О. В. Маркова, М. А. Хрыстик, Длина групповой алгебры группы диэдра порядка 2^k, *Зап. научн. сем. ПОМИ*, 2020, том 496, 169–181

Записки научных
семинаров ПОМИ
Том 496, 2020 г.

О. В. Маркова, М. А. Хрыстик

ДЛИНА ГРУППОВОЙ АЛГЕБРЫ ГРУППЫ ДИЭДРА ПОРЯДКА 2^k

§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 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 $\mathcal{A}$, $l(\mathcal{A})$, назовём максимальную длину среди её систем порождающих (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 [16] и до сих пор является открытой. Вычисление длины в общем случае является довольно трудной задачей. Нетривиальная верхняя оценка длины произвольной алгебры получена в работе К. Паппачены [14]. Основные алгебраические свойства функции длины были изучены О. В. Марковой в работе [12].

Отдельный интерес представляет вопрос вычисления длины групповых алгебр. Ввиду наличия их матричных представлений, решение

Ключевые слова: конечномерные алгебры, длина алгебры, групповые алгебры, диэдральная группа.

Работа выполнена при финансовой поддержке РНФ (грант No. 17-11-01124.)

этого вопроса тесно связано и с решением проблемы Паза. Для групповых алгебр групп малых порядков удаётся точно вычислить длину над произвольными полями; так для группы подстановок S_3, группы Клейна V_4 и группы кватернионов Q_8 значения длины найдены в [4,5].

Систематическому изучению общей задачи нахождения длины групповых алгебр конечных абелевых групп посвящены работы [6, 7]. В работе [7] для получения оценки длины групповых алгебр использованы методы теории полей, теории колец и оценка длины коммутативных алгебр (см. [11, 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. [13, теорема 1, следствие 1], теорема 2.8). Вычисление индекса нильпотентности радикала Джекобсона групповой алгебры основано на *теории Дженнингса* (см. [9], [15, Глава 11, §1], теорема 4.4).

Аналогичное исследование всех неабелевых групп представляется слишком трудным ввиду разнообразия их структур. Поэтому предлагается исследовать функцию длины для семейств классических неабелевых групп по отдельности. Так, в работе [10] 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 имеют порядок один, в то время как размеры матричных алгебр в разложении в прямую сумму групповых алгебр диэдральных групп не превышают двух. В данной работе мы продолжаем исследование длины групповых алгебр диэдральных групп и вычисляем их длины в модулярном случае в предположении, что рассматриваемые группы являются 2-группами.

Пусть $\mathbb{F}$ – произвольное поле и G – конечная группа. Через $\mathbb{F}G$ будем обозначать групповую алгебру группы G над полем $\mathbb{F}$. Пусть также $\mathbf{D}_n$ – диэдральная группа порядка $2n$.

Исследуя вопросы связанные с образующими групповых алгебр, в качестве порождающей системы групповой алгебры $\mathbb{F}G$ естественно рассматривать 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 $g \in G$. Основное отличие заключается в

том, что при решении соответствующих групповых задач алфавит, по определению, расширяется всеми обратными к элементам порождающего множества, и рассматриваются слова от элементов $S \cup S^{-1}$. *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 [1] получены асимптотические оценки диаметра групп. 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. Задача получения верхних оценок и, тем более, точного вычисления длин конкретных групповых алгебр остаётся актуальной.

В работе [10] был получен следующий результат для полупростого случая (т.е. случая, когда характеристика поля не делит порядок группы).

Теорема 1.1 ([10, теорема 1.15]). *Пусть* $\mathbb{F}$ *– поле,* $\operatorname{char}\mathbb{F} \nmid 2n$, $n \geqslant 3$. *Тогда* $l(\mathbb{F}\mathbf{D}_n) = n$.

Отметим, что значение длины n реализуемо на групповой системе образующих группы диэдра (лемма 3.6), т.е. для данной групповой алгебры рассмотрение систем образующих, отличных от порождающих множеств группы, не повышает значения длины.

В данной работе мы рассмотрим различные подходы к изучению длины этой алгебры в модулярном случае.

В §2 приведены основные определения и общие результаты о функции длины, используемые в работе.

§3 посвящен нахождению длины алгебры $\mathbb{F}\mathbf{D}_4$. Результат основан на вычислении такого инварианта, как максимальная степень минимального многочлена, где максимум берётся по всем элементам алгебры, и применении общей оценки длины, содержащей этот инвариант.

В §4 длина алгебр $\mathbb{F}\mathbf{D}_{2^k}$, $k \geqslant 2$, вычислена другим методом, который ранее был использован для изучения длины групповых алгебр только в абелевом случае. А именно, вычислен индекс нильпотентности радикала Джекобсона и применена общая оценки длины, содержащая этот инвариант.

§2. Основные определения и используемые результаты о функции длины

Сперва напомним основные определения, связанные с функцией длины.

Пусть $B = \{b_1, \dots, b_M\}$ – 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 $v = b_{i_1} \dots b_{i_t}$, $b_{i_j} \in B$, 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 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 найдётся 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 найдётся такой номер h, что $\mathcal{L}_h(\mathcal{S}) = \mathcal{L}_{h+1}(\mathcal{S})$. Если для некоторого $h \geqslant 0$ выполнено равенство $\mathcal{L}_h(\mathcal{S}) = \mathcal{L}_{h+1}(\mathcal{S})$, 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 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

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

Для длины алгебры всегда справедлива следующая тривиальная верхняя оценка.

Замечание 2.6 ([11, лемма 5.3])**.** Пусть $\mathcal{A}$ – алгебра размерности d над произвольным полем. Тогда $l(\mathcal{A}) \leqslant d-1$, причём оценка превращается в равенство тогда и только тогда, когда алгебра $\mathcal{A}$ является однопорождённой, из чего автоматически следует, что она коммутативна.

Обозначение 2.7. 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 $\deg a \leqslant \dim \mathcal{A}$. Тогда для любого непустого подмножества $\mathcal{B} \subseteq \mathcal{A}$ положим $m(\mathcal{B}) = \max\{\deg b : b \in \mathcal{B}\}$.

Приведём основной результат работы [13], позволяющий получить верхнюю оценку длины алгебры в терминах длины её фактор-алгебры по радикалу Джекобсона и индекса нильпотентности радикала.

Теорема 2.8 ([13, теорема 1, следствие 1])**.** *Пусть* $\mathbb{F}$ *– произвольное поле и* $\mathcal{A}$ *–* $\mathbb{F}$*-алгебра. Через* $N = N(J(\mathcal{A}))$ *обозначим индекс нильпотентности радикала Джекобсона* $J(\mathcal{A})$ *алгебры* $\mathcal{A}$*. Тогда*

$$l(\mathcal{A}) \leqslant (l(\mathcal{A}/J(\mathcal{A})) + 1)N - 1.$$

Докажем следующую общую оценку длины алгебры, которая понадобится для доказательства основного утверждения §3. В её доказательстве будет использовано утверждение о сохранении длины системы образующих при выделении линейно независимой системы. Приведём его формулировку для полноты изложения.

Утверждение 2.9 ([12, 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 2.10. *Пусть $\mathcal{A}$ – $\mathbb{F}$-алгебра, $\dim \mathcal{A} \leqslant m(\mathcal{A}) + 4$, $m(\mathcal{A}) \geqslant 3$. Тогда $l(\mathcal{A}) \leqslant m(\mathcal{A})$.*

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 2.9). 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 слове 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 $\dim \mathcal{L}_{m(\mathcal{A})}(\mathcal{S}) = \dim\langle 1_{\mathcal{A}}, A_1, B_1, A_2, B_2, \dots, A_{m(\mathcal{A})}, B_{m(\mathcal{A})}\rangle = 2m(\mathcal{A}) + 1$. 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 $m(\mathcal{A}) \geqslant 3$ 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. □

§3. Длина алгебры $\mathbb{F}\mathbf{D}_4$

Далее в данном тексте $\mathbb{F}$ – 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 $\mathbb{F}\mathbf{D}_4$, состоящий из элементов группы $\mathbf{D}_4$. Рассмотрим базис $S = \{e, r^2, r+r^3, s+sr^2, sr+sr^3, r^3, sr^2, sr^3\}$. Обозначим через S_c множество $\{e, r^2, r+r^3, s+sr^2, sr+sr^3\}$, а через S_{nc} – множество $\{r^3, sr^2, sr^3\}$. Обозначим $\langle S\rangle$ через L, $\langle S_c\rangle$ через L_c, $\langle S_{nc}\rangle$ через L_{nc}. Тогда $L = L_c \oplus L_{nc}$, $L = \mathbb{F}\mathbf{D}_4$ как множества. Заметим, что L_c лежит в центре алгебры $\mathbb{F}\mathbf{D}_4$ (даже если $\mathbb{F}$ имеет произвольную характеристику).

Утверждение 3.1. *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 факта, что $\operatorname{char}\mathbb{F} = 2$, получаем $v^2 = \lambda_1^2 e^2 + \lambda_2^2 (r^2)^2 + \lambda_3^2 (r+r^3)^2 + \lambda_4^2 (s+sr^2)^2 + \lambda_5^2 (sr+sr^3)^2$. 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 3.2. *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 $v^2 = \lambda_1^2(r^3)^2 + \lambda_2^2(sr^2)^2 + \lambda_3^2(sr^3)^2 + \lambda_1\lambda_2(r^3sr^2 + sr^2r^3) + \lambda_1\lambda_3(r^3sr^3 + sr^3r^3) + \lambda_2\lambda_3(sr^2sr^3 + sr^3sr^2)$. Но $(r^3)^2 = r^2$, $(sr^2)^2 = e$, $(sr^3)^2 = e$, $r^3sr^2 + sr^2r^3 = sr^3 + sr$, $r^3sr^3 + sr^3r^3 = s + sr^2$, $sr^2sr^3 + sr^3sr^2 = r + r^3$. Таким образом, $v^2 \in L_c$. □

Утверждение 3.3. *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 $v^2 = v_c^2 + v_cv_{nc} + v_{nc}v_c + v_{nc}^2$. В силу того, что L_c лежит в центре L и $\operatorname{char}\mathbb{F} = 2$, получаем $v_cv_{nc} + v_{nc}v_c = 2v_cv_{nc} = 0$. Согласно утверждению 3.1, имеем $v_c^2 \in \langle e\rangle \in L_c$. В силу утверждения 3.2, $v_{nc}^2 \in L_c$. Следовательно, $v^2 \in L_c$. □

Утверждение 3.4. *Пусть* $v \in L$. *Тогда* $v^4 \in \langle e\rangle$.

Доказательство. По условию, $v \in L$. Тогда, в силу утверждения 3.3, $v^2 \in L_c$. Следовательно, из утверждения 3.1 получаем, что $(v^2)^2 \in \langle e\rangle$. Таким образом, $v^4 \in \langle e\rangle$. □

Лемма 3.5. *Пусть* $\operatorname{char}\mathbb{F} = 2$. *Тогда* $m(\mathbb{F}\mathbf{D}_4) = 4$.

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

Покажем, что $m(\mathbb{F}\mathbf{D}_4) \leqslant 4$. Действительно, пусть $v \in \mathbb{F}\mathbf{D}_4 = L$. Тогда, в силу утверждения 3.4, $v^4 = \lambda e$. Таким образом, многочлен $t^4 - \lambda$ является аннулирующим для v и $m(v) \leqslant 4$. В силу произвольности выбора v, получаем требуемое неравенство, что завершает доказательство леммы. □

Лемма 3.6 ([10, лемма 2.1])**.** *Пусть* $\mathbf{D}_n$ – *группа диэдра порядка* $2n$, $n \geqslant 3$, $\mathbb{F}$ – *произвольное поле. Тогда* $l(\mathbb{F}\mathbf{D}_n) \geqslant n$.

Доказательство. Предъявим систему порождающих длины не меньшей n. Пусть r – поворот на угол $\frac{2\pi}{n}$, а s – симметрия вокруг некоторой оси. Тогда $\mathcal{S} = \{rs, s\} = \{a, b\}$ – система порождающих для рассматриваемой алгебры. Действительно, произведением двух данных симметрий можно получить поворот r и породить вместе с симметрией s всю алгебру.

Докажем, что данная система порождающих имеет длину не меньшую n. Заметим, что квадрат любого образующего равен единице. Значит, несократимыми словами от образующих могут быть только два слова для каждой длины (слова $abab\ldots$ и $baba\ldots$), кроме нулевой длины, где будет только единица. Следовательно, $\dim \mathcal{L}_{n-1}(\mathcal{S}) \leqslant (n-1)\cdot 2 +1 < 2n$, то есть $l(\mathcal{S}) \geqslant n$. □

Теорема 3.7. *Пусть* $\operatorname{char}\mathbb{F} = 2$. *Тогда* $l(\mathbb{F}\mathbf{D}_4) = 4$.

Доказательство. В силу леммы 3.6, получаем $l(\mathbb{F}\mathbf{D}_4) \geqslant 4$. По лемме 3.5, $m(\mathbb{F}\mathbf{D}_4) = 4$; кроме того, $\dim \mathbb{F}\mathbf{D}_4 = 8$. Таким образом, алгебра $\mathbb{F}\mathbf{D}_4$ удовлетворяет условиям леммы 2.10, применяя которую, получаем оценку $l(\mathbb{F}\mathbf{D}_4) \leqslant m(\mathbb{F}\mathbf{D}_4) = 4$. □

§4. Длина алгебры $\mathbb{F}\mathbf{D}_{2^k}$

В работе [7] для получения оценки длины групповых алгебр использованы методы теории полей, теории колец и оценка длины коммутативных алгебр (см. [11, теорема 3.11]). В той же работе вычисление длины алгебры сведено к вычислению длины фактор-алгебры по радикалу Джекобсона и индекса нильпотентности радикала (см. [13, теорема 1, следствие 1]). Вычисление индекса нильпотентности радикала Джекобсона групповой алгебры основано на *теории Дженнингса* (см. [9], [15, Глава 11, §1]). В данном параграфе мы применим те же методы для диэдральных групп.

Напомним некоторые понятия теории идеалов.

Определение 4.1. *Фундаментальный идеал* алгебры $\mathbb{F}G$ – это

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

Лемма 4.2 ([15, лемма 3.1.6])**.** *Если G – конечная p-группа, то идеал $\Delta(\mathbb{F}G)$ совпадает с радикалом Джекобсона $J(\mathbb{F}G)$ алгебры $\mathbb{F}G$.*

Определение 4.3 ([15, глава 3, §3, определение перед леммой 3.2])**.** Для заданного поля $\mathbb{F}$ последовательность *размерных подгрупп* группы G, соответствующих фундаментальному идеалу алгебры $\mathbb{F}G$, определяется по правилу

$$\mathcal{D}(\mathbb{F}G)_t = \{x \in G :\ x - 1 \in \Delta(\mathbb{F}G)^t\}.$$

Эта последовательность подгрупп определяет многие свойства степеней фундаментального идеала группового кольца (см. [15, глава 3, §3], недавний обзор [8] и их библиографию). 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 имеют приложения в теории кодирования. Они используются в работах [2,3,18,19] для построения некоторых линейно оптимальных кодов, кодов Рида–Соломона и кодов Рида–Маллера соответственно.

В частности, нам понадобится следующий результат об индексе нильпотентности идеала $\Delta(\mathbb{F}G)$.

Теорема 4.4 (Формула Дженнингса [15, глава 3, §3, лемма 3.2, теоремы 3.6–3.7])**.** *Пусть $\mathbb{F}$ – поле характеристики $p > 0$ и пусть G – конечная p-группа.*

Через N обозначим индекс нильпотентности идеала $\Delta(\mathbb{F}G)$. Положим $d_t = |\mathcal{D}(\mathbb{F}G)_t/\mathcal{D}(\mathbb{F}G)_{t+1}|$. Тогда

$$N = 1 + (p-1)\sum_t t \log_p d_t.$$

Следующие результаты показывают, как в общем случае найти размерные подгруппы.

Обозначение 4.5. Для подгруппы K группы G через $[K, G]$ обозначим подгруппу группы G, порождённую всеми коммутаторами $[x, y]$, где $x \in K$ и $y \in G$. Для подгруппы H через $H^{(t)}$ обозначим подгруппу, порождённую t-ми степенями элементов группы H.

Определение 4.6 ([15, Глава 11, §1, определение перед леммой 1.17])**.** Для фиксированного простого числа p *последовательность Брауэра–Дженнингса–Цассенхауза* (или $\mathcal{M}$-*последовательность*) подгрупп группы G определяется индуктивно правилами $\mathcal{M}_1 = \mathcal{M}_{1,p}(G) = G$ и

$$\mathcal{M}_{i+1} = \mathcal{M}_{i+1,p}(G) = [\mathcal{M}_i, G]\mathcal{M}_j^{(p)}$$

для всех $i \geqslant 1$, где j – наименьшее неотрицательное целое число, удовлетворяющее неравенству $j \geqslant \dfrac{i+1}{p}$.

Теорема 4.7 ([15, глава 11, §1, теорема 1.19])**.** *Для группы G и поля $\mathbb{F}$ характеристики p размерные подгруппы, соответствующие кольцу*

$\mathbb{F}G$, определяются равенством

$$\mathcal{D}_t(\mathbb{F}G) = \mathcal{M}_t.$$

Перейдём к вычислениям для групповой алгебры группы диэдра.

Лемма 4.8 ([17, предложение 4.15])**.** *Пусть $\mathbf{D}_{2^k}$ – группа диэдра порядка 2^{k+1}. Пусть $r \in \mathbf{D}_{2^k}$ – поворот на угол $\frac{\pi}{2^{k-1}}$. Тогда*

$$\mathcal{M}_{2^j+1}(\mathbf{D}_{2^k}) = \cdots = \mathcal{M}_{2^{j+1}}(\mathbf{D}_{2^k}) = \langle r^{2^{j+1}} \rangle$$

для всех $j = 0, \ldots, k-2$ и $\mathcal{M}_t(\mathbf{D}_{2^k}) = \{e\}$ при всех $t \geqslant 2^{k-1}+1$.

Лемма 4.9. *Пусть* $\operatorname{char}\mathbb{F} = 2$. *Тогда $N(J(\mathbb{F}\mathbf{D}_{2^k})) = 2^k + 1$.*

Доказательство. Для краткости положим $G = \mathbf{D}_{2^k}$. Воспользуемся теоремой 4.4. По лемме 4.8 имеем:

$$d_1 = |\mathcal{M}_1(G)/\mathcal{M}_2(G)| = \frac{|G|}{|\langle r^2 \rangle|} = 4,$$

$$d_{2^j} = |\mathcal{M}_{2^j}(G)/\mathcal{M}_{2^j+1}(G)| = \frac{|\langle r^{2^j} \rangle|}{|\langle r^{2^{j+1}} \rangle|} = 2$$

для всех $j = 1, \ldots, k-1$,
$d_t = 1$ для всех остальных t, $3 \leqslant t \leqslant 2^{k-1}-1$. Тогда

$$N(J(\mathbb{F}\mathbf{D}_{2^k})) = 1 + \sum_t t \log_2 d_t = 1 + 2 + \sum_{j=1}^{k-1} 2^j = 2 + \sum_{j=0}^{k-1} 2^j = 2 + (2^k - 1) = 2^k + 1.$$

□

Теорема 4.10. *Пусть* $\operatorname{char}\mathbb{F} = 2$. *Тогда $l(\mathbb{F}\mathbf{D}_{2^k}) = 2^k$.*

Доказательство. Положим $G = \mathbf{D}_{2^k}$.

Для доказательства верхней оценки $l(\mathbb{F}G) \leqslant 2^k$ воспользуемся теоремой 2.8 и леммой 4.9. Поскольку $\dim_{\mathbb{F}} \mathbb{F}G/J(\mathbb{F}G) = 1$ и данная алгебра содержит единицу, то $\mathbb{F}G/J(\mathbb{F}G) \cong \mathbb{F}$ и $l(\mathbb{F}G/J(\mathbb{F}G)) = l(\mathbb{F}) = 0$. Получаем $l(\mathbb{F}G) \leqslant (l(\mathbb{F}G/J(\mathbb{F}G))+1)N(J(\mathbb{F}G))-1 = N(J(\mathbb{F}G))-1 = 2^k$.

Нижняя оценка следует из леммы 3.6. □

Авторы выражают глубокую благодарность А. Э. Гутерману за полезные обсуждения при подготовке статьи.

Список литературы

1. L. Babai, Á. Seress, *On the diameter of permutation groups.* — Eur. J. Combin. **13**, No. 4 (1992), 231–243.
2. E. Couselo, S. González, V. Markov, C. Martínez, A. Nechaev, *Some constructions of linearly optimal group codes.* — Linear Algebra Appl. **433**, No. 2 (2010), 356–364.
3. Е. Коусело, С. Гонсалес, В. Т. Марков, К. Мартинес, А. А. Нечаев, *Представления кодов Рида–Соломона и Рида–Маллера идеалами.* — Алгебра и логика **51**, No. 3 (2012), 297–320.
4. А. Э. Гутерман, О. В. Маркова, *Длина групповых алгебр групп небольшого размера.* — Зап. научн. семин. ПОМИ **472** (2018), 76–87.
5. 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.
6. A. E. Guterman, O. V. Markova, M. A. Khrystik, *On the lengths of group algebras of finite Abelian groups in the semi-simple case.* Preprint, 2020.
7. A. E. Guterman, M. A. Khrystik, O. V. Markova, *On the lengths of group algebras of finite Abelian groups in the modular case.* Preprint, 2020.
8. T. Hurley, *Dimension and Fox subgroups.* — Resenhas IME-USP **5**, No. 4 (2002), 293–304.
9. 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.
10. M. A. Khrystik, O. V. Markova, *On the length of the group algebra of the dihedral group in the semi-simple case.* Preprint, 2020.
11. О. В. Маркова, *Верхняя оценка длины коммутативных алгебр.* — Матем. сб. **200**, No. 12 (2009), 41–62.
12. О. В. Маркова, *Функция длины и матричные алгебры.* — Фунд. прикл. матем. **17**, No. 6 (2012), 65–173.
13. О. В. Маркова, *О связи длины алгебры и индекса нильпотентности ее радикала Джекобсона.* — Матем. заметки **94**, No. 5 (2013), 682–688.
14. C. J. Pappacena, *An upper bound for the length of a finite-dimensional algebra.* — J. Algebra **197** (1997), 535–545.
15. D. S. Passman, *The Algebraic Structure of Group Rings.* John Wiley & Sons, New York, London, Sydney, Toronto, 1977.
16. A. Paz, *An application of the Cayley–Hamilton theorem to matrix polynomials in several variables.* — Linear Multilinear Algebra **15** (1984), 161–170.
17. J. N. Roksvold, *Applying Jennings theory and the $\mathcal{M}$-series to modular isomorphism problems.* Thesis for the degree of Master in Mathematics (Master of Science), Department of Mathematics, Faculty of Mathematics and Natural Sciences, University of Oslo, 2011.
18. И. Н. Тумайкин, *Базисные коды Рида–Маллера как групповые коды.* — Фунд. прикл. матем. **18**, No. 4 (2013), 137–154.
19. И. Н. Тумайкин, *Идеалы групповых колец, связанные с кодами Рида–Маллера.* — Фунд. прикл. матем. **21**, No. 1 (2016), 211–215.

Markova O. V., Khrystik M. A. The length of the group algebra of the dihedral group of order 2^k.

In this paper, the length of the group algebra of a dihedral group in the modular case is computed under the assumption that the order of the group is a power of two. Various methods for studying the length of a group algebra in the modular case are considered. It is proved that the length of the group algebra of a dihedral group of order 2^{k+1} over an arbitrary field of characteristic 2 is equal to 2^k.

Московский государственный университет
им. М. В. Ломоносова, 119991, Москва, Россия

Московский Центр фундаментальной и
прикладной математики, 119991, Москва, Россия

Московский физико-технический институт
(государственный университет), 141701,
Московская обл., г. Долгопрудный, Россия
E-mail: ov_markova@mail.ru

Московский государственный университет
им. М. В. Ломоносова, 119991, Москва, Россия
E-mail: good_michael@mail.ru

Поступило 15 октября 2020 г.