Пример вычисления длины групповой алгебры нециклической абелевой группы в модулярном случае*

О. В. МАРКОВА
Московский государственный университет им. М. В. Ломоносова,
Московский центр фундаментальной и прикладной математики,
Московский физико-технический институт (государственный университет)
e-mail: ov_markova@mail.ru

УДК 512.552

Ключевые слова: функция длины алгебры, групповые алгебры, коммутативные алгебры.

Аннотация

В работе показано, что технику вычисления длины двублочных матричных алгебр, разработанную автором ранее, можно применить для вычисления длин групповых алгебр абелевых групп. Вычислена длина групповой алгебры нециклической абелевой группы порядка $2p^2$, $p > 2$ — простое число, над полем характеристики p, а именно доказано, что длина данной алгебры равна $3p - 2$.

Abstract

O. V. Markova, An example of length computation for a group algebra of a noncyclic Abelian group in the modular case, Fundamentalnaya i prikladnaya matematika, vol. 23 (2020), no. 2, pp. 217—229.

We demonstrate that the technique for calculating the length of two-block matrix algebras, developed by the author earlier, can be used to calculate the lengths of group algebras of Abelian groups. We find the length of the group algebra of a noncyclic Abelian group of order $2p^2$, where $p > 2$ is a prime number, over a field of characteristic p, namely, we prove that the length of this algebra is equal to $3p - 2$.

Светлой памяти моего отца Виктора Тимофеевича Маркова

1. Введение

Напомним основные определения, связанные с функцией длины. Термины и результаты теории колец, использованные в статье, можно найти, например, в [21]. Все рассматриваемые в работе алгебры — ассоциативные конечномерные алгебры с единицей над полями. Важную роль в изучении конечномерных алгебр играет такой инвариант алгебры, как *длина*. Определим её, следуя [18].

*Работа выполнена при финансовой поддержке гранта РНФ 17-11-01124.

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

Определение 1.1. *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, $i \geqslant 0$.

Рассмотрим алгебру $\mathcal{A}$ над произвольным полем $\mathbb{F}$ и её 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 1.2. 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 $\mathcal{S}$.

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

Определение 1.3. *Длиной системы порождающих* $\mathcal{S}$ алгебры $\mathcal{A}$ называется число

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

Определение 1.4. *Длиной алгебры* $\mathcal{A}$ называется число

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

Отметим, что вычисление длины заданного множества $\mathcal{S}$ является стандартной задачей линейной алгебры построения некоторого специального базиса пространства $\mathcal{L}(\mathcal{S})$, хотя её вычислительная сложность основана на том факте, что количество слов в каждом множестве $\mathcal{S}^i$ растёт в геометрической прогрессии. С другой стороны, в определении длины алгебры $\mathcal{A}$ мы рассматриваем множество всех порождающих систем для $\mathcal{A}$. Этим объясняется сложность вычисления длины даже для классических алгебр.

Для длины алгебры всегда справедлива следующая тривиальная верхняя оценка.

Замечание 1.5 [4, лемма 5.3]. Пусть $\mathcal{A}$ — алгебра размерности n над произвольным полем $\mathcal{A}$. Тогда $l(\mathcal{A}) \leqslant n - 1$, причём оценка превращается в равенство тогда и только тогда, когда алгебра $\mathcal{A}$ является однопорождённой, из чего автоматически следует, что она коммутативна.

Обозначение 1.6. Пусть $\mathbb{F}$ — произвольное поле и G — конечная группа. Через $\mathbb{F}G$ (иногда через $\mathbb{F}[G]$) будем обозначать групповую алгебру группы G над полем $\mathbb{F}$. Через $\mathrm{M}_n(R)$ будем обозначать алгебру матриц над произвольным кольцом R.

В общей формулировке проблема вычисления длины впервые была сформулирована А. Пазом [20] в 1984 году для полной алгебры матриц $\mathrm{M}_n(\mathbb{F})$ над полем и до сих пор является открытой. Вычисление длины в общем случае является довольно трудной задачей, однако для конкретных подмножеств и собственных подалгебр матричной алгебры удаётся явно вычислить длину или получить хорошие оценки (см. [2, 5, 14, 15, 18] и библиографию там).

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 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 [1, 16].

В общем случае из тривиальной оценки для групповых алгебр получаем, что для произвольной конечной группы G и произвольного поля $\mathbb{F}$ справедливы следующие утверждения:

1) $l(\mathbb{F}G) \leqslant |G| - 1$, причём оценка превращается в равенство тогда и только тогда, когда алгебра $\mathbb{F}G$ является однопорождённой;
2) если G — циклическая группа, то $l(\mathbb{F}G) = |G| - 1$;
3) если G неабелева, то $l(\mathbb{F}G) \leqslant |G| - 2$.

Изучению общей задачи нахождения длины групповых алгебр конечных абелевых групп посвящены работы [12, 13]. В [12] исследованы длины групповых алгебр абелевых групп в так называемом модулярном случае, т. е. в предположении, что характеристика основного поля делит порядок группы. Этой же теме посвящена данная работа.

В [12] для получения оценки длины групповых алгебр использованы методы теории полей, теории колец и методы работы с функцией длины алгебры сведением к длине фактор-алгебры по радикалу Джекобсона и индексу нильпотентности радикала (см. [6, теорема 1, следствие 1]) и оценке длины коммутативных алгебр (см. [4, теорема 3.11]). Вычисление индекса нильпотентности радикала Джекобсона групповой алгебры основано на теории Дженнингса (см. [17; 19, гл. 11, § 1]).

Напомним некоторые понятия теории идеалов.

Определение 1.7. *Фундаментальный идеал* алгебры $\mathbb{F}G$ — это

$$\Delta(\mathbb{F}G) = \Big\{ \sum_{g\in G} a_g g \;\Big|\; \sum_{g\in G} a_g = 0 \Big\}.$$

Лемма 1.8 [19, лемма 3.1.6]. *Если G — конечная p-группа, то идеал $\Delta(\mathbb{F}G)$ совпадает с радикалом Джекобсона $J(\mathbb{F}G)$ алгебры $\mathbb{F}G$.*

Используя теорию Дженнингса, можно построить взвешенный базис идеала $\Delta(\mathbb{F}G)$, т. е. базис, составленный из базисных элементов каждого из идеалов $\Delta(\mathbb{F}G)^i$, $i \in \mathbb{N}$. Эти степени фундаментального идеала также используются в [9], [3], [7], [8] для построения некоторых линейно оптимальных кодов, кодов Рида—Соломона и кодов Рида—Маллера соответственно. Предполагается использование вычисленных нами числовых характеристик групповых алгебр, в частности длины, для решения вопросов, связанных с групповыми кодами, представленных в [10, 11].

В данной работе предложен ещё один подход к вычислению длины групповых алгебр, отличный от методов из [12]. Показано, что для вычисления длин групповых алгебр абелевых групп можно применить технику вычисления длины двублочных матричных алгебр, разработанную автором в [5]. С её помощью вычислена длина групповой алгебры нециклической абелевой группы порядка $2p^2$, где $p > 2$ — простое число, над полем характеристики p, а именно доказано, что длина данной алгебры равна $3p - 2$.

2. Длина групповой алгебры $\mathbb{F}[\mathbb{Z}_2 \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p]$

Всюду в данном разделе $\mathbb{F}$ обозначает поле характеристики $p > 2$, P обозначает группу $\mathbb{Z}_p \oplus \mathbb{Z}_p$ в мультипликативной записи, т. е. $P = \langle a \rangle_p \times \langle b \rangle_p$, и $\mathcal{A} = \mathbb{F}P$ — её групповая алгебра.

Сперва докажем несколько вспомогательных утверждений.

Лемма 2.1. *Элементы $x = a - 1_{\mathcal{A}}$ и $y = b - 1_{\mathcal{A}}$ являются порождающими для радикала Джекобсона $J(\mathcal{A})$ алгебры $\mathcal{A}$, удовлетворяют соотношениям $x^p = y^p = 0$, $xy = yx$,*

$$J(\mathcal{A}) = \langle x^i y^j \mid 0 \leqslant i, j \leqslant p - 1, \ i + j \geqslant 1 \rangle$$

и

$$\mathcal{A} = \langle 1_{\mathcal{A}}, x^i y^j \mid 0 \leqslant i, j \leqslant p - 1, \ i + j \geqslant 1 \rangle.$$

Доказательство. Соотношения $x^p = y^p = 0$, $xy = yx$ следуют из коммутативности группы и условий на поле. По определению $P = \{a^i b^j \mid 0 \leqslant i, j \leqslant p-1\}$. Образующие a, b группы P порождают её групповую алгебру $\mathcal{A}$, следовательно, порождающими будут и элементы $1_{\mathcal{A}}$, $x = a - 1_{\mathcal{A}}$, $y = b - 1_{\mathcal{A}} \in \mathcal{A}$ и

$$\mathcal{A} = \langle x^i y^j \mid 0 \leqslant i, j \leqslant p - 1 \rangle.$$

Поскольку любое нетривиальное слово от x, y является нильпотентным элементом, то мы также получаем, что

$$J(\mathcal{A}) = \langle x^i y^j \mid 0 \leqslant i, j \leqslant p - 1, \ i + j \geqslant 1 \rangle. \qquad \square$$

Следствие 2.2. *Индекс нильпотентности радикала $J(\mathcal{A})$ равен $2p - 1$, при этом любой элемент $A \in J(\mathcal{A})$ удовлетворяет соотношению $A^p = 0$.*

Доказательство. Утверждение следует из соотношений $x^p = y^p = 0$, $xy = yx$ и конструкции базиса пространства $J(\mathcal{A})$. $\square$

В дальнейшем мы возьмём элементы $x^i y^j$, $0 \leqslant i, j \leqslant p-1$, в качестве стандартного базиса алгебры $\mathcal{A}$.

Далее мы несколько раз будем использовать описание поведения длины при изменении системы порождающих (см. [15, предложения 2.1, 2.2 и 2.4]), поэтому для удобства приведём формулировки этих утверждений.

Предложение 2.3 [15, предложение 2.1]. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — алгебра над $\mathbb{F}$. Если $\mathcal{S} = \{a_1, \ldots, a_k\}$ — система порождающих этой алгебры и $C = \{c_{i,j}\} \in \mathrm{M}_k(\mathbb{F})$ — невырожденная матрица, то множество*

$$\mathcal{S}_c = \{c_{1,1}a_1 + c_{1,2}a_2 + \ldots + c_{1,k}a_k, \ldots, c_{k,1}a_1 + c_{k,2}a_2 + \ldots + c_{k,k}a_k\}$$

является системой порождающих алгебры $\mathcal{A}$ и $l(\mathcal{S}_c) = l(\mathcal{S})$.

Предложение 2.4 [15, предложение 2.2]. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — алгебра с единицей над $\mathbb{F}$. Пусть $\mathcal{S} = \{a_1, \ldots, a_k\}$ — система порождающих этой алгебры, такая что $1_{\mathcal{A}} \notin \langle a_1, \ldots, a_k \rangle$. Тогда для любых $\gamma_1, \ldots, \gamma_k \in \mathbb{F}$ множество*

$$\mathcal{S}_1 = \left\{a_1 + \gamma_1 1_{\mathcal{A}}, \ldots, a_k + \gamma_k 1_{\mathcal{A}}\right\} -$$

система порождающих алгебры $\mathcal{A}$ и $l(\mathcal{S}_1) = l(\mathcal{S})$.

Предложение 2.5 [15, предложение 2.4]. *Пусть $\mathbb{F}$ — произвольное поле, пусть $\mathcal{A}$ — $\mathbb{F}$-алгебра с единицей $1_{\mathcal{A}}$, и пусть $\mathcal{S} = \{a_1, \ldots, a_k\}$ — 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) $l(\mathcal{S}') = l(\mathcal{S})$.

Техника, используемая в этом разделе для работы с прямой суммой двух копий групповой алгебры $\mathcal{A}$, основана на методе, изначально разработанном в [5, разд. 5.1.1] для двублочных алгебр верхнетреугольных матриц со скалярной диагональю.

Лемма 2.6. *Пусть $\mathcal{S} = \{A_i \mid i = 1, \ldots, k\}$ — произвольная система порождающих алгебры $\mathcal{B} = \mathcal{A} \oplus \mathcal{A}$, которая по определению имеет вид $A_1 = (u_1, w_1)$, $A_i = (u_i, v_i)$, где $u_1, w_1, u_i, v_i \in \mathcal{A}$, $i = 2, \ldots, k$, множества*

$$\mathcal{S}' = \{u_i \mid i = 1, \ldots, k\}, \quad \mathcal{S}'' = \{w_1, v_i \mid i = 2, \ldots, k\}$$

являются порождающими системами для $\mathcal{A}$. Тогда достаточно вычислить длину $l(\mathcal{S})$ при условии, что все элементы u_i, $i = 1, \ldots, k$, нильпотентны, $w_1 = 1_{\mathcal{A}} + v_1$ и все v_i, $i = 1, \ldots, k$, также нильпотентны.

Доказательство. Применяя предложения 2.3—2.5 к $\mathcal{S}$, действуя по аналогии с [5, лемма 5.17], мы построим множество $\tilde{\mathcal{S}} \subseteq \mathcal{L}_1(\mathcal{S})$, длины $l(\tilde{\mathcal{S}}) = l(\mathcal{S})$, порождающее алгебру $\mathcal{A}$ и удовлетворяющее требуемым условиям на элементы. Поэтому без ограничения общности в дальнейшем корректно будет рассматривать $\tilde{\mathcal{S}}$ вместо $\mathcal{S}$.

Будем последовательно преобразовывать $\mathcal{S}$ до системы порождающих, удовлетворяющей условиям на элементы.

Обозначим

$$u_t = \sum_{0 \leqslant i,j \leqslant p-1} \alpha_{t;i,j} x^i y^j, \quad t = 1, \ldots, k;$$

$$w_1 = \sum_{0 \leqslant i,j \leqslant p-1} \beta_{1;i,j} x^i y^j, \quad v_t = \sum_{0 \leqslant i,j \leqslant p-1} \beta_{t;i,j} x^i y^j, \quad t = 2, \ldots, k.$$

Шаг 1. Поскольку $(1, 0) \in \mathcal{L}(\mathcal{S})$, то существует элемент $A_m \in \mathcal{S}$, такой что $\alpha_{m;0,0} \neq \beta_{m;0,0}$. При необходимости перенумеровав элементы $\mathcal{S}$, не ограничивая общности считаем, что $m = 1$. Положим

$$A_1' = (\beta_{1;0,0} - \alpha_{1;0,0})^{-1}(A_1 - \alpha_{1;0,0} 1_{\mathcal{B}}).$$

По предложению 2.4 с сохранением длины перейдём к системе порождающих

$$\mathcal{S}_1 = \{A_1', A_2, \ldots, A_k\}.$$

Элемент A_1' удовлетворяет условиям леммы.

Шаг 2. По предложению 2.4 с сохранением длины перейдём к системе порождающих

$$\mathcal{S}_2 = \{A_1',\, A_i' = A_i - \alpha_{i;0,0} 1_{\mathcal{B}} \mid i = 2, \ldots, k\}.$$

Мы добились нильпотентности первых компонент всех элементов системы образующих.

Шаг 3. По предложению 2.3 с сохранением длины перейдём к системе порождающих

$$\mathcal{S}_3 = \{A_1',\, A_i'' = A_i' - (\beta_{i;0,0} - \alpha_{i;0,0}) A_1' \mid i = 2, \ldots, k\}.$$

Этим мы добились нильпотентности вторых компонент всех элементов системы образующих, кроме первого.

Таким образом, можно взять $\tilde{\mathcal{S}} = \mathcal{S}_3$. $\square$

Лемма 2.7. *Пусть $\mathcal{S} = \{A_i \mid i = 1, \ldots, k\}$ — произвольная система порождающих алгебры $\mathcal{B} = \mathcal{A} \oplus \mathcal{A}$. Предположим, что $A_1 = (u_1, w_1)$, $A_i = (u_i, v_i)$, где все элементы $u_i \in \mathcal{A}$, $i = 1, \ldots, k$, нильпотентны, $w_1 = 1_{\mathcal{A}} + v_1$ и все элементы $v_i \in \mathcal{A}$, $i = 1, \ldots, k$, также нильпотентны. Тогда*

1) *найдутся индексы $1 \leqslant l < m \leqslant k$, такие что u_l, u_m линейно независимы по модулю $J(\mathcal{A})^2$, т. е.*

$$\langle u_l + J(\mathcal{A})^2,\, u_m + J(\mathcal{A})^2 \rangle = \langle x + J(\mathcal{A})^2,\, y + J(\mathcal{A})^2 \rangle;$$

2) *найдутся индексы $1 \leqslant q < r \leqslant k$, такие что v_q, v_r линейно независимы по модулю $J(\mathcal{A})^2$.*

Доказательство. Замечаем, что любое слово длины, не меньшей 2, от элементов $\{u_i \mid i = 1, \ldots, k\}$ либо от элементов $\{v_i \mid i = 1, \ldots, k\}$ содержится в $J(\mathcal{A})^2$. Значит, для того чтобы породить $J(\mathcal{A})$, необходимо выполнение условия

$$\langle u_i + J(\mathcal{A})^2 \mid i = 1, \ldots, k\rangle = \langle v_i + J(\mathcal{A})^2 \mid i = 1, \ldots, k\rangle = \\ = J(\mathcal{A})/J(\mathcal{A})^2 = \langle x + J(\mathcal{A})^2, y + J(\mathcal{A})^2\rangle. \quad \square$$

Лемма 2.8. *В условиях леммы 2.7*

1) *если $l > 1$, то можно выбрать базис $\{B_1, B_2\}$ пространства $\langle A_l, A_m\rangle$ вида*
$$B_1 = (x + Y_1, Z_1), \quad B_2 = (y + Y_2, Z_2),$$
где $Y_1, Y_2 \in J(\mathcal{A})^2$, $Z_1, Z_2 \in J(\mathcal{A})$; в противном случае $\langle A_1, A_m\rangle$ содержит базис $\{B_1, B_2\}$ вида
$$B_1 = \big(\beta x + Y_1,\, 1_{\mathcal{A}} + Z_1\big), \quad B_2 = (\gamma x + y + Y_2, Z_2),$$
где $\beta, \gamma \in \mathbb{F}$, $\beta \neq 0$, $Y_1, Y_2 \in J(\mathcal{A})^2$, $Z_1, Z_2 \in J(\mathcal{A})$. (Заметим, что не требуется рассматривать случай $B_1 = (\beta y + Y_1,\, 1 + Z_1)$, $B_2 = (\gamma y + x + Y_2, Z_2)$ отдельно, поскольку структура $J(\mathcal{A})$ симметрична относительно x, y.);
2) *если $q > 1$, то пространство $\langle A_q, A_r\rangle$ содержит базис $\{D_1, D_2\}$ вида*
$$D_1 = (U_1,\, x + W_1), \quad D_2 = (U_2,\, y + W_2),$$
где $U_1, U_2 \in J(\mathcal{A})$, $W_1, W_2 \in J(\mathcal{A})^2$; в противном случае $\langle A_1, A_r\rangle$ содержит базис $\{D_1, D_2\}$ одного из двух видов: либо
$$D_1 = (U_1,\, 1_{\mathcal{A}} + \delta x + W_1), \quad D_2 = (\gamma U_2, \varepsilon x + y + W_2),$$
либо
$$D_1 = (U_1,\, 1_{\mathcal{A}} + \delta y + W_1), \quad D_2 = (\gamma U_2, \varepsilon y + x + W_2),$$
где $\delta, \varepsilon \in \mathbb{F}$, $\delta \neq 0$, $U_1, U_2 \in J(\mathcal{A})$, $W_1, W_2 \in J(\mathcal{A})^2$.

Доказательство. Утверждение 1 аналогично пункту 4.a леммы 5.17 из [5]. Утверждение 2 аналогично пункту 4.b леммы 5.17 из [5]. $\square$

Рассмотрим по отдельности все возможности для значений l и q в нескольких последующих технических леммах.

Лемма 2.9. *В условиях леммы 2.8*

1) *если $l > 1$, то $J(\mathcal{A}) \oplus \{0\} \subset \mathcal{L}_{2p-1}(\{B_1, B_2, A_1\})$;*
2) *если $q > 1$, то $\{0\} \oplus J(\mathcal{A}) \subset \mathcal{L}_{2p-1}(\{D_1, D_2, A_1\})$;*
3) *если $l > 1$ и $q > 1$, то $J(\mathcal{A}) \oplus J(\mathcal{A}) \subset \mathcal{L}_{2p-1}(\mathcal{S})$.*

Доказательство. 1. Достаточно доказать, что базис

$$\{(x^i y^j, 0) \mid 0 \leqslant i, j \leqslant p-1,\ i+j \geqslant 1\}$$

пространства $J(\mathcal{A}) \oplus \{0\}$ содержится в пространстве $\mathcal{L}_{2p-1}(\{B_1, B_2, A_1\})$.

Используем индукцию по параметру $n = 2p-2-l(x^i y^j) = 2p-2-(i+j)$, $n = 0, \ldots, 2p-3$.

Начнём с базы индукции $n = 0$, т. е. базисного элемента $(x^{p-1}y^{p-1}, 0)$. Рассмотрим произведение $B_1^{p-1}B_2^{p-1} \in \mathcal{L}_{2p-2}(\{B_1, B_2\})$:

$$B_1^{p-1}B_2^{p-1} = (x^{p-1}y^{p-1}, Z_1^{p-1}Z_2^{p-1}),$$

где

$$Z_1^{p-1}Z_2^{p-1} \in J(\mathcal{A})^{2p-2}, \quad Z_1^{p-1}Z_2^{p-1} = \alpha x^{p-1}y^{p-1}.$$

Чтобы обнулить вторую координату, домножаем на $1_{\mathcal{B}} - A_1$. Получаем

$$B_1^{p-1}B_2^{p-1}(1_{\mathcal{B}} - A_1) =$$
$$= (x^{p-1}y^{p-1}(1_{\mathcal{A}} - u_1), -Z_1^{p-1}Z_2^{p-1}v_1) = (x^{p-1}y^{p-1}, 0) \in \mathcal{L}_{2p-1}(\{B_1, B_2, A_1\}),$$

поскольку $x^{p-1}y^{p-1}u_1, Z_1^{p-1}Z_2^{p-1}v_1 \in J(\mathcal{A})^{2p-1}$ и $J(\mathcal{A})^{2p-1} = \{0\}$.

Для n из промежутка $[1, 2p-3]$ и одночлена $f_t(x_1, x_2) \in \mathbb{F}[x_1, x_2]$ степени $t = 2p-2-n$ имеем

$$f_t(B_1, B_2)(1 - A_1)^{n+1} = (f_t(x, y) + V_{t+1}^f,\ f_t(Z_1, Z_2)(-v_1)^{n+1}),$$

где $V_{t+1}^f \in J(\mathcal{A})^{t+1}$ и $f_t(Z_1, Z_2)(-v_1)^{n+1} \in J(\mathcal{A})^{2p-1} = \{0\}$. Элемент V_{t+1}^f выражается через базисные слова радикала длин, не меньших $t+1$, поэтому по предположению индукции выполнено включение $(V_{t+1}^f, 0) \in \mathcal{L}_{2p-1}(\{B_1, B_2, A_1\})$. Следовательно,

$$(f_t(x, y), 0) = f_t(B_1, B_2)(1 - A_1)^{n+1} - (V_{t+1}^f, 0) \in \mathcal{L}_{2p-1}(\{B_1, B_2, A_1\}).$$

Поэтому пространство $\mathcal{L}_{2p-1}(\{B_1, B_2, A_1\})$ содержит стандартный базис пространства $J(\mathcal{A}) \oplus \{0\}$.

2. Повторяя тот же процесс с D_1, D_2 вместо B_1, B_2 и с A_1 вместо $1_{\mathcal{B}} - A_1$, получаем, что пространство $\mathcal{L}_{2p-1}(\{D_1, D_2, A_1\})$ содержит базис пространства $\{0\} \oplus J(\mathcal{A})$.

3. Поскольку по построению

$$\mathcal{L}_{2p-1}(\{B_1, B_2, A_1\}), \mathcal{L}_{2p-1}(\{D_1, D_2, A_1\}) \subseteq \mathcal{L}_{2p-1}(\mathcal{S}),$$

то, объединяя утверждения 1) и 2), получаем, что выполнено включение $J(\mathcal{A}) \oplus J(\mathcal{A}) \subset \mathcal{L}_{2p-1}(\mathcal{S})$. □

Лемма 2.10. *В условиях леммы 2.8, если $l = 1$ и $q > 1$, то $\mathcal{L}_{2p-1}(\mathcal{S}) \supset$ $\supset J(\mathcal{A}) \oplus J(\mathcal{A})$.*

Доказательство. Поскольку $q > 1$, то включение $\{0\} \oplus J(\mathcal{A}) \subset \mathcal{L}_{2p-1}(\mathcal{S})$ выполнено по лемме 2.9.

Остаётся доказать, что базис

$$\{(x^i y^j, 0) \mid 0 \leqslant i, j \leqslant p-1,\ i+j \geqslant 1\}$$

пространства $J(\mathcal{A}) \oplus \{0\}$ содержится в пространстве $\mathcal{L}_{2p-1}(\mathcal{S})$. Как и при доказательстве леммы 2.9, используем индукцию по параметру n — длине слова, $n = 0, \ldots, 2p-3$.

1. Начнём с базы индукции $n = 0$, т. е. базисного элемента $(x^{p-1}y^{p-1}, 0)$. Рассмотрим произведение $B_1^{p-1}B_2^{p-1} \in \mathcal{L}_{2p-2}(\mathcal{S})$:

$$B_1^{p-1}B_2^{p-1} = \big((\beta x + Y_1)^{p-1}, (1_{\mathcal{A}} + Z_1)^{p-1}\big) \cdot \big((\gamma x + y + Y_2)^{p-1}, Z_2^{p-1}\big).$$

Раскрывая скобки и учитывая, что $J(\mathcal{A})^{2p-1} = \{0\}$, получаем

$$B_1^{p-1}B_2^{p-1} = (\beta^{p-1}x^{p-1}y^{p-1}, T_2),$$

где $T_2 \in J(\mathcal{A})^{p-1}$.

Включение $(0, T_2) \in \mathcal{L}_{2p-1}(\mathcal{S})$ доказано выше. Значит, выполнено и включение $(x^{p-1}y^{p-1}, 0) = \beta^{1-p}(B_1^{p-1}B_2^{p-1} - (0, T_2)) \in \mathcal{L}_{2p-1}(\mathcal{S})$.

2. Для n из промежутка $[1, 2p-3]$ и одночлена $f_t(x_1, x_2) \in \mathbb{F}[x_1, x_2]$ степени $t = 2p - 2 - n$ имеем

$$f_t(B_1, B_2)(1 - A_1) = \big(f_t(\beta x, \gamma x + y) + V_{t+1}^f,\ -v_1 \cdot f_t(1 + Z_1, Z_2)\big),$$

где $V_{t+1}^f \in J(\mathcal{A})^{t+1}$ и $-v_1 \cdot f_t(1 + Z_1, Z_2) \in J(\mathcal{A})$. Включение

$$\big(0, -v_1 \cdot f_t(1 + Z_1, Z_2)\big) \in \mathcal{L}_{2p-1}(\mathcal{S})$$

следует из доказанного выше. Элемент V_{t+1}^f выражается через базисные слова радикала длин, не меньших $t+1$, поэтому по предположению индукции выполнено включение $(V_{t+1}^f, 0) \in \mathcal{L}_{2p-1}(\mathcal{S})$. Следовательно,

$$\begin{aligned}(f_t(\beta x, \gamma x + y), 0) &= \\ &= f_t(B_1, B_2)(1 - A_1) - (V_{t+1}^f, 0) + \big(0, v_1 \cdot f_t(1 + Z_1, Z_2)\big) \in \mathcal{L}_{2p-1}(\mathcal{S}).\end{aligned}$$

Поскольку $\beta \neq 0$, то $x, y \in \langle \beta x, \gamma x + y\rangle$. Поэтому для данного $t > 0$ пространство, порождённое множеством одночленов степени t от βx, $\gamma x + y$, содержит в себе все одночлены степени t от x, y. Окончательно заключаем, что множество $\{(x^i y^j, 0) \mid 0 \leqslant i, j \leqslant p-1,\ i+j \geqslant 1\}$ содержится в $\mathcal{L}_{2p-1}(\mathcal{S})$, что полностью доказывает утверждение леммы. □

Лемма 2.11. *В условиях леммы* 2.8 *если* $l > 1$ *и* $q = 1$, *то* $\mathcal{L}_{2p-1}(\mathcal{S}) \supset J(\mathcal{A}) \oplus J(\mathcal{A})$.

Доказательство. Утверждение следует из леммы 2.10 ввиду идентичности блоков алгебры $\mathcal{A} \oplus \mathcal{A}$. □

Лемма 2.12. *В условиях леммы* 2.8 *если* $l = 1$ *и* $q = 1$, *то* $\mathcal{L}_{3p-2}(\mathcal{S}) \supset J(\mathcal{A}) \oplus J(\mathcal{A})$.

Доказательство. Достаточно показать, что базис

$$\{(x^iy^j,0),(0,x^iy^j)\mid 0\leqslant i,j\leqslant p-1,\ i+j\geqslant 1\}$$

пространства $J(\mathcal{A})\oplus J(\mathcal{A})$ содержится в $\mathcal{L}_{2p-1}(\mathcal{S})$. Как и ранее, используем индукцию по параметру

$$n=2p-2-l(x^iy^j)=2p-2-(i+j),\quad n=0,\dots,2p-3.$$

1. Начнём с базы индукции $n=0$, т. е. базисных элементов $(x^{p-1}y^{p-1},0)$, $(0,x^{p-1}y^{p-1})$.

Рассмотрим произведение $B_1^{p-1}B_2^{p-1}\in\mathcal{L}_{2p-2}(\mathcal{S})$:

$$B_1^{p-1}B_2^{p-1}=(\beta^{p-1}x^{p-1}y^{p-1},T_2),$$

где $T_2\in J(\mathcal{A})^{p-1}$. Далее перейдём к произведению

$$B_1^{p-1}B_2^{p-1}(1-A_1)^p=(\beta^{p-1}x^{p-1}y^{p-1},T_2(-v_1)^p)\in\mathcal{L}_{3p-2}(\mathcal{S}),$$

$T_2(-v_1)^p=0$. Следовательно, $(x^{p-1}y^{p-1},0)\in\mathcal{L}_{3p-2}(\mathcal{S})$. Аналогично, рассматривая произведение

$$(D_1-1_{\mathcal{B}})^{p-1}D_2^{p-1}A_1^p=(0,\delta^{p-1}x^{p-1}y^{p-1})\in\mathcal{L}_{3p-2}(\mathcal{S}),$$

заключаем, что $(0,x^{p-1}y^{p-1})\in\mathcal{L}_{3p-2}(\mathcal{S})$.

2. Пусть n лежит в промежутке $[1,2p-3]$. Рассматриваем произвольный одночлен $f_t(x_1,x_2)\in\mathbb{F}[x_1,x_2]$ степени $t=2p-2-n$.

Имеем

$$f_t(B_1,B_2)(1-A_1)^p=$$
$$=(f_t(\beta x,\gamma x+y)+V_{t+1}^f,f_t(1+Z_1,Z_2)(-v_1)^p)=(f_t(\beta x,\gamma x+y)+V_{t+1}^f,0),$$

где $V_{t+1}^f\in J(\mathcal{A})^{t+1}$. Элемент V_{t+1}^f выражается через базисные слова радикала длин, не меньших $t+1$, поэтому по предположению индукции выполнено включение $(V_{t+1}^f,0)\in\mathcal{L}_{3p-2}(\mathcal{S})$. Следовательно,

$$(f_t(\beta x,\gamma x+y),0)=f_t(B_1,B_2)(1-A_1)^p-(V_{t+1}^f,0)\in\mathcal{L}_{3p-2}(\mathcal{S}).$$

Как показано в пункте 2 доказательства леммы 2.10, отсюда сразу следует, что множество $\{(x^iy^j,0)\mid 0\leqslant i,j\leqslant p-1,\ i+j\geqslant 1\}$ содержится в $\mathcal{L}_{3p-2}(\mathcal{S})$.

Аналогично, рассматривая произведение $f_t(D_1-1_{\mathcal{B}},D_2)A_1^p\in\mathcal{L}_{3p-2}(\mathcal{S})$, получаем, что

$$f_t(D_1-1_{\mathcal{B}},D_2)A_1^p=(0,f_t(\delta x,\varepsilon x+y)+W_{t+1}^f)$$

либо

$$f_t(D_1-1_{\mathcal{B}},D_2)A_1^p=(0,f_t(\delta y,\varepsilon y+x)+W_{t+1}^f),$$

где $W_{t+1}^f\in J(\mathcal{A})^{t+1}$. Пользуясь предположением индукции для элемента $(0,W_{t+1}^f)$, заключаем, что $\big(0,f_t(\delta x,\varepsilon x+y)\big)\in\mathcal{L}_{3p-2}(\mathcal{S})$ или $\big(0,f_t(\delta y,\varepsilon y+x)\big)\in\mathcal{L}_{3p-2}(\mathcal{S})$ соответственно. Отсюда следует, что множество

$$\{(0,x^iy^j)\mid 0\leqslant i,j\leqslant p-1,\ i+j\geqslant 1\}$$

содержится в $\mathcal{L}_{3p-2}(\mathcal{S})$. □

Лемма 2.13. *Пусть $\mathcal{S} = \{A_i \mid i = 1, \ldots, k\}$ — произвольная система порождающих алгебры $\mathcal{B} = \mathcal{A} \oplus \mathcal{A}$. Предположим, что $A_1 = (u_1, w_1)$, $A_i = (u_i, v_i)$, где все элементы $u_i \in \mathcal{A}$, $i = 1, \ldots, k$, нильпотентны, $w_1 = 1_{\mathcal{A}} + v_1$ и все элементы $v_i \in \mathcal{A}$, $i = 1, \ldots, k$, также нильпотентны. Тогда $l(\mathcal{S}) \leqslant 3p - 2$.*

Доказательство. По лемме 2.8, система порождающих $\mathcal{S}$ удовлетворяет условиям одной из лемм 2.9—2.12. Следовательно, пространство $\mathcal{L}_{3p-2}(\mathcal{S})$ содержит базис пространства $J(\mathcal{A}) \oplus J(\mathcal{A})$.

Пара элементов $1_{\mathcal{B}}$ и A_1 из $\mathcal{L}_1(\mathcal{S})$ линейно независима по модулю пространства $J(\mathcal{A}) \oplus J(\mathcal{A})$, следовательно, вместе с базисом пространства $J(\mathcal{A}) \oplus J(\mathcal{A})$ это множество образует базис алгебры $\mathcal{A} \oplus \mathcal{A}$.

Окончательно заключаем, что $l(\mathcal{S}) \leqslant 3p - 2$. □

Теперь докажем основной результат.

Теорема 2.14. *Пусть $\mathbb{F}$ — поле характеристики $p > 2$. Тогда*

$$l(\mathbb{F}[\mathbb{Z}_2 \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p]) = 3p - 2.$$

Доказательство. 1. Сначала докажем верхнюю оценку $l(\mathbb{F}[\mathbb{Z}_2 \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p]) \leqslant$ $\leqslant 3p - 2$.

Поскольку поле $\mathbb{F}$ содержит элемент $-1 \neq 1$, то имеет место изоморфизм алгебр $\mathbb{F}\mathbb{Z}_2 \cong \mathbb{F}[x]/(x^2 - 1) \cong \mathbb{F} \oplus \mathbb{F}$. Поэтому $\mathbb{F}[\mathbb{Z}_2 \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p] \cong \mathcal{A} \oplus \mathcal{A}$, где $\mathcal{A}$ — групповая алгебра $\mathbb{F}[\mathbb{Z}_p \oplus \mathbb{Z}_p]$.

Рассмотрим произвольную систему порождающих $\mathcal{S}$ алгебры $\mathcal{A} \oplus \mathcal{A}$. По лемме 2.6 без ограничения общности можно считать, что $\mathcal{S}$ удовлетворяет условиям леммы 2.13. Отсюда получаем, что $l(\mathcal{S}) \leqslant 3p - 2$. Следовательно,

$$l(\mathbb{F}[\mathbb{Z}_2 \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p]) = l(\mathcal{A} \oplus \mathcal{A}) = \max\{l(\mathcal{S})\colon \mathcal{L}(\mathcal{S}) = \mathcal{A} \oplus \mathcal{A}\} \leqslant 3p - 2.$$

2. Для доказательства нижней оценки рассмотрим пару

$$\{X = (x, x + 1),\ Y = (y, y)\},$$

где x, y — элементы, определённые в лемме 2.1. Поскольку $X^p = (0, 1_{\mathcal{A}})$ и пара $\{x, y\}$ порождает $J(\mathcal{A})$ как алгебру, то пара $\{X, Y\}$ порождает алгебру $\mathcal{A} \oplus \mathcal{A}$.

Непосредственно посчитаем количество нетривиальных слов от X, Y. Заметим, что $Y^p = 0$, в то время как X имеет минимальный многочлен $t^p(t-1)^p$ степени $2p$. Таким образом, нам подходят слова, в которые входит не более $p-1$ букв Y и не более $2p - 1$ букв X, что даёт $p \cdot 2p = 2p^2$ слов длины, не большей $3p - 2$, и $2p^2 - 1$ слов длины, строго меньшей $3p - 2$. Следовательно,

$$\dim \mathcal{L}_{3p-3}(\mathcal{S}) \leqslant 2p^2 - 1 < 2p^2 = \dim \mathcal{A} \oplus \mathcal{A}.$$

Тогда $l(\mathcal{S}) \geqslant 3p - 2$. Поэтому, учитывая верхнюю оценку из пункта 1, получаем, что $l(\mathcal{S}) = 3p - 2$, что и требовалось. □

Данная теорема обобщает теорему 5.2 из [12], в которой аналогичный результат был получен для случая $p = 3$.

Замечание 2.15. Поскольку методика, использованная в доказательстве теоремы 2.14, аналогична методике, используемой в [5, раздел 5.1.1] (особенно [5, лемма 5.23]), можно ожидать её дальнейшего обобщения на случай групповой алгебры группы $\mathbb{Z}_2 \oplus P$, где P — конечная абелева p-группа нечётного порядка над полем характеристики p. Для вычисления длины в случае групповой алгебры группы $\mathbb{Z}_3 \oplus P$, где P — конечная абелева p-группа порядка, не делящегося на 3, над полем характеристики p, возможно использовать тот же подход, что и при доказательстве теоремы 5.40 из [5, раздел 5.1.2].

Литература

[1] Гутерман А. Э., Маркова О. В. Длина групповых алгебр групп небольшого размера // Зап. научн. сем. ПОМИ. — 2018. — Т. 472. — С. 76—87.

[2] Колегов Н. А., Маркова О. В. Системы порождающих матричных алгебр инцидентности над конечными полями // Зап. научн. сем. ПОМИ. — 2018. — Т. 472. — С. 120—144.

[3] Коусело Е., Гонсалес С., Марков В. Т., Мартинес К., Нечаев А. А. Представления кодов Рида—Соломона и Рида—Маллера идеалами, // Алгебра и логика. — 2012. — Т. 51, № 3. — С. 297—320.

[4] Маркова О. В. Верхняя оценка длины коммутативных алгебр // Матем. сб. — 2009. — Т. 200, № 12. — С. 41—62.

[5] Маркова О. В. Функция длины и матричные алгебры // Фундамент. и прикл. матем. — 2012. — Т. 17, вып. 6. — С. 65—173.

[6] Маркова О. В. О связи длины алгебры и индекса нильпотентности её радикала Джекобсона // Матем. заметки. — 2013. — Т. 94, № 5. — С. 682—688.

[7] Тумайкин И. Н. Базисные коды Рида—Маллера как групповые коды // Фундамент. и прикл. матем. — 2013. — Т. 18, № 4. — С. 137—154.

[8] Тумайкин И. Н. Идеалы групповых колец, связанные с кодами Рида—Маллера // Фундамент. и прикл. матем. — 2016. — Т. 21, № 1. — С. 211—215.

[9] Couselo E., González S., Markov V., Martínez C., Nechaev A. Some constructions of linearly optimal group codes // Linear Algebra Appl. — 2010. — Vol. 433, no. 2. — P. 356—364.

[10] García Pillado C., González S., Markov V., Markova O., Martínez C. Group codes of dimension 2 and 3 are Abelian // Finite Fields Appl. — 2019. — Vol. 55. — P. 167—176.

[11] González S., Markov V., Markova O., Martínez C. Group codes // Algebra, Codes and Cryptology. A2C 2019 / C. Gueye, E. Persichetti, P.-L. Cayrel, J. Buchmann, eds. — Berlin: Springer, 2019. — (Commun. Comput. Inform. Sci.; Vol. 1133). — P. 83—96.

[12] Guterman A. E., Khrystik M. A., Markova O. V. On the lengths of group algebras of finite Abelian groups in the modular case: Preprint. — 2020.

[13] Guterman A. E., Khrystik M. A., Markova O. V. On the lengths of group algebras of finite Abelian groups in the semi-simple case: Preprint. — 2020.

[14] Guterman A., Laffey T., Markova O., Šmigoc H. A resolution of Paz's conjecture in the presence of a nonderogatory matrix // Linear Algebra Appl. — 2018. — Vol. 543. — P. 234—250.

[15] Guterman A. E., Markova O. V. Commutative matrix subalgebras and length function // Linear Algebra Appl. — 2009. — Vol. 430. — P. 1790—1805.

[16] Guterman A. E., Markova O. V. The length of the group algebra of the group $\mathbf{Q}_8$ // New Trends in Algebra and Combinatorics. Proc. of the 3rd Int. Congress in Algebra and Combinatorics / K. P. Shum, E. Zelmanov, P. Kolesnikov, A. Wong, eds. — Singapore: World Scientific, 2019. — P. 106—134.

[17] Jennings S. A. The structure of the group ring of a p-group over a modular field // Trans. Am. Math. Soc. — 1941. — Vol. 50. — P. 175—185.

[18] Pappacena C. J. An upper bound for the length of a finite-dimensional algebra // J. Algebra. — 1997. — Vol. 197. — P. 535—545.

[19] Passman D. S. The Algebraic Structure of Group Rings. — New York: Wiley, 1977.

[20] Paz A. An application of the Cayley—Hamilton theorem to matrix polynomials in several variables // Linear Multilinear Algebra. — 1984. — Vol. 15. — P. 161—170.

[21] Pierce R. Associative Algebras. — Berlin: Springer, 1982.