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

М.А. Хрыстик*

УДК 512.552.7
MSC 16S34

Аннотация

В данной работе вычислена длина групповой алгебры прямого произведения циклической группы и элементарной абелевой p-группы над полем характеристики p.

Ключевые слова: Конечномерные алгебры, длина алгебры, групповые алгебры, абелевы группы, p-группы.

M.A. Khrystik, Length of the group algebra of the direct product of a cyclic group and an elementary abelian p-group in the modular case.

In this paper, the length of the group algebra of the direct product of a cyclic group and an elementary abelian p-group over a field of characteristic p is calculated.

Keywords: Finite-dimensional algebras, length of an algebra, group algebras, abelian groups, p-groups.

1 Введение

Все рассматриваемые в работе алгебры — **ассоциативные конечномерные алгебры с единицей над полями**. Важную роль в изучении конечномерных алгебр играет такая числовая характеристика алгебры, как *длина*.

Пусть $\mathcal{A}$ — алгебра. Любое произведение конечного числа элементов конечного подмножества $\mathcal{S} \subset \mathcal{A}$ является словом над алфавитом $\mathcal{S}$. Длина слова равна количеству букв в этом произведении, отличающихся от $1_{\mathcal{A}}$. Будем считать $1_{\mathcal{A}}$ пустым словом длины 0.

Если $\mathcal{S}$ — система порождающих алгебры $\mathcal{A}$, то есть $\mathcal{A}$ — минимальная подалгебра $\mathcal{A}$, содержащая $\mathcal{S}$, то любой элемент алгебры $\mathcal{A}$ может быть

*1. Национальный исследовательский университет «Высшая школа экономики», Москва; E-mail: good_michael@mail.ru

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 $l(\mathcal{A})$ (подробнее см. определение 2.5). В определении длины алгебры $\mathcal{A}$ мы рассматриваем множество **всех** порождающих систем для $\mathcal{A}$. Этим объясняется сложность вычисления длины даже для классических алгебр.

В общей формулировке проблема вычисления длины впервые была сформулирована А. Пазом в 1984 году для полной алгебры матриц $M_n(\mathbb{F})$ над полем в работе [12] и до сих пор является открытой. Существует гипотеза, состоящая в том, что длина полной матричной алгебры равна $2n-2$, где n — порядок матриц. Известно, что эта гипотеза верна при $n = 2, 3, 4, 5$. Вычисление длины в общем случае является довольно трудной задачей. Нетривиальная верхняя оценка длины произвольной алгебры получена в работе К. Паппачены [11] в виде функции от двух других ее числовых характеристик — размерности и максимальной степени минимального многочлена элемента алгебры. Основные алгебраические свойства функции длины были изучены О.В. Марковой в работе [10].

Отдельный интерес представляет вопрос вычисления длины групповых алгебр. Ввиду наличия их матричных представлений, решение этого вопроса тесно связано и с решением проблемы Паза. Для групповых алгебр групп малых порядков удается 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 [2, 3].

Систематическому изучению общей задачи нахождения длины групповых алгебр конечных абелевых групп посвящены работы [4, 1]. В работе [1] для получения оценки длины групповых алгебр использованы методы теории полей, теории колец и оценка длины коммутативных алгебр (см. теорема 6.1). В той же работе вычисление длины групповой алгебры абелевой p-группы сведено к вычислению длины фактор-алгебры по радикалу Джекобсона и индекса нильпотентности радикала.

Аналогичное исследование всех неабелевых групп представляется слишком трудным ввиду разнообразия их структуры. Поэтому предлагается исследование функции длины отдельно для семейств классических неабелевых групп. Так, в работе [7] начато исследование длины групповых алгебр диэдральных групп, вычислена длина в полупростом случае. 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 [6] результат о длине групповых алгебр диэдральных групп обобщен на модулярный случай для 2-групп, то есть над полями характеристики 2.

Изучение абелевых групп в модулярном случае было продолжено в статье [9], где была вычислена длина групповой алгебры нециклической абелевой группы порядка $2p^2$ над полем характеристики $p > 2$. Затем в работе [5] была вычислена длина групповой алгебры прямого произведения циклической группы и циклической p-группы над полем характеристики $p > 0$. Данная работа продолжает исследования в этом направлении и обобщает результат работы [9].

В разделе 2 приведены основные определения и обозначения, используемые в работе.

В разделе 3 приведены некоторые известные на данный момент результаты о длине групповых алгебр абелевых групп в модулярном случае. Сформулирован основной результат работы — теорема 3.6, которая содержит значение длины групповой алгебры прямого произведения циклической группы и элементарной абелевой p-группы над полем характеристики p.

Раздел 4 посвящен нижней оценке длины рассматриваемой алгебры.

Раздел 5 посвящен разработке техники, с помощью которой будет доказана верхняя оценка длины рассматриваемой алгебры.

В разделе 6 иллюстрируется, что техника, разработанная в разделе 5, обобщает технику, которая ранее использовалась при работе с длинами коммутативных алгебр.

Раздел 7 содержит доказательство верхней оценки длины групповой алгебры прямого произведения циклической группы и элементарной абелевой p-группы над полем характеристики p, которым завершается доказательство основного результата работы.

Раздел 8 содержит обобщениние основного результата работы над достаточно большими совершенными полями.

2 Основные определения

Сперва напомним основные определения, связанные с функцией длины.

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 — свободный моноид над алфавитом B, т.е. B^* с операцией конкатенации.

Определение 2.1. *Длина* $l(v)$ слова $v = b_{i_1} \ldots b_{i_t}$, $b_{i_j} \in B$, равна t. Пустое слово считается словом от элементов B длины 0.

Пусть B^i обозначает множество всех слов в алфавите B длины не большей i, $i \geq 0$.

Рассмотрим алгебру $\mathcal{A}$ над произвольным полем $\mathbb{F}$ и ее конечную систему порождающих $\mathcal{S}$. Произведения элементов из порождающего множества $\mathcal{S}$ можно рассматривать как образы элементов свободного моноида $F_{\mathcal{S}}$ при естественном гомоморфизме в мультипликативный моноид алгебры $\mathcal{A}$, и их также можно называть словами от образующих и использовать естественное обозначение $\mathcal{S}^i$. Заметим, что $\mathcal{S}^0 = \{1_{\mathcal{A}}\}$.

Обозначение 2.2. Положим $\mathcal{L}_i(\mathcal{S}) = \langle \mathcal{S}^i \rangle$, где $\langle S \rangle$ обозначает линейную оболочку множества S в некотором линейном пространстве над полем $\mathbb{F}$. Заметим, что $\mathcal{L}_0(\mathcal{S}) = \langle 1_{\mathcal{A}} \rangle = \mathbb{F}$. Пусть также $\mathcal{L}(\mathcal{S}) = \bigcup\limits_{i=0}^{\infty} \mathcal{L}_i(\mathcal{S})$ обозначает линейную оболочку всех слов в алфавите $\mathcal{S}$.

Определение 2.3. Слово $v \in \mathcal{S}^j$ длины j называется *сократимым над* $\mathcal{S}$, если найдется такой номер $i < j$, что $v \in \mathcal{L}_i(\mathcal{S})$, (т.е. v представляется в виде линейной комбинации слов меньшей длины). Если слово v не является сократимым, то оно называется *несократимым над* $\mathcal{S}$.

Из конечномерности $\mathcal{A}$ получаем, что найдется такой номер h, что $\mathcal{L}_h(\mathcal{S}) = \mathcal{L}_{h+1}(\mathcal{S})$. Если для некоторого $h \geq 0$ выполнено $\mathcal{L}_h(\mathcal{S}) = \mathcal{L}_{h+1}(\mathcal{S})$, то

$$\mathcal{L}_{h+2}(\mathcal{S}) = \langle \mathcal{L}_1(\mathcal{S})\mathcal{L}_{h+1}(\mathcal{S}) + \mathcal{L}_1(\mathcal{S}) \rangle = \langle \mathcal{L}_1(\mathcal{S})\mathcal{L}_h(\mathcal{S}) + \mathcal{L}_1(\mathcal{S}) \rangle = \mathcal{L}_{h+1}(\mathcal{S})$$

и также $\mathcal{L}_i(\mathcal{S}) = \mathcal{L}_h(\mathcal{S})$ для всех $i \geq h$.

Определение 2.4. *Длиной системы порождающих* $\mathcal{S}$ алгебры $\mathcal{A}$ называется число

$$l(\mathcal{S}) = \min\{k \in \mathbb{Z}_+ : \mathcal{L}_k(\mathcal{S}) = \mathcal{A}\}.$$

Определение 2.5. *Длиной алгебры* $\mathcal{A}$ называется число

$$l(\mathcal{A}) = \max\{l(\mathcal{S}) : \mathcal{L}(\mathcal{S}) = \mathcal{A}\}.$$

Обозначение 2.6. Пусть $a \in \mathcal{A}$ и $\deg a$ обозначает степень минимального многочлена элемента a над полем $\mathbb{F}$. Из конечномерности алгебры $\mathcal{A}$ следует, что для любого $a \in \mathcal{A}$ справедлива оценка $\deg a \leq \dim \mathcal{A}$. Тогда для любого непустого подмножества $\mathcal{B} \subseteq \mathcal{A}$ положим $m(\mathcal{B}) = \max\{\deg b : b \in \mathcal{B}\}$.

3 Известные результаты

В данном разделе мы приведем основные результаты о длинах групповых алгебр абелевых групп в модулярном случае, известные на данный момент.

Циклическую группу порядка n будем обозначать C_n. Групповую алгебру группы G над полем $\mathbb{F}$ будем обозначать $\mathbb{F}G$ или $\mathbb{F}[G]$.

В работе [1] вычислена длина групповых алгебр p-групп над полем характеристики p.

Теорема 3.1 ([1, теорема 3.8])**.** *Пусть $\mathbb{F}$ — поле характеристики $p > 0$. Пусть $m \in \mathbb{N}$ и пусть G — конечная абелева p-группа, которая содержит a_i копий C_{p^i} в своем разложении на примарные циклические, $a_1, \ldots, a_{m-1} \in \mathbb{Z}_+, a_m \in \mathbb{N}$, то есть,*

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

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

В той же работе вычислена длина групповой алгебры $\mathbb{F}_3[C_2 \times C_3 \times C_3]$.

Теорема 3.2 ([1, теорема 5.2])**.** $l(\mathbb{F}_3[C_2 \times C_3 \times C_3]) = 7$.

Затем этот результат был обобщен О.В. Марковой в работе [9].

Теорема 3.3 ([9, теорема 2.14])**.** *Пусть* $\mathbb{F}$ *— поле характеристики* $p > 2$. *Тогда*
$$l(\mathbb{F}[C_2 \times C_p \times C_p]) = 3p - 2.$$

Затем этот результат был обобщен автором в работе [5].

Теорема 3.4 ([5, теорема 3.4])**.** *Пусть* $\mathbb{F}$ *— поле характеристики* $p > 0$, $p \nmid K$, $k \geq l$. *Тогда*
$$l(\mathbb{F}[C_{p^l} \times C_{p^k} \times C_K]) = Kp^k + p^l - 2.$$

В той же работе автором была сформулирована гипотеза о длине групповой алгебры в случае прямого произведения циклической группы и абелевой p-группы над полем характеристики p.

Гипотеза 3.5 ([5, гипотеза 7.1])**.** *Пусть* $\mathbb{F}$ *— поле характеристики* $p > 0$, $P = C_{p^{k_1}} \times C_{p^{k_2}} \times \cdots \times C_{p^{k_q}}$, $p \nmid K$, $k_1 \geq k_i$ $\forall i$. *Тогда*
$$l(\mathbb{F}[P \times C_K]) = Kp^{k_1} + \sum_{i=2}^{q} p^{k_i} - q.$$

В данной работе мы докажем эту гипотезу в случае, когда абелева p-группа является элементарной, то есть является прямым произведением нескольких копий C_p, что с другой стороны будет обобщением теоремы 3.3.

Сформулируем основной результат работы.

Теорема 3.6. *Пусть* $\mathbb{F}$ *— поле характеристики* $p > 0$, $p \nmid K$, P *— элементарная абелева* p*-группа порядка* p^q. *Тогда*
$$l(\mathbb{F}[P \times C_K]) = (K + q - 1)p - q.$$

4 Нижняя оценка

В работе [5] была доказана нижняя оценка длины коммутативных групповых алгебр.

Лемма 4.1 ([5, лемма 4.1])**.** *Пусть $\mathbb{F}$ — произвольное поле, G — конечная абелева группа. Представим группу G в следующем виде:*

$$G \cong C_{p_1^{k_{11}}} \times \dots \times C_{p_1^{k_{1t}}} \times C_{p_2^{k_{21}}} \times \dots \times C_{p_2^{k_{2t}}} \times \dots \times C_{p_s^{k_{s1}}} \dots \times C_{p_s^{k_{st}}}, \quad (4.1)$$

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

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

Непосредственным применением этой леммы к рассматриваемой в работе групповой алгебре получаем нижнюю оценку.

Лемма 4.2. *Пусть $\mathbb{F}$ — поле характеристики $p > 0$, $p \nmid K$, P — элементарная абелева p-группа порядка p^q. Тогда*

$$l(\mathbb{F}[P \times C_K]) \ge (K + q - 1)p - q.$$

5 Вспомогательные леммы

Для доказательства верхней оценки нам понадобится доказать несколько вспомогательных лемм.

Замечание. В данной работе мы не раз будем представлять натуральное число l в определенном виде. Пусть $(m_1, m_2, \dots)$ — невозрастающая последовательность натуральных чисел. Рассмотрим равенство $l = \sum_{i=1}^{N} m_i + r$, где $0 \le r < m_{N+1}$. В частном случае, когда все m_i попарно равны, это представление является делением с остатком числа l на m_i. Однако легко показать, что и в общем случае такое представление существует и единственно.

Лемма 5.1. *Пусть $x_1, \dots, x_n \in \mathbb{Z}$, $l \in \mathbb{N}$, $(m_1 - 1, m_2 - 1, \dots)$ — невозрастающая последовательность натуральных чисел. Пусть $l = \sum_{i=1}^{N}(m_i - 1) + r$, где $0 \le r < m_{N+1} - 1$. Рассмотрим функцию*

$$P(x_1, \dots, x_n) = (x_1 + 1) \cdots (x_n + 1).$$

Тогда

$$\min\{P(x_1, \dots, x_n) : x_1 + \dots + x_n = l, \forall i (0 \le x_i \le m_i - 1)\} = m_1 \cdots m_N (r + 1).$$

Доказательство. Рассмотрим значение функции $P(\overline{x})$ на произвольном наборе $b_1, \dots, b_n$, удовлетрояющем условиям. Так как $P(\overline{x})$ — симметрическая и последовательность $(m_1 - 1, m_2 - 1, \dots)$ — невозрастающая, мы можем считать, что $b_1 \ge b_2 \ge \dots \ge b_n$.

Рассмотрим $m = \max\{i : b_i \ne 0\}$, $M = \min\{i : b_i \ne m_i - 1\}$. Пусть $M < m$.

Рассмотрим $P(b_1, \dots, b_{M-1}, b_M + 1, b_{M+1}, \dots, b_{m-1}, b_m - 1, b_{m+1}, \dots, b_n)$. Этот новый набор значений удовлетворяет всем условиям, в том числе он невозрастающий. Действительно, по определению m и M имеем $b_m - 1 \geq 0 = b_{m+1}$ и $b_{M-1} = m_{M-1} - 1 \geq m_M - 1 \geq b_M + 1$.

Отметим, что

$$P(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n) = (x_i + 1)P(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n).$$

Таким образом,

$$P(b_1, \dots, b_{M-1}, b_M + 1, b_{M+1}, \dots, b_{m-1}, b_m - 1, b_{m+1}, \dots, b_n) =$$

$$(b_M + 2)b_m P(b_1, \dots, b_{M-1}, 0, b_{M+1}, \dots, b_{m-1}, 0, b_{m+1}, \dots, b_n) =$$

$$((b_M+1)(b_m+1) - b_M - 1 + b_m)P(b_1, \dots, b_{M-1}, 0, b_{M+1}, \dots, b_{m-1}, 0, b_{m+1}, \dots, b_n) =$$

$$P(b_1, \dots, b_n) - (b_M + 1 - b_m)P(b_1, \dots, b_{M-1}, 0, b_{M+1}, \dots, b_{m-1}, 0, b_{m+1}, \dots, b_n).$$

То есть

$$P(b_1, \dots, b_{M-1}, b_M + 1, b_{M+1}, \dots, b_{m-1}, b_m - 1, b_{m+1}, \dots, b_n) < P(b_1, \dots, b_n),$$

так как $b_M + 1 > b_m$.

Таким образом, если $M < m$, то мы можем уменьшить значение функции $P(\overline{x})$, перенеся единицу из самого маленького ненулевого значения в самое большое из тех, что еще не достигло максимума $m_i - 1$. Но случаю $M \geq m$ удовлетворяет только один набор значений переменных — $(m_1 - 1, \dots, m_N - 1, r, 0, \dots, 0)$. В силу конечности множества допустимых наборов значений переменных из этого следует, что на нем и достигается минимальное значение функции. То есть

$$\min P(\overline{x}) = P(m_1 - 1, \dots, m_N - 1, r, 0, \dots, 0) = m_1 \cdots m_N (r + 1).$$

□

Лемма 5.2. *Пусть $\mathcal{A}$ — коммутативная алгебра, $\mathcal{S} = \{a_1, \dots, a_n\}$ — система порождающих алгебры $\mathcal{A}$. Пусть $v = a_1^{t_1} \cdots a_n^{t_n}$ — лексикографически минимальное слово среди всех несократимых слов длины $t = t_1 + \cdots + t_n$. Пусть $H = \{v_i \in \mathcal{S}^t : v_i$— подслово $v\}$. Тогда все слова в H линейно независимы.*

Доказательство. Предположим, что слова в H линейно зависимы. То есть в H существуют слова, которые линейно выражаются через остальные. Выберем среди них наибольшее в градуированном лексикографическом порядке слово w. Подставив в v вместо подслова w его выражение через меньшие слова, получим что v выражается через слова меньшей длины и слова той же длины, которые лексикографически меньше v (то есть сократимые по условию). Таким образом, v сократимо. Противоречие. □

Непосредственным следствием из предыдущей леммы является следующая лемма.

Лемма 5.3. *Пусть $\mathcal{A}$ — коммутативная алгебра, $\mathcal{S} = \{a_1, \ldots, a_n\}$ — система порождающих алгебры $\mathcal{A}$. Пусть $v = a_1^{t_1} \cdots a_n^{t_n}$ — лексикографически минимальное слово среди всех несократимых слов длины $t = t_1 + \cdots + t_n$. Тогда $(t_1 + 1) \cdots (t_n + 1) \leq \dim \mathcal{A}$.*

Доказательство. Действительно, пусть $H = \{v_i \in \mathcal{S}^t : v_i$— подслово $v\}$. Тогда $|H| = (t_1 + 1) \cdots (t_n + 1)$. Но по лемме 5.2 $|H| \leq \dim \mathcal{A}$. □

Главным результатом раздела является следующая лемма, с помощью которой будет доказана верхняя оценка.

Лемма 5.4. *Пусть $\mathcal{A}$ — коммутативная алгебра, $\mathcal{S} = \{a_1, \ldots, a_n\}$ — система порождающих алгебры $\mathcal{A}$ длины $l = l(\mathcal{A})$, $(m_1-1, m_2-1, \ldots)$ — невозрастающая последовательность натуральных чисел. Пусть $v = a_1^{t_1} \cdots a_n^{t_n}$ — лексикографически минимальное слово среди всех несократимых слов длины $l = t_1 + \cdots + t_n$. Пусть $l = \sum_{i=1}^{N} (m_i - 1) + r$, где $0 \leq r < m_{N+1} - 1$. Пусть $t_1 \leq m_1 - 1, \ldots, t_n \leq m_n - 1$. Тогда $m_1 \cdots m_N (r + 1) \leq \dim \mathcal{A}$.*

Доказательство. По лемме 5.3 $\prod_{i=1}^{n} (t_i + 1) \leq \dim \mathcal{A}$. Но по лемме 5.1

$$m_1 \cdots m_N (r + 1) \leq \prod_{i=1}^{n} (t_i + 1) \leq \dim \mathcal{A}.$$

□

6 Случай $m_i = m(\mathcal{A})$

Отвлечемся от доказательства основного результата работы и в качестве применения последней полученной леммы рассмотрим важный частный случай последовательности $(m_1 - 1, m_2 - 1, \ldots) = (m(\mathcal{A}) - 1, m(\mathcal{A}) - 1, \ldots)$. В этом случае из леммы 5.4 следует доказанная ранее О.В. Марковой в работе [8] оценка длины коммутативных алгебр. Продемонстрируем это.

Теорема 6.1 ([8, 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 $l(\mathcal{A}) \leq g(\dim \mathcal{A}, m(\mathcal{A}))$.

Доказательство. В случае $m(\mathcal{A}) = 1$ все элементы алгебры пропорциональны единице данной алгебры, то есть алгебра изоморфна базовому полю и ее длина равна нулю.

Пусть теперь $m = m(\mathcal{A}) > 1$. Тогда $(m - 1, m - 1, \ldots)$ — невозрастающая последовательность натуральных чисел, степени вхождения элементов системы порождающих в несократимые слова ограничены числом $m-1$. Пусть $d = \dim \mathcal{A}$, $l = l(\mathcal{A})$, N таково, что $l = (m-1)N + r$, где $0 \le r < m-1$. Тогда по лемме 5.4 имеем

$$m^N(r+1) \le d = m^{\log_m d} = m^{[\log_m d]+\{\log_m d\}}.$$

Рассмотрим два случая.

Пусть $r+1 > m^{\{\log_m d\}}$. Тогда $m^N < m^{[\log_m d]}$, то есть $N < [\log_m d]$. Тогда $N+1 \le [\log_m d]$, то есть $\frac{l}{m-1} - \frac{r}{m-1} + 1 \le [\log_m d]$. Следовательно, $\frac{l}{m-1} < [\log_m d]$, то есть $l < (m-1)[\log_m d] \le g(d,m)$.

Пусть $r+1 \le m^{\{\log_m d\}}$. Но и в этом случае $N \le \log_m d$, и, так как $N \in \mathbb{Z}$, $N \le [\log_m d]$, то есть $\frac{l-r}{m-1} \le [\log_m d]$. Следовательно,

$$l \le (m-1)[\log_m d] + r \le (m-1)[\log_m d] + m^{\{\log_m d\}} - 1 = g(d,m).$$

$\square$

7 Верхняя оценка

Нетрудно проверить, что если в рассматриваемой в работе групповой алгебре порядок элементарной абелевой p-группы больше p^2, то верхняя оценка, полученная с помощью теоремы 6.1, не будет точна. Поэтому нам потребуется построить менее грубую оценку степеней вхождения букв в несократимые слова, чем рассмотренная в разделе 6.

Лемма 7.1. *Пусть $\mathbb{F}$ — поле характеристики p, H — абелева группа порядка K. Пусть $\mathcal{A} = \mathbb{F}[H \times \bigotimes C_p]$, $\mathcal{S} = \{a_1, \ldots, a_n\}$ — система порождающих алгебры $\mathcal{A}$. Пусть $v = a_1^{t_1} \cdots a_n^{t_n}$ — лексикографически минимальное слово среди всех несократимых слов длины $t = t_1 + \cdots + t_n$. Тогда существует упорядоченный невозрастающий набор целых неотрицательных чисел $(k_1, \ldots, k_n)$, такой что $k_1 + \cdots + k_n = K - 1$ и $\forall i : t_i \le (k_i+1)p - 1$.*

Доказательство. Для каждого i рассмотрим минимальное целое λ_i, такое что $t_i \le (\lambda_i+1)p-1$. Таким образом, для каждого i: $t_i \ge \lambda_i p$. Следовательно, $e, a_1^p, a_1^{2p}, \ldots, a_1^{\lambda_1 p}, a_2^p, \ldots, a_2^{\lambda_2 p}, \ldots, a_n^{\lambda_n p}$ являются подсловами в v и, согласно лемме 5.2, обязаны быть линейно независимыми.

Заметим, что для любого i и любого натурального μ элемент $a_i^{\mu p} = \alpha(h, 0, \ldots, 0)$, где $\alpha \in \mathbb{F}$, $h \in H$. То есть $e, a_1^p, \ldots, a_n^{\lambda_n p}$ — линейно независимые элементы K-мерной подалгебры в $\mathcal{A}$, изоморфной $F[H]$. Следовательно, $1 + \lambda_1 + \cdots + \lambda_n \le K$.

При необходимости переименуем элементы $\mathcal{S}$ так, чтобы набор $(\lambda_1, \ldots, \lambda_n)$ был невозрастающим и увеличим λ_1 так, чтобы сумма чисел в этом наборе была равна $K-1$. Положим $(k_1, \ldots, k_n) = (\lambda_1, \ldots, \lambda_n)$. $\square$

Лемма 7.2. *Пусть $\mathbb{F}$ — поле характеристики p, H — абелева группа порядка K, $p \nmid K$. Пусть $\mathcal{A} = \mathbb{F}[H \times \bigotimes_{i=1}^q C_p]$. Тогда $l(\mathcal{A}) \le (K+q-1)p - q$.*

Доказательство. Пусть $\mathcal{S} = \{a_1, \ldots, a_n\}$ — произвольная система порождающих алгебры $\mathcal{A}$ длины $l = l(\mathcal{A})$. Пусть $v = a_1^{t_1} \cdots a_n^{t_n}$ — лексикографически минимальное слово среди всех несократимых слов длины $l = t_1 + \cdots + t_n$. С помощью леммы 7.1 построим невозрастающую последовательность натуральных чисел $((k_1+1)p-1, \ldots, (k_n+1)p-1, p-1, p-1, \ldots)$, такую что $k_1 + \cdots + k_n = K - 1$ и $\forall i : t_i \leq (k_i+1)p - 1$.

Пусть $l = \sum_{i=1}^{N}((k_i+1)p-1) + r$, где $0 \leq r < (k_{N+1}+1)p - 1$ (можем считать $k_i = 0$ при $i > n$). Тогда из леммы 5.4 следует неравенство

$$(k_1+1)\cdots(k_N+1)p^N(r+1) \leq Kp^q. \tag{7.1}$$

Разберем несколько случаев.

Случай 1. Пусть $N \geq q$, $(k_1+1)\cdots(k_N+1) < K$.

Если $k_{N+1} = 0$, то $k_i = 0$ $\forall i \geq N+1$, так как последовательность k_i не возрастает. Следовательно, $(k_1+1)\cdots(k_N+1) = (k_1+1)\cdots(k_n+1)$. По построению k_i имеем $k_1 + \cdots + k_n = K - 1$, $k_i \leq K - 1$ $\forall i$. Тогда, применяя лемму 5.1, получаем $(k_1+1)\cdots(k_N+1) = (k_1+1)\cdots(k_n+1) \geq K$. Противоречие.

Если $k_{N+1} \neq 0$, то $k_i + 1 \geq 2$ $\forall i \leq N+1$, так как последовательность k_i не возрастает. Если $q \leq 2$, то утверждение леммы напрямую следует из теоремы 3.4, поэтому можем считать, что $N \geq q \geq 3$. Тогда,

$$K > (k_1+1)\cdots(k_N+1) = (k_1+1)\cdots(k_{N-1}+1) + (k_1+1)\cdots(k_{N-1}+1)k_N \geq$$

$$(k_1+1)\cdots(k_{N-1}+1) + 4k_N \geq (k_1+1)\cdots(k_{N-1}+1) + (k_N+1) + (k_{N+1}+1) =$$

$$(k_1+1)\cdots(k_{N-2}+1) + (k_1+1)\cdots(k_{N-2}+1)k_{N-1} + (k_N+1) + (k_{N+1}+1) \geq$$

$$(k_1+1)\cdots(k_{N-2}+1) + 2k_{N-1} + (k_N+1) + (k_{N+1}+1) \geq$$

$$(k_1+1)\cdots(k_{N-2}+1) + (k_{N-1}+1) + (k_N+1) + (k_{N+1}+1) \geq \ldots \geq \sum_{i=1}^{N+1}(k_i+1).$$

Таким образом,

$$l = \sum_{i=1}^{N}((k_i+1)p-1) + r < \sum_{i=1}^{N+1}((k_i+1)p-1) =$$

$$p\sum_{i=1}^{N+1}(k_i+1) - (N+1) < Kp - (q+1) < (K+q-1)p - q.$$

Случай 2. Пусть $N \geq q$, $(k_1+1)\cdots(k_N+1) \geq K$.

В силу последнего неравенства и неравенства 7.1 имеем $p^N(r+1) \leq p^q$. Следовательно, $N = q$ и $r = 0$. Тогда

$$l = \sum_{i=1}^{q}((k_i+1)p-1) \leq p\sum_{i=1}^{q}k_i + pq - q \leq (K-1+q)p - q.$$

Случай 3. Пусть $N \leq q-1$.
В этом случае

$$l = \sum_{i=1}^{N}((k_i+1)p-1) + r < \sum_{i=1}^{N+1}((k_i+1)p-1) \leq$$

$$\sum_{i=1}^{q}((k_i+1)p-1) \leq (K-1+q)p-q.$$

□

Применяя лемму 7.2 к рассматриваемой в работе групповой алгебре, получаем верхнюю оценку, которая есть ее частный случай при $H = C_K$, что завершает доказательство основного результата работы — теоремы 3.6.

Лемма 7.3. *Пусть* $\mathbb{F}$ *— поле характеристики* $p > 0$*,* $p \nmid K$*,* P *— элементарная абелева* p*-группа порядка* p^q*. Тогда*

$$l(\mathbb{F}[P \times C_K]) \leq (K+q-1)p-q.$$

8 Обобщения теоремы 3.6

В данном разделе будут приведены 2 обобщения теоремы 3.6. Первое не требует усилий. Мы лишь заметим, что при замене во всех доказанных утверждениях p на p^s, где s — произвольное натуральное число (кроме, разумеется, указания характеристики поля), все рассуждения остаются верными. Таким образом, мы получаем следующее обобщение.

Теорема 8.1. *Пусть* $\mathbb{F}$ *— поле характеристики* $p > 0$*,* $P = \bigotimes_{i=1}^{q} C_{p^s}$*,* $p \nmid K$*. Тогда*

$$l(\mathbb{F}[P \times C_K]) = (K+q-1)p^s - q.$$

Для доказательства второго обобщения отметим, что в лемме 7.2 мы не требовали, чтобы группа H была циклической, однако нижняя оценка в лемме 4.2 не выполняется при замене C_K на произвольную абелеву группу порядка K. Поэтому для доказательства нижней оценки нам понадобятся несколько вспомогательных результатов.

Лемма 8.2 ([10, лемма 3.23])**.** *Пусть* $\mathbb{F}$ *— произвольное поле,* $\mathcal{A}$ *и* $\mathcal{B}$ *— конечномерные алгебры с единицами над* $\mathbb{F}$*. Тогда* $l(\mathcal{A} \otimes_{\mathbb{F}} \mathcal{B}) \geq l(\mathcal{A}) + l(\mathcal{B})$.

Определение 8.3. 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 8.4 ([1, теорема 4.7])**.** *Пусть $K \in \mathbb{N}$, $\mathbb{F}$ — совершенное поле характеристики $p > 0$, $|\mathbb{F}| \geq K$ и $(K, p) = 1$. Рассмотрим конечную абелеву группу $G \cong H \times P$, где P — циклическая p-группа и $|H| = K$. Тогда алгебра $\mathbb{F}G$ является однопорожденной и $l(\mathbb{F}G) = |G| - 1$.*

Последние два утверждения позволяют доказать обобщение теоремы 3.6 при дополнительных условиях на поле.

Теорема 8.5. *Пусть $\mathbb{F}$ — совершенное поле характеристики $p > 0$, H — абелева группа порядка K, $|\mathbb{F}| \geq K$, $p \nmid K$, $P = \bigotimes_{i=1}^{q} C_{p^s}$. Тогда*

$$l(\mathbb{F}[P \times H]) = (K + q - 1)p^s - q.$$

Доказательство. Так как групповая алгебра прямого произведения групп является тензорным произведением соответствующих групповых алгебр, мы можем представить рассматриваемую алгебру в следующем виде (тензорное произведение обозначено символом $\otimes_{\mathbb{F}}$).

$$\mathbb{F}[P \times H] = \mathbb{F}\left[\bigotimes_{i=1}^{q-1} C_{p^s} \times C_{p^s} \times H\right] \cong \mathbb{F}\left[\bigotimes_{i=1}^{q-1} C_{p^s}\right] \otimes_{\mathbb{F}} \mathbb{F}[C_{p^s} \times H].$$

Тогда из леммы 8.2 следует, что

$$l(\mathbb{F}[P \times H]) \geq l(\mathbb{F}\left[\bigotimes_{i=1}^{q-1} C_{p^s}\right]) + l(\mathbb{F}[C_{p^s} \times H]).$$

Из теоремы 3.1 следует, что $l(\mathbb{F}[\bigotimes_{i=1}^{q-1} C_{p^s}]) = (q-1)(p^s-1)$. Из теоремы 8.4 следует, что $l(\mathbb{F}[C_{p^s} \times H]) = Kp^s - 1$. Таким образом,

$$l(\mathbb{F}G) \geq (q-1)(p^s-1) + Kp^s - 1 = (K + q - 1)p^s - q.$$

Верхняя оценка следует из леммы 7.2. □

Список литературы

[1] A. E. Guterman, M. A. Khrystik, O. V. Markova, *On the lengths of group algebras of finite abelian groups in the modular case.* — J. Algebra its Appl., **21**:6 (2022), 2250117–2250130.

[2] A. E. Guterman, O. V. Markova, *The length of group algebras of small-order groups.* — Zap. Nauchn. Sem. POMI, **472** (2018), 76–87; English transl. in J. Math. Sci. **240**:6 (2019), 754–761.

[3] 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.

[4] A. E. Guterman, O. V. Markova, M. A. Khrystik, *On the lengths of group algebras of finite abelian groups in the semi-simple case.* — J. Algebra its Appl., **21**:7 (2022), 2250140–2250153.

[5] M. A. Khrystik, *Length of the group algebra of the direct product of a cyclic group and a cyclic p-group in the modular case.* — Zap. Nauchn. Sem. POMI, **524**(2023), 166–176.

[6] M. A. Khrystik, O. V. Markova *The length of the group algebra of the dihedral group of order 2^k.* — Zap. Nauchn. Sem. POMI, **496**(2020), 169–181; English transl. in J. Math. Sci. (N. Y.), **255**:3 (2021), 324–331.

[7] M. A. Khrystik, O. V. Markova, *On the length of the group algebra of the dihedral group in the semi-simple case.* — Commun. Algebra, **50**:5 (2022), 2223–2232.

[8] O. V. Markova, *Upper bound for the length of commutative algebras.* — Mat. Sb., **200**:12 (2009), 41–62; English transl. in Sb. Math., **200**:12 (2009), 1767–1787.

[9] O. V. Markova, *An example of length computation for a group algebra of a noncyclic abelian group in the modular case.* — Fundam. Prikl. Mat., **23**:2 (2020), 217–229; English transl. in J. Math. Sci. **262**:5 (2022) 740–748.

[10] O. V. Markova, *The length function and matrix algebras.* — Fundam. Prikl. Mat., **17**:6 (2012), 65–173; English transl. in J. Math. Sci. **193**:5 (2013) 687–768.

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

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