Московский государственный университет
имени М.В. Ломоносова
Механико-математический факультет

На правах рукописи

**Хрыстик Михаил Андреевич**

# Длины групповых алгебр

1.1.5. Математическая логика, алгебра, теория чисел
и дискретная математика

диссертация на соискание ученой степени
кандидата физико-математических наук

Научный руководитель:

кандидат физико-математических наук,
доцент Маркова Ольга Викторовна

Москва 2024

# Содержание

# Введение

## Общая характеристика работы

Работа подготовлена на кафедре высшей алгебры механико-математического факультета Московского государственного университета имени М. В. Ломоносова. В работе исследуются

- длины групповых алгебр абелевых групп;
- длины групповых алгебр диэдральных групп;
- длины групповых алгебр групп малых порядков.

### Актуальность темы исследования

Диссертация является исследованием в области групповых алгебр. В работе изучаются системы порождающих групповых алгебр, вычисляются длины и другие числовые характеристики различных групповых и матричных алгебр.

Введём центральное понятие темы исследования — понятие длины конечномерной ассоциативной алгебры. Если $\mathcal{S}$ — система порождающих алгебры $\mathcal{A}$, то есть $\mathcal{A}$ совпадает с минимальной своей подалгеброй, содержащей $\mathcal{S}$, то любой элемент алгебры $\mathcal{A}$ может быть представлен в виде линейной комбинации слов над $\mathcal{S}$. Минимальное $k$ такое, что мы можем выразить все элементы $\mathcal{A}$, используя слова длины не более $k$, назовем длиной системы порождающих $\mathcal{S}$. Длиной алгебры $\mathcal{A}$ назовем максимальную длину среди её систем порождающих, будем обозначать её $l(\mathcal{A})$.. В определении длины алгебры $\mathcal{A}$ мы рассматриваем множество всех порождающих систем для $\mathcal{A}$. Этим объясняется сложность вычисления длины даже для классических алгебр.

Важным примером конечномерных ассоциативных алгебр являются групповые алгебры конечных групп, которые и являются объектом исследования.

Изучение строения групповых алгебр является классическим направлением исследований, имеющих важное значение в теории представлений. Здесь можно от-

метить такие классические результаты, как теорема Машке и теорема Веддербёрна-Артина. Строение групповых алгебр конечных абелевых групп было подробно рассмотрено в работе С. Перлиса и Г. Волкера [29] в 1950 г.

При исследовании вопросов, связанных с образующими групповых алгебр, естественным образом возникает потребность в качестве порождающей системы групповой алгебры $\mathbb{F}G$ рассмотреть систему образующих группы $G$. Отметим, что для группы $G$ и её системы порождающих $S$ широко изучается соответствующая задача нахождения кратчайшего слова от образующих, представляющего элемент $g \in G$. Подробное рассмотрение этой темы можно найти в обзоре [8] и его библиографии. Одним из ключевых понятий при изучении соответсвующего вопроса для групп является диаметр группы. *Диаметром* группы $G$ относительно системы образующих $S$ называется максимум по $g \in G$ длин кратчайших слов от $S \cup S^{-1}$, представляющих $g$. В работе [3] Л. Бабаи получил асимптотические оценки диаметра групп. Эти исследования были продолжены Х. Хельфготтом в работе [12] в 2019 г.

Отметим, что изучение порождающих систем групповой алгебры $\mathbb{F}G$ не сводится к изучению систем образующих группы $G$, что иллюстрирует, в частности, доказанная в ходе исследования теорема о том, что над полем характеристики ноль групповая алгебра любой (в том числе не являющейся циклической) конечной абелевой группы имеет максимальную длину, что равносильно однопорождённости.

Системы порождающих групповых алгебр на данный момент изучены гораздо меньше. Поскольку порождающие множества групповой алгебры, вообще говоря, не исчерпываются порождающими множествами соответствующей группы, имеющиеся вычисления диаметра групп могут обеспечить лишь нижние оценки длины групповых алгебр. Вопрос получения верхних оценок, и, тем более, точного вычисления длин конкретных групповых алгебр остаётся открытым и актуальным.

Ввиду наличия матричных представлений изучение числовых характеристик групповых алгебр неразрывно связано с изучением чиловых характеристик матричных алгебр. Для функции размерности эти исследования восходят к работе Шура 1905 г. [1], в которой получена верхняя оценка размерности $\left[\frac{n^2}{4}\right] + 1$ коммутативных подалгебр алгебры матриц порядка $n$ над полем комплексных чисел, где

$[x]$ обозначает наибольшее целое число, не превосходящее $x$. Эта область активно развивается в течение XX века, достаточно упомянуть работы Джекобсона 1944 г. [10], в которой оценка Шура была перенесена на случай произвольного поля, Герштенхабера 1961 г. [11], в которой получена оценка размерности коммутативной алгебры, порожденной двумя матрицами, Паза 1984 г. [7], результаты которого описаны ниже, монографию Супруненко и Тышкевич 1966 г. [9], а также работы [36] и [35].

Задача вычисления длины впервые возникла в работах Спенсера и Ривлина 1959–60гг. [4], [5] для полной алгебры матриц порядка 3 в связи с возможным применением в механике сплошных сред. В общей формулировке проблема вычисления длины полной алгебры матриц $M_n(\mathbb{F})$ как функции порядка матриц была поставлена Пазом в 1984 году в работе [7] и до сих пор является открытой. Существует гипотеза, состоящая в том, длина полной матричной алгебры равна $2n-2$, где $n$ — порядок матриц. Известно, что эта гипотеза верна при $n = 2, 3, 4, 5$ (см. [7], [30]). Однако все существующие верхние оценки длины алгебры матриц не являются линейными.

В работе Паза [7, теорема 2] также было доказано, что верхняя оценка длины коммутативной матричной подалгебры над полем комплексных чисел $\mathbb{C}$ равна $n-1$, т.е. для коммутативных подалгебр получена линейная относительно порядка матриц точная верхняя оценка длины.

Основные алгебраические свойства функции длины, такие как поведение длины при взятии прямых сумм алгебр, тензорных произведений алгебр, присоединении к алгебре единицы и многие другие, были изучены О.В. Марковой в работе 2012 года “Функция длины и матричные алгебры” [2].

Поскольку групповые алгебры имеют матричные представления, изучение длин групповых алгебр не только имеет теоретический интерес, но и тесно связано с изучением длин матричных алгебр. Длинам групповых алгебр посвящена серия работ 2018-23гг. [25], [26], [38], [37], [39], [40], [27], [41], которая будет подробно рассмотрена в диссертации.

Таким образом, тема исследований, рассмотренных в работе представляет интерес и активно развивается.

## Цели и задачи работы

В работе решаются следующие задачи:

- исследуются длины групповых алгебр абелевых групп;
- вычисляются длины некоторых матричных алгебр, являющихся представлениями групповых алгебр;
- исследуются длины групповых алгебр диэдральных групп;
- вычисляются длины групповых алгебр групп малых порядков.

## Объект и предмет исследования

Объект исследования — групповые и матричные алгебры.

Предмет исследования — функция длины конечномерной ассоциативной алгебры.

## Методы исследования

В работе применяются как классические методы линейной и общей алгебры, так и некоторые новые методы доказательства, использующие связи между длиной алгебры и другими её числовыми характеристиками, такими как размерность алгебры и максимальная степень минимального многочлена элемента алгебры. При переходе от групповых алгебр к матричным используется теорема Машке и теорема Веддерберна-Артина.

## Теоретическая и практическая значимость

Приложения разрабатываемой теории возникают в следующем классе задач вычислительных методов теории матриц (см., например, [17], [18], [19]): пусть дана подалгебра в полной алгебре матриц $M_n(\mathbb{F})$ порядка $n$ над полем $\mathbb{F}$ (обычно полем комплексных или действительных чисел), заданная порождающим множеством $A_1, \ldots, A_k$, и требуется проверить, обладает ли данная алгебра, некоторым заданным свойством. При этом процедура проверки должна быть *рациональной*, т.е.

использующей конечное число арифметических операций с элементами матриц. Такие процедуры как правило включают в себя рациональную процедуру вычисления базиса алгебры; длина порождающего множества $A_1, \ldots, A_k$ ограничивает сверху число матриц, участвующих в рассматриваемых произведениях матриц, т.е. является мерой сложности этой процедуры. Также длина определяет сложность рациональной процедуры проверки, является ли некоторое множество системой порождающих для заданной алгебры.

Отметим, что в ряде вычислительных задач требуется оценить длину произвольного подмножества $\mathcal{S}'$ в алгебре $\mathcal{A}$, которое может порождать не всю алгебру, а ее собственную подалгебру $\mathcal{A}' \subset \mathcal{A}$. Или, найти такое число $M \in \mathbb{N}$, что для любой подалгебры $\mathcal{A}' \subseteq \mathcal{A}$ будет справедлива оценка $l(\mathcal{A}') \leq M$. В силу тривиальной оценки длины $l(\mathcal{A}') \leq \dim \mathcal{A}' - 1$, всегда можно положить $M = \dim \mathcal{A} - 1$. Однако, как показывает, например, оценка в теореме 1.2.4, тривиальная оценка может не быть точной.

Таким образом, вопросы, связанные с вычислением и оцениванием длин различных матричных подалгебр мотивированы приложениями и активно разрабатываются. Поэтому построение общей теории функции длины представляет не только самостоятельный теоретический интерес, но и является эффективным инструментом работы с различными классами вычислительных задач в прикладной и теоретической алгебре.

## Степень достоверности и апробация результатов

Результаты опубликованы в статьях:

- Guterman A., Khrystik M., Markova O.

  On the lengths of group algebras of finite abelian groups in the modular case,

  *Journal of Algebra and its Applications*, **21**:6 (2022), 2250117–2250130.

  (М.А.Хрыстиком доказано следствие 3.10.)

- Guterman A., Markova O., Khrystik M.

  On the lengths of group algebras of finite abelian groups in the semi-simple case,

*Journal of Algebra and its Applications*, **21**:7 (2022), 2250140–2250153.

(М.А.Хрыстиком доказаны следствия 3.8, 3.11 и теорема 3.16.)

- Khrystik M.A., Markova O.V.

  On the length of the group algebra of the dihedral group in the semi-simple case,

  *Communications in Algebra*, **50**:5 (2022), 2223–2232.

  (М.А.Хрыстиком доказаны теорема 1.15, леммы 3.5, 3.7, 3.9, 4.2 и 4.3.)

- Маркова О. В., Хрыстик М. А.

  Длина групповой алгебры группы диэдра порядка $2^k$,

  *Зап. научн. сем. ПОМИ*, **496** (2020), 169–181.

  (М.А.Хрыстиком доказаны леммы 2.10, 3.5 и теорема 3.7)

  English transl.:

  Markova O.V., Khrystik M.A., Length of the group algebra of the dihedral group of order $2^k$, Journal of Mathematical Sciences. (N. Y.), **255**:3 (2021), 324–331.

- Хрыстик М. А.

  Длина групповой алгебры прямого произведения циклической группы и циклической p-группы в модулярном случае,

  *Зап. научн. сем. ПОМИ*, **524** (2023), 166–176.

и представлены на конференциях:

- XXVI Международная конференция студентов, аспирантов и молодых ученых «Ломоносов-2019», Москва, Россия, с 8 по 12 апреля 2019 года (устная презентация на русском);

- Международная конференция, посвящённая 90-летию кафедры высшей алгебры механико-математического факультета МГУ «Кафедре высшей алгебры — 90 лет», Москва, Россия, с 28 по 31 мая 2019 года (устная презентация на русском);

- XXVII Международная научная конференция студентов, аспирантов и молодых ученых «Ломоносов-2020», Москва, Россия, с 10 по 27 ноября 2020 года (устный доклад в формате онлайн).

Автор выступал с докладами по результатам работы на следующих спецсеминарах:

- Научный семинар «Кольца, модули и матрицы», механико-математический факультет МГУ имени М. В. Ломоносова, 2020, 2021 (устные доклады);
- Научно-исследовательский семинар по алгебре, механико-математический факультет МГУ имени М. В. Ломоносова, 2023 (устный доклад);
- Научный семинар «Теория групп», механико-математический факультет МГУ имени М. В. Ломоносова, 2023 (устный доклад).

### Структура и объём работы

Диссертация состоит из введения, четырех глав, разбитых на параграфы, заключения, списка литературы и списка публикаций автора. Общий объем работы: 66 страниц. Список литературы включает 41 наименование.

## Содержание работы

**Введение** содержит информацию об актуальности рассматриваемой темы, краткую историю вопроса, изложение цели работы, методов и основных результатов.

**Глава 1**. В этой главе более подробно описываются история задачи исследования длин конечномерных ассоциативных алгебр, вводятся необходимые обозначения и определения, формулируются некоторые известные на момент написания работы результаты.

В разделе 1.1 вводятся основные определения и обозначения, используемые на протяжении всего текста.

Кольцо $\mathcal{A}$, являющееся также векторным пространством над полем $\mathbb{F}$, называется *алгеброй* над $\mathbb{F}$ или $\mathbb{F}$-*алгеброй*, если для любого $\lambda \in \mathbb{F}$ и любых $a, b \in \mathcal{A}$ выполняется равенство $\lambda(ab) = (\lambda a)b = a(\lambda b)$. Алгебра называется *конечномерной*, если соответствующее векторное пространство имеет конечную размерность над $\mathbb{F}$. Алгебра называется *конечно порожденной*, если в ней существует такое конечное подмножество $\mathcal{S} = \{a_1, \ldots, a_k\}$, называемое *системой порождающих*, что каждый элемент алгебры является линейной комбинацией конечного числа произведений элементов из $\mathcal{S}$, включая пустое произведение, равное единичному элементу (если он есть). Легко видеть, что любая конечномерная алгебра порождается своим базисом, т.е. является конечно порожденной.

**Обозначение** (1.1.7)**.** Обозначим через $\mathcal{L}_i(\mathcal{S})$ линейную оболочку слов из $\mathcal{S}^i$. Заметим, что $\mathcal{L}_0(\mathcal{S}) = \langle 1_{\mathcal{A}} \rangle = \mathbb{F}$ для алгебр с единицей, и $\mathcal{L}_0(\mathcal{S}) = 0$, иначе. Пусть также $\mathcal{L}(\mathcal{S}) = \bigcup\limits_{i=0}^{\infty} \mathcal{L}_i(\mathcal{S})$ обозначает линейную оболочку всех слов в алфавите $\{a_1, \ldots, a_k\}$.

**Определение** (1.1.9)**.** *Длиной системы порождающих* $\mathcal{S}$ алгебры $\mathcal{A}$ называется $l(\mathcal{S}) = \min\{k \in \mathbb{Z}_+ : \mathcal{L}_k(\mathcal{S}) = \mathcal{A}\}$.

**Определение** (1.1.11)**.** *Длиной алгебры* $\mathcal{A}$ называется $l(\mathcal{A}) = \max\{l(\mathcal{S}) : \mathcal{L}(\mathcal{S}) = \mathcal{A}\}$.

**Обозначение** (1.1.12)**.** Пусть $m(a)$ — степень минимального многочлена элемента $a$ алгебры $\mathcal{A}$. Тогда $m(\mathcal{A}) = \max\{m(a) : a \in \mathcal{A}\}$.

**Обозначение** (1.1.13)**.** Введём обозначения. $\mathbb{F}G$ или $\mathbb{F}[G]$ — групповая алгебра группы $G$ над полем $\mathbb{F}$, $M_n(\mathbb{F})$ — полная матричная алгебра над полем $\mathbb{F}$, $A_n(\mathbb{F}) = \bigoplus\limits_{i=1}^{n} M_2(\mathbb{F})$, $D_n(\mathbb{F})$ — алгебра диагональных матриц над полем $\mathbb{F}$, $E_{i,j}$ — матричная единица, $G_n$ — циклическая группа порядка $n$, $\mathcal{D}_n$ — диэдральная группа порядка $2n$, $S_n$ — симметрическая группа, $Q_8$ — группа кватернионов.

В разделе 1.2 рассматривается возникновение понятия функции длины алгебры, формулировка гипотезы Паза. Приводится обзор продвижений в направлении доказательства гипотезы, в том числе оценки Паза, Паппачены, Шитова.

**Гипотеза** (1.2.1)**.** Пусть $\mathbb{F}$ — произвольное поле. Тогда $l(M_n(\mathbb{F})) = 2n - 2$.

В разделе 1.3 фокус внимания смещается на групповые алгебры. Приводится краткий обзор на серию работ о длинах групповых алгебр.

**Глава 2**. В этой главе рассматриваются результаты изучения длин групповых алгебр абелевых групп. Для полноты повествования в тексте указаны основные результаты работ по теме длин групповых алгебр, в том числе те, которые не принадлежат автору. Такие результаты сопровождаются соответствующим комментарием, а их доказательства, как правило, опущены.

В разделе 2.1 рассматривается связь между длиной алгебры и её однопорождённостью. Формулируется утверждение о длине групповой алгебры для циклических групп.

**Утверждение** (2.1.1)**.** Пусть $\mathcal{A}$ — ассоциативная алгебра с единицей размерности $d$ над произвольным полем. Тогда $l(\mathcal{A}) \leq d - 1$, причём оценка превращается в равенство тогда и только тогда, когда алгебра $\mathcal{A}$ является однопорождённой, из чего автоматически следует, что она коммутативна.

**Утверждение** (2.1.2)**.** Пусть $G$ — циклическая группа порядка $n < \infty$. Тогда $l(\mathbb{F}G) = n - 1$.

В разделе 2.2 рассматривается случай групповых алгебр абелевых групп, когда характеристика поля не делит порядок группы (полупростой случай). Результаты данного раздела получены в совместной работе и не принадлежат автору, поэтому доказательства будут опущены. Однако техника работы с представлением групповой алгебры в виде прямой суммы конечных расширений поля, лёгшая в основу результатов в полупростом случае, будет рассмотрена на примерах групп малых порядков в главе 4.

**Теорема** (2.2.1)**.** Пусть $G$ — конечная абелева группа, $\mathrm{char}\,(\mathbb{F}) \nmid |G|$, $|\mathbb{F}| \geq |G|$. Тогда групповая алгебра $\mathbb{F}G$ является однопорождённой и, как следствие, $l(\mathbb{F}G) = |G| - 1$.

**Теорема** (2.2.2)**.** Пусть $G$ — конечная абелева группа, $q \leq |G| - 1$, $\exp(G)|(q-1)$. Тогда $l(\mathbb{F}_q G) = (q-1)[\log_q |G|] + [q^{\{\log_q |G|\}}] - 1$.

В разделе 2.3 рассматривается случай групповых алгебр абелевых групп, когда характеристика поля делит порядок группы (модулярный случай). В частности, вычисляется длины групповых алгебр для $p$-групп над полями характеристики $p > 0$. Результаты данного раздела получены в совместной работе и не принадлежат автору, поэтому доказательства будут опущены.

**Теорема** (2.3.1)**.** Пусть $\mathbb{F}$ — поле характеристики $p > 0$. Пусть $m \in \mathbb{N}$ и пусть $G$ — конечная абелева $p$-группа, которая содержит $a_i$ копий $G_{p^i}$ в своём разложении на примарные циклические, $a_1, \ldots, a_{m-1} \in \mathbb{Z}_+, a_m \in \mathbb{N}$, то есть,

$$G \cong \underbrace{G_p \times \cdots \times G_p}_{a_1 \text{ копий}} \times \cdots \times \underbrace{G_{p^m} \times \cdots \times G_{p^m}}_{a_m \text{ копий}}.$$

Тогда

$$l(\mathbb{F}G) = \sum_{i=1}^{m} a_i(p^i - 1).$$

Для остальных групп получены верхняя и нижняя оценки.

**Теорема** (2.3.2)**.** Пусть $\mathbb{F}$ — поле характеристики $p > 0$. Пусть $G$ — абелева группа порядка $|G| = p^t \cdot m$, $(m, p) = 1$ разлагается в прямое произведение $G \cong H \times P$, где $P$ — это $p$-группа, $|H| = m$. Тогда

$$l(\mathbb{F}P) + l(\mathbb{F}H) \leq l(\mathbb{F}G) \leq |H| \cdot (l(\mathbb{F}P) + 1) - 1.$$

Над достаточно большими совершенными полями удаётся точно вычислить значение длины групповой алгебры в случае, когда $p$-компонента в разложении группы — циклическая.

**Теорема** (2.3.4)**.** Пусть $m \in \mathbb{N}$, $\mathbb{F}$ — совершенное поле характеристики $p > 0$, $|\mathbb{F}| \geq m$ и $(m, p) = 1$. Рассмотрим конечную абелеву группу $G \cong H \times P$, где $P$ — циклическая $p$-группа и $|H| = m$. Тогда алгебра $\mathbb{F}G$ является однопорождённой и $l(\mathbb{F}G) = |G| - 1$.

В разделе 2.4 продолжается исследование групповых алгебр, для которых значение длины может быть точно вычислено. Основным результатом данного раз-

дела является вычисление длины групповой алгебры прямого произведения циклической группы и циклической $p$-группы над полем характеристики $p$.

**Теорема** (2.4.3)**.** Пусть $\mathbb{F}$ — поле характеристики $p > 0$, $p \nmid q$, $k \geq l$. Тогда

$$l(\mathbb{F}[G_{p^l} \times G_{p^k} \times G_q]) = p^k q + p^l - 2.$$

В разделе 2.5 теоремы 2.3.4 и 2.4.3 получают своё обобщение в виде следующей теоремы.

**Теорема** (2.5.1)**.** Пусть $\mathbb{F}$ — совершенное поле характеристики $p > 0$, $H$ — абелева группа порядка $q$, $|\mathbb{F}| \geq q$, $p \nmid q$, $k \geq l$. Тогда

$$l(\mathbb{F}[G_{p^l} \times G_{p^k} \times H]) = p^k q + p^l - 2.$$

**Глава 3**. В этой главе рассматриваются результаты изучения длин групповых алгебр диэдральных групп. Для изучения групповых алгебр диэдральных групп используются матричные представления, поэтому в главе также присутствуют результаты о длине матричных алгебр. Основным результатом главы является следующая теорема.

**Теорема** (3.0.1)**.** Пусть $\mathbb{F}$ — поле, такое что $\operatorname{char}\mathbb{F}$ не делит $2n$, $n \geq 3$. Тогда $l(\mathbb{F}\mathcal{D}_n) = n$.

В разделе 3.1 доказывается нижняя оценка длины в случае диэдральных групп.

**Лемма** (3.1.1)**.** Пусть $\mathcal{D}_n$ — группа диэдра порядка $2n$, $n \geq 3$, $\mathbb{F}$ — произвольное поле. Тогда $l(\mathbb{F}\mathcal{D}_n) \geq n$.

В разделе 3.2 доказываются результаты о длине матричных алгебр, интересные и сами по себе, которые будут использованы для доказательства основной теоремы главы.

**Лемма** (3.2.8)**.** Пусть $\mathcal{A}$ — конечномерная ассоциативная $\mathbb{F}$-алгебра, $\dim\mathcal{A} < 2l(\mathcal{A}) + 2$. Тогда

$$l(\mathcal{A} \oplus M_2(\mathbb{F})) \leq l(\mathcal{A}) + 2.$$

Напомним, что в этой главе $A_n(\mathbb{F}) = \bigoplus_{i=1}^{n} M_2(\mathbb{F})$, $D_n(\mathbb{F}) = \bigoplus_{i=1}^{n} \mathbb{F}$.

**Лемма** (3.2.9)**.** Пусть $|\mathbb{F}| > n$. Тогда $l(A_n(\mathbb{F})) = 2n$.

**Лемма** (3.2.11)**.** Пусть $\mathcal{A}$ — коммутативная алгебра. Пусть $|\mathbb{F}| > n$. Тогда

$$l(A_n(\mathbb{F}) \oplus \mathcal{A}) \leq \max\{2n+2, l(\mathcal{A})\}.$$

В разделе 3.3 результат леммы 3.2.11 обобщается на случай произвольных полей в случае $n = 2$, а также доказывается верхняя оценка длины алгебры, которая будет использована при рассмотрении групп малых порядков в главе 4.

**Лемма** (3.3.1)**.** Пусть $\mathcal{A}$ — конечномерная ассоциативная алгебра, $\dim \mathcal{A} \leq m(\mathcal{A})+4$, $m(\mathcal{A}) \geq 3$. Тогда $l(\mathcal{A}) \leq m(\mathcal{A})$.

**Теорема** (3.3.2)**.** $l(M_2(\mathbb{F}) \oplus M_2(\mathbb{F})) = 4$.

Раздел 3.4 посвящён доказательству основной теоремы главы. Для этого рассматривается матричное представление групповых алгебр диэдральных групп.

**Утверждение** (3.4.1)**.** Пусть $\mathbb{F}$ — алгебраически замкнутое поле и $\operatorname{char}\mathbb{F}$ не делит порядок группы. Тогда

$$\mathbb{F}\mathcal{D}_{2n+1} \cong A_n(\mathbb{F}) \oplus D_2(\mathbb{F}),$$

$$\mathbb{F}\mathcal{D}_{2n+2} \cong A_n(\mathbb{F}) \oplus D_4(\mathbb{F}).$$

Далее с помощью лемм, доказанных в разделе 3.2, доказываются следующие результаты о длинах матричных алгебр.

**Лемма** (3.4.2)**.** Пусть $\mathbb{F}$ — алгебраически замкнутое поле, такое что $\operatorname{char}\mathbb{F}$ не делит $4n+2$. Тогда

$$l(A_n(\mathbb{F}) \oplus D_2(\mathbb{F})) = 2n+1.$$

**Лемма** (3.4.3)**.** Пусть $\mathbb{F}$ — алгебраически замкнутое поле, такое что $\operatorname{char}\mathbb{F}$ не делит $4n+4$. Тогда

$$l(A_n(\mathbb{F}) \oplus D_4(\mathbb{F})) = 2n+2.$$

Из доказанных в этом разделе утверждений и того факта, что длина не уменьшается при переходе к расширению поля следует основной результат главы.

В разделе 3.5 основной результат главы обобщается на модулярный случай для диэдральных 2-групп.

**Теорема** (3.5.1)**.** Пусть $\operatorname{char}\mathbb{F} = 2$, $k \geq 2$. Тогда $l(\mathbb{F}\mathcal{D}_{2^k}) = 2^k$.

Доказательство этого результата не принадлежит автору, поэтому опущено, однако в главе 4 подробно рассмотрен частный случай этой теоремы при $k = 2$.

**Глава 4**. В этой главе рассматриваются результаты изучения длин групповых алгебр групп, порядок которых не превышает 9. Для этих групп длины соответствующих групповых алгебр вычислены над произвольными полями.

В разделе 4.1, посвящённом абелевым группам, рассматриваются группы $G_2 \times G_2$, $G_2 \times G_2 \times G_2$, $G_2 \times G_4$ и $G_3 \times G_3$, так как случай циклических групп тривиален. Также в этом разделе представлен сюжет о коммутативных групповых алгебрах над полями нулевой характеристики, где рассматривается ещё один подход к изучению длин групповых алгебр с помощью матричных представлений.

**Теорема** (4.1.8)**.** Коммутативные групповые алгебры над полями нулевой характеристики имеют длину $n - 1$, где $n$ – порядок группы.

Для краткости и наглядности представим полученные в разделе результаты в виде таблицы, где на пересечении строки с группой и столбца с полем будет стоять длина соответствующей групповой алгебры.

| Группа\Поле | $\mathbb{F}_2$ | $\mathbb{F}_3$ | $\mathbb{F}_4$ | $\mathbb{F}_5$ | $\mathbb{F}_7$ | $\mathbb{F}_8$ | $\lvert\mathbb{F}\rvert \geq 9$, $\operatorname{char}\mathbb{F} \nmid \lvert G\rvert$ | $\lvert\mathbb{F}\rvert \geq 9$, $\operatorname{char}\mathbb{F} \mid \lvert G\rvert$ |
|---|---|---|---|---|---|---|---|---|
| $G_1$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - |
| $G_2$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $G_3$ | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| $G_4$ | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| $G_2 \times G_2$ | 2 | 2 | 2 | 3 | 3 | 2 | 3 | 2 |
| $G_5$ | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| $G_6$ | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| $G_7$ | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| $G_8$ | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| $G_2 \times G_2 \times G_2$ | 3 | 3 | 3 | 4 | 6 | 3 | 7 | 3 |
| $G_2 \times G_4$ | 4 | 6 | 4 | 4 | 7 | 4 | 7 | 4 |
| $G_9$ | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| $G_3 \times G_3$ | 4 | 4 | 4 | 8 | 6 | 8 | 8 | 4 |

В частности, на этой таблице можно наглядно увидеть отсутствие монотонности функции длины, как по порядку группы, так и по порядку поля, даже если говорить только о нециклических группах в полупростом случае.

В разделе 4.2 приведены результаты совместных статей А.Э. Гутермана и О.В. Марковой о случаях групп $S_3$ и $Q_8$.

**Теорема** (4.2.1)**.** Пусть $\mathbb{F}$ — произвольное поле. Тогда $l(\mathbb{F}S_3) = 3$.

**Теорема** (4.2.2)**.** Пусть $\mathbb{F}$ — произвольное поле. Тогда

1. $l(\mathbb{F}Q_8) = 4$, если $\operatorname{char}\mathbb{F} \neq 2$ и в поле $\mathbb{F}$ существуют элементы $\alpha$, $\beta$, такие, что $\alpha^2 + \beta^2 = -1$;

2. $l(\mathbb{F}Q_8) = 3$, в остальных случаях.

Завершается раздел рассмотрением диэдральной группы порядка 8. Из теоремы 3.0.1 следует, что в полупростом случае $l(\mathbb{F}\mathcal{D}_4) = 4$. Для вычисления длины в случае диэдральной группы $\mathcal{D}_4$ над полем характеристики 2 вычисляется максимальная степень минимального многочлена элемента алгебры и применяется лемма 3.3.1.

**Лемма** (4.2.7)**.** Пусть $\operatorname{char}\mathbb{F} = 2$. Тогда $m(\mathbb{F}\mathcal{D}_4) = 4$.

**Теорема** (4.2.8)**.** Пусть $\operatorname{char}\mathbb{F} = 2$. Тогда $l(\mathbb{F}\mathcal{D}_4) = 4$.

## Благодарность

Автор выражает глубокую благодарность своему научному руководителю кандидату физико-математических наук, доценту Марковой Ольге Викторовне за постановку задач и постоянное внимание к работе, заведующему кафедры высшей алгебры и всем сотрудникам кафедры высшей алгебры за тёплую доброжелательную атмосферу.

Глава 1

# История задачи: возникновение понятия функции длины

Цель главы — ввести необходимые определения, сформулировать уже известные результаты о длинах ассоциативных алгебр и обозначить мотивацию исследуемых в работе задач.

## 1.1 Обозначения

Кольцо $\mathcal{A}$, являющееся также векторным пространством над полем $\mathbb{F}$, называется *алгеброй* над $\mathbb{F}$ или $\mathbb{F}$-*алгеброй*, если для любого $\lambda \in \mathbb{F}$ и любых $a, b \in \mathcal{A}$ выполняется равенство $\lambda(ab) = (\lambda a)b = a(\lambda b)$. Алгебра называется *конечномерной*, если соответствующее векторное пространство имеет конечную размерность над $\mathbb{F}$. Алгебра называется *конечно порожденной*, если в ней существует такое конечное подмножество $\mathcal{S} = \{a_1, \ldots, a_k\}$, называемое *системой порождающих*, что каждый элемент алгебры является линейной комбинацией конечного числа произведений элементов из $\mathcal{S}$, включая пустое произведение, равное единичному элементу (если он есть). Легко видеть, что любая конечномерная алгебра порождается своим базисом, т.е. является конечно порожденной.

**Обозначение 1.1.1.** Через $\langle S \rangle$ будем обозначать линейную оболочку (множество всех конечных линейных комбинаций с коэффициентами из $\mathbb{F}$) подмножества $S$ некоторого векторного пространства над $\mathbb{F}$.

**Обозначение 1.1.2.** Пусть $B = \{b_1, \ldots, b_m\}$ — непустое конечное множество (алфавит). Конечные последовательности букв из $B$ назовем словами. Пусть $B^*$ обозначает множество всех слов в алфавите $B$, $F_B$ — свободную полугруппу над алфавитом $B$, т.е. $B^*$ с операцией конкатенации.

**Определение 1.1.3.** *Длина* слова $b_{i_1} \ldots b_{i_t}$, где $b_{i_j} \in B$, равна $t$. Будем считать 1 (пустое слово) словом от элементов $B$ *длины* 0.

**Обозначение 1.1.4.** Пусть $B^i$ обозначает множество всех слов в алфавите $B$ длины не большей $i$, $i \geqslant 0$. Тогда через $B^{=i}$ обозначим множество всех слов в алфавите $B$ длины равной $i$, $i \geqslant 1$.

**Замечание 1.1.5.** Произведения элементов из порождающего множества $\mathcal{S}$ можно рассматривать как образы элементов свободной полугруппы $F_{\mathcal{S}}$ при естественном гомоморфизме, и их также можно называть словами от образующих и использовать естественные обозначения $\mathcal{S}^i$ и $S^{=i}$.

**Обозначение 1.1.6.** Положим $\mathcal{S}^0 = \{1_{\mathcal{A}}\}$, если алгебра $\mathcal{A}$ содержит единицу $1_{\mathcal{A}}$, иначе, положим $\mathcal{S}^0 = \emptyset$.

**Обозначение 1.1.7.** Обозначим через $\mathcal{L}_i(\mathcal{S})$ линейную оболочку слов из $\mathcal{S}^i$. Заметим, что $\mathcal{L}_0(\mathcal{S}) = \langle 1_{\mathcal{A}} \rangle = \mathbb{F}$ для алгебр с единицей, и $\mathcal{L}_0(\mathcal{S}) = 0$, иначе. Пусть также $\mathcal{L}(\mathcal{S}) = \bigcup\limits_{i=0}^{\infty} \mathcal{L}_i(\mathcal{S})$ обозначает линейную оболочку всех слов в алфавите $\{a_1, \ldots, a_k\}$.

**Замечание 1.1.8.** Так как $\mathcal{S}$ является системой порождающих для $\mathcal{A}$, то $\mathcal{A} = \mathcal{L}(\mathcal{S})$. Из определения $\mathcal{S}^i$ для $i, j > 0$ получаем, что

$$\mathcal{S}^{i+j} = \mathcal{S}^i \mathcal{S}^j \cup \mathcal{S}^1, \tag{1}$$

$$\mathcal{L}_{i+j}(\mathcal{S}) = \langle \mathcal{L}_i(\mathcal{S}) \mathcal{L}_j(\mathcal{S}) + \mathcal{L}_1(\mathcal{S}) \rangle, \tag{2}$$

и

$$\mathcal{L}_0(\mathcal{S}) \subseteq \mathcal{L}_1(\mathcal{S}) \subseteq \ldots \subseteq \mathcal{L}_h(\mathcal{S}) \subseteq \ldots \subseteq \mathcal{L}(\mathcal{S}) = \mathcal{A}. \tag{3}$$

**В дальнейшем, все рассматриваемые алгебры имеют конечную размерность.**

**Определение 1.1.9.** *Длиной системы порождающих* $\mathcal{S}$ алгебры $\mathcal{A}$ называется $l(\mathcal{S}) = \min\{k \in \mathbb{Z}_+ : \mathcal{L}_k(\mathcal{S}) = \mathcal{A}\}$.

**Замечание 1.1.10.** В случае алгебр с единицей равенства (1) и (2) можно упростить

$$\mathcal{S}^{i+j} = \mathcal{S}^i \mathcal{S}^j, \tag{4}$$

$$\mathcal{L}_{i+j}(\mathcal{S}) = \langle \mathcal{L}_i(\mathcal{S})\mathcal{L}_j(\mathcal{S}) \rangle. \tag{5}$$

**Определение 1.1.11.** *Длиной алгебры* $\mathcal{A}$ называется $l(\mathcal{A}) = \max\{l(\mathcal{S}) : \mathcal{L}(\mathcal{S}) = \mathcal{A}\}$.

**Обозначение 1.1.12.** Пусть $m(a)$ — степень минимального многочлена элемента $a$ алгебры $\mathcal{A}$. Тогда $m(\mathcal{A}) = \max\{m(a) : a \in \mathcal{A}\}$.

**Обозначение 1.1.13.** Введём обозначения. $\mathbb{F}G$ или $\mathbb{F}[G]$ — групповая алгебра группы $G$ над полем $\mathbb{F}$, $M_n(\mathbb{F})$ — полная матричная алгебра над полем $\mathbb{F}$, $A_n(\mathbb{F}) = \bigoplus_{i=1}^{n} M_2(\mathbb{F})$, $D_n(\mathbb{F})$ — алгебра диагональных матриц над полем $\mathbb{F}$, $E_{i,j}$ — матричная единица, $G_n$ — циклическая группа порядка $n$, $\mathcal{D}_n$ — диэдральная группа порядка $2n$, $S_n$ — симметрическая группа, $Q_8$ — группа кватернионов.

**Обозначение 1.1.14.** Пусть $a$ — элемент алгебры $\mathcal{A} = \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus \cdots \oplus \mathcal{A}_n$. Тогда обозначим $\pi_i(a)$ проекцию $a$ на $\mathcal{A}_i$.

## 1.2 Возникновение понятия длины и гипотеза Паза

Задача вычисления длины впервые возникла в работах Спенсера и Ривлина 1959–60гг. [4], [5] для полной алгебры матриц порядка 3 в связи с возможным применением в механике сплошных сред. В общей формулировке проблема вычисления длины полной алгебры матриц $M_n(\mathbb{F})$ как функции порядка матриц была поставлена Пазом в 1984 году в работе [7] и до сих пор является открытой. Существует гипотеза, состоящая в том, что зависимость между длиной и порядком матриц линейная и задается следующей формулой:

**Гипотеза 1.2.1** ([7])**.** *Пусть* $\mathbb{F}$ *— произвольное поле. Тогда* $l(M_n(\mathbb{F})) = 2n - 2$.

Известно, что эта гипотеза верна при $n = 2, 3, 4$ (см. [7, пример]). Однако все существующие верхние оценки длины алгебры матриц не являются линейными.

Оценка, полученная в работе Паза, является квадратичной относительно порядка матриц.

**Теорема 1.2.2** ([7, теорема 1, замечание 1]). *Пусть* $\mathbb{F}$ *— произвольное поле. Тогда*

$$l(M_n(\mathbb{F})) \leq \left\lceil \frac{n^2+2}{3} \right\rceil,$$

*где* $\lceil . \rceil$ *обозначает наименьшее целое число, большее или равное данному.*

В работе 1997 г. [6] Паппачена предложил обобщение метода комбинаторного подсчета линейно независимых слов, использованного Пазом, и с его помощью получил верхнюю оценку длины произвольной ассоциативной алгебры $\mathcal{A}$ в виде функции двух ее инвариантов: размерности и $m(\mathcal{A})$ — максимальной степени минимального многочлена элементов алгебры.

**Теорема 1.2.3** ([6, теорема 3.1]). *Пусть* $\mathbb{F}$ *— произвольное поле и пусть*

$$f(d,m) = m\sqrt{\frac{2d}{m-1} + \frac{1}{4}} + \frac{m}{2} - 2.$$

*Тогда* $l(\mathcal{A}) < f(\dim \mathcal{A}, m(\mathcal{A}))$.

Для матричной алгебры эта теорема дает верхнюю оценку асимптотики $O(n^{3/2})$:

**Теорема 1.2.4** ([6, следствие 3.2]). *Пусть* $\mathbb{F}$ *— произвольное поле. Тогда*

$$l(M_n(\mathbb{F})) < n\sqrt{\frac{2n^2}{n-1} + \frac{1}{4}} + \frac{n}{2} - 2.$$

Некоторые системы порождающих, длины которых не превосходят $2n-2$, рассмотрены в работе Константайна и Дарнолла [16] и в работах Лонгстаффа и Розенталя [13], [14]. Пример системы порождающих длины $2n-2$ в случае, когда основное поле является алгебраически замкнутым характеристики 0, построен в работе Лаффи [15, раздел 4].

Асимптотически лучшая на данный момент оценка длины полной матричной алгебры получена Шитовым в работе [30] и не является линейной:

**Теорема 1.2.5** ([30, теорема 3]). *Для всех множеств* $\mathcal{S} \subset M_n(\mathbb{F})$ *выполнена оценка*

$$l(\mathcal{S}) \leq 2n\log_2 n + 4n - 4.$$

Хотя в общем виде гипотеза Паза всё ещё остается открытой, некоторые линейные оценки были доказаны при дополнительных ограничениях на системы порождающих. В частности, Гутерманом, Лаффи, Марковой и Шмигоц [31] было установлено, что гипотеза Паза верна для следующего широкого класса порождающих множеств.

**Определение 1.2.6.** Матрица $C \in M_n(\mathbb{F})$ называется *циклической*, если её минимальный многочлен совпадает с характеристическим.

**Теорема 1.2.7** ([31, теорема 2.4])**.** *Пусть $\mathbb{F}$ — произвольное поле. Если система порождающих $\mathcal{S}$ матричной алгебры $M_n(\mathbb{F})$ содержит циклическую матрицу, то $l(\mathcal{S}) \leq 2n - 2$.*

Основные алгебраические свойства функции длины были изучены О.В. Марковой в работе [2].

## 1.3 Исследования длин групповых алгебр

Отдельный интерес представляет вопрос вычисления длины групповых алгебр. Ввиду наличия их матричных представлений, решение этого вопроса тесно связано и с решением проблемы Паза.

Результаты исследований, упоминаемых в этой секции, будут подробно рассмотрены далее, поэтому здесь мы лишь обозначим их.

Для групповых алгебр групп малых порядков удаётся вычислить длину точно над произвольными полями, так для группы подстановок $S_3$, группы Клейна $V_4$ и группы кватернионов $Q_8$, значения длины найдены в работах Гутермана и Марковой [25, 26].

Систематическому изучению общей задачи нахождения длины групповых алгебр конечных абелевых групп посвящены работы [38, 37], в которых автор присоединился к научному коллективу Гутермана и Марковой. В работе [37] для получения оценки длины групповых алгебр использованы методы теории полей, теории колец и оценка длины коммутативных алгебр (см. [32, теорема 3.11]). В той же работе вычисление длины групповой алгебры абелевой $p$-группы сведено к вычислению длины фактор-алгебры по радикалу Джекобсона и индекса нильпотентности

радикала (см. [33, теорема 1, следствие 1]). Вычисление индекса нильпотентности радикала Джекобсона групповой алгебры основано на *теории Дженнингса* (см. [28], [34, Глава 11, §1]).

Аналогичное исследование всех неабелевых групп представляется слишком трудным ввиду разнообразия их структуры. Поэтому исследование функции длины продолжается отдельно для семейств классических неабелевых групп. Так, в работе [39] исследованы длины групповых алгебр диэдральных групп, вычислена длина в полупростом случае, которая для группы симметрий правильного $n$-угольника равна $n$. Эта серия групп в полупростом случае является естественным следующим шагом после абелевого случая. Действительно, для групповых алгебр абелевых групп в разложении в прямую сумму матричных алгебр все слагаемые одномерны, в то время как размеры матричных алгебр в разложении в прямую сумму групповых алгебр диэдральных групп не превышают двух. В работе [40] исследованы длины групповых алгебр диэдральных групп и вычислена их длина в модулярном случае, в ограничении, что рассматриваемые группы являются 2-группами.

# Глава 2

# Длины групповых алгебр абелевых групп

Результаты, представленные в этой главе, опубликованы в цикле статей [38, 37, 27, 41] совместно с А.Э. Гутерманом и О.В. Марковой. Для полноты повествования в тексте указаны основные результаты работ, в том числе те, которые не принадлежат автору. Такие результаты сопровождаются соответствующим комментарием, а их доказательства, как правило, опущены.

## 2.1 Циклические группы

Размерность групповой алгебры $\mathbb{F}G$ равна $|G|$. Так как $\dim \mathcal{L}_0(\mathcal{S}) = 1$ и размерность в цепочке подпространств 3 должна увеличиваться на каждом шаге хотя бы на единицу до стабилизации, заведомо $\dim \mathcal{L}_{|G|-1}(\mathcal{S}) = |G|$, то есть $l(\mathbb{F}G) \leq |G| - 1$. Для некоммутативных алгебр данную тривиальную оценку можно улучшить, так как некоммутативная алгебра не может быть однопорождённой, то есть $\dim \mathcal{L}_1(\mathcal{S}) \geq 3$. Таким образом, в данном случае $\dim \mathcal{L}_{|G|-2}(\mathcal{S}) = |G|$, то есть $l(\mathbb{F}G) \leq |G| - 2$. Следовательно, если алгебра имеет максимальную длину $|G| - 1$, то она является однопорождённой. Верно и обратное. Если алгебра $\mathbb{F}G$ порождается некоторым своим элементом $u$, то мы можем взять в качестве $\mathcal{S}$ этот элемент. В таком случае для того, чтобы породить алгебру, нам понадобятся все степени $u$ от нулевой до степени $|G|-1$. Таким образом, максимальность длины равносильна однопорождённости алгебры, из чего следует, что длина групповой алгебры циклической группы всегда имеет максимальную длину $|G| - 1$ независимо от поля коэффициентов. Сформулируем результаты этих рассуждений в виде утверждений.

**Утверждение 2.1.1.** *Пусть $\mathcal{A}$ — ассоциативная алгебра с единицей размерности $d$ над произвольным полем. Тогда $l(\mathcal{A}) \leq d-1$, причём оценка превращается*

*в равенство тогда и только тогда, когда алгебра $\mathcal{A}$ является однопорождённой, из чего автоматически следует, что она коммутативна.*

**Утверждение 2.1.2.** *Пусть $G$ — циклическая группа порядка $n < \infty$. Тогда $l(\mathbb{F}G) = n - 1$.*

## 2.2 Полупростой случай

В случае, когда группа $G$ не является циклической, задача вычисления длины становится весьма нетривиальной.

Результаты данной секции получены в совместной работе и не принадлежат автору, поэтому доказательства будут опущены. Однако техника работы с представлением групповой алгебры в виде прямой суммы конечных расширений поля, лёгшая в основу результатов в полупростом случае, будет рассмотрена на примерах групп малых порядков в главе 4.

В данной секции рассматривается полупростой случай, то есть групповые алгебры $\mathbb{F}G$, для которых характеристика поля $\mathbb{F}$ не делит порядок группы $G$. В этом случае для алгебры $\mathbb{F}G$ выполнены условия теоремы Машке. Тогда рассматриваемая алгебра раскладывается в прямую сумму конечных расширений поля $\mathbb{F}$. При взгляде на групповые алгебры с этой точки зрения удалось добиться значительных результатов, которые представлены в работе [38]. Например, оказалось, что для достаточно больших полей, в частности бесконечных, групповая алгебра является однопорождённой даже если сама группа $G$ не циклическая.

**Теорема 2.2.1.** *Пусть $G$ — конечная абелева группа,* $\mathrm{char}\,(\mathbb{F}) \nmid |G|$, $|\mathbb{F}| \geq |G|$. *Тогда групповая алгебра $\mathbb{F}G$ является однопорождённой и, как следствие, $l(\mathbb{F}G) = |G| - 1$.*

В случае малых полей удалось вычислить длину при определённом условии на экспоненту группы. Напомним, что экспонентой конечной группы $G$ называется наименьшее общее кратное порядков всех элементов группы $G$ и обозначается $\exp(G)$.

**Теорема 2.2.2.** *Пусть $G$ — конечная абелева группа, $q \leq |G| - 1$,* $\exp(G)|(q-1)$. *Тогда $l(\mathbb{F}_q G) = (q-1)[\log_q |G|] + [q^{\{\log_q |G|\}}] - 1$.*

Из последней теоремы легко следует результат о длине элементарной 2-группы порядка $2^k$. Действительно, для такой группы $\exp(G) = 2$ и при любом нечётном $q \leq 2^k - 1$ условие $\exp(G)|(q-1)$ выполняется. Таким образом, получено

**Следствие 2.2.3.** *Пусть* $G = \underbrace{G_2 \times \cdots \times G_2}_{k \text{ times}}$, $k \geq 2$, $q \leq 2^k - 1$ *нечётно. Тогда* $l(\mathbb{F}_q G) = (q-1)[k \log_q 2] + [q^{\{k \log_q 2\}}] - 1$.

Таким образом, для достаточно больших полей получен полный ответ. В случае малых полей явные формулы для вычисления длины получены при дополнительных ограничениях. Тем не менее для некоторых групп удаётся вычислить длину групповой алгебры над произвольным полем, даже если она не попадает ни под одно из представленных в этой секции общих утверждений. Примеры подобных вычислений будут представлены в главе 4.

## 2.3 Модулярный случай. p-группы

В данной секции рассматривается модулярный случай, то есть групповые алгебры $\mathbb{F}G$, для которых характеристика поля $\mathbb{F}$ делит порядок группы $G$.

Результаты данной секции получены в совместной работе и не принадлежат автору, поэтому доказательства будут опущены.

В работе [37] для получения оценки длины групповых алгебр использованы методы теории полей, теории колец и оценка длины коммутативных алгебр (теорема 2.4.8 в данной работе). В той же работе вычисление длины групповой алгебры абелевой $p$-группы сведено к вычислению длины фактор-алгебры по радикалу Джекобсона и индекса нильпотентности радикала (см. [33, теорема 1, следствие 1]). Вычисление индекса нильпотентности радикала Джекобсона групповой алгебры основано на *теории Дженнингса* (см. [28], [34, Глава 11, §1]).

**Теорема 2.3.1.** *Пусть* $\mathbb{F}$ *— поле характеристики* $p > 0$. *Пусть* $m \in \mathbb{N}$ *и пусть* $G$ *— конечная абелева* $p$*-группа, которая содержит* $a_i$ *копий* $G_{p^i}$ *в своём разло-*

*жении на примарные циклические,* $a_1, \ldots, a_{m-1} \in \mathbb{Z}_+, a_m \in \mathbb{N}$, *то есть,*

$$G \cong \underbrace{G_p \times \cdots \times G_p}_{a_1 \text{ копий}} \times \cdots \times \underbrace{G_{p^m} \times \cdots \times G_{p^m}}_{a_m \text{ копий}}.$$

*Тогда*

$$l(\mathbb{F}G) = \sum_{i=1}^{m} a_i(p^i - 1).$$

**Теорема 2.3.2.** *Пусть* $\mathbb{F}$ *— поле характеристики* $p > 0$. *Пусть* $G$ *— абелева группа порядка* $|G| = p^t \cdot m$, $(m, p) = 1$ *разлагается в прямое произведение* $G \cong H \times P$, *где* $P$ *— это* $p$*-группа,* $|H| = m$. *Тогда*

$$l(\mathbb{F}P) + l(\mathbb{F}H) \leq l(\mathbb{F}G) \leq |H| \cdot (l(\mathbb{F}P) + 1) - 1.$$

**Определение 2.3.3.** Поле $\mathbb{F}$ называется *совершенным*, если любой неприводимый многочлен над $\mathbb{F}$ имеет различные корни в алгебраическом замыкании $\mathbb{F}$.

Отметим, что совершенными полями являются, в частности, все поля характеристики ноль, все конечные поля, все алгебраически замкнутые поля.

**Теорема 2.3.4.** *Пусть* $m \in \mathbb{N}$, $\mathbb{F}$ *— совершенное поле характеристики* $p > 0$, $|\mathbb{F}| \geq m$ *и* $(m, p) = 1$. *Рассмотрим конечную абелеву группу* $G \cong H \times P$, *где* $P$ *— циклическая* $p$*-группа и* $|H| = m$. *Тогда алгебра* $\mathbb{F}G$ *является однопорождённой и* $l(\mathbb{F}G) = |G| - 1$.

Таким образом, в модулярном случае получен точный ответ для $p$-групп над произвольным полем и для прямого произведения циклической $p$-группы и абелевой группы, порядок которой не кратен $p$, над достаточно большими совершенными полями характеристики $p > 0$. Для остальных же групп получены верхняя и нижняя оценки.

## 2.4 Модулярный случай. Прямое произведение циклической группы и циклической p-группы

В работе [37] вычислена длина групповой алгебры $\mathbb{F}_3[G_2 \times G_3 \times G_3]$.

**Теорема 2.4.1.** $l(\mathbb{F}_3[G_2 \times G_3 \times G_3]) = 7$.

Затем этот результат был обобщён О.В. Марковой в работе [27].

**Теорема 2.4.2** ([27, теорема 2.14])**.** *Пусть* $\mathbb{F}$ *— поле характеристики* $p > 2$*. Тогда*

$$l(\mathbb{F}[G_2 \times G_p \times G_p]) = 3p - 2.$$

Затем этот результат был обобщён автором в работе [41], где была вычислена длина групповой алгебры прямого произведения циклической группы и циклической $p$-группы.

Пусть $G$ есть прямое произведение циклической группы и циклической $p$-группы, то есть $G = G_q \times G_{p^l}$, где $p$ — простое. Тогда мы можем выделить циклическую $p$-группу из $G_q$ прямым множителем. Следовательно, можем считать, что $G = G_{p^l} \times G_{p^k} \times G_q$, $p \nmid q$.

**Теорема 2.4.3.** *Пусть* $\mathbb{F}$ *— поле характеристики* $p > 0$*,* $p \nmid q$*,* $k \geq l$*. Тогда*

$$l(\mathbb{F}[G_{p^l} \times G_{p^k} \times G_q]) = p^k q + p^l - 2.$$

Приведём доказательство последней теоремы. Начнём с нижней оценки.

Пусть $G$ — конечная абелева группа, $s$ — количество различных простых делителей порядка группы $G$, $t_i$ — количество циклических $p_i$-групп в разложении $G$ на примарные циклические группы. Обозначим за $t$ максимум $t_i$ по всем $p_i \mid |G|$. Тогда группу $G$ можно представить в следующем виде:

$$G \cong G_{p_1^{k_{11}}} \times \cdots \times G_{p_1^{k_{1t}}} \times G_{p_2^{k_{21}}} \times \cdots \times G_{p_2^{k_{2t}}} \times \cdots \times G_{p_s^{k_{s1}}} \cdots \times G_{p_s^{k_{st}}},$$

где $k_{ij} = 0$ при $j > t_i$. Для группы $G$, представленной в подобном виде, сформулируем нижнюю оценку длины соответствующей групповой алгебры.

**Лемма 2.4.4.** *Пусть* $\mathbb{F}$ *— произвольное поле,* $G$ *— конечная абелева группа. Представим группу* $G$ *в следующем виде:*

$$G \cong G_{p_1^{k_{11}}} \times \cdots \times G_{p_1^{k_{1t}}} \times G_{p_2^{k_{21}}} \times \cdots \times G_{p_2^{k_{2t}}} \times \cdots \times G_{p_s^{k_{s1}}} \cdots \times G_{p_s^{k_{st}}}, \qquad (6)$$

*где $p_i$ — различные простые, $k_{ij} \leq k_{iq}$ при $j > q$, быть может, некоторые $k_{ij}$ равны нулю. Тогда*

$$l(\mathbb{F}G) \geq p_1^{k_{11}} p_2^{k_{21}} \cdots p_n^{k_{n1}} + p_1^{k_{12}} p_2^{k_{22}} \cdots p_n^{k_{n2}} + \cdots + p_1^{k_{1t}} p_2^{k_{2t}} \cdots p_n^{k_{nt}} - t.$$

*Доказательство.* Так как $p_i$ в разложении 6 различны, мы можем представить $G$ в виде разложения на циклические (не обязательно примарные), перегрупперовав примарные множители в разложении 6.

$$G \cong H_1 \times H_2 \times \cdots \times H_t, \tag{7}$$

где $G_j = G_{p_1^{k_{1j}}} \times G_{p_2^{k_{2j}}} \times \cdots \times G_{p_n^{k_{nj}}}$ — циклическая группа порядка $p_1^{k_{1j}} p_2^{k_{2j}} \cdots p_n^{k_{nj}}$. В соответствии с разложением 7 группы $G$ в прямое произведение циклических групп будем представлять элементы $G$ в виде $(g_1, \ldots, g_t)$, где $g_j \in H_j$.

Рассмотрим систему порождающих $\mathcal{S} = \{a_1, \ldots, a_t\}$, где $a_1 = (1, 0, \ldots, 0)$, $a_2 = (0, 1, 0, \ldots, 0), \ldots,$ $a_t = (0, \ldots, 0, 1)$. Заметим, что

$$(-1, -1, \ldots, -1) = a_1^{|H_1|-1} a_2^{|H_2|-1} \cdots a_t^{|H_t|-1}$$

и данный элемент алгебры, очевидно, не получить словами меньшей длины. Следовательно,

$$l(\mathbb{F}G) \geq l(\mathcal{S}) \geq \sum_{j=1}^{t} (|H_j| - 1) = \sum_{j=1}^{t} (p_1^{k_{1j}} p_2^{k_{2j}} \cdots p_n^{k_{nj}}) - t.$$

□

**Замечание 2.4.5.** Вообще говоря, лемма 2.4.4 верна и без условия $k_{ij} \leq k_{iq}$ при $j > q$. Однако нетрудно убедиться, что именно при такой группировке примарных циклических групп нижняя оценка будет принимать максимальное значение.

**Замечание 2.4.6.** При применении леммы 2.4.4 к группе $G = G_2 \times G_p \times G_p$ получаем оценку $l(\mathbb{F}G) \geq 3p-2$. Согласно теореме 2.4.2 $l(\mathbb{F}_p G) = 3p-2$. Следовательно, доказанная оценка точна.

Применяя оценку из леммы 2.4.4 к рассматриваемой группе, получаем непосредственное

**Следствие 2.4.7.** *Пусть $\mathbb{F}$ — произвольное поле, $G = G_{p^l} \times G_{p^k} \times G_q$, $p$ — простое, $p \nmid q$, $k \geq l$. Тогда $l(\mathbb{F}G) \geq p^k q + p^l - 2$.*

Для доказательства верхней оценки мы воспользуемся верхней оценкой длины для коммутативных алгебр.

**Теорема 2.4.8** ([32, теорема 3.11])**.** *Пусть $\mathbb{F}$ — произвольное поле. Пусть $\mathcal{A}$ — ассоциативная конечномерная коммутативная $\mathbb{F}$-алгебра с единицей. Пусть*

$$g(d,m) = \begin{cases} (m-1)[\log_m d] + [m^{\{\log_m d\}}] - 1 \text{ при } m \geq 2; \\ 0 \text{ при } m = 1. \end{cases}$$

*Тогда $l(\mathcal{A}) \leq g(\dim \mathcal{A}, m(\mathcal{A}))$.*

Также полезным является следующее свойство функции $g(d,m)$.

**Теорема 2.4.9** ([32, теорема 3.3])**.** *При фиксированном значении $d \geq 2$ функция $g(d,m)$ является неубывающей по $m$ на множестве $[2,d] \cap \mathbb{N}$.*

**Лемма 2.4.10.** *Пусть $\mathbb{F}$ — поле характеристики $p > 0$, $p \nmid q$, $k \geq l$, $G = G_{p^l} \times G_{p^k} \times G_q$. Тогда $l(\mathbb{F}G) \leq p^k q + p^l - 2$.*

*Доказательство.* При $q = 1$ группа $G$ является $p$-группой и утверждение леммы следует из теоремы 2.3.1. Поэтому далее мы будем предполагать $q \geq 2$.

Рассмотрим произвольный элемент $w \in \mathbb{F}G$. Пусть $w = \alpha_1 g_1 + \cdots \alpha_{|G|} g_{|G|}$, где $\alpha_i \in \mathbb{F}$, $g_i \in G$. Тогда $w^{p^k} = \alpha_1^{p^k} g_1^{p^k} + \cdots \alpha_{|G|}^{p^k} g_{|G|}^{p^k}$, так как все полиномиальные коэффициенты равны нулю над полем характеристики $p$. Но $g_i^{p^k} = (0,0,h_i)$, где $h_i \in G_q$. Следовательно, $w^{p^k}$ является элементом $q$-мерной подалгебры в $G$, порождённой элементом $(0,0,1) \in G_{p^l} \times G_{p^k} \times G_q$. Таким образом, $\deg w^{p^k} \leq q$. Тогда $\deg w \leq p^k q$, то есть $m(\mathbb{F}G) \leq p^k q$. С другой стороны $\deg v = p^k q$, где $v = (0,1,1) \in G_{p^l} \times G_{p^k} \times G_q$, так как $G_{p^k} \times G_q$ — циклическая подгруппа в $G$ порядка $p^k q$, а $v$ — порождающий её (и соответствующую $p^k q$-мерную подалгебру) элемент, то есть $m(\mathbb{F}G) \geq p^k q$. Таким образом, $m(\mathbb{F}G) = p^k q$.

Так как $k \geq l$ и $q \geq 2$, $m(\mathbb{F}G)^2 = p^{2k}q^2 > p^{k+l}q = |G|$. Тогда

$$[\log_{m(\mathbb{F}G)} |G|] = 1$$

и

$$[m(\mathbb{F}G)^{\{\log_{m(\mathbb{F}G)} |G|\}}] = \left[\frac{|G|}{m(\mathbb{F}G)^{[\log_{m(\mathbb{F}G)} |G|]}}\right] = \left[\frac{p^{k+l}q}{p^k q}\right] = p^l.$$

Применение теоремы 2.4.8 завершает доказательство. □

Из следствия 2.4.7 и леммы 2.4.10 непосредственно следует теорема 2.4.3.

## 2.5 Обобщение теорем 2.3.4 и 2.4.3

Основным результатом данной секции является следующая теорема. С одной стороны, она является обобщением теоремы 2.3.4, с другой — обобщением теоремы 2.4.3.

**Теорема 2.5.1.** *Пусть $\mathbb{F}$ — совершенное поле характеристики $p > 0$, $H$ — абелева группа порядка $q$, $|\mathbb{F}| \geq q$, $p \nmid q$, $k \geq l$. Тогда*

$$l(\mathbb{F}[G_{p^l} \times G_{p^k} \times H]) = p^k q + p^l - 2.$$

Докажем верхнюю оценку. Лемму 2.4.10 можно обобщить, отказавшись от цикличности третьего прямого множителя в разложении $G$.

**Лемма 2.5.2.** *Пусть $\mathbb{F}$ — поле характеристики $p > 0$, $H$ — абелева группа порядка $q$, $k \geq l$, $G = G_{p^l} \times G_{p^k} \times H$. Тогда $l(\mathbb{F}G) \leq p^k q + p^l - 2$.*

*Доказательство.* При доказательстве леммы 2.4.10 мы пользовались цикличностью $H$ и условием $p \nmid q$ лишь для того, чтобы предьявить элемент $v$, такой что $\deg v = p^k q$, показав тем самым, что $m(\mathbb{F}G) = p^k q$. Но в силу теоремы 2.4.9 нам достаточно неравенства $m(\mathbb{F}G) \leq p^k q$ для доказательства утверждения.

В остальном доказательство повторяет доказательство леммы 2.4.10. □

Однако нижняя оценка из следствия 2.4.7 не выполняется при отказе от цикличности третьего прямого множителя. Для доказательства нижней оценки нам понадобится вспомогательный результат о длине тензорного произведения алгебр.

**Лемма 2.5.3** ([2, лемма 3.23]). *Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{A}$ и $\mathcal{B}$ — конечномерные алгебры с единицами над $\mathbb{F}$. Тогда $l(\mathcal{A} \otimes_{\mathbb{F}} \mathcal{B}) \geq l(\mathcal{A}) + l(\mathcal{B})$.*

Теперь мы готовы доказать сформулированную в начале секции теорему 2.5.1.

*Доказательство.* Так как $\mathbb{F}[G_{p^l} \times G_{p^k} \times H] \cong \mathbb{F}G_{p^l} \otimes_{\mathbb{F}} \mathbb{F}[G_{p^k} \times H]$, из леммы 2.5.3 следует, что $l(\mathbb{F}[G_{p^l} \times G_{p^k} \times H]) \geq l(\mathbb{F}G_{p^l}) + l(\mathbb{F}[G_{p^k} \times H])$. Группа $G_{p^l}$ — циклическая, значит алгебра $\mathbb{F}G_{p^l}$ — однопорождённая и, согласно лемме 2.1.1, $l(\mathbb{F}G_{p^l}) = p^l - 1$. Из теоремы 2.3.4 следует, что $l(\mathbb{F}[G_{p^k} \times H]) = p^k q - 1$. Таким образом, $l(\mathbb{F}[G_{p^l} \times G_{p^k} \times H]) \geq p^k q + p^l - 2$. Верхняя оценка $l(\mathbb{F}[G_{p^l} \times G_{p^k} \times H]) \leq p^k q + p^l - 2$ следует из леммы 2.5.2. □

**Замечание 2.5.4.** Отметим, что в доказательстве леммы 2.4.4 мы могли после получения равенства 7 вместо рассмотрения системы порождающих сослаться на лемму 2.5.3 аналогично тому, как это было сделано в доказательстве теоремы 2.5.1, из чего следовала бы нужная нижняя оценка.

Покажем, что условие на мощность поля в теореме 2.5.1 существенно. Рассмотрим в качестве примера $\mathbb{F} = \mathbb{F}_3$, $k = l = 1$, $H = G_2 \times G_2$. В данном случае $p = 3$, $q = 4$ и $p^k q + p^l - 2 = 13$. Однако $l(\mathbb{F}_3[G_3 \times G_3 \times G_2 \times G_2]) \neq 13$. Докажем это.

**Утверждение 2.5.5.** $10 \leq l(\mathbb{F}_3[G_3 \times G_3 \times G_2 \times G_2]) \leq 11$.

*Доказательство.* Обозначим $\mathbb{F}_3[G_3 \times G_3 \times G_2 \times G_2]$ за $\mathcal{A}$. Рассмотрим произвольный элемент $w \in \mathcal{A}$. Тогда

$$w^3 = \alpha_0 e + \alpha_1 g_1 + \alpha_2 g_2 + \alpha_3 g_3,$$

где $\alpha_i \in \mathbb{F}_3$, $e = (0,0,0,0)$, $g_1 = (0,0,1,0)$, $g_2 = (0,0,0,1)$, $g_3 = (0,0,1,1)$. Тогда

$$w^9 = (w^3)^3 = \alpha_0^3 e^3 + \alpha_1^3 g_1^3 + \alpha_2^3 g_2^3 + \alpha_3^3 g_3^3 = \alpha_0 e + \alpha_1 g_1 + \alpha_2 g_2 + \alpha_3 g_3.$$

Таким образом, для произвольного элемента алгебры $\mathcal{A}$ многочлен $x^9 - x^3$ является аннулирующим, то есть $m(\mathcal{A}) \leq 9$.

Из теорем 2.4.8 и 2.4.9 следует, что $l(\mathcal{A}) \leq g(\dim \mathcal{A}, m(\mathcal{A})) \leq g(36, 9) = 11$.

Нижняя оценка следует из леммы 2.4.4. $\square$

# Глава 3

# Диэдральные группы

Результаты, представленные в этой главе, опрубликованы в совместных работах автора и О.В. Марковой [39], [40].

Глава посвящена длине групповой алгебры $\mathbb{F}\mathcal{D}_n$. Случай $n = 1$ — тривиальный, так как $\mathcal{D}_1 = G_2$. Случай $n = 2$ будет рассмотрен в главе 4, так как $\mathcal{D}_2 \cong G_2 \times G_2$. Поэтому мы рассматриваем случай $n \geq 3$. Основным результатом, который будет доказан в этой главе, является следующая

**Теорема 3.0.1.** *Пусть* $\mathbb{F}$ *— поле, такое что* $\operatorname{char}\mathbb{F}$ *не делит* $2n$, $n \geq 3$. *Тогда* $l(\mathbb{F}\mathcal{D}_n) = n$.

## 3.1 Нижняя оценка

В данной секции мы рассмотрим нижнюю оценку длины алгебры $\mathbb{F}\mathcal{D}_n$ с помощью рассмотрения групповой системы порождающих. Очевидно, эта система является системой порождающих групповой алгебры. Отметим, что для группы $G$ и её системы порождающих $\mathcal{S}$ схожая задача отыскания кратчайшего слова от порождающих, представляющего элемент $g \in G$, широко исследована. Главным отличием в данном случае является то, что в схожих вопросах теории групп алфавит по определению расширен обратными к элементам системы порождащих элементами.

**Лемма 3.1.1.** *Пусть* $\mathcal{D}_n$ *— группа диэдра порядка* $2n$, $n \geq 3$, $\mathbb{F}$ *— произвольное поле. Тогда* $l(\mathbb{F}\mathcal{D}_n) \geq n$.

*Доказательство.* Предъявим систему порождающих длины не меньшей, чем $n$. Пусть $r$ — поворот на угол $\dfrac{2\pi}{n}$ и $s$ отражение. Тогда система из двух отражений $\mathcal{S} = \{rs, s\} = \{u, v\}$ есть система порождающих для рассматриваемой алгебры. Действительно,

$$\mathbb{F}\mathcal{D}_n = \mathcal{L}(\{r, s\}) = \mathcal{L}(\{uv, v\}) \subseteq \mathcal{L}(\{u, v\}) = \mathcal{L}(\{rs, s\}) \subseteq \mathcal{L}(\{r, s\}) = \mathbb{F}\mathcal{D}_n.$$

Докажем, что данная система порождающих имеет длину не меньшую, чем $n$. Заметим, что $u^2 = v^2 = e$, где $e$ — нейтральный элемент группы. Таким образом, несократимыми словами от образующих могут быть только два слова для каждой длины (то есть, слова $uvuv\dots$ и $vuvu\dots$), кроме нулевой длины, где будет только тодно пустое слово $e$. Следовательно, $\dim \mathcal{L}_{n-1}(\mathcal{S}) \leq (n-1)\cdot 2 + 1 < 2n$, то есть $l(\mathcal{S}) \geq n$.

□

**Замечание 3.1.2.** Рассмотрим длину стандартной системы порождающих из поворота и отражения $\mathcal{S} = \{r, s\} = \{a, b\}$. Так как $b^2 = e$, $aba = b$, слова, содержащие данные подслова, сократимы. Таким образом, несократимые слова длины $k$ имеют один из следующих видов $a^{k-1}b$, $ba^{k-1}$ — отражения с осями симметрий симметричными относительно оси симметрии отражения $b$, $a^k$ — поворот на угол $\frac{2\pi k}{n}$, $ba^{k-2}b$ — поворот на угол $-\frac{2\pi(k-2)}{n}$. Таким образом, за слово длины $k$ (при $k > 2$) мы получаем $2k-1$ поворотов и $2k-1$ отражений. Следовательно словами длины $[\frac{n}{2}] + 1$ можно заведомо породить все элементы группы, а значит и всю алгебру. Таким образом, в данном случае $l(\mathcal{S}) \leq [\frac{n}{2}] + 1 < n$, чем и обусловлен выбор системы порождающих из двух отражений.

## 3.2 Результаты для матричных алгебр

В данной секции получены результаты о длине матричных алгебр, которые интересны и сами по себе. Мы же воспользуемся ими для получения верхней оценки и завершения доказательства основного результата главы.

Введём понятие эквивалентности слов от элементов $\mathcal{S}$.

**Определение 3.2.1.** Будем называть два слова $u$ и $v$ длины $i$ от образующих *эквивалентными*, если $u - \alpha v \in \mathcal{L}_{i-1}(\mathcal{S})$, для некоторого ненулевого $\alpha \in \mathbb{F}$. Будем использовать в этом случае обозначение $u \sim v$.

**Определение 3.2.2.** Будем называть слово $u$ длины $i$ от образующих *сократимым*, если $u \in \mathcal{L}_{i-1}(\mathcal{S})$.

**Определение 3.2.3.** Будем называть *слогом* слово или подслово из двух букв, *$k$-м слогом* будем называть подслово из $k$-й и $(k+1)$-й букв.

Для доказательства леммы 3.2.8 нам потребуется несколько свойств введённого понятия.

**Лемма 3.2.4.** *Эквивалентность слов является отношением эквивалентности на множестве слов.*

*Доказательство. Рефлексивность.* $u - \alpha u \in \mathcal{L}_{i-1}(\mathcal{S})$ при $\alpha = 1$.

*Симметричность.* Пусть $u - \alpha v \in \mathcal{L}_{i-1}(\mathcal{S})$. Тогда, домножив элемент $u - \alpha v$ на $-\alpha^{-1}$, получим $v - \alpha^{-1}u \in \mathcal{L}_{i-1}(\mathcal{S})$.

*Транзитивность.* Пусть $u - \alpha_1 v \in \mathcal{L}_{i-1}(\mathcal{S})$, $v - \alpha_2 w \in \mathcal{L}_{i-1}(\mathcal{S})$. Тогда, прибавив к первому элементу второй, домноженный на $\alpha_1$, получим $u - \alpha_1\alpha_2 w \in \mathcal{L}_{i-1}(\mathcal{S})$.

□

**Лемма 3.2.5.** *Пусть $u \sim v$. Тогда $u$ сократимо тогда и только тогда, когда $v$ сократимо.*

*Доказательство.* Очевидно.

□

**Лемма 3.2.6.** *Пусть слово $u$ несократимо. Тогда любое подслово слова $u$ несократимо.*

*Доказательство.* Очевидно.

□

**Лемма 3.2.7.** *Пусть слово $w$ длины $i$ содержит подслово $u$ длины $j$, $u \sim v$. Тогда $w \sim w'$, где $w'$ — слово, полученное из $w$ заменой подслова $u$ на подслово $v$.*

*Доказательство.* По условию, $u - \alpha v \in \mathcal{L}_{j-1}(\mathcal{S})$, $w = w_1 u w_2$, для некоторых слов $w_1$, $w_2$. Тогда, домножив выражение $u - \alpha v$ слева на $w_1$ и справа на $w_2$, получим $w - \alpha w' \in \mathcal{L}_{i-1}(\mathcal{S})$. □

Докажем теперь несколько лемм о длине, которые нам потребуются для доказательства основного результата.

**Лемма 3.2.8.** *Пусть $\mathcal{A}$ — конечномерная ассоциативная $\mathbb{F}$-алгебра с единицей,* $\dim \mathcal{A} < 2l(\mathcal{A}) + 2$. *Тогда*

$$l(\mathcal{A} \oplus M_2(\mathbb{F})) \leq l(\mathcal{A}) + 2.$$

*Доказательство.* Пусть $\dim \mathcal{L}_{l(\mathcal{A})+2}(\mathcal{S}) < \dim A + 4$, иначе утверждение доказано. Тогда из условия следует, что $\dim \mathcal{L}_{l(\mathcal{A})+2}(\mathcal{S}) \leq 2l(\mathcal{A}) + 4$. В то же время $\dim \mathcal{L}_0(\mathcal{S}) = 1$, из чего следует, что для некоторого $k < l(\mathcal{A}) + 3$ выполнено равенство $\dim \mathcal{L}_k(\mathcal{S}) = \dim \mathcal{L}_{k-1}(\mathcal{S}) + 1$, то есть все слова длины $k$ эквивалентны некоторому одному слову $u = xy_1y_2 \dots y_{k-1}$.

Покажем, что любое слово длины $l(\mathcal{A}) + 3$ сократимо. Пусть $w$ — произвольное слово длины $l(\mathcal{A}) + 3$. Заменим первое $k$-подслово (то есть первые $k$ букв) слова $w$ на $u$. Затем заменим на $u$ второе $k$-подслово. Обозначим полученное слово $xxy_1y_2 \dots y_{l(\mathcal{A})+1}$ за $w'$. Из лемм 3.2.4 и 3.2.7 следует, что $w \sim w'$.

По теореме Гамильтона-Кэли можно найти такие $\alpha$ и $\beta$, что $\pi_2(x^2 - \alpha x - \beta e) = 0$. С другой стороны из определения длины следует, что существует такой элемент $v \in \mathcal{L}_{l(\mathcal{A})}$, что $\pi_1(y_1y_2 \dots y_{l(\mathcal{A})+1} - v) = 0$. Таким образом, $(x^2 - \alpha x - \beta e)(y_1y_2 \dots y_{l(\mathcal{A})+1} - v) = 0$, следовательно $w' = \alpha x y_1y_2 \dots y_{l(\mathcal{A})+1} + \beta y_1y_2 \dots y_{l(\mathcal{A})+1} + x^2V - \alpha xV - \beta V \in \mathcal{L}_{l(\mathcal{A})+2}$. Таким образом, $w'$ сократимо. Следовательно из леммы 3.2.5 следует, что $w$ сократимо. □

Напомним, что в этой главе $A_n(\mathbb{F}) = \bigoplus_{i=1}^{n} M_2(\mathbb{F})$, $D_n(\mathbb{F}) = \bigoplus_{i=1}^{n} \mathbb{F}$.

**Лемма 3.2.9.** *Пусть $|\mathbb{F}| > n$. Тогда $l(A_n(\mathbb{F})) = 2n$.*

*Доказательство.* Покажем, что $l(A_n(\mathbb{F})) \geq 2n$. Рассмотрим систему порождающих $\mathcal{S} = \{a, b\}$ такую, что $\pi_i(a) = E_{2,1}$, $\pi_i(b) = \alpha_i E_{1,2}$ for all $1 \leq i \leq n$, $\alpha_i \neq 0$, $\alpha_i \neq \alpha_j$, if $i \neq j$ (здесь мы пользуемся тем, что $|\mathbb{F}| > n$).

Сначала мы покажем, что $\mathcal{S}$ — система порождающих для рассматриваемой алгебры. Отметим, что

$$\pi_i(ab + ba - \alpha_i 1) = 0,$$

$$\pi_j(ab + ba - \alpha_i 1) = (\alpha_j - \alpha_i)I \neq 0,$$

if $j \neq i$. Рассмотрим

$$\pi_j \left( \prod_{i \neq k} (ab + ba - \alpha_i I) \cdot \prod_{i \neq k} (\alpha_k - \alpha_i)^{-1} \right) = \delta_{jk} I,$$

где $\delta_{ij}$ — символ Кронекера, $1 \leq k \leq n$. Обозначим $\prod_{i \neq k}(ab + ba - \alpha_i 1) \cdot \prod_{i \neq k}(\alpha_k -$

$\alpha_i)^{-1}$ за $E_k$. Тогда множество $\{E_i a, E_i b, E_i ab, E_i ba : 1 \le i \le n\}$ является базисом $A_n(\mathbb{F})$, следовательно $\mathcal{S}$ — система порождающих.

Покажем, что $l(\mathcal{S}) \ge 2n$. Отметим, что $a^2 = b^2 = 0$. Тогда несократимыми могут быть только 2 слова каждой длины ($abab\dots$ и $baba\dots$) за исключением длины 0, где будет лишь одно слово $I$. Следовательно $\dim \mathcal{L}_{2n-1}(\mathcal{S}) \le (2n-1) \cdot 2 + 1 < 4n$, то есть $l(\mathcal{S}) \ge 2n$.

Теперь докажем индукцией по $n$, что $l(\mathcal{S}) \le 2n$.

При $n = 1$ в силу некоммутативности алгебры $l(A_1(\mathbb{F})) \le \dim A_1(\mathbb{F}) - 2 = 2$. Предположим, что $l(A_k(\mathbb{F}) \le 2k)$, для некоторого $k$. Но нижняя оценка верна для всех $n$, следовательно $l(A_k(\mathbb{F})) = 2k$. Для завершения индукции докажем, что $l(A_{k+1}(\mathbb{F}) \le 2(k+1)$. Заметим, что $\dim(A_k(\mathbb{F}) = 4k$, а $2l(A_k(\mathbb{F}))+2 = 4k+2$. Таким образом, условие леммы 3.2.8 выполнено. Применяя её, получаем $l(A_{k+1}(\mathbb{F})) = l(A_k(\mathbb{F}) \oplus M_2(\mathbb{F})) \le l(A_k(\mathbb{F})) + 2 = 2k + 2 = 2(k+1)$. □

Этот результат в частности показывает, что оценка из леммы 3.2.8 достижима.

Чтобы доказать последнюю лемму в этой секции, нам понадобится следующее утверждение о системах порождающих.

**Утверждение 3.2.10** ([2, предложение 3.4])**.** *Пусть $\mathbb{F}$ — произвольное поле, пусть $\mathcal{A}$ — конечномерная $\mathbb{F}$-алгебра с единицей $1_\mathcal{A}$ и пусть $\mathcal{S} = \{a_1, \dots, a_k\}$ — система порождающих для алгебры $\mathcal{A}$. Тогда существует система порождающих $\mathcal{S}'$ для $\mathcal{A}$, удовлетворяющая следующим условиям:*
*1.* $\mathcal{S}' \subseteq \mathcal{S}$;
*2.* $1_\mathcal{A} \notin \langle \mathcal{S}' \rangle$
*3.* $\dim \mathcal{L}_1(\mathcal{S}') = |\mathcal{S}'| + 1$;
*4.* $l(\mathcal{S}') = l(\mathcal{S})$.

**Лемма 3.2.11.** *Пусть $\mathcal{A}$ — коммутативная алгебра. Пусть $|\mathbb{F}| > n$. Тогда*

$$l(A_n(\mathbb{F}) \oplus \mathcal{A}) \le \max\{2n+2, l(\mathcal{A})\}.$$

*Доказательство.* Пусть $\mathcal{S}$ — система порождающих алгебры $A_n(\mathbb{F}) \oplus \mathcal{A}$. Докажем, что для каждого слагаемого $M_2(\mathbb{F})$ прямой суммы $A_n(\mathbb{F})$ существует два

элемента $a, b \in \mathcal{L}_1(\mathcal{S})$ таких, что $\pi_i(a)$ и $\pi_i(b)$ являются системой порождающих для соответствующего прямого слагаемого (то есть $i$-й компоненты).

Действительно, $\pi_i(\mathcal{S})$ является системой порождающих для соответствующего прямого слагаемого. Так как $M_2(\mathbb{F})$ некоммутативна, получаем, что $M_2(\mathbb{F})$ не однопорождена и $\dim \mathcal{L}_1(\pi_i(\mathcal{S})) \geq 3$. Если $\dim \mathcal{L}_1(\pi_i(\mathcal{S})) = 3$, тогда из предложения 3.2.10 следует, что мы можем рассматривать систему порождающих $\mathcal{S}' \subseteq \mathcal{S}$ такую, что $|\mathcal{S}'| = 2$. Если $\dim \mathcal{L}_1(\pi_i(\mathcal{S})) = 4$, то есть $\mathcal{L}_1(\pi_i(\mathcal{S})) = M_2(\mathbb{F})$, то все матрицы содержатся в $\mathcal{L}_1(\pi_i(\mathcal{S}))$, включая систему порождающих $\mathcal{S}'$ такую, что $|\mathcal{S}'| = 2$ (например, рассмотренную в доказательстве леммы 3.2.9).

Так как мы можем использовать линейные комбинации, мы можем предполагать, что $\pi_i(a) = E_{1,2} + xE_{2,2}$ и $\pi_i(b) = E_{2,1} + yE_{2,2}$ или $\pi_i(a) = E_{1,2} + zE_{2,1}$ и $\pi_i(b) = E_{2,2}$, где $x, y, z \in \mathbb{F}$ и $z \neq 0$ (в противном случае, $\pi_i(a)$ и $\pi_i(b)$ не порождают алгебру). Рассмотрим коммутатор $[\pi_i(a), \pi_i(b)] = \pi_i(a)\pi_i(b) - \pi_i(b)\pi_i(a)$. Он равен $E_{1,1} + yE_{1,2} + xE_{2,1} - E_{2,2}$ или $E_{1,2} - zE_{2,1}$. Покажем, что этот коммутатор невырожден в обоих случаях.

В первом случае определитель коммутатора равен $-1-xy$. Допустим $xy = -1$, тогда $\pi_i(b)\pi_i(a) = 0$ и $(\pi_i(a) + \pi_i(b))^2 = \pi_i(a)^2 + \pi_i(b)^2 + \pi_i(a)\pi_i(b) + \pi_i(b)\pi_i(a)$. Тогда из теоремы Гамильтона-Кэли следует, что $\mathcal{L}_2(\pi_i(\{a, b\})) = \mathcal{L}_1(\pi_i(\{a, b\}))$. Следовательно $\pi_i(a)$ и $\pi_i(b)$ не порождают $M_2(\mathbb{F})$. Противоречие.

Во втором случае определитель коммутатора равен $z \neq 0$.

Из леммы 3.2.9 следует, что мы можем получить произвольную матрицу в $i$-й компоненте прямой суммы $A_n(\mathbb{F})$ и нулевые матрицы во всех остальных компонентах, используя слова длины не более $2n$. Обозначим этот элемент $A_n(\mathbb{F}) \oplus \mathcal{A}$ за $c$ (мы не знаем, что в $\pi_{n+1}(c)$). Из коммутативности $\mathcal{A}$ следует, что $\pi_{n+1}([a, b]) = 0$. Так как $[a, b]$ невырожден и $\pi_{n+1}([a, b]) = 0$, получаем, что $\pi_i([a, b]c)$ есть произвольная матрица из $M_2(\mathbb{F})$ и $\pi_k([a, b]c) = 0$, где $1 \leq k \leq n + 1$, $k \neq i$. Наконец, мы можем получить произвольный элемент $\mathcal{A}$ в $(n + 1)$-й компоненте прямой суммы $A_n(\mathbb{F}) \oplus \mathcal{A}$, используя слова длины не более $l(\mathcal{A})$. Таким образом, мы можем получить произвольный элемент алгебры $A_n(\mathbb{F}) \oplus \mathcal{A}$ используя слова длины не более $\max\{2n + 2, l(\mathcal{A})\}$. □

## 3.3 Длина прямой суммы двух полных матричных алгебр порядка 2

Отвлечёмся от доказательства основного результата. В лемме 3.2.9 вычислена длина прямой суммы $M_2(\mathbb{F})$ при некотором ограничении на поле коэффициентов. В этом разделе мы вычислим длину $M_2(\mathbb{F}) \oplus M_2(\mathbb{F})$ независимо от предыдущих результатов и без каких-либо оговороок. Для этого докажем лемму, интересную саму по себе.

**Лемма 3.3.1.** *Пусть $\mathcal{A}$ — конечномерная ассоциативная алгебра с единицей,* $\dim \mathcal{A} \leq m(\mathcal{A}) + 4$, $m(\mathcal{A}) \geq 3$. *Тогда* $l(\mathcal{A}) \leq m(\mathcal{A})$.

*Доказательство.* Будем рассуждать от противного. Пусть существует система порождающих $\mathcal{S}$, такая что $l(\mathcal{S}) > m(\mathcal{A})$. Тогда

$$\dim \mathcal{L}_{m(\mathcal{A})}(\mathcal{S}) < \dim \mathcal{A},$$

$$\dim \mathcal{L}_{m(\mathcal{A})-1}(\mathcal{S}) < \dim \mathcal{A} - 1,$$

$$\dots$$

$$\dim \mathcal{L}_2(\mathcal{S}) < 6,$$

$$\dim \mathcal{L}_1(\mathcal{S}) < 5.$$

Таким образом, в $\mathcal{S}$ может быть 1, 2 или 3 элемента (здесь и далее будем считать, что из системы порождающих мы выбираем линейно независимую подсистему согласно утверждению 3.2.10). Рассмотрим все возможные случаи.

(i) $\dim \mathcal{L}_1(\mathcal{S}) = 2$. В случае однопорождённой алгебры $l(\mathcal{A}) = \dim \mathcal{A} - 1 = m(\mathcal{A}) - 1 < m(\mathcal{A})$.

(ii) $\dim \mathcal{L}_1(\mathcal{S}) = 3$. Имеем $\mathcal{S} = \{a, b\}$, множество слов длины 2 от $\mathcal{S}$ имеет вид $\{a^2, b^2, ab, ba\}$.

Если $a^2$ и $b^2$ сократимы, то несократимыми словами могут быть только слова вида $A_t := abab\dots$ и $B_t := baba\dots$ (в словах по $t$ букв). Если $A_h$ выражается через $B_h$ и слова меньшей длины (без ограничения общности), то $A_l$ и $B_l$ сократимы при $l > h$, так как они содержат $A_h$ как подслово и при замене его на $B_h$, в сло-

ве появится сократимое $a^2$ или $b^2$. Таким образом, чтобы $A_{m(\mathcal{A})+1}$ или $B_{m(\mathcal{A})+1}$ были несократимы, необходимо, чтобы $\dim \mathcal{L}_{m(\mathcal{A})}(\mathcal{S}) = \dim\langle 1_{\mathcal{A}}, A_1, B_1, A_2, B_2, \ldots, A_{m(\mathcal{A})}, B_{m(\mathcal{A})}\rangle = 2m(\mathcal{A}) + 1$. Но, так как мы предполагаем, что $\dim \mathcal{L}_{m(\mathcal{A})}(\mathcal{S}) < \dim \mathcal{A}$, получаем неравенство $2m(\mathcal{A})+1 < m(\mathcal{A})+4$, что невозможно, так как $m(\mathcal{A}) \geq 3$ по условию.

Пусть без ограничения общности несократимо $a^2$. Если $ab$ и $ba$ оба выражаются через $\{1_{\mathcal{A}}, a, b, a^2\}$, то любые слова длины $m(\mathcal{A}) + 1$, содержащие разные буквы, эквивалентны $\alpha a^{m(\mathcal{A})+1}$ (то есть представимы в виде $\alpha a^{m(\mathcal{A})+1}$+«слова меньшей длины»), но $\alpha a^{m(\mathcal{A})+1}$ сократимо по условию (равно как и $b^{m(\mathcal{A})+1}$ — слово, не содержащее разных букв). Следовательно, в этом случае любое слово длины $m(\mathcal{A}) + 1$ сократимо. Таким образом, хотя бы одно из слов $ab$ и $ba$ не выражается через $\{1_{\mathcal{A}}, a, b, a^2\}$.

Пусть $ab$ не выражается через $\{1_{\mathcal{A}}, a, b, a^2\}$ (в случае $ba$ можно провести аналогичные рассуждения). Тогда $\dim\langle 1_{\mathcal{A}}, a, b, a^2, ab\rangle = 5$, то есть все оставшиеся слоги (*слогом* в этом доказательстве будем называть слова или подслова длины 2) выражаются через данные слова, так как $\dim \mathcal{L}_2(\mathcal{S}) < 6$. Тогда любое слово длины $m(\mathcal{A})+1$ можно заменить на эквивалентное ему (по модулю $\mathcal{L}_{m(\mathcal{A})}(\mathcal{S})$) слово $\alpha a^{m(\mathcal{A})+1} + \beta a^{m(\mathcal{A})} b$ поочерёдно выразив все слоги, начиная с первого, через $ab$, $a^2$ и буквы, но $a^{m(\mathcal{A})}$ сократимо по условию. Следовательно, в этом случае любое слово длины $m(\mathcal{A}) + 1$ сократимо.

(iii) $\dim \mathcal{L}_1(\mathcal{S}) = 4$. Тогда $\dim \mathcal{L}_2(\mathcal{S}) = 5$, так как $\dim \mathcal{L}_2(\mathcal{S}) < 6$. В этом случае все слоги выражаются через буквы и какой-то один слог $xy$ (быть может, $x$ и $y$ — одна и та же буква). Тогда любое слово длины $m(\mathcal{A})+1$ эквивалентно (по модулю $\mathcal{L}_{m(\mathcal{A})}(\mathcal{S})$) слову $\alpha x^{m(\mathcal{A})} y$, но $x^{m(\mathcal{A})}$ сократимо по условию. Следовательно, в этом случае любое слово длины $m(\mathcal{A}) + 1$ сократимо. □

**Теорема 3.3.2.** $l(M_2(\mathbb{F}) \oplus M_2(\mathbb{F})) = 4$.

*Доказательство.* Неравенство $l(M_2(\mathbb{F}) \oplus M_2(\mathbb{F})) \leq 4$ следует из леммы 3.3.1, так как для данной алгебры $\dim \mathcal{A} = 8$ и $m(\mathcal{A}) = 4$.

Неравенство $l(M_2(\mathbb{F}) \oplus M_2(\mathbb{F})) \geq 4$ получим, предъявив систему порождающих $\mathcal{S}$ длины 4.

Представим данную алгебру в виде алгебры блочно-диагональных матриц с двумя блоками размера 2. Возьмём $a = (E_{2,1} + E_{3,4} + E_{4,3})$ и $b = (E_{1,2} + E_{4,3})$.

Добавим к ним элемент $ab = (E_{2,2} + E_{3,3})$, который очевидно не выражается через $a$, $b$ и $e$. Далее добавим $a^2 = (E_{3,3} + E_{4,4})$, который также не выражается через предыдущие слова. Тогда $ba = e - ab$, $b^2 = 0$, то есть $\dim \mathcal{L}_2(\mathcal{S}) = 5$.

Далее рассмотрим элементы $a^2b = (E_{4,3})$ и $a^3 = (E_{3,4} + E_{4,3})$. Отметим, что с помощью элементов $ab$, $a^2$, $a^2b$ и $a^3$ можно получить произвольный элемент во втором блоке, при этом в первом блоке на всех местах будут стоять нули, за исключением, быть может, правого нижнего угла. Тогда с помощью $e$, $a$, и $b$ можно получить что угодно в первом блоке, за исключением правого нижнего угла блока. Следовательно рассмотренные 7 элементов линейно независимы. Покажем, что все оставшиеся 5 слов длины 3 выражаются через рассмотренные ранее. Все 3 слова содержащие $b^2$ равны нулю, $aba = a(e-ab) = a-a^2b$, $bab = (e-ab)b = b-ab^2 = b$, $ba^2 = (e-ab)a = a - aba = a^2b$. Таким образом, $\dim \mathcal{L}_3(\mathcal{S}) = 7$.

Далее рассмотрим $a^3b = E_{3,3}$. На предыдущем шаге нам оставалось научиться получать что угодно в правом нижнем углу первого блока, что мы теперь можем сделать с помощью $ab - a^3b = E_{2,2}$. Таким образом, $\dim \mathcal{L}_4(\mathcal{S}) = 8$ и $l(\mathcal{S}) = 4$.

□

**Замечание 3.3.3.** В последнем доказательстве верхняя оценка могла быть получена и с помощью леммы 3.2.8.

## 3.4 Доказательство основной теоремы

**Утверждение 3.4.1.** *Пусть* $\mathbb{F}$ — *алгебраически замкнутое поле и* $\operatorname{char}\mathbb{F}$ *не делит порядок группы. Тогда*

$$\mathbb{F}\mathcal{D}_{2n+1} \cong A_n(\mathbb{F}) \oplus D_2(\mathbb{F}),$$

$$\mathbb{F}\mathcal{D}_{2n+2} \cong A_n(\mathbb{F}) \oplus D_4(\mathbb{F}).$$

*Доказательство.* Пусть $\mathbb{F}$ — алгебраически замкнутое поле и $\operatorname{char}\mathbb{F}$ не делит $2m$ (то есть групповая алгебра $\mathbb{F}\mathcal{D}_m$ — полупростая). Тогда, применяя теорему Машке [22, § 3.6, теорема, стр. 72] и теорему Веддербарна-Артина [22, § 3.5, теорема, стр. 69], представим данную алгебру в виде прямой суммы матричных алгебр над

$\mathbb{F}$. Какие именно будут в данном представлении слагаемые можно посмотреть, например, в [23, глава 11, § 4, задача 1, стр. 473]. □

Мы воспользуемся матричным представлением из утверждения 3.4.1 для доказательства верхней оценки $l(\mathbb{F}\mathcal{D}_n) \leq n$.

**Лемма 3.4.2.** *Пусть* $\mathbb{F}$ *— алгебраически замкнутое поле, такое что* $\operatorname{char}\mathbb{F}$ *не делит* $4n+2$*. Тогда*

$$l(A_n(\mathbb{F}) \oplus D_2(\mathbb{F})) = 2n+1.$$

*Доказательство.* Нижняя оценка $2n+1 \leq l(A_n(\mathbb{F})\oplus D_2(\mathbb{F}))$ получается из нижней оценки длины групповой алгебры диэдральной группы в лемме 3.1.1 и утверждения 3.4.1.

Верхнюю оценку $l(A_n(\mathbb{F}) \oplus D_2(\mathbb{F})) \leq 2n+1$ получим с помощью индукции по $n$. Пусть $n = 1$. Длина алгебры $D_2(\mathbb{F})$ в силу тривиальной оценки равна 1, $\dim D_2(\mathbb{F}) = 2$. Таким образом, условие леммы 3.2.8 выполено. Следовательно $l(M_2(\mathbb{F}) \oplus D_2(\mathbb{F})) \leq 3$. Предположим, что $l(A_k(\mathbb{F}) \oplus D_2(\mathbb{F})) \leq 2k+1$. Но нижняя оценка верна для всех $n$, следовательно $l(A_k(\mathbb{F})\oplus D_2(\mathbb{F})) = 2k+1$. Для завершения индукции докажем, что $l(A_{k+1}(\mathbb{F})\oplus D_2(\mathbb{F})) \leq 2(k+1)+1$. Заметим, что $\dim(A_k(\mathbb{F})\oplus D_2(\mathbb{F})) = 4k+2$, а $2l(A_k(\mathbb{F}) \oplus D_2(\mathbb{F})) + 2 = 4k+4$. Таким образом, условие леммы 3.2.8 выполнено. Применяя её, получаем $l(A_{k+1}(\mathbb{F}) \oplus D_2(\mathbb{F})) = l(A_k(\mathbb{F}) \oplus D_2(\mathbb{F}) \oplus M_2(\mathbb{F})) \leq l(A_k(\mathbb{F}) \oplus D_2(\mathbb{F})) + 2 = 2k+1+2 = 2(k+1)+1$.

□

**Лемма 3.4.3.** *Пусть* $\mathbb{F}$ *— алгебраически замкнутое поле, такое что* $\operatorname{char}\mathbb{F}$ *не делит* $4n+4$*. Тогда*

$$l(A_n(\mathbb{F}) \oplus D_4(\mathbb{F})) = 2n+2.$$

*Доказательство.* Нижняя оценка $2n+2 \leq l(A_n(\mathbb{F})\oplus D_4(\mathbb{F}))$ получается из нижней оценки длины групповой алгебры диэдральной группы в лемме 3.1.1 и утверждения 3.4.1.

Верхнюю оценку $l(A_n(\mathbb{F}) \oplus D_4(\mathbb{F})) \leq 2n+2$ получим с помощью индукции по $n$. Пусть $n = 1$. Длина алгебры $D_4(\mathbb{F})$ в силу тривиальной оценки не более 3. Применяя теорему 3.2.11 при $n = 1$ и $\mathcal{A} = D_4(\mathbb{F})$, получаем оценку $l(M_2(\mathbb{F}) \oplus D_4(\mathbb{F})) \leq 4$ (в силу алгебраической замкнутости поле бесконечно). Предположим,

что $l(A_k(\mathbb{F}) \oplus D_4(\mathbb{F})) \leq 2k+2$. Но нижняя оценка верна для всех $n$, следовательно $l(A_k(\mathbb{F}) \oplus D_4(\mathbb{F})) = 2k+2$. Для завершения индукции докажем, что $l(A_{k+1}(\mathbb{F}) \oplus D_4(\mathbb{F})) \leq 2(k+1)+2$. Заметим, что $\dim(A_k(\mathbb{F}) \oplus D_4(\mathbb{F})) = 4k+4$, а $2l(A_k(\mathbb{F}) \oplus D_4(\mathbb{F}))+2 = 4k+6$. Таким образом, условие леммы 3.2.8 выполнено. Применяя её, получаем $l(A_{k+1}(\mathbb{F}) \oplus D_4(\mathbb{F})) = l(A_k(\mathbb{F}) \oplus D_4(\mathbb{F}) \oplus M_2(\mathbb{F})) \leq l(A_k(\mathbb{F}) \oplus D_4(\mathbb{F}))+2 = 2k+2+2 = 2(k+1)+2$.

□

Для доказательства основного результата нам потребуется следующее утверждение о поведение длины при переходе к расширению поля.

**Теорема 3.4.4** ([2, предложение 3.19])**.** *Пусть $\mathcal{A}$ — конечномерная алгебра с единицей над полем $\mathbb{F}$. Тогда для любого расширения $\mathbb{K}$ поля $\mathbb{F}$ выполняется неравенство $l(\mathcal{A}_{\mathbb{F}}) \leq l(\mathcal{A}_{\mathbb{K}})$.*

Теперь мы готовы доказать сформулированную в начале главы теорему 3.0.1.

*Доказательство.* Рассмотрим 2 случая.

(i) Пусть поле $\mathbb{F}$ алгебраически замкнуто. Тогда в силу утверждения 3.4.1, а также лемм 3.4.2 и 3.4.3 $l(\mathbb{F}\mathcal{D}_{2n+1}) = l(A_n(\mathbb{F}) \oplus D_2(\mathbb{F})) = 2n+1$ и $l(\mathbb{F}\mathcal{D}_{2n+2}) = l(A_n(\mathbb{F}) \oplus D_4(\mathbb{F})) = 2n+2$, то есть $l(\mathbb{F}\mathcal{D}_n) = n$ при $n \geq 3$.

(ii) Пусть теперь поле $\mathbb{F}$ не является алгебраически замкнутым. При переходе от алгебры над исходным полем к алгебре над расширением этого поля (в частности, замыканием этого поля) длина не уменьшается согласно теореме 3.4.4. В силу доказанного в пункте (i) и теоремы 3.4.4 $l(\mathbb{F}\mathcal{D}_n) \leq l(\overline{\mathbb{F}}\mathcal{D}_n) = n$ при $n \geq 3$. В силу леммы 3.1.1 $l(\mathbb{F}\mathcal{D}_n) \geq n$ при $n \geq 3$. □

**Замечание 3.4.5.** Установленный результат позволяет вычислить в полупростом случае длины некоторых групповых алгебр, вычисленные ранее в работах [25, Теорема 3.1] и [26, Теорема 1.3]. Сформулируем это в виде следствий.

**Следствие 3.4.6.** *Пусть $\mathbb{F}$ — поле,* $\operatorname{char}\mathbb{F} \neq 2, 3$. *Тогда $l(\mathbb{F}S_3) = 3$.*

*Доказательство.* Заметим, что существует естественный инъективный гомоморфизм $S_3 \to \mathcal{D}_3$, так как любая подстановка трёх вершин треугольника соответствует их симметрии. Так как группы имеют одинаковый порядок, это изоморфизм. Следовательно из теоремы 3.0.1 следует, что $l(\mathbb{F}S_3) = l(\mathbb{F}\mathcal{D}_3) = 3$. □

**Следствие 3.4.7.** *Пусть* $\mathbb{F}$ *— алгебраически замкнутое поле,* $\operatorname{char}\mathbb{F} \neq 2$. *Тогда* $l(\mathbb{F}Q_8) = 4$.

*Доказательство.* При требуемых условиях на поле, применяя лемму [26, Лемма 5.1] и утверждение 3.4.1, мы получаем следующее разложение:

$$\mathbb{F}Q_8 \cong M_2(\mathbb{F}) \oplus D_4(\mathbb{F}) \cong \mathbb{F}\mathcal{D}_4.$$

Следовательно, из теоремы 3.0.1 следует, что $l(\mathbb{F}Q_8) = l(\mathbb{F}\mathcal{D}_4) = 4$. □

## 3.5 Диэдральные 2-группы над полями характеристики 2

В заключении главы отметим, что длина групповых алгебр диэдральных групп вычеслена для произвольных порядков групп, но с ограничением на поле. Однако для диэдральных 2-групп О.В. Марковой в совместной работе с автором [40, Теорема 4.10] удалось вычислить длину и для полей характеристики 2 (так называемый модулярный случай). Результат будет приведён без доказательства, так как оно не принадлежит автору.

**Теорема 3.5.1.** *Пусть* $\operatorname{char}\mathbb{F} = 2$, $k \geq 2$. *Тогда* $l(\mathbb{F}\mathcal{D}_{2^k}) = 2^k$.

# Глава 4

# Группы малых порядков

*Кто малого не может, тому и большее невозможно.* —*М.В. Ломоносов*

Несмотря на значительные продвижения в области изучения длин групповых алгебр, полный ответ для произвольных групп над произвольными полями не получен ни в случае абелевых, ни в случае диэдральных групп. В этой главе мы сосредоточимся не на изучении длины большой общности групп, напротив, мы получим ответ для весьма конкретных групп над произвольными полями. Изучение длин групповых алгебр групп малых порядков может способствовать развитию новых техник, которые было трудно заметить и разработать при рассмотрении целых семейств групп.

В данной главе мы найдём длины всех групп порядка не более 9. Результаты, представленные в этой главе опубликованы в работах А.Э. Гутермана и О.В. Марковой [25] и [26], а также в совместных с автором работах [38] и [40].

Некоторые результаты главы следуют из общих теорем предыдущих глав работы. Однако мы по возможности не будем на них ссылаться по следующим причинам. С одной стороны, это поможет целостности повествования в этой главе. С другой стороны, приведённые доказательства будут либо иллюстрировать иные подходы к изучению длин, либо иллюстрировать на частных случаях ранее опущенные доказательства общих утверждений.

## 4.1 Абелевы группы

Как было уже показано в главе 2, случай циклических групп тривиален. Нам остаётся рассмотреть группы $G_2 \times G_2$, $G_2 \times G_2 \times G_2$, $G_2 \times G_4$ и $G_3 \times G_3$. Но перед этим обсудим отдельно случай полей нулевой харатеристики.

### 4.1.1 Длина коммутативной групповой алгебры над полем нулевой характеристики

Сразу же отметим, что из теоремы 2.1.2 и того факта, что любое поле нулевой характеристики бесконечно, следует главный результат данной подсекции. Здесь можно было бы переходить к следующей подсекции, однако автору представляется интересным доказательство, независимое от ранее представленных результатов и иллюстрирующее связь между коммутативными групповыми алгебрами и кронекеровским произведением циркулянтов.

Для доказательства основной теоремы подсекции нам понадобится несколько вспомогательных утверждений и понятий.

**Теорема 4.1.1** ([21, глава 12 теорема 3])**.** *Собственными значениями кронекеровского произведения матриц $A$ и $B$ являются произведения $\lambda_i\mu_j$, где $\lambda_i$ и $\mu_j$ – соответственно собственные значения матриц $A$ и $B$.*

**Определение 4.1.2.** Матрица $F_n \in M_n(\mathbb{C})$ называется *матрицей Фурье*, если она имеет вид

$$F_n = [\varepsilon^{kl}],\ 0 \le k, l \le n-1.$$

**Замечание 4.1.3.** Пусть $\mathbb{F}$ поле, содержащее первообразный корень степени $n$ из единицы $\varepsilon$. Обозначим $\bar{F}_n = [\varepsilon^{-kl}]$, $0 \le k, l \le n-1$, и $F_n^* = \bar{F}_n^t$. Тогда непосредственными вычислениями проверяется, что $F_nF_n^* = nE$. В частности, $F_n^{-1} = n^{-1}F_n^*$.

Далее нам понадобятся матрицы специального вида.

**Определение 4.1.4.** Матрица $C_n \in M_n(\mathbb{F})$ называется *циркулянтом*, если каждая следующая её строка является циклическим сдвигом вправо предыдущей.

**Замечание 4.1.5.** Обозначим $P_n^m = \sum_{i=1}^{n-m} E_{i+m,i} + \sum_{j=1}^{m} E_{j,j+n-m}$. Тогда любой циркулянт есть линейная комбинация этих матриц, то есть любой циркулянт есть некий многочлен от $P_n$. И наоборот – любой многочлен от $P_n$ есть некий циркулянт.

**Теорема 4.1.6.** [20, теорема 3.1] *Для любой комплексной циркулянтной матрицы $A$ порядка $n$ с первым столбцом $a$ имеет место разложение $A = n^{-1}F_n^* diag(F_n a)F_n$ Кроме того, для любой диагональной матрицы $D$ матрица $F_n^* D F_n$ есть циркулянт.*

Выведем из последней теоремы непосредственное

**Следствие 4.1.7.** *Пусть дана комплексная циркулянтная матрица $A$ порядка $n$ с первым столбцом $a$. Обозначим $f_A(x) = \sum_{k=0}^{n-1} a_k x^k$. Тогда собственные значения $A$ есть $f_A(\varepsilon_i)$, где $\varepsilon_i$ – $i$-й корень $n$-й степени из единицы, $i = \overline{1,n}$.*

*Доказательство.*

$$0 = \det(A - \lambda E) = \det(n^{-1}F_n^* \mathrm{diag}(F_n a)F_n - n^{-1}F_n^* \lambda E F_n) = \\ = \det(n^{-1}F_n^*(\mathrm{diag}(F_n a) - \lambda E)F_n) = \det(\mathrm{diag}(F_n a) - \lambda E). \quad (8)$$

Но $F_n a = (f_A(\varepsilon_1), \ldots, f_A(\varepsilon_n))$. □

**Теорема 4.1.8.** *Коммутативные групповые алгебры над полями нулевой характеристики имеют длину $n-1$, где $n$ – порядок группы.*

*Доказательство.* Напомним обозначение

$$P_n^m = \sum_{i=1}^{n-m} E_{i+m,i} + \sum_{j=1}^{m} E_{j,j+n-m}.$$

Пусть $\mathbb{F}$ — произвольное поле и пусть $G_n = \langle g \rangle_n$ — циклическая группа порядка $n$. Отображение $\varphi : \mathbb{F}G_n \to C_n(\mathbb{F})$, заданное на $G_n$ по правилу $\varphi(g^k) = P_n^k$ и продолженное на $\mathbb{F}G_n$ по линейности, есть изоморфизм алгебр. Таким образом, любой элемент групповой алгебры циклической группы можно представлять как циркулянтную матрицу.

Любая конечная абелева группа есть прямая сумма конечных циклических. Групповая алгебра прямой суммы групп есть тензорное произведение групповых алгебр слагаемых. В терминах матриц элементы тензорного произведения алгебр

есть кронекеровы произведения элементов тензорных множителей. Теперь мы можем представлять элементы алгебр, как кронекеровы произведения цикрулянтных матриц.

Покажем, что над $\mathbb{Q}$ существует матрица, которая является системой порождающих для $\mathbb{Q}G$. Для этого достаточно найти матрицу, все собственные значения которой различны (то есть степень минимального многочлена равна порядку матрицы). Однопорождённые алгебры заведомо имеют максимальную длину, так как нам наверняка понадобятся степени от нулевой до $\dim \mathcal{A} - 1$, чтобы набрать базис из $\dim \mathcal{A}$ элементов. Если мы покажем, что над $\mathbb{Q}$ рассматриваемые алгебры имеют максимальную длину, то из того факта, что любое поле нулевой характеристики есть расширение $\mathbb{Q}$ и теоремы 3.4.4 будет следовать утверждение теоремы.

С помощью теоремы 4.1.1 и следствия 4.1.7 мы можем легко определять собственные значения матрицы, являющейся кронекеровым произведением циркулянтов. Нам нужно показать, что мы можем подобрать такие матрицы, что собственные значения кронекерова произведения заведомо будут попарно различны.

Далее будем говорить не о циркулянтах, а об определённых в следствии 4.1.7 многочленах $f_A(x)$, которые им однозначно соответствуют. Построим конструкцию индуктивно по количеству множителей в произведении. В качестве базы можно возьмём многочлен $x$ (то есть возьмём ранее описанную матрицу $P_n$, её собственные значения $\mu_i = \varepsilon_i$ действительно различны). Предположение – собственные значения $\lambda_i$ – различны. Шаг – рассмотрим многочлен $C + x$ (то есть собственные значения очередного множителя есть $C + \varepsilon^i$), тогда собственные значения произведения будут $\nu_j = C\lambda_i + \varepsilon^k \lambda_i$. Осталось лишь взять $C$ настолько большое, что расстояния между $C\lambda_i$ для любых $i$ было бы больше $2\lambda_j$ для любого $j$. Пусть $p = \max_i |\lambda_i|$, $q = \min_{i \neq j} |\lambda_i - \lambda_j|$. Возьмём $C$ больше $\frac{2p}{q}$. Тогда $|\nu_j - \nu_l| = |C\lambda_i + \varepsilon^k \lambda_i - C\lambda_s - \varepsilon^t \lambda_s| \geqslant C|\lambda_i - \lambda_s| - |\varepsilon^k \lambda_i| - |\varepsilon^t \lambda_s| \geqslant Cq - p - p > 0$. $\square$

### 4.1.2 2-группы

Для вычисления длин групповых алгебр нам потребуется несколько известных утверждений.

**Теорема 4.1.9** ([2, теорема 4.60]). *Пусть $\mathbb{F}$ — произвольное поле.*
*1. Если $\mathbb{F}$ — бесконечно, то $l(D_n(\mathbb{F})) = n - 1$.*
*2.* $l(D_n(\mathbb{F}_q)) = \begin{cases} n-1, \text{ при } q \geq n; \\ (q-1)[\log_q n] + [q^{\{\log_q n\}}] - 1, \text{ при } q < n. \end{cases}$

**Теорема 4.1.10** ([2, теорема 3.9]). *Пусть $\mathcal{A}$ и $\mathcal{B}$ — конечномерные ассоциативные алгебры над полем $\mathbb{F}$ длин $l_\mathcal{A}$ и $l_\mathcal{B}$, соответственно. Тогда выполнены следующие неравенства:*

$$\max\{l_\mathcal{A}, l_\mathcal{B}\} \leq l(\mathcal{A} \oplus \mathcal{B}) \leq l_\mathcal{A} + l_\mathcal{B} + 1. \tag{9}$$

Приступим к рассмотрению групповых алгебр.

**Утверждение 4.1.11.** *Пусть* $\operatorname{char}\mathbb{F} = 2$, *тогда* $l(\mathbb{F}[G_2 \times G_2]) = 2$.

*Доказательство.* Квадрат любого элемента рассматриваемой алгебры пропорционален единице данной алгебры. Следовательно, алгебра не является однопорожденной и имеет длину не более двух. С другой стороны, она порождается двумя своими элементами $(0,1)$ и $(1,0)$, не являющимися базисом, то есть длина не менее двух. □

**Утверждение 4.1.12.** *Пусть* $\operatorname{char}\mathbb{F} \neq 2$. *Если* $|\mathbb{F}| > 3$, *то* $l(\mathbb{F}[G_2 \times G_2]) = 3$. *Если же* $\mathbb{F} = \mathbb{F}_3$, *то* $l(\mathbb{F}[G_2 \times G_2]) = 2$.

*Доказательство.* Так как $\operatorname{char}\mathbb{F} \neq 2$, алгебра раскладывается в прямую сумму четырёх копий $\mathbb{F}$. Применением теоремы 4.1.9 к $D_4(\mathbb{F})$ получаем требуемое утверждение. □

**Утверждение 4.1.13.** *Пусть* $\operatorname{char}\mathbb{F} = 2$, *тогда* $l(\mathbb{F}[G_2 \times G_2 \times G_2]) = 3$.

*Доказательство.* Вторая степень любого элемента рассматриваемой алгебры пропорциональна единице данной алгебры. При том элемент $(0,0,1)$ имеет минимальный многочлен степени 2. Следовательно, $m(\mathbb{F}[G_2 \times G_2 \times G_2]) = 2$ и по теореме 2.4.8 $l(\mathbb{F}[G_2 \times G_2 \times G_2]) \leqslant 3$. С другой стороны, система порождающих $\{(1,0,0),(0,1,0),(0,0,1)\}$ имеет длину 3. □

**Утверждение 4.1.14.** *Пусть* $\operatorname{char}\mathbb{F} \neq 2$, $G = G_2 \times G_2 \times G_2$. *Тогда*

$$l(\mathbb{F}G) = \begin{cases} 3, \ \textit{при}\ \mathbb{F} = \mathbb{F}_3; \\ 4, \ \textit{при}\ \mathbb{F} = \mathbb{F}_5; \\ 6, \ \textit{при}\ \mathbb{F} = \mathbb{F}_7; \\ 7, \ \textit{в остальных случаях.} \end{cases}$$

*Доказательство.* Так как $\operatorname{char}\mathbb{F} \neq 2$, алгебра раскладывается в прямую сумму восьми копий $\mathbb{F}$. Применением теоремы 4.1.9 к $D_8(\mathbb{F})$ получаем требуемое утверждение. □

Следующий уже менее тривиальный пример — $G_2 \times G_4$. Случай поля нулевой характеристики попадает под теорему 4.1.8, рассмотрим другие случаи.

**Утверждение 4.1.15.** *Пусть* $\operatorname{char}\mathbb{F} = 2$, *тогда* $l(\mathbb{F}[G_2 \times G_4]) = 4$.

*Доказательство.* Четвёртая степень любого элемента рассматриваемой алгебры пропорциональна единице данной алгебры. При том элемент $(0, 1)$ имеет минимальный многочлен степени 4. Следовательно, $m(\mathbb{F}[G_2 \times G_4]) = 4$ и по теореме 2.4.8 $l(\mathbb{F}[G_2 \times G_4]) \leqslant 4$. С другой стороны, система порождающих $\{(0, 1), (1, 0)\}$ имеет длину 4. □

**Утверждение 4.1.16.** $l(\mathbb{F}_3[G_2 \times G_4]) = 6$.

*Доказательство.* Разложим алгебру в прямую сумму полей.

$$\mathbb{F}_3[G_2 \times G_4] = \mathbb{F}_3[G_2][G_4] = (\mathbb{F}_3 \oplus \mathbb{F}_3)[G_4] = \mathbb{F}_3 G_4 \oplus \mathbb{F}_3 G_4 =$$

$$= \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_9 \oplus \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_9 = \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_9 \oplus \mathbb{F}_9$$

Сгруппируем первые 4 слагаемых и последние 2. С помощью теоремы 4.1.9 получаем $l(\mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_3) = 2$. Алгебра же $\mathbb{F}_9 \oplus \mathbb{F}_9$ (будем представлять $\mathbb{F}_9$ как фактор $\mathbb{F}_3[x]$ по идеалу, порождённому $x^2+1$) порождена элементом $u = (x, x+1)$. Действительно, $u^2 = (2, 2x)$, $u^3 = (2x, 2x + 1)$, $u^4 = (1, 2)$. $2u^3 - u = (0, 1)$, что вместе с $u^4$ даст все константы, а значит из $u^2$ можно будет легко получить $(0, x)$, и, наконец, из $u$ получим $(x, 0)$. Следовательно $\mathbb{F}_9 \oplus \mathbb{F}_9$ имеет максимальную длину

3. Согласно теореме 4.1.10 длина прямой суммы двух слагаемых не превосходит суммы длин плюс 1. Таким образом, искомая длина не превосходит 6.

Рассмотрим теперь последние 5 слагаемых. 7-мерная алгебра $\mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_9 \oplus \mathbb{F}_9$ порождается элементом $(0, 1, 2, x, x+1)$. Рассмотрим многочлены $t^2+1$ и $t^2+t+2$ аннулирующие соответственно четвертую и пятую координаты. Применяя их произведение получим элемент $(0, 1, 2, 0, 0)$, из которого получаются второй и третий орты, а также элемент $(0, 0, 0, x, x+1)$, степени которого порождают подалгебру последних двух координат. Таким образом, $l(\mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_9 \oplus \mathbb{F}_9) = 6$. Согласно той же теореме 4.1.10 длина прямой суммы двух слагаемых не меньше максимума длин слагаемых, то есть не меньше 6.

□

**Утверждение 4.1.17.** $l(\mathbb{F}_5[G_2 \times G_4]) = 4$.

*Доказательство.* Разложим алгебру в прямую сумму полей.

$$\mathbb{F}_5[G_2 \times G_4] = \mathbb{F}_5[G_2][G_4] = (\mathbb{F}_5 \oplus \mathbb{F}_5)[G_4] = \mathbb{F}_5 G_4 \oplus \mathbb{F}_5 G_4 =$$

$$= \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5 = D_8(\mathbb{F}_5)$$

По теореме 4.1.9 $l(\mathbb{F}_5[G_2 \times G_4]) = 4$.

□

**Утверждение 4.1.18.** *Пусть* $p = 4k-1 > 3$. $\mathbb{F}$ *— поле характеристики* $p$. *Тогда* $l(\mathbb{F}[G_2 \times G_4]) = 7$.

*Доказательство.* Рассмотрим в поле $\mathbb{F}$ подполе $\mathbb{F}_p$. Докажем, что $l(\mathbb{F}_p[G_2 \times G_4]) = 7$, тогда и при возвращении к расширению поля длина не уменьшится, следовательно, останется максимальной. Разложим алгебру в прямую сумму полей. Так как при данном $p$ $x^2-1$ и $x^4-1$ над $\mathbb{F}_p$ раскладываются на неприводимые точно так же, как и в случае $\mathbb{F}_3$ (а именно $(x+1)(x-1)$ и $(x+1)(x-1)(x^2+1)$ соответственно), мы получим такой же результат.

$$\mathbb{F}_p[G_2 \times G_4] = \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_{p^2} \oplus \mathbb{F}_{p^2}$$

Докажем, что данная алгебра порождается элементом $u = (0, 1, 2, 3, x, x + 1)$. Применим к элементу многочлен $t(t - 1)(t - 2)(t - 3)$. Результатом будет являться $(0, 0, 0, 0, a, b)$, где $a, b$ — некоторые ненулевые элементы поля. Возведем этот результат в степень $p - 1$, получим $v = (0, 0, 0, 0, 1, 1)$. Степенями $uv = (0, 0, 0, 0, x, x + 1)$ породим подалгебру пятой и шестой координат (это заведомо возможно, так как минимальные многочлены элементов $x$ и $x + 1$ квадратичны и взаимно просты, а значит минимальный многочлен $uv$ имеет степень 4). Далее получим элемент $(0, 1, 2, 3, 0, 0)$ и породим всё оставшееся. □

**Утверждение 4.1.19.** *Пусть $p = 4k+1 > 5$. $\mathbb{F}$ — поле характеристики $p$. Тогда $l(\mathbb{F}[G_2 \times G_4]) = 7$.*

*Доказательство.* Рассмотрим в поле $\mathbb{F}$ подполе $\mathbb{F}_p$. Докажем, что $l(\mathbb{F}_p[G_2 \times G_4]) = 7$, тогда и при возвращении к расширению поля длина не уменьшится, следовательно, останется максимальной. Разложим алгебру в прямую сумму полей. Так как при данном $p$ $x^4 - 1$ над $\mathbb{F}_p$ раскладываются на линейные множители, мы получим следующее разложение

$$\mathbb{F}_p[G_2 \times G_4] = \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p = D_8(\mathbb{F}_p)$$

По теореме 4.1.9 $l(\mathbb{F}[G_2 \times G_4]) = 7$. □

**Теорема 4.1.20.** *Пусть $G = G_2 \times G_4$. Тогда*

$$l(\mathbb{F}G) = \begin{cases} 4, & \text{при } \operatorname{char}\mathbb{F} = 2 \text{ или } \mathbb{F} = \mathbb{F}_5; \\ 6, & \text{при } \mathbb{F} = \mathbb{F}_3; \\ 7, & \text{в остальных случаях.} \end{cases}$$

*Доказательство.* Отметим, что большинство случаев уже рассмотрено в предыдущих утверждениях. Осталось рассмотреть алгебры над полями характеристик 3 и 5, не являющихся простыми. В этом случае мощность поля не менее 9-и. Обозначим квадратичное расширение поля $\mathbb{F}$ символом $\mathbb{F}^2$. Снова разложим алгебру в прямую сумму полей. В зависимости от разложения на неприводимые множители многочлена $x^4 - 1$ над $\mathbb{F}$ возможны два случая.

$$\mathbb{F}[G_2 \times G_4] = \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F}^2 \oplus \mathbb{F}^2$$

либо

$$\mathbb{F}[G_2 \times G_4] = \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F}$$

В каждом из случаев можно применить рассуждение из доказательства одного из предыдущих утверждений и получить вывод о максимальности длины в этих случаях. □

### 4.1.3 3-группы

**Утверждение 4.1.21.** *Пусть* $\operatorname{char}\mathbb{F} = 3$*, тогда* $l(\mathbb{F}[G_3 \times G_3]) = 4$*.*

*Доказательство.* Третья степень любого элемента рассматриваемой алгебры пропорциональна единице данной алгебры. При том элемент $(0,1)$ имеет минимальный многочлен степени 3. Следовательно, $m(\mathbb{F}[G_3 \times G_3]) = 3$ и по теореме 2.4.8 $l(\mathbb{F}[G_3 \times G_3]) \leqslant 4$. С другой стороны, система порождающих $\{(0,1),(1,0)\}$ имеет длину 4. □

Для полупростого случая мы сформулируем и докажем общее утверждение для 3 групп, с помощью которого будет вычислена длина для частного случая группы $G_3 \times G_3$. Для этого нам понадобится несколько вспомогательных понятий и утверждений.

Напомним поятие *функции Мёбиуса*. Это функция $\mu : \mathbb{N} \to \mathbb{Z}_+$, определённая следующими условиямиs:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1 \\ (-1)^k, & \text{если } n \text{ равно произведению } k \text{ различных простых чисел} \\ 0, & \text{если } n \text{ делится на квадрат простого числа.} \end{cases}$$

**Теорема 4.1.22** ([24, Глава 3, Теорема 3.25])**.** *Количество* $N_q(n)$ *приведённых неприводимых многочленов степени* $n$ *над* $\mathbb{F}_q$ *вычисляется по следующей форму-*

*ле:*

$$N_q(n) = \frac{1}{n}\sum_{d|n}\mu(d)q^{\frac{n}{d}} = \frac{1}{n}\sum_{d|n}\mu(\frac{n}{d})q^d.$$

**Обозначение 4.1.23.** $U_{m,N} := (m-1)[\log_m N] + [m^{\{\log_m N\}}] - 1$

Доказательство следующего утверждения опубликовано в совместной статье автора с А.Э. Гутерманом и О.В. Марковой [38], но не принадлежит автору.

**Утверждение 4.1.24.** *Пусть $p, n \in \mathbb{N}$, $n \geq 2$ и $p$ — нечётное простое число. Рассмотрим элементарную абелеву $p$-группу $G$ порядка $N = p^n$. Пусть $\mathbb{F}_q$ — конечное поле порядка $q \leq p^n - 1$, $\operatorname{char}\mathbb{F} \neq p$ и $p \nmid (q-1)$. Обозначим $m = q^d$, где $d = \min\{j \in \mathbb{N} : q^j \equiv 1(\mod p)\}$, иными словами, $d$ — порядок элемента $q$ в мультипликативной группе $\mathbb{F}_p^*$. В частности, $1 < d \leq p-1$.*

*1. Если $N_q(d) \geq \dfrac{p^n-1}{d}$, то $l(\mathbb{F}_q G) = p^n - 1$.*

*2. Если $N_q(d) < \dfrac{p^n-1}{d}$, то $d \cdot N_q(d) \leq l(\mathbb{F}_q G) \leq U_{m,N}$.*

Из этого утверждения выведем следствие для 3-групп.

**Следствие 4.1.25.** *Пусть $n \in \mathbb{N}$, $n \geq 2$. Рассмотрим элементарную абелеву 3-группу порядка $N = 3^n$. Пусть $\mathbb{F}_q$ — конечное поле порядка $q \leq 3^n - 1$, $\operatorname{char}\mathbb{F}_q \neq 3$.*

*1. Если $q = 3k+1$, то $l(\mathbb{F}_q G) = U_{q,N}$.*

*2. Если $q = 3k+2$ и $q^2 - q \geq 3^n - 1$, то $l(\mathbb{F}_q G) = 3^n - 1$.*

*3. Если $q = 3k+2$ и $q^2 - q < 3^n - 1$, то $q^2 - q \leq l(\mathbb{F}_q G) \leq U_{q^2,N}$.*

*Доказательство.* 1. Если $q = 3k+1$, то $3|(q-1)$ и первый пункт следует из теоремы 2.2.2.

2. Рассмотрим $m = q^d$ и $d = \min\{j \in \mathbb{N} : q^j \equiv 1(\mod 3)\}$ из утверждения 4.1.24. Если $q = 3k+2$, то $q \equiv -1(\mod 3)$, следовательно $d = \min\{j \in \mathbb{N} : (-1)^j \equiv 1(\mod 3)\} = 2$ и $m = q^2$. Из теоремы 4.1.22 получаем $N_q(d) = \dfrac{q^2-q}{2}$. Тогда второй и третий пункты следуют из утверждения 4.1.24. □

**Утверждение 4.1.26.** *Пусть* $\operatorname{char}\mathbb{F} \neq 3$, $G = G_3 \times G_3$. *Тогда*

$$l(\mathbb{F}G) = \begin{cases} 4, \ \textit{при } \mathbb{F} = \mathbb{F}_2 \textit{ или } \mathbb{F} = \mathbb{F}_4; \\ 6, \ \textit{при } \mathbb{F} = \mathbb{F}_7; \\ 8, \ \textit{в остальных случаях.} \end{cases}$$

*Доказательство.* Система порождающих $\{(0,1),(1,0)\}$ имеет длину 4, следовательно $l(\mathbb{F}G) \geq 4$.

Поле $\mathbb{F}_2$ удовлетворяет третьему пункту следствия 4.1.25, следовательно $l(\mathbb{F}_2 G) \leq U_{4,9} = 4$.

Поле $\mathbb{F}_4$ удовлетворяет первому пункту следствия 4.1.25, следовательно $l(\mathbb{F}_4 G) = U_{4,9} = 4$.

Поле $\mathbb{F}_5$ удовлетворяет второму пункту следствия 4.1.25, следовательно $l(\mathbb{F}_5 G) = 8$.

Поле $\mathbb{F}_7$ удовлетворяет первому пункту следствия 4.1.25, следовательно $l(\mathbb{F}_7 G) = U_{7,9} = 6$.

Поле $\mathbb{F}_8$ удовлетворяет второму пункту следствия 4.1.25, следовательно $l(\mathbb{F}_8 G) = 8$.

Оставшиеся поля имеют порядок больший, чем порядок группы, следовательно по теореме 2.2.1 длина алгебры для оставшихся полей равна восьми.

□

### 4.1.4 Итог секции про малые абелевы группы

Получен полный ответ для всех малых абелевых групп. Для наглядности соберём все полученные результаты в таблицу, где на пересечении строки с группой и столбца с полем будет стоять длина соответствующей групповой алгебры.

| Группа\Поле | $\mathbb{F}_2$ | $\mathbb{F}_3$ | $\mathbb{F}_4$ | $\mathbb{F}_5$ | $\mathbb{F}_7$ | $\mathbb{F}_8$ | $\lvert\mathbb{F}\rvert \geq 9$, $\operatorname{char}\mathbb{F} \nmid \lvert G\rvert$ | $\lvert\mathbb{F}\rvert \geq 9$, $\operatorname{char}\mathbb{F} \mid \lvert G\rvert$ |
|---|---|---|---|---|---|---|---|---|
| $G_1$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - |
| $G_2$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $G_3$ | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| $G_4$ | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| $G_2 \times G_2$ | 2 | 2 | 2 | 3 | 3 | 2 | 3 | 2 |
| $G_5$ | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| $G_6$ | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| $G_7$ | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| $G_8$ | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| $G_2 \times G_2 \times G_2$ | 3 | 3 | 3 | 4 | 6 | 3 | 7 | 3 |
| $G_2 \times G_4$ | 4 | 6 | 4 | 4 | 7 | 4 | 7 | 4 |
| $G_9$ | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| $G_3 \times G_3$ | 4 | 4 | 4 | 8 | 6 | 8 | 8 | 4 |

В частности, на этой таблице можно наглядно увидеть отсутствие монотонности функции длины, как по порядку группы, так и по мощности поля, даже если говорить только о нециклических группах в полупростом случае.

## 4.2 Неабелевы группы

Так как $\mathcal{D}_3 \cong S_3$, неабелевы группы малых порядков представлены тремя группами: симметрической группой $S_3$, группой кватернионов $Q_8$ и диэдральной группой $\mathcal{D}_4$.

### 4.2.1 Симметрическая группа

В следствии 3.4.6 установлено, что в полупростом случае длина симметрической группы порядка 6 равна трём. Оказывается, это верно и в общем случае. Этот результат получен в ранее упомянутой статье А.Э. Гутермана и О.В. Марковой [25].

**Теорема 4.2.1** ([25, Теорема 3.1]). *Пусть* $\mathbb{F}$ *— произвольное поле. Тогда* $l(\mathbb{F}S_3) = 3$.

### 4.2.2 Группа кватернионов

В следствии 3.4.7 установлено, что алгебраически замкнутых полей характеристики отличной от двух длина группы кватернионов равна четырём. Оказывается, для других полей длина может отличаться. Следующий результат получен в ранее упомянутой статье А.Э. Гутермана и О.В. Марковой [26].

**Теорема 4.2.2** ([26]). *Пусть* $\mathbb{F}$ *— произвольное поле. Тогда*

*1.* $l(\mathbb{F}Q_8) = 4$, *если* $\operatorname{char}\mathbb{F} \neq 2$ *и в поле* $\mathbb{F}$ *существуют элементы* $\alpha$, $\beta$, *такие, что* $\alpha^2 + \beta^2 = -1$;

*2.* $l(\mathbb{F}Q_8) = 3$, *в остальных случаях.*

### 4.2.3 Диэдральная группа

Из теоремы 3.0.1 следует, что в полупростом случае $l(\mathbb{F}\mathcal{D}_4) = 4$.

Из ранее упомянутой теоремы 3.5.1 из работы [40] следует, что и в модулярном случае $l(\mathbb{F}\mathcal{D}_4) = 4$. Однако мы в этой подсекции приведём альтернативное доказательство этого факта, опубликованное в той же работе [40], содержащее вычисление максимальной степени минимального многочлена элемента алгебры и применение оценки из леммы 3.3.1.

Далее в данной подсекции $\mathbb{F}$ — поле характеристики 2, если не оговорено обратное. Пусть $r$ — поворот на угол $\frac{\pi}{2}$, а $s$ — симметрия вокруг некоторой оси. Тогда $S_0 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$ — стандартный базис алгебры $\mathbb{F}\mathcal{D}_4$, состоящий из элементов группы $\mathcal{D}_4$. Рассмотрим базис $S = \{e, r^2, r + r^3, s + sr^2, sr + sr^3, r^3, sr^2, sr^3\}$. Обозначим $S_c$ множество $\{e, r^2, r+r^3, s+sr^2, sr+sr^3\}$. Обозначим $S_{nc}$ множество $\{r^3, sr^2, sr^3\}$. Обозначим $\langle S\rangle$ за $L$, $\langle S_c\rangle$ за $L_c$, $\langle S_{nc}\rangle$ за $L_{nc}$. Тогда $L = L_c \oplus L_{nc}$, $L = \mathbb{F}\mathcal{D}_4$ как множества. Заметим, что $L_c$ лежит в центре алгебры $\mathbb{F}\mathcal{D}_4$ (даже если $\mathbb{F}$ имеет произвольную характеристику).

**Утверждение 4.2.3.** *Пусть* $v \in L_c$. *Тогда* $v^2 \in \langle e\rangle$.

*Доказательство.* По условию $v = \lambda_1 e + \lambda_2 r^2 + \lambda_3(r + r^3) + \lambda_4(s + sr^2) + \lambda_5(sr + sr^3)$. Тогда в силу коммутативности $L_c$ и того, что $\operatorname{char}\mathbb{F} = 2$, получаем, что $v^2 = \lambda_1^2 e^2 + \lambda_2^2 (r^2)^2 + \lambda_3^2 (r + r^3)^2 + \lambda_4^2 (s + sr^2)^2 + \lambda_5^2 (sr + sr^3)^2$. Но $e^2 = e$, $(r^2)^2 = e$, $(r + r^3)^2 = r^2 + 2e + r^2 = 0$, $(s + sr^2)^2 = e + 2r^2 + e = 0$, $(sr + sr^3)^2 = e + 2r^2 + e = 0$. Таким образом, $v^2 \in \langle e \rangle$. □

**Утверждение 4.2.4.** *Пусть $v \in L_{nc}$. Тогда $v^2 \in L_c$.*

*Доказательство.* По условию $v = \lambda_1 r^3 + \lambda_2 sr^2 + \lambda_3 sr^3$. Тогда $v^2 = \lambda_1^2 (r^3)^2 + \lambda_2^2 (sr^2)^2 + \lambda_3^2 (sr^3)^2 + \lambda_1\lambda_2 (r^3 sr^2 + sr^2 r^3) + \lambda_1\lambda_3 (r^3 sr^3 + sr^3 r^3) + \lambda_2\lambda_3 (sr^2 sr^3 + sr^3 sr^2)$. Но $(r^3)^2 = r^2$, $(sr^2)^2 = e$, $(sr^3)^2 = e$, $r^3 sr^2 + sr^2 r^3 = sr^3 + sr$, $r^3 sr^3 + sr^3 r^3 = s + sr^2$, $sr^2 sr^3 + sr^3 sr^2 = r + r^3$. Таким образом, $v^2 \in L_c$. □

**Утверждение 4.2.5.** *Пусть $v \in L$. Тогда $v^2 \in L_c$.*

*Доказательство.* По условию $v = v_c + v_{nc}$, где $v_c \in L_c$, $v_{nc} \in L_{nc}$. Тогда $v^2 = v_c^2 + v_c v_{nc} + v_{nc} v_c + v_{nc}^2$. В силу того, что $L_c$ лежит в центре $L$ и $\operatorname{char}\mathbb{F} = 2$, получаем $v_c v_{nc} + v_{nc} v_c = 2 v_c v_{nc} = 0$. Согласно утверждению 4.2.3, имеем $v_c^2 \in \langle e \rangle \in L_c$. В силу утверждения 4.2.4 $v_{nc}^2 \in L_c$. Следовательно, $v^2 \in L_c$. □

**Утверждение 4.2.6.** *Пусть $v \in L$. Тогда $v^4 \in \langle e \rangle$.*

*Доказательство.* По условию $v \in L$. Тогда в силу утверждения 4.2.5 $v^2 \in L_c$. Следовательно, из утверждения 4.2.3 получаем, что $(v^2)^2 \in \langle e \rangle$. Таким образом, $v^4 \in \langle e \rangle$. □

**Лемма 4.2.7.** *Пусть* $\operatorname{char}\mathbb{F} = 2$. *Тогда $m(\mathbb{F}\mathcal{D}_4) = 4$.*

*Доказательство.* Покажем сначала, что $m(\mathbb{F}\mathcal{D}_4) \geq 4$. Действительно, минимальным многочленом $r$ является $t^4 - 1$.

Покажем, что $m(\mathbb{F}\mathcal{D}_4) \leq 4$. Действительно, пусть $v \in \mathbb{F}\mathcal{D}_4 = L$. Тогда в силу утверждения 4.2.6, $v^4 = \lambda e$. Таким образом, многочлен $t^4 - \lambda$ является аннулирующим для $v$ и $m(v) \leq 4$. В силу произвольности выбора $v$ получаем требуемое неравенство, что завершает доказательство леммы. □

**Теорема 4.2.8.** *Пусть* $\operatorname{char}\mathbb{F} = 2$. *Тогда $l(\mathbb{F}\mathcal{D}_4) = 4$.*

*Доказательство.* В силу леммы 3.1.1, получаем $l(\mathbb{F}\mathcal{D}_4) \geq 4$. По лемме 4.2.7 $m(\mathbb{F}\mathcal{D}_4) = 4$, кроме того $\dim \mathbb{F}\mathcal{D}_4 = 8$. Таким образом, алгебра $\mathbb{F}\mathcal{D}_4$ удовлетворяет условиям леммы 3.3.1, применяя которую, получаем оценку $l(\mathbb{F}\mathcal{D}_4) \leq m(\mathbb{F}\mathcal{D}_4) = 4$. □

Таким образом получен полный ответ для всех малых групп над произвольными полями.

# Заключение

В ходе работы проведёно большое исследование длин групповых алгебр. Получены значения длин для довольно широких классов групп. В ходе изучения длин групповых алгебр доказаны верхние оценки функции длины, применение которых может выходить за рамки случая групповых алгебр, как, например, в разделе 3.3. Разработаны различные техники работы с алгебрами как групповыми, так и матричными. Тем не менее существует большой простор для дальнейших исследований.

Как уже было отмечено, в полупростом случае для коммутативных групповых алгебр задача нахождения длины не решена полностью только для маленьких полей. Несмотря на то, что в главе 4 показан пример рассмотрения алгебр, не покрываемых теоремами главы 2, нахождение ответа на вопрос о длине над произвольными малыми полями в этом случае представляется автору весьма трудной задачей.

В модулярном случае для коммутативных групповых алгебр задача нахождения длины решена в общем виде для $p$-групп и групп, являющихся прямым произведением циклической группы и циклической $p$-группы. Для остальных групп доказаны верхние и нижние оценки.

В случае некоммутативных алгебр длина вычислена для диэдральных групп произвольного порядка в полупростом случае. Следующее, над чем стоит подумать с точки зрения данной работы — длина $\mathbb{F}\mathcal{D}_n$ в модулярном случае. Но и в полупростом случае задача оказывается весьма непростой, ведь разложение групповой алгебры в прямую сумму полных матричных алгебр эффективно, если известна длины матричных алгебр. Однако в общем случае гипотеза Паза о длине $M_n(\mathbb{F})$ не доказана. А следовательно и получать какие-либо общие утверждения о длине некоммутативных групповых алгебр с помощью данного подхода пока не представляется возможным (но это, конечно, не единственная сложность). Вообще говоря, вполне возможно, что именно рассмотрение групповых алгебр поможет доказать гипотезу Паза, а не наоборот, чем отчасти и вызван интерес к ним.

# Список литературы


[1] I. Schur, Zur theorie der vertauschbären matrizen, J. Reine Angew. Math., **130**(1905), 66–76.

[2] О. В. Маркова, Функция длины и матричные алгебры, Фундамент. и прикл. матем. 17:6 (2012), 65–173.

[3] L. Babai, Á. Seress, On the diameter of permutation groups. European J. Combin. **13**:4 (1992), 231–243.

[4] A. J. M. Spencer, R. S. Rivlin, The theory of matrix polynomials and its applications to the mechanics of isotropic continua, Arch. Ration. Mech. Anal., **2**(1959), 309–336.

[5] A. J. M. Spencer, R. S. Rivlin, Further results in the theory of matrix polynomials, Arch. Ration. Mech. Anal., **4**(1960), 214–230.

[6] C. J. Pappacena, An upper bound for the length of a finite-dimensional algebra, J. Algebra, **197**(1997), 535–545.

[7] A. Paz, An Application of the Cayley–Hamilton theorem to matrix polynomials in several variables, Linear and Multilinear Algebra, **15**(1984), 161–170.

[8] М.М. Глухов, А.Ю. Зубов, О длинах симметрических и знакопеременных групп подстановок в различных системах образующих (обзор), Математические вопросы кибернетики. Вып. 8. – М.: Наука, 1999. – С. 5–32.

[9] Д. А. Супруненко, Р. И. Тышкевич, Перестановочные матрицы. 2-е изд. М.: УРСС, 2003.

[10] N. Jacobson, Schur's theorems on commutative matrices, Bull. Am. Math. Soc., **50**(1944), 431–436.

[11] M. Gerstenhaber, On dominance and varieties of commuting matrices, Ann. Math., **73** (1961), Issue 2, 324–348.

[12] H.A. Helfgott, Growth and expansion in algebraic groups over finite fields, Contemporary Mathematics, **740** (2019), 71–111.

[13] W. E. Longstaff, Burnside's theorem: irreducible pairs of transformations, Linear Algebra Appl., **382**(2004), 247–269.

[14] W.E. Longstaff, P. Rosenthal, On the lengths of irreducible pairs of complex matrices, Proc. Am. Math. Soc., **139**:11(2011), 3769–3777.

[15] T. J. Laffey, Simultaneous reduction of sets of matrices under similarity, Linear Algebra Appl., **84**(1986), 123–138.

[16] D. Constantine, M. Darnall, Lengths of finite dimensional representations of PWB algebras, Linear Algebra Appl., **395**(2005), 175–181.

[17] Ю.А. Альпин, Х.Д. Икрамов, Об унитарном подобии матричных семейств, Матем. заметки, **74**:6 (2003), 815–826.

[18] Yu.A. Al'pin, Kh.D. Ikramov, Reducibility theorems for pairs of matrices as rational criteria, Linear Algebra Appl., **313**(2000), 155–161.

[19] О.В. Маркова, Функция длины и одновременная триангулизуемость пар матриц, Зап. научн. сем. ПОМИ, **514**(2022), 126–137.

[20] В. В. Воеводин, Е. Е. Тыртышников, Вычислительные процессы с теплицевыми матрицами, Москва: Наука, 1987.

[21] Р. Беллман, Теория Матриц, Мир, 1972.

[22] Р. Пирс, Ассоциативные алгебры, Москва: Мир, 1986.

[23] Э. Б. Винберг, Курс Алгебры, Москва: Факториал Пресс, 2001.

[24] R. Lidl, H. Niederreiter, Finite fields, Cambridge University Press, Cambridge, 1996.

[25] А.Э. Гутерман, О.В. Маркова, Длина групповых алгебр групп небольшого размера, Зап. научн. сем. ПОМИ, **472**(2018), 76–87; English transl. in J. Math. Sci. (N. Y.), **240**:6 (2019), 754–761.

[26] A. E. Guterman, O. V. Markova, The length of the group algebra of the group $\mathbf{Q}_8$, New Trends in Algebra and Combinatorics. Proceedings of the 3rd International Congress in Algebra and Combinatorics (Ed. by K.P. Shum, E. Zelmanov, P. Kolesnikov, A. Wong), World Sci., Singapore, (2019), 106–134.

[27] О. В. Маркова, *Пример вычисления длины групповой алгебры нециклической абелевой группы в модулярном случае.* — Фунд. прикл. матем., **23**:2 (2020), 217–229.

[28] S. A. Jennings, The structure of the group ring of a $p$-group over a modular field, Trans. Amer. Math. Sot. **50** (1941), 175–185.

[29] S. Perlis, G. L. Walker, Abelian group algebras of finite order, Trans. Amer. Math. Soc., **68**:3 (1950), 420–426.

[30] Ya. Shitov, An improved bound for the lengths of matrix algebras. — Algebra Number Theory **13**, No. 6 (2019), 1501–1507.

[31] A. E. Guterman, T. Laffey, O. V. Markova, H. Smigoc, A resolution of Paz's conjecture in the presence of a nonderogatory matrix. — Linear Algebra Appl. **543** (2018), 234–250.

[32] О. В. Маркова, Верхняя оценка длины коммутативных алгебр, Матем. сб., **200**:12 (2009), 41–62; English transl. in Sb. Math., **200**:12 (2009), 1767–1787.

[33] О. В. Маркова, О связи длины алгебры и индекса нильпотентности ее радикала Джекобсона, Матем. заметки, **94**:5 (2013), 682–688; English transl. in Math. Notes, **94**:5 (2013), 636–641.

[34] D. S. Passman, The algebraic structure of group rings, John Wiley & Sons, New York, London, Sydney, Toronto, 1977.

[35] A. Wadsworth, The algebra generated by two commuting matrices, Linear and Multilinear Algebra, **27**(1990), 159–162.

[36] W. C. Brown, F. W. Call, Maximal commutative subalgebras of $n \times n$ Matrices, Communications in Algebra, **21(12)**(1993), 4439–4460.

# Публикации автора по теме диссертации

## Статьи в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5 «Математическая логика, алгебра, теория чисел и дискретная математика»


[37] Guterman A., Khrystik M., Markova O., On the lengths of group algebras of finite abelian groups in the modular case, Journal of Algebra and its Applications, **21**:6 (2022), 2250117–2250130. М.А. Хрыстиком доказано следствие 3.10.

DOI: 10.1142/S0219498822501171

Журнал индексируется в **Scopus**. IF: SJR 0.538.

[38] Guterman A., Markova O., Khrystik M., On the lengths of group algebras of finite abelian groups in the semi-simple case, Journal of Algebra and its Applications, **21**:7 (2022), 2250140–2250153. М.А. Хрыстиком доказаны следствия 3.8, 3.11 и теорема 3.16.

DOI: 10.1142/S0219498822501407

Журнал индексируется в **Scopus**. IF: SJR 0.538.

[39] Khrystik M.A., Markova O.V., On the length of the group algebra of the dihedral group in the semi-simple case, Communications in Algebra, **50**:5 (2022), 2223–2232. М.А. Хрыстиком доказаны теорема 1.15, леммы 3.5, 3.7, 3.9, 4.2 и 4.3.

DOI: 10.1080/00927872.2021.2003810

Журнал индексируется в **Scopus**. IF: SJR 0.642.

[40] Маркова О. В., Хрыстик М. А., Длина групповой алгебры группы диэдра порядка $2^k$, Записки научных семинаров ПОМИ, **496**(2020), 169–181;

English transl.:

Markova O.V., Khrystik M.A., Length of the group algebra of the dihedral group of order $2^k$, Journal of Mathematical Sciences. (N. Y.), **255**:3 (2021), 324–331.

DOI: 10.1007/s10958-021-05375-6

Журнал индексируется в **Scopus**. IF: SJR 0.357.

# Другие публикации

[41] Хрыстик М. А., Длина групповой алгебры прямого произведения циклической группы и циклической p-группы в модулярном случае, Записки научных семинаров ПОМИ, **524**(2023), 166–176.

http://ftp.pdmi.ras.ru/pub/publicat/znsl/v524/p166.pdf

Журнал индексируется в **RSCI**. IF: 0.157.