

УПРАЖНЕНИЕ 5.2.3. Доказать предложение 5.2.3.

**Теорема 5.2.4.** Пусть  $f \in F[x]$ ,  $f \neq 0$ . Тогда существуют  $a \in F$  и неразложимые многочлены  $p_1, p_2, \dots, p_r$  со старшими коэффициентами, равными 1, такие, что

$$f = ap_1p_2 \dots p_r. \quad (3)$$

Разложение (3) единственно с точностью до перестановки сомножителей.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $a$  — старший коэффициент многочлена  $f$ . Если  $\deg f = 0$ , то  $f = a$ ,  $r = 0$ , и теорема доказана. Поэтому в дальнейшем мы полагаем, что  $\deg f > 0$ .

Докажем сначала существование разложения (3). Если  $f$  неразложим, то многочлен  $p_1 = \frac{1}{a}f$  тоже неразложим и его старший коэффициент равен 1. Тогда  $f = ap_1$  — искомое разложение.

Допустим, что  $f$  разложим. Воспользуемся индукцией по степени многочлена  $f$ . Поскольку  $f$  разложим, существуют многочлены  $u, v \in F[x]$ , такие, что  $f = uv$  и  $\deg u < \deg f$ ,  $\deg v < \deg f$ . По предположению индукции  $u = bp_1 \dots p_s$ ,  $v = cp_{s+1} \dots p_r$ . Тогда  $f = (bc)p_1 \dots p_r$ .

Нам осталось доказать единственность разложения (3). Пусть  $f = ap_1p_2 \dots p_r = bq_1q_2 \dots q_s$  — два разложения для  $f$ . Очевидно, что  $a = b$ , поскольку оба числа равны старшему коэффициенту многочлена  $f$ . Поскольку кольцо  $F[x]$  не имеет делителей нуля, из равенства  $a(p_1 \dots p_r - q_1 \dots q_s) = 0$  следует равенство  $p_1 \dots p_r = q_1 \dots q_s$ . Пусть для определённости  $r \leq s$ . Мы уже доказали теорему при  $r = 0$ . Поэтому предположим, что  $r > 0$ , и докажем единственность разложения индукцией по  $r$ .

Поскольку  $p_r \mid q_1 \dots q_s$ , найдётся  $j \in \{1, \dots, s\}$ , такое, что  $p_r \mid q_j$ . Переставив при необходимости сомножители, можем считать, что  $p_r \mid q_s$ , т. е.  $q_s = up_r$ . Многочлен  $q_s$  неразложим, а значит, степень  $u$  равна 0. С другой стороны, старшие коэффициенты многочленов  $p_r$  и  $q_s$  равны единице, откуда  $u = 1$  и  $p_r = q_s$ . Следовательно,  $p_r(p_1 \dots p_{r-1} -$

$-q_1 \dots q_{s-1}) = 0$ , откуда  $p_1 \dots p_{r-1} = q_1 \dots q_{s-1}$ , так как  $p_r \neq 0$ . Использование индукционного предположения завершает доказательство теоремы.  $\square$

**ЗАМЕЧАНИЕ.** Доказанная нами теорема — очевидный аналог *основной теоремы арифметики* о разложении целого числа в произведение простых множителей.

### § 5.3. Значения и корни многочленов

**Определение 5.3.1.** Пусть  $f = a_n x^n + \dots + a_1 x + a_0 \in F[x]$ ,  $\alpha \in F$ . Значение многочлена  $f$  в точке  $\alpha$  — это элемент  $f(\alpha) = a_n \alpha^n + \dots + a_1 \alpha + a_0$  поля  $F$ .

**УПРАЖНЕНИЕ 5.3.1.** Пусть  $f, g \in F[x]$ ,  $\alpha \in F$ . Тогда

1.  $(f + g)(\alpha) = f(\alpha) + g(\alpha)$ .
2.  $(fg)(\alpha) = f(\alpha)g(\alpha)$ .

**Определение 5.3.2.** Элемент  $\alpha$  поля  $F$  называется *корнем* многочлена  $f \in F[x]$ , если  $f(\alpha) = 0$ .

**Теорема 5.3.1 (Безу).** Пусть  $f \in F[x]$ ,  $\alpha \in F$ . Значение многочлена  $f$  в точке  $\alpha$  равно остатку от деления  $f$  на  $x - \alpha$ . В частности, элемент  $\alpha$  — корень многочлена  $f$  тогда и только тогда, когда  $(x - \alpha) \mid f$ .

**ДОКАЗАТЕЛЬСТВО.** Разделим многочлен  $f$  с остатком на  $x - \alpha$ . Имеем  $f = q(x - \alpha) + r$ , где  $r = 0$  или  $\deg r = 0$ . Поскольку стоящие в левой и правой части равенства многочлены равны, равны и их значения в точке  $\alpha$ . Поэтому  $f(\alpha) = r$ . Отсюда следует утверждение теоремы.  $\square$

#### Теорема 5.3.2.

1. Нулевой многочлен  $f \in F[x]$  степени  $n$  имеет не более  $n$  корней.

2. Пусть для  $i = 1, \dots, n$  заданы элементы  $\alpha_i \in F$ , причём  $\alpha_i \neq \alpha_j$ , если  $i \neq j$ . Пусть  $f, g \in F[x]$ , степени многочленов  $f, g$  меньше  $n$  и  $f(\alpha_i) = g(\alpha_i)$  для каждого  $i = 1, \dots, n$ . Тогда  $f = g$ .

3. Пусть для  $i = 1, \dots, n$  заданы элементы  $\alpha_i, \beta_i \in F$ , причём  $\alpha_i \neq \alpha_j$ , если  $i \neq j$ . Тогда существует и единствен многочлен  $f$  степени меньше  $n$ , такой, что для каждого  $i = 1, \dots, n$  выполняется  $f(\alpha_i) =$

$\beta_i$ . Многочлен  $f$  определяется формулой

$$f(x) = \sum_{i=1}^n \beta_i \frac{(x - \alpha_1) \dots (x - \alpha_{i-1})(x - \alpha_{i+1}) \dots (x - \alpha_n)}{(\alpha_i - \alpha_1) \dots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \dots (\alpha_i - \alpha_n)}. \quad (1)$$

ЗАМЕЧАНИЕ. Многочлен, определённый формулой (1), называется *интерполяционным многочленом Лагранжа*.

ДОКАЗАТЕЛЬСТВО. 1. Пусть  $\alpha_1, \dots, \alpha_s$  — различные корни многочлена  $f$ . Заметим, что при  $i \neq j$  выполняется  $(x - \alpha_i, x - \alpha_j) = 1$ . Действительно, оба многочлена неразложимы, поскольку они первой степени. Если бы их наибольший общий делитель имел ненулевую степень, то он равнялся бы каждому из этих многочленов. Следовательно, они были бы равны между собой, что невозможно. Из предложения о свойствах взаимно простых многочленов вытекает, что  $g = (x - \alpha_1) \dots (x - \alpha_s) \mid f$ . А значит, число  $s = \deg g$  различных корней многочлена  $f$  не превосходит  $n = \deg f$ .

2. Положим  $h = f - g$ . Тогда  $\deg h \leq \max\{\deg f, \deg g\} < n$  и  $h(\alpha_i) = f(\alpha_i) - g(\alpha_i) = 0$  для каждого  $i = 1, \dots, n$ . Если  $h \neq 0$ , то получаем противоречие с п. 1 теоремы.

3. Подставляя элементы  $\alpha_i$  в формулу (1), получаем  $f(\alpha_i) = \beta_i$  для  $i = 1, \dots, n$ . Единственность многочлена  $f$  следует из п. 2 теоремы.  $\square$

ЗАМЕЧАНИЕ. Если поле  $F$  бесконечно, то, как показывает утверждение п. 2 теоремы, абстрактное определение многочлена  $f$  над полем  $F$  (определение 5.1.1) совпадает с определением  $f$  как отображения. Иными словами, многочлены  $f, g \in F[x]$  равны тогда и только тогда, когда для любого  $\alpha \in F$  выполняется  $f(\alpha) = g(\alpha)$ .

УПРАЖНЕНИЕ 5.3.2. Используя формулу (1), найти многочлен, принимающий в точках 1, 2, 3 значения 1, 4, 9 соответственно.

Если  $\alpha$  — корень многочлена  $f$ , то  $f$  может делиться не только на  $x - \alpha$ , но и на некоторую большую степень  $x - \alpha$ . В этом случае  $\alpha$  принято называть *кратным корнем*. Сформулируем это более точно.

**Определение 5.3.3.** Пусть  $f \in F[x]$ ,  $r \in \mathbb{N}_0$ . Элемент  $\alpha$  поля  $F$  называется корнем многочлена  $f$  *кратности*  $r$ , если  $(x - \alpha)^r \mid f$  и  $(x - \alpha)^{r+1} \nmid f$ . Корень кратности 1 будем называть *простым* корнем, а корень, кратность которого больше 1, — *кратным* корнем многочлена  $f$ .

ЗАМЕЧАНИЕ. Корень кратности 0, очевидно, корнем многочлена не является.

В ситуации, когда  $\alpha$  — корень кратности  $r$ , полезно бывает считать, что многочлен  $f$  имеет  $r$  корней, равных  $\alpha$ . В этом случае мы будем говорить, что рассматриваем корни многочлена *с учётом их кратности*.

**Теорема 5.3.3.** *Нулевой многочлен  $f \in F[x]$  степени  $n$  имеет не более  $n$  корней с учётом их кратности. Кроме того,  $f$  имеет ровно  $n$  корней тогда и только тогда, когда он разлагается над  $F$  на линейные множители, т. е.  $f = a(x - \alpha_1)^{r_1} \dots (x - \alpha_s)^{r_s}$ , где  $a, \alpha_i \in F$  и  $\sum_{i=1}^s r_i = n$ .*

**ДОКАЗАТЕЛЬСТВО.** Доказательство практически аналогично доказательству п. 1 теоремы 5.3.2. Пусть  $\alpha_1, \dots, \alpha_s$  — различные корни многочлена  $f$  и их кратности равны  $r_1, \dots, r_s$  соответственно. Покажем, что  $((x - \alpha_i)^{r_i}, (x - \alpha_j)^{r_j}) = 1$  при  $i \neq j$ . Действительно, из единственности разложения многочлена в произведение неразложимых (теорема 5.2.4) следует, что если многочлен  $d$  делит многочлен  $(x - \alpha)^m$ , то  $d = c(x - \alpha)^k$ , где  $c \in F$  и  $0 \leq k \leq m$ . Поэтому наибольший общий делитель многочленов  $(x - \alpha_i)^{r_i}$  и  $(x - \alpha_j)^{r_j}$  должен одновременно иметь вид  $(x - \alpha_i)^{k_i}$  и  $(x - \alpha_j)^{k_j}$ , что по той же теореме о разложении в произведение неразложимых возможно, только если  $d$  — многочлен нулевой степени.

Таким образом, многочлен  $g = (x - \alpha_1)^{r_1} \dots (x - \alpha_s)^{r_s}$  делит многочлен  $f$ . Поэтому  $\deg g \leq \deg f$ . Последнее утверждение теоремы следует из того, что в данном случае равносильны равенства  $\deg g = \deg f$  и  $f = ag$ , где  $a$  — многочлен нулевой степени, т. е. ненулевой скаляр.  $\square$

Кратность корня многочлена можно интерпретировать также с помощью понятия производной. Ясно, что аналитическое определение производной может не иметь смысла в случае произвольного поля. Поэтому мы дадим следующее абстрактное определение.

**Определение 5.3.4.** Пусть  $f(x) = \sum_{k=0}^n a_k x^k$  — многочлен степени  $n$  над полем  $F$ . Многочлен  $f'$ , определённый по правилу

$$f'(x) = \sum_{k=1}^n k a_k x^{k-1},$$

называется *производной* многочлена  $f$ .

**ЗАМЕЧАНИЕ.** В определении производной предполагается, что  $ka$ , где  $k \in \mathbb{N}$  и  $a \in F$ , — это элемент поля  $F$ , равный сумме  $k$  элементов  $a$  поля  $F$ .

**УПРАЖНЕНИЕ 5.3.3.** Пусть  $f, g \in F[x]$ ,  $\alpha, \beta \in F$ ,  $k \in \mathbb{N}$ . По определению производной доказать следующие утверждения.

1.  $(\alpha f + \beta g)' = \alpha f' + \beta g'$ .
2.  $(fg)' = f'g + fg'$ .
3.  $(\alpha(x - \beta)^k)' = k\alpha(x - \beta)^{k-1}$ .

**Определение 5.3.5.** Пусть  $f \in F[x]$ . Если  $k$  — натуральное число и  $f^{(0)} = f$ , то  $k$ -я производная многочлена  $f$  определяется по индукции:  $f^{(k)} = (f^{(k-1)})'$ .

Отметим, что над произвольным полем некоторые очевидные с аналитической точки зрения свойства производной могут не выполняться. Например, если мы рассмотрим полином  $f(x) = x^2$  над полем  $F = \mathbb{Z}_2$ , то обнаружим, что его производная  $f'(x) = 2x = 0x = 0$ . Ниже мы ограничимся рассмотрением только тех полей, в которых  $ka \neq 0$  для любого натурального числа  $k$  и ненулевого скаляра  $a \in F$ . Иными словами, полями *нулевой характеристики*. Приведём точное определение характеристики поля.

**Определение 5.3.6.** Пусть  $F$  — поле. Наименьшее натуральное число  $p$ , такое, что  $p1 = 0$  (сумма  $p$  единиц поля равна 0), если оно существует, называется *характеристикой* поля  $F$ . Если такого числа нет, то *характеристика* поля  $F$  по определению равна 0. Характеристика поля обозначается как  $\text{char } F$ .

**ПРИМЕР.** Поле  $\mathbb{Z}_2$  имеет характеристику 2. Числовые поля  $\mathbb{Q}$ ,  $\mathbb{R}$  и  $\mathbb{C}$  имеют нулевую характеристику.

**УПРАЖНЕНИЕ 5.3.4.** Если  $p$  — ненулевая характеристика некоторого поля, то  $p$  — простое число.

*Указание.* Использовать тот факт, что в поле нет делителей нуля.

**УПРАЖНЕНИЕ 5.3.5.** Если  $\text{char } F = 0$ ,  $a \in F$  и  $k \in \mathbb{N}$ , то  $ka = 0$  тогда и только тогда, когда  $a = 0$ . В частности, для любого  $b \in F$  и  $k \in \mathbb{N}$  определён элемент  $b/k = b \cdot (k1)^{-1}$  поля  $F$ .

Сделав в многочлене  $f(x) = a_0 + a_1x + \dots + a_nx^n$  замену  $x = y + \alpha$ , мы получим новый многочлен (той же степени) от переменной  $y = x - \alpha$ . Фактически, мы получим представление

$$f(x) = b_0 + b_1(x - \alpha) + \dots + b_n(x - \alpha)^n, \quad (2)$$

которое называется *разложением  $f$  по степеням  $x - \alpha$* .

**Теорема 5.3.4** (формула Тейлора). Пусть  $\text{char } F = 0$ ,  $\alpha \in F$ ,  $f \in F[x]$  и  $\deg f = n$ . Разложение многочлена  $f$  по степеням  $x - \alpha$



определяется формулой

$$f(x) = \sum_{k=0}^n \frac{f^{(k)}(\alpha)}{k!} (x - \alpha)^k. \quad (3)$$

Эта формула называется формулой Тейлора для многочленов.

**ДОКАЗАТЕЛЬСТВО.** Продифференцируем равенство (2)  $k$  раз и подставим  $x = \alpha$ . Тогда  $f^{(k)}(\alpha) = k!b_k$ . Отсюда и следует формула (3).  $\square$

**Следствие** (о кратных корнях многочлена). Пусть  $\text{char } F = 0$ ,  $f \in F[x]$  и  $r \in \mathbb{N}$ . Тогда выполняются следующие утверждения.

1. Элемент  $\alpha$  поля  $F$  — корень кратности  $r$  многочлена  $f$  тогда и только тогда, когда  $f^{(k)}(\alpha) = 0$  для всех  $k = 0, \dots, r-1$  и  $f^{(r)}(\alpha) \neq 0$ . В частности,  $\alpha$  — корень кратности  $r-1$  производной  $f'$  многочлена  $f$ .

2. Множество корней многочлена  $f$  совпадает с множеством корней многочлена  $g = \frac{f}{(f, f')}$ , и все корни многочлена  $g$  простые. В частности, многочлен  $f$  не имеет кратных корней тогда и только тогда, когда  $(f, f') = 1$ .

**ЗАМЕЧАНИЕ.** В п. 1 подразумевается, что если  $\alpha$  — простой корень многочлена  $f$  ( $r = 1$ ), то  $\alpha$  не является корнем его производной  $f'$  ( $\alpha$  — корень нулевой кратности для  $f'$ ).

**ДОКАЗАТЕЛЬСТВО.** 1. Кратность корня  $\alpha$  многочлена  $f$ , очевидно, равна номеру первого отличного от нуля коэффициента в разложении (2). Поэтому утверждение следует из формулы Тейлора.

2. Если  $\alpha$  — корень  $f$  кратности  $r$ , то  $(x - \alpha)^{r-1} \mid (f, f')$  и  $(x - \alpha)^r \nmid (f, f')$ . Следовательно,  $\alpha$  — простой корень многочлена  $g$ . С другой стороны, поскольку  $f = g(f, f')$ , то любой корень многочлена  $g$  будет и корнем многочлена  $f$ .  $\square$

**УПРАЖНЕНИЕ 5.3.6.** Для многочлена  $f(x) = x^5 - 3x^4 - 6x^3 + 10x^2 + 21x + 9$  найти многочлен  $g = \frac{f}{(f, f')}$  и решить уравнение  $f(x) = 0$ .

В случае, когда поле имеет ненулевую характеристику, утверждение следствия о кратных корнях может не выполняться. Тем не менее, можно доказать его ослабленную версию.

**УПРАЖНЕНИЕ 5.3.7.** Доказать следующее утверждение. Если  $F$  — произвольное поле,  $f$  — многочлен из  $F[x]$  и  $\alpha$  — его корень кратности  $r$ , то для каждого  $i \in \{0, 1, \dots, r-1\}$  выполняется  $f^{(i)}(\alpha) = 0$ . В частности, если  $(f, f') = 1$ , то  $f$  не имеет кратных корней.

Последнее утверждение в этом параграфе — теорема о существовании так называемого многочлена Лагранжа — Сильвестра. Этот мно-

гочлен не только имеет фиксированные значения в данных точках, но и фиксированные значения своих последовательных производных в тех же точках. Он понадобится нам в шестой главе.

**Теорема 5.3.5.** Пусть  $\text{char } F = 0$ ,  $s \in \mathbb{N}$  и для каждого  $i = 1, \dots, s$  заданы числа  $r_i \in \mathbb{N}_0$  и элементы  $\alpha_i, \beta_{i0}, \dots, \beta_{ir_i} \in F$ , причём  $\alpha_m \neq \alpha_k$  при  $m \neq k$ . Тогда существует единственный многочлен  $f$  степени меньше, чем  $\sum_{i=1}^s (r_i + 1)$ , такой, что для каждого  $i = 1, \dots, s$  и каждого  $j = 0, \dots, r_i$  выполняется  $f^{(j)}(\alpha_i) = \beta_{ij}$ .

**ДОКАЗАТЕЛЬСТВО.** Будем искать многочлен  $f$  в виде  $f = \sum_{i=1}^s f_i$ , где  $f_i = d_i g_i$  и  $d_i, g_i \in F[x]$  для каждого  $i = 1, \dots, s$ . При этом  $d_i(x) = \prod_{k \neq i} (x - \alpha_k)^{r_k + 1}$ , а  $g_i$  подбираются, исходя из следующей леммы.

**Лемма.** Пусть даны  $\alpha, \beta_0, \dots, \beta_r \in F$  и  $d \in F[x]$ , такие, что  $d(\alpha) \neq 0$ . Тогда существует многочлен  $g$  степени, не превосходящей  $r$ , такой, что  $(dg)^{(j)}(\alpha) = \beta_j$  для всех  $j = 0, \dots, r$ .

**ДОКАЗАТЕЛЬСТВО ЛЕММЫ.** Сначала докажем, что для любого многочлена  $u \in F[x]$  и каждого  $t = 1, \dots, n$ , где  $n \in \mathbb{N}$ , найдётся многочлен  $v \in F[x]$ , такой, что

$$(u(x - \alpha)^n)^{(t)} = \frac{n!}{(n - t)!} u(x - \alpha)^{n-t} + v(x - \alpha)^{n-t+1}. \quad (4)$$

Доказательство формулы (4) проводится индукцией по  $t$ . При  $t = 1$  имеем

$$(u(x - \alpha)^n)' = n(x - \alpha)^{n-1}u + u'(x - \alpha)^n$$

и, полагая  $v = u'$ , получаем требуемое.

По предположению индукции существует многочлен  $v_1$ , такой, что

$$(u(x - \alpha)^n)^{(t-1)} = \frac{n!}{(n - t + 1)!} u(x - \alpha)^{n-t+1} + v_1(x - \alpha)^{n-t+2}.$$

Следовательно,

$$\begin{aligned} (u(x - \alpha)^n)^{(t)} &= \left( \frac{n!}{(n - t + 1)!} u(x - \alpha)^{n-t+1} \right)' + (v_1(x - \alpha)^{n-t+2})' = \\ &= \frac{n!}{(n - t)!} u(x - \alpha)^{n-t} + v(x - \alpha)^{n-t+1}, \end{aligned}$$

что и требовалось.

Утверждение леммы мы докажем индукцией по  $r$ . При  $r = 0$  искомым скаляр  $g$  (в данном случае степень  $g$  не должна превосходить 0) находится из равенства  $(dg)(\alpha) = \beta_0$ . Действительно, если  $g = \frac{\beta_0}{d(\alpha)}$ , то  $gd(\alpha) = g(\alpha)d(\alpha) = (dg)(\alpha) = \beta_0$ .

Пусть  $r > 0$  и для чисел, меньших  $r$ , утверждение леммы доказано. Иными словами, существует многочлен  $h$  степени, меньшей  $r$ , такой, что для каждого  $j = 0, \dots, r-1$  выполняется  $(dh)^{(j)}(\alpha) = \beta_j$ . Тогда для любого  $\gamma \in F$  многочлен  $g = h + \gamma(x - \alpha)^r$  удовлетворяет условию  $(dg)^{(j)}(\alpha) = \beta_j$  при  $j = 0, \dots, r-1$ . Действительно,

$$(dg)^{(j)} = (dh)^{(j)} + (d\gamma(x - \alpha)^r)^{(j)} = (dh)^{(j)} + (x - \alpha)w \quad (\text{см. формулу (4)}).$$

Поэтому  $(dg)^{(j)}(\alpha) = (dh)^{(j)}(\alpha) + 0 = \beta_j$  при  $j < r$ . Осталось подобрать  $\gamma$  так, чтобы  $(dg)^{(r)} = \beta_r$ . Имеем

$$(dg)^{(r)} = (dh)^{(r)} + (d\gamma(x - \alpha)^r)^{(r)} = (dh)^{(r)} + d\gamma r!(x - \alpha)^0 + v(x - \alpha).$$

Выражая  $\gamma$  из равенства

$$(dg)^{(r)}(\alpha) = (dh)^{(r)}(\alpha) + d(\alpha)\gamma r! = \beta_r,$$

получаем, что при

$$\gamma = \frac{\beta_r - (dh)^{(r)}(\alpha)}{d(\alpha)r!}$$

выполняется последнее необходимое равенство  $(dg)^{(r)}(\alpha) = \beta_r$ . Отметим, что  $\gamma$  находится всегда, поскольку  $r! \neq 0$  в силу того, что  $\text{char } F = 0$ , а  $d(\alpha) \neq 0$  по условию.  $\square$

Вернёмся к доказательству теоремы. Введённые нами многочлены  $d_i$  обладают тем свойством, что  $d_i(\alpha_i) \neq 0$  для каждого  $i = 1, \dots, s$ . Следовательно, для каждого из них в силу утверждения леммы найдётся многочлен  $g_i$  степени, не превосходящей  $r_i$ , такой, что  $f_i^{(j)}(\alpha_i) = (d_i g_i)^{(j)}(\alpha_i) = \beta_{ij}$ , где  $i = 1, \dots, s$ , а  $j = 0, \dots, r_i$ .

Поскольку  $(x - \alpha_i)^{r_i+1} \mid d_k$  при  $k \neq i$ , имеем  $f_k^{(j)}(\alpha_i) = 0$  для всех  $k \neq i$  и всех  $j = 0, \dots, r_i$ . Таким образом, для всех  $i = 1, \dots, s$  и всех  $j = 0, \dots, r_i$  выполняется

$$f^{(j)}(\alpha_i) = \sum_{k=1}^s f_k^{(j)}(\alpha_i) = f_i^{(j)}(\alpha_i) = \beta_{ij}.$$

Далее,

$$\deg f \leq \max_{i=1, \dots, s} \{\deg f_i\} < \sum_{i=1}^s (r_i + 1).$$

Пусть  $g$  — многочлен, удовлетворяющий условию теоремы, и  $g \neq f$ . Положим  $h = f - g$ . Тогда  $h^{(j)}(\alpha_i) = 0$  для  $i = 1, \dots, s$  и  $j = 0, \dots, r_i$ . По следствию теоремы 5.3.4 о кратных корнях имеем  $\prod_{i=1}^s (x - \alpha_i)^{r_i+1} \mid h$ . Следовательно,  $\deg h \geq \sum_{i=1}^s (r_i + 1)$ ; противоречие.  $\square$

**УПРАЖНЕНИЕ 5.3.8.** *Используя в качестве руководства доказательство теоремы, построить интерполяционный многочлен Лагранжа — Сильвестра  $f$ , удовлетворяющий следующим условиям:  $f(1) = 1$ ,  $f'(1) = 2$ ,  $f(2) = 4$ .*

## § 5.4. Симметрические многочлены

В этом параграфе речь пойдёт о многочленах от нескольких переменных. Хотя для них, так же как и в случае многочленов от одной переменной, существует содержательная теория, мы затронем в этих лекциях лишь один важный факт, относящийся к многочленам специального вида, так называемым *симметрическим многочленам*. Начнём с того, что дадим общее определение многочленов от нескольких переменных, используя доказанные нами свойства кольца многочленов от одной переменной и индукцию, базисом которой является определение кольца многочленов от одной переменной.

**Определение 5.4.1.** Пусть  $n$  — натуральное число, большее 1,  $R$  — кольцо и уже определено кольцо  $R[x_1, \dots, x_{n-1}]$  многочленов над  $R$  от  $n - 1$  переменной. *Кольцом многочленов над  $R$  от  $n$  переменных* называется кольцо  $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$ , т. е. кольцо многочленов от переменной  $x_n$  над кольцом  $R[x_1, \dots, x_{n-1}]$ .

**ЗАМЕЧАНИЕ.** Корректность определения множества  $R[x_1, \dots, x_n]$  как кольца следует из теоремы 5.1.1. Кроме того, из той же теоремы сразу следует, что свойства коммутативности или существования единицы в кольце  $R$  влекут те же свойства кольца  $R[x_1, \dots, x_n]$ .

**Определение 5.4.2.** Многочлен вида  $ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ , где  $a \in R$ , называется *одночленом* (или *мономом*). Элемент  $a$  будем называть *коэффициентом* одночлена,  $n$ -ку  $(k_1, k_2, \dots, k_n)$  — *степенью* одночлена, число  $k_i$  — *степенью* одночлена по переменной  $x_i$ , а сумму  $k_1 + k_2 + \dots + k_n$  — его *степенью по совокупности переменных*.

В дальнейшем мы будем рассматривать многочлены над полем  $F$ .

Анализ определения показывает, что многочлен  $f \in F[x_1, \dots, x_n]$  имеет вид

$$f(x_1, x_2, \dots, x_n) = \sum_{k_1, k_2, \dots, k_n} a_{k_1 k_2 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}, \quad (1)$$

где суммирование происходит по упорядоченным наборам  $k_1, k_2, \dots, k_n$  неотрицательных целых чисел, элементы  $a_{k_1 k_2 \dots k_n} \in F$  и лишь конечное их число отлично от нуля. Два многочлена равны, если для каждого набора индексов  $(k_1, k_2, \dots, k_n)$  их коэффициенты совпадают. Таким образом, каждый многочлен от  $n$  переменных можно считать суммой конечного числа одночленов. Мы будем упорядочивать одночлены с ненулевыми коэффициентами, составляющие многочлен, лексикографически упорядочивая их степени. Степень  $(k_1, k_2, \dots, k_n)$  и соответствующий ей одночлен *старше*, чем степень  $(l_1, l_2, \dots, l_n)$  и соответствующий ей одночлен, если найдётся  $i \in \{1, 2, \dots, n\}$ , такое, что  $k_1 = l_1, \dots, k_{i-1} = l_{i-1}$  и  $k_i > l_i$ . Если  $u, v$  — одночлены, мы будем обозначать через  $u \succ v$  тот факт, что  $u$  старше  $v$ . *Степенью многочлена* мы будем называть старшую степень его одночленов.

**ПРИМЕР.** Следующий многочлен упорядочен по убыванию степеней его одночленов:

$$x_1^2 x_2 - 2x_1 x_2 x_3 + 3x_1 x_3^3 - 2x_2^2 x_3 + 1.$$

Отметим, что одночлен  $3x_1 x_3^3$  младше, чем старший одночлен  $x_1^2 x_2$ , а также одночлен  $-2x_1 x_2 x_3$ , хотя его степень по совокупности переменных больше соответствующих степеней двух последних одночленов.

Несложно проверить следующие свойства лексикографического упорядочения одночленов над полем  $F$ .

**Предложение 5.4.1.** Пусть  $F$  — поле,  $u, v, w, z$  — одночлены из  $F[x_1, \dots, x_n]$ . Тогда выполняются следующие утверждения.

1. Если  $u \succ v, v \succ w$ , то  $u \succ w$ .
2. Если  $u \succ v$  и  $w \neq 0$ , то  $uw \succ vw$ .
3. Если  $u \succ v, w \succ z$ , то  $uw \succ vz$ .

**УПРАЖНЕНИЕ 5.4.1.** Доказать предложение 5.4.1.

**Следствие.** Старший одночлен произведения многочленов из кольца  $F[x_1, \dots, x_n]$  равен произведению старших одночленов сомножителей. В частности, кольцо  $F[x_1, \dots, x_n]$  не имеет делителей нуля.

**Определение 5.4.3.** Многочлен  $f \in F[x_1, x_2, \dots, x_n]$  называется *симметрическим*, если для любой подстановки  $\sigma \in S_n$  выполняется равенство  $f(x_1, x_2, \dots, x_n) = f(x_{1\sigma}, x_{2\sigma}, \dots, x_{n\sigma})$ , т. е. многочлен  $f$  не меняется при любой перестановке переменных.

ПРИМЕРЫ. 1. Многочлены

$$s_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k}, \quad (2)$$

где  $k = 1, 2, \dots, n$ , являются симметрическими. Они называются *элементарными симметрическими многочленами*.

2. Многочлен  $x_1^m + x_2^m + \dots + x_n^m$  является симметрическим при любом натуральном  $m$ .

3. Всякий многочлен нулевой степени по совокупности переменных является симметрическим.

4. Многочлен  $3x_1x_2 + 3x_1x_3$  не является симметрическим, поскольку подстановка переменных  $\sigma = (1, 2) \in S_3$  переводит его в многочлен  $3x_1x_2 + 3x_2x_3$ .

**Предложение 5.4.2.** Сумма и произведение двух симметрических многочленов — симметрические многочлены. Множество всех симметрических многочленов от  $n$  переменных образует подкольцо кольца  $F[x_1, \dots, x_n]$ . Если  $g \in F[y_1, \dots, y_m]$  и  $p_1, \dots, p_m$  — симметрические многочлены от переменных  $x_1, \dots, x_n$ , то  $g(p_1, \dots, p_m)$  — симметрический многочлен от переменных  $x_1, \dots, x_n$ .

УПРАЖНЕНИЕ 5.4.2. Доказать предложение 5.4.2.

Мы готовы сформулировать основной результат этого параграфа.

**Теорема 5.4.1** (основная теорема о симметрических многочленах).

Пусть  $f \in F[x_1, \dots, x_n]$  — симметрический многочлен. Тогда существует многочлен  $g \in F[y_1, \dots, y_n]$ , такой, что  $f(x_1, \dots, x_n) = g(s_1, \dots, s_n)$ , где  $s_k$  — элементарные симметрические многочлены от переменных  $x_1, \dots, x_n$  над полем  $F$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $u = ax_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$  — старший одночлен многочлена  $f$ . Сначала мы докажем, что для его степени выполняются неравенства  $k_1 \geq k_2 \geq \dots \geq k_n$ . Иначе рассмотрим наименьшее число  $i$  такое, что  $k_i < k_{i+1}$ . Транспозиция  $\sigma = (i, i+1)$  переводит одночлен  $u = ax_1^{k_1} \dots x_i^{k_i} x_{i+1}^{k_{i+1}} \dots x_n^{k_n}$  в одночлен  $v = ax_1^{k_1} \dots x_i^{k_{i+1}} x_{i+1}^{k_i} \dots x_n^{k_n}$ , степень которого по нашему предположению старше степени  $v$ . С дру-

гой стороны, поскольку  $f$  симметрический, он должен содержать одночлен  $v$ , что противоречит выбору  $u$  в качестве старшего одночлена.

Если  $f$  — многочлен нулевой степени, т.е. многочлен степени  $(0, \dots, 0)$ , то утверждение теоремы очевидно. Поскольку существует только конечное число степеней  $(l_1, \dots, l_n)$ , удовлетворяющих неравенству  $l_1 \geq l_2 \geq \dots \geq l_n$  и младших, чем старшая степень  $(k_1, \dots, k_n)$  многочлена  $f$ , можно использовать индукцию по степени  $f$ . Таким образом, мы можем считать, что для всех многочленов, младших многочлена  $f$ , утверждение теоремы уже доказано.

Рассмотрим многочлен  $h = as_1^{k_1-k_2} \dots s_{n-1}^{k_{n-1}-k_n} s_n^{k_n}$ . Поскольку многочлены  $s_k$  симметрические, в силу предложения 5.4.2 сам  $h$  — симметрический многочлен от переменных  $x_1, \dots, x_n$ . Пусть  $v$  — старший одночлен многочлена  $h$ . Для каждого  $i \in \{1, 2, \dots, n\}$  степень  $v$  по переменной  $x_i$  равна  $k_i$ , так как  $x_i$  входит в старшие одночлены элементарных симметрических многочленов  $s_i, \dots, s_n$  по одному разу и не входит в старшие одночлены многочленов  $s_1, \dots, s_{i-1}$ . Следовательно, старший одночлен  $v$  многочлена  $h$  совпадает с  $u$ , старшим одночленом многочлена  $f$ . Поэтому многочлен  $f_1 = f - h$  является симметрическим многочленом, степень которого младше степени  $f$ . По предположению индукции существует многочлен  $g_1$  из  $F[y_1, \dots, y_n]$ , такой, что  $f_1(x_1, \dots, x_n) = g_1(s_1, \dots, s_n)$ . Значит, многочлен  $g = ay_1^{k_1-k_2} \dots y_{n-1}^{k_{n-1}-k_n} y_n^{k_n} + g_1(y_1, \dots, y_n)$  является искомым.  $\square$

**ЗАМЕЧАНИЕ.** Доказательство теоремы можно использовать для выражения любого симметрического многочлена через элементарные симметрические многочлены.

**УПРАЖНЕНИЕ 5.4.3.** Доказать, что  $x_1^2 + \dots + x_n^2 = s_1^2 - 2s_2$  и  $x_1^3 + \dots + x_n^3 = s_1^3 - 3s_1s_2 + 3s_3$ .

## § 5.5. Алгебраическая замкнутость поля комплексных чисел

Результаты предыдущих параграфов ничего не говорят о существовании у многочлена хотя бы одного корня. Более того, как показывают несложные примеры, существуют многочлены, не имеющие корней в поле, над которым они заданы. Так, многочлен  $f(x) = x^2 - 2 \in \mathbb{Q}[x]$  не имеет рациональных корней, а многочлен  $g = x^2 + 1$  не имеет корней даже в  $\mathbb{R}$ . Тем не менее  $f$  имеет корни в  $\mathbb{R}$ , а  $g$  — в  $\mathbb{C}$ , т.е. в полях, которые содержат поля коэффициентов многочлена в качестве подполя. Иными словами, в *расширениях* полей коэффициентов.

**Определение 5.5.1.** Поле  $K$  называется *расширением* поля  $F$ , если  $F$  — подполе поля  $K$ , т.е.  $F$  — подмножество в  $K$  и операции, заданные на  $F$ , являются сужениями на  $F$  соответствующих операций, заданных на  $K$ .

Оказывается, что отмеченное нами свойство многочленов  $x^2 - 2$  и  $x^2 + 1$ , которые имеют корни в расширении поля своих коэффициентов, носит универсальный характер.

**Теорема 5.5.1.** Пусть  $F$  — поле, многочлен  $f \in F[x]$  и  $\deg f > 0$ . Тогда существует расширение  $K$  поля  $F$ , такое, что для некоторого элемента  $\alpha \in K$  выполняется  $f(\alpha) = 0$ .

**ЗАМЕЧАНИЕ.** Выражение  $f(\alpha)$  в формулировке теоремы имеет смысл, поскольку коэффициенты многочлена  $f$ , лежащие в  $F$ , лежат и в расширении  $K$  этого поля. Кроме того, операции сложения и умножения на скаляр (коэффициент) можно рассматривать как операции в поле  $K$ . Иными словами, если  $K$  — расширение поля  $F$  и  $f \in F[x]$ , то всегда можно считать, что  $f$  задан и над  $K$ . Таким образом,  $f(\alpha)$  — это значение многочлена  $f$  в точке  $\alpha$ , где  $f \in K[x]$ .

**ДОКАЗАТЕЛЬСТВО.** По теореме 5.2.4 многочлен  $f$  разлагается над  $F$  в произведение неразложимых многочленов со старшими коэффициентами, равными единице:  $f = ap_1p_2 \dots p_s$ . Если  $\alpha$  — корень многочлена  $p_1$  в расширении  $K$  поля  $F$ , то  $f(\alpha) = ap_1(\alpha) \dots p_s(\alpha) = 0$ , и поле  $K$  и его элемент  $\alpha$  — искомые. Таким образом, можно считать, что многочлен  $f$  неразложим над  $F$  и его старший коэффициент равен 1. Пусть  $\deg f = n$  и

$$f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n. \quad (1)$$

Заметим, что можно считать, что  $\deg f > 1$ . Иначе  $f = a_0 + x$ ,  $-a_0$  — корень многочлена  $f$  в поле  $F$ , и мы полагаем, что  $K = F$ .

Теперь мы явным образом построим поле, которое удовлетворяет условиям теоремы. Обозначим через  $K$  множество многочленов над  $F$  от переменной  $t$ , степень которых строго меньше  $n$ . Иными словами,

$$K = \{g(t) \in F[t] \mid \deg g < \deg f\}.$$

Определим на  $K$  операции сложения и умножения, которые мы обозначим через  $+$  и  $\circ$ , следующим образом. Сложение  $+$  — это обычное сложение многочленов. А результат умножения  $\circ$  для многочленов  $g, h \in K$  — это остаток от деления обычного произведения многочленов  $g(t)h(t)$  на многочлен  $f(t)$ , т.е.  $g \circ h = r$ , где  $r$  удовлетворяет условиям  $gh = fq + r$  и  $\deg r < \deg f$ . Отметим, что  $K$  замкнуто относительно определённых нами операций. Действительно,  $\deg(g + h) \leq$



$\max\{\deg g, \deg h\} < \deg f$  и  $\deg r < \deg f$  по теореме о делении с остатком. Кроме того, по той же теореме остаток  $r$  определяется однозначно, поэтому предложенная нами операция умножения корректно определена на  $K$ .

Проверим, что  $K$  — поле относительно введённых нами операций.

Тот факт, что  $\langle K, + \rangle$  — абелева группа, очевиден, поскольку сложение многочленов обладает всеми необходимыми свойствами.

Проверим аксиому правой дистрибутивности. Пусть  $g, h, u \in K$  и  $gu = fq_1 + r_1$ ,  $hu = fq_2 + r_2$  и  $(g+h)u = fq + r$ . Тогда  $g \circ u + h \circ u = r_1 + r_2$ , а  $(g+h) \circ u = r$ . С другой стороны,  $F[t]$  — кольцо. Следовательно, для многочленов  $g, h, u \in F[t]$  выполняется  $gu + hu = (g+h)u$ . Поэтому, если мы обозначим многочлен  $(g+h)u$  через  $w$ , то  $w = f(q_1 + q_2) + (r_1 + r_2) = fq + r$ . В силу теоремы о делении с остатком имеем  $r_1 + r_2 = r$ , а значит,  $g \circ u + h \circ u = (g+h) \circ u$ . Закон левой дистрибутивности проверяется аналогично.

Доказательство ассоциативности умножения в  $K$  проводится схожим образом и основано на ассоциативности умножения многочленов в кольце  $F[t]$ . Коммутативность умножения следует из определения операции  $\circ$ . Единицей в  $K$ , как и в кольце  $F[t]$ , является многочлен нулевой степени, равный единице поля  $F$ . Таким образом, нам осталось для каждого ненулевого элемента из  $K$  указать обратный к нему элемент.

Пусть  $g(t) \in K$  и  $g(t) \neq 0$ . Поскольку  $f(t)$  неразложим над  $F$  и  $\deg g < \deg f$ , по п. 3 предложения 5.2.3 имеем  $(g, f) = 1$ . Следовательно, существуют многочлены  $u, v \in F[t]$ , такие, что  $gu + fv = 1$  и  $\deg u < \deg f$ . Поэтому  $u \in K$  и  $g \circ u = 1$ , так как  $gu = f(-v) + 1$ . Следовательно, многочлен  $u \in K$  является обратным по умножению элементом к многочлену  $g$ . Таким образом,  $K$  — поле.

Пусть  $a, b \in F$ . Рассмотрим их как многочлены нулевой степени из  $K$ . Тогда их сумма в поле  $F$  — это многочлен нулевой степени из  $K$ , равный  $a + b$ . Остаток от деления  $ab$  на  $f$  равен, очевидно,  $ab$ . Поэтому  $a \circ b = ab \in F$ . Таким образом,  $F$  — подполе поля  $K$ , а значит,  $K$  — расширение поля  $F$ .

Рассмотрим теперь элемент  $\alpha \in K$ , равный многочлену  $t = 0 + 1 \cdot t + 0 \cdot t^2 \dots + 0 \cdot t^{n-1} \in F[t]$ . Отметим, что  $\alpha = t$  действительно лежит в  $K$ , поскольку мы считаем, что  $\deg f > 1$ . Найдём теперь  $f(\alpha)$  в поле  $K$ . Подставляя  $t$  в равенство (1), получим

$$f(\alpha) = a_0 + a_1 \circ t + a_2 \circ t^2 + \dots + a_{n-1} \circ t^{n-1} + t^n,$$

причём для  $k = 1, \dots, n$  под  $t^k$  понимается произведение  $k$  элементов  $t$  в

поле  $K$ , т. е.

$$t^k = \underbrace{t \circ \dots \circ t}_{k \text{ раз}}.$$

Остатки от деления многочлена  $a_k t^k$ , рассматриваемого в обычном смысле, на  $f$  при  $k < n$ , очевидно, равны  $a_k t^k$ , поскольку  $\deg a_k t^k < \deg f$ . Это неверно для многочлена  $t^n$  ( $\deg t^n = n = \deg f$ ). Разделим с остатком  $t^n$  на  $f$ :

$$t^n = f(t) \cdot 1 - (a_0 + a_1 t + \dots + a_{n-1} t^{n-1}).$$

Поэтому в поле  $K$  произведение из  $n$  элементов, равных  $t$ , равно  $-(a_0 + a_1 t + \dots + a_{n-1} t^{n-1})$ . Следовательно,

$$f(\alpha) = a_0 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1} - (a_0 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1}) = 0.$$

**ПРИМЕР.** Рассмотрим многочлен  $g(x) = x^2 + 1 \in \mathbb{R}[x]$ . Он неразложим над  $\mathbb{R}$ . Построим, пользуясь способом, указанным при доказательстве теоремы, расширение поля  $\mathbb{R}$ , в котором  $g$  имеет корень. Имеем  $K = \{a + bt \mid a, b \in \mathbb{R}\}$ . Остаток от деления  $t^2$  на  $t^2 + 1$  равен  $-1$ . Следовательно,  $(t \circ t) + 1 = -1 + 1 = 0$ , а значит, многочлен  $t \in K$  является корнем многочлена  $g(x) \in K[x]$ . Несложно заметить, что построенное нами поле  $K$  изоморфно полю  $\mathbb{C}$  комплексных чисел. Достаточно положить  $t = i$ .

**УПРАЖНЕНИЕ 5.5.1.** Проверить, что многочлен  $g(x) = x^2 + 1$  имеет корень в поле  $F = \mathbb{Z}_2$  вычетов по модулю 2, а многочлен  $f(x) = x^2 + x + 1$  неразложим над тем же полем. Построить расширение  $K$  поля  $F$ , в котором  $f$  будет иметь корень. Сколько элементов имеет получившееся поле  $K$ ?

**Следствие 1** (о разложении многочлена на линейные множители). Пусть  $f \in F[x]$  и  $\deg f = n$ . Тогда существуют расширение  $K$  поля  $F$  и элементы  $\alpha_1, \alpha_2, \dots, \alpha_n \in K$  (не обязательно различные), такие, что

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n), \quad (2)$$

т. е.  $f$  разлагается над  $K$  на линейные множители.

**ДОКАЗАТЕЛЬСТВО.** Индукция по степени  $f$ . Если  $\deg f = 0$ , то  $F = K$  и  $f = a \in F$  — искомое разложение. Если  $\deg f > 0$ , то по теореме существуют расширение  $K_1$  поля  $F$  и элемент  $\alpha_1 \in K_1$ , такие, что

$f(\alpha_1) = 0$ . Поэтому над полем  $K_1$  многочлен  $f$  разложим в произведение  $f = (x - \alpha_1)f_1$ . Степень многочлена  $f_1$  равна  $n - 1$ . Следовательно, по предположению индукции найдутся расширение  $K$  поля  $K_1$  и элементы  $\alpha_2, \dots, \alpha_n \in K$ , такие, что  $f_1 = a(x - \alpha_2) \dots (x - \alpha_n) \in K[x]$ . Поэтому имеет место разложение (2) многочлена  $f$  над  $K$ . Осталось заметить, что расширение  $K$  поля  $K_1$  является и расширением поля  $F$ .  $\square$

**ПРИМЕР.** Многочлен  $x^2 + 1 \in \mathbb{R}[x]$  не только имеет корень в  $\mathbb{C}$ , но и разлагается над ним на линейные множители.

**УПРАЖНЕНИЕ 5.5.2.** Показать, что многочлен  $f(x) = x^4 - 5x^2 + 6$  из  $\mathbb{Q}[x]$  имеет корень в поле  $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ , но не разлагается над ним на линейные множители. Построить расширение поля  $\mathbb{Q}$ , над которым  $f$  разлагается на линейные множители.

Ещё одно следствие доказанной нами теоремы связано с так называемыми *формулами Виета* для коэффициентов многочлена.

**Следствие 2** (формулы Виета). *Предположим, что многочлен  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in F[x]$  имеет разложение  $f(x) = a_n (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$  в расширении  $K$  поля  $F$ . Тогда для каждого  $k = 1, \dots, n$*

$$s_k(\alpha_1, \dots, \alpha_n) = (-1)^k \frac{a_{n-k}}{a_n}, \quad (3)$$

где  $s_k$  —  $k$ -ый элементарный симметрический многочлен от  $n$  переменных. В частности, если  $g$  — произвольный симметрический многочлен от  $n$  переменных с коэффициентами из поля  $F$ , то  $g(\alpha_1, \dots, \alpha_n)$  лежит в  $F$ .

**ДОКАЗАТЕЛЬСТВО.** Формулы (3) проверяются непосредственно. Последнее же утверждение вытекает из теоремы 5.4.1 о представлении произвольного симметрического многочлена в виде многочлена от элементарных симметрических многочленов.  $\square$

**ЗАМЕЧАНИЕ.** Последнее утверждение следствия достаточно любопытно. Несмотря на то, что сами корни  $\alpha_1, \dots, \alpha_n$  не обязаны лежать в поле  $F$ , значение любого симметрического многочлена с коэффициентами из  $F$  от этих корней лежит в  $F$ .

**ПРИМЕР.** Корни  $i$  и  $-i$  многочлена  $x^2 + 1$  не лежат в  $\mathbb{R}$ , но сумма их квадратов  $i^2 + (-i)^2 = -2$  лежит в  $\mathbb{R}$ . Более того, для вычисления суммы квадратов корней многочлена  $x^2 + 1$  нам совершенно не обязательно знать, чему они равны. Действительно, если обозначить эти корни через  $\alpha_1, \alpha_2$ , то в силу утверждения упражнения 5.4.3 выполняются равенства

$\alpha_1^2 + \alpha_2^2 = s_1^2(\alpha_1, \alpha_2) - 2s_2(\alpha_1, \alpha_2)$ . С другой стороны, по формулам Виета  $s_1(\alpha_1, \alpha_2) = 0/1 = 0$ ,  $s_2(\alpha_1, \alpha_2) = 1/1 = 1$ , и мы получаем тот же результат.

В каком-то смысле историю развития алгебры как теории алгебраических уравнений можно рассматривать в контексте доказанной нами теоремы. Действительно, невозможность решения уравнений вида  $x^2 - 2 = 0$  в поле рациональных чисел приводит к необходимости его расширения до поля действительных чисел, а желание найти корни многочлена  $x^2 + 1$  — к построению поля комплексных чисел.

Возникает естественный вопрос, имеет ли каждый многочлен с комплексными коэффициентами корень в поле комплексных чисел, или требуется новое расширение уже этого поля? Оказывается, поле комплексных чисел в отличие от полей рациональных и действительных чисел обладает тем замечательным свойством, что любой многочлен, заданный над ним, имеет в  $\mathbb{C}$  корень, иными словами, поле комплексных чисел *алгебраически замкнуто*.

**Определение 5.5.2.** Поле  $F$  называется *алгебраически замкнутым*, если каждый многочлен из  $F[x]$  ненулевой степени имеет в  $F$  корень.

Теорема об алгебраической замкнутости поля комплексных чисел, впервые доказанная Гауссом в конце XVIII века, является одним из самых замечательных достижений всей математики. Поэтому её иногда называют *основной теоремой алгебры*.

Любопытно отметить, что, несмотря на название теоремы, любое её доказательство — а таких доказательств существует множество — по необходимости использует в той или иной мере аппарат математического анализа, а точнее, те свойства действительных и комплексных чисел, которые связаны с непрерывностью.

Приведённое далее доказательство почти целиком алгебраическое. Единственный факт из анализа, который мы будем использовать, интуитивно очевиден. А именно, непрерывность многочлена с действительными коэффициентами как вещественной функции позволяет утверждать, что любой такой многочлен нечётной степени имеет хотя бы один корень в  $\mathbb{R}$ .

ЗАМЕЧАНИЕ. Восходящее к Гауссу доказательство теоремы, использующее так называемую лемму Даламбера, напротив, почти целиком аналитично. Его можно прочесть в [5] или [13].

**Теорема 5.5.2** (основная теорема алгебры). Пусть  $f$  — многочлен

из  $\mathbb{C}[x]$  и  $\deg f > 0$ . Тогда существует элемент  $\alpha$  из  $\mathbb{C}$ , такой, что  $f(\alpha) = 0$ .

**ДОКАЗАТЕЛЬСТВО.** Поскольку при умножении на ненулевой скаляр корни многочлена не изменятся, можно полагать, что старший коэффициент многочлена  $f$  равен 1, т. е.

$$f = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n. \quad (4)$$

Мы начнём с уже упомянутого нами утверждения о существовании действительного корня у многочлена нечётной степени с действительными коэффициентами.

**Лемма 1.** Пусть  $f \in \mathbb{R}[x]$  и  $\deg f$  — нечётное число. Тогда существует такое  $\alpha \in \mathbb{R}$ , что  $f(\alpha) = 0$ .

**ДОКАЗАТЕЛЬСТВО** ЛЕММЫ. Положим  $A = \max\{|a_0|, |a_1|, \dots, |a_{n-1}|\}$ . Пусть  $\beta \in \mathbb{R}$  удовлетворяет условию  $|\beta| > 1 + A$ . Тогда

$$\begin{aligned} |a_0 + a_1\beta + \dots + a_{n-1}\beta^{n-1}| &\leq A(1 + |\beta| + \dots + |\beta|^{n-1}) = \\ &= A \frac{|\beta|^n - 1}{|\beta| - 1} < \frac{A}{|\beta| - 1} |\beta|^n < |\beta|^n. \end{aligned} \quad (5)$$

Поскольку степень  $n$  многочлена  $f$  нечётна, из неравенства (5) следует, что если  $\beta > 0$ , то  $f(\beta) > 0$ , а  $f(-\beta) < 0$ . Поскольку  $f(x)$  — непрерывная действительная функция действительного аргумента, по теореме Коши — Больцано она имеет действительный корень  $\alpha$  на отрезке  $[-\beta, \beta]$ , и лемма доказана.  $\square$

**ЗАМЕЧАНИЕ.** Отметим, что цепочка неравенств (5) выполняется и в том случае, когда  $a_i, \beta \in \mathbb{C}$ . Фактически она позволяет оценить значение модуля корня произвольного многочлена с числовыми коэффициентами. Мы сформулируем этот результат вместе с необходимым утверждением о свойствах модуля комплексного числа в качестве упражнения.

### УПРАЖНЕНИЕ 5.5.3.

1. Если  $\alpha, \beta \in \mathbb{C}$ , то  $|\alpha + \beta| \leq |\alpha| + |\beta|$  и  $|\alpha\beta| = |\alpha||\beta|$ .
2. Если  $f \in \mathbb{C}[x]$  имеет вид (4),  $\alpha \in \mathbb{C}$  и  $f(\alpha) = 0$ , то  $|\alpha| \leq 1 + A$ , где  $A = \max\{|a_0|, |a_1|, \dots, |a_{n-1}|\}$ . Иными словами, любой корень многочлена  $f$  лежит на комплексной плоскости в круге радиуса  $1 + A$  с центром в начале координат.

Вернёмся к доказательству теоремы. Следующая ключевая лемма показывает, что произвольный многочлен с действительными коэффициентами имеет хотя бы один комплексный корень.

**Лемма 2.** Пусть  $f \in \mathbb{R}[x]$  и  $\deg f > 0$ . Тогда существует такое  $\alpha \in \mathbb{C}$ , что  $f(\alpha) = 0$ .

**ДОКАЗАТЕЛЬСТВО ЛЕММЫ.** Пусть  $f$  — многочлен вида (4) и  $n = 2^k m$ , где  $k \in \mathbb{N}_0$  и  $m$  — нечётное натуральное число. Будем вести индукцию по  $k$ , воспользовавшись тем, что база индукции нами уже установлена в предыдущей лемме. Таким образом, предположение индукции состоит в том, что любой многочлен из  $\mathbb{R}[x]$ , степень которого не делится на  $2^k$ , имеет комплексный корень.

Поскольку  $\mathbb{R} \subseteq \mathbb{C}$ , можно считать, что  $f \in \mathbb{C}[x]$ . В силу следствия о разложении многочлена на линейные множители в расширении поля из теоремы 5.5.1 существует расширение  $K$  поля  $\mathbb{C}$ , такое, что  $f(x) = (x - \alpha_1) \dots (x - \alpha_n)$ , где  $\alpha_i \in K$  для любого  $i = 1, \dots, n$ . Пусть  $\gamma$  — произвольное действительное число. Для  $i, j \in \{1, \dots, n\}$ , таких, что  $i < j$ , положим

$$\beta_{ij} = \alpha_i \alpha_j + \gamma(\alpha_i + \alpha_j). \quad (6)$$

Элементы  $\beta_{ij}$  лежат в поле  $K$ , и общее их число равно

$$\frac{n(n-1)}{2} = \frac{2^k m(2^k m - 1)}{2} = 2^{k-1} l,$$

где число  $l$  нечётно. Кроме того, несложно заметить, что любая перестановка в наборе  $\alpha_i$  приводит лишь к перестановке в наборе  $\beta_{ij}$ .

Пусть многочлен  $g(x) \in K[x]$  имеет в качестве корней в точности все элементы  $\beta_{ij}$ , т. е

$$g(x) = \prod_{i < j} (x - \beta_{ij}). \quad (7)$$

Докажем, что многочлен  $g$  имеет действительные коэффициенты. В силу формул Виета коэффициенты многочлена  $g$  являются элементарными симметрическими многочленами от  $\beta_{ij}$ . Следовательно, ввиду (6) они являются многочленами от  $\alpha_1, \dots, \alpha_n$  с действительными коэффициентами (число  $\gamma$  действительное). Более того, поскольку любая перестановка в наборе  $\alpha_1, \dots, \alpha_n$  влечёт лишь перестановку в наборе  $\beta_{ij}$ , коэффициенты  $g$  — симметрические многочлены с действительными коэффициентами от  $\alpha_1, \dots, \alpha_n$ . В силу основной теоремы о симметрических многочленах коэффициенты  $g$  — многочлены с действительными коэффициентами от элементарных симметрических многочленов от  $\alpha_1, \dots, \alpha_n$ , т. е от коэффициентов многочлена  $f$ , которые по условию лежат в  $\mathbb{R}$ . Таким образом,  $g \in \mathbb{R}[x]$ .

С другой стороны, степень многочлена  $g$  равна  $2^{k-1} l$  и не делится на  $2^k$ , (хотя, возможно, и больше степени многочлена  $f$ ). Значит, по

предположению индукции  $g$  имеет хотя бы один комплексный корень. Поскольку действительное число  $\gamma$  мы выбирали произвольно, для каждого  $\gamma \in \mathbb{R}$  найдутся такие  $i, j \in \{1, \dots, n\}$ , где  $i < j$ , что  $\beta_{ij} \in \mathbb{C}$ . Кроме того, имеется лишь конечное число пар  $(i, j)$ , а множество  $\mathbb{R}$  бесконечно. Поэтому найдётся два различных действительных числа  $\gamma_1$  и  $\gamma_2$ , таких, что для одной и той же пары индексов  $(i, j)$  числа  $a$  и  $b$ , удовлетворяющие равенствам

$$\begin{cases} a = \alpha_i \alpha_j + \gamma_1 (\alpha_i + \alpha_j), \\ b = \alpha_i \alpha_j + \gamma_2 (\alpha_i + \alpha_j), \end{cases} \quad (8)$$

одновременно лежат в поле комплексных чисел. Из системы равенств (8) вытекает, что  $(\gamma_1 - \gamma_2)(\alpha_i + \alpha_j) = a - b$ . Следовательно, сумма

$$\alpha_i + \alpha_j = \frac{a - b}{\gamma_1 - \gamma_2}$$

является комплексным числом. Но тогда и произведение  $\alpha_i \alpha_j$  — комплексное число. Следовательно,  $\alpha_i, \alpha_j$  — корни квадратного уравнения с комплексными коэффициентами, а значит, сами лежат в поле  $\mathbb{C}$ . Лемма доказана.  $\square$

Завершим доказательство теоремы. Пусть  $f \in \mathbb{C}[x]$ . Положим

$$\bar{f}(x) = \bar{a}_0 + \bar{a}_1 x + \dots + \bar{a}_{n-1} x^{n-1} + x^n,$$

где черта над коэффициентами означает комплексное сопряжение, и рассмотрим многочлен

$$h(x) = f(x)\bar{f}(x) = b_0 + b_1 x + \dots + b_{2n-1} x^{2n-1} + b_{2n} x^{2n}.$$

Коэффициенты многочлена  $h$  удовлетворяют равенствам

$$b_k = \sum_{i+j=k} a_i \bar{a}_j.$$

Поэтому

$$\bar{b}_k = \sum_{i+j=k} \bar{a}_i a_j = b_k,$$

откуда  $b_k \in \mathbb{R}$  для любого  $k = 0, \dots, 2n$ . Следовательно,  $h \in \mathbb{R}[x]$  и по лемме 2 существует такой  $\alpha \in \mathbb{C}$ , что  $h(\alpha) = f(\alpha)\bar{f}(\alpha) = 0$ . Если  $f(\alpha) \neq 0$ , то  $\bar{f}(\alpha) = 0$ . Отсюда  $f(\bar{\alpha}) = \overline{\bar{f}(\alpha)} = \bar{0} = 0$ . В любом случае, либо  $\alpha$ , либо  $\bar{\alpha}$  — корень многочлена  $f$ .  $\square$

**Следствие** (о разложимости многочленов над полями действительных и комплексных чисел). 1. *Каждый многочлен  $f \in \mathbb{C}[x]$  степени, большей 0, разлагается над  $\mathbb{C}$  на линейные множители.*

2. *Каждый многочлен  $f \in \mathbb{R}[x]$  степени, большей 0, разлагается над  $\mathbb{R}$  в произведение многочленов степени не выше 2.*

**ДОКАЗАТЕЛЬСТВО.** 1. Индукция по степени многочлена. Поскольку в силу доказанной нами теоремы  $f$  имеет корень  $\alpha$  в  $\mathbb{C}$ , для некоторого многочлена  $f_1 \in \mathbb{C}$  выполняется  $f = (x - \alpha)f_1$ . Степень  $f_1$  меньше степени  $f$ , значит, для него по предположению индукции искомое разложение существует. Следовательно, оно существует и для  $f$ .

2. Снова индукция по степени  $f$ . Если  $f$  имеет хотя бы один действительный корень, то, рассуждая как при доказательстве п. 1, приходим к многочлену  $f_1 \in \mathbb{R}$ , имеющему степень меньше степени  $f$ . Таким образом, можно считать, что действительных корней у  $f$  нет. Тем не менее, по основной теореме алгебры хотя бы один комплексный корень у  $f$  имеется. Заметим, что в нашем случае  $\overline{f(x)} = f(x)$ . Следовательно, если  $\alpha$  — комплексный корень многочлена  $f$ , то  $f(\overline{\alpha}) = \overline{f(\alpha)} = \overline{f(\alpha)} = \overline{0} = 0$ . Поэтому  $\overline{\alpha}$  — ещё один корень многочлена  $f$ . Поскольку  $(x - \alpha, x - \overline{\alpha}) = 1$ , многочлен  $f$  делится на многочлен  $g(x) = (x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}$ , коэффициенты которого, как несложно проверить, лежат в  $\mathbb{R}$ . Таким образом,  $f = gf_1$ , где степень  $f_1$  меньше степени  $f$ .  $\square$

## § 5.6. Разложимость над полем рациональных чисел

В этом параграфе мы рассмотрим вопрос о разложимости многочленов с рациональными коэффициентами. В отличие от многочленов с действительными и комплексными коэффициентами, в этом случае явного описания неразложимых многочленов получить не удаётся. В частности, как мы покажем ниже, существуют неразложимые над  $\mathbb{Q}$  многочлены сколь угодно большой степени.

Пусть

$$f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Q}[x], a_i = \frac{p_i}{q_i}, p_i \in \mathbb{Z}, q_i \in \mathbb{N}. \quad (1)$$

Если обозначить через  $a$  наименьшее общее кратное чисел  $q_i$ ,  $i = 1, \dots, n$ , то многочлен  $af(x)$  имеет уже целые коэффициенты. С другой стороны, вопрос о разложимости  $f$  равносильен вопросу о разложимости  $af$  (см. предложение 5.2.3). Поэтому в дальнейшем мы будем предполагать, что  $f \in \mathbb{Z}[x]$ , т. е. его коэффициенты  $a_i$  — целые числа.



**Определение 5.6.1.** Многочлен  $f \in \mathbb{Z}[x]$  называется *примитивным*, если наибольший общий делитель его коэффициентов равен 1.

Если  $f \in \mathbb{Z}[x]$ , то  $f(x) = dp(x)$ , где  $d$  — наибольший общий делитель  $a_i$ , а  $p(x)$  — примитивный многочлен. Таким образом, решая вопрос о разложимости многочлена  $f$  с рациональными коэффициентами над  $\mathbb{Q}$ , мы можем полагать, что  $f$  — примитивный многочлен с целыми коэффициентами. Оказывается, что вопрос о разложимости многочлена с целыми коэффициентами над  $\mathbb{Q}$  равносильен вопросу о его разложимости над  $\mathbb{Z}$ .

**Теорема 5.6.1.** *Если многочлен  $f \in \mathbb{Z}[x]$  неразложим над  $\mathbb{Z}$ , то  $f$  неразложим и над  $\mathbb{Q}$ .*

**ДОКАЗАТЕЛЬСТВО.** Ключевую роль в доказательстве играет следующая лемма.

**Лемма (Гаусса).** *Произведение примитивных многочленов есть примитивный многочлен.*

**ДОКАЗАТЕЛЬСТВО ЛЕММЫ.** Пусть  $f(x) = a_0 + a_1x + \dots + a_nx^n$  и  $g(x) = b_0 + b_1x + \dots + b_mx^m$  — примитивные многочлены и  $h = fg = \sum_{k=0}^{n+m} c_kx^k$ . Предположим, что найдётся простое число  $p$ , которое делит  $c_k$  для каждого  $k = 0, 1, \dots, n+m$ . Из примитивности многочленов  $f$  и  $g$  следует, что  $p$  не может делить все коэффициенты этих многочленов. Пусть  $a_r$  — коэффициент с наименьшим индексом в  $f$ , который не делится на  $p$ , а  $b_s$  — коэффициент с наименьшим индексом в  $g$ , который не делится на  $p$ . Коэффициент  $c_{r+s}$  многочлена  $h$  равен

$$\sum_{i+j=r+s} a_i b_j = \underbrace{(a_0 b_{r+s} + \dots + a_{r-1} b_{s+1})}_{\vdots p} + \underbrace{a_r b_s}_{\not\vdots p} + \underbrace{(a_{r+1} b_{s-1} + \dots + a_{r+s} b_0)}_{\vdots p}.$$

Таким образом,  $c_{r+s}$  не делится на  $p$ ; противоречие.  $\square$

Вернёмся к доказательству теоремы. Пусть  $f$  — многочлен с целыми коэффициентами. Предположим, что  $f$  разлагается в произведение многочленов  $g, h \in \mathbb{Q}[x]$  и  $\deg g < \deg f$ ,  $\deg h < \deg f$ . Многочлены  $g$  и  $h$  можно представить в виде

$$g(x) = \frac{a}{b}u(x), \quad h = \frac{c}{d}v(x),$$

где  $a, b, c, d \in \mathbb{N}$ ,  $u, v$  — примитивные многочлены над  $\mathbb{Z}$ . Тогда

$$f = \frac{ac}{bd}uv = \frac{p}{q}uv, \quad \text{где } (p, q) = 1.$$

Отсюда вытекает равенство

$$qf = puv. \quad (2)$$

В силу леммы Гаусса произведение  $uv$  — снова примитивный многочлен. Поэтому наибольший общий делитель коэффициентов многочлена, стоящего в правой части равенства (2), равен  $p$ . С другой стороны, все коэффициенты многочлена, стоящего в левой части равенства (2), делятся на  $q$ . Следовательно,  $q$  делит  $p$ . Поскольку  $(p, q) = 1$ , имеем  $q = 1$ . Таким образом,  $f = puv = (pu)v$  разлагается в произведение многочленов  $(pu)$  и  $v$  с целыми коэффициентами, степень которых меньше степени  $f$ .  $\square$

Теперь мы укажем признак неразложимости многочлена над  $\mathbb{Q}$ .

**Теорема 5.6.2** (признак Эйзенштейна). Пусть  $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$ . Если существует простое число  $p$ , удовлетворяющее следующим условиям:

- 1)  $p \mid a_k$  для каждого  $k = 0, 1, \dots, n - 1$ ;
- 2)  $p \nmid a_n$ ;
- 3)  $p^2 \nmid a_0$ ,

то многочлен  $f$  неразложим над  $\mathbb{Q}$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $f = gh$ ,  $g, h \in \mathbb{Q}[x]$ ,  $\deg g < n$ ,  $\deg h < n$  и  $g = \sum_{i=0}^m b_i x^i$ ,  $h = \sum_{j=0}^s c_j x^j$ . В силу теоремы 5.6.1 можно считать, что коэффициенты  $b_i, c_j$  многочленов  $g$  и  $h$  — целые числа.

Поскольку  $p$  делит  $a_0 = b_0 c_0$ , оно делит либо  $b_0$ , либо  $c_0$ . Пусть для определённости  $p \mid b_0$ . С другой стороны,  $p^2$  не делит  $a_0$ , следовательно,  $p$  не делит  $c_0$ . Рассмотрим следующий коэффициент:  $a_1 = b_0 c_1 + b_1 c_0$ . Число  $p$  делит  $a_1$  и  $b_0$ , следовательно,  $p$  делит  $b_1 c_0 = a_1 - b_0 c_1$ . Поскольку  $p$  — простое число и  $p$  не делит  $c_0$ , оно делит  $b_1$ . Действуя аналогичным образом, можно показать, что  $p$  делит  $b_i$  для любого  $i = 0, 1, \dots, m$ . Действительно, пусть для  $i < k$  это уже доказано. В силу того, что  $p$  делит  $a_k = b_0 c_1 + \dots + b_{k-1} c_1 + b_k c_0$ , оно делит  $b_k c_0$ . Отсюда  $p$  делит  $b_k$ . В частности,  $p$  делит старший коэффициент  $b_m$  многочлена  $g$ . Но тогда  $p$  делит и старший коэффициент  $a_n = b_m c_s$  многочлена  $f$ , что противоречит условию теоремы.  $\square$

**Следствие.** Для любого натурального числа  $n$  существует многочлен  $f \in \mathbb{Z}[x]$ , неразложимый над  $\mathbb{Q}$ . В частности, над  $\mathbb{Q}$  неразложим многочлен  $x^n - 2$ .

**ДОКАЗАТЕЛЬСТВО.** Достаточно применить признак Эйзенштейна к многочлену  $x^n - 2$ .  $\square$

Таким образом, как уже говорилось в начале этого параграфа, явного описания многочленов, неразложимых над  $\mathbb{Q}$ , получить нельзя. Однако для каждого конкретного многочлена  $f \in \mathbb{Q}[x]$  за конечное число шагов можно определить, разложим ли он над  $\mathbb{Q}$  или нет. Иными словами, проблема разложимости многочлена в  $\mathbb{Q}[x]$  *алгоритмически разрешима*.

**Теорема 5.6.3.** *Проблема разложимости многочлена из  $\mathbb{Q}[x]$  алгоритмически разрешима: если  $f \in \mathbb{Q}[x]$ , то за конечное число шагов можно определить, разложим ли  $f$  в  $\mathbb{Q}[x]$ , и, если  $f$  разложим, найти представление  $f = uv$ , где  $u, v \in \mathbb{Q}[x]$  и  $\deg u < \deg f$ ,  $\deg v < \deg f$ .*

**ДОКАЗАТЕЛЬСТВО.** Можно считать, что  $f \in \mathbb{Z}[x]$  и  $\deg f > 1$ . По теореме 5.6.1 многочлен  $f$  разложим над  $\mathbb{Q}$  тогда и только тогда, когда он разложим над  $\mathbb{Z}$ . Поэтому, если  $f$  разложим, то найдутся такие многочлены  $u, v \in \mathbb{Z}[x]$ , что  $f = uv$ . Поскольку для степеней многочленов  $u$  и  $v$  выполняется  $\deg u + \deg v = n$ , меньшая из этих степеней не превосходит числа  $m = \lfloor \frac{n}{2} \rfloor$ . Пусть для определённости  $\deg u \leq m$ . Рассмотрим некоторый набор  $\alpha_0, \alpha_1, \dots, \alpha_m$  из  $m + 1$  целого числа, такой, что все числа, входящие в набор, попарно различны. Для каждого  $k = 0, 1, \dots, m$  выполняется  $f(\alpha_k) = u(\alpha_k)v(\alpha_k)$ . Поэтому целое число  $u(\alpha_k)$  делит целое число  $f(\alpha_k)$ . Заметим, что мы можем считать, что  $f(\alpha_k) \neq 0$ , иначе  $f = (x - \alpha_k)f_1$ , многочлен  $f$  разложим и искомое разложение найдено. Поэтому для каждого  $k = 0, 1, \dots, m$  множество  $M_k = \{\beta \in \mathbb{Z} \mid \beta \text{ делит } f(\alpha_k)\}$  состоит из конечного числа элементов. Конечным будет и множество  $M = \{(\beta_0, \beta_1, \dots, \beta_m) \mid \beta_k \in M_k\}$ . Зафиксируем некоторый элемент  $c = (\beta_0, \beta_1, \dots, \beta_m) \in M$ . Построим интерполяционный многочлен Лагранжа  $u_c$ , для которого  $u_c(\alpha_k) = \beta_k$  для всех  $k = 0, 1, \dots, m$ . Поскольку многочлен степени, не превосходящей  $m$ , однозначно определяется своими значениями в  $m + 1$  точке, если многочлен  $f$  разложим, то многочлен  $u$  должен совпасть с одним из многочленов  $u_c$  для некоторого  $c \in M$ . Следовательно, деля последовательно многочлен  $f$  на интерполяционные многочлены  $u_c$ , где  $c \in M$ , мы либо найдём подходящие многочлены  $u$  и  $v$ , либо, исключив все возможности, придём к выводу, что  $f$  неразложим. В любом случае потребуется лишь конечное число шагов, так как множество  $M$  конечно.  $\square$

**Следствие.** *Многочлен  $f \in \mathbb{Q}[x]$  за конечное число шагов можно разложить в произведение неразложимых многочленов из  $\mathbb{Q}[x]$ . В частности, за конечное число шагов можно определить все рациональные корни многочлена  $f$ .*

**ДОКАЗАТЕЛЬСТВО.** Индукция по степени  $f$ . Если  $f$  неразложим, то в силу доказанной нами теоремы мы определим это за конечное число шагов. Если он разложим, то за конечное число шагов мы найдём представление  $f$  в виде произведения двух многочленов из  $\mathbb{Q}[x]$ , для каждого из которых утверждение следствия выполняется по предположению индукции. Следовательно, и разложение для  $f$  будет получено за конечное число шагов. Далее, если  $\alpha_1, \dots, \alpha_s$  — все рациональные корни многочлена  $f$ , то в полученном нами за конечное число шагов разложении  $f$  на неразложимые множители, которое единственно в силу теоремы 5.2.4, встретятся делители  $(x - \alpha_1), \dots, (x - \alpha_s)$ .  $\square$

Заметим, что вопрос о рациональных корнях многочлена с целыми (рациональными) коэффициентами можно решить и не прибегая к методу, развитому в доказательстве теоремы 5.6.3. В частности, для решения этого вопроса достаточно следующих утверждений, которые мы сформулируем в качестве упражнения.

**УПРАЖНЕНИЕ 5.6.1.** Пусть  $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$ ,  $\alpha = \frac{p}{q}$ , где  $p \in \mathbb{Z}$ ,  $q \in \mathbb{N}$ ,  $(p, q) = 1$  и  $f(\alpha) = 0$ . Тогда выполняются следующие утверждения:

- 1)  $p \mid a_0$ ;
- 2)  $q \mid a_n$ ;
- 3)  $(p - tq) \mid f(m)$  для каждого  $m \in \mathbb{Z}$ .

**ЗАМЕЧАНИЕ.** На самом деле уже первых двух пунктов достаточно, чтобы свести вопрос о рациональных корнях многочлена  $f$  к перебору конечного числа вариантов. Применение же п. 3 зачастую позволяет свести такой перебор к минимуму.

**УПРАЖНЕНИЕ 5.6.2.** Рассмотрим многочлен  $f(x) = 2x^6 + 5x^5 - 3x^4 + 2x^3 + 7x^2 + 2x - 3$ .

1. Используя предыдущее упражнение, найти рациональные корни  $f$ .
2. Используя метод, изложенный при доказательстве теоремы, а также результаты предыдущего пункта, разложить  $f$  в произведение неразложимых многочленов из  $\mathbb{Q}[x]$ .

В заключение отметим, что не существует алгоритма разложения произвольного многочлена в произведение неразложимых многочленов над полями  $\mathbb{R}$  и  $\mathbb{C}$ , даже если предположить, что его коэффициенты — целые числа. Скажем, для многочлена  $f(x) = x^5 - 10x + 10$  нельзя явно записать его корни (их можно найти только приближённо), а значит, нельзя найти его разложение на линейные множители над полем  $\mathbb{C}$ . Это

утверждение, как и решение общего вопроса о разрешимости уравнений степени, большей 4, является следствием основной теоремы теории Галуа, изложение которой лежит за рамками этого курса.

## Глава 6

### Линейные преобразования

#### § 6.1. Линейное преобразование и его матрица

Эта глава посвящена общей теории линейных преобразований векторных пространств, которая является основным источником приложений линейной алгебры в различных областях математики. Напомним, что преобразование — это отображение множества в себя.

**Определение 6.1.1.** Пусть  $V$  — векторное пространство над полем  $F$ . Преобразование  $\varphi$  пространства  $V$ , т. е. отображение  $\varphi : V \rightarrow V$ , называется *линейным*, если

- 1)  $(v + w)\varphi = v\varphi + w\varphi$  для любых  $v, w \in V$ ;
- 2)  $(\alpha v)\varphi = \alpha(v\varphi)$  для любых  $v \in V$  и  $\alpha \in F$ .

Линейное преобразование  $\varphi$  также называется *линейным оператором* пространства  $V$ . Множество всех линейных преобразований пространства  $V$  мы обозначим через  $\mathcal{L}(V)$ .

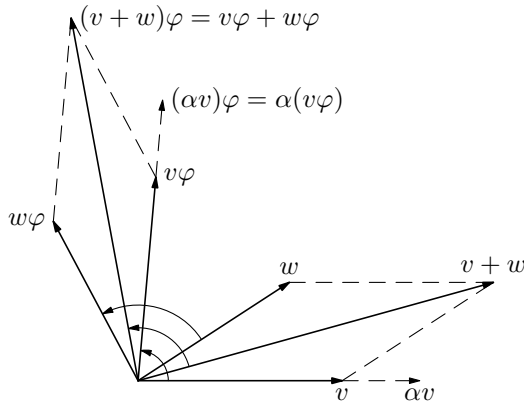
Непосредственно из определения вытекают следующие свойства линейных преобразований.

**УПРАЖНЕНИЕ 6.1.1.** Пусть  $\varphi : V \rightarrow V$  — преобразование пространства  $V$ . Доказать, что справедливы следующие утверждения.

1. Если  $\varphi$  линейно, то  $0\varphi = 0$ .
2. Если  $\varphi$  линейно, то  $(-v)\varphi = -(v\varphi)$  для любого  $v \in V$ .
3. Преобразование  $\varphi$  линейно тогда и только тогда, когда для любой линейной комбинации  $\alpha_1 v_1 + \dots + \alpha_s v_s$  векторов из  $V$  выполняется равенство

$$(\alpha_1 v_1 + \dots + \alpha_s v_s)\varphi = \alpha_1(v_1\varphi) + \dots + \alpha_s(v_s\varphi). \quad (1)$$

**ПРИМЕРЫ.** 1. Поворот является линейным преобразованием векторов плоскости (см. рисунок). Линейным преобразованием этого же пространства будет, как несложно проверить, любая осевая или центральная симметрия.



2. Проектирование векторов геометрического пространства  $V$  на плоскость  $U$  параллельно некоторой прямой  $W$  — линейный оператор пространства  $V$ . Указанный пример обобщается следующим образом. Пусть  $V$  — произвольное векторное пространство, которое раскладывается в прямую сумму своих подпространств:  $V = U \oplus W$ . Тогда, как мы знаем, каждый вектор  $v$  из  $V$  однозначно представим в виде  $v = u + w$ , где  $u \in U$ ,  $w \in W$ . Оператор  $\varphi : V \rightarrow V$ , действующий по правилу  $v\varphi = u$ , называется *оператором проектирования* из  $V$  на  $U$  параллельно  $W$ .

УПРАЖНЕНИЕ 6.1.2. Проверить, что оператор проектирования линейен.

3. Если рассматривать множество  $F[x]$  всех многочленов от одной переменной над полем  $F$  как векторное пространство относительно естественных операций сложения и умножения на скаляр, то оператор дифференцирования  $f(x) \mapsto f'(x)$ , т. е. взятия производной, является линейным оператором на  $F[x]$  в силу известных свойств производной.

4. Пусть  $\alpha$  — некоторый скаляр из поля  $F$ , над которым задано векторное пространство  $V$ . Рассмотрим преобразование  $\varphi_\alpha$  пространства  $V$ , действующее по правилу  $v\varphi_\alpha = \alpha v$ . Поскольку для любой линейной комбинации  $\alpha_1 v_1 + \dots + \alpha_s v_s$  выполняется  $\alpha(\alpha_1 v_1 + \dots + \alpha_s v_s) = \alpha_1(\alpha v_1) + \dots + \alpha_s(\alpha v_s)$ , преобразование  $\varphi_\alpha$  линейно. В частности, линейны нулевое преобразование  $0 = \varphi_0$ , переводящее каждый вектор пространства в нуль-вектор, и тождественное преобразование  $\varepsilon = \varphi_1$ , оставляющее каждый вектор пространства на месте. В дальнейшем мы будем называть преобразования  $\varphi_\alpha$  *скалярными* и обозначать через  $\alpha\varepsilon$ .

С другой стороны, перенос на фиксированный ненулевой вектор  $a \in$

$V$ , т. е. преобразование вида  $v \mapsto v + a$ , не является линейным, поскольку  $(v + w) + a \neq (v + a) + (w + a)$  при  $a \neq 0$ .

5. Пусть  $V = F^n$  — арифметическое пространство строк над полем  $F$ , а  $A \in M_n(F)$  — произвольная  $(n \times n)$ -матрица над полем  $F$ . Рассмотрим преобразование  $\varphi : V \rightarrow V$ , действующее по правилу  $x\varphi = xA$ , где  $xA$  — произведение матриц соответствующих размеров. Имеем:  $(x + y)\varphi = (x + y)A = xA + yA = x\varphi + y\varphi$  и  $(\alpha x)\varphi = (\alpha x)A = \alpha(xA) = \alpha(x\varphi)$ . Поэтому  $\varphi$  — линейное преобразование пространства  $V$ .

**ЗАМЕЧАНИЕ.** Последний пример в некотором точном смысле является универсальным. Оказывается, что существует естественная биекция между множеством  $\mathcal{L}(V)$  линейных преобразований пространства  $V$  размерности  $n$  над полем  $F$  и множеством  $M_n(F)$  всех квадратных матриц размера  $n$  над полем  $F$ . Установление такой биекции и является основной целью этого параграфа.

**Определение 6.1.2.** Пусть  $V$  — векторное пространство над полем  $F$ ,  $\varphi, \psi \in \mathcal{L}(V)$ ,  $\alpha \in F$ . Преобразование  $\varphi + \psi$  пространства  $V$ , определённое правилом  $v(\varphi + \psi) = v\varphi + v\psi$  для любого вектора  $v$  из  $V$ , называется *суммой* преобразований  $\varphi$  и  $\psi$ . Преобразование  $\varphi\psi$ , определённое правилом  $v(\varphi\psi) = (v\varphi)\psi$ , называется *произведением* преобразований  $\varphi$  и  $\psi$ , а преобразование  $\alpha\varphi$ , определённое правилом  $v(\alpha\varphi) = (\alpha v)\varphi$ , — *произведением скаляра  $\alpha$  и преобразования  $\varphi$* .

**Предложение 6.1.1.** Пусть  $V$  — векторное пространство над полем  $F$ ,  $\varphi, \psi \in \mathcal{L}(V)$ ,  $\alpha \in F$ . Тогда  $\varphi + \psi$ ,  $\varphi\psi$ ,  $\alpha\varphi$  — линейные преобразования пространства  $V$ .

**ДОКАЗАТЕЛЬСТВО.** Для любых  $v, u \in V$  выполняется  $(v + u)(\varphi + \psi) = (v + u)\varphi + (v + u)\psi = (v\varphi + u\varphi) + (v\psi + u\psi) = (v\varphi + v\psi) + (u\varphi + u\psi) = v(\varphi + \psi) + u(\varphi + \psi)$ , а для любых  $v \in V$  и  $\alpha \in F$  выполняется  $(\alpha v)(\varphi + \psi) = (\alpha v)\varphi + (\alpha v)\psi = \alpha(v\varphi) + \alpha(v\psi) = \alpha(v(\varphi + \psi))$ . Поэтому  $\varphi + \psi \in \mathcal{L}(V)$ . Аналогично доказывается, что  $\varphi\psi$ ,  $\alpha\varphi$  лежат в  $\mathcal{L}(V)$ .  $\square$

Таким образом, множество  $\mathcal{L}(V)$  замкнуто относительно операций, заданных в определении 6.1.2. Эти операции мы будем называть соответственно сложением, умножением и умножением на скаляр линейных преобразований. Прямая проверка аксиом показывает, что относительно указанных операций множество линейных преобразований образует алгебру над полем  $F$ . Однако мы докажем этот факт по-другому, установив изоморфизм между данной алгебраической системой и алгеброй матриц.

**Определение 6.1.3.** Пусть  $V$  — векторное пространство размерно-



сти  $n$  над полем  $F$  и  $\varphi$  — линейное преобразование этого пространства. Зафиксируем некоторый базис  $B$  пространства  $V$ , состоящий из векторов  $b_1, \dots, b_n$ . Матрицей линейного преобразования  $\varphi$  в базисе  $B$  называется матрица  $[\varphi]_B = A = (\alpha_{ij}) \in M_n(F)$ , коэффициенты которой определяются следующими равенствами:

$$\begin{cases} b_1\varphi = \alpha_{11}b_1 + \alpha_{12}b_2 + \dots + \alpha_{1n}b_n \\ b_2\varphi = \alpha_{21}b_1 + \alpha_{22}b_2 + \dots + \alpha_{2n}b_n \\ \vdots \\ b_n\varphi = \alpha_{n1}b_1 + \alpha_{n2}b_2 + \dots + \alpha_{nn}b_n. \end{cases} \quad (2)$$

**ЗАМЕЧАНИЕ.** Определение корректно, поскольку каждый из векторов  $b_1\varphi, b_2\varphi, \dots, b_n\varphi$ , лежащих в  $V$ , однозначно выражается через векторы базиса  $b_1, \dots, b_n$ .

В матричной форме: если  $b = (b_1, \dots, b_n)'$  и  $b\varphi = (b_1\varphi, \dots, b_n\varphi)'$  — столбцы векторов базиса и их образов под действием  $\varphi$  соответственно, то

$$b\varphi = [\varphi]_B b = Ab. \quad (3)$$

Напомним, что через  $[v]_B$  мы обозначаем строку координат вектора  $v \in V$  в базе  $B$ . В соответствии с этим обозначением  $v = [v]_B b$ . Если базис заранее фиксирован, то для краткости мы будем опускать нижний индекс в обозначениях строки координат и матрицы линейного преобразования, т. е. писать просто  $[v]$  и  $[\varphi]$ .

**Предложение 6.1.2.** Пусть  $[\varphi]$  — матрица линейного преобразования  $\varphi$  векторного пространства  $V$  в базе  $B$ . Тогда для любого вектора  $v \in V$  выполняется равенство

$$[v\varphi] = [v][\varphi]. \quad (4)$$

**ДОКАЗАТЕЛЬСТВО.** Пусть  $v = \alpha_1 b_1 + \dots + \alpha_n b_n$ , т. е.  $[v] = (\alpha_1, \dots, \alpha_n)$ . В силу равенства (1) имеем  $v\varphi = (\alpha_1 b_1 + \dots + \alpha_n b_n)\varphi = \alpha_1(b_1\varphi) + \dots + \alpha_n(b_n\varphi)$ , или в матричной форме:  $[v\varphi]b = [v](b\varphi)$ . С другой стороны, в силу равенства (3) и ассоциативности умножения матриц выполнено  $[v](b\varphi) = [v]([\varphi]b) = ([v][\varphi])b$ . Поэтому  $[v\varphi]b = ([v][\varphi])b$ . Поскольку векторы базиса линейно независимы, используя предложение 3.2.3, получаем требуемое равенство  $[v\varphi] = [v][\varphi]$ .  $\square$

**ЗАМЕЧАНИЕ.** Поскольку каждый вектор однозначно определяется своей строкой координат в некотором фиксированном базисе, из только

что доказанного предложения вытекает, что линейное преобразование однозначно определяется своей матрицей, т. е. своим действием на векторах базиса.

**ПРИМЕРЫ.** 1. Пусть  $\varphi$  — осевая симметрия относительно оси абсцисс в декартовой системе координат на плоскости и орты  $e_1, e_2$  выбраны в качестве базиса. Тогда

$$\begin{cases} e_1\varphi = 1 \cdot e_1 + 0 \cdot e_2 \\ e_2\varphi = 0 \cdot e_1 - 1 \cdot e_2 \end{cases}$$

и, следовательно,

$$[\varphi] = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Если  $x$  — произвольный вектор с координатами  $[x] = (x_1, x_2)$ , то в соответствии с предложением 6.1.2 имеем

$$[x\varphi] = [x][\varphi] = (x_1, x_2) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = (x_1, -x_2).$$

**УПРАЖНЕНИЕ 6.1.3.** Доказать, что в той же системе координат и том же базисе матрица поворота на угол  $\alpha$  (против часовой стрелки) имеет вид

$$\begin{pmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{pmatrix}.$$

2. Пусть  $V = \langle b_1, b_2, b_3 \rangle$  и  $\varphi$  — оператор проектирования на подпространство  $U = \langle b_1, b_2 \rangle$  параллельно подпространству  $W = \langle b_3 \rangle$ . Тогда в базисе  $b_1, b_2, b_3$  матрица оператора выглядит следующим образом:

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

3. Пусть для некоторого скаляра  $\alpha \in F$  преобразование  $\varphi_\alpha : V \rightarrow V$  определено правилом  $v\varphi_\alpha = \alpha v$  для любого  $v \in V$  (см. пример 4 после определения 6.1.1). Тогда несложно проверить, что в любом базисе  $[\varphi_\alpha] = \alpha E$ , где  $E$  — единичная матрица. В частности, в любом базисе  $[0] = 0$  и  $[\varepsilon] = E$ .

**УПРАЖНЕНИЕ 6.1.4.** Записать матрицу оператора дифференцирования пространства многочленов степени не выше  $n$  в базисах:

- 1)  $x^n, x^{n-1}, \dots, x, 1$ ;

$$2) \frac{x^n}{n!}, \frac{x^{n-1}}{(n-1)!}, \dots, x, 1.$$

Напомним, что множество квадратных матриц  $M_n(F)$  над полем  $F$  относительно операций сложения, умножения и умножения на скаляр образует алгебру (см. определение 3.1.2 и упражнение 3.1.2).

**Теорема 6.1.1.** Пусть  $V$  — векторное пространство размерности  $n$  над полем  $F$ . Тогда алгебраическая система с основным множеством  $\mathcal{L}(V)$  и операциями сложения, умножения и умножения на скаляр изоморфна алгебре матриц  $M_n(F)$ .

**ДОКАЗАТЕЛЬСТВО.** Зафиксируем некоторый базис  $B$ , состоящий из векторов  $b_1, \dots, b_n$ , в пространстве  $V$ . Мы докажем, что отображение  $[\ ] : \mathcal{L}(V) \rightarrow M_n(F)$ , сопоставляющее каждому линейному преобразованию  $\varphi$  его матрицу  $[\varphi]$  в базисе  $B$ , является искомым изоморфизмом.

Предположим, что у двух различных линейных преобразований  $\varphi$  и  $\psi$  одна и та же матрица в базисе  $B$ , т. е.  $[\varphi] = [\psi]$ . Поскольку  $\varphi \neq \psi$ , существует вектор  $u \in V$ , такой, что  $u\varphi \neq u\psi$ . Тогда строки координат этих векторов в базисе  $B$  также не равны:  $[u\varphi] \neq [u\psi]$ . Однако в силу предложения 6.1.2 имеют место равенства  $[u\varphi] = [u][\varphi] = [u][\psi] = [u\psi]$ ; противоречие. Следовательно, рассматриваемое нами отображение взаимно однозначно.

Чтобы показать, что наше отображение сюръективно, рассмотрим произвольную матрицу  $A = (\alpha_{ij}) \in M_n(F)$ . Зададим преобразование  $\varphi_A$  пространства  $V$  правилом  $v\varphi_A = ([v]A)b$ , где через  $b$  обозначен столбец  $(b_1, \dots, b_n)'$  векторов базиса  $B$  (сравните с примером 5 к определению 6.1.1 линейного преобразования). Тогда, рассуждая аналогично указанному примеру, получим, что

$$(v+w)\varphi_A = ([v+w]A)b = ([v]A + [w]A)b = ([v]A)b + ([w]A)b = v\varphi_A + w\varphi_A$$

и

$$(\alpha v)\varphi_A = (\alpha[v]A)b = \alpha([v]A)b = \alpha(v\varphi_A),$$

а значит,  $\varphi_A \in \mathcal{L}(V)$ . Далее, в силу выбора  $\varphi_A$  для любого  $i = 1, \dots, n$  выполняется

$$b_i\varphi_A = ([b_i]A)b = \sum_{j=1}^n \alpha_{ij}b_j.$$

Следовательно,  $[\varphi_A] = A$  по определению матрицы линейного преобразования. Таким образом, рассматриваемое отображение сюръективно, а значит, является биекцией.

Осталось доказать, что данное отображение сохраняет операции, заданные на  $\mathcal{L}(V)$ . Пусть  $[\varphi] = (\alpha_{ij})$ ,  $[\psi] = (\beta_{ij})$ .

Проверим, что  $[\varphi + \psi] = [\varphi] + [\psi]$ . Если  $[\varphi + \psi] = (\gamma_{ij})$ , то для каждого  $i = 1, \dots, n$  имеем  $b_i(\varphi + \psi) = \sum_{j=1}^n \gamma_{ij} b_j$ . С другой стороны,

$$b_i(\varphi + \psi) = b_i\varphi + b_i\psi = \sum_{j=1}^n \alpha_{ij} b_j + \sum_{j=1}^n \beta_{ij} b_j = \sum_{j=1}^n (\alpha_{ij} + \beta_{ij}) b_j.$$

Поскольку  $B$  — базис пространства  $V$ , для всех  $i, j \in \{1, \dots, n\}$  выполняется  $\gamma_{ij} = \alpha_{ij} + \beta_{ij}$ , т.е.  $[\varphi + \psi] = [\varphi] + [\psi]$ .

Пусть теперь  $[\varphi\psi] = (\gamma_{ij})$  и, следовательно,  $b_i(\varphi\psi) = \sum_{j=1}^n \gamma_{ij} b_j$ . Поскольку для любого  $i = 1, \dots, n$  выполняется

$$\begin{aligned} b_i(\varphi\psi) &= (b_i\varphi)\psi = \left( \sum_{k=1}^n \alpha_{ik} b_k \right) \psi = \sum_{k=1}^n \alpha_{ik} (b_k\psi) = \sum_{k=1}^n \alpha_{ik} \left( \sum_{j=1}^n \beta_{kj} b_j \right) = \\ &= \sum_{k=1}^n \sum_{j=1}^n \alpha_{ik} \beta_{kj} b_j = \sum_{j=1}^n \sum_{k=1}^n \alpha_{ik} \beta_{kj} b_j = \sum_{j=1}^n \left( \sum_{k=1}^n \alpha_{ik} \beta_{kj} \right) b_j, \end{aligned}$$

для всех  $i, j \in \{1, \dots, n\}$  справедливо  $\gamma_{ij} = \sum_{k=1}^n \alpha_{ik} \beta_{kj}$ . Отсюда  $[\varphi\psi] = [\varphi][\psi]$ .

Равенство  $[\alpha\varphi] = \alpha[\varphi]$  для произвольных  $\alpha \in F$  и  $\varphi \in \mathcal{L}(V)$  проверяется аналогично, и мы оставляем эту проверку читателям.  $\square$

**ЗАМЕЧАНИЕ.** Рассуждение в доказательстве теоремы, устанавливающее равенство  $[\varphi\psi] = [\varphi][\psi]$ , показывает, что выбор правила для умножения матриц, принятого нами без излишних объяснений в параграфе 2.3, был не случаен. Если воспринимать матрицы как записи линейных преобразований, то их умножение соответствует композиции, т.е. последовательному выполнению соответствующих линейных преобразований.

Теперь мы рассмотрим вопрос о связи между матрицами линейного преобразования в разных базисах. Пусть  $A$  и  $B$  — два базиса векторного пространства  $V$  над полем  $F$ , состоящие из векторов  $a_1, \dots, a_n$  и  $b_1, \dots, b_n$  соответственно. Если обозначить через  $a$  и  $b$  столбцы, состоящие из векторов базисов  $A$  и  $B$ , а через  $T = (t_{ij})$  — матрицу перехода от базиса  $A$  к базису  $B$ , то, как мы знаем,  $b = Ta$  и для любого вектора  $v \in V$  выполняется  $[v]_A = [v]_B T$ . Для произвольного  $\varphi \in \mathcal{L}(V)$  обозначим через  $[\varphi]_A$  и  $[\varphi]_B$  матрицы преобразования  $\varphi$  в базисах  $A$  и  $B$  соответственно. Имеем  $b\varphi = [\varphi]_B b = [\varphi]_B (Ta) = ([\varphi]_B T)a$ .

С другой стороны,  $b\varphi = (Ta)\varphi = T(a\varphi) = T([\varphi]_A a) = (T[\varphi]_A)a$ . Заметим, что равенство  $(Ta)\varphi = T(a\varphi)$  имеет место, так как в силу линейности оператора  $\varphi$  для каждого  $i = 1, \dots, n$  выполняется равенство  $(t_{i1}a_1 + \dots + t_{in}a_n)\varphi = t_{i1}(a_1\varphi) + \dots + t_{in}(a_n\varphi)$ . Таким образом,  $([\varphi]_B T)a = (T[\varphi]_A)a$ . Из предложения 3.2.3 следует, что  $[\varphi]_B T = T[\varphi]_A$ . Используя тот факт, что матрица перехода всегда обратима, можно записать полученное равенство в виде

$$[\varphi]_B = T[\varphi]_A T^{-1}. \quad (5)$$

Мы формализуем приведённое рассуждение с помощью следующего определения.

**Определение 6.1.4.** Матрицы  $A, B \in M_n(F)$  называются *сопряжёнными* (или *подобными*) над  $F$ , если существует невырожденная матрица  $T \in M_n(F)$ , для которой  $B = TAT^{-1}$ . Матрица  $T$  называется *сопрягающей* (осуществляющей подобие) для матриц  $A$  и  $B$ .

Выше мы доказали следующее утверждение.

**Теорема 6.1.2.** Пусть  $\varphi$  — линейное преобразование конечномерного векторного пространства  $V$  над полем  $F$ ,  $A$  и  $B$  — две базы пространства  $V$ . Тогда матрицы  $[\varphi]_A$  и  $[\varphi]_B$  преобразования  $\varphi$  в базах  $A$  и  $B$  сопряжены над  $F$ , причём в качестве сопрягающей их матрицы можно взять матрицу перехода от базы  $A$  к базе  $B$ .

**УПРАЖНЕНИЕ 6.1.5.** Пусть на плоскости задана декартова система координат. Записать матрицу поворота на угол  $\frac{\pi}{2}$  в базисе, состоящем из векторов  $b_1 = (0, 2)$  и  $b_2 = (1, -1)$ , используя результат упражнения 6.1.3 и формулу (5).

В заключение этого параграфа мы кратко остановимся на понятии линейного отображения, обобщающего понятие линейного преобразования.

**Определение 6.1.5.** Пусть  $V, U$  — векторные пространства над полем  $F$ . Отображение  $\psi : V \rightarrow U$ , называется *линейным*, если

- 1)  $(v + w)\psi = v\psi + w\psi$  для любых  $v, w \in V$ ;
- 2)  $(\alpha v)\psi = \alpha(v\psi)$  для любых  $v \in V$  и  $\alpha \in F$ .

Множество всех линейных отображений пространства  $V$  на пространство  $U$  мы обозначим через  $\mathcal{L}(V, U)$ . Сложение двух линейных отображений  $\varphi, \psi$  из  $V$  в  $U$  определяется правилом  $v(\varphi + \psi) = v\varphi + v\psi$ , а умножение отображения  $\psi$  на скаляр  $\alpha \in F$  — правилом  $(\alpha v)\psi = \alpha(v\psi)$  для всех векторов  $v \in V$ .

ПРИМЕРЫ. 1. Если  $V = F(\mathbb{R}, \mathbb{R})$  — пространство всех вещественных функций вещественной переменной, непрерывных на отрезке  $[a, b]$ , а  $U = \mathbb{R}$  — множество действительных чисел, рассматриваемое как одномерное векторное пространство над самим собой, то отображение

$$f \mapsto \int_a^b f(x) dx$$

является линейным отображением из  $V$  в  $U$ .

2. Пусть  $V = F^m$  и  $U = F^n$  — арифметические пространства строк над полем  $F$ , а  $A \in M_{m \times n}(F)$  — произвольная  $(m \times n)$ -матрица над полем  $F$ . Рассмотрим отображение  $\varphi : V \rightarrow U$ , действующее по правилу  $x\varphi = xA$ , где  $xA$  — произведение матриц соответствующих размеров. Имеем  $(x + y)\varphi = (x + y)A = xA + yA = x\varphi + y\varphi$  и  $(\alpha x)\varphi = (\alpha x)A = \alpha(xA) = \alpha(x\varphi)$ . Поэтому  $\varphi$  — линейное отображение из  $V$  в  $U$ .

**Определение 6.1.6.** Если зафиксированы базисы  $A$  и  $B$  пространств  $V$  и  $U$  соответственно, состоящие из векторов  $a_1, \dots, a_m$  и  $b_1, \dots, b_n$ , и выполняются равенства

$$\begin{cases} a_1\psi = \alpha_{11}b_1 + \alpha_{12}b_2 + \dots + \alpha_{1n}b_n \\ a_2\psi = \alpha_{21}b_1 + \alpha_{22}b_2 + \dots + \alpha_{2n}b_n \\ \vdots \\ a_m\psi = \alpha_{m1}b_1 + \alpha_{m2}b_2 + \dots + \alpha_{mn}b_n, \end{cases} \quad (6)$$

то матрица  $[\psi] = (\alpha_{ij}) \in M_{m \times n}(F)$  называется *матрицей линейного отображения*  $\psi$ , соответствующей базисам  $A$  и  $B$ .

УПРАЖНЕНИЕ 6.1.6. Доказать, что отображение  $[\ ] : \mathcal{L}(V, U) \rightarrow M_{m \times n}(F)$ , сопоставляющее каждому отображению  $\psi \in \mathcal{L}(V, U)$  его матрицу  $[\psi]$ , является изоморфизмом алгебраической системы  $\langle \mathcal{L}(V, U), +, f_\alpha \rangle$  на векторное пространство  $\langle M_{m \times n}(F), +, f_\alpha \rangle$ , где через  $f_\alpha$  обозначена операция умножения на скаляр  $\alpha \in F$ .

УПРАЖНЕНИЕ 6.1.7. Пусть  $V, U, W$  — конечномерные векторные пространства над полем  $F$  с базами  $A, B, C$  соответственно. Рассмотрим линейные отображения  $\varphi : V \rightarrow U$ ,  $\psi : U \rightarrow W$  и матрицы  $[\varphi]_{AB}$ ,  $[\psi]_{BC}$  этих отображений в соответствующих базисах. Доказать, что отображение  $\varphi\psi : V \rightarrow W$ , являющееся композицией отображений  $\varphi$  и  $\psi$ , линейно, а матрица  $[\varphi\psi]_{AC}$  этого отображения, соответствующая базисам  $A$  и  $C$ , равна произведению матриц  $[\varphi]_{AB}$  и  $[\psi]_{BC}$ .

УПРАЖНЕНИЕ 6.1.8. Пусть  $V$  и  $U$  — конечномерные векторные пространства над полем  $F$  и  $\psi \in \mathcal{L}(V, U)$ . Предположим, что  $T$  — матрица перехода от базиса  $A$  к базису  $A'$  пространства  $V$ , а  $S$  — матрица перехода от базиса  $B$  к базису  $B'$  пространства  $U$ . Пусть  $[\psi]_{AB}$  и  $[\psi]_{A'B'}$  — матрицы отображения  $\psi$  в соответствующих базисах. Доказать, что  $[\psi]_{A'B'} = T[\psi]_{AB}S^{-1}$ .

## § 6.2. Ядро и образ линейного преобразования

**Определение 6.2.1.** Пусть  $\varphi$  — линейное преобразование векторного пространства  $V$ ,  $U$  — некоторое подмножество множества  $V$ . *Образом  $U$  под действием  $\varphi$*  называется множество  $U\varphi = \{u\varphi \mid u \in U\}$ . В случае, когда  $U = V$ , множество  $\text{Im } \varphi = V\varphi$  называется *образом* линейного преобразования  $\varphi$ .

**Определение 6.2.2.** Пусть  $\varphi$  — линейное преобразование векторного пространства  $V$ . *Ядром* линейного преобразования  $\varphi$  называется множество  $\text{Ker } \varphi = \{v \in V \mid v\varphi = 0\}$ .

**Предложение 6.2.1.** Пусть  $\varphi$  — линейное преобразование векторного пространства  $V$ . Тогда  $\text{Im } \varphi$  и  $\text{Ker } \varphi$  — подпространства пространства  $V$ .

УПРАЖНЕНИЕ 6.2.1. Доказать предложение 6.2.1.

**Определение 6.2.3.** Размерность образа линейного преобразования  $\varphi$  называется *рангом* преобразования и обозначается как  $\text{rank}(\varphi)$ . Размерность ядра преобразования  $\varphi$  называется *дефектом* преобразования и обозначается как  $\text{def}(\varphi)$ .

**Теорема 6.2.1.** Пусть  $\varphi$  — линейное преобразование конечномерного векторного пространства  $V$  над полем  $F$ . Тогда выполняются следующие утверждения.

1.  $\text{rank}(\varphi) + \text{def}(\varphi) = \dim V$ .
2. Ранг преобразования  $\varphi$  равен рангу матрицы  $[\varphi]_B$  этого преобразования в любой базе  $B$  пространства  $V$ .

ДОКАЗАТЕЛЬСТВО. 1. Пусть  $w_1, \dots, w_s$  — базис  $\text{Ker } \varphi$  и  $u_1, \dots, u_r$  — базис  $V\varphi$ . Для каждого  $i = 1, \dots, r$  выберем вектор  $v_i \in V$  так, чтобы  $v_i\varphi = u_i$ . Мы докажем, что набор  $B$ , состоящий из векторов  $w_1, \dots, w_s, v_1, \dots, v_r$ , образует базис пространства  $V$ , откуда будет следовать требуемое утверждение.

Для любого  $v \in V$  выполняется  $v\varphi \in V\varphi$ , поэтому найдутся  $\alpha_1, \dots, \alpha_r \in F$ , для которых  $v\varphi = \alpha_1 u_1 + \dots + \alpha_r u_r = \alpha_1(v_1\varphi) + \dots + \alpha_r(v_r\varphi) = (\alpha_1 v_1 + \dots + \alpha_r v_r)\varphi$ . Положим  $w = v - (\alpha_1 v_1 + \dots + \alpha_r v_r)$ . Тогда  $w\varphi = v\varphi - (\alpha_1 v_1 + \dots + \alpha_r v_r)\varphi = v\varphi - v\varphi = 0$ . Следовательно,  $w \in \text{Ker } \varphi$ , а значит, найдутся  $\beta_1, \dots, \beta_s \in F$ , такие, что  $w = \beta_1 w_1 + \dots + \beta_s w_s$ . Тогда  $v = \alpha_1 v_1 + \dots + \alpha_r v_r + w = \alpha_1 v_1 + \dots + \alpha_r v_r + \beta_1 w_1 + \dots + \beta_s w_s$ . Таким образом,  $L(B) = V$ .

Предположим, что  $\alpha_1 v_1 + \dots + \alpha_r v_r + \beta_1 w_1 + \dots + \beta_s w_s = 0$ . Имеем  $0 = 0\varphi = (\alpha_1 v_1 + \dots + \alpha_r v_r + \beta_1 w_1 + \dots + \beta_s w_s)\varphi = (\alpha_1 v_1 + \dots + \alpha_r v_r)\varphi + (\beta_1 w_1 + \dots + \beta_s w_s)\varphi = \alpha_1 u_1 + \dots + \alpha_r u_r$ . Из линейной независимости набора векторов  $u_1, \dots, u_r$  как базиса пространства  $V\varphi$ , вытекает, что  $\alpha_1 = \dots = \alpha_r = 0$ . Поэтому  $\beta_1 w_1 + \dots + \beta_s w_s = 0$ . Поскольку набор  $w_1, \dots, w_s$  также является базисом, имеем  $\beta_1 = \dots = \beta_s = 0$ . Таким образом, набор  $B$  линейно независим, а следовательно, является базисом пространства  $V$ .

2. Пусть произвольный базис  $B$  пространства  $V$  состоит из векторов  $b_1, \dots, b_n$ . Поскольку отображение, сопоставляющее каждому вектору  $v \in V$  его строку координат  $[v]$  в базисе  $B$ , является изоморфизмом пространства  $V$  на арифметическое пространство  $F^n$ , ранг набора векторов  $b_1\varphi, \dots, b_n\varphi$  равен рангу набора строк  $[b_1\varphi], \dots, [b_n\varphi]$ .

Любой вектор  $v \in V$  является линейной комбинацией векторов базиса  $B$ :  $v = \alpha_1 b_1 + \dots + \alpha_n b_n$ . Поэтому  $v\varphi = \alpha_1(b_1\varphi) + \dots + \alpha_n(b_n\varphi)$ . Следовательно,  $V\varphi = \langle b_1\varphi, \dots, b_n\varphi \rangle$ , и  $\text{rang}(\varphi)$  равен рангу набора  $b_1\varphi, \dots, b_n\varphi$ .

С другой стороны, по определению матрицы линейного преобразования строки матрицы  $[\varphi]$  в базе  $B$  — это строки  $[b_1\varphi], \dots, [b_n\varphi]$ . Таким образом, ранг матрицы  $[\varphi]$  равен рангу набора  $[b_1\varphi], \dots, [b_n\varphi]$ , а значит, рангу преобразования  $\varphi$ .  $\square$

**ПРИМЕРЫ.** 1. Пусть  $\varphi$  — осевая симметрия относительно оси абсцисс в декартовой системе координат на плоскости и орты  $e_1, e_2$  выбраны в качестве базиса. Поскольку  $e_1\varphi = e_1, e_2\varphi = -e_2$  и векторы  $e_1, -e_2$  образуют базис пространства,  $V\varphi = V$  и  $\text{rang}(\varphi) = 2$ . В силу теоремы 6.2.1 имеем  $\text{def}(\varphi) = \dim V - \text{rang}(\varphi) = 0$  и  $\text{Ker } \varphi = 0$ . Последний факт несложно установить непосредственно, так как при осевой симметрии лишь нуль-вектор может быть прообразом нуль-вектора.

2. Пусть  $V = U \oplus W$  и  $\varphi$  — оператор проектирования на подпространство  $U$  параллельно пространству  $W$ . Тогда, как несложно проверить,  $\text{Im } \varphi = U$  и  $\text{Ker } \varphi = W$ .

**ЗАМЕЧАНИЕ.** В обоих приведённых выше примерах имеет место ра-



венство  $\text{Im } \varphi \cap \text{Ker } \varphi = 0$  и, следовательно,  $V = \text{Im } \varphi \oplus \text{Ker } \varphi$ . Однако, несмотря на справедливость равенства  $\dim V = \text{rank}(\varphi) + \text{def}(\varphi)$ , в общем случае такое разложение выполняется далеко не всегда.

**УПРАЖНЕНИЕ 6.2.2.** Пусть  $V = \mathbb{R}_2[x]$  — пространство многочленов степени не выше 2 над полем действительных чисел. Найти образ и ядро оператора дифференцирования  $\varphi$  указанного пространства и проверить, что  $V \neq \text{Im } \varphi \oplus \text{Ker } \varphi$ .

**УПРАЖНЕНИЕ 6.2.3.** Пусть  $\varphi$  — линейное преобразование пространства  $V$ . Доказать, что  $V = V\varphi \oplus \text{Ker } \varphi$  тогда и только тогда, когда  $V\varphi = V\varphi^2$ .

В следующем упражнении мы укажем удобный практический способ одновременного отыскания базиса образа и ядра линейного преобразования конечномерного векторного пространства. Для краткости мы будем отождествлять векторы пространства с их строками координат в выбранном базисе.

**УПРАЖНЕНИЕ 6.2.4.** Пусть  $N = [\varphi]_A$  — матрица линейного преобразования  $n$ -мерного пространства  $V$  над полем  $F$  в базисе  $A$ . Пусть матрица  $B \in M_n(F)$  выбрана так, что её строки составляют базис пространства  $V$ , и  $C = BN$ . Если прямоугольную  $(n \times 2n)$ -матрицу  $(B \mid C)$  элементарными преобразованиями строк привести к виду  $(B' \mid C')$ , где матрица  $C'$  ступенчатая, то

- а) ненулевые строки матрицы  $C'$  образуют базис  $\text{Im } \varphi$ ;
- б) строки матрицы  $B'$ , стоящие напротив нулевых строк матрицы  $C'$ , образуют базис  $\text{Ker } \varphi$ .

В заключение этого параграфа мы рассмотрим понятие невырожденности линейного преобразования.

**Определение 6.2.4.** Линейное преобразование  $\varphi$  векторного пространства  $V$  называется *невырожденным*, если  $\text{Ker } \varphi = 0$ , и *вырожденным* в противном случае.

**Теорема 6.2.2.** Пусть  $\varphi$  — линейное преобразование конечномерного векторного пространства  $V$  над полем  $F$ . Следующие утверждения эквивалентны.

1. Преобразование  $\varphi$  невырождено.
2.  $\text{Im } \varphi = V$ .
3. Под действием  $\varphi$  любой базис пространства  $V$  переходит в базис.
4. Матрица  $[\varphi]_B$  преобразования  $\varphi$  в любом базисе  $B$  пространства  $V$  невырождена.

5. Преобразование  $\varphi$  обратимо, т. е. существует преобразование  $\varphi^{-1} \in \mathcal{L}(V)$ , такое, что  $\varphi\varphi^{-1} = \varphi^{-1}\varphi = \varepsilon$ .

ДОКАЗАТЕЛЬСТВО. (1  $\Rightarrow$  2) Поскольку  $\text{Ker } \varphi = 0$ , выполняется  $\dim \text{Im } \varphi = \dim V - \dim \text{Ker } \varphi = \dim V$ . Поэтому  $\text{Im } \varphi = V$ .

(2  $\Rightarrow$  3) Пусть  $b_1, \dots, b_n$  — базис  $V$ . Тогда  $V = V\varphi = \langle b_1\varphi, \dots, b_n\varphi \rangle$ . По следствию из теоремы 3.2.2 о базисе набор  $b_1\varphi, \dots, b_n\varphi$  — базис пространства  $V$ .

(3  $\Rightarrow$  4) Поскольку  $b_1\varphi, \dots, b_n\varphi$  — базис пространства  $V$ , набор строк  $[b_1\varphi], \dots, [b_n\varphi]$  матрицы  $[\varphi]$  в этой базе линейно независим. Следовательно,  $\det[\varphi] \neq 0$ .

(4  $\Rightarrow$  5) Пусть базис  $B$  пространства  $V$  состоит из векторов  $b_1, \dots, b_n$  и  $b = (b_1, \dots, b_n)'$  — столбец векторов базиса. Пусть  $[\varphi]$  — матрица преобразования  $\varphi$  в базисе  $B$ . Поскольку  $\det[\varphi] \neq 0$ , матрица  $[\varphi]$  обратима и существует обратная к ней матрица  $[\varphi]^{-1}$ . Зададим преобразование  $\varphi^{-1} : V \rightarrow V$  правилом  $v\varphi^{-1} = ([v][\varphi]^{-1})b$ . Тогда  $\varphi^{-1} \in \mathcal{L}(B)$  и  $[\varphi^{-1}] = [\varphi]^{-1}$ . В силу изоморфизма между  $\mathcal{L}(V)$  и  $M_n(F)$  выполняется  $[\varphi\varphi^{-1}] = [\varphi][\varphi^{-1}] = [\varphi][\varphi]^{-1} = [\varepsilon] = [\varphi]^{-1}[\varphi] = [\varphi^{-1}][\varphi] = [\varphi^{-1}\varphi]$ . Из равенства матриц  $[\varphi\varphi^{-1}] = [\varphi^{-1}\varphi] = [\varepsilon]$  следует равенство соответствующих линейных преобразований.

(5  $\Rightarrow$  1) Пусть  $v \in \text{Ker } \varphi$ . Тогда  $v = v\varepsilon = v(\varphi\varphi^{-1}) = (v\varphi)\varphi^{-1} = 0\varphi^{-1} = 0$ . Поэтому  $\text{Ker } \varphi = 0$ .  $\square$

ЗАМЕЧАНИЕ. Пусть  $A, B$  — базисы пространства  $V$  и  $\varphi$  — его линейное преобразование. Поскольку  $[\varphi]_B = T[\varphi]_A T^{-1}$ , где  $T$  — матрица перехода от  $A$  к  $B$ , то по теореме 2.4.1 об определителе произведения матриц выполняется  $\det[\varphi]_B = \det[\varphi]_A$ . Следовательно, определитель матрицы линейного преобразования не зависит от выбора базиса. Таким образом, корректно следующее определение.

**Определение 6.2.5.** *Определитель линейного преобразования  $\varphi$  векторного пространства  $V$  — это определитель матрицы этого преобразования.*

В частности, из теоремы 6.2.2 следует, что преобразование вырождено тогда и только тогда, когда его определитель равен 0.

УПРАЖНЕНИЕ 6.2.5. Доказать, что линейное преобразование  $\varphi$  векторного пространства  $V$  является изоморфизмом  $V$  на себя тогда и только тогда, когда  $\varphi$  невырождено.

УПРАЖНЕНИЕ 6.2.6. Пусть  $V$  — векторное пространство над полем  $F$ . Положим  $GL(V) = \{\varphi \in \mathcal{L}(V) \mid \det \varphi \neq 0\}$ . Доказать, что  $GL(V)$  — группа относительно операции умножения линейных преобразований.

**Определение 6.2.6.** Группа  $GL(V)$ , определенная в упражнении 6.2.6, называется *общей группой линейных преобразований* пространства  $V$ , а любая её подгруппа — *группой линейных преобразований* пространства  $V$ .

ЗАМЕЧАНИЕ. Сравните упражнение 6.2.6 и определение 6.2.6 с упражнением 2.4.8 и определением 2.4.8 из второй главы.

### § 6.3. Инвариантные подпространства и собственные векторы

**Определение 6.3.1.** Пусть  $\varphi$  — линейное преобразование векторного пространства  $V$  над полем  $F$ . Подпространство  $U$  пространства  $V$  называется  $\varphi$ -инвариантным, если  $U\varphi \subseteq U$ .

ПРИМЕРЫ. 1. Из определения линейного преобразования и упражнения 6.1.1 следует, что само пространство и нулевое подпространство являются  $\varphi$ -инвариантными относительно любого линейного преобразования  $\varphi$ .

2. Пусть  $\varphi$  — осевая симметрия относительно оси абсцисс в декартовой системе координат на плоскости. Тогда подпространства  $U_1 = \langle e_1 \rangle$  и  $U_2 = \langle e_2 \rangle$   $\varphi$ -инвариантны, а подпространство  $U_3 = \langle e_1 + e_2 \rangle$  — нет.

УПРАЖНЕНИЕ 6.3.1. Пусть  $\varphi$  — поворот декартовой плоскости относительно начала координат на угол, не кратный  $\pi$ . Доказать, что пространство геометрических векторов плоскости над полем  $\mathbb{R}$  не имеет  $\varphi$ -инвариантных подпространств, отличных от нулевого подпространства и самого пространства.

3. Пусть  $V = \mathbb{R}[x]$  — пространство многочленов одной переменной с действительными коэффициентами. Тогда подпространство  $U = \mathbb{R}_n[x] = \{f \in V \mid \deg f \leq n\}$  инвариантно относительно оператора дифференцирования, действующего на  $V$ .

**Предложение 6.3.1.** Пусть  $\varphi, \psi$  — линейные преобразования векторного пространства  $V$ , причём  $\varphi\psi = \psi\varphi$ . Тогда  $\text{Ker } \psi$  и  $\text{Im } \psi$  являются  $\varphi$ -инвариантными подпространствами пространства  $V$ . В частности,  $\varphi$ -инвариантны подпространства  $\text{Ker } \varphi$  и  $\text{Im } \varphi$ .

ДОКАЗАТЕЛЬСТВО. Для любого  $w \in \text{Ker } \psi$  выполняется  $(w\varphi)\psi = w(\varphi\psi) = w(\psi\varphi) = (w\psi)\varphi = 0\varphi = 0$ . Поэтому  $w\varphi \in \text{Ker } \psi$  и, следовательно,  $(\text{Ker } \psi)\varphi \subseteq \text{Ker } \psi$ .

Для любого  $v\psi \in V\psi$  выполняется  $(v\psi)\varphi = (v\varphi)\psi \in V\psi$ . Следовательно,  $(V\psi)\varphi \subseteq V\psi$ .  $\square$

**Определение 6.3.2.** Пусть  $\varphi$  — линейное преобразование пространства  $V$  и  $U$  —  $\varphi$ -инвариантное подпространство в  $V$ . Преобразование  $\psi : U \rightarrow U$ , действующее по правилу  $u\psi = u\varphi$  для любого  $u \in U$ , называется *сужением* (или *ограничением*) преобразования  $\varphi$  на подпространство  $U$ . Обозначение:  $\psi = \varphi|_U$ .

**ЗАМЕЧАНИЕ.** Легко проверить, что сужение  $\varphi|_U$  является линейным преобразованием пространства  $U$ .

**Теорема 6.3.1.** Пусть  $\varphi$  — линейное преобразование  $n$ -мерного векторного пространства  $V$  над полем  $F$ . Тогда выполняются следующие утверждения.

1. Если  $U$  —  $\varphi$ -инвариантное подпространство пространства  $V$ ,  $A$  — база  $U$ , состоящая из векторов  $u_1, \dots, u_r$ , то в базе  $B$  пространства  $V$ , состоящей из векторов  $u_1, \dots, u_r, v_{r+1}, \dots, v_n$ , матрица преобразования  $\varphi$  имеет вид

$$[\varphi]_B = \left( \begin{array}{c|c} [\varphi|_U]_A & 0 \\ \hline * & * \end{array} \right),$$

где  $[\varphi|_U]_A$  — матрица сужения  $\varphi$  на подпространство  $U$  в базе  $A$ .

2. Если  $V = U_1 \oplus \dots \oplus U_s$ , где для любого  $i = 1, \dots, s$  подпространства  $U_i$   $\varphi$ -инвариантны, то в базе  $B$  пространства  $V$ , являющейся объединением баз  $B_1, \dots, B_s$  подпространств  $U_1, \dots, U_s$ , матрица преобразования  $\varphi$  клеточно диагональна и имеет вид

$$[\varphi]_B = \left( \begin{array}{ccc} [\varphi|_{U_1}]_{B_1} & & 0 \\ & \ddots & \\ 0 & & [\varphi|_{U_s}]_{B_s} \end{array} \right).$$

**ДОКАЗАТЕЛЬСТВО.** Положим  $\psi = \varphi|_U$ . Так как  $U$  —  $\varphi$ -инвариантное подпространство, то для любого  $i = 1, \dots, r$  выполняется  $u_i\varphi \in U$ , и, следовательно,  $u_i\varphi = \alpha_{i1}u_1 + \dots + \alpha_{ir}u_r + 0 \cdot v_{r+1} + \dots + 0 \cdot v_n$ . Кроме того,  $u_i\psi = u_i\varphi = \alpha_{i1}u_1 + \dots + \alpha_{ir}u_r$ . Отсюда следует утверждение п. 1 теоремы.

Утверждение п. 2 сразу вытекает из п. 1 в случае  $s = 2$ , а при  $s > 2$  несложно доказывается индукцией.  $\square$

**УПРАЖНЕНИЕ 6.3.2.** Провести полное доказательство п. 2 теоремы.

**ЗАМЕЧАНИЕ.** Основная задача теории линейных преобразований состоит в выборе для данного линейного преобразования такого базиса

пространства, в котором матрица преобразования имеет наиболее простой вид. Из формулировки только что доказанной теоремы ясно, что поиск инвариантных относительно преобразования подпространств является важным шагом в решении этой задачи.

**Определение 6.3.3.** Пусть  $\varphi$  — линейное преобразование векторного пространства  $V$  над полем  $F$ . Ненулевой вектор  $u$  называется *собственным вектором* преобразования  $\varphi$ , если существует  $\lambda \in F$ , для которого  $u\varphi = \lambda u$ . Скаляр  $\lambda$  называется *собственным числом* (или *собственным значением*) преобразования  $\varphi$ , соответствующим вектору  $u$ .

**ПРИМЕРЫ.** 1. Пусть  $\varphi$  — осевая симметрия относительно оси абсцисс в декартовой системе координат на плоскости. Тогда орт  $e_1$  — собственный вектор преобразования  $\varphi$  с собственным числом 1, а орт  $e_2$  — собственный вектор преобразования  $\varphi$  с собственным числом  $-1$ , так как  $e_1\varphi = 1 \cdot e_1$  и  $e_2\varphi = -1 \cdot e_2$ . С другой стороны, так как вектор  $e_1 + e_2$  не коллинеарен вектору  $(e_1 + e_2)\varphi = e_1 - e_2$ , он не является собственным вектором преобразования  $\varphi$ .

2. Любой многочлен нулевой степени является собственным вектором оператора дифференцирования пространства многочленов с числовыми коэффициентами от одной переменной с собственным числом 0. Других собственных векторов и собственных чисел для данного оператора в этом пространстве нет.

**УПРАЖНЕНИЕ 6.3.3.** Доказать следующие утверждения.

1. Пусть  $u$  — собственный вектор преобразования  $\varphi$ . Тогда одномерное подпространство  $U = \langle u \rangle$ , натянутое на вектор  $u$ ,  $\varphi$ -инвариантно.

2. Пусть  $U = \langle u \rangle$  — одномерное  $\varphi$ -инвариантное подпространство, натянутое на вектор  $u$ . Тогда  $u$  — собственный вектор преобразования  $\varphi$ . Более того, если  $u\varphi = \lambda u$ , то для любого вектора  $v \in U$  выполняется  $v\varphi = \lambda v$ .

**Определение 6.3.4.** Пусть  $F$  — поле и  $A = (a_{ij}) \in M_n(F)$ . Многочлен

$$f(x) = \begin{vmatrix} a_{11} - x & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - x & \dots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} - x \end{vmatrix} = |A - xE| \in F[x]$$

называется *характеристическим многочленом матрицы  $A$*  и обозначается через  $f_A(x)$ . Корни характеристического многочлена называются

характеристическими корнями матрицы  $A$ , их множество называется спектром матрицы  $A$  и обозначается через  $\text{Sp}(A)$ .

**ЗАМЕЧАНИЕ.** Поскольку корни многочлена могут не лежать в поле его коэффициентов, в обозначениях определения 6.3.4  $\text{Sp}(A)$  может не лежать в  $F$ . Тем не менее, как мы знаем, всегда найдётся расширение  $K$  поля  $F$ , для которого  $\text{Sp}(A) \subseteq K$ .

**УПРАЖНЕНИЕ 6.3.4.** Доказать, что спектр треугольной матрицы  $A \in M_n(F)$  совпадает с множеством элементов матрицы, стоящих на её главной диагонали.

**Предложение 6.3.2.** Пусть  $A$  и  $B$  — подобные матрицы из  $M_n(F)$ . Тогда  $f_A(x) = f_B(x)$ .

**ДОКАЗАТЕЛЬСТВО.** Поскольку  $B = TAT^{-1}$ , для некоторой невырожденной матрицы  $T \in M_n(F)$  имеют место равенства  $f_B(x) = |B - xE| = |TAT^{-1} - T(xE)T^{-1}| = |T(A - xE)T^{-1}| = |T||A - xE||T^{-1}| = f_A(x)$ .  $\square$

Из предложения 6.3.2 вытекает корректность следующего определения.

**Определение 6.3.5.** Характеристическим многочленом линейного преобразования  $\varphi$  конечномерного векторного пространства называется характеристический многочлен матрицы  $[\varphi]$  этого преобразования в некотором базисе. Спектром преобразования  $\varphi$  называется спектр матрицы  $[\varphi]$ . Обозначения:  $f_\varphi(x) = f_{[\varphi]}(x)$  и  $\text{Sp}(\varphi) = \text{Sp}([\varphi])$ .

**Предложение 6.3.3.** Пусть  $f_\varphi$  — характеристический многочлен линейного преобразования  $\varphi$  конечномерного векторного пространства  $V$ . Тогда выполняются следующие утверждения.

1. Если  $U$  —  $\varphi$ -инвариантное подпространство, то характеристический многочлен  $f_{\varphi|_U}$  сужения  $\varphi$  на  $U$  делит многочлен  $f_\varphi$ .
2. Если  $V = U_1 \oplus \dots \oplus U_s$  и для любого  $i = 1, \dots, s$  подпространства  $U_i$   $\varphi$ -инвариантны, то  $f_\varphi = f_{\varphi|_{U_1}} \cdots f_{\varphi|_{U_s}}$ .

**УПРАЖНЕНИЕ 6.3.5.** Доказать предложение 6.3.3. Указание. Применить теорему 6.3.1.

**Теорема 6.3.2.** Пусть  $\varphi$  — линейное преобразование  $n$ -мерного векторного пространства  $V$  над полем  $F$ . Тогда выполняются следующие утверждения.

1. Вектор  $u \in V$  является собственным вектором преобразования  $\varphi$  с собственным числом  $\lambda$  тогда и только тогда, когда  $u \neq 0$  и  $u \in \text{Ker}(\varphi - \lambda\varepsilon)$ .

2. Скаляр  $\lambda$  — собственное число преобразования  $\varphi$  тогда и только тогда, когда  $\lambda \in F$  и  $\lambda$  — корень характеристического многочлена преобразования  $\varphi$ .

3. Собственные векторы преобразования  $\varphi$ , соответствующие различным собственным значениям, линейно независимы.

ДОКАЗАТЕЛЬСТВО. 1. Рассмотрим произвольный вектор  $u$  из  $V$ . Утверждение п. 1 вытекает из следующих соображений:

$$u\varphi = \lambda u \Leftrightarrow 0 = u\varphi - \lambda u = u\varphi - u(\lambda\varepsilon) = u(\varphi - \lambda\varepsilon) \Leftrightarrow u \in \text{Ker}(\varphi - \lambda\varepsilon).$$

2. Пусть  $\lambda \in F$ . Утверждение п. 2 получается из следующих соображений:

$$\exists u \neq 0 : u\varphi = \lambda u \Leftrightarrow \text{Ker}(\varphi - \lambda\varepsilon) \neq 0 \Leftrightarrow 0 = |[\varphi - \lambda\varepsilon]| = |[\varphi] - \lambda E| = f_\varphi(\lambda).$$

3. Пусть  $u_1, \dots, u_s$  — собственные векторы преобразования  $\varphi$ , соответствующие собственным числам  $\lambda_1, \dots, \lambda_s$ , причём  $\lambda_i \neq \lambda_j$  при  $i \neq j$ . Докажем утверждение индукцией по  $s$ . При  $s = 1$  оно очевидно. Пусть  $0 = \alpha_1 u_1 + \dots + \alpha_{s-1} u_{s-1} + \alpha_s u_s$ . Тогда

$$\begin{aligned} 0 &= 0(\varphi - \lambda_s \varepsilon) = (\alpha_1 u_1 + \dots + \alpha_{s-1} u_{s-1} + \alpha_s u_s)(\varphi - \lambda_s \varepsilon) = \\ &= \alpha_1(\lambda_1 - \lambda_s)u_1 + \dots + \alpha_{s-1}(\lambda_{s-1} - \lambda_s)u_{s-1}. \end{aligned}$$

По предположению индукции векторы  $u_1, \dots, u_{s-1}$  линейно независимы. Поэтому  $\alpha_1 = \dots = \alpha_{s-1} = 0$ . Но тогда и  $\alpha_s = 0$ .  $\square$

Из п. 1 теоремы 6.3.2 следует, что множество собственных векторов преобразования  $\varphi$ , соответствующих одному собственному числу  $\lambda$ , вместе с нулевым вектором (для него тоже выполняется  $0\varphi = \lambda 0$ ) образует подпространство пространства  $V$  (и даже  $\varphi$ -инвариантное подпространство). Мы будем называть его *подпространством собственных векторов преобразования  $\varphi$ , соответствующих  $\lambda$* . Поскольку это подпространство есть ядро преобразования  $\varphi - \lambda\varepsilon$ , используя методы предыдущего параграфа, можно найти его базис. Далее, из п. 2 теоремы вытекает, что задача определения всех собственных чисел преобразования  $\varphi$  сводится к поиску корней характеристического многочлена  $f_\varphi(x)$ , лежащих в поле  $F$ . Если эту задачу удаётся решить, то для данного преобразования  $\varphi$  мы можем определить все его собственные векторы (точнее, базисы подпространств его собственных векторов). Из п. 3 теоремы и определения прямой суммы подпространств следует, что сумма подпространств собственных векторов, соответствующих различным собственным значениям, всегда прямая.

**Определение 6.3.6.** Линейное преобразование  $\varphi$   $n$ -мерного векторного пространства  $V$  над полем  $F$  называется *диагонализируемым*, если в некотором базисе пространства  $V$  его матрица диагональна. Матрица  $A \in M_n(F)$  называется *диагонализируемой*, если она подобна над  $F$  диагональной матрице.

**Предложение 6.3.4.** Пусть  $\varphi$  — линейное преобразование конечно-мерного векторного пространства  $V$  над полем  $F$ . Следующие утверждения эквивалентны.

1. Преобразование  $\varphi$  диагонализируемо.
2. Пространство  $V$  обладает базисом, составленным из собственных векторов преобразования  $\varphi$ .
3.  $\text{Sp}(\varphi) \subseteq F$  и  $V = \bigoplus_{\lambda \in \text{Sp}(\varphi)} \text{Ker}(\varphi - \lambda\varepsilon)$ .

УПРАЖНЕНИЕ 6.3.6. Доказать предложение 6.3.4.

УПРАЖНЕНИЕ 6.3.7. Доказать, что линейное преобразование, характеристический многочлен которого не имеет кратных корней, диагонализуемо над полем, содержащим спектр этого преобразования.

ПРИМЕРЫ. 1. Пусть  $\varphi$  — осевая симметрия относительно оси абсцисс в декартовой системе координат на плоскости. Орты  $e_1$  и  $e_2$  являются собственными векторами преобразования  $\varphi$  и составляют базис пространства, в котором матрица  $\varphi$  диагональна.

2. Пусть  $\varphi$  — поворот на угол  $\frac{\pi}{2}$  относительно начала координат декартовой плоскости. В базисе из ортов  $e_1$  и  $e_2$  матрица этого оператора имеет вид

$$[\varphi] = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Следовательно, характеристический многочлен  $f_\varphi(x)$  равен  $x^2 + 1$ . Его корни  $i, -i$  не лежат в поле  $\mathbb{R}$ . Поэтому оператор  $\varphi$  (и его матрица) не диагонализуем над  $\mathbb{R}$ . Однако, если рассматривать ту же матрицу как матрицу из  $M_2(\mathbb{C})$ , то она оказывается подобной диагональной матрице

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

Следовательно, в соответствии с нашим определением она диагонализуема над  $\mathbb{C}$ .

3. Пусть  $\varphi$  — оператор дифференцирования пространства  $\mathbb{R}_1[x]$ . В



базе  $x, 1$  его матрица имеет вид

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

Характеристический многочлен  $f_\varphi(x)$  равен  $x^2$ , число  $0$  — его единственный корень кратности  $2$  — лежит в  $\mathbb{R}$ . Подпространство  $\text{Ker } \varphi$  собственных векторов, соответствующих этому числу, очевидно, совпадает с множеством всех многочленов нулевой степени и не равно всему пространству  $V$ . Таким образом, оператор  $\varphi$  и его матрица не диагонализуемы.

**УПРАЖНЕНИЕ 6.3.8.** *Найти базисы подпространств собственных векторов линейного преобразования  $\varphi$ , заданного в некотором базисе матрицей*

$$[\varphi] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix},$$

*и определить, является ли  $\varphi$  диагонализуемым.*

## § 6.4. Корневые подпространства и корневое разложение

Напомним, что наша основная задача состоит в том, чтобы для данного линейного преобразования векторного пространства найти базис этого пространства, в котором матрица преобразования имеет наиболее простой вид. Как следует из результатов предыдущего параграфа, если линейное преобразование имеет базис из собственных векторов, то задача решена, поскольку существует базис, в котором матрица преобразования диагональна. К сожалению, как показывает последний пример с оператором дифференцирования из того же параграфа, линейное преобразование может не иметь базиса из собственных векторов даже в том случае, когда все корни его характеристического многочлена лежат в поле, над которым определено векторное пространство. В этом параграфе мы введём понятие корневого вектора, в некотором смысле обобщающее понятие собственного вектора, и покажем, что в случае, когда спектр линейного оператора содержится в поле, над которым определено векторное пространство, пространство раскладывается в прямую сумму корневых, т. е. состоящих из корневых векторов, подпространств.

**Определение 6.4.1.** Пусть  $\lambda$  — собственное число линейного преобразования  $\varphi$  векторного пространства  $V$  над полем  $F$ . Ненулевой век-

тор  $u \in V$  называется *корневым вектором* преобразования  $\varphi$  с собственным числом  $\lambda$ , если существует натуральное число  $k$ , такое, что  $u(\varphi - \lambda\varepsilon)^k = 0$ . Наименьшее натуральное число  $k$  с этим условием называется *высотой* корневого вектора.

**ЗАМЕЧАНИЕ.** Из определения вытекает, что любой собственный вектор линейного преобразования является корневым вектором высоты 1 с тем же собственным числом. Удобно, хотя и не совсем корректно, считать нулевой вектор корневым вектором высоты 0 (для любого собственного числа  $\lambda$ ).

**ПРИМЕР.** Поскольку  $(n + 1)$ -ая производная от любого многочлена степени  $n$  равна нулю, каждый многочлен есть корневой вектор с собственным числом 0 оператора дифференцирования пространства многочленов, причём высота многочлена, как корневого вектора, равна  $n + 1$ , где  $n$  — его степень.

Поскольку образ и ядро линейного преобразования инвариантны относительно него, для любого линейного оператора  $\psi$  и любых чисел  $k, m \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ , таких, что  $k < m$ , выполняются очевидные включения  $V\psi^k \supseteq V\psi^m$  и  $\text{Ker} \psi^k \subseteq \text{Ker} \psi^m$ . Пусть теперь пространство  $V$  конечномерно и  $\lambda \in F$  — собственное число оператора  $\varphi \in \mathcal{L}(V)$ . В этом случае включение  $V \supset V(\varphi - \lambda\varepsilon)$  обязательно строгое, так как оператор  $\varphi - \lambda\varepsilon$  вырожден на  $V$ . Составим ряд из последовательно вложенных образов  $V$  под действием  $\varphi - \lambda\varepsilon$ :

$$V \supset V(\varphi - \lambda\varepsilon) \supset \dots \supset V(\varphi - \lambda\varepsilon)^k = V(\varphi - \lambda\varepsilon)^{k+1} = \dots = V(\varphi - \lambda\varepsilon)^m \quad (1)$$

Пространство  $V$  имеет конечную размерность, поэтому строгие вложения не могут продолжаться бесконечно. Значит, на некотором  $k$ -ом шаге выполнится равенство  $V(\varphi - \lambda\varepsilon)^k = V(\varphi - \lambda\varepsilon)^{k+1}$ . Это равенство означает, что сужение оператора  $\varphi - \lambda\varepsilon$  на подпространство  $V(\varphi - \lambda\varepsilon)^k$  является невырожденным оператором. Поэтому для любого  $m > k$  выполняется  $V(\varphi - \lambda\varepsilon)^k = V(\varphi - \lambda\varepsilon)^m$ . Мы будем говорить, что ряд (1) *стабилизируется* на  $k$ -ом шаге. Рассматривая теперь последовательные вложения ядер операторов вида  $(\varphi - \lambda\varepsilon)^i$ , получаем ряд

$$0 \subset \text{Ker}(\varphi - \lambda\varepsilon) \subset \dots \subset \text{Ker}(\varphi - \lambda\varepsilon)^k = \text{Ker}(\varphi - \lambda\varepsilon)^{k+1} = \dots = \text{Ker}(\varphi - \lambda\varepsilon)^m \quad (2)$$

Этот ряд также стабилизируется на  $k$ -ом шаге, что следует из теоремы 6.2.1 о сумме ранга и дефекта линейного преобразования. Поскольку

каждый корневой вектор высоты  $i$ , соответствующий собственному числу  $\lambda$ , по определению лежит в  $\text{Ker}(\varphi - \lambda\varepsilon)^i$ , получается, что все (любой высоты) корневые векторы, соответствующие  $\lambda$ , образуют подпространство  $\text{Ker}(\varphi - \lambda\varepsilon)^k$ , на котором стабилизируется ряд (2). Таким образом, корректно следующее определение.

**Определение 6.4.2.** Пусть  $V$  — конечномерное векторное пространство над полем  $F$ ,  $\lambda$  — собственное число линейного преобразования  $\varphi$  пространства  $V$ . Пусть  $k = k(\lambda)$  — наименьшее натуральное число с условием  $V(\varphi - \lambda\varepsilon)^k = V(\varphi - \lambda\varepsilon)^{k+1}$ . Подпространство  $U_\lambda = \text{Ker}(\varphi - \lambda\varepsilon)^k$  называется *корневым подпространством* преобразования  $\varphi$  пространства  $V$ , соответствующим собственному числу  $\lambda$ . Число  $k$  называется *высотой* корневого подпространства.

**ЗАМЕЧАНИЕ.** Высота корневого подпространства равна максимальной высоте корневого вектора.

**ПРИМЕР.** Пусть  $\varphi$  — оператор дифференцирования на пространстве  $V = \mathbb{R}_n[x]$  многочленов степени не выше  $n$ . Его характеристический многочлен  $f_\varphi(x)$  равен  $x^{n+1}$ , поэтому  $0$  — единственный корень этого многочлена кратности  $n + 1$ . В этом примере  $V = U_0 = \text{Ker} \varphi^{n+1}$  и  $n + 1$  — высота корневого подпространства  $U_0$ .

**Теорема 6.4.1** (о корневом разложении). Пусть  $V$  —  $n$ -мерное векторное пространство над полем  $F$ ,  $\varphi$  — линейное преобразование пространства  $V$ , спектр которого  $\text{Sp}(\varphi) = \{\lambda_1, \dots, \lambda_s\}$  лежит в поле  $F$ , и для каждого  $i = 1, \dots, s$  корневое подпространство  $U_i = \text{Ker}(\varphi - \lambda_i\varepsilon)^{k_i}$  имеет высоту  $k_i$ . Тогда  $V = \bigoplus_{i=1}^s U_i$  и для каждого  $i = 1, \dots, s$  выполняется  $k_i \leq \dim U_i = n_i$ , где  $n_i$  — кратность корня  $\lambda_i$  в характеристическом многочлене преобразования  $\varphi$ .

**ДОКАЗАТЕЛЬСТВО.** Мы будем доказывать теорему индукцией по размерности пространства  $V$ . При  $n = 1$  утверждение теоремы очевидно выполняется. В дальнейшем будем предполагать, что для любого пространства, размерность которого меньше  $n$ , теорема доказана.

Обозначим для краткости  $\lambda = \lambda_1$ ,  $k = k_1$ ,  $U = U_1 = \text{Ker}(\varphi - \lambda\varepsilon)^k$  и  $W = V(\varphi - \lambda\varepsilon)^k$ . По определению корневого подпространства

$$W = V(\varphi - \lambda\varepsilon)^k = V(\varphi - \lambda\varepsilon)^{k+1} = W(\varphi - \lambda\varepsilon).$$

В силу теоремы 6.2.2 оператор  $\varphi - \lambda\varepsilon$  невырожден на  $W$ . Это значит, что невырождена на  $W$  и любая степень этого оператора. Следовательно,  $U \cap W = 0$ . Поскольку  $\dim U + \dim W = \dim V$ , пространство  $V$  раскладывается в прямую сумму подпространств  $U$  и  $W$ . Оба подпространства

$U$  и  $W$   $\varphi$ -инвариантны, так как операторы  $\varphi$  и  $(\varphi - \lambda\varepsilon)^k$  перестановочны. Пусть  $\sigma = \varphi|_U$  и  $\tau = \varphi|_W$ . По теореме 6.3.1 в базисе пространства  $V$ , составленном из базисов подпространств  $U$  и  $W$ , матрица преобразования  $\varphi$  имеет вид

$$[\varphi] = \begin{pmatrix} [\sigma] & 0 \\ 0 & [\tau] \end{pmatrix}.$$

Кроме того, из предложения 6.3.3 следует, что для характеристического многочлена преобразования  $\varphi$  имеет место разложение  $f_\varphi = f_\sigma \cdot f_\tau$ , где  $f_\sigma$  и  $f_\tau$  — характеристические многочлены сужений  $\sigma$  и  $\tau$  соответственно.

Теперь докажем, что  $f_\sigma(x) = (x - \lambda)^{n_1}$ , где  $n_1$  — кратность корня  $\lambda = \lambda_1$  в характеристическом многочлене  $f_\varphi$ . Предположим, что линейный многочлен  $x - \mu$  делит  $f_\sigma$ . Тогда существует ненулевой вектор  $u \in U$ , такой, что  $u\sigma = u\varphi = \mu u$ . Поэтому  $u(\varphi - \lambda\varepsilon) = (\mu - \lambda)u$ . Поскольку  $U$  — корневое подпространство с собственным числом  $\lambda$ , выполняется  $0 = u(\varphi - \lambda\varepsilon)^k = (\mu - \lambda)^k u$ . Следовательно,  $(\mu - \lambda)^k = 0$ . Отсюда  $\mu = \lambda$ . Следовательно,  $f_\sigma$  делит  $(x - \lambda)^{n_1}$ . С другой стороны, как мы уже выяснили, оператор  $\tau - \lambda\varepsilon = (\varphi - \lambda\varepsilon)|_W$  невырожден на  $W$ . Поэтому  $x - \lambda$  не делит  $f_\tau$ . Таким образом,  $f_\sigma(x) = (x - \lambda)^{n_1}$ . Из этого равенства сразу следует, что кратность  $n_1$  корня  $\lambda_1$  в характеристическом многочлене  $f_\varphi$  совпадает с размерностью корневого подпространства  $U_1$ , соответствующего этому корню. Кроме того, поскольку в ряду (2) после каждого строгого включения размерность подпространства увеличивается по крайней мере на единицу, высота  $k_1$  корневого подпространства  $U_1$  не превосходит размерности этого подпространства, т. е.  $k_1 \leq \dim U_1$ .

Рассмотрим теперь оператор  $\tau$  на пространстве  $W$ . Поскольку  $f_\tau = f_\varphi/f_\sigma$  и  $f_\sigma(x) = (x - \lambda_1)^{n_1}$ , выполняется равенство

$$f_\tau(x) = \prod_{i=2}^s (x - \lambda_i)^{n_i}.$$

Пространство  $W$ , размерность которого меньше размерности  $V$ , и оператор  $\tau$  удовлетворяют всем условиям теоремы. Поэтому по предположению индукции имеем  $W = \bigoplus_{i=2}^s U'_i$ , где  $U'_i = \text{Ker}(\tau - \lambda_i\varepsilon)^{k'_i}$  и  $k'_i \leq \dim U'_i = n_i$ . Нам осталось доказать, что для  $i = 2, \dots, s$  подпространства  $U_i$  и  $U'_i$  совпадают и  $k_i = k'_i$ . Поскольку на подпространстве  $W$  операторы  $\varphi$  и  $\tau = \varphi|_W$  действуют одинаково, для каждого  $i = 2, \dots, s$  выполняются равенства  $U'_i = U_i \cap W$ . Следовательно, для завершения доказательства теоремы достаточно показать, что  $U_i \subseteq W$  для любого  $i = 2, \dots, s$ .

Пусть для некоторого  $i \in \{2, \dots, s\}$  вектор  $v$  лежит в  $U_i = \text{Ker}(\varphi - \lambda_i \varepsilon)^{k_i}$ . Поскольку  $V = U \oplus W$ , существуют векторы  $u \in U$  и  $w \in W$ , такие, что  $v = u + w$ . Тогда

$$0 = v(\varphi - \lambda_i \varepsilon)^{k_i} = u(\varphi - \lambda_i \varepsilon)^{k_i} + w(\varphi - \lambda_i \varepsilon)^{k_i}.$$

Положим  $u_1 = u(\varphi - \lambda_i \varepsilon)^{k_i}$  и  $w_1 = w(\varphi - \lambda_i \varepsilon)^{k_i}$ . Поскольку операторы  $(\varphi - \lambda_i \varepsilon)^{k_i}$  и  $(\varphi - \lambda_1 \varepsilon)^{k_1}$  перестановочны, подпространства  $U$  и  $W$  инвариантны относительно оператора  $(\varphi - \lambda_i \varepsilon)^{k_i}$ . Поэтому  $u_1 \in U$  и  $w_1 \in W$ . Так как сумма подпространств  $U$  и  $W$  прямая, из равенства  $0 = u_1 + w_1$  следует, что  $u_1 = w_1 = 0$ . Но тогда  $u \in \text{Ker}(\varphi - \lambda_i \varepsilon)^{k_i}$ . Поскольку многочлен  $x - \lambda_i$  не делит  $f_\sigma(x) = (x - \lambda_1)^{n_1}$ , оператор  $\varphi - \lambda_i \varepsilon$  невырожден на  $U$ , а значит, невырожден на нём и оператор  $(\varphi - \lambda_i \varepsilon)^{k_i}$ . Поэтому из равенства  $0 = u_1 = u(\varphi - \lambda_i \varepsilon)^{k_i}$  вытекает, что  $u = 0$ . Таким образом,  $v \in W$ , а значит,  $U_i = U_i \cap W = U'_i$  и, в частности,  $k_i = k'_i$  для любого  $i = 2, \dots, s$ .  $\square$

**Следствие.** В условиях теоремы 6.4.1 существует базис пространства  $V$ , составленный из базисов корневых подпространств  $U_i$ ,  $i = 1, \dots, s$ , в котором матрица преобразования  $\varphi$  имеет клеточно диагональный вид:

$$[\varphi] = \begin{pmatrix} [\varphi|_{U_1}] & & 0 \\ & \ddots & \\ 0 & & [\varphi|_{U_s}] \end{pmatrix}, \quad (3)$$

причём количество клеток равно количеству различных корней в спектре  $\varphi$ , а размер каждой клетки равен кратности соответствующего корня в характеристическом многочлене.

**ЗАМЕЧАНИЕ.** Из доказательства теоремы вытекает практический метод отыскания баз корневых подпространств (предполагается, что собственные числа оператора уже известны и лежат в поле определения пространства), основанный на последовательном *отщеплении* корневых подпространств.

**УПРАЖНЕНИЕ 6.4.1.** Пусть линейное преобразование  $\varphi$  пространства  $V$  задано в некотором базисе матрицей  $[\varphi] = A$ . Обосновать следующий поэтапный метод поиска баз корневых подпространств. Предположим, что перед началом  $i$ -ого этапа этого процесса нам известны базы корневых подпространств  $U_1, \dots, U_{i-1}$ , а также база подпространства  $W = V(\varphi - \lambda_1 \varepsilon)^{k_1} \dots (\varphi - \lambda_{i-1} \varepsilon)^{k_{i-1}}$  (из доказательства теоремы следует, что  $V = U_1 \oplus \dots \oplus U_{i-1} \oplus W$  и  $W = U_i \oplus \dots \oplus U_s$ ). Обозначим через

$N = A - \lambda_i E$  матрицу преобразования  $\varphi - \lambda_i \varepsilon$ , а через  $B_0$  — матрицу, составленную из строк базиса подпространства  $W$ . Проведём цепочку преобразований:

$$(B_0 \mid B_0 N) \rightarrow (B_1 \mid C_1) \rightarrow (B_1 \mid C_1 \mid C_1 N) \rightarrow (B_2 \mid * \mid C_2) \rightarrow \dots \\ \dots \rightarrow (B_k \mid * \mid \dots \mid * \mid C_k),$$

где на каждом шаге мы пользуемся элементарными преобразованиями строк, матрицы  $C_j$  ступенчатые для всех  $j = 1, \dots, k$  и число нулевых строк матрицы  $C_k$  равно кратности корня  $\lambda_i$  в характеристическом многочлене преобразования  $\varphi$ . Тогда строки матрицы  $B_k$ , стоящие напротив нулевых строк матрицы  $C_k$ , образуют базис корневого подпространства  $U_i = \text{Ker}(\varphi - \lambda_i \varepsilon)^{k_i}$ , число шагов  $k$  равно высоте  $k_i$  подпространства  $U_i$ , а ненулевые строки матрицы  $C_k$  образуют базис пространства  $W' = W(\varphi - \lambda_i \varepsilon)^{k_i} = U_{i+1} \oplus \dots \oplus U_s$ . Переходим к следующему этапу, переобозначая  $N = A - \lambda_{i+1} E$  и  $B_0 = C_k$  (более точно,  $B_0$  — матрица, составленная из строк базиса пространства  $W'$ ).

**ЗАМЕЧАНИЕ.** Эффективность этого метода основана на том, что количество строк в исходной матрице  $B_0$  уменьшается от этапа к этапу, что сокращает вычисления. Более того, если число различных характеристических корней преобразования равно  $s$ , то последним этапом будет  $(s - 1)$ -ый, поскольку ненулевые строки матрицы  $C_k$ , получившейся в результате этого этапа, образуют базис подпространства  $V(\varphi - \lambda_1 \varepsilon)^{k_1} \dots (\varphi - \lambda_{s-1} \varepsilon)^{k_{s-1}} = \text{Ker}(\varphi - \lambda_s \varepsilon)^{k_s}$ , т. е. последнего корневого подпространства  $U_s$ .

**УПРАЖНЕНИЕ 6.4.2.** Для преобразования  $\varphi$  из упражнения 6.3.8 найти базисы корневых подпространств. Записать матрицу  $\varphi$  в базисе пространства, составленном из найденных базисов.

**УПРАЖНЕНИЕ 6.4.3.** Пусть линейный оператор  $\varphi$  конечномерного векторного пространства удовлетворяет тождеству  $\varphi^2 = \varphi$ . Используя теорему о корневом разложении, доказать, что  $\varphi$  — оператор проектирования на подпространство  $\text{Ker}(\varphi - \varepsilon)$  параллельно подпространству  $\text{Ker} \varphi$ .

## § 6.5. Нильпотентные преобразования

Заметим, что на корневом подпространстве  $U_\lambda = \text{Ker}(\varphi - \lambda \varepsilon)^k$  оператор  $\psi = \varphi - \lambda \varepsilon$  обладает следующим замечательным свойством:

$U_\lambda \psi^k = 0$ . Поскольку  $\varphi = \psi + \lambda \varepsilon$ , действие оператора  $\varphi$  на подпространстве  $U_\lambda$  несложно восстановить, зная, как оператор  $\psi$  действует на  $U_\lambda$ . Поэтому в этом параграфе мы подробно изучим линейные преобразования, которые в некоторой степени превращаются в нулевое преобразование.

**Определение 6.5.1.** Линейное преобразование  $\psi$  векторного пространства  $V$  называется *нильпотентным*, если найдётся  $k \in \mathbb{N}$ , такое, что  $\psi^k = 0$ .

ПРИМЕРЫ. 1. Нулевое преобразование nilьпотентно.

2. Оператор дифференцирования пространства многочленов ограниченной степени nilьпотентен.

3. Если  $\varphi$  — произвольное линейное преобразование конечномерного векторного пространства и  $\lambda$  — его собственное число, то сужение оператора  $\varphi - \lambda \varepsilon$  на корневое подпространство  $U_\lambda$  — nilьпотентный оператор.

**Предложение 6.5.1.** *Линейное преобразование  $\psi$  конечномерного векторного пространства nilьпотентно тогда и только тогда, когда  $\text{Sp}(\psi) = \{0\}$ .*

ДОКАЗАТЕЛЬСТВО. Следует из теоремы о корневом разложении.  $\square$

**Определение 6.5.2.** Пусть  $\psi$  — nilьпотентное преобразование пространства  $V$ ,  $v \in V$ . Упорядоченный набор векторов  $v_0, v_1, \dots, v_{l-1}$  называется *ниль-слоем длины  $l$  с началом в  $v$* , если  $v_0 = v$ ,  $v_i = v_{i-1}\psi = v\psi^i$  для  $i = 1, \dots, l-1$  и  $v_{l-1}\psi = 0$ . Подпространство  $U = \langle v_0, v_1, \dots, v_{l-1} \rangle$ , натянутое на векторы nilь-слоя, называется *циклическим*.

ЗАМЕЧАНИЕ. Поскольку  $\psi$  nilьпотентен, для каждого вектора  $v \in V$  можно построить nilь-слой конечной длины с началом в  $v$ .

ЗАМЕЧАНИЕ. В определении не предполагается, что  $v_i \neq 0$  при  $i < l$ .

ПРИМЕР. Пусть  $V = \mathbb{R}_n[x]$ ,  $v = x^2 + 2x + 3$  и  $\psi$  — оператор дифференцирования. Тогда  $v_0 = x^2 + 2x + 3$ ,  $v_1 = 2x + 2$ ,  $v_2 = 2$  — nilь-слой длины 3 с началом в  $v$ .

**Определение 6.5.3.** Пусть  $\psi$  — nilьпотентное преобразование. Набор векторов называется *жордановым* относительно  $\psi$ , если он состоит из (одного или нескольких) nilь-слоёв. Базис пространства, являющийся жордановым набором векторов, называется *жордановым базисом* пространства относительно преобразования  $\psi$ .

**Определение 6.5.4.** Жорданова таблица — способ записи жорданова набора векторов в виде таблицы, строки которой являются ниль-слоями, выровненными по правому краю. Элементарными преобразованиями жордановой таблицы называются:

- 1) перестановка ниль-слоёв;
- 2) умножение ниль-слоя на ненулевой скаляр;
- 3) сдвиг ниль-слоя вправо на одну позицию, если последний вектор ниль-слоя является нулевым;
- 4) прибавление ко всем векторам ниль-слоя умноженных на один и тот же скаляр векторов другого ниль-слоя, имеющего большую или равную длину, стоящих под или над векторами исходного ниль-слоя.

$$\begin{array}{|c|c|c|c|c|c|c|} \hline u & u\psi & \dots & u\psi^k & u\psi^{k+1} & \dots & u\psi^{l-1} \\ \hline & & & v & v\psi & \dots & u\psi^{m-1} \\ \hline \end{array} \rightarrow \text{преобразование 4-го типа}$$

$$\rightarrow \begin{array}{|c|c|c|c|c|c|c|} \hline u & u\psi & \dots & u\psi^k & u\psi^{k+1} & \dots & u\psi^{l-1} \\ \hline & & & v + \alpha u\psi^k & v\psi + \alpha u\psi^{k+1} & \dots & v\psi^{m-1} + \alpha u\psi^{l-1} \\ \hline \end{array}$$

**Предложение 6.5.2.** 1. Линейная оболочка векторов жордановой таблицы не изменяется при её элементарных преобразованиях.

2. Свойство таблицы быть жордановой не меняется при её элементарных преобразованиях.

**ДОКАЗАТЕЛЬСТВО.** 1. Доказательство аналогично рассуждению о сохранении строчного ранга матрицы при элементарных преобразованиях в параграфе 4.1.

2. Стоит проверить лишь сохранение свойства таблицы быть жордановой при преобразовании 4-го типа, поскольку для преобразований остальных типов всё очевидно. При преобразовании 4-го типа (см. рисунок) ниль-слой вида  $v, v\psi, \dots, v\psi^{m-1}$  заменяется на упорядоченный набор векторов  $v + \alpha u\psi^k, v\psi + \alpha u\psi^{k+1}, \dots, v\psi^{m-1} + \alpha u\psi^{l-1}$ , который является ниль-слоем, так как  $v\psi^i + \alpha u\psi^{k+i} = (v + \alpha u\psi^k)\psi^i$  для любого  $i$ . □

**Предложение 6.5.3.** Если набор векторов, составляющих правый столбец жордановой таблицы, линейно независим, то и весь жорданов набор, из которого составлена жорданова таблица, линейно независим.

**ДОКАЗАТЕЛЬСТВО.** Начнём с небольшого предварительного рассуждения. Пусть набор векторов  $v, v\psi, \dots, v\psi^{l-1}$  является ниль-слоем



длины  $l$ . Предположим, что  $\alpha_0 v + \dots + \alpha_k v \psi^k + \dots + \alpha_{l-1} v \psi^{l-1} = \alpha_k v \psi^k + \dots + \alpha_{l-1} v \psi^{l-1}$  — линейная комбинация векторов этого набора, в которой все коэффициенты с индексом, меньшим  $k$ , равны 0. Тогда, положив  $m = l-1-k$ , получим, что  $(\alpha_0 v + \dots + \alpha_k v \psi^k + \dots + \alpha_{l-1} v \psi^{l-1}) \psi^m = \alpha_k v \psi^{l-1}$ , так как по определению ниль-слоя  $(v \psi^i) \psi^m = 0$  при  $i > k$ .

Предположим теперь, что утверждение предложения неверно. Тогда найдётся нетривиальная линейная комбинация векторов жордановой таблицы, равная 0. Сгруппировав слагаемые в этой линейной комбинации по ниль-слоям, получим равенство:

$$0 = \sum_{i=1}^s \left( \sum_{j=0}^{l_i-1} \alpha_{ij} v_i \psi^j \right),$$

где  $v_1, \dots, v_s$  — векторы, с которых начинаются ниль-слои жордановой таблицы, а  $l_1, \dots, l_s$  — длины этих слоёв. Теперь для каждого  $i \in \{1, \dots, s\}$  выберем число  $k_i$  так, чтобы в линейной комбинации  $\sum_{j=0}^{l_i-1} \alpha_{ij} v_i \psi^j$  коэффициент  $\alpha_{ik_i}$  не равнялся 0, а коэффициенты  $\alpha_{ij}$  при  $j < k_i$  равнялись 0. Если такого числа нет, т.е. для данного  $i$  все  $\alpha_{ij}$  равны 0, положим  $k_i = l_i - 1$ . Для каждого  $i = 1, \dots, s$  положим  $m_i = l_i - 1 - k_i$ . Пусть  $m = \max\{m_1, \dots, m_s\}$  и  $r_1, \dots, r_t$  — те числа из множества  $\{1, \dots, s\}$ , для которых  $m_{r_1} = \dots = m_{r_t} = m$ . Переставив при необходимости ниль-слои между собой, можно добиться того, чтобы  $m_1 = \dots = m_t = m$ . Тогда

$$0 = 0 \psi^m = \left( \sum_{i=1}^s \left( \sum_{j=0}^{l_i-1} \alpha_{ij} v_i \psi^j \right) \right) \psi^m = \alpha_{1k_1} v_1 \psi^{l_1-1} + \dots + \alpha_{tk_t} v_t \psi^{l_t-1}.$$

Мы получили равную нулю нетривиальную линейную комбинацию векторов, которые образуют поднабор набора векторов правого столбца жордановой таблицы, что противоречит условию.  $\square$

**ЗАМЕЧАНИЕ.** Из предложения 6.5.3, в частности, следует, что все векторы ниль-слоя, оканчивающегося ненулевым вектором, образуют линейно независимый набор.

**Теорема 6.5.1** (о жордановом базисе для нильпотентного линейного преобразования). *Конечномерное векторное пространство  $V$  относительно нильпотентного линейного преобразования  $\psi$  имеет жорданов базис. Для каждого  $k \in \mathbb{N}$  число  $s_k$  ниль-слоёв длины  $k$  не зависит от выбора базиса и равно  $s_k = r_{k-1} - 2r_k + r_{k+1}$ , где  $r_i = \dim V \psi^i$ .*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $e_1, \dots, e_n$  — некоторый базис пространства  $V$ . Составим жорданову таблицу из ниль-слоёв, начинающихся в векторах этого базиса. Очевидно, что линейная оболочка данной жордановой таблицы совпадает со всем пространством. Используя перестановки слоёв жордановой таблицы, упорядочим их по убыванию длины. Предположим, что векторы  $u_1, \dots, u_n$ , составляющие правый столбец жордановой таблицы, линейно зависимы. Тогда в силу критерия линейной зависимости (предложение 3.2.1) в этом столбце найдётся вектор  $u_k$ , который выражается через векторы  $u_1, \dots, u_{k-1}$ , стоящие в таблице над ним. Поскольку длины первых  $k - 1$  ниль-слоёв по крайней мере не меньше, чем длина  $k$ -го слоя, элементарными преобразованиями типа 4 можно занулить вектор  $u_k$ . Сдвинув  $k$ -й слой на этот нулевой вектор, получим таблицу, состоящую из меньшего числа векторов. В силу предложения 6.5.2 эта таблица снова будет жордановой, а её линейная оболочка по-прежнему будет совпадать со всем пространством. Продолжая указанный процесс, мы за конечное число шагов получим жорданову таблицу, в которой набор векторов правого столбца линейно независим. Тогда из предложения 6.5.3 вытекает, что и весь жорданов набор линейно независим, а значит, образует искомый базис пространства  $V$ .

Если  $s_k$  — число ниль-слоёв длины  $k$  жорданова базиса  $B$ , то размерность пространства  $V$ , очевидно, равна  $s_1 + 2s_2 + \dots + ts_t$ , где  $t$  — наибольшая длина ниль-слоя в жордановом базисе. Рассмотрим набор векторов  $B\psi$ , состоящий из образов векторов базиса  $B$  под действием преобразования  $\psi$ . Из определения ниль-слоя вытекает, что набор  $B\psi$  является поднабором набора  $B$ , состоящим из всех векторов жордановой таблицы, за исключением векторов, с которых начинаются ниль-слои. Поскольку любой поднабор линейно независимого набора снова линейно независим и линейная оболочка набора  $B\psi$  есть образ  $V\psi$  преобразования  $\psi$ , набор  $B\psi$  — базис пространства  $V\psi$ . Поэтому размерность пространства  $V\psi$  равна  $s_2 + 2s_3 + \dots + (t - 1)s_t$ . Рассуждая аналогично при всех  $i = 0, \dots, t$ , получим следующую систему равенств для  $r_i = \dim V\psi^i$ :

$$\begin{aligned} r_0 &= s_1 + 2s_2 + \dots + ts_t \\ r_1 &= s_2 + 2s_3 + \dots + (t - 1)s_t \\ &\dots \\ r_i &= s_{i+1} + 2s_{i+2} + \dots + (t - i)s_t \\ &\dots \\ r_{t-1} &= s_t. \end{aligned} \tag{1}$$

Заметим, что  $r_i = 0$  при  $i \geq t$ . Вычитая из каждого равенства в системе (1) следующее, получим систему равенств:

$$\begin{aligned} r_0 - r_1 &= s_1 + s_2 + \dots + s_t \\ r_1 - r_2 &= s_2 + s_3 + \dots + s_t \\ &\dots \\ r_{i-1} - r_i &= s_i + s_{i+1} + \dots + s_t \\ r_i - r_{i+1} &= s_{i+1} + s_{i+2} + \dots + s_t \\ &\dots \\ r_{t-2} - r_{t-1} &= s_{t-1} + s_t \\ r_{t-1} &= s_t \end{aligned} \quad (2)$$

Вычитая из каждого равенства в системе (2) следующее и меняя левые и правые части равенств местами, получим, что для каждого  $i = 1, \dots, t$  имеет место равенство  $s_i = r_{i-1} - 2r_i + r_{i+1}$ . Поскольку размерности  $r_i$  пространств  $V\psi^i$  не зависят от выбора базиса, не зависят от него и числа  $s_i$ , выражающие количество ниль-слоёв длины  $i$  в жордановом базисе.  $\square$

**Следствие.** Конечномерное векторное пространство  $V$  относительно нильпотентного преобразования  $\psi$  разлагается в прямую сумму  $\psi$ -инвариантных циклических подпространств  $W_i$ ,  $i = 1, \dots, m$ :  $V = \bigoplus_{i=1}^m W_i$ . В базисе пространства  $V$ , составленном из ниль-слоёв, на которые натянуты подпространства  $W_i$ , матрица преобразования  $\psi$  имеет клеточно диагональный вид:

$$[\psi] = \begin{pmatrix} [\psi|_{W_1}] & & 0 & & \\ & \ddots & & & \\ & & 0 & & \\ & & & \ddots & \\ & & 0 & & [\psi|_{W_m}] \end{pmatrix}, \text{ где } [\psi|_{W_i}] = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix},$$

и размер матрицы  $[\psi|_{W_i}]$  равен длине ниль-слоя, соответствующего циклическому подпространству  $W_i$ .

**ДОКАЗАТЕЛЬСТВО.** Из доказанной нами теоремы вытекает, что пространство  $V$  относительно нильпотентного оператора  $\psi$  обладает жордановым базисом, состоящим из ниль-слоёв. Циклические подпространства  $W_i$ , натянутые на ниль-слои, очевидно,  $\psi$ -инвариантны. Поэтому по теореме 6.3.1 в соответствующем базисе матрица оператора  $\psi$  клеточно диагональна. Вид клетки, соответствующей сужению оператора  $\psi$  на циклическое подпространство, вытекает из определения ниль-слоя.  $\square$

**ЗАМЕЧАНИЕ.** Матрицу из следствия мы будем называть *жордановой формой* матрицы нильпотентного преобразования, а клетки, из которых она состоит, *жордановыми* клетками.

**УПРАЖНЕНИЕ 6.5.1.** Доказать, что если максимальная длина ниль-слоя нильпотентного преобразования  $\psi$  (максимальный размер жордановой клетки в жордановой форме матрицы  $[\psi]$ ) равна  $t$ , то  $\psi^t = 0$ , а  $\psi^{t-1} \neq 0$ .

**ЗАМЕЧАНИЕ.** Практический способ отыскания жорданова базиса нильпотентного преобразования основан на тех же соображениях, что и доказательство теоремы 6.5.1. Полезное с точки зрения уменьшения выкладок упрощение состоит лишь в том, чтобы строить ниль-слои один за другим, последовательно добиваясь линейной независимости векторов из правого столбца.

**УПРАЖНЕНИЕ 6.5.2.** Для линейного преобразования  $\psi$ , заданного в некотором базисе матрицей

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

найти его жорданов базис и жорданову форму.

**УПРАЖНЕНИЕ 6.5.3.** Найти жорданов базис и жорданову форму оператора дифференцирования в пространстве  $V = \mathbb{R}_n[x]$  многочленов степени не выше  $n$ .

## § 6.6. Жорданова форма матрицы линейного преобразования

**Определение 6.6.1.** Пусть  $\varphi$  — линейное преобразование конечно-мерного векторного пространства  $V$  над полем  $F$ , содержащим спектр преобразования  $\varphi$ . *Жордановым базисом* векторного пространства  $V$  относительно преобразования  $\varphi$  называется базис, составленный из жордановых базисов корневых подпространств  $U_i = \text{Ker}(\varphi - \lambda_i \varepsilon)^{k_i}$  относительно преобразований  $\psi_i = (\varphi - \lambda_i \varepsilon)|_{U_i}$ .

**Теорема 6.6.1** (Жордан). Пусть  $\varphi$  — линейное преобразование конечно-мерного векторного пространства  $V$  над полем  $F$ , содержа-

щим спектр преобразования  $\varphi$ . Тогда существует жорданов базис пространства  $V$  относительно преобразования  $\varphi$ . В этом базисе матрица преобразования  $\varphi$  имеет клеточно диагональный вид:

$$[\varphi] = \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_m \end{pmatrix}, \text{ где } J_k = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & \lambda \end{pmatrix}$$

для некоторого  $\lambda \in \text{Sp}(\varphi)$ , и размер клетки равен длине ниль-слоя соответствующего циклического подпространства.

**ДОКАЗАТЕЛЬСТВО.** По теореме 6.4.1 о корневом разложении в условиях нашей теоремы существует базис пространства  $V$ , состоящий из базисов корневых подпространств. Пусть  $U$  — одно из этих корневых подпространств, соответствующее собственному числу  $\lambda$ . Тогда сужение  $\psi = (\varphi - \lambda\varepsilon)|_U$  является нильпотентным линейным преобразованием пространства  $U$ . В силу следствия из теоремы 6.5.1 подпространство  $U$  есть прямая сумма циклических подпространств, соответствующих ниль-слоям некоторого жорданова базиса преобразования  $\psi$ . Пусть  $W$  — одно из этих циклических подпространств, соответствующее ниль-слою  $w_0, w_1, \dots, w_{l-1}$  длины  $l$ . Для каждого  $i = 0, \dots, l-2$  выполняется  $w_i(\varphi - \lambda\varepsilon) = w_i\psi = w_{i+1}$  и  $w_{l-1}(\varphi - \lambda\varepsilon) = w_{l-1}\psi = 0$ . Поэтому для каждого  $i = 0, \dots, l-2$  выполняется  $w_i\varphi = \lambda w_i + w_{i+1}$  и  $w_{l-1}\varphi = \lambda w_{l-1}$ . Из приведённых равенств следует, что подпространство  $W$  является  $\varphi$ -инвариантным. Поэтому пространство  $V$  разлагается в прямую сумму циклических  $\varphi$ -инвариантных подпространств, матрица преобразования  $\varphi$  в базисе, составленном из базисов этих подпространств, клеточно диагональна и каждому циклическому подпространству соответствует клетка требуемого вида.  $\square$

**Определение 6.6.2.** Матрица, имеющая форму, как в теореме 6.6.1, называется *жордановой*, а клетки, из которых она состоит, — *жордановыми клетками*.

**Следствие.** Если в некотором базисе пространства  $V$  матрица линейного преобразования  $\varphi$  жорданова, то этот базис жорданов для преобразования  $\varphi$ . Кроме того, в жордановой матрице линейного преобразования  $\varphi$  для каждого  $\lambda \in \text{Sp}(\varphi)$  количество жордановых клеток фиксированного размера со скаляром  $\lambda$  на главной диагонали не зависит от выбора жорданова базиса.

**ДОКАЗАТЕЛЬСТВО.** Векторы базиса, которым соответствует жорданова клетка размера  $l$  со скаляром  $\lambda$  на главной диагонали, очевидно, образуют ниль-слой длины  $l$  относительно преобразования  $\varphi - \lambda\varepsilon$ . Поэтому базис, в котором матрица преобразования  $\varphi$  жорданова, есть объединение базисов  $\varphi$ -инвариантных циклических подпространств, а значит, является жордановым для преобразования  $\varphi$ . Объединение базисов циклических подпространств, соответствующих одному и тому же собственному числу  $\lambda$ , даст нам базис корневого подпространства  $U_\lambda = \text{Ker}(\varphi - \lambda\varepsilon)^{k_\lambda}$ . Оператор  $\varphi - \lambda\varepsilon|_{U_\lambda}$  нильпотентен на  $U_\lambda$ . По теореме 6.5.1 число ниль-слоёв фиксированной длины в жордановом базисе этого оператора не зависит от выбора базиса. Поэтому не зависит от выбора базиса и число клеток фиксированного размера со скаляром  $\lambda$  на главной диагонали в жордановой матрице оператора  $\varphi$ .  $\square$

**УПРАЖНЕНИЕ 6.6.1.** Доказать, что максимальный размер жордановой клетки с собственным числом  $\lambda$  на главной диагонали равен высоте  $k$  корневого подпространства  $U_\lambda = \text{Ker}(\varphi - \lambda\varepsilon)^k$ .

**Теорема 6.6.2** (матричная форма теоремы Жордана). Пусть  $F$  — поле,  $A \in M_n(F)$ ,  $K$  — расширение поля  $F$ , для которого  $\text{Sp}(A) \subseteq K$ . Тогда существуют невырожденная матрица  $T \in M_n(K)$  и жорданова матрица  $J \in M_n(K)$ , такие, что  $J = TAT^{-1}$ . Матрица  $J$  определена однозначно с точностью до перестановки жордановых клеток, причём если  $s_{ij}$  — число жордановых клеток размера  $j$  со скаляром  $\lambda_i$  на главной диагонали, то  $s_{ij} = r_{i,j-1} - 2r_{ij} + r_{i,j+1}$ , где  $r_{ij} = \text{rank}(A - \lambda_i E)^j$ .

**ДОКАЗАТЕЛЬСТВО.** Рассмотрим арифметическое векторное пространство  $V = K^n$  над полем  $K$ . Преобразование  $\varphi$  этого пространства, заданное правилом  $v\varphi = vA$ , линейно, и в стандартном базисе  $B$ , состоящем из строк  $e_1, \dots, e_n$  единичной матрицы, матрица этого преобразования  $[\varphi]_B$  равна матрице  $A$ . Поскольку  $\text{Sp}(\varphi) = \text{Sp}(A) \subseteq K$ , по теореме Жордана существует жорданов базис  $C$  преобразования  $\varphi$ , в котором матрица  $J = [\varphi]_C$  преобразования является жордановой. Матрица  $T \in M_n(K)$ , составленная из строк базиса  $C$ , записанных в стандартном базисе  $B$ , является матрицей перехода от базиса  $B$  к базису  $C$ . Поэтому  $T$  невырождена и  $J = TAT^{-1}$ . В силу следствия из теоремы Жордана матрица  $J$  определена однозначно с точностью до перестановки жордановых клеток. В силу теоремы о жордановой форме нильпотентного оператора число  $s_{ij}$  клеток размера  $j$  со скаляром  $\lambda_i$  на главной диагонали равно  $r_{j-1}(\lambda_i) - 2r_j(\lambda_i) + r_{j+1}(\lambda_i)$ , где  $r_j(\lambda_i) = \dim U_i(\varphi - \lambda_i\varepsilon)^j$  и  $U_i$  — корневое подпространство высоты  $k_i$ , соответствующее собствен-

ному числу  $\lambda_i$ . В силу теоремы о корневом разложении  $V = U_i \oplus W_i$ , где  $W_i = V(\varphi - \lambda_i \varepsilon)^{k_i}$  и  $W_i(\varphi - \lambda_i \varepsilon) = W_i$ . Поэтому  $V(\varphi - \lambda_i \varepsilon)^j = U_i(\varphi - \lambda_i \varepsilon)^j + W_i$ . Обозначим размерность пространства  $W_i$  через  $r_i$ . Так как размерность образа линейного преобразования равна рангу матрицы этого преобразования, то  $r_{ij} = \text{rank}(A - \lambda_i E)^j = r_j(\lambda_i) + r_i$ . Поэтому  $s_{ij} = r_{j-1}(\lambda_i) - 2r_j(\lambda_i) + r_{j+1}(\lambda_i) = (r_{i,j-1} - r_i) - 2(r_{ij} - r_i) + (r_{i,j+1} - r_i) = r_{i,j-1} - 2r_{ij} + r_{i,j+1}$ , что и требовалось доказать.  $\square$

УПРАЖНЕНИЕ 6.6.2. Для матрицы

$$A = \begin{pmatrix} 0 & -1 & -1 & 2 \\ 6 & 5 & 1 & -4 \\ -2 & -1 & -1 & 4 \\ 2 & 1 & -1 & 2 \end{pmatrix},$$

у которой  $f_A(x) = x(x-2)^3$ , построить в пространстве  $V = \mathbb{R}^4$  жорданов базис, найти жорданову форму матрицы  $A$  в этом базисе и указать матрицу  $T$  перехода к этому базису.

## § 6.7. Многочлены и функции от линейных преобразований

**Определение 6.7.1.** Пусть  $F$  — поле,  $f(x) = a_0 + a_1x + \dots + a_mx^m \in F[x]$ ,  $A \in M_n(F)$ ,  $\varphi \in \mathcal{L}(V)$ , где  $V$  — векторное пространство над полем  $F$ . Значением многочлена  $f(x)$  от матрицы  $A$  называется матрица  $f(A) = a_0E + a_1A + \dots + a_mA^m$ . Значением многочлена  $f(x)$  от линейного преобразования  $\varphi$  называется линейное преобразование  $f(\varphi) = a_0\varepsilon + a_1\varphi + \dots + a_m\varphi^m$ .

**Предложение 6.7.1.** Пусть  $F$  — поле и  $f(x) \in F[x]$ . Тогда выполняются следующие утверждения.

1. Если  $\varphi$  — линейное преобразование векторного пространства  $V$  над полем  $F$  и  $[\varphi]$  — матрица этого преобразования в некоторой базе, то  $f([\varphi]) = [f(\varphi)]$ .

2. Если  $A, B, T \in M_n(F)$  и  $B = TAT^{-1}$ , то  $f(B) = Tf(A)T^{-1}$ .

**ДОКАЗАТЕЛЬСТВО.** 1. Пусть  $f(x) = a_0 + a_1x + \dots + a_mx^m$ . Имеем  $[f(\varphi)] = [a_0\varepsilon + a_1\varphi + \dots + a_m\varphi^m] = a_0[\varepsilon] + a_1[\varphi] + \dots + a_m[\varphi]^m = f([\varphi])$ .

2. Пусть  $V = F^n$  — арифметическое векторное пространство строк. Определим линейное преобразование  $\varphi$  этого пространства правилом  $v\varphi = vA$ . Тогда в стандартном базисе  $[\varphi]_1 = A$ . Поскольку  $|T| \neq 0$ , строки матрицы  $T$  образуют ещё один базис пространства  $V$ . Матрица  $[\varphi]_2$  преобразования  $\varphi$  в этом базисе равна  $B$ , так как в силу равенства

$B = TAT^{-1}$  матрица  $T$  есть матрица перехода к этому базису. Поэтому  $f(B) = f([\varphi]_2) = [f(\varphi)]_2 = T[f(\varphi)]_1T^{-1} = Tf([\varphi]_1)T^{-1} = Tf(A)T^{-1}$ .

**УПРАЖНЕНИЕ 6.7.1.** Доказать п. 2 предложения 6.7.1 непосредственно, воспользовавшись законом дистрибутивности в кольце матриц.

**Предложение 6.7.2.** Пусть  $F$  — поле,  $f, g \in F[x]$ ,  $u = f + g$ ,  $v = fg$ ,  $A \in M_n(F)$ ,  $\varphi \in \mathcal{L}(V)$ , где  $V$  — векторное пространство над  $F$ . Тогда  $u(A) = f(A) + g(A)$ ,  $u(\varphi) = f(\varphi) + g(\varphi)$ ,  $v(A) = f(A)g(A)$ ,  $v(\varphi) = f(\varphi)g(\varphi)$ .

**УПРАЖНЕНИЕ 6.7.2.** Доказать предложение 6.7.2.

**ЗАМЕЧАНИЕ.** Из предложения 6.7.2 следует, что равенства для многочленов, основанные на свойствах операций в кольце многочленов, приводят к соответствующим равенствам для значений многочленов от матриц и линейных преобразований. Например, равенство многочленов  $fg = gf$ , вытекающее из коммутативности умножения, приводит к равенству линейных преобразований  $f(\varphi)g(\varphi) = g(\varphi)f(\varphi)$ .

**Определение 6.7.2.** Пусть  $\varphi$  — линейное преобразование векторного пространства  $V$  над полем  $F$ ,  $A$  — матрица из  $M_n(F)$ . Многочлен  $f(x) \in F[x]$  аннулирует преобразование  $\varphi$  (матрицу  $A$ ), если  $f(\varphi) = 0$  ( $f(A) = 0$ ). Многочлен наименьшей степени со старшим коэффициентом, равным 1, который аннулирует преобразование  $\varphi$  (матрицу  $A$ ), называется минимальным аннулирующим многочленом для  $\varphi$  (для  $A$ ).

**Теорема 6.7.1** (о минимальном аннулирующем многочлене). Пусть  $V$  — конечномерное векторное пространство над полем  $F$ ,  $\varphi$  — линейное преобразование пространства  $V$ , спектр которого лежит в  $F$ , и  $f_\varphi(x) = \prod_{i=1}^s (x - \lambda_i)^{n_i}$  — характеристический многочлен преобразования  $\varphi$ , причём  $\lambda_i \neq \lambda_j$  при  $i \neq j$ . Пусть для каждого  $i = 1, \dots, s$  число  $k_i$  — высота корневого подпространства  $U_i = \text{Ker}(\varphi - \lambda_i \varepsilon)^{k_i}$ . Тогда многочлен  $g(x) = \prod_{i=1}^s (x - \lambda_i)^{k_i}$  является минимальным аннулирующим многочленом для преобразования  $\varphi$ .

**ДОКАЗАТЕЛЬСТВО.** Для каждого  $i = 1, \dots, s$  положим

$$g_i(x) = \frac{g(x)}{(x - \lambda_i)^{k_i}}.$$

Докажем сначала, что  $g(x)$  аннулирует  $\varphi$ . По теореме 6.4.1 о корневом разложении  $V = \bigoplus_{i=1}^s U_i$ . Поэтому для любого  $v \in V$  имеем



$v = u_1 + \dots + u_s$ , где  $u_i \in U_i$ . Тогда

$$\begin{aligned} vg(\varphi) &= \left( \sum_{i=1}^s u_i \right) g(\varphi) = \sum_{i=1}^s (u_i g(\varphi)) = \sum_{i=1}^s u_i ((\varphi - \lambda_i \varepsilon)^{k_i} g_i(\varphi)) = \\ &= \sum_{i=1}^s (u_i (\varphi - \lambda_i \varepsilon)^{k_i}) g_i(\varphi) = 0, \end{aligned}$$

так как  $u_i \in \text{Ker}(\varphi - \lambda_i \varepsilon)^{k_i}$  для каждого  $i = 1, \dots, s$ .

Пусть теперь  $h(x)$  — минимальный аннулирующий многочлен для преобразования  $\varphi$ . Если многочлен  $h$  не делит  $g$ , то ненулевой остаток от деления  $g$  на  $h$  имеет степень, меньшую степени  $h$ , и аннулирует  $\varphi$ , что противоречит выбору  $h$  в качестве минимального аннулирующего многочлена. Следовательно,  $h$  делит  $g$ , а значит,  $h(x) = \prod_{i=1}^s (x - \lambda_i)^{m_i}$ , где  $m_i \leq k_i$  для любого  $i = 1, \dots, s$ . Допустим, что степень  $h$  меньше степени  $g$ , т. е. найдётся  $i \in \{1, \dots, s\}$ , для которого  $m_i < k_i$ . Не теряя общности, можно считать, что  $m_1 < k_1$ . Из определения высоты корневого подпространства следует, что найдётся вектор  $u_1 \in U_1$ , такой, что  $u_1(\varphi - \lambda_1 \varepsilon)^{k_1 - 1} \neq 0$ . Поскольку  $m_1 < k_1$ , имеем  $u_1(\varphi - \lambda_1 \varepsilon)^{m_1} = w_1 \neq 0$ . Поэтому  $u_1 h(\varphi) = (u_1(\varphi - \lambda_1 \varepsilon)^{m_1}) \prod_{i=2}^s (\varphi - \lambda_i \varepsilon)^{m_i} = w_1 \prod_{i=2}^s (\varphi - \lambda_i \varepsilon)^{m_i}$ . Подпространство  $U_1$  инвариантно относительно каждого преобразования  $\varphi - \lambda_i \varepsilon$ , где  $i = 1, \dots, s$ . Более того, из теоремы о корневом разложении следует, что каждое из этих преобразований невырождено на  $U_1$  при  $i \neq 1$ . Поэтому  $w_1(\varphi - \lambda_2 \varepsilon)^{m_2} = w_2 \neq 0, w_2(\varphi - \lambda_3 \varepsilon)^{m_3} = w_3 \neq 0, \dots, w_{s-1}(\varphi - \lambda_s \varepsilon)^{m_s} = w_s \neq 0$ . Таким образом,  $u_1 h(\varphi) = w_s \neq 0$ ; противоречие. Следовательно,  $g(x) = h(x)$ .  $\square$

**Следствие.** Если матрица  $A = [\varphi]$  есть матрица некоторого линейного преобразования  $\varphi$  и  $g(x)$  — минимальный аннулирующий многочлен для  $\varphi$ , то  $g(x)$  — минимальный аннулирующий многочлен для матрицы  $A$ .

**Теорема 6.7.2** (Гамильтон — Кэли). Пусть  $F$  — поле. Имеют место следующие утверждения.

1. Если  $A \in M_n(F)$  и  $f(x)$  — характеристический многочлен для  $A$ , то  $f(A) = 0$ .

2. Если  $\varphi \in \mathcal{L}(V)$ , где  $V$  — конечномерное пространство над полем  $F$ , и  $f(x)$  — характеристический многочлен для  $\varphi$ , то  $f(\varphi) = 0$ .

**Доказательство.** Если  $\text{Sp}(A)$  (или  $\text{Sp}(\varphi)$ ) лежит в поле  $F$ , то теорема Гамильтона — Кэли есть следствие теоремы о минимальном аннулирующем многочлене, поскольку по теореме о корневом разложении

для каждого корня  $\lambda_i$  характеристического многочлена  $f(x)$  имеет место неравенство  $k_i \leq n_i$ , где  $n_i$  — кратность  $\lambda_i$  в  $f(x)$ , а  $k_i$  — высота корневого подпространства  $U_i = \text{Ker}(\varphi - \lambda_i \varepsilon)^{k_i}$ , т. е. кратность  $\lambda_i$  в минимальном аннулирующем многочлене  $g(x)$ .

Предположим, что  $\text{Sp}(A)$  не лежит в  $F$ . Рассмотрим расширение  $K$  поля  $F$ , над которым многочлен  $f(x)$  разлагается на линейные множители. Рассмотрим отображение  $v \mapsto vA$  арифметического пространства  $V = K^n$ , матрицей которого в стандартном базисе, очевидно, является матрица  $A$ . Из теоремы 6.7.1 вытекает, что минимальный аннулирующий многочлен  $g(x)$  матрицы  $A$  делит её характеристический многочлен, а потому  $f(A) = 0$  в поле  $K$ . Поскольку все коэффициенты многочлена  $f(x)$  лежат в поле  $F$ , равенство  $f(A) = 0$  имеет место и над полем  $F$ . Таким образом, п. 1 теоремы доказан. П. 2 вытекает из п. 1 и равенства  $[f(\varphi)] = f([\varphi])$ .  $\square$

**ЗАМЕЧАНИЕ.** Теорему Гамильтона — Кэли кратко формулируют так: матрица — корень своего характеристического многочлена.

Теперь мы займёмся обобщением теоремы о корневом разложении, убрав из формулировки требование о том, чтобы поле содержало спектр оператора.

**Теорема 6.7.3** (о ядерном распаде). Пусть  $\varphi$  — линейное преобразование конечномерного векторного пространства  $V$  над полем  $F$ . Предположим, что многочлен  $f \in F[x]$ , аннулирующий преобразование  $\varphi$ , разлагается в произведение  $f = \prod_{i=1}^s f_i$  многочленов  $f_1, \dots, f_s \in F[x]$ , таких, что  $(f_i, f_j) = 1$  при  $i \neq j$ . Тогда имеет место разложение  $V = \bigoplus_{i=1}^s \text{Ker } f_i(\varphi)$ .

**ДОКАЗАТЕЛЬСТВО.** Мы начнём с доказательства вспомогательного утверждения.

**Лемма.** Пусть  $\alpha, \beta, \gamma, \delta$  — попарно перестановочные линейные преобразования пространства  $V$ , для которых  $\alpha\beta = 0$  и  $\alpha\gamma + \beta\delta = \varepsilon$ . Тогда  $V = \text{Ker } \alpha \oplus \text{Ker } \beta = \text{Ker } \alpha \oplus V\alpha = \text{Ker } \beta \oplus V\beta = V\alpha \oplus V\beta$ .

**ДОКАЗАТЕЛЬСТВО ЛЕММЫ.** Имеем  $V = V\varepsilon = V(\alpha\gamma + \beta\delta) = V\alpha\gamma + V\beta\delta = (V\gamma)\alpha + (V\delta)\beta \subseteq V\alpha + V\beta \subseteq V$ . Поэтому  $V = V\alpha + V\beta$ . С другой стороны,  $0 = V(\alpha\beta) = (V\alpha)\beta$ . Отсюда  $V\alpha \subseteq \text{Ker } \beta$ . Следовательно,  $V = \text{Ker } \beta + V\beta$ . Поскольку  $\dim \text{Ker } \beta + \dim V\beta = \dim V$ , эта сумма прямая, т. е.  $V = \text{Ker } \beta \oplus V\beta$  и  $\text{Ker } \beta \cap V\beta = 0$ .

Вспоминая, что  $V\alpha \subseteq \text{Ker } \beta$ , получаем  $V\alpha \cap V\beta = 0$ . Следовательно,  $V = V\alpha \oplus V\beta$  и  $V\alpha = \text{Ker } \beta$ . Аналогично  $V\beta = \text{Ker } \alpha$ , поэтому  $V = \text{Ker } \alpha \oplus V\alpha$  и  $V = \text{Ker } \alpha \oplus \text{Ker } \beta$ .  $\square$

Докажем теорему индукцией по числу  $s$  многочленов в разложении  $f = \prod_{i=1}^s f_i$ . Для  $s = 1$  утверждение теоремы очевидно. Докажем его для  $s > 1$ , предполагая, что для числа, меньшего  $s$ , теорема доказана. Положим  $\tilde{f}_2 = f_2 \cdots f_s$ . Поскольку  $(f_1, \tilde{f}_2) = 1$ , найдутся многочлены  $u, v \in F[x]$ , такие, что  $f_1 u + \tilde{f}_2 v = 1$ . Линейные преобразования  $\alpha = f_1(\varphi)$ ,  $\beta = \tilde{f}_2(\varphi)$ ,  $\gamma = u(\varphi)$ ,  $\delta = v(\varphi)$  удовлетворяют условиям леммы. Поэтому  $V = \text{Ker } \alpha \oplus \text{Ker } \beta = \text{Ker } f_1(\varphi) \oplus \text{Ker } \tilde{f}_2(\varphi)$ .

Положим  $W = \text{Ker } \tilde{f}_2(\varphi)$ . Поскольку преобразование  $\tilde{f}_2(\varphi)$  перестановочно с  $\varphi$ , подпространство  $W$  является  $\varphi$ -инвариантным. Пусть  $\psi = \varphi|_W$ . Тогда  $\tilde{f}_2(\psi) = 0$  на  $W$ . По предположению индукции  $W = \bigoplus_{i=2}^s \text{Ker } f_i(\psi)$ . Осталось доказать, что  $\text{Ker } f_i(\psi) = \text{Ker } f_i(\varphi)$  для каждого  $i = 2, \dots, s$ . Если для произвольного  $v \in V$  и для некоторого  $i \in \{2, \dots, s\}$  выполняется  $v f_i(\varphi) = 0$ , то  $v \tilde{f}_2(\varphi) = 0$ . Поэтому для всех  $i = 2, \dots, s$  имеет место включение  $\text{Ker } f_i(\varphi) \subseteq \text{Ker } \tilde{f}_2(\varphi) = W$ . Поскольку для любого вектора  $w \in W$  выполняется  $w\psi = w\varphi$ , то для любого  $i = 2, \dots, s$  имеет место  $w f_i(\psi) = w f_i(\varphi)$ , а значит,  $\text{Ker } f_i(\psi) = \text{Ker } f_i(\varphi)$ .  $\square$

**УПРАЖНЕНИЕ 6.7.3.** Линейное преобразование  $\varphi$  пространства  $V$  над полем  $\mathbb{R}$  задано в некотором базисе матрицей

$$\begin{pmatrix} 2 & -1 & 2 \\ 2 & 2 & -1 \\ -1 & 2 & 2 \end{pmatrix}.$$

Разложить  $V$  в прямую сумму одномерного и двумерного подпространств, инвариантных относительно  $\varphi$ . Найти базисы этих подпространств и матрицу преобразования  $\varphi$  в базисе, составленном из данных базисов.

**Теорема 6.7.4.** Пусть  $F$  — поле,  $\text{char } F = 0$ ,  $A \in M_n(F)$ ,  $K$  — расширение поля  $F$ , для которого  $\text{Sp}(A) \subseteq K$ ,

$$J = \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_m \end{pmatrix} = TAT^{-1} \text{ — жорданова форма матрицы } A,$$

$T$  — сопрягающая матрица и  $T, J \in M_n(K)$ . Пусть  $p(x)$  — многочлен из  $F[x]$ . Тогда выполняются следующие утверждения.

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

2.

$$p(J) = \begin{pmatrix} p(J_1) & & 0 \\ & \ddots & \\ 0 & & p(J_m) \end{pmatrix}.$$

3. Если  $P = (p_{ij})_{t \times t} = p(J_k)$ , где  $k \in \{1, \dots, m\}$  и

$$J_k = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & \lambda \end{pmatrix},$$

то  $p_{ij} = 0$  при  $i > j$  и  $p_{ij} = \frac{p^{(j-i)}(\lambda)}{(j-i)!}$  при  $i \leq j$ , т. е.

$$P = \begin{pmatrix} p(\lambda) & p'(\lambda) & \frac{p''(\lambda)}{2!} & \dots & \frac{p^{(t-1)}(\lambda)}{(t-1)!} \\ 0 & p(\lambda) & p'(\lambda) & \dots & \frac{p^{(t-2)}(\lambda)}{(t-2)!} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & p'(\lambda) \\ 0 & 0 & 0 & \dots & p(\lambda) \end{pmatrix}_{t \times t}.$$

**ДОКАЗАТЕЛЬСТВО.** Существование матриц  $J$  и  $T$  следует из теоремы 6.6.2 (матричная форма теоремы Жордана). П. 1 теоремы следует из п. 2 предложения 6.7.1, поскольку  $A = T^{-1}JT$ . П. 2 следует из предложения 2.3.2. Докажем п. 3, начав с несложной леммы.

**Лемма.** Пусть  $H$  — квадратная матрица размерности  $t$ , равная

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}. \text{ Тогда } H^k = \begin{pmatrix} 0 & \dots & 0 & \overbrace{1}^{k+1} & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & 0 & \dots & 1 \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

при  $k < t$  и  $H^k = 0$  при  $k \geq t$ .

ДОКАЗАТЕЛЬСТВО ЛЕММЫ. Рассмотрим матрицу  $H$  как матрицу линейного преобразования арифметического пространства  $F^t$  в стандартном базисе из векторов  $e_1, \dots, e_t$ . Тогда для каждого  $i = 1, \dots, t$  выполняются равенства:  $e_i H^k = e_{i+k}$  при  $k + i \leq t$  и  $e_i H^k = 0$  при  $k + i > t$ , что и доказывает лемму.  $\square$

Вернёмся к доказательству теоремы. Пусть

$$B = J_k = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & \lambda \end{pmatrix}_{t \times t} = \lambda E + H,$$

где матрица  $H$  определена в лемме. Поскольку  $\text{char } F = 0$ , по формуле Тейлора (теорема 5.3.4) имеем  $p(x) = \sum_{k=0}^{\infty} \frac{p^{(k)}(\lambda)}{k!} (x - \lambda)^k$ , где  $p^{(0)}(\lambda) = p(\lambda)$  и  $p^{(k)}(\lambda) = 0$  при  $k > \deg p$ . Подставляя матрицу  $B$  в выражение для  $p(x)$ , получаем

$$P = p(B) = \sum_{k=0}^{\infty} \frac{p^{(k)}(\lambda)}{k!} (B - \lambda E)^k = \sum_{k=0}^{\infty} \frac{p^{(k)}(\lambda)}{k!} H^k.$$

Отсюда следует, что  $p_{ij} = 0$  при  $i > j$  и  $p_{ij} = \frac{p^{(j-i)}(\lambda)}{(j-i)!}$  при  $i \leq j$ .  $\square$

**Определение 6.7.3.** Пусть поле  $F$  — это либо  $\mathbb{R}$ , либо  $\mathbb{C}$ ,  $X \subseteq F$  и  $f : X \rightarrow F$  — функция. Предположим, что  $A \in M_n(F)$ ,  $\text{Sp}(A) \subseteq F$  и  $g(x) = \prod_{i=1}^s (x - \lambda_i)^{k_i}$  — минимальный аннулирующий многочлен для матрицы  $A$ . Если для каждого  $i = 1, \dots, s$  определены значения  $f(\lambda_i), f'(\lambda_i), \dots, f^{(k_i-1)}(\lambda_i)$ , то говорят, что  $f$  определена на спектре матрицы  $A$ . В этом случае полагают значение функции  $f$  от матрицы  $A$  равным  $f(A) = T^{-1}f(J)T$ , где  $T$  — матрица перехода к жорданову базису матрицы  $A$ ,

$$J = \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_m \end{pmatrix} \text{ — жорданова форма матрицы } A,$$

$$f(J) = \begin{pmatrix} f(J_1) & & 0 \\ & \ddots & \\ 0 & & f(J_m) \end{pmatrix} \text{ и } f(J_k) = f \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & \lambda \end{pmatrix} =$$

$$= \begin{pmatrix} f(\lambda) & f'(\lambda) & \frac{f''(\lambda)}{2!} & \cdots & \frac{f^{(t-1)}(\lambda)}{(t-1)!} \\ 0 & f(\lambda) & f'(\lambda) & \cdots & \frac{f^{(t-2)}(\lambda)}{(t-2)!} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \cdots & f'(\lambda) \\ 0 & 0 & 0 & \cdots & f(\lambda) \end{pmatrix}_{t \times t}.$$

**Теорема 6.7.5.** *В обозначениях определения 6.7.3, если функция  $f$  определена на спектре матрицы  $A$ , то значение  $f(A)$  не зависит от выбора сопрягающей матрицы  $T$ . Существует и единствен многочлен  $p(x) \in F[x]$ , такой, что его степень меньше степени минимального аннулирующего многочлена  $g(x)$  и  $p(A) = f(A)$ .*

**ДОКАЗАТЕЛЬСТВО.** По теореме 5.3.5 об интерполяционном многочлене Лагранжа — Сильвестра существует и единствен многочлен  $p(x) \in F[x]$  степени, меньшей  $\sum_{i=1}^s k_i$  (т.е. степени  $g(x)$ ), такой, что  $p^{(j)}(\lambda_i) = f^{(j)}(\lambda_i)$  при всех  $i = 1, \dots, s$  и  $j = 0, \dots, k_i - 1$ . Тогда из определения  $f(J)$  и теоремы 6.7.4 вытекает, что  $p(J) = f(J)$  для жордановой формы  $J$  матрицы  $A$ . Если  $A = T^{-1}JT$ , то  $f(A) = T^{-1}f(J)T = T^{-1}p(J)T = p(A)$ . В частности, значение  $f(A)$  функции  $f$  от матрицы  $A$  не зависит от выбора матрицы  $T$ , так как значение  $p(A)$ , очевидно, не зависит от выбора  $T$ .  $\square$

**Определение 6.7.4.** Пусть поле  $F$  — это либо  $\mathbb{R}$ , либо  $\mathbb{C}$ ,  $V$  — конечномерное векторное пространство над  $F$ ,  $B$  — базис пространства  $V$ ,  $\varphi$  — линейное преобразование пространства  $V$ ,  $A = [\varphi]_B$  — матрица преобразования  $\varphi$  в базисе  $B$ ,  $X \subseteq F$  и  $f : X \rightarrow F$  — функция. Если определена матрица  $f(A)$ , то линейное преобразование  $\psi$ , матрица которого в базисе  $B$  равна  $f(A)$ , называется *значением функции  $f$  от преобразования  $\varphi$*  и обозначается как  $f(\varphi)$ . Если  $f(A)$  не определено, то и  $f(\varphi)$  не определено.

**Следствие.** *В обозначениях определения 6.7.4, если определено преобразование  $f(\varphi)$ , то оно определено однозначно, т.е. не зависит от выбора базиса  $B$ . Существует и единствен многочлен  $p(x) \in F[x]$ , такой, что его степень меньше степени минимального аннулирующего многочлена для преобразования  $\varphi$  и  $p(\varphi) = f(\varphi)$ .*

**ДОКАЗАТЕЛЬСТВО.** В силу теоремы 6.7.5 существует и единствен многочлен  $p(x) \in F[x]$ , степень которого меньше степени минимального аннулирующего многочлена матрицы  $A$  (а значит, и преобразования  $\varphi$ ) и для которого  $p(A) = f(A)$ . Тогда  $[p(\varphi)]_B = p([\varphi]_B) = f([\varphi]_B) =$

$[f(\varphi)]_B$ . Следовательно,  $p(\varphi) = f(\varphi)$ . Поскольку  $p(\varphi)$  не зависит от выбора базиса, то от него не зависит и  $f(\varphi)$ .  $\square$

УПРАЖНЕНИЕ 6.7.4. Линейное преобразование  $\varphi$  пространства  $V$  задано в некоторой базе матрицей

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

Найти:

- а) жорданову базу и жорданову форму преобразования  $\varphi$ ;
- б) минимальный аннулирующий многочлен;
- в) матрицу  $A^{100}$ ;
- г) матрицу  $e^A$ , используя жорданову форму матрицы  $A$ ;
- д) матрицу  $e^A$ , вычисляя соответствующий многочлен Лагранжа — Сильвестра.

## Глава 7

### Евклидовы и унитарные пространства

#### § 7.1. Скалярное произведение на векторном пространстве

На протяжении этой главы под полем определения векторного пространства мы будем подразумевать либо поле действительных, либо поле комплексных чисел. В зависимости от выбора поля соответствующее пространство называется *действительным* или *комплексным*. Поскольку в общей теории векторных пространств нет понятий, соответствующих понятиям длины вектора, угла между векторами и т. п., многие естественные и полезные свойства трёхмерного пространства геометрических векторов и их преобразований не нашли отражения в этой теории. Указанный пробел будет восполнен в данной главе с помощью понятия скалярного произведения, которое мы определим на произвольном действительном или комплексном пространстве.

**Определение 7.1.1.** Пусть  $F$  — поле действительных или комплексных чисел,  $V$  — векторное пространство над  $F$ . Функция  $(, ) : V \times V \rightarrow F$ , сопоставляющая каждой упорядоченной паре векторов  $a, b \in V$  число  $(a, b) \in F$ , называется *скалярным произведением* на пространстве  $V$ , если для любых векторов  $a, b, c \in V$  и скаляра  $\alpha \in F$  выполняются следующие условия:

- 1)  $(a, b) = \overline{(b, a)}$ ;
- 2)  $(a + b, c) = (a, c) + (b, c)$ ;
- 3)  $(\alpha a, b) = \alpha(a, b)$ ;
- 4) если  $a \neq 0$ , то  $(a, a) > 0$ .

**ЗАМЕЧАНИЯ.** 1. В условии 1 черта над числом означает взятие комплексно сопряжённого. В случае действительного векторного пространства, естественно, комплексное сопряжение оставляет число на месте, т. е. для этого пространства свойство 1 имеет вид:  $(a, b) = (b, a)$ .

2. Из условия 1 вытекает, что число  $(a, a) = \overline{(a, a)}$  лежит в поле действительных чисел для любого вектора  $a$ , а потому сравнение числа  $(a, a)$  с нулём в условии 4 имеет смысл и в случае комплексного векторного пространства.

**УПРАЖНЕНИЕ 7.1.1.** Докажите, что для любых векторов  $a, b, c \in V$



и скаляра  $\alpha \in F$  имеют место следующие свойства скалярного произведения:

- 1)  $(a, b + c) = (a, b) + (a, c)$ ;
- 2)  $(a, \alpha b) = \bar{\alpha}(a, b)$ ;
- 3)  $a = 0 \Leftrightarrow (a, a) = 0$ ;
- 4)  $(a, 0) = (0, a) = 0$ .

**Определение 7.1.2.** Векторное пространство  $V$  над полем  $F$ , на котором задано скалярное произведение, называется *евклидовым*, если  $F = \mathbb{R}$ , и *унитарным* (или *эрмитовым*), если  $F = \mathbb{C}$ .

**ПРИМЕРЫ.** 1. Пусть  $V = E^2$  или  $E^3$  — пространство геометрических векторов (над полем  $\mathbb{R}$ ). Тогда функция  $(, ) : V \times V \rightarrow \mathbb{R}$ , определённая правилом  $(\vec{a}, \vec{b}) = |\vec{a}| |\vec{b}| \cos(\angle \vec{a}, \vec{b})$ , является скалярным произведением на  $V$ , а пространство  $V$  с ним будет евклидовым.

2. Пусть  $V = \mathbb{R}[x]$  — пространство многочленов. Функция  $(f, g) = \int_0^1 f(x)g(x)dx$  — скалярное произведение на  $V$ . Аналогично, если  $V$  — пространство действительных функций, непрерывных на  $[a, b] \subseteq \mathbb{R}$ , то  $(f, g) = \int_a^b f(x)g(x)dx$  — скалярное произведение на  $V$ .

3. Пусть  $V = F^n$  — арифметическое векторное пространство над полем  $F$ , где  $F$  — это  $\mathbb{R}$  или  $\mathbb{C}$ . Для векторов-строк  $a = (\alpha_1, \dots, \alpha_n)$  и  $b = (\beta_1, \dots, \beta_n)$  положим

$$(a, b) = \sum_{i=1}^n \alpha_i \bar{\beta}_i = a \bar{b}' \quad (1)$$

Заданная таким образом функция является скалярным произведением на  $V$ . Мы будем называть её *стандартным скалярным произведением*.

**Определение 7.1.3.** *Длиной (нормой)* вектора  $a$  в евклидовом (унитарном) пространстве  $V$  называется неотрицательное действительное число  $|a| = \sqrt{(a, a)}$  (здесь  $\sqrt{\phantom{x}}$  — арифметический корень). Вектор  $a$  называется *нормированным*, если его длина равна 1.

**УПРАЖНЕНИЕ 7.1.2.** Доказать, что для любых  $a \in V$ ,  $\alpha \in F$  выполняется  $|\alpha a| = |\alpha| |a|$ . В частности, при  $a \neq 0$  вектор  $\frac{a}{|a|}$  всегда нормирован, и  $|a| = 0 \Leftrightarrow a = 0$ .

**Предложение 7.1.1** (неравенство Коши — Буняковского). Если  $V$  — евклидово или унитарное пространство, то для любых векторов

$a, b \in V$  выполняется  $(a, b)(b, a) \leq (a, a)(b, b)$ , причём равенство имеет место тогда и только тогда, когда векторы  $a$  и  $b$  линейно зависимы.

УПРАЖНЕНИЕ 7.1.3. Доказать неравенство Коши — Буняковского.

**Следствие.** Если  $V$  — евклидово (унитарное) пространство, то для любых векторов  $a, b \in V$  выполняется  $|(a, b)| \leq |a||b|$ , причём равенство имеет место тогда и только тогда, когда векторы  $a$  и  $b$  линейно зависимы.

**Определение 7.1.4.** Пусть  $V$  — евклидово пространство. Число  $\frac{(a, b)}{|a||b|}$  называется косинусом угла между векторами  $a$  и  $b$ .

**Определение 7.1.5.** Пусть  $V$  — евклидово или унитарное пространство. Векторы  $a$  и  $b$  из  $V$  ортогональны, если  $(a, b) = 0$ .

ЗАМЕЧАНИЕ. Если  $(a, b) = 0$ , то  $(b, a) = \overline{(a, b)} = \overline{0} = 0$ .

**Определение 7.1.6.** Пусть  $V$  — евклидово или унитарное пространство. Набор векторов  $a_1, \dots, a_s$  называется ортогональным, если для всех  $i \in \{1, \dots, s\}$  вектор  $a_i \neq 0$  и для всех  $i, j \in \{1, \dots, s\}$  выполняется  $(a_i, a_j) = 0$  при  $i \neq j$ . Ортогональный набор векторов называется ортонормированным, если все векторы этого набора нормированы.

**Теорема 7.1.1.** Пусть  $V$  — евклидово или унитарное пространство. Тогда выполняются следующие утверждения.

1. Любой ортогональный набор векторов из  $V$  линейно независим.
2. Если  $a_1, \dots, a_t$  — произвольный набор векторов из  $V$ , содержащий хотя бы один ненулевой вектор, то найдётся ортогональный набор векторов  $b_1, \dots, b_s$  из  $V$ , такой, что  $\langle a_1, \dots, a_t \rangle = \langle b_1, \dots, b_s \rangle$  и  $s \leq t$ .
3. Если пространство  $V$  конечномерно, то в  $V$  существует ортонормированный базис. Более того, каждый ортонормированный набор векторов из  $V$  можно дополнить до ортонормированного базиса.
4. Если  $e_1, \dots, e_n$  — ортонормированный базис пространства  $V$ , то для любых векторов  $a, b \in V$  выполняется  $(a, b) = [a][b]'$ , где  $[a], [b]$  — строки координат векторов  $a$  и  $b$  в базисе  $e_1, \dots, e_n$ , а  $[b]'$  — столбец, все элементы которого комплексно сопряжены соответствующим элементам столбца  $[b]'$ .

ДОКАЗАТЕЛЬСТВО. 1. Пусть  $a_1, \dots, a_s$  — ортогональный набор векторов. Предположим, что  $\alpha_1 a_1 + \dots + \alpha_s a_s = 0$ . Тогда для каждого  $i = 1, \dots, s$  выполняется  $0 = (0, a_i) = (\alpha_1 a_1 + \dots + \alpha_s a_s, a_i) = \alpha_i (a_i, a_i)$ . Поскольку  $a_i \neq 0$ , имеем  $(a_i, a_i) \neq 0$ . Следовательно,  $\alpha_i = 0$  для каждо-

го  $i = 1, \dots, s$ .

2. Как мы уже знаем (см. доказательство теоремы 3.2.2 о базисе), из набора векторов  $a_1, \dots, a_t$ , содержащего хотя бы один ненулевой вектор, можно выделить линейно независимый поднабор, линейная оболочка которого совпадает с линейной оболочкой исходного набора. Пользуясь при необходимости перенумерацией, можно считать, что  $\langle a_1, \dots, a_t \rangle = \langle a_1, \dots, a_s \rangle$ , где  $s \leq t$  и набор векторов  $a_1, \dots, a_s$  линейно независим. Мы получим искомым ортогональный набор векторов  $b_1, \dots, b_s$  индуктивно с помощью специального алгоритма, который называется *методом ортогонализации Грама — Шмидта*.

Положим  $b_1 = a_1$ . Если  $s = 1$ , то всё доказано, так как вектор  $a_1$  не может быть равен 0. Предположим, что мы уже построили ортогональный набор векторов  $b_1, \dots, b_{k-1}$ , такой, что  $\langle b_1, \dots, b_{k-1} \rangle = \langle a_1, \dots, a_{k-1} \rangle$ . Будем искать вектор  $b_k$  в форме  $b_k = a_k - \sum_{i=1}^{k-1} \alpha_i b_i$ , так как в этом случае наборы  $a_1, \dots, a_k$  и  $b_1, \dots, b_k$ , очевидно, эквивалентны. Подберём теперь скаляры  $\alpha_1, \dots, \alpha_{k-1}$  так, чтобы вектор  $b_k$  оказался ортогонален каждому вектору из набора  $b_1, \dots, b_{k-1}$ . Для каждого  $j = 1, \dots, k-1$  необходимо выполнение следующей цепочки равенств:  $0 = (b_k, b_j) = (a_k - \sum_{i=1}^{k-1} \alpha_i b_i, b_j) = (a_k, b_j) - \alpha_j (b_j, b_j)$ . Следовательно, требуется положить  $\alpha_j = (a_k, b_j) / (b_j, b_j)$ . Таким образом, искомым вектор определяется формулой

$$b_k = a_k - \sum_{i=1}^{k-1} \frac{(a_k, b_i)}{(b_i, b_i)} b_i.$$

Последовательно определяя векторы  $b_k$ , где  $k = 1, \dots, s$ , получаем требуемый ортогональный набор.

ЗАМЕЧАНИЕ. Несложно заметить, что в том случае, когда поднабор  $a_1, \dots, a_k$ , состоящий из первых векторов набора  $a_1, \dots, a_s$ , является ортогональным, в процессе ортогонализации методом Грама — Шмидта набора  $a_1, \dots, a_s$  указанный поднабор не изменится. В обозначениях предыдущего абзаца сказанное означает, что  $b_1 = a_1, \dots, b_k = a_k$ .

3. Выберем в конечномерном пространстве произвольный базис. Применив к нему метод ортогонализации Грама — Шмидта, получим ортогональный набор векторов, линейная оболочка которого в силу п. 2 совпадает со всем пространством. Поскольку в силу п. 1 полученный ортогональный набор линейно независим, он является базисом пространства. Нормируя каждый вектор этого набора, получаем ортонормированный базис пространства.

Пусть  $e_1, \dots, e_s$  — произвольный ортонормированный набор векторов. Поскольку этот набор линейно независим, по теореме 3.2.2 о базисе его можно дополнить до базиса всего пространства  $e_1, \dots, e_s, a_{s+1}, \dots, a_n$ . В силу замечания после доказательства п. 2, применяя к этому базису метод ортогонализации, получим ортогональный базис  $e_1, \dots, e_s, b_{s+1}, \dots, b_n$ . Нормирование последних  $n - s$  векторов этого базиса даст искомый ортонормированный базис.

4. Пусть  $e_1, \dots, e_n$  — ортонормированный базис пространства, а  $[a] = (\alpha_1, \dots, \alpha_n)$  и  $[b] = (\beta_1, \dots, \beta_n)$  — строки координат векторов  $a$  и  $b$  в этом базисе. Имеем

$$\begin{aligned} (a, b) &= \left( \sum_{i=1}^n \alpha_i e_i, \sum_{j=1}^n \beta_j e_j \right) = \sum_{i=1}^n \sum_{j=1}^n \alpha_i \bar{\beta}_j (e_i, e_j) = \\ &= \sum_{i=1}^n \alpha_i \bar{\beta}_i (e_i, e_i) = \sum_{i=1}^n \alpha_i \bar{\beta}_i = [a][b]', \end{aligned}$$

что и требовалось доказать.  $\square$

**УПРАЖНЕНИЕ 7.1.4.** Ортогонализировать, а затем нормировать набор векторов  $1, x, x^2$  в евклидовом пространстве  $V = \mathbb{R}[x]$  многочленов относительно скалярного произведения, заданного правилом  $(f, g) = \int_0^1 f(x)g(x)dx$ .

**Определение 7.1.7.** Евклидовы (унитарные) пространства  $V$  и  $U$  изоморфны, если существует изоморфизм  $\varphi$  векторных пространств  $U$  и  $V$ , такой, что для любых векторов  $a, b \in V$  имеет место равенство  $(a\varphi, b\varphi) = (a, b)$ .

**Следствие.** Каждое  $n$ -мерное евклидово (унитарное) пространство изоморфно евклидову пространству  $\mathbb{R}^n$  (унитарному пространству  $\mathbb{C}^n$ ) со стандартным скалярным произведением. В частности, два конечномерных евклидовых (унитарных) пространства изоморфны тогда и только тогда, когда их размерности совпадают.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $V$  — евклидово (унитарное) пространство над полем  $F$ , причём  $\dim V = n$ . Выберем в  $V$  ортонормированный базис  $e_1, \dots, e_n$  (п. 3 теоремы). Из п. 4 теоремы следует, что изоморфизм векторного пространства  $V$  на арифметическое пространство  $F^n$ , сопоставляющий каждому вектору из  $V$  строку его координат в данном базисе, будет являться изоморфизмом евклидовых (унитарных) пространств  $V$  и  $F^n$ , если в качестве скалярного произведения на  $F^n$  рас-

смаатривать стандартное скалярное произведение (см. пример 3 к определению 7.1.2). Если  $U$  — ещё одно евклидово (унитарное) пространство той же размерности, то оно по доказанному изоморфно  $F^n$ . Поэтому  $V$  и  $U$  изоморфны между собой.  $\square$

**ЗАМЕЧАНИЕ.** Предположим, что на одном и том же конечномерном векторном пространстве  $V$  заданы две различные функции, каждая из которых является скалярным произведением на  $V$ . Из только что доказанного следствия вытекает, что существует изоморфизм пространства  $V$  на себя, при котором одно скалярное произведение “заменяется” другим. Иными словами, с точностью до изоморфизма на конечномерном векторном пространстве можно задать только одно скалярное произведение.

**УПРАЖНЕНИЕ 7.1.5.** Доказать, что планету Земля можно изометрично, т. е. сохраняя длины векторов, расположить внутри  $n$ -мерного евклидова кубика с ребром в 1 см, если  $n \geq 5 \cdot 10^{18}$ .

**Определение 7.1.8.** Пусть  $V$  — евклидово (унитарное) пространство и  $M \subseteq V$ . Множество  $M^* = \{v \in V \mid \forall m \in M (m, v) = 0\}$  называется *ортгоналъным дополнением* множества  $M$  в  $V$  (ещё одно обозначение этого множества:  $M^\perp$ ).

**УПРАЖНЕНИЕ 7.1.6.** Пусть  $V$  — евклидово (унитарное) пространство и  $M, N \subseteq V$ . Если  $M \subseteq N$ , то  $N^* \subseteq M^*$ .

**Предложение 7.1.2.** Пусть  $V$  — евклидово (унитарное) пространство и  $M \subseteq V$ . Тогда выполняются следующие утверждения.

1.  $M^* = (L(M))^*$ .
2.  $M^*$  — подпространство пространства  $V$ .

**ДОКАЗАТЕЛЬСТВО.** 1. Поскольку  $M \subseteq L(M)$ , имеем  $(L(M))^* \subseteq M^*$ . С другой стороны, если вектор  $v \in M^*$ , то для произвольной линейной комбинации  $\alpha_1 m_1 + \dots + \alpha_s m_s$  векторов из  $M$  выполняется  $(\alpha_1 m_1 + \dots + \alpha_s m_s, v) = \alpha_1 (m_1, v) + \dots + \alpha_s (m_s, v) = 0$ . Значит,  $v \in (L(M))^*$  и  $M^* \subseteq (L(M))^*$ .

2. Пусть  $\alpha_1 v_1 + \dots + \alpha_s v_s$  — линейная комбинация векторов из  $M^*$ . Тогда для любого  $m \in M$  имеем  $(m, \alpha_1 v_1 + \dots + \alpha_s v_s) = \alpha_1 (m, v_1) + \dots + \alpha_s (m, v_s) = 0$ . Следовательно,  $\alpha_1 v_1 + \dots + \alpha_s v_s \in M^*$ .  $\square$

**Теорема 7.1.2.** Пусть  $U, W$  — подпространства конечномерного евклидова (унитарного) пространства  $V$ . Тогда выполняются следующие утверждения.

1.  $V = U \oplus U^*$ .
2.  $U^{**} = U$ .
3.  $(U + W)^* = U^* \cap W^*$ .
4.  $(U \cap W)^* = U^* + W^*$ .

**ДОКАЗАТЕЛЬСТВО.** 1. В силу п. 3 теоремы 7.1.1 подпространство  $U$  обладает ортонормированным базисом  $e_1, \dots, e_s$  и его можно дополнить до ортонормированного базиса  $e_1, \dots, e_s, e_{s+1}, \dots, e_n$  пространства  $V$ . Из п. 1 предложения 7.1.2 следует, что  $\{e_1, \dots, e_s\}^* = \langle e_1, \dots, e_s \rangle^* = U^*$ . Поскольку для любых  $i, j \in \{1, \dots, n\}$  выполняется  $\langle e_i, e_j \rangle = 0$  при  $i \neq j$ , то  $\langle e_{s+1}, \dots, e_n \rangle \subseteq U^*$ . Следовательно,  $V = U + U^*$ . Если вектор  $u \in U \cap U^*$ , то  $\langle u, u \rangle = 0$  и  $u = 0$ . Таким образом,  $V = \overline{U \oplus U^*}$ .

2. Пусть  $u \in U, w \in U^*$ . В силу свойства  $\langle a, b \rangle = \overline{\langle b, a \rangle}$  скалярного произведения равенства  $\langle u, w \rangle = 0$  и  $\langle w, u \rangle = 0$  равносильны. Отсюда  $U^{**} = U$ .

3. Так как  $U \subseteq U + W$ , то  $(U + W)^* \subseteq U^*$ . Аналогично  $(U + W)^* \subseteq W^*$ . Поэтому  $(U + W)^* \subseteq U^* \cap W^*$ . Для произвольного вектора  $z \in U^* \cap W^*$  и любых векторов  $u \in U, w \in W$  имеем  $\langle u + w, z \rangle = \langle u, z \rangle + \langle w, z \rangle = 0$ . Следовательно,  $z \in (U + W)^*$  и  $U^* \cap W^* \subseteq (U + W)^*$ .

4. Из пп. 2 и 3 теоремы следует, что  $U^* + W^* = (U^* + W^*)^{**} = ((U^* + W^*)^*)^* = (U^{**} \cap W^{**})^* = (U \cap W)^*$ .  $\square$

**Определение 7.1.9.** Пусть  $U$  — подпространство евклидова (унитарного) пространства  $V$ . Каждый вектор  $v \in V$  единственным образом разлагается в сумму  $v = u + w$ , где  $u \in U, w \in U^*$ . Вектор  $u$  из этого разложения называется *ортогональной проекцией* вектора  $v$  на подпространство  $U$ , а вектор  $w$  — *ортогональной составляющей* вектора  $v$  относительно  $U$ .

**УПРАЖНЕНИЕ 7.1.7.** Указать приём вычисления ортогональной проекции и ортогональной составляющей вектора  $v$ , если известны вектор  $v$  и базис  $u_1, \dots, u_s$  подпространства  $U$ . Найти ортогональную проекцию и ортогональную составляющую вектора  $v = x^2$  относительно подпространства  $U = \langle 1, x \rangle$  в евклидовом пространстве многочленов  $\mathbb{R}_2[x]$  относительно скалярного произведения, заданного правилом  $\langle f, g \rangle = \int_0^1 f(x)g(x)dx$ .

## § 7.2. Преобразования евклидовых и унитарных пространств

Начиная с этого параграфа, мы займёмся теорией линейных преобразований евклидовых и унитарных пространств, выделяя среди них

те, которые естественным образом согласуются со скалярным произведением, заданным на соответствующем пространстве.

**Определение 7.2.1.** Пусть  $F$  — поле действительных или комплексных чисел,  $A \in M_{m \times n}(F)$ . Матрица  $A^* = \overline{A}'$ , т. е. матрица, полученная из матрицы  $A$  транспонированием и комплексным сопряжением всех её элементов, называется *сопряжённой* к  $A$ .

УПРАЖНЕНИЕ 7.2.1. Проверьте следующие свойства сопряжённых матриц.

1.  $A^{**} = A$  и  $E^* = E$ .

2. Если  $A$  и  $B$  — матрицы одного и того же размера и  $\alpha, \beta \in F$ , то выполняется равенство  $(\alpha A + \beta B)^* = \overline{\alpha}A^* + \overline{\beta}B^*$ .

3. Если  $A$  и  $B$  — матрицы согласованных размеров, то выполняется равенство  $(AB)^* = B^*A^*$ .

ЗАМЕЧАНИЕ. Для произвольной строки  $[a]$ , используя принятое определение, мы можем обозначить столбец  $[\overline{a}]'$  через  $[a]^*$ . В частности, в ортонормированном базисе скалярное произведение векторов находится как  $(a, b) = [a][\overline{b}]' = [a][b]^*$ .

**Определение 7.2.2.** Пусть  $\varphi$  — линейное преобразование евклидова (унитарного) пространства  $V$ . Преобразование  $\varphi^*$  пространства  $V$  называется *сопряжённым* к преобразованию  $\varphi$ , если для любых векторов  $a, b \in V$  выполняется равенство  $(a\varphi, b) = (a, b\varphi^*)$ .

**Теорема 7.2.1** (о сопряжённом преобразовании). Пусть  $\varphi$  — линейное преобразование конечномерного евклидова (унитарного) пространства  $V$ . Тогда выполняются следующие утверждения.

1. Сопряжённое к  $\varphi$  преобразование  $\varphi^*$  существует, определено однозначно и является линейным преобразованием пространства  $V$ .

2. В любом ортонормированном базисе пространства  $V$  матрица сопряжённого преобразования сопряжена к матрице исходного преобразования, т. е.  $[\varphi^{**}] = [\varphi]^*$ .

3.  $\varphi^{**} = \varphi$  и  $\varepsilon^* = \varepsilon$ .

4. Для любых  $\varphi, \psi \in \mathcal{L}(V)$  и произвольных  $\alpha, \beta \in F$  выполняется  $(\alpha\varphi + \beta\psi)^* = \overline{\alpha}\varphi^* + \overline{\beta}\psi^*$ .

5. Для любых  $\varphi, \psi \in \mathcal{L}(V)$  выполняется  $(\varphi\psi)^* = \psi^*\varphi^*$ .

6. Если  $U$  —  $\varphi$ -инвариантное подпространство пространства  $V$ , то его ортогональное дополнение  $U^*$  инвариантно относительно  $\varphi^*$ .

ДОКАЗАТЕЛЬСТВО. 1. Зафиксируем некоторый ортонормированный базис пространства  $V$ . Пусть  $[\varphi]$  — матрица преобразования  $\varphi$  в данном

базисе. Обозначим через  $\psi$  линейное преобразование пространства  $V$ , матрица которого в том же базисе сопряжена к матрице  $[\varphi]$ , т. е.  $[\psi] = [\varphi]^* = \overline{[\varphi]}$ . Для любых векторов  $a, b \in V$  имеем

$$\begin{aligned} (a\varphi, b) &= [a\varphi][b]^* = ([a][\varphi])[b]^* = [a]([\varphi][b]^*) = [a]([\varphi]^*[b]^*) = \\ &= [a]([b][\varphi]^*)^* = [a][b\psi]^* = (a, b\psi). \end{aligned}$$

Таким образом, преобразование  $\psi = \varphi^*$  искомо. Из нашего определения  $\psi$  следует, что оно линейно. Осталось доказать, что преобразование  $\psi$  единственно.

**Лемма.** Пусть  $\varphi, \psi$  — произвольные (не обязательно линейные) преобразования пространства  $V$ . Если для любых  $a, b \in V$  выполняется  $(a, b\varphi) = (a, b\psi)$ , то  $\varphi = \psi$ .

**ДОКАЗАТЕЛЬСТВО ЛЕММЫ.** Из равенства  $(a, b\varphi) = (a, b\psi)$  следует, что  $0 = (a, b\varphi) - (a, b\psi) = (a, b\varphi - b\psi)$ . Поскольку эти равенства имеют место для любых векторов  $a$  и  $b$  пространства  $V$ , они выполняются и в случае, когда  $a = b\varphi - b\psi$ . Поэтому  $(b\varphi - b\psi, b\varphi - b\psi) = 0$ , откуда  $b\varphi - b\psi = 0$ . Следовательно, для любого вектора  $b \in V$  имеем  $b\varphi = b\psi$ , а значит,  $\varphi = \psi$ . Лемма доказана.

Пусть  $\tau$  — преобразование пространства  $V$ , сопряжённое к  $\varphi$ . Тогда  $(a, b\tau) = (a\varphi, b) = (a, b\psi)$ . По лемме  $\tau = \psi$ , и первый пункт теоремы полностью доказан.

2. Следует из доказательства п. 1.

Пп. 3–5 следуют из п. 2 и свойств матрицы, сопряжённой к данной (упражнение 7.2.1).

6. Пусть  $w \in U^*$ . Для любого  $u \in U$  вектор  $u\varphi \in U$ . Поэтому  $0 = (u\varphi, w) = (u, w\varphi^*)$ . Следовательно,  $w\varphi^* \in U^*$ .  $\square$

**УПРАЖНЕНИЕ 7.2.2.** Доказать пп. 3–5 непосредственно из определения сопряжённого преобразования.

В дальнейшем мы рассмотрим преобразования евклидовых и унитарных пространств, которые *согласованы* (в некотором точном смысле) с заданным на этих пространствах скалярным произведением. Существенную роль здесь будет играть понятие сопряжённого преобразования, поскольку *согласование* скалярного произведения и преобразования можно рассматривать как взаимосвязь между преобразованием и преобразованием, сопряжённым к нему. Наш первый шаг — изучение преобразований евклидовых и унитарных пространств, которые перестановочны со своими сопряжёнными.



**Определение 7.2.3.** Пусть  $\varphi$  — линейное преобразование евклидова (унитарного) пространства  $V$ . Преобразование  $\varphi$  называется *нормальным*, если  $\varphi\varphi^* = \varphi^*\varphi$ . Матрица  $A \in M_n(F)$ , где  $F = \mathbb{R}$  или  $\mathbb{C}$ , называется *нормальной*, если  $AA^* = A^*A$ .

**Теорема 7.2.2** (о свойствах нормального преобразования). Пусть  $\varphi$  — нормальное преобразование конечномерного евклидова (унитарного) пространства  $V$  над полем  $F$ ,  $A$  — нормальная матрица из  $M_n(F)$ . Тогда выполняются следующие утверждения.

1. Для любого многочлена  $f \in F[x]$  линейное преобразование  $f(\varphi)$  и матрица  $f(A)$  нормальны.
2. Если  $a$  — собственный вектор преобразования  $\varphi$  с собственным числом  $\lambda$ , то  $a$  — собственный вектор сопряжённого преобразования  $\varphi^*$  с собственным значением  $\bar{\lambda}$ .
3. Собственные векторы преобразования  $\varphi$ , соответствующие различным собственным значениям, ортогональны.

**ДОКАЗАТЕЛЬСТВО.** 1. Пусть  $f(x) = a_0 + a_1x + \dots + a_mx^m$ . Тогда из теоремы 7.2.1 следует, что  $f(\varphi)^* = (a_0\varepsilon + a_1\varphi + \dots + a_m\varphi^m)^* = \bar{a}_0 + \bar{a}_1\varphi^* + \dots + \bar{a}_m(\varphi^*)^m$ . Поскольку  $\varphi$  нормально, для любых  $i, j \in \mathbb{N}_0$  имеем  $(\varphi)^i(\varphi^*)^j = (\varphi^*)^j\varphi^i$ . Поэтому  $f(\varphi)f(\varphi)^* = f(\varphi)^*f(\varphi)$ . Для матриц проводится аналогичное рассуждение.

2. Положим  $\psi = \varphi - \lambda\varepsilon$ . В силу п. 1 преобразование  $\psi$  нормально, т. е. перестановочно с сопряжённым к нему преобразованием  $\psi^*$ , которое по теореме 7.2.1 равно  $\varphi^* - \bar{\lambda}\varepsilon$ . Для собственного вектора  $a$  преобразования  $\varphi$  с собственным числом  $\lambda$  выполняется  $a\psi = 0$ . Имеем  $0 = (a\psi, a\psi) = (a, a\psi\psi^*) = (a, \psi^*\psi) = (a\psi^*, a\psi^*)$ . Следовательно,  $0 = a\psi^* = a(\varphi^* - \bar{\lambda}\varepsilon)$ , т. е.  $a\varphi^* = \bar{\lambda}a$ .

3. Пусть  $a\varphi = \lambda a$ ,  $b\varphi = \mu b$ , где  $\lambda \neq \mu$ . Тогда  $\lambda(a, b) = (\lambda a, b) = (a\varphi, b) = (a, b\varphi^*) = (a, \bar{\mu}b) = \mu(a, b)$ . Поэтому  $(\lambda - \mu)(a, b) = 0$ , откуда  $(a, b) = 0$ .  $\square$

**Теорема 7.2.3** (о каноническом виде матрицы нормального преобразования в унитарном пространстве). Пусть  $\varphi$  — нормальное преобразование конечномерного унитарного пространства  $V$ . Тогда существует ортонормированный базис пространства  $V$ , состоящий из собственных векторов преобразования  $\varphi$ , и матрица преобразования  $\varphi$  в этом базисе диагональна.

**ДОКАЗАТЕЛЬСТВО.** Докажем теорему индукцией по  $n = \dim V$ . При  $n = 1$  утверждение очевидно. Предположим, что  $n > 1$  и что для пространств размерности, меньшей  $n$ , теорема уже доказана.

Предположим, что в  $V$  есть собственное ненулевое подпространство  $U$ , инвариантное относительно преобразований  $\varphi$  и  $\varphi^*$ . Пространство  $V$  есть прямая сумма  $U$  и его ортогонального дополнения:  $V = U \oplus U^*$ . Поскольку по нашему предположению  $U$  является  $\{\varphi, \varphi^*\}$ -инвариантным подпространством, из п. 6 теоремы 7.2.1 вытекает, что  $U^*$  инвариантно относительно этих преобразований. Положим  $\psi = \varphi|_U$  и  $\tau = \varphi|_{U^*}$ . Очевидно, что  $\psi^* = \varphi^*|_U$  и  $\tau^* = \varphi^*|_{U^*}$ . Поэтому преобразования  $\psi$  и  $\tau$  нормальны, а значит, удовлетворяют условию теоремы. По предположению индукции подпространства  $U$  и  $U^*$  обладают ортонормированными базисами, состоящими из собственных векторов этих преобразований. Но собственные векторы преобразований  $\psi$  и  $\tau$  являются собственными векторами преобразования  $\varphi$ . Следовательно, объединение этих базисов — ортонормированный базис пространства  $V$ , в котором матрица преобразования  $\varphi$  диагональна. Таким образом, при доказательстве теоремы индукцией по  $n$  можно считать, что каждое ненулевое  $\{\varphi, \varphi^*\}$ -инвариантное подпространство совпадает с самим пространством  $V$ .

Поскольку поле  $\mathbb{C}$  алгебраически замкнуто, корни характеристического многочлена  $f_\varphi(x)$  преобразования  $\varphi$  лежат в  $\mathbb{C}$ , а значит, являются собственными числами преобразования  $\varphi$ . Если  $\lambda$  — один из этих корней, то найдётся ненулевой собственный вектор  $u$ , такой, что  $u\varphi = \lambda u$ . Из п. 2 теоремы 7.2.2 следует, что  $u\varphi^* = \bar{\lambda}u$ . Поэтому одномерное подпространство  $U$ , натянутое на вектор  $u$ , является  $\{\varphi, \varphi^*\}$ -инвариантным. Тогда  $U$  должно совпадать с  $V$ , и теорема доказана.

**Теорема 7.2.4** (о каноническом виде матрицы нормального преобразования в евклидовом пространстве). Пусть  $\varphi$  — нормальное преобразование конечномерного евклидова пространства  $V$ . Тогда существует ортонормированный базис пространства  $V$ , такой, что матрица преобразования  $\varphi$  в этом базисе имеет клеточно диагональный вид

$$[\varphi] = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_m \end{pmatrix}.$$

Каждая клетка этой матрицы либо одномерна и содержит в качестве элемента вещественный характеристический корень преобразования  $\varphi$ , либо двумерна, имеет вид

$$r \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$$

и соответствует паре комплексно сопряжённых характеристических корней преобразования  $\varphi$ , один из которых равен  $\lambda = r(\cos \alpha + i \sin \alpha)$ .

Снова воспользуемся индукцией по  $n = \dim V$ . Как и при доказательстве предыдущей теоремы, мы можем считать, что  $V$  не содержит собственных ненулевых  $\{\varphi, \varphi^*\}$ -инвариантных подпространств. В частности, если  $\lambda$  — вещественный характеристический корень преобразования  $\varphi$ , то, рассуждая как при доказательстве предыдущей теоремы, получим, что пространство  $V$  совпадает с одномерным подпространством, натянутым на собственный вектор преобразования  $\varphi$ , соответствующий  $\lambda$ . Следовательно, можно считать, что все корни характеристического многочлена  $f(x)$  преобразования  $\varphi$  не лежат в поле действительных чисел. Пусть один из корней равен  $\lambda = r(\cos \alpha + i \sin \alpha)$ . Поскольку  $f(x)$  имеет действительные коэффициенты, то комплексно сопряжённое число  $\bar{\lambda} = r(\cos \alpha - i \sin \alpha)$  тоже лежит в спектре преобразования  $\varphi$ .

Зафиксируем в пространстве  $V$  ортонормированный базис, состоящий из векторов  $e_1, \dots, e_n$ . Пусть  $A$  — матрица преобразования  $\varphi$  в этом базисе. Рассмотрим теперь унитарное арифметическое пространство  $\mathbb{C}^n$ , на котором задано стандартное скалярное произведение. Поскольку можно считать, что  $A \in M_n(\mathbb{C})$ , матрицу  $A$  можно рассматривать как линейное преобразование пространства  $\mathbb{C}^n$ . Преобразование  $\varphi$  нормально, поэтому нормальна и матрица  $A$ , а значит, нормально и преобразование, задаваемое ею в  $\mathbb{C}^n$ . По теореме 7.2.3 пространство  $\mathbb{C}^n$  обладает ортонормированным базисом из собственных векторов преобразования  $A$ . Так как характеристические многочлены матрицы  $A$  и преобразования  $\varphi$  равны, корни  $\lambda$  и  $\bar{\lambda}$  являются собственными числами преобразования  $A$  пространства  $\mathbb{C}^n$ . Пусть строка  $[v] \in \mathbb{C}^n$  — собственный вектор преобразования  $A$ , соответствующий  $\lambda$ . Из равенства  $[v]A = \lambda[v]$  и вещественности элементов матрицы  $A$  следует, что  $[v]A = \overline{[v]A} = \overline{[v]}A = \lambda[v] = \bar{\lambda}[\bar{v}]$ . Значит, строка  $[\bar{v}]$  — собственный вектор преобразования  $A$  с собственным числом  $\bar{\lambda}$ . В частности, векторы  $[v]$  и  $[\bar{v}]$  ортогональны (см. п. 3 теоремы 7.2.2). Пусть  $[v] = (\alpha_1 + i\beta_1, \dots, \alpha_n + i\beta_n)$ , где  $\alpha_k, \beta_k \in \mathbb{R}$  — действительная и мнимая части  $k$ -го элемента строки  $[v]$ . Тогда  $[\bar{v}] = (\alpha_1 - i\beta_1, \dots, \alpha_n - i\beta_n)$ . Несложно также заметить, что эти векторы имеют одинаковую длину. Рассмотрим теперь строки

$$[a] = \frac{1}{2}([v] + [\bar{v}]) = (\alpha_1, \dots, \alpha_n),$$

$$[b] = \frac{1}{2i}([v] - \overline{[v]}) = (\beta_1, \dots, \beta_n)$$

пространства  $\mathbb{C}^n$ , элементы которых вещественны и равны действительной и мнимой частям соответствующих элементов строки  $[v]$ . Заметим, что  $|[a]| = |[b]| = |[v]|/\sqrt{2}$ , поэтому если выбрать  $[v]$  так, чтобы  $|[v]| = \sqrt{2}$ , то  $[a]$  и  $[b]$  будут иметь единичную длину. Далее,  $([a], [b]) = (\frac{1}{2}([v] + \overline{[v]}), \frac{1}{2i}([v] - \overline{[v]})) = 0$ . Поэтому векторы  $[a]$  и  $[b]$  образуют ортонормированный базис двумерного подпространства в  $\mathbb{C}^n$ .

Вычислим теперь образы векторов  $[a]$  и  $[b]$  под действием преобразований  $A$  и  $A^*$ . Имеем

$$\begin{aligned} ([a] + i[b])A &= [v]A = \lambda[v] = r(\cos \alpha + i \sin \alpha)([a] + i[b]) = \\ &= r(\cos \alpha [a] - \sin \alpha [b]) + ir(\sin \alpha [a] + \cos \alpha [b]). \end{aligned}$$

Сравнивая действительные и мнимые части, окончательно получаем равенства

$$\begin{aligned} [a]A &= r(\cos \alpha [a] - \sin \alpha [b]), \\ [b]A &= r(\sin \alpha [a] + \cos \alpha [b]). \end{aligned} \quad (1)$$

Исходя из равенств (1) и используя п. 2 теоремы 7.2.2, несложно проверить следующие два равенства:

$$\begin{aligned} [a]A^* &= r(\cos \alpha [a] + \sin \alpha [b]), \\ [b]A^* &= r(-\sin \alpha [a] + \cos \alpha [b]). \end{aligned} \quad (2)$$

Вернёмся теперь к исходному евклидову пространству  $V$  и рассмотрим в нём подпространство, натянутое на векторы  $a = \sum_{k=1}^n \alpha_k e_k$  и  $b = \sum_{k=1}^n \beta_k e_k$ , строки которых в зафиксированном нами ортонормированном базисе равны  $[a]$  и  $[b]$ . По доказанному векторы  $a$  и  $b$  образуют ортонормированный базис двумерного подпространства  $U = \langle a, b \rangle$  пространства  $V$ . Поскольку матрицы преобразований  $\varphi$  и  $\varphi^*$  в этом базисе равны  $A$  и  $A^*$  соответственно, из равенств (1) и (2) следует, что подпространство  $U$  инвариантно относительно  $\varphi$  и  $\varphi^*$ . Следовательно, можно считать, что  $V = U$ . Снова применяя (1), получаем, что матрица преобразования  $\varphi$  имеет вид

$$r \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}.$$

**УПРАЖНЕНИЕ 7.2.3.** Указать и обосновать практический способ поиска ортонормированного базиса унитарного и евклидова пространств,

в котором матрица нормального преобразования имеет канонический вид. Проверить, что матрица

$$A = \begin{pmatrix} 3 & 1 & -\sqrt{6} \\ 1 & 3 & \sqrt{6} \\ \sqrt{6} & -\sqrt{6} & 2 \end{pmatrix}$$

нормальна. Найти канонический вид матрицы  $A$  нормального преобразования сначала в унитарном, а затем евклидовом пространстве. Указать ортонормированный базис, в котором этот вид достигается.

### § 7.3. Ортогональные и унитарные преобразования

**Определение 7.3.1.** Линейное преобразование  $\varphi$  евклидова (унитарного) пространства  $V$  называется *ортогональным (унитарным)*, если для любых векторов  $a, b \in V$  выполняется равенство  $(a\varphi, b\varphi) = (a, b)$

ЗАМЕЧАНИЕ. Иными словами, преобразование ортогонально (соответственно унитарно), если оно *сохраняет* скалярное произведение.

**Определение 7.3.2.** Матрица  $A$  из  $M_n(\mathbb{R})$  (из  $M_n(\mathbb{C})$ ) называется *ортогональной (унитарной)*, если  $AA^* = E$ .

ПРИМЕР. Пусть  $V = E^2$  — пространство геометрических векторов плоскости со стандартным скалярным произведением (см. пример 1 после определения 7.1.2). Поворот на угол  $\alpha$  относительно начала координат и осевая симметрия относительно оси абсцисс сохраняют скалярное произведение, а значит, являются ортогональными операторами на  $V$ .

**Теорема 7.3.1.** Пусть  $\varphi$  — линейное преобразование конечномерного евклидова (унитарного) пространства  $V$ . Следующие утверждения эквивалентны.

1. Преобразование  $\varphi$  ортогонально (унитарно).
2. Для любого  $a \in V$  выполняется  $|a\varphi| = |a|$ .
3. Имеет место равенство  $\varphi\varphi^* = \varepsilon$ .
4. Матрица преобразования  $\varphi$  в любом ортонормированном базисе ортогональна (унитарна).
5. Преобразование  $\varphi$  переводит любой ортонормированный базис снова в ортонормированный базис.

ДОКАЗАТЕЛЬСТВО. (1  $\Rightarrow$  2) Очевидно, так как  $|a\varphi| = |a|$  тогда и только тогда, когда  $(a\varphi, a\varphi) = (a, a)$ .

(2  $\Rightarrow$  1) Для любых  $x, y \in V$  и  $\lambda \in F$  (где  $F = \mathbb{R}$  или  $\mathbb{C}$ ) имеем

$$(x + \lambda y, x + \lambda y) = (x, x) + \lambda(y, x) + \bar{\lambda}(x, y) + \lambda\bar{\lambda}(y, y).$$

С другой стороны,

$$\begin{aligned} (x + \lambda y, x + \lambda y) &= ((x + \lambda y)\varphi, (x + \lambda y)\varphi) = (x\varphi + \lambda y\varphi, x\varphi + \lambda y\varphi) = \\ &= (x\varphi, x\varphi) + \lambda(y\varphi, \lambda\varphi) + \bar{\lambda}(x\varphi, y\varphi) + \lambda\bar{\lambda}(y\varphi, y\varphi). \end{aligned}$$

Таким образом,

$$\lambda(y, x) + \bar{\lambda}(x, y) = \lambda(y\varphi, x\varphi) + \bar{\lambda}(x\varphi, y\varphi). \quad (1)$$

Полагая  $\lambda = 1$  в равенстве (1), получаем

$$(y, x) + (x, y) = (y\varphi, x\varphi) + (x\varphi, y\varphi). \quad (2)$$

Если  $F = \mathbb{R}$ , то требуемое доказано, так как в этом случае  $(x, y) = (y, x)$ .

Если  $F = \mathbb{C}$ , то положим дополнительно  $\lambda = i$  в равенстве (1). Тогда

$$i(y, x) - i(x, y) = i(y\varphi, x\varphi) - i(x\varphi, y\varphi),$$

откуда

$$(y, x) - (x, y) = (y\varphi, x\varphi) - (x\varphi, y\varphi). \quad (3)$$

Вычитая из равенства (2) равенство (3), получим  $2(x, y) = 2(x\varphi, y\varphi)$ , что и требовалось.

(1  $\Rightarrow$  3) Для всех  $a, b \in V$  выполняются равенства  $(a, b\varepsilon) = (a, b) = (a\varphi, b\varphi) = (a, b\varphi\varphi^*)$ . В силу леммы из доказательства теоремы 7.2.1 имеем  $\varphi\varphi^* = \varepsilon$ .

(3  $\Rightarrow$  4) По условию  $\varphi\varphi^* = \varepsilon$ . Следовательно, в любом ортонормированном базисе для матриц соответствующих преобразований выполняются равенства:

$$E = [\varepsilon] = [\varphi\varphi^*] = [\varphi][\varphi^*] = [\varphi][\varphi]^*,$$

причём последнее из них имеет место в силу п. 2 теоремы 7.2.1.

(4  $\Rightarrow$  5) Пусть  $e_1, \dots, e_n$  — ортонормированный базис. Докажем, что  $e_1\varphi, \dots, e_n\varphi$  тоже является ортонормированным базисом, т. е.  $(e_i\varphi, e_j\varphi) = (e_i, e_j)$  для всех  $i, j \in \{1, \dots, n\}$ . Имеем:

$$(e_i\varphi, e_j\varphi) = [e_i\varphi][e_j\varphi]^* = [e_i][\varphi][\varphi]^*[e_j]^* = [e_i][e_j]^* = (e_i, e_j).$$

(5  $\Rightarrow$  1) Пусть  $e_1, \dots, e_n$  — ортонормированный базис. Тогда для любых  $a, b \in V$

$$\begin{aligned} (a\varphi, b\varphi) &= \left( \left( \sum_{i=1}^n a_i e_i \right) \varphi, \left( \sum_{j=1}^n b_j e_j \right) \varphi \right) = \\ &= \left( \sum_{i=1}^n a_i (e_i \varphi), \sum_{j=1}^n b_j (e_j \varphi) \right) = \sum_{i=1}^n a_i \bar{b}_i = \left( \sum_{i=1}^n a_i e_i, \sum_{j=1}^n b_j e_j \right) = (a, b). \end{aligned}$$

□

**Следствие.** Матрица перехода от ортонормированного базиса к ортонормированному базису ортогональна (унитарна).

**УПРАЖНЕНИЕ 7.3.1. 1.** Пусть  $V$  — евклидово (унитарное) пространство. Обозначим через  $GO(V)$  (через  $GU(V)$ ) множество всех ортогональных (унитарных) преобразований пространства  $V$ . Доказать, что  $GO(V)$  (соответственно  $GU(V)$ ) — подгруппа общей группы  $GL(V)$  невырожденных линейных преобразований пространства  $V$ .

2. Положим  $GO_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid AA^* = E\}$  и  $GU_n(\mathbb{C}) = \{A \in GL_n(\mathbb{C}) \mid AA^* = E\}$ . Доказать, что  $GO_n(\mathbb{R})$  и  $GU_n(\mathbb{C})$  — подгруппы групп  $GL_n(\mathbb{R})$  и  $GL_n(\mathbb{C})$  соответственно.

**Определение 7.3.3.** Группы, определённые в упражнении 7.3.1, называются:

$GO(V)$  — общая группа ортогональных преобразований евклидова пространства  $V$ ;

$GU(V)$  — общая группа унитарных преобразований унитарного пространства  $V$ ;

$GO_n(\mathbb{R})$  — общая группа ортогональных матриц размерности  $n$  над полем  $\mathbb{R}$ ;

$GU_n(\mathbb{C})$  — общая группа унитарных матриц размерности  $n$  над полем  $\mathbb{C}$ .

Подгруппы этих групп носят те же названия, но без прилагательного “общая”.

**Теорема 7.3.2. 1.** Пусть  $A$  — нормальная матрица из  $M_n(\mathbb{C})$ . Тогда существует матрица  $U \in GU_n(\mathbb{C})$ , такая, что матрица  $D = UAU^*$  диагональна.

2. Пусть  $A$  — нормальная матрица из  $M_n(\mathbb{R})$ . Тогда существует матрица  $O \in GO_n(\mathbb{R})$ , такая, что матрица  $B = OAO^*$  клеточно

диагональна и каждая клетка либо одномерна, либо двумерна и имеет вид

$$r \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}.$$

**ДОКАЗАТЕЛЬСТВО.** 1. Пусть  $V = \mathbb{C}^n$  — унитарное арифметическое пространство. Рассмотрим преобразование  $\varphi$  этого пространства, матрица которого  $[\varphi]_1$  в стандартном базисе равна  $A$ . Преобразование  $\varphi$  нормально, так как нормальна матрица  $A$ . По теореме 7.2.3 существует ортонормированный базис пространства  $V$ , для которого  $[\varphi]_2 = D$  — диагональная матрица. Матрица перехода  $U$  от стандартного базиса к этому базису унитарна по следствию из теоремы 7.3.1, следовательно,  $D = UAU^{-1} = UAU^*$ .

2. Аналогично пусть  $\varphi$  — преобразование евклидова арифметического пространства  $V = \mathbb{R}^n$ , такое, что в стандартном базисе выполняется  $[\varphi]_1 = A$ . По теореме 7.2.4 существует ортонормированный базис, в котором матрица  $[\varphi]_2 = B$  преобразования  $\varphi$  имеет требуемый вид и матрица перехода  $O$  к данному базису ортогональна. Тогда  $B = OAO^{-1} = OAO^*$ .  $\square$

**Теорема 7.3.3** (о каноническом виде матрицы унитарного и ортогонального преобразований). 1. Собственные числа унитарного преобразования конечномерного унитарного пространства по модулю равны единице.

2. Характеристические корни унитарной матрицы по модулю равны единице.

3. Характеристические корни ортогонального преобразования конечномерного евклидова пространства по модулю равны единице.

4. Если  $A$  — унитарная матрица, то существует унитарная матрица  $U$ , такая, что  $UAU^* = \begin{pmatrix} \lambda & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$ , где  $|\lambda_i| = 1$ .

5. Если  $A$  — ортогональная матрица, то существует ортогональная матрица  $O$ , такая, что  $OAO^* = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_s \end{pmatrix}$ , где  $A_i = (\pm 1)$

или  $\begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$ .

**ДОКАЗАТЕЛЬСТВО.** 1. Пусть  $\lambda$  — собственное число унитарного преобразования  $\varphi$ . Тогда существует  $a \neq 0$ , для которого  $a\varphi = \lambda a$  и, следо-



вательно,

$$(a\varphi, a\varphi) = (\lambda a, \lambda a) = \lambda\bar{\lambda}(a, a).$$

Так как преобразование  $\varphi$  унитарно, то  $(a, a) = (a\varphi, a\varphi) = \lambda\bar{\lambda}(a, a)$ . Поэтому  $\lambda\bar{\lambda} = 1$ . Отсюда  $|\lambda| = 1$ .

2. Пусть  $A \in GU_n(\mathbb{C})$ . Рассмотрим  $V = \mathbb{C}^n$  — унитарное арифметическое пространство со стандартным скалярным произведением. Выберем линейное преобразование  $\varphi$  пространства  $V$  так, чтобы в стандартном базисе его матрица равнялась  $A$ . Тогда характеристические корни матрицы  $A$  — это собственные числа преобразования  $\varphi$ , модули которых в силу п. 1 равны единице.

3. Утверждение вытекает из п. 2. Действительно, пусть  $[\varphi] = A$  — матрица исходного ортогонального преобразования  $\varphi$  в ортонормированном базисе. Матрица  $A$  ортогональна, значит, если рассматривать  $A$  как матрицу из  $M_n(\mathbb{C})$ , то  $A$  унитарна. Следовательно, характеристические корни матрицы  $A$  равны единице. Осталось заметить, что  $\text{Sp}(\varphi) = \text{Sp}(A)$ .

4. Так как  $A$  — унитарная матрица, то  $AA^* = E = A^*A$ , поэтому  $A$  нормальна. Значит, по теореме 7.3.2 имеет место равенство  $D = UAU^*$ , где  $D$  — диагональная матрица. Числа, стоящие на главной диагонали этой матрицы совпадают с характеристическими корнями матрицы  $A$ , которые в силу п. 2 по модулю равны единице.

5. Поскольку матрица  $A$  нормальна, аналогично п. 4 используется теорема 7.3.2. Далее, характеристические корни матрицы  $A$  по модулю равны 1. Поэтому если  $\lambda \in \text{Sp}(A)$  лежит в  $\mathbb{R}$ , то  $\lambda = \pm 1$ . Если же  $\lambda = r(\cos \alpha + i \sin \alpha) \in \mathbb{C} \setminus \mathbb{R}$ , то  $r = 1$  и соответствующая двумерная клетка имеет вид  $\begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$ .  $\square$

**УПРАЖНЕНИЕ 7.3.2.** Доказать, что в пространстве  $E^2$  геометрических векторов плоскости каждое ортогональное преобразование является либо поворотом, либо осевой симметрией.

**УПРАЖНЕНИЕ 7.3.3** (теорема Эйлера). Доказать, что в пространстве  $E^3$  геометрических векторов пространства каждое ортогональное преобразование является либо поворотом относительно прямой, либо композицией поворота относительно прямой и симметрии относительно плоскости, ортогональной к этой прямой.

§ 7.4. Самосопряжённые и косоэрмитовы преобразования

**Определение 7.4.1.** Пусть  $\varphi$  — линейное преобразование евклидова или унитарного пространства  $V$ . Преобразование  $\varphi$  называется *самосопряжённым* (или *симметрическим*), если  $\varphi^* = \varphi$ . Преобразование  $\varphi$  называется *косоэрмитовым* (или *кососимметрическим*), если  $\varphi^* = -\varphi$ .

УПРАЖНЕНИЕ 7.4.1. Преобразование  $\varphi$  евклидова или унитарного пространства  $V$  является самосопряжённым (соответственно косоэрмитовым) тогда и только тогда, когда для любых  $a, b \in V$  выполняется  $(a\varphi, b) = (a, b\varphi)$  (соответственно  $(a\varphi, b) = -(a, b\varphi)$ ).

Напомним, что квадратная матрица  $A$  называется симметрической, если она совпадает с матрицей, транспонированной к ней:  $A = A'$ , и кососимметрической, если  $A = -A'$ .

**Определение 7.4.2.** Матрица  $A \in M_n(\mathbb{C})$  называется *эрмитовой* (соответственно косоэрмитовой), если  $A = \overline{A}'$  (соответственно  $A = -\overline{A}'$ ).

ПРИМЕР. В силу теоремы 7.2.1 матрица самосопряжённого преобразования в ортонормированном базисе эрмитова, причём в случае евклидова пространства она также является симметрической. Аналогично матрица косоэрмитова преобразования в ортонормированном базисе косоэрмитова, причём в случае евклидова пространства она является и кососимметрической.

**Теорема 7.4.1** (о каноническом виде матрицы самосопряжённого преобразования). 1. *Собственные числа самосопряжённого преобразования конечномерного унитарного пространства являются вещественными.*

2. *Характеристические корни эрмитовой матрицы вещественны.*

3. *Собственные числа самосопряжённого преобразования конечномерного евклидова пространства вещественны.*

4. *Если  $\varphi$  — самосопряжённое преобразование конечномерного евклидова (унитарного) пространства, то существует ортонормированный базис, состоящий из собственных векторов преобразования  $\varphi$ .*

5. *Если  $A$  — симметрическая (эрмитова) матрица, то существует ортогональная (унитарная) матрица  $U$ , такая, что  $D = UAU^*$  — вещественная диагональная матрица.*

ДОКАЗАТЕЛЬСТВО. 1. Поскольку  $\varphi\varphi^* = \varphi^2 = \varphi^*\varphi$ , преобразование  $\varphi$  нормально. Следовательно, собственный вектор  $a$  преобразования  $\varphi$

с собственным числом  $\lambda$  является собственным вектором для  $\varphi^* = \varphi$  с собственным числом  $\bar{\lambda}$  (теорема 7.2.2). Отсюда  $\lambda = \bar{\lambda} \in \mathbb{R}$ .

2. Если  $V = \mathbb{C}^n$  — унитарное пространство со стандартным скалярным произведением, то эрмитова матрица  $A$  соответствует самосопряжённому преобразованию этого пространства и требуется вытекает из п. 1.

3. Пусть  $\varphi$  — самосопряжённое преобразование евклидова пространства  $V$  и  $A$  — его матрица в ортонормированном базисе. Тогда матрица  $A \in M_n(\mathbb{R}) \subseteq M_n(\mathbb{C})$  является эрмитовой. Остается применить п. 2.

4. Если  $V$  — унитарное пространство, то утверждение следует из нормальности  $\varphi$  и п. 1.

Если  $V$  — евклидово пространство, то в силу нормальности  $\varphi$  существует ортонормированный базис, в котором  $[\varphi] = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_s \end{pmatrix}$ ,

где  $A_i$  одномерны или двумерны. Но двумерные клетки соответствуют только тем характеристическим корням преобразования  $\varphi$ , которые не лежат в  $\mathbb{R}$ , а таких в силу п. 3 преобразование  $\varphi$  не имеет.

5. Следует из теоремы 7.3.2 и п. 2.  $\square$

**Теорема 7.4.2** (о каноническом виде матрицы косоэрмитова преобразования). 1. Собственные числа косоэрмитова преобразования конечномерного унитарного пространства лежат в множестве  $i\mathbb{R}$ .

2. Спектр косоэрмитова преобразования (косоэрмитовой матрицы) лежит в множестве  $i\mathbb{R}$ .

3. Если  $\varphi$  — косоэрмитово преобразование конечномерного унитарного пространства, то существует ортонормированный базис, в котором матрица преобразования  $\varphi$  диагональна.

4. Если  $\varphi$  — косоэрмитово преобразование конечномерного евклидова пространства, то существует ортонормированный базис, в котором матрица преобразования  $\varphi$  клеточно диагональна. Каждая клетка этой матрицы либо одномерная нулевая, либо имеет вид  $\begin{pmatrix} 0 & -b \\ b & 0 \end{pmatrix}$ , где  $b \in \mathbb{R}$ .

УПРАЖНЕНИЕ 7.4.2. Доказать теорему 7.4.2.

УПРАЖНЕНИЕ 7.4.3. 1. Если  $\varphi$  — линейное преобразование евклидова (унитарного) пространства, то  $\varphi + \varphi^*$  и  $\varphi\varphi^*$  — самосопряжённые, а  $\varphi - \varphi^*$  — косоэрмитово преобразования.

2. Если  $\varphi, \psi$  — самосопряжённые (косоэрмитовы) преобразования,  $\alpha \in \mathbb{R}$ , то  $\varphi + \psi, \alpha\varphi$  — тоже самосопряжённые (косоэрмитовы) преобразования.

3. Если  $\varphi, \psi$  — самосопряжённые преобразования, то преобразование  $\varphi\psi$  самосопряжённое тогда и только тогда, когда  $\varphi\psi = \psi\varphi$ .

4. Каждое линейное преобразование евклидова (унитарного) пространства может быть представлено в виде суммы самосопряжённого и косоэрмитова преобразований.

5. Каждое линейное преобразование  $\varphi$  унитарного пространства может быть представлено в виде  $\varphi = \psi + i\tau$ , где  $\psi$  и  $\tau$  — самосопряжённые преобразования.

Теперь мы рассмотрим самосопряжённые преобразования специального вида, которые играют важную роль в дальнейшем изложении.

**Определение 7.4.3.** Самосопряжённое преобразование  $\varphi$  евклидова (унитарного) пространства  $V$  называется *неотрицательным*, если для любого  $a \in V$  число  $(a\varphi, a)$  является вещественным неотрицательным числом. Если, кроме того, для любого  $a \neq 0$  число  $(a\varphi, a)$  положительно, то  $\varphi$  называется *положительным*.

**Теорема 7.4.3.** Пусть  $V$  — конечномерное евклидово или унитарное пространство. Тогда выполняются следующие утверждения.

1. Самосопряжённое преобразование  $\varphi$  неотрицательно тогда и только тогда, когда характеристические корни преобразования  $\varphi$  неотрицательны.

2. Для неотрицательного преобразования  $\varphi$  определено значение  $\sqrt{\varphi}$  функции  $f(x) = \sqrt{x}$  (арифметический корень). Преобразование  $\psi = \sqrt{\varphi}$  является единственным неотрицательным линейным преобразованием пространства  $V$ , для которого  $\psi^2 = \varphi$ .

**ДОКАЗАТЕЛЬСТВО.** 1. Пусть  $\varphi$  неотрицательно. Каждый характеристический корень  $\lambda$  преобразования  $\varphi$  является вещественным числом, а значит, является собственным числом преобразования  $\varphi$ . Поэтому существует собственный вектор  $a$  преобразования  $\varphi$ , для которого  $a\varphi = \lambda a$ . Тогда по определению неотрицательного преобразования имеем  $\lambda(a, a) = (\lambda a, a) = (a\varphi, a) \geq 0$ , откуда  $\lambda \geq 0$ .

Пусть все характеристические корни самосопряжённого преобразования  $\varphi$  неотрицательны. Рассмотрим ортонормированный базис  $V$ , состоящий из собственных векторов  $e_1, \dots, e_n$  преобразования  $\varphi$  (он существует в силу теоремы 7.4.1). Пусть  $a$  — произвольный вектор

из  $V$  и  $a = \sum_{i=1}^n \alpha_i e_i$ . Тогда  $(a\varphi, a) = \left( \left( \sum_{i=1}^n \alpha_i e_i \right) \varphi, \sum_{j=1}^n \alpha_j e_j \right) = \left( \sum_{i=1}^n \lambda_i \alpha_i e_i, \sum_{j=1}^n \alpha_j e_j \right) = \sum_{i=1}^n \lambda_i \alpha_i \bar{\alpha}_i (e_i, e_i) = \sum_{i=1}^n \lambda_i |\alpha_i|^2 \geq 0$ .

**УПРАЖНЕНИЕ 7.4.4.** Доказать, что в определении неотрицательного преобразования можно сразу считать, что число  $(a\varphi, a) \in \mathbb{R}$ .

**УПРАЖНЕНИЕ 7.4.5.** Самосопряжённое преобразование  $\varphi$  положительно тогда и только тогда, когда собственные значения  $\varphi$  положительны.

2. Поскольку преобразование  $\varphi$  неотрицательно, существует ортонормированный базис, в котором  $[\varphi] = D(\lambda_1, \dots, \lambda_n)$  — диагональная матрица и  $\lambda_i \geq 0$  для любого  $i = 1, \dots, n$ . Тогда  $[\sqrt{\varphi}] = D(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_n})$  по определению функции от линейного преобразования. Преобразование  $\psi = \sqrt{\varphi}$  в силу п. 1 является неотрицательным самосопряжённым преобразованием, и  $\psi^2 = \varphi$ . Докажем, что  $\psi$  — единственное неотрицательное преобразование с этим свойством. Пусть  $\tau$  — неотрицательное преобразование, для которого  $\tau^2 = \varphi$ . Рассмотрим ортонормированный базис пространства  $V$ , в котором  $[\tau] = D(\mu_1, \dots, \mu_n)$  и  $\mu_i \geq 0$  для любого  $i = 1, \dots, n$ . Тогда в этом же базисе  $[\varphi] = [\tau]^2 = D(\mu_1^2, \dots, \mu_n^2) = D(\lambda_1, \dots, \lambda_n)$ . Снова в том же базисе имеем:

$$[\psi] = [\sqrt{\varphi}] = D(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_n}) = D(\mu_1, \dots, \mu_n) = [\tau].$$

Таким образом,  $\psi = \tau$ , что и требовалось.  $\square$

**Определение 7.4.4.** Эрмитова или симметрическая матрица  $A$  называется *неотрицательной* (*положительной*), если её характеристические корни неотрицательны (*положительны*).

**Следствие.** Неотрицательное (*положительное*) преобразование евклидова (*соответственно унитарного*) пространства в ортонормированном базисе имеет неотрицательную (*положительную*) симметрическую (*соответственно эрмитову*) матрицу.

## § 7.5. Сингулярные числа, полярное и сингулярное разложения

**Определение 7.5.1.** Два линейных преобразования  $\varphi$  и  $\psi$  евклидова (*унитарного*) пространства  $V$  *изометричны*, если для любых  $a, b \in V$

выполняется  $(a\varphi, b\varphi) = (a\psi, b\psi)$ .

**ПРИМЕР.** Каждое унитарное (ортогональное) преобразование  $\varphi$  изометрично тождественному преобразованию  $\varepsilon$ , так как  $(a\varphi, b\varphi) = (a, b) = (a\varepsilon, b\varepsilon)$ .

**УПРАЖНЕНИЕ 7.5.1.** Доказать, что  $\varphi$  нормально тогда и только тогда, когда  $\varphi$  и  $\varphi^*$  изометричны.

**Теорема 7.5.1.** Пусть  $\varphi$  — линейное преобразование евклидова (унитарного) пространства  $V$ . Тогда преобразование  $\varphi\varphi^*$  является неотрицательным самосопряжённым преобразованием, а преобразование  $\psi = \sqrt{\varphi\varphi^*}$  изометрично преобразованию  $\varphi$ .

**ДОКАЗАТЕЛЬСТВО.** Преобразование  $\varphi\varphi^*$  является самосопряжённым (см. п. 1 упражнения 7.4.3). Кроме того,  $(a\varphi\varphi^*, a) = (a\varphi, a\varphi) \geq 0$ , а значит,  $\varphi$  неотрицательно. Следовательно, в силу теоремы 7.4.3 неотрицательное преобразование  $\psi = \sqrt{\varphi\varphi^*}$  определено однозначно. Имеем:

$$(a\psi, b\psi) = (a, b\psi\psi^*) = (a, b\psi^2) = (a, b\varphi\varphi^*) = (a\varphi, b\varphi),$$

т. е.  $\varphi$  и  $\psi$  изометричны. □

**Определение 7.5.2.** Характеристические корни неотрицательного преобразования  $\psi = \sqrt{\varphi\varphi^*}$  называются *сингулярными числами* линейного преобразования  $\varphi$  евклидова (унитарного) пространства  $V$ . Характеристические корни неотрицательной матрицы  $\sqrt{AA^*}$  называются *сингулярными числами* матрицы  $A \in M_n(F)$  ( $F = \mathbb{R}$  или  $\mathbb{C}$ ).

**УПРАЖНЕНИЕ 7.5.2.** Пусть

$$A_\delta = \begin{pmatrix} 0 & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & 1 \\ \delta & 0 & \dots & 0 \end{pmatrix}_{10 \times 10}.$$

Сравните характеристические корни и сингулярные числа матриц  $A_\delta$  при  $\delta = 0$  и  $\delta = 10^{-10}$ .

**Теорема 7.5.2.** Если  $\varphi$  — нормальное преобразование евклидова (унитарного) пространства  $V$ , то сингулярные числа  $\varphi$  — это модули характеристических корней преобразования  $\varphi$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть сначала пространство  $V$  унитарно. По условию  $\varphi$  нормально, значит, существует ортонормированный базис,

в котором

$$[\varphi] = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}, \text{ а значит, } [\varphi^*] = [\varphi]^* = \begin{pmatrix} \overline{\lambda_1} & & \\ & \ddots & \\ & & \overline{\lambda_n} \end{pmatrix}.$$

Отсюда

$$[\varphi\varphi^*] = \begin{pmatrix} |\lambda_1|^2 & & \\ & \ddots & \\ & & |\lambda_n|^2 \end{pmatrix},$$

и следовательно,

$$[\psi] = [\sqrt{\varphi\varphi^*}] = \begin{pmatrix} |\lambda_1| & & 0 \\ & \ddots & \\ 0 & & |\lambda_n| \end{pmatrix}.$$

Случай евклидова пространства разбирается аналогично. Нужно лишь заметить, что

$$r \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \cdot r \begin{pmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{pmatrix} = \begin{pmatrix} r^2 & 0 \\ 0 & r^2 \end{pmatrix}.$$

**Теорема 7.5.3** (о полярном разложении). 1. Пусть  $\varphi$  — линейное преобразование конечномерного евклидова (унитарного) пространства  $V$ . Тогда существуют неотрицательное преобразование  $\psi$  и ортогональное (унитарное) преобразование  $\tau$  пространства  $V$ , такие, что  $\varphi = \psi\tau$ . Преобразование  $\psi = \sqrt{\varphi\varphi^*}$  определяется однозначно, и его характеристические корни — это сингулярные числа преобразования  $\varphi$ . Если преобразование  $\varphi$  невырождено, то  $\tau$  также определяется однозначно.

2. Если  $A$  — вещественная (комплексная) матрица, то существуют неотрицательная матрица  $B$  и ортогональная (унитарная) матрица  $C$ , такие, что  $A = BC$ . Матрица  $B$  определена однозначно и равна  $\sqrt{AA^*}$ . Если  $|A| \neq 0$ , то  $C$  также определена однозначно.

**ДОКАЗАТЕЛЬСТВО.** Докажем только п. 1, так как п. 2 вытекает из п. 1. в силу соответствия между линейными преобразованиями и матрицами.

Пусть  $e_1, \dots, e_r$  — ортонормированный базис пространства  $V\varphi$  — образа  $V$  относительно  $\varphi$ . Пусть векторы  $x_1, \dots, x_r \in V$  таковы, что

$x_i\varphi = e_i$  для  $i = 1, \dots, r$ . Рассмотрим набор векторов  $v_1, \dots, v_r$ , для которого  $v_i = x_i\psi$ ,  $i = 1, \dots, r$ , где  $\psi = \sqrt{\varphi\varphi^*}$ . Для всех  $i, j \in \{1, \dots, r\}$  выполняются равенства:

$$(v_i, v_j) = (x_i\psi, x_j\psi) = (x_i\varphi, x_j\varphi) = (e_i, e_j) = \begin{cases} 1, & i = j; \\ 0, & i \neq j, \end{cases}$$

иными словами,  $v_1, \dots, v_r$  — ортонормированный набор векторов. Дополним наборы  $e_1, \dots, e_r$  и  $v_1, \dots, v_r$  до ортонормированных базисов  $e_1, \dots, e_r, \dots, e_n$  и  $v_1, \dots, v_r, \dots, v_n$  пространства  $V$ . Существует линейное преобразование  $\tau$ , которое переводит базис  $v_1, \dots, v_n$  в базис  $e_1, \dots, e_n$  по правилу  $v_i\tau = e_i$  для всех  $i = 1, \dots, n$ . Преобразование  $\tau$  переводит ортонормированный базис в ортонормированный базис, следовательно,  $\tau$  ортогонально (унитарно) (следствие теоремы 7.3.1). Докажем, что  $\varphi = \psi\tau$ .

**Лемма.** Если  $\varphi$  и  $\psi$  изометричны, то  $\text{Ker } \varphi = \text{Ker } \psi$ .

**ДОКАЗАТЕЛЬСТВО ЛЕММЫ.** Если  $u \in \text{Ker } \varphi$ , то  $(u\psi, u\psi) = (u\varphi, u\varphi) = 0$ . Отсюда  $u\psi = 0$  и  $\text{Ker } \varphi \subseteq \text{Ker } \psi$ . В обратную сторону доказательство аналогично. Лемма доказана.

Пусть  $u \in V$  и  $u\varphi = \sum_{i=1}^r \alpha_i e_i$ . Так как  $x_i\varphi = e_i$ , то  $(u - \sum_{i=1}^r \alpha_i x_i)\varphi = 0$ .

В силу леммы выполняется равенство  $(u - \sum_{i=1}^r \alpha_i x_i)\psi = 0$ . Тогда  $u\psi =$

$\left(\sum_{i=1}^r \alpha_i x_i\right)\psi = \sum_{i=1}^r \alpha_i v_i$  и, следовательно,

$$u(\psi\tau) = \left(\sum_{i=1}^r \alpha_i v_i\right)\tau = \sum_{i=1}^r \alpha_i (v_i\tau) = \sum_{i=1}^r \alpha_i e_i = u\varphi,$$

откуда  $\varphi = \psi\tau$ . Так как это равенство выполнено для любого  $u \in V$ , то  $\varphi = \psi\tau$ .

Пусть  $\varphi = \psi_1\tau_1$  — ещё одно разложение, причём  $\psi_1$  — неотрицательное, а  $\tau_1$  — ортогональное (унитарное) преобразования. Тогда

$$\varphi\varphi^* = (\psi_1\tau_1)(\psi_1\tau_1)^* = \psi_1\tau_1\tau_1^*\psi_1^* = \psi_1^2.$$

По теореме 7.4.3 имеем  $\psi_1 = \psi$ .

Если  $\varphi$  невырождено, то невырождено и  $\psi$ , а значит,  $\tau = \psi^{-1}\varphi$  определено однозначно.  $\square$

**Определение 7.5.3.** Разложение, описанное в теореме 7.5.3, называется *полярным*.



**Теорема 7.5.4** (о сингулярном разложении). Пусть  $F$  — это поле вещественных (комплексных) чисел и  $A \in M_n(F)$ . Тогда существуют диагональная матрица  $D$  с неотрицательными вещественными числами на главной диагонали и ортогональные (унитарные) матрицы  $Q_1$  и  $Q_2$  из  $M_n(F)$ , для которых  $A = Q_1 D Q_2$ . В каждом таком разложении спектр матрицы  $D$  определён однозначно и состоит из сингулярных чисел матрицы  $A$ .

**ДОКАЗАТЕЛЬСТВО.** Из теоремы 7.5.3 следует, что  $A = BC$ , где  $B = \sqrt{AA^*}$  и  $C$  — ортогональная (унитарная) матрица. По п. 5 теоремы 7.4.1 для матрицы  $B$  существует ортогональная (унитарная) матрица  $Q$ , такая, что  $B = Q^* D Q$ , где  $D$  — диагональная вещественная матрица. Поскольку спектры  $B$  и  $D$  совпадают, спектр  $D$  состоит из сингулярных чисел матрицы  $A$ , в частности, все эти числа вещественные и неотрицательные. Подставляя равенство  $B = Q^* D Q$  в равенство  $A = BC$ , получаем

$$A = Q^* D Q C.$$

Произведение двух ортогональных (унитарных) матриц — снова ортогональная (унитарная) матрица. Поэтому  $Q_1 = Q^*$ ,  $Q_2 = QC$  и  $D$  — искомые матрицы.

Предположим, что  $A = Q_1 D Q_2$  — произвольное разложение матрицы  $A$ , в котором  $D$  диагональна и её спектр состоит из неотрицательных вещественных чисел, а  $Q_1$  и  $Q_2$  — ортогональные (унитарные) матрицы. Заметим, что для  $D$  выполняется  $\sqrt{D^* D} = \sqrt{D^2} = D$ , следовательно, сингулярные числа матрицы  $D$  равны её собственным числам. С другой стороны,

$$AA^* = (Q_1 D Q_2)(Q_1 D Q_2)^* = Q_1 D^2 Q_1^*,$$

поэтому собственные числа матриц  $AA^*$  и  $D^2$  совпадают. Значит, совпадают и собственные числа матриц  $\sqrt{AA^*}$  и  $D = \sqrt{DD^*}$ . Поэтому собственные числа матрицы  $D$  равны сингулярным числам матрицы  $A$ .  $\square$

**ЗАМЕЧАНИЕ.** Разложение из теоремы 7.5.4 называется *сингулярным разложением*. Фактически в теореме 7.5.4 мы дали новое определение сингулярных чисел как чисел, стоящих на главной диагонали в диагональной матрице, возникающей в сингулярном разложении.

**УПРАЖНЕНИЕ 7.5.3.** Для матрицы  $A = \begin{pmatrix} 2 & -1 \\ 2 & 1 \end{pmatrix}$  найти сингулярные числа, а также полярное и сингулярное разложения.

**УПРАЖНЕНИЕ 7.5.4.** Напомним, что объём  $n$ -мерного параллелепипеда в  $n$ -мерном евклидовом пространстве, натянутого на векторы  $a_1,$

$\dots, a_n$ , равен модулю определителя матрицы, составленной из строк координат векторов  $a_1, \dots, a_n$ . Найти условия на сингулярные числа оператора  $\varphi$  этого пространства, при выполнении которых  $\varphi$  “сохраняет” объёмы всех таких параллелепипедов.

# Глава 8

## Квадратичные формы

### § 8.1. Квадратичная форма и её матрица

**Определение 8.1.1.** *Квадратичной формой*  $f(x_1, \dots, x_n)$  от переменных  $x_1, \dots, x_n$  над полем  $F$  называется однородный многочлен степени два из  $F[x_1, \dots, x_n]$ , т. е. многочлен вида

$$f(x_1, \dots, x_n) = \sum_{1 \leq i \leq j \leq n} f_{ij} x_i x_j,$$

где  $f_{ij} \in F$ .

**ЗАМЕЧАНИЕ.** Напомним, что однородность многочлена означает, что все его одночлены имеют одну и ту же степень по совокупности переменных. В случае квадратичной формы это означает, что все её одночлены имеют степень два по совокупности переменных. Иногда в индукционных рассуждениях удобно считать квадратичной формой нулевой многочлен.

**ПРИМЕР.** Многочлен  $f(x_1, x_2) = x_1^2 + 3x_1x_2 + 2x_2^2$  из  $\mathbb{R}[x_1, x_2]$  является квадратичной формой, а многочлен  $x_1^2 + x_2^2 + 3$  — нет.

Заметим, что если при суммировании не предполагать, что  $i \leq j$ , то нарушается однозначность записи. Например, для  $f(x_1, x_2)$  из предыдущего примера имеем:

$$f(x_1, x_2) = x_1^2 + 2x_1x_2 + x_2x_1 + 2x_2^2 = x_1^2 + x_1x_2 + 2x_2x_1 + 2x_2^2.$$

С другой стороны, полезно избавиться от этого ограничения следующим способом.

**Определение 8.1.2.** Предположим, что поле  $F$  имеет характеристику, не равную двум, и  $f(x_1, \dots, x_n) = \sum_{1 \leq i \leq j \leq n} f_{ij} x_i x_j$  — квадратичная форма над  $F$ . Для любых  $i, j \in \{1, \dots, n\}$  положим

$$a_{ij} = \begin{cases} f_{ij}, & \text{если } i = j; \\ \frac{f_{ij}}{2}, & \text{если } i < j; \\ \frac{f_{ji}}{2}, & \text{если } i > j. \end{cases}$$

Тогда  $f(x_1, \dots, x_n) = \sum_{i,j=1}^n a_{ij}x_ix_j$  — стандартная запись квадратичной формы  $f$ . Матрица  $A = (a_{ij})_{n \times n}$  называется матрицей квадратичной формы  $f$ . Если  $x = (x_1, \dots, x_n)$ , то  $f(x) = xAx'$  — матричная форма записи квадратичной формы  $f(x)$ .

ПРИМЕР. Для  $f(x_1, x_2)$  из вышеприведённого примера имеем

$$A = \begin{pmatrix} 1 & \frac{3}{2} \\ \frac{3}{2} & 2 \end{pmatrix} \text{ и } f(x) = (x_1, x_2) \begin{pmatrix} 1 & \frac{3}{2} \\ \frac{3}{2} & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

В дальнейшем на протяжении этой главы мы рассматриваем поля, характеристика которых не равна двум.

**Предложение 8.1.1.** 1. Квадратичная форма  $f$  однозначно определяется своей матрицей  $A$ , т. е. если  $f(x) = xAx'$  и  $g(x) = xBx'$  — квадратичные формы, то  $f(x) = g(x)$  тогда и только тогда, когда  $A = B$ .

2. Матрица  $A$  квадратичной формы симметрическая, т. е.  $A = A'$ .

ДОКАЗАТЕЛЬСТВО. Вытекает из определения 8.1.2.  $\square$

**Определение 8.1.3.** Пусть  $x = (x_1, \dots, x_n)$ ,  $y = (y_1, \dots, y_n)$ ,  $f(x) = \sum_{i,j=1}^n a_{ij}x_ix_j = xAx'$  и  $g(y) = \sum_{i,j=1}^n b_{ij}y_iy_j = yBy'$  — квадратичные формы над полем  $F$  от переменных  $x_1, \dots, x_n$  и  $y_1, \dots, y_n$  соответственно. Говорят, что форма  $f$  эквивалентна форме  $g$ , если существует такая невырожденная матрица  $T = (t_{ij}) \in M_n(F)$ , что при линейной замене переменных  $x = yT$  (иными словами, при замене  $x_i = \sum_{j=1}^n t_{ji}y_j$  для любых  $i = 1, \dots, n$ ) форма  $f$  переходит в  $g$ . Матрица  $T$  называется матрицей замены. Обозначение:  $f \sim g$  (или  $f \sim_T g$ ).

ПРИМЕР. Пусть  $f(x_1, x_2) = x_1^2 + 3x_1x_2 + 2x_2^2$  и замена  $(x_1, x_2) = (y_1, y_2)T$  задана матрицей

$$T = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix},$$

т. е.  $x_1 = y_1 - y_2$ ,  $x_2 = y_1 + y_2$ . Тогда  $g(y) = (y_1 - y_2)^2 + 3(y_1 - y_2)(y_1 + y_2) + 2(y_1 + y_2)^2 = 6y_1^2 + 2y_1y_2$  — форма, эквивалентная форме  $f$ .

**Предложение 8.1.2.** 1.  $f \sim f$ ;

2. Если  $f \sim g$ , то  $g \sim f$ ;

3. Если  $f \sim g \sim h$ , то  $f \sim h$ .

ДОКАЗАТЕЛЬСТВО. 1. Очевидно.

2. Если  $T$  — матрица замены  $x = yT$ , то  $T^{-1}$  — матрица замены  $y = xT^{-1}$ .

3. Если  $T$  и  $S$  — матрицы замен  $x = yT$  и  $y = zS$  и  $f \underset{T}{\sim} g \underset{S}{\sim} h$ , то замена  $x = z(ST)$  осуществляет эквивалентность  $f \underset{ST}{\sim} h$ .  $\square$

**Предложение 8.1.3.** Если  $f(x) = xAx'$ ,  $g(y) = yBy'$  и  $f \underset{T}{\sim} g$ , то  $B = TAT'$ .

ДОКАЗАТЕЛЬСТВО. Так как  $f \underset{T}{\sim} g$ , то  $f(x) = xAx' \underset{T}{\sim} (yT)A(yT)' = y(TAT')y' = g(y)$ , следовательно, по предложению 8.1.1  $B = TAT'$ .  $\square$

**Определение 8.1.4.** Рангом квадратичной формы  $f$  называется ранг её матрицы.

**Следствие.** Ранги эквивалентных форм равны.

ДОКАЗАТЕЛЬСТВО. Утверждение следует из того, что если  $|T| \neq 0$ , то ранг  $A$  совпадает с рангом  $TAT'$ .  $\square$

## § 8.2. Диагонализация квадратичных форм

**Определение 8.2.1.** Квадратичная форма с матрицей  $A$  имеет диагональный вид, если  $A$  — диагональная матрица, т. е.  $f(x) = a_{11}x_1^2 + \dots + a_{nn}x_n^2$ .

**Теорема 8.2.1.** Каждая квадратичная форма  $f$  от  $n$  переменных над полем характеристики, отличной от двух, эквивалентна квадратичной форме диагонального вида.

ДОКАЗАТЕЛЬСТВО. Заметим, что если  $n = 1$ , то форма  $f = ax^2$  диагональна. Будем доказывать теорему индукцией по числу переменных  $n$ , т. е. будем полагать, что для всех квадратичных форм от  $s$  переменных, где  $s < n$ , теорема доказана.

Случай 1. Пусть существует  $i \in \{1, \dots, n\}$ , такое, что  $a_{ii} \neq 0$ . Поскольку замена  $y_1 = x_i$ ,  $y_i = x_1$ ,  $y_j = x_j$  для всех  $j \notin \{1, i\}$  невырожденная, то можно считать, что  $a_{11} \neq 0$ . Сгруппировав одночлены, в которые входит  $x_1$ , получим

$$f(x) = a_{11}x_1^2 + 2a_{12}x_1x_2 + \dots + 2a_{1n}x_1x_n + f_1(x_2, \dots, x_n),$$

где  $f_1(x_2, \dots, x_n)$  — квадратичная форма от  $n - 1$  переменных. С другой стороны, квадратичная форма

$$\begin{aligned} h(x) &= a_{11} \left( x_1 + \frac{a_{12}}{a_{11}}x_2 + \dots + \frac{a_{1n}}{a_{11}}x_n \right)^2 = \\ &= a_{11}x_1^2 + 2a_{12}x_1x_2 + \dots + 2a_{1n}x_1x_n + h_1(x_2, \dots, x_n) \end{aligned}$$

имеет те же одночлены, включающие переменную  $x_1$ . Поэтому

$$g = f - h = f_1 - h_1$$

является квадратичной формой от переменных  $x_2, \dots, x_n$ . По предположению индукции существует  $T_1 \in M_{n-1}(F)$ , такая, что  $|T_1| \neq 0$ , и замена  $(x_2, \dots, x_n) = (y_2, \dots, y_n)T_1$  приводит форму  $g$  к диагональному виду  $b_2y_2^2 + \dots + b_ny_n^2$ . Пусть

$$y_1 = x_1 + \frac{a_{12}}{a_{11}}x_2 + \dots + \frac{a_{1n}}{a_{11}}x_n.$$

Подставляя в это равенство выражения переменных  $x_2, \dots, x_n$  через  $y_2, \dots, y_n$ , найдём  $t_{21}, \dots, t_{n1} \in F$ , для которых

$$x_1 = y_1 + t_{21}y_2 + \dots + t_{n1}y_n.$$

Тогда матрица

$$T = \left( \begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline t_{21} & & & \\ \vdots & & & \\ t_{n1} & & & T_1 \end{array} \right)$$

осуществляет замену, при которой форма  $f = h + g$  переходит в форму  $a_{11}y_1^2 + b_2y_2^2 + \dots + b_ny_n^2$ . Матрица  $T$  невырождена, так как  $|T| = |T_1| \neq 0$ .

Случай 2. Пусть для любого  $i = 1, \dots, n$  имеет место  $a_{ii} = 0$ . Если  $a_{ij} = 0$  для  $i, j \in \{1, \dots, n\}$ , то форма имеет вид  $f(x) = 0$  и её матрица диагональна. Значит, можно считать, что  $a_{12} \neq 0$ . Рассмотрим следующую замену переменных:

$$x_1 = y_1 - y_2, \quad x_2 = y_1 + y_2, \quad x_3 = y_3, \quad \dots, \quad x_n = y_n.$$

Тогда

$$f(x) = 2a_{12}x_1x_2 + f_2(x) = 2a_{12}(y_1 - y_2)(y_1 + y_2) + g_2(y),$$

причём в записи  $g_2(y)$  коэффициенты при  $y_1^2$  и  $y_2^2$  равны нулю, следовательно, указанная замена переводит форму  $f(x)$  в форму  $g(y) = 2a_{12}y_1^2 + \dots$ , у которой коэффициент при  $y_1^2$  не равен нулю. Мы пришли к случаю 1. Матрица замены

$$T = \begin{pmatrix} 1 & 1 & & & & \\ -1 & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}$$

невырождена, так как  $\begin{vmatrix} 1 & 1 \\ -1 & 1 \end{vmatrix} = 2 \neq 0$  в поле характеристики, не равной двум.  $\square$

ПРИМЕР.

$$\begin{aligned} f(x_1, x_2) &= x_1^2 + 3x_1x_2 + 2x_2^2 = \left(x_1 + \frac{3}{2}x_2\right)^2 - \frac{9}{4}x_2^2 + 2x_2^2 = \\ &= \left(x_1 + \frac{3}{2}x_2\right)^2 - \frac{1}{4}x_2^2, \end{aligned}$$

следовательно,

$$y_1 = x_1 + \frac{3}{2}x_2, \quad y_2 = x_2.$$

Замена  $x_1 = y_1 - \frac{3}{2}y_2$ ,  $x_2 = y_2$  с матрицей  $T = \begin{pmatrix} 1 & 0 \\ -\frac{3}{2} & 1 \end{pmatrix}$  приводит форму  $f$  к виду  $y_1^2 - \frac{1}{4}y_2^2$ .

ЗАМЕЧАНИЕ. Метод диагонализации, использованный в теореме 8.2.1, называется *алгоритмом Лагранжа*.

Теперь мы обратимся к случаю, когда поле  $F = \mathbb{R}$ . В этом случае говорят, что  $f$  — *вещественная* квадратичная форма.

**Теорема 8.2.2** (нормальный вид вещественной квадратичной формы). *Каждая вещественная квадратичная форма  $f(x)$  от  $n$  переменных невырожденной заменой переменных приводится к виду*

$$z_1^2 + \dots + z_s^2 - z_{s+1}^2 - \dots - z_r^2 + 0 \cdot z_{r+1}^2 + \dots + 0 \cdot z_n^2.$$





эквивалентную форму  $f$ . Предположим, что  $k \neq s$  (для определённости считаем  $k < s$ ). Так как  $h \sim f \sim g$ , то  $h \sim g$ , следовательно, существует такая невырожденная матрица  $T$ , что замена  $z = yT$  переводит  $h$  в  $g$ , т. е.

$$z_i = \sum_{j=1}^r t_{ji} y_j.$$

Рассмотрим систему однородных линейных уравнений относительно переменных  $y_1, \dots, y_r$ :

$$\left\{ \begin{array}{l} y_1 = 0 \\ \vdots \\ y_k = 0 \\ t_{1,s+1}y_1 + \dots + t_{r,s+1}y_r = 0, \quad \text{эквивалентно уравнению } z_{s+1} = 0 \\ \vdots \\ t_{1,r}y_1 + \dots + t_{r,r}y_r = 0, \quad \text{эквивалентно уравнению } z_r = 0 \end{array} \right. \quad (1)$$

Так как  $k < s$ , то число уравнений в этой системе меньше числа неизвестных, следовательно, существует ненулевое решение  $y^0 = (0, \dots, 0, a_{k+1}, \dots, a_r)$  этой системы. Положим  $z^0 = (b_1, \dots, b_r) = y^0 T$ . Поскольку  $|T| \neq 0$ , то  $z^0$  — ненулевая строка. Однако из системы (1) следует, что  $b_{s+1} = \dots = b_r = 0$ .

Так как замена  $z = yT$  переводит  $h$  в  $g$ , то  $h(z^0) = g(y^0)$ . Но

$$h(z^0) = b_1^2 + \dots + b_s^2 > 0,$$

так как хотя бы один  $b_i \neq 0$ , а

$$g(y^0) = -a_{k+1}^2 - \dots - a_r^2 < 0.$$

Противоречие. Значит,  $s = k$ . □

**ПРИМЕР.**

$$f(x) = x_1^2 + 3x_1x_2 + 2x_2^2 \sim y_1^2 - \frac{1}{4}y_2^2 \sim z_1^2 - z_2^2,$$

следовательно,  $s = 1$ ,  $r - s = 1$  для  $f(x)$ .

**Теорема 8.2.4.** Пусть  $f(x)$  — вещественная квадратичная форма с матрицей  $A$ . Существует ортогональная матрица  $Q$ , такая, что замена  $x = yQ$  приводит  $f$  к диагональному виду

$$g(y) = \lambda_1 y_1^2 + \dots + \lambda_n y_n^2,$$

где  $\lambda_i$  — характеристические корни матрицы  $A$ .

**ЗАМЕЧАНИЕ.** Характеристические корни матрицы  $A$  вещественны, так как  $A$  симметрическая.

**ДОКАЗАТЕЛЬСТВО.** В силу теоремы 7.4.1 для симметрической матрицы  $A$  найдётся ортогональная матрица  $Q$ , такая, что  $QAQ^{-1} = D(\lambda_1, \dots, \lambda_n)$ , где  $\lambda_1, \dots, \lambda_n$  — характеристические корни матрицы  $A$ . Поскольку для ортогональной матрицы  $Q$  выполняется  $Q^{-1} = Q'$ , то при замене переменных  $x = yQ$  форма  $f$  перейдёт в форму с матрицей  $D = QAQ'$ .  $\square$

**Следствие.** Число положительных характеристических корней матрицы  $A$  формы  $f$  равно положительному индексу инерции, число отрицательных — отрицательному индексу, а ранг  $f$  равен числу ненулевых характеристических корней матрицы  $A$  с учётом их кратности.

### Определение 8.2.3. Форма

$$g(y) = \lambda_1 y_1^2 + \dots + \lambda_n y_n^2,$$

где  $\lambda_i$  — характеристические корни матрицы формы  $f(x)$  называется *каноническим видом* формы  $f$ . Процесс приведения формы к каноническому виду с помощью ортогональной замены переменных называется *приведением формы к главным осям*.

Геометрическая интерпретация. 1. Если  $h(x) = 0$  — уравнение эллипса, то в возникающей квадратичной форме  $f(x)$  выполняется  $r = s = 2$ .

2. Если  $h(x) = 0$  — уравнение гиперболы, то  $s = 1, r = 2$ .

3. Если  $h(x) = 0$  — уравнение параболы, то  $r = 1$ .

Заметим, что ортогональная замена переменных — это замена, сохраняющая расстояния.

## § 8.3. Положительно определённые квадратичные формы

**Определение 8.3.1.** Вещественная квадратичная форма  $f(x_1, \dots, x_n)$  называется *положительно определённой* (краткое обозначение:  $f(x) > 0$ ), если для любого ненулевого набора  $(a_1, \dots, a_n) \in \mathbb{R}^n$  выполняется  $f(a_1, \dots, a_n) > 0$ .

**ПРИМЕРЫ.** 1. Форма  $f(x_1, \dots, x_n) = x_1^2 + \dots + x_n^2$  положительно определена.

2. Формы  $f(x_1, x_2) = x_1^2 + 0 \cdot x_2^2$  и  $f(x_1, x_2) = x_1^2 + 3x_1x_2 + x_2^2$  не являются положительно определёнными.

**Определение 8.3.2.** Пусть  $A = (a_{ij})_{n \times n} \in M_n(F)$  и  $k \in \{1, \dots, n\}$ . Угловым  $k$ -ым минором матрицы  $A$  называется минор

$$A_k = \begin{pmatrix} a_{11} & \dots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{k1} & \dots & a_{kk} \end{pmatrix}.$$

Определитель минора  $A_k$  обозначается как  $\mathcal{D}_k(A)$ .

**Теорема 8.3.1.** Пусть  $f(x) = xAx'$  — вещественная квадратичная форма от  $n$  переменных с матрицей коэффициентов  $A$ . Следующие утверждения эквивалентны:

- 1)  $f(x) \sim y_1^2 + \dots + y_n^2$ ;
- 2)  $f(x) > 0$  (положительно определена);
- 3) для любого  $k = 1, \dots, n$  выполняется  $\mathcal{D}_k(A) > 0$ .

ДОКАЗАТЕЛЬСТВО. (1  $\Rightarrow$  2) Вытекает из следующей леммы.

**Лемма.** Если  $f \underset{T}{\sim} g$ , то  $f > 0$  тогда и только тогда, когда  $g > 0$ .

Пусть  $x = yT$  — замена, переводящая  $f$  в  $g$ , и  $(b_1, \dots, b_n) \neq (0, \dots, 0)$ . Тогда

$$(a_1, \dots, a_n) = (b_1, \dots, b_n)T \neq \bar{0},$$

так как  $|T| \neq 0$  и

$$g(b_1, \dots, b_n) = f(a_1, \dots, a_n) > 0,$$

а это значит, что  $g > 0$ . В обратную сторону аналогично. Лемма доказана.

(2  $\Rightarrow$  1) Приведём положительно определённую форму к нормальному виду:

$$f \sim g(y) = y_1^2 + \dots + y_s^2 - y_{s+1}^2 - \dots - y_r^2 + 0 \cdot y_{r+1}^2 + \dots + 0 \cdot y_n^2.$$

Если  $s < n$ , то  $g(\underbrace{0, \dots, 0}_s, 1, 0, \dots, 0) \leq 0$ , т. е.  $g$  не является положительно определённой, что противоречит лемме.

(1  $\Rightarrow$  3) Если  $f(x) = xAx' \underset{T}{\sim} g(y) = yBy'$  и  $B = TAT'$ , то  $|B| = |TAT'| = |T|^2 \cdot |A|$ , откуда  $\operatorname{sgn} |A| = \operatorname{sgn} |B|$ , т. е.  $\operatorname{sgn} |A|$  не меняется при невырожденной замене переменных. Так как  $f(x) \sim g(y) = y_1^2 + \dots + y_n^2$ , то  $\operatorname{sgn} |A| = \operatorname{sgn} |B| > 0$ , т. е.  $\mathcal{D}_n(A) > 0$ . Пусть существует  $k$ ,  $1 \leq k < n$ ,

такое, что  $\mathcal{D}_k(A) \leq 0$ . Рассмотрим форму от  $k$  переменных

$$f_1(x_1, \dots, x_k) = f(x_1, \dots, x_k, 0, \dots, 0) = (x_1, \dots, x_k)A_k \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}.$$

Форма  $f_1(x_1, \dots, x_k)$  не является положительно определённой, так как  $|A_k| = \mathcal{D}_k(A_k) = \mathcal{D}_k(A) \leq 0$ . Значит, существуют такие  $a_1, \dots, a_k \in \mathbb{R}$ , для которых  $f_1(a_1, \dots, a_k) \leq 0$ . Но тогда  $f(a_1, \dots, a_k, 0, \dots, 0) = f_1(a_1, \dots, a_k) \leq 0$ , т.е.  $f$  не является положительно определённой. Полученное противоречие показывает, что  $\mathcal{D}_k(A) > 0$  для всех  $k = 1, \dots, n$ .

(3  $\Rightarrow$  1) Пусть все  $\mathcal{D}_k(A) > 0$ . Докажем, что  $f > 0$ , индукцией по числу переменных (для  $n = 1$  утверждение очевидно). Пусть

$$f(x) = \sum_{i,j=1}^n a_{ij}x_i x_j = \sum_{i,j=1}^{n-1} a_{ij}x_i x_j + 2a_{1,n}x_1 x_n + \dots + 2a_{n-1,n}x_{n-1} x_n + a_{nn}x_n^2.$$

Рассмотрим форму от  $n - 1$  переменной

$$f_1(x_1, \dots, x_{n-1}) = f(x_1, \dots, x_{n-1}, 0) = (x_1, \dots, x_{n-1})A_{n-1} \begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \end{pmatrix}.$$

Так как для любого  $k = 1, \dots, n - 1$  имеет место  $\mathcal{D}_k(A_{n-1}) = \mathcal{D}_k(A) > 0$ , то существует  $T_1 \in M_{n-1}(\mathbb{R})$ , такая, что  $|T_1| \neq 0$  и

$$f_1(x_1, \dots, x_{n-1}) \underset{T_1}{\sim} g_1(y_1, \dots, y_{n-1}) = y_1^2 + \dots + y_{n-1}^2.$$

Пусть

$$T = \left( \begin{array}{ccc|c} & & & 0 \\ & & & \vdots \\ & T_1 & & 0 \\ \hline 0 & \dots & 0 & 1 \end{array} \right)$$

и  $x = yT$ . Тогда

$$f(x) \underset{T}{\sim} g(y) = \sum_{i=1}^{n-1} y_i^2 + \sum_{i=1}^{n-1} 2b_{i,n}y_i y_n + b_{nn}y_n^2.$$

Рассмотрим замену  $y = zR$ , где

$$R = \left( \begin{array}{ccc|c} & & & 0 \\ & E & & \vdots \\ & & & 0 \\ \hline -b_{1n} & \dots & -b_{n-1,n} & 1 \end{array} \right).$$

Тогда

$$\begin{aligned} g(y) \underset{R}{\sim} h(z) &= \sum_{i=1}^{n-1} (z_i - b_{i,n}z_n)^2 + \sum_{i=1}^{n-1} 2b_{i,n}(z_i - b_{i,n}z_n)z_n + b_{n,n}z_n^2 = \\ &= \sum_{i=1}^{n-1} z_i^2 + cz_n^2, \end{aligned}$$

где  $c \in \mathbb{R}$ . Так как  $\operatorname{sgn} \mathcal{D}_n(A) = \operatorname{sgn}(\det A)$  не меняется при невырожден-

ной замене, то  $\left| \begin{array}{ccc|c} & E & & 0 \\ & & & \vdots \\ & & & 0 \\ \hline 0 & \dots & 0 & c \end{array} \right| > 0$ , откуда  $c > 0$ . Замена

$$z_1 = u_1, \quad \dots \quad z_{n-1} = u_{n-1}, \quad z_n = \frac{u_n}{\sqrt{c}}$$

приводит  $h(z)$  к виду  $u_1^2 + \dots + u_n^2$ . Следовательно,  $f(x) \sim u_1^2 + \dots + u_n^2$ .  $\square$

**Следствие.** 1. Квадратичная форма над  $\mathbb{R}$  с матрицей  $A$  положительно определена тогда и только тогда, когда  $A$  — положительная симметрическая матрица.

2. Симметрическая матрица  $A \in M_n(\mathbb{R})$  положительна тогда и только тогда, когда  $\mathcal{D}_k(A) > 0$  для всех  $k = 1, \dots, n$ .

УПРАЖНЕНИЕ 8.3.1. Доказать следствие.

**Теорема 8.3.2.** Пусть  $f(x)$ ,  $g(x)$  — квадратичные формы над  $\mathbb{R}$  и  $f(x) > 0$ . Тогда существует  $T \in M_n(\mathbb{R})$ , такая, что  $|T| \neq 0$  и  $f \underset{T}{\sim} z_1^2 + \dots + z_n^2$ ,  $g \underset{T}{\sim} \lambda_1 z_1^2 + \dots + \lambda_n z_n^2$ , т. е. одной и той же невырожденной заменой переменных  $x = zT$  форма  $f$  приводится к нормальному виду, а форма  $g$  — к диагональному виду.

**Доказательство.** Форма  $f$  положительно определена, следовательно, существует  $R \in M_n(\mathbb{R})$ , такая, что  $x = yR$  приводит  $f$  к виду

$f_1(y) = y_1^2 + \dots + y_n^2$ . В частности,  $f_1(y) = yEy'$ . Эта же замена приводит  $g$  к некоторой форме  $g_1(y_1, \dots, y_n) = yBy'$ . Рассмотрим ортогональную замену  $y = zQ$ , приводящую форму  $g_1$  к каноническому виду:

$$g_1(y_1, \dots, y_n) \underset{Q}{\sim} g_2(z_1, \dots, z_n) = \lambda_1 z_1^2 + \dots + \lambda_n z_n^2,$$

где  $\lambda_i$  — характеристические корни матрицы  $B$ . Имеем  $g(x) \underset{T}{\sim} g_2(z)$ , где  $T = QR$  — невырожденная матрица замены. Кроме того,  $f_1(y) \underset{Q}{\sim} f_2(z) = zCz'$ . Так как

$$C = QEQ' = QEQ^{-1} = E,$$

то  $f_2(z) = z_1^2 + \dots + z_n^2$ , т.е. замена  $x = zT$  приводит форму  $f$  к нормальному виду:  $f(x) \underset{T}{\sim} f_2(z) = z_1^2 + \dots + z_n^2$ .  $\square$

Если формы  $f(x)$  и  $g(x)$  выбраны произвольно, то ответ на вопрос, можно ли привести их одновременно к диагональному виду, вообще говоря, отрицательный, как показывают следующие упражнения.

**УПРАЖНЕНИЕ 8.3.2.** Пусть вещественные квадратичные формы  $f(x) = xAx'$  и  $g(x) = xBx'$  таковы, что замена  $x = yT$  приводит их одновременно к диагональному виду. Доказать, что все корни многочлена  $h(\lambda) = |A - \lambda B|$  вещественны.

*Указание.* Пусть  $\alpha$  — корень  $h(\lambda)$ . Тогда  $0 = |A - \alpha B| = |T|^2 |A - \alpha B| = |T(A - \alpha B)T'| = \dots$

**ЗАМЕЧАНИЕ.** Утверждение, обратное к утверждению упражнения **8.3.2**, неверно.

**УПРАЖНЕНИЕ 8.3.3.** Используя упражнение **8.3.2**, доказать, что формы  $f(x) = 2x_1x_2$  и  $g(x) = x_1^2 - x_2^2$  нельзя привести к диагональному виду одной и той же заменой переменных.

# Глава 9

## Начала теории групп

### § 9.1. Группы и их подгруппы

В этой главе мы познакомимся с некоторыми базовыми понятиями и фактами теории групп. В первом параграфе мы для удобства напомним уже известные начальные определения и иллюстрируем их примерами, знакомыми читателю из других разделов курса.

**Определение 9.1.1.** Алгебраическая система  $\mathfrak{G} = \langle G, \cdot \rangle$  с одной бинарной операцией называется *группой*, если справедливы следующие условия (*аксиомы группы*):

1. Для любых элементов  $a, b, c \in G$  выполняется  $(ab)c = a(bc)$  (аксиома ассоциативности).
2. Существует элемент  $e \in G$ , такой, что для любого элемента  $a \in G$  выполняется  $ae = ea = a$  (аксиома нейтрального элемента).
3. Для любого  $a \in G$  существует элемент  $a^{-1} \in G$ , такой, что выполняется  $aa^{-1} = a^{-1}a = e$  (аксиома обратного элемента).

**Определение 9.1.2.** Непустое подмножество  $H$  группы  $G$  — *подгруппа* группы  $G$  (обозначение:  $H \leq G$ ) тогда и только тогда, когда  $H$  — группа относительно сужения на  $H$  групповой операции на  $G$ , что, в свою очередь, выполняется в точности тогда, когда  $h_1 h_2 \in H$  для любых  $h_1, h_2 \in H$  и  $h^{-1} \in H$  для любого  $h \in H$ .

**Определение 9.1.3.** *Порядком* группы (подгруппы)  $G$  называется количество элементов в  $G$ . *Порядком* элемента  $g$  группы называется наименьшее  $n \in \mathbb{N}$ , для которого  $g^n = e$ , если такое  $n$  существует; иначе говорят, что  $g$  имеет бесконечный порядок. Обозначения:  $|G|$  и  $|g|$  соответственно.

**Определение 9.1.4.** Две группы *изоморфны* (обозначение:  $\langle G, \cdot \rangle \simeq \langle H, * \rangle$ ) тогда и только тогда, когда существует биекция  $\varphi : G \rightarrow H$ , такая, что для любых  $g_1, g_2 \in G$  выполняется  $(g_1 \cdot g_2)\varphi = (g_1\varphi)*(g_2\varphi)$ . Эта биекция при этом называется *изоморфизмом* группы  $G$  на группу  $H$ . Изоморфизм группы  $G$  на саму себя называется *автоморфизмом*.

**ПРИМЕРЫ.** 1. а) Относительно операции сложения  $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ .

б) Относительно операции умножения  $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$ .

УПРАЖНЕНИЕ 9.1.1. 1. а) Доказать, что  $2\mathbb{Z} \leq \mathbb{Z}$  и  $2\mathbb{Z} \simeq \mathbb{Z}$ .

б) Доказать, что  $C_n = \{\xi \in \mathbb{C} \mid \xi^n = 1\} \leq \langle \mathbb{C}, \cdot \rangle$  и  $\langle C_n, \cdot \rangle \simeq \langle \mathbb{Z}_n, + \rangle$ .

ПРИМЕРЫ. 2. Знакопеременная группа подстановок — подгруппа симметрической группы:  $A_n \leq S_n$ ; кроме того,  $|S_n| = 2|A_n| = n!$ .

3. Множество всех невырожденных матриц

$$GL_n(F) = \{A \in M_n(F) \mid \det(A) \neq 0\}$$

над полем  $F$  образует группу относительно умножения.

Подмножества

$$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1\},$$

$$GO_n(F) = \{A \in M_n(F) \mid A^{-1} = A'\},$$

$$GU_n(F) = \{A \in M_n(F) \mid A^{-1} = \overline{A'}\},$$

$$Z(GL_n(F)) = \{A \in GL_n(F) \mid A = \alpha E\}$$

являются подгруппами группы  $GL_n(F)$ , где в третьем примере  $F = \mathbb{C}$ .

4. Следующие множества преобразований аффинной евклидовой плоскости  $E^2$  (пространства  $E^3$ ) являются группами:

$\text{Isom}_2$  ( $\text{Isom}_3$ ) — группа движений плоскости (пространства);

$\text{Tran}_2$  ( $\text{Tran}_3$ ) — группа параллельных переносов;

$O_2$  и  $O_3$  — группы движений с неподвижной точкой (началом координат).

УПРАЖНЕНИЕ 9.1.2. Пусть  $F$  — фигура на плоскости.

1. Доказать, что множество  $S_F = \{\varphi \in \text{Isom}_2 \mid F\varphi = F\}$  — подгруппа группы  $\text{Isom}_2$ . Она называется группой симметрий фигуры  $F$ .

2. Доказать, что  $S_F$ , где  $F$  — правильный треугольник, изоморфна  $S_3$ .

3. Найти  $|S_F|$ , где  $F$  — правильный  $n$ -угольник.

УПРАЖНЕНИЕ 9.1.3. Пусть  $G$  — группа,  $g \in G$  и  $|g| = n$ . Доказать следующие утверждения:

1)  $g^m = e \iff n \mid m$ ;

2)  $g^k = g^l \iff k \equiv l \pmod{n}$ .

УПРАЖНЕНИЕ 9.1.4. Множество всех автоморфизмов группы  $G$  образует группу относительно операции композиции биекций. Обозначение:  $\text{Aut}(G)$ .



### § 9.2. Порождающее множество и циклическая подгруппа

**Определение 9.2.1.** Пусть  $G$  — группа и  $A, B \subseteq G$ . Введём обозначения:  $AB = \{ab \mid a \in A, b \in B\}$ ,  $A^{-1} = \{a^{-1} \mid a \in A\}$ ,  $A^n = \{a_1 \cdots a_n \mid a_i \in A\}$ .

УПРАЖНЕНИЕ 9.2.1. Пусть  $A, B, C, D \subseteq G$ . Доказать, что:

- 1)  $(AB)C = A(BC)$ ;
- 2) если  $A \subseteq C$  и  $B \subseteq D$ , то  $AB \subseteq CD$  и  $A^{-1} \subseteq C^{-1}$ .

**Предложение 9.2.1.** *Непустое подмножество  $H$  является подгруппой группы  $G$  тогда и только тогда, когда  $HH^{-1} \subseteq H$ .*

ДОКАЗАТЕЛЬСТВО. По определению

$$HH^{-1} = \{h_1 \cdot h_2^{-1} \mid h_1, h_2 \in H\}.$$

Мы знаем, что  $H \leq G$  тогда и только тогда, когда 1)  $h_1 \cdot h_2 \in H$  для любых  $h_1, h_2 \in H$ ; 2)  $h^{-1} \in H$  для любого  $h \in H$ .

( $\Rightarrow$ ) Если  $h_1, h_2 \in H$ , то  $h_2^{-1} \in H$  в силу 2) и  $h_1 \cdot h_2^{-1} \in H$  в силу 1).

( $\Leftarrow$ ) Пусть  $h \in H$  (по крайней мере один такой элемент в  $H$  найдётся). Тогда  $h \cdot h^{-1} \in H$ , следовательно,  $e \in H$ , а значит,  $e \cdot h^{-1} \in H$  и  $h^{-1} \in H$ . Если  $h_1, h_2 \in H$ , то  $h_2^{-1} \in H$ , и  $h_1 \cdot h_2 = h_1 \cdot (h_2^{-1})^{-1} \in H$ .  $\square$

**Предложение 9.2.2.** Пусть  $I$  — множество индексов,  $\{H_i \mid i \in I\}$  — множество подгрупп группы  $G$ , занумерованных элементами из  $I$ . Тогда  $K = \bigcap_{i \in I} H_i$  является подгруппой группы  $G$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $k_1, k_2 \in K$ . Тогда  $k_1, k_2 \in H_i$  для любого  $i \in I$ . Значит,  $k_1 \cdot k_2^{-1} \in H_i$  для любого  $i \in I$ , т. е.  $k_1 \cdot k_2^{-1} \in \bigcap_{i \in I} H_i = K$ , откуда  $K \leq G$ .  $\square$

**Определение 9.2.2.** Пусть  $G$  — группа,  $A \subseteq G$ . Подгруппой, порождённой множеством  $A$ , называется пересечение всех подгрупп группы  $G$ , содержащих  $A$ . Обозначение:  $\langle A \rangle = \bigcap_{\substack{H \leq G \\ H \supseteq A}} H$ .

**Теорема 9.2.1.** Пусть  $G$  — группа,  $A \subseteq G$ ,  $K = \langle A \rangle$  и

$$R = \{a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} \mid a_i \in A, \varepsilon_i = \pm 1, n \in \mathbb{N}\}.$$

Тогда  $K = R$ .

ДОКАЗАТЕЛЬСТВО. Положим  $B = A \cup A^{-1}$ . Тогда  $B^{-1} = B$  и  $R = \bigcup_{n \in \mathbb{N}} B^n$ .

Пусть  $g_1, g_2 \in R$ . Тогда  $g_1 = b_1 \dots b_s$ ,  $g_2 = c_1 \dots c_t$ , где  $s, t \in \mathbb{N}$  и  $b_i, c_j \in B$ . Следовательно,  $g_1^{-1} \in R$  и  $g_1 g_2 \in R$ , откуда  $R \leq G$ . Кроме того, очевидно, что  $A \subseteq R$ , т. е.  $K \leq R$ .

Пусть  $H$  — произвольная подгруппа группы  $G$ , такая, что  $A \subseteq H$ . Так как  $H \leq G$ , то  $A^{-1} \subseteq H$ , а значит,  $B \subseteq H$  и  $B \subseteq K$ . Далее,  $B^2 = B \cdot B \subseteq H$ , т. е.  $B^2 \subseteq K$ . Используя индукцию по  $n$ , получаем, что для любого  $n$  выполняется  $B^n \subseteq H$ . Таким образом,  $B^n \subseteq K$  и  $R = \bigcup_{n \in \mathbb{N}} B^n \subseteq K$ .  $\square$

**Определение 9.2.3.** Если  $G = \langle A \rangle$ , то  $A$  — порождающее множество группы  $G$ .

ПРИМЕРЫ. 1.  $\mathbb{Z} = \langle \{1\} \rangle = \langle \{2, 3\} \rangle$ , но  $\langle \{2\} \rangle = 2\mathbb{Z} \neq \mathbb{Z}$ .

2.  $S_n = \langle \{(ij) \mid i, j \in \{1, \dots, n\}\} \rangle$ .

3.  $GL_n(F)$  порождается множеством всех элементарных и невырожденных диагональных матриц.

УПРАЖНЕНИЕ 9.2.2. Доказать, что  $\text{Isom}_2$  порождается осевыми симметриями.

Указание. 1. Доказать, что движение можно представить в виде композиции параллельного переноса, поворота и осевой симметрии.

2. Доказать, что параллельный перенос и поворот представляют собой композицию двух осевых симметрий.

**Определение 9.2.4.** Группа (подгруппа) называется *циклической*, если она порождается одноэлементным множеством. Обозначение:  $G = \langle g \rangle$ , где  $g \in G$ .

ПРИМЕРЫ. 1.  $\mathbb{Z} = \langle 1 \rangle$ ,  $\mathbb{Z}_n = \langle \bar{1} \rangle$ .

2.  $S_2 = \langle (12) \rangle$ ,  $A_3 = \langle (123) \rangle$ , но  $S_3$ ,  $A_4$  не циклические.

**Теорема 9.2.2.** Каждая циклическая группа изоморфна либо  $\langle \mathbb{Z}, + \rangle$ , либо  $\langle \mathbb{Z}_n, + \rangle$  для некоторого  $n \in \mathbb{N}$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $G = \langle a \rangle$ . В силу теоремы 9.2.1  $G = \{e = a^0, a^{\pm 1}, a^{\pm 2}, \dots\} = \{a^k \mid k \in \mathbb{Z}\}$  и  $a^k \cdot a^l = a^{k+l}$  для  $k, l \in \mathbb{Z}$ . Предположим сначала, что  $a^k \neq a^l$  при  $k \neq l$  для любых  $k, l \in \mathbb{Z}$ . Тогда отображение  $\varphi : G \rightarrow \mathbb{Z}$ , действующее по правилу  $(a^k)\varphi = k$ , — это биекция. Кроме того,  $(a^k \cdot a^l)\varphi = (a^{k+l})\varphi = k + l = (a^k)\varphi + (a^l)\varphi$ , т. е.  $\varphi$  сохраняет операцию, а значит, является изоморфизмом.

Пусть существуют  $k, l, k \neq l$ , такие, что  $a^k = a^l$ . Будем считать, что  $k > l$ . Тогда  $k - l \in \mathbb{N}$  и  $a^{k-l} = a^k \cdot a^{-l} = a^0 = e$ . Значит, элемент  $a$  имеет конечный порядок, который мы обозначим через  $n$ . В силу п. 2 упражнения 9.1.3 равенство  $a^k = a^l$  имеет место тогда и только тогда, когда  $k \equiv l \pmod{n}$ . Таким образом,  $G = \{a^k \mid k = 0, 1, \dots, n-1\}$  и отображение  $\varphi : G \rightarrow \mathbb{Z}$ , действующее по правилу  $(a^k)\varphi = \bar{k}$ , является биекцией. Кроме того,  $(a^k \cdot a^l)\varphi = (a^{k+l})\varphi = \overline{k+l} = \bar{k} + \bar{l} = (a^k)\varphi + (a^l)\varphi$ .  $\square$

**УПРАЖНЕНИЕ 9.2.3.** Порядок элемента равен порядку порождённой им циклической подгруппы.

**УПРАЖНЕНИЕ 9.2.4.** Подгруппа циклической группы — снова циклическая группа.

**УПРАЖНЕНИЕ 9.2.5.** Доказать, что в группе симметрий  $S_\Delta$  правильного треугольника все собственные подгруппы циклические, а сама  $S_\Delta$  — нет.

### § 9.3. Смежные классы по подгруппе

**Определение 9.3.1.** Пусть  $G$  — группа,  $H \leq G$  и  $x \in G$ . Множество

$$Hx = \{hx \mid h \in H\} = H\{x\}$$

называется *правым смежным классом группы  $G$  по подгруппе  $H$  с представителем  $x$* . Аналогично  $xH$  — *левый смежный класс*.

**ПРИМЕРЫ.** 1.  $G = S_3$ ,  $H = \{\varepsilon, (12)\}$ ,  $x = (123)$ . Тогда  $Hx = \{(123), (13)\}$ , а  $xH = \{(123), (23)\}$ .

2.  $G = \mathbb{Z}$ ,  $H = 2\mathbb{Z}$ ,  $x = 1$ . Тогда  $H+1 = \{2k+1 \mid k \in \mathbb{Z}\}$ . В частности,  $H+1 = H+3 = 1+H = H+(2t+1)$  при любом  $t \in \mathbb{Z}$ .

**Определение 9.3.2.** Множество  $G/H = \{Hx \mid x \in G\}$  всех правых смежных классов называется *фактормножеством группы  $G$  по подгруппе  $H$* . Мощность множества  $G/H$  обозначается как  $|G : H|$  и называется *индексом подгруппы  $H$  в группе  $G$* .

**ПРИМЕРЫ.** 1. Пусть  $G = S_3$ ,  $H = \{\varepsilon, (12)\}$ . Тогда  $G/H = \{H, H(123), H(132)\}$  (проверить!) и  $|G : H| = 3$ .

2.  $G = \mathbb{Z}$ ,  $H = 2\mathbb{Z}$ . Тогда  $G/H = \{H, H+1\}$  и  $|G : H| = 2$ .

**УПРАЖНЕНИЕ 9.3.1.**  $G = \mathbb{Z}$ ,  $H = n\mathbb{Z}$ . Доказать, что  $G/H = \mathbb{Z}_n$  и  $|G : H| = n$ .

УПРАЖНЕНИЕ 9.3.2. 1. Пусть  $G = S_n$ . Доказать, что  $H = \{\pi \in G \mid n\pi = n\}$  — множество всех подстановок, оставляющих на месте символ  $n$ , образует подгруппу в  $G$ . Найти индекс  $H$  в  $G$ .

2. Пусть  $p$  — простое число,  $G = GL_n(\mathbb{Z}_p)$ ,  $H = SL_n(\mathbb{Z}_p)$ . Найти  $|G : H|$ .

**Теорема 9.3.1.** Пусть  $G$  — группа,  $H \leq G$ . Справедливы следующие утверждения.

1. Если  $x \in G$ , то  $x \in Hx$ .
2. Если  $z \in Hx \cap Hy$ , то  $Hx = Hy$ .
3. Для любого  $x \in G$  отображение  $\varphi_x : H \rightarrow Hx$ , действующее по правилу  $h\varphi_x = hx$ , — биекция.
- 4 (теорема Лагранжа). Если  $G$  — конечная группа, то  $|G| = |H| \cdot |G : H|$ . В частности, порядок конечной группы делится на порядок каждой своей подгруппы.

ДОКАЗАТЕЛЬСТВО. 1. Поскольку  $e \in H$ , то  $x = e \cdot x \in Hx$ .

2. Пусть  $z \in Hx$ . Тогда  $Hx \subseteq H \cdot (Hx) = (H \cdot H)x = Hx$ . Кроме того, раз  $z \in Hx$ , то  $z = hx$  и  $x = h^{-1}z \in Hz$ , т.е.  $Hx \subseteq Hz$  и  $Hx = Hz$ .

Аналогично  $z \in Hy$ , откуда  $Hy = Hz$  и  $Hy = Hx$ .

3. Рассмотрим отображение  $\varphi : H \rightarrow Hx$ , действующее по правилу  $h\varphi = hx$ . Очевидно, что  $\varphi$  — сюръекция. Кроме того, если  $h_1\varphi = h_2\varphi$ , то  $h_1x = h_2x$ , откуда  $(h_1x)x^{-1} = (h_2x)x^{-1}$  и, значит,  $h_1 = h_2$ . Следовательно,  $\varphi$  — инъекция.

4. В силу п. 1 для любого  $x \in G$  существует смежный класс  $Hx$ , такой, что  $x \in Hx$ , следовательно,  $G = \bigcup_{x \in G} Hx$ . В силу п. 2 каждый  $x \in G$

содержится ровно в одном смежном классе. Наконец, из п. 3 следует, что каждый смежный класс имеет одно и то же число элементов, равное  $|H|$ , значит,  $|G| = |H| \cdot |G : H|$ .  $\square$

**Следствие.** Порядок элемента делит порядок группы.

ДОКАЗАТЕЛЬСТВО. Если  $g \in G$ , то  $|g| = |\langle g \rangle|$  делит  $|G|$ .  $\square$

УПРАЖНЕНИЕ 9.3.3. Если порядок группы  $G$  равен простому числу, то  $G$  циклическая.

**Следствие.** Если  $|G| = n$  и  $g \in G$ , то  $g^n = 1$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $|g| = k$ . Тогда  $n = k \cdot s$ , следовательно,  $g^n = (g^k)^s = 1^s = 1$ .  $\square$

УПРАЖНЕНИЕ 9.3.4 (малая теорема Ферма). Если  $a \in \mathbb{Z}$ ,  $p$  простое

и  $(a, p) = 1$ , то  $a^{p-1} \equiv 1 \pmod{p}$ .

Указание. Рассмотреть группу  $\langle \mathbb{Z}_p^*, \cdot \rangle$ , где  $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\bar{0}\}$ .

УПРАЖНЕНИЕ 9.3.5. Если  $H, K$  — конечные подгруппы группы  $G$ , то  $|HK| = |H||K|/|H \cap K|$ .

**Определение 9.3.3.** Пусть  $G$  — группа и  $x, g \in G$ . Элемент  $x^g = g^{-1}xg$  называется сопряжённым с элементом  $x$  посредством элемента  $g$  (или просто сопряжённым с  $x$ ).

УПРАЖНЕНИЕ 9.3.6. Пусть  $x, y, g, h$  — элементы группы  $G$ . Тогда

- 1)  $x^y = x \iff xy = yx$ ;
- 2)  $y = x^g \implies x = y^{g^{-1}}$ ;
- 3)  $y = x^g, z = y^h \implies z = x^{gh}$ .

УПРАЖНЕНИЕ 9.3.7. Две подстановки  $\pi$  и  $\tau$  из  $S_n$  сопряжены тогда и только тогда, когда они имеют одинаковое циклическое строение, т. е. для любого  $k \in \mathbb{N}$  число циклов длины  $k$  в разложении на независимые циклы у  $\pi$  и  $\tau$  совпадает.

**Определение 9.3.4.** Пусть  $G$  — группа,  $A \subseteq G$  и  $g \in G$ . Положим  $A^g = \{a^g \mid a \in A\}$ .

**Предложение 9.3.1.** Если  $H \leq G$ , то  $H^g \leq G$  — подгруппа (она называется подгруппой, сопряжённой с  $H$ ).

ДОКАЗАТЕЛЬСТВО. Пусть  $h, h_1, h_2 \in H$ . Тогда

$$\begin{aligned}(h^g)^{-1} &= (g^{-1}hg)^{-1} = g^{-1}h^{-1}g \in H^g, \\ (h_1^g) \cdot (h_2^g) &= g^{-1}h_1gg^{-1}h_2g = (h_1h_2)^g \in H^g.\end{aligned}$$

□

УПРАЖНЕНИЕ 9.3.8. Если  $g \in G$ , то преобразование  $\varphi_g : G \rightarrow G$  группы  $G$ , действующее по правилу  $x\varphi_g = x^g$  для любого  $x \in G$ , является автоморфизмом группы  $G$ . Множество всех таких автоморфизмов — подгруппа группы  $\text{Aut}(G)$ . Она называется группой внутренних автоморфизмов (обозначение:  $\text{Inn}(G)$ ).

**Определение 9.3.5.** Пусть  $x, y \in G$ . Элемент  $[x, y] = x^{-1}y^{-1}xy$  называется коммутатором элементов  $x$  и  $y$ .

ЗАМЕЧАНИЕ. Если  $z = [x, y]$ , то  $xy = yxz$  (элементы  $x$  и  $y$  “коммутируют с точностью до коммутатора”).

**Определение 9.3.6.** Подгруппа  $H$  группы  $G$  называется *нормальной* в  $G$ , если для любого  $g \in G$  выполняется  $Hg = gH$ . Обозначение:  $H \trianglelefteq G$ .

**ЗАМЕЧАНИЕ.** Утверждение о том, что  $Hx = xH$ , не эквивалентно тому, что  $hx = xh$  для любого  $h \in H$ , но эквивалентно другому: для любого  $h \in H$  существует  $h' \in H$ , такой, что  $hx = xh'$ .

**Теорема 9.3.2.** Пусть  $H \trianglelefteq G$ . Следующие утверждения эквивалентны:

- 1)  $H \trianglelefteq G$ ;
- 2)  $H^g \subseteq H$  для любого  $g \in G$ ;
- 3)  $[h, g] \subseteq H$  для любых  $h \in H$  и  $g \in G$ .

**ДОКАЗАТЕЛЬСТВО.** (1  $\Rightarrow$  2) Пусть  $Hg = gH$ . Тогда  $H^g = g^{-1}Hg = g^{-1}(gH) = H$ .

(2  $\Rightarrow$  3) Для любого  $h \in H$  и  $g \in G$  имеем  $h^g = g^{-1}hg \in H$ , откуда  $[h, g] = h^{-1}g^{-1}hg = h^{-1}h^g \in H$ .

(3  $\Rightarrow$  1) Для любых  $h \in H$  и  $g \in G$  имеем  $hg = gh[h, g] \in gH$ , следовательно,  $Hg \subseteq gH$ . Далее,  $Hg^{-1} \subseteq g^{-1}H$ , значит,  $(Hg^{-1})^{-1} \subseteq (g^{-1}H)^{-1}$ , следовательно,  $gH \subseteq Hg$  и  $Hg = gH$ .  $\square$

**ПРИМЕРЫ.** 1. Если  $G$  абелева и  $H \trianglelefteq G$ , то  $H \trianglelefteq G$ .

2. Если  $G = S_3$  и  $H = \{\varepsilon, (12)\}$ , то  $H \not\trianglelefteq G$ , так как  $H(123) \neq (123)H$ .

3.  $A_n \trianglelefteq S_n$ . Действительно,  $\text{sgn}(g^{-1}hg) = \text{sgn } g^{-1} \text{sgn } h \text{sgn } g = \text{sgn } h$ .

4.  $SL_n(F) \trianglelefteq GL_n(F)$ , так как  $\det(g^{-1}hg) = \det h$ .

**УПРАЖНЕНИЕ 9.3.9.** Доказать, что если  $|G : H| = 2$ , то  $H \trianglelefteq G$ .

**УПРАЖНЕНИЕ 9.3.10.**  $K_4 = \{\varepsilon, (12)(34), (13)(24), (14)(23)\} \trianglelefteq S_4$ . Группа  $K_4$  называется четверной группой Клейна.

**Указание.** Использовать упражнение 9.3.7.

**УПРАЖНЕНИЕ 9.3.11.** Пусть  $G$  — группа. Тогда  $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$ .

**Предложение 9.3.2.** Пусть  $H \trianglelefteq G$ . Тогда на фактормножестве  $G/H$  корректно задана бинарная алгебраическая операция (умножение) по правилу  $Hg_1 \cdot Hg_2 = H(g_1g_2)$ . Относительно этой операции  $G/H$  образует группу.

**ДОКАЗАТЕЛЬСТВО.** Проверим корректность.

$$Hg_1 \cdot Hg_2 = H(g_1H)g_2 = H(Hg_1)g_2 = H(g_1g_2).$$

Ассоциативность следует из упражнения 9.2.1. Единица в  $G/H$  — это смежный класс  $H = He$ , так как  $H \cdot Hg = Hg \cdot H = Hg$ . Наконец,

$(Hg)^{-1} = Hg^{-1}$ , поскольку  $Hg^{-1} \cdot Hg = H(g^{-1}g) = H$ .  $\square$

**Определение 9.3.7.** Группа  $\langle G/H, \cdot \rangle$  называется *факторгруппой* группы  $G$  по подгруппе  $H$ .

ПРИМЕР.  $\langle \mathbb{Z}_n, + \rangle = \langle \mathbb{Z}/n\mathbb{Z}, + \rangle$ .

УПРАЖНЕНИЕ 9.3.12. Привести пример, когда  $H \leq G$ , но  $H \not\trianglelefteq G$  и  $Hg_1 \cdot Hg_2 \neq H(g_1g_2)$ .

УПРАЖНЕНИЕ 9.3.13. Составить таблицу умножения в следующих факторгруппах:  $S_3/A_3$  и  $S_4/K_4$ .

## § 9.4. Гомоморфизмы групп

**Определение 9.4.1.** Пусть  $G$  и  $G'$  — группы. Отображение  $\varphi : G \rightarrow G'$  называется *гомоморфизмом* из  $G$  в  $G'$ , если для любых  $g_1, g_2 \in G$  выполняется  $(g_1g_2)\varphi = (g_1\varphi)(g_2\varphi)$ .

ЗАМЕЧАНИЕ. Изоморфизм — это биективный гомоморфизм.

ПРИМЕРЫ. 1. Отображение  $\varphi : \mathbb{R}^* \rightarrow \mathbb{R}^*$ , действующее по правилу  $x \rightarrow |x|$ , является гомоморфизмом, так как  $|xy| = |x||y|$ .

2.  $G = S_n$ ,  $G' = \mathbb{R}^*$ . Отображение  $\varphi : G \rightarrow G'$ , действующее по правилу  $g\varphi = \operatorname{sgn} g$ , является гомоморфизмом, так как  $\operatorname{sgn}(g_1 \cdot g_2) = \operatorname{sgn} g_1 \cdot \operatorname{sgn} g_2$ .

3.  $G = GL_n(F)$ ,  $G' = F^*$ . Отображение  $\varphi : G \rightarrow G'$ , заданное правилом  $g\varphi = \det g$ , является гомоморфизмом, так как  $\det(g_1 \cdot g_2) = \det g_1 \cdot \det g_2$ .

4. Пусть  $V$  — векторное пространство над  $F$  и  $\varphi \in \mathcal{L}(V)$ . Если  $G = G' = \langle V, + \rangle$ , то  $\varphi$  — гомоморфизм из  $G$  в  $G'$ , так как  $(v+u)\varphi = v\varphi + u\varphi$ .

**Определение 9.4.2.** Пусть  $\varphi : G \rightarrow G'$  — гомоморфизм группы  $G$  в группу  $G'$ . *Ядром* гомоморфизма  $\varphi$  называется множество  $\operatorname{Ker} \varphi = \{g \in G \mid g\varphi = 1_{G'}\}$ . *Образом* гомоморфизма  $\varphi$  называется множество  $\operatorname{Im} \varphi = G\varphi = \{g\varphi \mid g \in G\}$ .

ЗАМЕЧАНИЕ.  $\operatorname{Ker} \varphi \subseteq G$ ,  $\operatorname{Im} \varphi \subseteq G'$ . В примере 4  $\operatorname{Ker} \varphi$  и  $\operatorname{Im} \varphi$  — это стандартные ядро и образ линейного преобразования.

**Теорема 9.4.1** (первая теорема о гомоморфизмах). Пусть  $G, G'$  — группы и  $\varphi : G \rightarrow G'$  — гомоморфизм. Тогда

- 1)  $\operatorname{Im} \varphi \leq G'$ ;
- 2)  $\operatorname{Ker} \varphi \trianglelefteq G$ ;
- 3)  $\operatorname{Im} \varphi \simeq G/\operatorname{Ker} \varphi$ .

**Лемма.** Если  $1$  и  $1'$  — единицы групп  $G$  и  $G'$  соответственно, то

а)  $1\varphi = 1'$ ;

б)  $(g^{-1})\varphi = (g\varphi)^{-1}$ .

**ДОКАЗАТЕЛЬСТВО ЛЕММЫ.** Поскольку  $\varphi$  — гомоморфизм, для любого  $g \in G$  выполнено

$$(g\varphi)(1\varphi) = (g \cdot 1)\varphi = g\varphi, \text{ что доказывает п. а);}$$

$$(g\varphi)(g^{-1}\varphi) = (gg^{-1})\varphi = 1\varphi = 1', \text{ что доказывает п. б).}$$

**ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ.** 1) Пусть  $g_1, g_2 \in G$ . Применяя лемму, получим  $(g_1\varphi)(g_2\varphi)^{-1} = (g_1\varphi)(g_2^{-1}\varphi) = (g_1g_2^{-1})\varphi \in G\varphi$ , следовательно,  $G\varphi \leq G'$ .

2) Докажем сначала, что  $H = \text{Ker } \varphi \leq G$ . Пусть  $h_1, h_2 \in H$ . Тогда в силу леммы

$$(h_1 \cdot h_2^{-1})\varphi = (h_1\varphi) \cdot (h_2^{-1}\varphi) = (h_1\varphi)(h_2\varphi)^{-1} = 1' \cdot 1' = 1',$$

а значит,  $h_1 \cdot h_2^{-1} \in H$ , что и требовалось.

Далее, для любых  $h \in H$  и  $g \in G$  имеем:

$$(g^{-1}hg)\varphi = (g^{-1})\varphi \cdot h\varphi \cdot g\varphi = (g\varphi)^{-1} \cdot 1' \cdot (g\varphi) = 1',$$

следовательно,  $H^g \subseteq H$  и  $H \trianglelefteq G$ .

3) Докажем сначала, что  $Hg_1 = Hg_2$  тогда и только тогда, когда  $g_1\varphi = g_2\varphi$ . Действительно,

$$Hg_1 = Hg_2 \Leftrightarrow g_1g_2^{-1} \in H \Leftrightarrow 1' = (g_1g_2^{-1})\varphi = g_1\varphi \cdot (g_2\varphi)^{-1} \Leftrightarrow g_1\varphi = g_2\varphi.$$

Таким образом, отображение  $\psi : G/H \rightarrow G\varphi$ , действующее по правилу  $(Hg)\psi = g\varphi$ , определено корректно и является биекцией. Для любых  $g_1, g_2 \in G$  выполняется

$$(Hg_1 \cdot Hg_2)\psi = (H(g_1g_2))\psi = (g_1g_2)\varphi = (g_1\varphi)(g_2\varphi) = (Hg_1)\psi \cdot (Hg_2)\psi,$$

следовательно,  $\psi$  — изоморфизм. □

**ПРИМЕРЫ.** Пусть  $\varphi : G \rightarrow G'$  — гомоморфизм групп.

1. Если  $G = G' = \mathbb{R}^*$ ,  $x\varphi = |x|$ , то  $\text{Ker } \varphi = \{1, -1\} \simeq \mathbb{Z}_2$  и  $G/\text{Ker } \varphi \simeq \text{Im } \varphi = \mathbb{R}^+$ .

2. Если  $G = S_n$ ,  $G' = \mathbb{R}^*$  и  $g\varphi = \text{sgn } g$ , то  $\text{Ker } \varphi = A_n$  и  $G/\text{Ker } \varphi \simeq \text{Im } \varphi = \{1, -1\}$ .



3. Пусть  $G = GL_n(F)$ ,  $G' = F^*$  и  $g\varphi = \det g$ . Тогда  $\text{Ker } \varphi = SL_n(F)$  и  $G/\text{Ker } \varphi \simeq G'$  (это отображение “на”, так как для любого  $\alpha \in F^*$   $\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \alpha \end{pmatrix} \varphi = \alpha$ ).

4. Пусть  $H \trianglelefteq G$ . Отображение  $\varphi : G \rightarrow G/H$ , определённое правилом  $g\varphi = Hg$ , является гомоморфизмом, так как  $Hg_1 \cdot Hg_2 = H(g_1g_2)$ . В этом случае  $\text{Ker } \varphi = H$ ,  $\text{Im } \varphi = G/H$ . Этот гомоморфизм называется *каноническим* (или *естественным*) относительно  $H$ .

УПРАЖНЕНИЕ 9.4.1. Доказать, что  $S_4/K_4 \simeq S_3$ . Сколько с точностью до изоморфизма существует гомоморфных образов группы  $S_4$ ?

УПРАЖНЕНИЕ 9.4.2 (теорема Кэли). Каждая группа изоморфна некоторой группе подстановок.

Указание. Пусть  $G$  — группа,  $S(G)$  — группа всех подстановок множества  $G$ . Доказать:

- 1) для любого  $x \in G$  отображение  $\varphi_x : G \rightarrow G$ , действующее по правилу  $g\varphi_x = gx$ , лежит в  $S(G)$ ;
- 2) отображение  $\psi : G \rightarrow S(G)$ , действующее по правилу  $g\psi = \varphi_g$ , — гомоморфизм;
- 3)  $\text{Ker } \psi = 1$ , а значит,  $G \simeq G/\text{Ker } \psi \simeq \text{Im } \psi \leq S(G)$ .

УПРАЖНЕНИЕ 9.4.3. Пусть  $G$  — группа. Множество

$$Z(G) = \{z \in G \mid zg = gz \text{ для любых } g \in G\}$$

называется центром группы  $G$ . Доказать, что  $Z(G) \trianglelefteq G$  и  $G/Z(G) \simeq \text{Inn}(G)$ .

**Теорема 9.4.2** (вторая теорема о гомоморфизмах). Пусть  $G$  — группа,  $H \trianglelefteq G$  и  $K \leq G$ . Тогда  $HK \leq G$ ,  $H \trianglelefteq HK$ ,  $K \cap H \trianglelefteq K$  и  $HK/H \simeq K/K \cap H$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $k_1, k_2 \in K$ ,  $h_1, h_2 \in H$ . Тогда

$$(h_1k_1) \cdot (h_2k_2)^{-1} = h_1k_1 \cdot k_2^{-1}h_2^{-1} \underset{K \leq G}{=} h_1 \cdot k' \cdot h_2^{-1} \underset{H \trianglelefteq G}{=} h_1 \cdot h_2' \cdot k' = h'k' \in HK,$$

следовательно,  $HK \leq G$ . Так как  $K \leq G$ , то  $1 \in K$  и  $H = H \cdot 1 \subseteq HK$ , откуда  $H \leq HK$ . Поскольку  $Hg = gH$  для любого  $g \in HK \subseteq G$ , имеем  $H \trianglelefteq HK$ .

Рассмотрим отображение  $\varphi : K \rightarrow G/H$ , действующее по правилу  $k\varphi = Hk \in G/H$ . Для любых  $k_1, k_2 \in K$

$$(k_1 \cdot k_2)\varphi = H(k_1k_2) = Hk_1 \cdot Hk_2 = (k_1)\varphi \cdot (k_2)\varphi,$$

следовательно,  $\varphi$  — гомоморфизм. Так как  $\text{Ker } \varphi = \{k \in K \mid k\varphi = Hk = H\} = K \cap H$ , то по п. 2 теоремы 9.4.1  $K \cap H \trianglelefteq K$ . В силу того, что  $\text{Im } \varphi = \{k\varphi = Hk \mid k \in K\} = HK/H$ , по п. 3. теоремы 9.4.1  $K/K \cap H = K/\text{Ker } \varphi \simeq \text{Im } \varphi = HK/H$ .  $\square$

**Теорема 9.4.3** (третья теорема о гомоморфизмах). Пусть  $H, K \trianglelefteq G$  и  $K \leq H \leq G$ . Тогда  $\overline{H} = H/K \trianglelefteq G/K = \overline{G}$  и  $G/H \simeq \overline{G}/\overline{H}$ .

ДОКАЗАТЕЛЬСТВО. Рассмотрим отображение  $\varphi : G/K \rightarrow G/H$ , действующее по правилу  $(Kg)\varphi = Hg$ . Тогда

- 1)  $\varphi$  — гомоморфизм;
- 2)  $\text{Ker } \varphi = H/K$ ; и
- 3)  $\text{Im } \varphi = G/H$ .

Из утверждений 1)–3) и п. 3 теоремы 9.4.1 вытекает, что  $\overline{G}/\overline{H} = \overline{G}/\text{Ker } \varphi \simeq \text{Im } \varphi = G/H$ .  $\square$

УПРАЖНЕНИЕ 9.4.4. Доказать утверждения 1)–3) и тем самым теорему 9.4.3.

ПРИМЕР. Если  $G = S_4$ ,  $H = A_4$ ,  $K = K_4$ , то  $G/H \simeq (G/K)/(H/K) \simeq S_2$ . Проверить!

## § 9.5. Прямое произведение групп

**Предложение 9.5.1.** Пусть  $G_1, \dots, G_n$  — группы. Декартово произведение  $G_1 \times \dots \times G_n$  множеств  $G_1, \dots, G_n$  образует группу относительно операции, заданной правилом  $(x_1, \dots, x_n)(y_1, \dots, y_n) = (x_1y_1, \dots, x_ny_n)$ , где  $x_i, y_i \in G_i$  для  $i = 1, \dots, n$ .

ДОКАЗАТЕЛЬСТВО. Проверка аксиом группы.  $\square$

**Определение 9.5.1.** Группа  $G = G_1 \times \dots \times G_n = \prod_{i=1}^n G_i$ , определённая в предложении 9.5.1, называется *прямым (декартовым) произведением групп*  $G_1, \dots, G_n$ .

- УПРАЖНЕНИЕ 9.5.1. 1)  $|G_1 \times \dots \times G_n| = |G_1| \cdot \dots \cdot |G_n|$ .  
 2)  $|(x_1, \dots, x_n)| = \text{НОК}(|x_1|, \dots, |x_n|)$ .

**Теорема 9.5.1.** Пусть  $G$  — группа и  $H_1, \dots, H_n$  — её нормальные подгруппы, такие, что:

- 1)  $G = \langle H_1, \dots, H_n \rangle$ ;
- 2)  $H_i \cap \langle H_1, \dots, H_{i-1}, H_{i+1}, \dots, H_n \rangle = 1$  для любого  $i = 1, \dots, n$ .

Тогда для любого  $g \in G$  существуют и единственны  $h_i \in H_i$ ,  $i =$

$1, \dots, n$ , для которых  $g = h_1 \cdots h_n$ . В частности,  $G \simeq \prod_{i=1}^n H_i$ .

Обратно, если  $G = G_1 \times \cdots \times G_n$ , то существуют  $H_i \trianglelefteq G$ ,  $i = 1, \dots, n$ , такие, что  $H_i \simeq G_i$  и  $H_i$  удовлетворяют условиям 1 и 2 теоремы.

**ЗАМЕЧАНИЕ.** Допуская некоторую вольность, говорят, что  $G$  является прямым произведением своих подгрупп  $H_1, \dots, H_n$  (в этом случае мы имеем дело с так называемым *внутренним* определением прямого произведения, в отличие от *внешнего* определения (см. определение 9.5.1)).

**Лемма.** Если  $H, K \trianglelefteq G$  и  $H \cap K = 1$ , то  $[h, k] = 1$  для любых  $h \in H$ ,  $k \in K$ .

**ДОКАЗАТЕЛЬСТВО ЛЕММЫ.** Действительно,  $[h, k] = h^{-1}(k^{-1}hk) = (h^{-1}k^{-1}h)k \in H \cap K = 1$  в силу нормальности подгрупп  $H$  и  $K$  (см. п. 2 теоремы 9.3.2).  $\square$

**ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ.** В силу леммы  $h_i h_j = h_j h_i$  для всех  $h_i \in H_i$ ,  $h_j \in H_j$  при любых  $i, j \in \{1, 2, \dots, n\}$ , для которых  $i \neq j$ . Поскольку каждый элемент из  $g$  равен конечному произведению элементов из  $H_1, \dots, H_n$ , то, переставляя влево сначала все элементы из  $H_1$ , затем все элементы из  $H_2$  и т. д., мы получим, что  $g = h_1 \cdots h_n$ , где  $h_i \in H_i$ . Предположим, что  $g = h_1 \cdots h_n = h'_1 \cdots h'_n$ . Докажем, что  $h_i = h'_i$  для всех  $i = 1, \dots, n$ , индукцией по  $n$ . База при  $n = 1$  очевидна. Пусть  $n \geq 2$ . Тогда  $h'_n h_n^{-1} \in \langle H_1, \dots, H_{n-1} \rangle$ , откуда следует, что  $h_n = h'_n$ , а значит,  $h_1 \cdots h_{n-1} = h'_1 \cdots h'_{n-1}$ . Таким образом, представление  $g = h_1 \cdots h_n$  единственно для каждого  $g \in G$ .

По доказанному отображение  $\varphi : G \rightarrow H_1 \times \cdots \times H_n$ , заданное правилом  $g = h_1 \cdots h_n \mapsto (h_1, \dots, h_n)$  биективно и сохраняет операцию, значит,  $\varphi$  — искомый изоморфизм.

Пусть  $G = G_1 \times \cdots \times G_n$ . Для каждого  $i = 1, \dots, n$  обозначим через

$$H_i = \{(1, \dots, 1, g_i, 1, \dots, 1) \mid g_i \in G_i\}$$

проекцию  $G$  на  $G_i$ . Несложно проверить, что  $H_i \trianglelefteq G$ ,  $H_i \simeq G_i$  и  $H_i$  удовлетворяет условиям 1 и 2.  $\square$

**УПРАЖНЕНИЕ 9.5.2.** Заполнить пропуски в доказательстве теоремы 9.5.1.

**ПРИМЕР.** Группа  $S_2 \times S_2 \simeq K_4 = \langle (12)(34) \rangle \times \langle (13)(24) \rangle$ . Проверить!

**Предложение 9.5.2.** Если группа  $G = A \times B$  является прямым произведением своих нормальных подгрупп  $A$  и  $B$ , то  $G/A \simeq B$ .

**ДОКАЗАТЕЛЬСТВО.** В силу теоремы 9.5.1 для любого  $g \in G$  имеется единственное представление  $g = ab$ , где  $a \in A$ ,  $b \in B$ . Следовательно, отображение  $\varphi : G \rightarrow B$ , заданное правилом  $g\varphi = (ab)\varphi = b$ , определено корректно и, как несложно проверить с использованием леммы, является гомоморфизмом. Осталось заметить, что  $\text{Ker } \varphi = A$ ,  $\text{Im } \varphi = B$ , и применить теорему 9.4.1.  $\square$

**Определение 9.5.2.** Пусть  $p$  — простое число. Конечная группа  $G$  называется  $p$ -группой, если  $|G| = p^n$  для некоторого  $n \in \mathbb{N}$ . Группа  $G$  называется *примарной*, если она является  $p$ -группой для некоторого простого  $p$ .

**ПРИМЕРЫ.** 1.  $A_3$  — 3-группа.

2. Группа симметрий квадрата — 2-группа.

3. Если  $V$  — векторное пространство размерности  $n$  над  $\mathbb{Z}_p$ , то  $\langle V, + \rangle$  —  $p$ -группа.

Если на группе задана аддитивная операция, т. е. сложение (как принято для абелевых групп), то прямое произведение называется *прямой суммой*. Обозначение:  $G = G_1 \oplus \cdots \oplus G_n = \bigoplus_{i=1}^n G_i$ . В следующей теореме о структуре конечных циклических групп используется именно аддитивная запись.

**Теорема 9.5.2.** Пусть  $n \in \mathbb{N}$  и  $n = p_1^{k_1} \cdots p_s^{k_s}$  — разложение  $n$  в произведение простых чисел ( $p_i \neq p_j$ ). Тогда циклическая группа порядка  $n$  изоморфна прямой сумме примарных циклических подгрупп порядков  $p_1^{k_1}, \dots, p_s^{k_s}$  соответственно.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $G = \langle x \rangle$  и  $|G| = |x| = n$ . Используем индукцию по  $s$ . Заметим, что при  $s = 1$  утверждение очевидно, и предположим, что оно верно, если в разложении числа  $n$  встречается меньше чем  $s$  простых чисел. Положим  $l = p_1^{k_1}$ ,  $m = n/l$ ,  $a = mx$ ,  $b = lx$ . Тогда  $|a| = l$ ,  $|b| = m$  и  $(l, m) = 1$ .

Пусть  $A = \langle a \rangle$ ,  $B = \langle b \rangle$ . Тогда, во-первых,  $A \cap B = 0$ . Действительно, если  $c \in A \cap B$ , то  $|c|$  делит  $(l, m) = 1$ . Во-вторых, существуют  $\alpha, \beta \in \mathbb{Z}$ , такие, что  $\alpha m + \beta l = 1$ , т. е.  $\alpha a + \beta b = \alpha mx + \beta lx = x$ , а значит,  $G = \langle A, B \rangle$ . В силу теоремы 9.5.1 отсюда следует, что  $G = A + B$ . Группа  $B$ , являясь циклической, как подгруппа циклической группы  $G$  имеет порядок  $|B| = p_2^{k_2} \cdots p_s^{k_s}$ . По предположению индукции она изоморфна прямой сумме циклических подгрупп порядков  $p_2^{k_2}, \dots, p_s^{k_s}$ . Таким образом,  $G$  — прямое произведение циклических примарных подгрупп, что и требовалось.  $\square$

**ПРИМЕР.**  $G = \mathbb{Z}_6 = \{\bar{0}, \bar{1}, \dots, \bar{5}\}$ ,  $A = \{\bar{0}, \bar{2}, \bar{4}\} \simeq \mathbb{Z}_3$ ,  $B = \{\bar{0}, \bar{3}\} \simeq \mathbb{Z}_2$  и  $G \simeq A + B$  ( $A + B \ni (\bar{k}, \bar{l})\varphi = \bar{k} + \bar{l} \in G$ ).

**Предложение 9.5.3.** *Группа  $\mathbb{Z}_p^n$ , где  $p$  — простое число, неразложима в прямую сумму нетривиальных собственных подгрупп.*

**УПРАЖНЕНИЕ 9.5.3.** Доказать предложение 9.5.3.

**Указание.** Для любых нетривиальных подгрупп  $A$  и  $B$  группы  $\mathbb{Z}_p^n$  существует такой ненулевой  $x \in \mathbb{Z}_p^n$ , что  $x \in A \cap B$ .

## § 9.6. Действие группы на множестве

**Определение 9.6.1.** *Действием группы  $G$  на множестве  $\Omega$  называется произвольный гомоморфизм  $\varphi : G \rightarrow S(\Omega)$  из  $G$  в симметрическую группу подстановок множества  $\Omega$ . При этом образом элемента  $\alpha \in \Omega$  под действием элемента  $g \in G$  называется элемент  $\alpha \circ g = \alpha(g\varphi) \in \Omega$ .*

**Предложение 9.6.1.** *Если группа  $G$  действует на множестве  $\Omega$ , то*

- 1) для любых  $\alpha \in \Omega$  и  $g, h \in G$  выполняется  $\alpha \circ (gh) = (\alpha \circ g) \circ h$ ;
- 2) для любого  $\alpha \in \Omega$  выполняется  $\alpha \circ e = \alpha$ ;
- 3) для любых  $\alpha, \beta \in \Omega$  и  $g \in G$  из  $\alpha \circ g = \beta$  следует  $\beta \circ g^{-1} = \alpha$ .

**ДОКАЗАТЕЛЬСТВО.** 1) По определению гомоморфизма  $\alpha \circ (gh) = \alpha(gh)\varphi = \alpha(g\varphi)(h\varphi) = (\alpha g\varphi)(h\varphi) = (\alpha \circ g) \circ h$ , что доказывает п. 1.

Пункты 2 и 3 вытекают из свойств гомоморфизма (см. лемму в доказательстве теоремы 9.4.1).  $\square$

**УПРАЖНЕНИЕ 9.6.1.** Доказать эквивалентность исходного определения действия группы на множестве следующему: группа  $G$  действует на множестве  $\Omega$ , если для любых  $\alpha \in \Omega$  и  $g \in G$  определён элемент  $\alpha \circ g \in \Omega$  и выполняются свойства 1 и 2 из предложения 9.6.1.

**ЗАМЕЧАНИЕ.** В дальнейшем мы будем опускать знак  $\circ$  и писать просто  $\alpha g$  — образ  $\alpha$  под действием  $g$ .

**ПРИМЕРЫ.** 1. Если  $G \leq S(\Omega)$ , то гомоморфизм  $\varphi : G \rightarrow S(\Omega)$ , действующий по правилу  $\alpha(g\varphi) = \alpha g$ , задаёт (естественное) действие  $G$  на  $\Omega$ .

2. Если  $G \leq GL(V)$ , то гомоморфизм  $\varphi : G \rightarrow GL(V)$ , действующий по правилу  $v(g\varphi) = vg$ , задаёт (естественное) действие  $H$  на  $V$  (заметим, что  $GL(V) \leq S(V)$ ).

3. Если  $\Omega = G$ , то гомоморфизм  $G \rightarrow S(G)$ , определённый правилом  $x \mapsto xg$ , задаёт действие  $G$  на  $G$  *правыми сдвигами*.

4. Если  $H \leq G$  и  $\Omega = G/H$ , то гомоморфизм  $G \rightarrow S(G/H)$ , определённый правилом  $Hx \mapsto Hxg$ , задаёт действие  $G$  на  $G/H$  *правыми сдвигами*.

5. Если  $\Omega = G$ , то гомоморфизм  $G \rightarrow S(G)$ , действующий по правилу  $x \mapsto x^g = g^{-1}xg$ , задаёт действие  $G$  на  $G$  *сопряжениями*.

6. Если  $\Omega = H$  — группа, то гомоморфизм  $\varphi : G \rightarrow \text{Aut}(H) \leq S(\Omega)$ , действующий по правилу  $h \mapsto h(g\varphi)$  задаёт действие  $G$  на  $H$  *автоморфизмами*.

**Определение 9.6.2.** Пусть гомоморфизм  $\varphi : G \rightarrow S(\Omega)$  задаёт действие группы  $G$  на множестве  $\Omega$ . Ядро гомоморфизма  $\varphi$  называется *ядром действия*. Действие называется *точным*, если его ядро тривиально (т. е. является единичной подгруппой).

УПРАЖНЕНИЕ 9.6.2. Найти ядра действий в примерах 1–6.

**Определение 9.6.3.** Пусть группа  $G$  действует на множестве  $\Omega$ ,  $\alpha \in \Omega$ . Множество  $G_\alpha = \{g \in G \mid \alpha g = \alpha\}$  называется *стабилизатором* элемента  $\alpha$  в  $G$ . Множество  $\alpha G = \{\beta \in \Omega \mid \exists g \in G : \beta = \alpha g\} = \{\alpha g \mid g \in G\}$  называется *орбитой* элемента  $\alpha$  под действием  $G$ . Группа  $G$  действует на  $\Omega$  *транзитивно*, если  $\alpha G = \Omega$  для некоторого (а значит, и для любого)  $\alpha \in \Omega$ .

**Теорема 9.6.1.** Пусть группа  $G$  действует на множестве  $\Omega$ . Тогда

- 1)  $G_\alpha \leq G$  для любого  $\alpha \in \Omega$ ;
- 2) для любого  $\alpha \in \Omega$  множества  $G/G_\alpha$  и  $\alpha G$  равномощны;
- 3) множество  $\Omega$  совпадает с объединением орбит действия, и две орбиты либо не пересекаются, либо совпадают.

ДОКАЗАТЕЛЬСТВО. Положим  $H = G_\alpha$ ,  $\Delta = \alpha G$ .

1) Для любых  $h_1, h_2 \in H$  имеем  $\alpha(h_1 h_2^{-1}) = (\alpha h_1) h_2^{-1} = \alpha h_2^{-1} = \alpha$ , где последнее равенство вытекает из п. 3 предложения 9.6.1, следовательно,  $H \leq G$ .

2) Рассмотрим отображение  $\varphi : \Delta \rightarrow G/H$ , действующее по правилу  $(\alpha g)\varphi = Hg$ . Очевидно, что отображение сюръективно. С другой стороны, если  $Hg_1 = Hg_2$ , то существует  $h \in H$ , такой, что  $g_1 = hg_2$ , значит,  $\alpha g_1 = \alpha(hg_2) = (\alpha h)g_2 = \alpha g_2$ . Таким образом,  $\varphi$  — биекция.

3) Рассмотрим отношение “*лежат в одной орбите*” на множестве  $\Omega$ . В силу соответственно п. 2, 3 и 1 предложения 9.6.1 это отношение рефлексивно, симметрично и транзитивно, а значит, является отношением

эквивалентности. Орбиты заданного действия — классы этого отношения.  $\square$

**Следствие.** Если  $G$  — конечная группа, действующая на множестве  $\Omega$ ,  $\alpha \in \Omega$ , то  $|G| = |G_\alpha| \cdot |\alpha G|$ . В частности, если  $G$  действует транзитивно, то  $|G| = |G_\alpha| \cdot |\Omega|$  для любого  $\alpha \in \Omega$ .

ДОКАЗАТЕЛЬСТВО. Вытекает из п. 2 теоремы, так как  $|G|/|G_\alpha| = |G/G_\alpha| = |\alpha G|$ .  $\square$

ПРИМЕРЫ. 1. Пусть  $\Omega = \{1, \dots, n\}$  и группа  $G = S_n$  естественно действует на  $\Omega$ . Это действие транзитивно, и для любого  $\alpha \in \Omega$  стабилизатор  $G_\alpha \simeq S_{n-1}$  имеет индекс  $n$  в  $G$ .

2. Группа  $G = GL(V)$  оставляет на месте нулевой вектор и действует транзитивно на множестве  $V \setminus \{0\}$  ненулевых векторов.

3. Действие группы  $G$  на себе правыми сдвигами точное (сравните с доказательством теоремы Кэли) и транзитивное, а стабилизатор любого элемента, очевидно, равен единице (в последнем случае говорят, что действие *регулярно*).

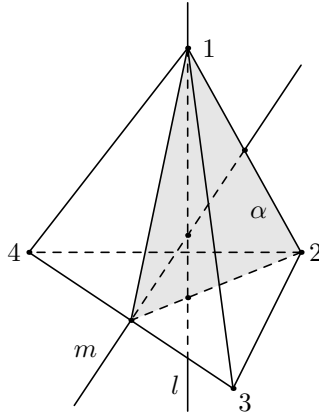
4. Пусть  $G$  действует на фактормножестве  $G/H$  правых смежных классов по подгруппе  $H$ . Это действие транзитивно, а стабилизатор точки  $\alpha = H$ , очевидно, равен  $H$ . Таким образом, если группа  $G$  конечна, то в соответствии со следствием из теоремы 9.6.1 мы получаем  $|G| = |H||G : H|$ , а значит, доказанная нами в § 3 теорема Лагранжа является частным случаем теоремы 9.6.1 и её следствия. По этой причине теорему 9.6.1 иногда называют обобщённой теоремой Лагранжа.

5. Пусть  $G$  действует на себе сопряжениями. Орбита этого действия  $xG = x^G = \{x^g \mid g \in G\}$  называется *классом сопряжённых элементов* (с представителем  $x$ ), а стабилизатор  $G_x = C_G(x) = \{g \in G \mid xg = gx\}$  элемента  $x$  в таком действии принято называть *централизатором*  $x$  в  $G$ . Теорема 9.6.1 в этом случае означает, что  $|G : C_G(x)| = |x^G|$ .

Покажем, как можно использовать доказанные нами утверждения в конкретных ситуациях.

ПРИМЕР. Пусть  $G$  — группа симметрий правильного тетраэдра. Покажем, что  $G \simeq S_4$ .

Пусть  $\Omega = \{1, 2, 3, 4\}$  — множество вершин тетраэдра. Поскольку любая симметрия тетраэдра переводит вершину в вершину, значит, определены естественный гомоморфизм  $\varphi : G \rightarrow S(\Omega)$  и действие  $G$  на  $\Omega$ . Это действие точное, так как только тождественная симметрия оставляет все вершины тетраэдра на месте. Поэтому  $G$  изоморфно вкладывается в  $S_4$ .



Найдём порядок группы  $G$ . Поскольку для каждой пары вершин найдётся симметрия, переводящая одну вершину в другую, группа  $G$  действует на  $\Omega$  транзитивно. Следовательно,  $|G| = 4 \cdot |G_1|$ , где  $G_1$  — стабилизатор вершины 1 в  $G$ .

Пусть  $G_{12} = (G_1)_2$  — стабилизатор вершины 2 в группе  $G_1$ . Тогда  $|G_1| = |G_{12}| \cdot |2 \cdot G_1|$ , где  $2 \cdot G_1$  — орбита вершины 2 под действием группы  $G_1$ . Однако длина такой орбиты равна 3, так как вращением относительно прямой  $l$ , проходящей через вершину 1 и центр противоположной грани, вершину 2 можно перевести в любую вершину, кроме первой (см. рисунок).

Наконец,  $|G_{12}| = 2$ , так как единственная нетривиальная симметрия, оставляющая на месте вершины 1 и 2 одновременно, — симметрия относительно плоскости  $\alpha$ , проходящей через вершины 1 и 2 и прямую  $m$ , соединяющую середины противоположащих рёбер.

Таким образом,  $|G| = 4 \cdot 3 \cdot 2 = 24 = |S_4|$ . Поскольку  $G$  изоморфно вкладывается в  $S_4$ , то  $G \simeq S_4$ .

Если мы вместо группы симметрий рассмотрим группу вращений правильного тетраэдра, состоящую только из тех симметрий, которые сохраняют ориентацию пространства, то аналогичные рассуждения показывают, что  $G \simeq A_4$  (в этом случае  $G_{12} = 1$ ). Поскольку она понадобится нам в следующем примере, взглянем на эту группу чуть подробнее. Группа  $G$  состоит из трёх видов преобразований:

- а) тождественного преобразования  $\varepsilon$ ;
- б) трёх поворотов на угол  $\pi$  относительно прямых, соединяющих середины противоположащих диагоналей (в частности, такому повороту относительно прямой  $m$  на рисунке соответствует цикл  $(12)(34)$  в  $A_4$ );



в) восьми поворотов на углы  $\frac{2\pi}{3}$  и  $\frac{4\pi}{3}$  относительно прямых, соединяющих вершину с центром противоположной грани (уже рассматривавшимся поворотам относительно прямой  $l$  в группе  $A_4$  соответствуют цикл (234) и обратный к нему).

**УПРАЖНЕНИЕ 9.6.3.** Найти порядки группы симметрий и группы вращений куба.

Чтобы сформулировать следующее утверждение о числе орбит действия конечной группы, которое принято называть *леммой Бернсайда*, нам понадобится следующее определение.

**Определение 9.6.4.** Пусть группа  $G$  действует на множестве  $\Omega$  и  $g \in G$ . Обозначим через  $\Omega_g = \{\alpha \in \Omega \mid \alpha g = \alpha\}$  множество неподвижных точек элемента  $g$  в  $\Omega$ .

**Теорема 9.6.2.** Пусть конечная группа  $G$  действует на конечном множестве  $\Omega$  и  $t(G)$  — число различных орбит этого действия. Тогда

$$|t(G)| \cdot |G| = \sum_{g \in G} |\Omega_g|.$$

**ДОКАЗАТЕЛЬСТВО.** Обозначим через  $F$  подмножество множества  $\Omega \times G$ , состоящее из всех пар  $(\alpha, g)$ , для которых  $\alpha g = \alpha$ . Идея доказательства состоит в подсчёте размера множества  $F$  двумя способами. С одной стороны,  $|F| = \sum_{g \in G} |\Omega_g|$ . С другой,  $|F| = \sum_{\alpha \in \Omega} |G_\alpha|$ . В силу

п. 3 теоремы 9.6.1 множество  $\Omega$  является объединением  $t = t(G)$  непересекающихся орбит  $\alpha_1 G, \dots, \alpha_t G$ , где  $\alpha_1, \dots, \alpha_t \in \Omega$ . Заметим, что порядки стабилизаторов элементов  $\alpha, \beta$  из одной орбиты равны, так как  $|G_\alpha| = |G|/|\alpha G| = |G|/|\beta G| = |G_\beta|$ . Поэтому

$$|F| = \sum_{\alpha \in \Omega} |G_\alpha| = \sum_{i=1}^t |G_{\alpha_i}| \cdot |\alpha_i G| = \sum_{i=1}^t |G| = t \cdot |G|,$$

где третье равенство выполняется в силу следствия из теоремы 9.6.1. Приравнивая к первому выражению для  $|F|$ , получаем требуемое.  $\square$

**ПРИМЕР.** Найдём решение следующей комбинаторной проблемы: *Найти число существенно различных раскрасок граней тетраэдра в три цвета. Раскраски существенно различны, если они не могут быть получены одна из другой вращением тетраэдра.*

Заметим, что, сопоставив грани противоположащую вершину, мы получим соответствие. Поэтому в этой задаче можно заменить грани на вершины.

Обозначим множество всех раскрасок с фиксированными вершинами через  $\Omega$ . Их число  $|\Omega|$ , очевидно, равно  $3^4 = 81$ .

Если рассмотреть действие группы  $G$  вращений тетраэдра на  $\Omega$ , то две раскраски будут существенно различны, если одну нельзя получить из другой с помощью действия некоторого элемента  $g \in G$ . Таким образом, искомое число  $t$  равно числу орбит действия  $G$  на  $\Omega$ . В силу леммы Бернсайда

$$t = \frac{1}{|G|} \sum_{g \in G} |\Omega_g|.$$

Как мы уже видели выше,  $G \simeq A_4$ , в частности  $|G| = 12$ . Заметим, что вращения одного и того же типа (с одинаковым циклическим типом подстановок вершин) оставляют неподвижными одно и то же количество раскрасок. Как мы знаем, таких типов всего три:

а) тождественное преобразование  $\varepsilon$  оставляет неподвижным все элементы множества  $\Omega$ , следовательно,  $|\Omega_\varepsilon| = 3^4$ ;

б) вращение, которому соответствует подстановка  $\pi = (12)(34)$ , оставляет неподвижными те раскраски, в которых совпадают цвета вершин 1 и 2 и одновременно вершин 3 и 4, поэтому  $|\Omega_\pi| = 3^2$ . Общее число таких симметрий равно 3;

в) вращение с перестановкой вершин  $\tau = (123)$  оставляет неподвижными те раскраски, в которых одинаков цвет вершин 1, 2 и 3, а значит,  $|\Omega_\tau| = 3^2$ ; общее число таких перестановок равно 8.

Окончательно получаем, что

$$t(G) = \frac{1}{12}(3^4 + 3 \cdot 3^2 + 8 \cdot 3^2) = \frac{3^2}{12}(3^2 + 3 + 8) = 15.$$

**УПРАЖНЕНИЕ 9.6.4.** Найти число раскрасок вершин тетраэдра в три цвета, не отличимых при его симметриях.

**УПРАЖНЕНИЕ 9.6.5.** Найти число различных ожерелий из семи бусин, раскрашенных в два цвета.

**УПРАЖНЕНИЕ 9.6.6. 1)** Доказать, что группа  $G$  вращений куба изоморфна  $S_4$ .

*Указание.* Рассмотреть действие  $G$  на множестве диагоналей куба.

- 2) Найти число неотличимых при вращениях раскрасок: а) вершин, б) граней, в) рёбер куба в  $n$  цветов.

## Предметный указатель

- Автоморфизм 214
- Алгебра 69
- Алгебраическая операция 13
  - а-ность операции 13
- Алгебраическая подсистема 15
- Алгебраическая система 13
- Алгебраическое дополнение 54
- Алгоритм Евклида 104
- Алгоритм Лагранжа 206
- Аннулирующий многочлен 167
  - минимальный 167
- Базис (база)
  - векторного пространства 73
  - согласованный с подпространством 81
- Биекция 9
- Векторное пространство 67
  - арифметическое 68
  - конечномерное 73
- Взаимно простые многочлены 105
- Высота
  - корневого вектора 153
  - корневого подпространства 154
- Гомоморфизм 222
  - канонический 224
- Группа 20, 214
  - $p$ -группа 227
  - Клейна четверная 221
  - абелева 20
  - автоморфизмов 215
    - – внутренних 220
    - линейная 59
  - линейных преобразований 146
  - ортогональных матриц 190
  - подстановок 29
    - – знакопеременная 35
    - – симметрическая 29
  - примарная 227
  - унитарных матриц 190
  - унитарных преобразований 190
  - циклическая 217
- Движение 11
- Действие группы на множестве 228
  - правыми сдвигами 229
  - автоморфизмами 229
  - регулярное 230
  - сопряжениями 229
  - точное 229
  - транзитивное 229
- Декартова степень множества 7
- Декартово произведение
  - групп 225
  - множеств 7
- Декремент подстановки 34
- Дефект
  - линейного преобразования 142
- Диагональный вид
  - квадратичной формы 204
- Дополнение множества 7
- Жорданов базис
  - нильпотентного преобразования 158
  - линейного преобразования 163
- Жорданов набор 158

- Жорданова
- клетка 164
  - матрица 164
- Знак подстановки 34
- Значение многочлена
- от матрицы 166
  - от преобразования 166
- Значение функции
- от матрицы 172
  - от преобразования 173
- Изоморфизм 16
- групп 214
- Индекс инерции
- отрицательный 207
  - положительный 207
- Индекс подгруппы 218
- Интерполяционный многочлен
- Лагранжа 109
  - Лагранжа — Сильвестра 112
- Инъекция 9
- Канонический вид
- квадратичной формы 209
- Квадратичная форма 202
- вещественная 206
  - положительно определённая 209
  - эквивалентные формы 203
- Класс
- сопряжённых элементов 230
- Кольцо 23
- ассоциативное 24
  - без делителей нуля 26
  - вычетов по модулю  $n$  26
  - квадратных матриц 38
  - коммутативное 24
  - многочленов
  - от нескольких переменных 115
  - от одной переменной 101
- с единицей 24
- Коммутатор 220
- Комплексное число 63
- аргумент к. ч. 65
  - действительная часть к. ч. 63
  - комплексно сопряжённое 64
  - корень  $n$ -ой степени из к. ч. 66
  - мнимая единица 63
  - мнимая часть к. ч. 63
  - модуль к. ч. 64
  - тригонометрическая форма 65
- Композиция отображений 8
- Координаты вектора 77
- Корневое подпространство 154
- Корневой вектор 153
- Коэффициенты
- системы уравнений
  - при неизвестных 92
  - свободные 92
- Критерий
- линейной зависимости 71
  - совместности системы линейных уравнений 93
- Лемма
- Бернсайда 232
  - Гаусса о примитивных многочленах 128
- Линейная зависимость 70
- Линейная комбинация 70
- нетривиальная 70
  - тривиальная 70
- Линейная независимость 70
- Линейная оболочка набора векторов 72
- Линейное отображение 140
- Линейное преобразование 133
- диагоналируемое 151
  - кососимметрическое 193
  - косоэрмитово 193

- невырожденное 144
- неотрицательное 195
- нильпотентное 158
- нормальное 184
- ортогональное 188
- положительное 195
- самосопряжённое 193
- симметрическое 193
- сопряженное к данному 182
- унитарное 188
- Линейные преобразования
  - изометричные 196
- Линейный оператор 133
- Матрица 35
  - перехода 78
  - вырожденная 58
  - главная диагональ м. 41
  - диагонализируемая 151
  - диагональная 40
  - единичная 40
  - замены 203
  - квадратичной формы 203
  - квадратная 36
  - клеточно диагональная 42
  - кососимметрическая 85
  - косоэрмитова 193
  - коэффициентов системы 92
  - – расширенная 92
  - линейного отображения 141
  - линейного преобразования 136
  - неотрицательная 196
  - нормальная 184
  - нулевая 40
  - обратная 59
  - ортогональная 188
  - положительная 196
  - присоединённая 58
  - редуцированная 93
  - симметрическая 85
  - скалярная 40
  - сопрягающая 140
  - сопряжённая к данной 182
  - ступенчатая 89
  - транспонированная 53
  - треугольная 52
  - унитарная 188
  - унифицированная 93
  - элементарная 43
  - эрмитова 193
- Матрицы
  - сопряжённые (подобные) 140
- Матричная форма записи
  - квадратичной формы 203
  - системы линейных уравнений 92
- Метод Гаусса 93
- Метод ортогонализации Грама — Шмидта 178
- Минор 86
  - дополнительный к элементу матрицы 54
  - окаймляющий 89
- Многочлен
  - от нескольких переменных 115
  - – лексикографически упорядоченный 116
  - – одночлен 115
  - – симметрический 117
  - – степень м. 116
  - – степень одночлена 115
  - – элементарный симметрический 117
  - от одной переменной 100
  - – делитель м. 103
  - – значение м. 108
  - – корень кратности  $r$  109
  - – корень м. 108
  - – кратное м. 103
  - – кратный корень м. 109
  - – неразложимый 106

- примитивный 128
- производная м. 110
- простой корень м. 109
- свободный коэффициент м. 100
- старший коэффициент м. 100
- степень м. 100
- Множество 6
  - неподвижных точек 232
  - пустое 7
- Моноид 22
- Набор векторов
  - ортогональный 177
  - ортонормированный 177
- Наибольший общий делитель многочленов 103
- Независимые циклы 31
- Неравенство Коши — Буняковского 176
- Ниль-слой 158
- Нормальный вид квадратичной формы 207
- Носитель подстановки 30
- Нуль-вектор 67
- Образ
  - гомоморфизма 222
  - линейного преобразования 142
  - элемента 228
- Общее решение системы 95
- Объединение множеств 7
- Определитель
  - линейного преобразования 145
  - матрицы 48
- Орбита
  - подстановки 30
  - элемента 229
- Ортогональное дополнение 180
- Основная теорема
  - алгебры 123
  - о симметрических многочленах 117
- Отображение 7
  - биективное 9
  - взаимно однозначное 9
  - на 8
  - обратное 9
- Пересечение множеств 7
- Подалгебра 69
- Подгруппа 22
  - нормальная 221
  - порождённая множеством 216
  - сопряжённая с данной 220
- Подкольцо 25
- Подмножество 6
  - замкнутое относительно операции 14
  - собственное 6
- Подполе 25
- Подпространство 69
  - инвариантное 146
  - циклическое 158
- Подстановка 27
- Поле 24
  - алгебраически замкнутое 123
  - комплексных чисел 61
  - числовое 63
- Полугруппа 22
- Полярное разложение 199
- Порождающее множество группы 217
- Порядок
  - группы 23, 214
  - кольца 25
  - поля 25
  - элемента группы 23, 214
- Преобразование 11
- Приведение квадратичной формы к главным осям 209

- Признак Эйзенштейна 129
- Проекция
- вектора на подпространство 85
- Произведение
- линейных преобразований 135
  - матриц 37
  - многочленов 101
  - отображений 8
  - подстановок 28
  - скаляра и вектора 67
  - скаляра и преобразования 135
- Пространство
- действительное 175
  - евклидово 176
  - комплексное 175
  - унитарное (эрмитово) 176
- Прямое произведение групп 225
- Равномощные множества 9
- Размерность
- векторного пространства 75
  - квадратной матрицы 36
- Разность множеств 7
- Ранг
- квадратичной формы 204
  - линейного преобразования 142
  - матрицы 89
  - – минорный 87
  - – столбцовой 86
  - – строчный 86
  - набора векторов 86
- Расширение поля 119
- Сингулярное разложение 200
- Сингулярное число
- линейного преобразования 197
  - матрицы 197
- Система линейных уравнений 92
- однородная 96
  - решение системы 92
  - совместность системы 92
  - эквивалентность систем 92
- Скалярное произведение 175
- стандартное 176
- Смежный класс
- левый 218
  - правый 218
  - представитель с. к. 218
- Собственное число (значение) 148
- Собственный вектор 148
- Спектр
- линейного преобразования 149
  - матрицы 149
- Стабилизатор элемента 229
- Стандартная запись
- квадратичной формы 203
- Столбец 36
- Строка 36
- Сужение
- линейного преобразования на подпространство 147
  - операции на подмножество 14
- Сумма
- векторов 67
  - линейных преобразований 135
  - матриц 37
  - многочленов 101
  - подпространств 81
  - – прямая 83
- Сюръекция 8
- Теорема
- Безу 108
  - Гамильтона — Кэли 168
  - Жордана 163
  - – в матричной форме 165
  - Кронекера — Капелли 93
  - Кэли 224
  - Ферма малая 219
  - Фредгольма 98



- вторая о гомоморфизмах 224
- закон инерции квадратичных форм 207
- о базисе 74
- о делении с остатком 102
- о жордановом базисе нильпотентного преобразования 160
- о замене 72
- о каноническом виде матрицы косоэрмитова преобразования 194
- о каноническом виде матрицы нормального преобразования в унитарном пространстве 184
- о каноническом виде матрицы самосопряжённого преобразования 193
- о каноническом виде матрицы унитарного и ортогонального преобразований 191
- о корневом разложении 154
- о минимальном аннулирующем многочлене 167
- о нормальном виде вещественной квадратичной формы 206
- о полярном разложении 198
- о разложении определителя по строке 55
- о ранге матрицы 87
- о свойствах нормального преобразования 184
- о сингулярном разложении 200
- о ядерном распаде 169
- об обратной матрице 59
- первая о гомоморфизмах 222
- третья о гомоморфизмах 225
- Трансвекция 43
- Транспозиция 33
- Угловой  $k$ -ый минор матрицы 210
- Упорядоченная пара 7
- Упорядоченный набор ( $n$ -ка) 7
- Факторгруппа 222
- Факормножество 218
- Формула
  - Муавра 66
  - Тейлора 111
  - извлечения корня из комплексного числа 66
  - разложения определителя по строке 55
  - умножения комплексных чисел в тригонометрической форме 65
- Формулы
  - Виета 122
  - Крамера 96
- Фундаментальный набор решений однородной системы 97
- Характеристика поля 111
- Характеристический корень
  - матрицы 149
- Характеристический многочлен
  - линейного преобразования 149
  - матрицы 148
- Центр группы 224
- Централизатор 230
- Цикл 31
- Чётность подстановки 34
- Элемент 6
  - группы
    - – нейтральный 20, 214
    - – обратный 20, 214

- 
- сопряжённый с данным 220
  - кольца
  - делитель нуля 26
  - обратимый 24
  - Элементарные преобразования
  - матрицы 45
  - Ядро
    - гомоморфизма 222
    - линейного преобразования 142
  - Ядро действия 229

## Указатель обозначений

$\emptyset$	7	$\varphi^*$	182
$2^A$	7	$f \sim_T g$	203
$\bigoplus_s U_i$	83	$f_A(x)$	148
$\langle A \rangle$	72, 216	$f_\varphi(x)$	149
$[\varphi]_B$	136	$f \dot{\vdash} g$	103
$[v]_B$	77	$G/H$	218
$[x, y]$	220	$GL(V)$	146
$ G $	23	$GL_n(F)$	59, 215
$ G : H $	218	$GO(V)$	190
$ g $	23	$GO_n(\mathbb{R})$	190
$ z $	65	$GU(V)$	190
$(f, g)$	103	$GU_n(\mathbb{C})$	190
$A'$	53	$G_\alpha$	229
$A^*$	182	$g \mid f$	103
$A^n$	7	$g \nmid f$	103
$A_1 \times A_2 \times \dots \times A_n$	7	$H \leq G$	22
$A_n$	35	$H \trianglelefteq G$	221
$\text{Aut}(G)$	215	$\text{Im } \varphi$	142, 222
$\alpha G$	229	$\text{Inn}(G)$	220
$\arg z$	65	$K_4$	221
$B \subseteq A$	6	$\text{Ker } \varphi$	142, 222
$\mathbb{C}$	61	$L(A)$	72
$\text{char } F$	111	$\mathcal{L}(V)$	133
$D(\alpha_1, \alpha_2, \dots, \alpha_n)$	40	$\mathcal{L}(V, U)$	140
$\deg f$	100	$M^*$	180
$\det(A)$	48	$M_{m \times n}(S)$	36
$\dim V$	75	$M_n(S)$	36
$\text{def}(\varphi)$	142	$\mathbb{N}$	6
$d(\pi)$	34	$\mathbb{N}_0$	100
$E$	40	$n\mathbb{Z}$	22
$E_{rs}(\alpha)$	43	$\Omega_g$	232
$\varepsilon$	28, 134	$P(A)$	7
$\varphi _U$	147		

$\prod_{i=1}^n G_i$  225 $\mathbb{Q}$  6 $R[x]$  100 $R^*$  24 $\mathbb{R}$  6 $\text{rank}(\varphi)$  142 $r(A)$  86, 89 $SL_n(F)$  215 $S_n$  29 $\sum_{i=1}^s U_i$  81 $\text{Sp}(A)$  149 $\text{Sp}(\varphi)$  149 $\text{Sym}(M)$  29 $\text{sgn}(\pi)$  34 $\text{supp}(\pi)$  30 $U\varphi$  142 $Z(G)$  224 $\mathbb{Z}$  6 $\mathbb{Z}_n$  26 $\bar{z}$  64

# Приложение

## Программа курса высшей алгебры

2016–17 учебный год

1 семестр

### 1. Введение

Множества, отображения, алгебраическая операция, алгебраическая система, сужение операции на подмножество, подсистема, изоморфизм [8, гл. 4, § 1], [5, гл. 1, § 1], [3, § 9], [15, гл. 1].

### 2. Группы, кольца, поля

Группа, кольцо, поле: аксиомы, примеры, элементарные свойства, кольцо вычетов [8, гл. 4, § 2,3], [5, гл. 1, § 3, 6], [3, § 6, 11, 12], [14, § 1, 2]. Группа подстановок: проверка аксиом, разложение подстановки в произведение циклов, декремент, чётность, разложение в произведение транспозиций, чётность произведения, знакопеременная группа [7, гл. 4, § 2.4], [8, гл. 1, § 8]. Кольцо квадратных матриц: проверка аксиом [16, § 1], [5, гл. 1, § 9], разложение матрицы в произведение элементарных и диагональной матриц. Определитель, его поведение при простейших преобразованиях. Определитель произведения матриц. Разложение определителя по строке (столбцу) [8, гл. 3, § 1, 2], [13, § 4–6]. Обратная матрица: существование, вычисление, решение линейных матричных уравнений [16, § 2], [5, гл. 2, § 5]. Поле комплексных чисел: существование, единственность. Геометрическая интерпретация комплексных чисел: модуль, аргумент, тригонометрическая форма записи, формула Муавра, извлечение корня  $n$ -ой степени из комплексного числа [8, гл. 5, § 1], [5, гл. 1, § 5].

### 3. Векторные пространства

Векторное пространство над полем: аксиомы, примеры, понятие подпространства. Алгебра и подалгебра над полем: примеры [16, § 4], [5,

гл. 1, § 7, 8], [23, § 3.1]. Базис и размерность векторного пространства: линейные комбинации, линейная зависимость, эквивалентные наборы векторов, теорема о замене и её следствия, базис пространства, размерность, координаты, изоморфизм пространств. Матрица перехода, её невырожденность, связь между координатами в разных базах [16, § 4, 5], [5, гл. 1, § 7, гл. 2, § 2], [23, § 3.2, 3.4, 3.5]. Подпространство, базис, согласованный с подпространством, взаимное расположение подпространств, сумма и пересечение подпространств, связь между их размерностями, прямая сумма [16, § 6]; [5, гл. 5, § 1], [23, § 3.2].

#### 4. Системы линейных уравнений

Ранг матрицы: ранг набора векторов, строчный и столбцовый ранги матрицы, минор, минорный ранг, теорема о совпадении трёх рангов, вычисление ранга приведением матрицы к ступенчатому виду, ранг суммы и произведения матриц [16, § 5], [13, § 10], [5, гл. 2, § 1]. Система линейных уравнений: векторная и матричная формы, критерий совместности системы линейных уравнений (теорема Кронекера–Капелли), общее решение и метод Гаусса его поиска, системы линейных уравнений с ненулевым определителем, формулы Крамера [13, § 1, 7]; [16, § 5]; [5, гл. 2, § 1]. Однородные системы: пространство решений, фундаментальный набор решений, связь между однородными и неоднородными системами, теорема Фредгольма [13, § 11, 12]; [16, § 5].

#### 5. Кольца многочленов

Многочлены от одной переменной: определение, кольцо многочленов над кольцом и полем, степень суммы и произведения многочленов [5, гл. 3, § 1], [13, § 20]. Делимость в кольце многочленов: деление с остатком, наибольший общий делитель, алгоритм Евклида, взаимно простые многочлены, неразложимые многочлены, разложение на линейные множители [8, гл. 5, § 2, 3], [13, § 21, 48], [5, гл. 3, § 5]. Значения и корни многочленов: теорема Безу, теорема о числе корней, интерполяционный многочлен Лагранжа, кратные корни, характеристика поля, производная и её приложения к многочленам над полем характеристики 0, формула Тейлора, интерполяционный многочлен Лагранжа–Сильвестра [13, § 22], [16, § 16.3], [5, гл. 3, § 2]. Кольцо многочленов от нескольких переменных: определение, элементарные свойства, лексикографическое упорядочение одночленов, старшая степень, симметрические многочлены, основная теорема о симметрических многочленах [13,

§ 51, 52], [5, гл. 3, § 7, 8], [8, гл. 6, § 2]. Теорема о существовании корня многочлена в расширении поля и её следствия: разложение на линейные множители в расширении поля, формулы Виета [13, § 49]. Алгебраическая замкнутость поля комплексных чисел и разложение многочленов на множители над полями комплексных и вещественных чисел [13, § 55], [8, гл. 6, § 3]. Разложимость многочлена над полем рациональных чисел: сведение к многочленам с целочисленными коэффициентами, признак неразложимости над кольцом целых чисел и существование неразложимого многочлена произвольной степени, алгоритмическая разрешимость проблемы разложения многочлена над полем рациональных чисел [13, § 56, 57], [5, гл. 3, § 6]. Оценка числа действительных корней: границы корней, ряд Штурма и теорема Штурма [13, § 39, 40], [8, гл. 6, § 4].

## 2 семестр

### 6. Линейные преобразования векторных пространств

Линейное преобразование и его матрица. Координаты образа, связь между матрицами линейного преобразования в разных базах, подобные матрицы. Операции над линейными преобразованиями, изоморфизм алгебраической системы линейных преобразований и алгебры матриц, линейное отображение и его матрица. Ядро и образ линейного преобразования, невырожденные линейные преобразования [16, § 8–10], [5, гл. 2, § 3, гл. 6, § 1], [21], [23, § 3.3]. Инвариантное пространство, ограничение на него линейного преобразования. Собственные векторы и собственные значения, характеристический многочлен [16, § 11], [9, гл. 2, § 3], [5, гл. 6, § 2], [21], [23, § 4.1]. Корневые подпространства, разложение в прямую сумму корневых подпространств. Нильпотентное преобразование, разложение в прямую сумму циклических подпространств. Жорданова база пространства. Жорданова форма матрицы [9, гл. 2, § 4], [5, гл. 6, § 4], [21], [23, гл. 5]. Многочлены от матриц и линейных преобразований. Минимальный аннулирующий многочлен, теорема Гамильтона–Кэли, теорема о ядерном разложении. Функции от матриц и линейных преобразований, представления их значений значениями многочленов [16, § 16], [5, гл. 6, § 5], [21].

## 7. Преобразования евклидовых и унитарных пространств

Евклидовы и унитарные пространства: аксиомы, примеры. Процесс ортогонализации, ортонормированные базы, ортогональное дополнение к подпространству [16, § 17]. Сопряжённые преобразования: связь между матрицами. Нормальные преобразования, свойство их собственных векторов, канонический вид матрицы нормального преобразования в унитарном и евклидовом пространстве [16, § 18]. Унитарные, ортогональные и самосопряжённые преобразования, их матрицы, канонический вид унитарного, ортогонального и самосопряжённого преобразований. Неотрицательные самосопряжённые преобразования, сингулярные числа, полярное и сингулярное разложение матрицы [16, § 19–20], [5, гл. 6, § 3], [9, гл. 3].

## 8. Квадратичные формы

Матрица квадратичной формы, её изменение при линейной замене. Алгоритм Лагранжа приведения к диагональному виду. Нормальная форма вещественной квадратичной формы, закон инерции квадратичных форм. Приведение к главным осям. Положительно определённые квадратичные формы и одновременная диагонализация двух форм [16, § 22, 23]; [13, §26–28], [5, гл. 5, § 3], [23, гл. 6].

## 9. Начала теории групп

Группы и их подгруппы: примеры [6, § 1], [5, гл. 4, § 1, 2]. Порождающее множество и циклическая подгруппа. Смежные классы по подгруппе, индекс подгруппы и теорема Лагранжа. Сопряжённые элементы, коммутаторы, нормальные подгруппы и факторгруппы [6, § 2], [5, гл. 4, § 3–5]. Теоремы о гомоморфизмах [6, § 4], [5, гл. 4, § 6]. Прямые произведения групп, связь между двумя определениями. Разложение циклической группы конечного порядка в прямое произведение примарных подгрупп [5, гл. 10 § 1], [3, гл. 2], [14, § 2–4]. Действие группы на множестве. Стабилизатор и орбита, связь между их порядками. Лемма Бернсайда о количестве орбит и её применение к задаче о раскраске тетраэдра [5, гл. 10, § 3].



## Список литературы

1. *Аржанцев И. В., Батырев В. В., Бунина Е. И. и др.* Студенческие олимпиады по алгебре на мехмате МГУ. – Электронное изд., – М.: МЦНМО, 2015.
2. *Бардаков В. Г.* Лекции по алгебре Ю. И. Мерзлякова: Учебное пособие. – Новосибирск: Изд. НГУ, 2012.
3. *Ван дер Варден Б. Л.* Алгебра. – М.: Наука, 1976.
4. *Васильев А. В., Мазуров В. Д.* Высшая алгебра: Конспект лекций. Ч. 1. – Новосибирск: Изд. НГУ, 2010.
5. *Винберг Э. Б.* Курс алгебры. – М.: Факториал Пресс, 2002.
6. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. – М.: Наука, 1982.
7. *Кострикин А. И.* Введение в алгебру. – М.: Наука, 1977.
8. *Кострикин А. И.* Введение в алгебру. Ч. 1. Основы алгебры: Учебник для вузов. – 3-е изд. – М.: Физматлит, 2004.
9. *Кострикин А. И.* Введение в алгебру. Ч. 2. Линейная алгебра: Учебник для вузов. – 3-е изд. – М.: Физматлит, 2004.
10. *Кострикин А. И.* Введение в алгебру. Ч. 3. Основные структуры: Учебник для вузов. – 3-е изд. – М.: Физматлит, 2004.
11. Сборник задач по алгебре / под ред. А. И. Кострикина: Учебник для вузов. – 3-е изд. – М.: Физматлит, 2001.
12. *Кострикин А. И., Манин Ю. И.* Линейная алгебра и геометрия. – 4-е изд. – М.: Лань, 2008.
13. *Курош А. Г.* Курс высшей алгебры. – М.: Наука, 1968.
14. *Ленг С.* Алгебра. – М.: Мир, 1968.
15. *Мальцев А. И.* Алгебраические системы. – М.: Наука, 1970.

16. *Мальцев А. И.* Основы линейной алгебры. – М.: Наука, 1970.
17. *Пожидаев А. П., Сверчков С. Р., Шестаков И. П.* Лекции по алгебре: Учебное пособие для студентов 1 курса ММФ НГУ. Ч. 1,2. – Новосибирск: Изд. НГУ, 2011.
18. *Проскураков И. В.* Сборник задач по линейной алгебре, 9-е изд. – М.: Бином. Лаб. знаний, 2005.
19. *Фаддеев Д. К.* Лекции по алгебре. – М.: Наука, 1984.
20. *Фаддеев Д. К., Соминский И. С.* Сборник задач по высшей алгебре. – М.: Наука, 1977.
21. *Чуркин В. А.* Жорданова классификация конечномерных линейных операторов. – Новосибирск: НГУ, 1991.
22. *Чуркин В. А.* Задания по алгебре для 1 курса ММФ. – Новосибирск: Изд. НГУ, 2007.
23. *Шафаревич И. Р., Ремезов А. О.* Линейная алгебра и геометрия. – М.: Физматлит, 2009.

Учебное издание

**Васильев** Андрей Викторович,  
**Лыткина** Дарья Викторовна,  
**Мазуров** Виктор Данилович

## ВЫСШАЯ АЛГЕБРА

конспект лекций

Подписано в печать 28.09.2020  
Формат 60 × 84 1/16. Офсетная печать  
Усл. печ. л. 14,65. Тираж 100 экз.  
Заказ № 35

Лицензия ЛР № 065614 от 8 января 1998 г.  
Издательство Института математики,  
пр. Академика Коптюга, 4, 630090 Новосибирск, Россия.

Отпечатано в ООО «Омега Принт»,  
пр. Академика Лаврентьева, 6, 630090 Новосибирск, Россия.