Записки научных
семинаров ПОМИ
Том 472, 2018 г.

А. Э. Гутерман, О. В. Маркова

ДЛИНА ГРУППОВЫХ АЛГЕБР ГРУПП НЕБОЛЬШОГО РАЗМЕРА

§1. Введение

Напомним основные определения, связанные с функцией длины. Термины и результаты теории колец, использованные в статье, можно найти, например, в [10]. 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 [8].

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 1.1. Длина *слова* $b_{i_1} \dots b_{i_t}$*, где* $b_{i_j} \in B$*, 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 $\mathcal{L}_0(\mathcal{S}) = \langle 1_{\mathcal{A}} \rangle = \mathbb{F}$ для алгебр с единицей. Пусть

Ключевые слова: функция длины алгебр, групповая алгебра, группа подстановок.

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

также $\mathcal{L}(\mathcal{S}) = \bigcup\limits_{i=0}^{\infty} \mathcal{L}_i(\mathcal{S})$ обозначает линейную оболочку всех слов в алфавите $\{a_1, \ldots, a_k\}$.

Определение 1.3. *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 $\mathcal{L}_h(\mathcal{S}) = \mathcal{L}_{h+1}(\mathcal{S})$, 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 1.4. 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 1.5. Длиной алгебры $\mathcal{A}$ *называется число*

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

Обозначение 1.6. Пусть $\mathbb{F}$ – произвольное поле и G – конечная группа. Через $\mathbb{F}G$ будем обозначать групповую алгебру группы G над полем $\mathbb{F}$. Через $M_n(R)$ будем обозначать алгебру матриц порядка n над произвольным кольцом R.

Исследуя вопросы, связанные с образующими групповых алгебр, естественно рассматривать в качестве порождающей системы групповой алгебры $\mathbb{F}G$ 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 $S \cup S^{-1}$.

Определение 1.7. Диаметром *группы G относительно системы образующих S называется максимум по $g \in G$ длин кратчайших слов от $S \cup S^{-1}$, представляющих g.*

Это понятие совпадает с диаметром графа Кэли группы G относительно системы образующих S (см. [1, §1]), а именно, графа, вершины которого занумерованы элементами группы, а две вершины соединены ребром тогда и только тогда, когда одна получается из другой домножением на элемент множества $S \cup S^{-1}$. 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. Вопрос получения верхних оценок и, тем более, точного вычисления длин конкретных групповых алгебр остаётся открытым и актуальным.

В представленной работе точно посчитаны длины групповых алгебр всех групп с не более чем семью элементами над произвольными полями. Отметим, что длине групповых алгебр абелевых групп над различными полями посвящены работы [4, 5]. Длины групповых алгебр групп $\mathbb{Q}_8$ и D_n, $n \geqslant 4$, над произвольными полями определены и также будут опубликованы отдельно. Тем самым, наименьшая группа, вычисление длины групповой алгебры которой остаётся открытым вопросом, имеет порядок 12; в частности, неизвестна длина групповой алгебры группы A_4.

Для длины алгебры всегда справедлива следующая тривиальная верхняя оценка.

Замечание 1.8 ([7, лемма 4.34, следствие 4.36])**.** Пусть $\mathcal{A}$ – алгебра размерности n над произвольным полем $\mathbb{F}$. 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.

Для групповых алгебр получаем

Следствие 1.9. *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 $l(\mathbb{F}G) \leqslant |G|-2$.*

В частности, для длины алгебры $\mathbb{F}S_3$ – групповой алгебры группы перестановок S_3 – отсюда сразу получаем верхнюю оценку $l(\mathbb{F}S_3) \leqslant 4$. Оказывается, что эту оценку можно улучшить, а именно ниже будет показано, что для произвольного поля $\mathbb{F}$ справедливо равенство $l(\mathbb{F}S_3) = 3$. Для длины групповой алгебры четверной группы Клейна $V_4 = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ тривиальная оценка даёт значение 3. Ниже мы покажем, что эта длина зависит от выбора основного поля. В общем случае, когда характеристика поля отлична от 2 и поле содержит более 3 элементов, тривиальная верхняя оценка достигается, однако в оставшихся случаях длина групповой алгебры группы V_4 равняется 2.

Хорошо известно, что любая группа порядка, не превосходящего 7, либо является циклической, либо изоморфна одной из групп V_4 или S_3. Длина групповых алгебр всех циклических групп над произвольными полями уже найдена (следствие 1.9).

Данная работа построена следующим образом: §2 посвящён вычислению длины групповой алгебры группы V_4, а в §3 аналогичная задача решается для группы S_3.

§2. Длина групповой алгебры группы V_4

В этом параграфе через $\mathbb{F}_q$ будем обозначать поле из q элементов, а $V_4 = \langle a, b | a^2 = b^2 = [a, b] = e\rangle$ обозначает единственную с точностью до изоморфизма нециклическую группу порядка 4, которая называется *четверной группой Клейна.*

Лемма 2.1.

(1) $V_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

(2) *Группа V_4 порождается любыми двумя различными неединичными элементами.*

(3) *Относительно системы образующих $\{x, y\}$, где $x, y \in V_4$ – произвольные неединичные элементы и $x \neq y$, группа V_4 имеет диаметр* 2.

Доказательство. (1). Изоморфизм $f : V_4 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ задаётся на образующих равенствами $f(a) = (1, 0)$, $f(b) = (0, 1)$.

Утвержденя (2) и (3) следуют из того, что любой из трёх неединичных элементов группы Клейна равен произведению двух других, но не выражается словом длины 1 от этих элементов. □

Следствие 2.2. *Пусть $\mathbb{F}$ – произвольное поле. Тогда $l(\mathbb{F}V_4) \geqslant 2$.*

Теорема 2.3.

1. *Пусть* $\mathbb{F}$ *– произвольное поле,* $\operatorname{char}\mathbb{F}\neq 2$*,* $\mathbb{F}\neq\mathbb{F}_3$*. Тогда* $l(\mathbb{F}V_4)=3$.
2. $l(\mathbb{F}_3V_4)=2$.
3. *Пусть* $\operatorname{char}\mathbb{F}=2$*. Тогда* $l(\mathbb{F}V_4)=2$.

Доказательство. Из следствия 1.9 вытекает, что во всех случаях $l(\mathbb{F}V_4)\leqslant 3$. Выясним теперь, когда это равенство достигается, а когда нет.

I. Пусть $\operatorname{char}\mathbb{F}\neq 2$. По теореме Машке [10, §3.6, теорема, стр. 72], алгебра $\mathbb{F}V_4$ полупроста. В силу конечномерности алгебра $\mathbb{F}V_4$ также является артиновой. Тогда, применяя теорему Веддербарна–Артина [10, §3.5, теорема, стр. 69], получаем, что

$$\mathbb{F}V_4\cong\bigoplus_{i=1}^{r}M_{n_i}(D_i),$$

где D_i – конечномерные тела над $\mathbb{F}$. Поскольку алгебра $\mathbb{F}V_4$ коммутативна, то $n_i=1$ и D_i – поля, являющиеся конечными расширениями поля $\mathbb{F}$, $i=1,\ldots,r$. Далее найдём это разложение явно. Заметим, что, по теореме о гомоморфизме для алгебр ([2, теорема 9.2.1 и замечание на стр. 359]), любая конечномерная однопорождённая $\mathbb{F}$-алгебра $\mathcal{L}(\{a\})$ изоморфна фактор-алгебре $\mathbb{F}[x]/(\mu_a(x))$, где $\mu_a(x)$ – минимальный многочлен элемента a. Поэтому групповая алгебра циклической группы $G=\langle g\rangle_n$ изоморфна алгебре $\mathbb{F}G\cong\mathbb{F}[x]/(x^n-1)$. Дальнейшее разложение алгебры $\mathbb{F}[x]/(x^n-1)$ на прямые слагаемые получается из разложения многочлена x^n-1 на неприводимые множители ([2, теорема 9.2.5]). Применяем это утверждение к группе порядка 2. Если $\operatorname{char}\mathbb{F}\neq 2$, то $-1\neq 1$, поэтому $(x-1)$ и $(x+1)$ – взаимно простые неприводимые многочлены. Тогда

$$\mathbb{F}\mathbb{Z}_2\cong\mathbb{F}[x]/(x^2-1)\cong\mathbb{F}[x]/(x-1)\oplus\mathbb{F}[x]/(x+1)\cong\mathbb{F}\oplus\mathbb{F}$$

([2, пример 9.2.14]).

Используя [9, лемма 1.3.4], получаем $\mathbb{F}[\mathbb{Z}_2\oplus\mathbb{Z}_2]\cong\mathbb{F}\mathbb{Z}_2\otimes\mathbb{F}\mathbb{Z}_2$. Далее, используя доказанное выше и [10, следствие a, §9.1], выводим

$$\mathbb{F}\mathbb{Z}_2\otimes\mathbb{F}\mathbb{Z}_2\cong(\mathbb{F}\oplus\mathbb{F})\otimes\mathbb{F}\mathbb{Z}_2\cong(\mathbb{F}\otimes\mathbb{F}\mathbb{Z}_2)\oplus(\mathbb{F}\otimes\mathbb{F}\mathbb{Z}_2)\cong\mathbb{F}\mathbb{Z}_2\oplus\mathbb{F}\mathbb{Z}_2.$$

Следовательно, $\mathbb{F}V_4\cong\mathbb{F}\oplus\mathbb{F}\oplus\mathbb{F}\oplus\mathbb{F}$. Заметим, что в общем случае длина прямой суммы нескольких копий основного поля как длина алгебры диагональных матриц уже вычислена (см. [6, теорема 5.4]), но для удобства читателя мы непосредственно докажем утверждение для четырех копий поля.

1. Если $|\mathbb{F}| \geqslant 4$, то алгебру $\mathcal{D} = \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F}$ можно породить одним элементом $d = (\delta_1, \delta_2, \delta_3, \delta_4)$, где $\delta_1, \delta_2, \delta_3, \delta_4$ – различные элементы поля $\mathbb{F}$, поскольку элементы алгебры $1_{\mathcal{D}}, d, d^2, d^3$ линейно независимы. Действительно, равенство $x_1 1_{\mathcal{D}} + x_2 d + x_3 d^2 + x_4 d^3 = 0$ для проверки линейной зависимости в алгебре равносильно системе покоординатных равенств $x_1 + x_2\delta_i + x_3\delta_i^2 + x_4\delta_i^3 = 0,\ i = 1, 2, 3, 4$, определитель матрицы которой есть определитель Вандермонда $V(\delta_1, \delta_2, \delta_3, \delta_4) \neq 0$. Значит, система имеет единственное решение $x_1 = x_2 = x_3 = x_4 = 0$. Следовательно, $l(\{d\}) = 3 = l(\mathcal{D}) = l(\mathbb{F}V_4)$.

2. Если $\mathbb{F} = \mathbb{F}_3$, то для любого элемента $d = (\delta_1, \delta_2, \delta_3, \delta_4)$ алгебры $\mathcal{D}$ выполняется неравенство $\dim \mathcal{L}(\{d\}) \leqslant 3 < 4 = \dim \mathcal{D}$, поскольку d аннулируется кубическим многочленом $x(x-1)(x-2)$. Тогда алгебра $\mathcal{D}$ не является однопорождённой, значит $l(\mathcal{D}) \leqslant \dim \mathcal{D} - 2 = 2$ в силу замечания 1.8. С другой стороны, по следствию 2.2 имеем $l(\mathbb{F}_3 V_4) \geqslant 2$, откуда $l(\mathcal{D}) = 2 = l(\mathbb{F}_3 V_4)$. Систему порождающих длины 2 для алгебры $\mathcal{D}$ можно также предъявить явно. Например, рассмотрим $d_1 = (1, 2, 0, 0)$, $d_2 = (0, 0, 1, 2)$ и $\mathcal{D} = \langle 1_{\mathcal{D}}, d_1, d_2, d_1^2 \rangle = \mathcal{L}_2(\{d_1, d_2\})$.

II. $\operatorname{char} \mathbb{F} = 2$. Нижняя оценка $l(\mathbb{F}V_4) \geqslant 2$ получена в следствии 2.2. В силу ограничения на характеристику поля, для произвольного элемента $d = \alpha a + \beta b + \gamma ab + \delta e \in \mathbb{F}V_4$ имеем $d^2 = (\alpha^2 + \beta^2 + \gamma^2 + \delta^2)e$, поэтому $\dim \mathcal{L}(\{d\}) \leqslant 2 < \dim \mathbb{F}V_4$, т.е. это не однопорождённая алгебра. Следовательно, выполняется оценка $l(\mathbb{F}V_4) \leqslant \dim \mathbb{F}V_4 - 2 = 2$. □

§3. Длина групповой алгебры группы S_3

Теорема 3.1. *Пусть $\mathbb{F}$ – произвольное поле. Тогда $l(\mathbb{F}S_3) = 3$.*

Сначала докажем нижнюю оценку $l(\mathbb{F}S_3) \geqslant 3$. Для доказательства этого факта нам достаточно предъявить систему порождающих для алгебры $\mathbb{F}S_3$ длины 3. Отметим, что как раз в этом случае максимум может быть достигнут на системе образующих группы.

Лемма 3.2. *Пусть $\mathbb{F}$ – произвольное поле. Тогда $l(\mathbb{F}S_3) \geqslant 3$.*

Доказательство. Рассмотрим $\tau = (12), \rho = (23) \in S_3$. Хорошо известно, что $S_3 = \langle \tau, \rho \rangle$ (см., например, [3, §2]).

Заметим, что все слова длины 2 от τ и ρ – чётные подстановки, поэтому транспозицию $(13) = \tau\rho\tau$ нельзя представить словом длины, меньшей 3.

Следовательно, $l(\mathbb{F}S_3) \geqslant l(\{\rho, \tau\}) \geqslant 3$. □

Для доказательства верхней оценки длины групповой алгебры $\mathbb{F}S_3$ нам понадобятся следующие результаты о длине, доказательства которых можно найти, например, в работе [7].

Предложение 3.3 ([7, предложение 3.1]). *Пусть $\mathbb{F}$ – произвольное поле и $\mathcal{A}$ – конечномерная алгебра над $\mathbb{F}$. Если $\mathcal{S} = \{a_1, \dots, a_k\}$ – система порождающих этой алгебры и $C = \{c_{i,j}\} \in M_k(\mathbb{F})$ – невырожденная матрица, то множество*

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

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

Предложение 3.4 ([7, предложение 3.2]). *Пусть $\mathbb{F}$ – произвольное поле и $\mathcal{A}$ – конечномерная алгебра с единицей над $\mathbb{F}$. Пусть $\mathcal{S} = \{a_1, \dots, a_k\}$ – система порождающих этой алгебры такая, что $1_{\mathcal{A}} \notin \langle a_1, \dots, a_k\rangle$. Тогда для любых $\gamma_1, \dots, \gamma_k \in \mathbb{F}$ множество*

$$\mathcal{S}_1 = \{a_1 + \gamma_1 1_{\mathcal{A}}, \dots, a_k + \gamma_k 1_{\mathcal{A}}\}$$

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

Предложение 3.5 ([7, предложение 3.4]). *Пусть $\mathbb{F}$ – произвольное поле, пусть $\mathcal{A}$ – конечномерная $\mathbb{F}$-алгебра с единицей $1_{\mathcal{A}}$ и пусть $\mathcal{S} = \{a_1, \dots, a_k\}$ – система порождающих для алгебры $\mathcal{A}$. Тогда существует система порождающих $\mathcal{S}'$ для $\mathcal{A}$, удовлетворяющая следующим условиям:*

(1) $\mathcal{S}' \subseteq \mathcal{S}$;
(2) $1_{\mathcal{A}} \notin \langle \mathcal{S}' \rangle$;
(3) $\dim \mathcal{L}_1(\mathcal{S}') = |\mathcal{S}'| + 1$;
(4) $l(\mathcal{S}') = l(\mathcal{S})$.

Лемма 3.6 ([7, лемма 3.17]). *Пусть $\mathbb{F}$ – произвольное поле. Тогда $l(M_2(\mathbb{F}) \oplus \mathbb{F}) = 2$.*

Лемма 3.7 ([7, лемма 3.18]). *Пусть $\mathbb{F}$ – произвольное поле. Тогда $l(M_2(\mathbb{F}) \oplus \mathbb{F} \oplus \mathbb{F}) = 3$.*

Предложение 3.8 ([7, предложение 3.19]). *Пусть даны поле $\mathbb{F}$ и его расширение $\mathbb{K}$. Рассмотрим конечномерное векторное пространство $\mathcal{A}_{\mathbb{F}}$ над $\mathbb{F}$. Определим пространство $\mathcal{A}_{\mathbb{K}}$ над $\mathbb{K}$ как тензорное произведение $\mathcal{A}_{\mathbb{F}} \otimes_{\mathbb{F}} \mathbb{K}$. Пусть $\mathcal{A}$ –конечномерная алгебра с единицей над полем*

$\mathbb{F}$. *Тогда для любого расширения* $\mathbb{K}$ *поля* $\mathbb{F}$ *выполняется неравенство* $l(\mathcal{A}_{\mathbb{F}}) \leqslant l(\mathcal{A}_{\mathbb{K}})$.

Лемма 3.9. *Пусть* $\mathbb{F}$ *– поле характеристики* 0*, либо характеристики* $p > 3$*. Тогда* $l(\mathbb{F}S_3) \leqslant 3$.

Доказательство. В силу предложения 3.8, достаточно рассмотреть случай, когда поле $\mathbb{F}$ алгебраически замкнуто.

Из условия теоремы получаем, что $\operatorname{char}\mathbb{F} \nmid |S_3|$, следовательно, по теореме Машке [10, §3.6, теорема, стр. 72], алгебра $\mathbb{F}S_3$ полупроста. В силу конечномерности, алгебра $\mathbb{F}S_3$ также является артиновой. Тогда, применяя теорему Веддербарна–Артина [10, §3.5, теорема, стр. 69], получаем, что

$$\mathbb{F}S_3 \cong \bigoplus_{i=1}^{r} M_{n_i}(D_i),$$

где D_i– конечномерные тела над $\mathbb{F}$. В силу алгебраической замкнутости поля $\mathbb{F}$, все D_i совпадают с $\mathbb{F}$. Таким образом,

$$\mathbb{F}S_3 \cong \bigoplus_{i=1}^{r} M_{n_i}(\mathbb{F}).$$

Из равенства размерностей получаем, что $\sum\limits_{i=1}^{r} n_i^2 = 6$. Следовательно, $n_i \leqslant 2$ для всех $i = 1, \ldots, r$. Поскольку алгебра $\mathbb{F}S_3$ не является коммутативной, $n_i = 2$ присутствует в разложении.

Таким образом, $\mathbb{F}S_3 \cong M_2(\mathbb{F}) \oplus \mathbb{F} \oplus \mathbb{F}$. Тогда из леммы 3.7 получаем, что

$$l(\mathbb{F}S_3) = l(M_2(\mathbb{F}) \oplus \mathbb{F} \oplus \mathbb{F}) = 3.$$

□

Предложение 3.10. *Пусть* $\mathbb{F}$ *– поле характеристики* 2*. Тогда*

(1) *радикал Джекобсона* $J(\mathbb{F}S_3)$ *алгебры* $\mathbb{F}S_3$ *состоит из элементов вида* $\alpha \sum\limits_{\sigma \in S_3} \sigma$, $\alpha \in \mathbb{F}$*, и, следовательно,* $\dim J(\mathbb{F}S_3) = 1$*;*

(2) $\mathbb{F}S_3 / J(\mathbb{F}S_3) \cong M_2(\mathbb{F}) \oplus \mathbb{F}$.

Доказательство. См. доказательство [11, теорема 2.1]. □

Лемма 3.11. *Пусть* $\mathbb{F}$ *– поле характеристики* 2*. Тогда* $l(\mathbb{F}S_3) \leqslant 3$.

Доказательство. В силу предложения 3.8, достаточно рассмотреть случай, когда поле $\mathbb{F}$ алгебраически замкнуто.

Для краткости обозначим $\mathcal{A} = \mathbb{F}S_3$.

Возьмём произвольную систему порождающих $\mathcal{S} = \{A_1, \dots, A_m\}$ алгебры $\mathcal{A}$ и покажем, что $l(\mathcal{S}) \leqslant 3$.

Положим $\mathcal{B} = \mathcal{A}/J(\mathcal{A})$ и рассмотрим канонический гомоморфизм алгебр $\pi : \mathcal{A} \to \mathcal{B}$.

Множество $\mathcal{S}_B = \{B_1 = \pi(A_1), \dots, B_m = \pi(A_m)\}$ является системой порождающих для алгебры $\mathcal{B}$. Поскольку $l(\mathcal{B}) = 2$ (согласно предложению 3.10 и лемме 3.6), то $\dim \mathcal{L}_2(\mathcal{S}_B) = \dim \mathcal{B} = 5$. С другой стороны, $\mathcal{L}_2(\mathcal{S}_B) = \mathcal{L}_2(\pi(\mathcal{S})) = \pi(\mathcal{L}_2(\mathcal{S}))$. Следовательно, $\dim \mathcal{L}_2(\mathcal{S}) \geqslant \dim \pi(\mathcal{L}_2(\mathcal{S})) = 5$. Получаем два возможных значения для $\dim \mathcal{L}_2(\mathcal{S})$:

1) если $\dim \mathcal{L}_2(\mathcal{S}) = 6 = \dim \mathcal{A}$, то $l(\mathcal{S}) \leqslant 2 < 3$;

2) если $\dim \mathcal{L}_2(\mathcal{S}) = 5$, то $\dim \mathcal{L}_3(\mathcal{S}) \geqslant \dim \mathcal{L}_2(\mathcal{S}) + 1 = 6 = \dim \mathcal{A}$ и $l(\mathcal{S}) = 3$.

Тем самым доказано, что $l(\mathbb{F}S_3) \leqslant 3$. □

Предложение 3.12. *Пусть* $\mathbb{F}$ *– поле характеристики* 3. *Тогда*

(1) *радикал Джекобсона* $J(\mathbb{F}S_3)$ *алгебры* $\mathbb{F}S_3$ *имеет размерность* $\dim J(\mathbb{F}S_3) = 4$ *и индекс нильпотентности* $N(J(\mathbb{F}S_3)) = 3$;

(2) $\mathbb{F}S_3/J(\mathbb{F}S_3) \cong \mathbb{F} \oplus \mathbb{F}$.

Доказательство. См. [9, глава 8, §1, лемма 1.17] и доказательство [11, теорема 2.2]. □

Лемма 3.13. *Пусть* $\mathbb{F}$ *– поле характеристики* 3. *Тогда* $l(\mathbb{F}S_3) \leqslant 3$.

Доказательство. В силу предложения 3.8, достаточно рассмотреть случай, когда поле $\mathbb{F}$ алгебраически замкнуто.

Для краткости обозначим $\mathcal{A} = \mathbb{F}S_3$.

Предположим, что существует система порождающих $\mathcal{S} = \{A_1, \dots, A_m\} \subseteq \mathcal{A}$ такая, что $l(\mathcal{S}) \geqslant 4$, и приведем это утверждение к противоречию.

Действительно, пусть $l(\mathcal{S}) \geqslant 4$. Тогда $\dim \mathcal{L}_h(\mathcal{S}) < 6 = \dim \mathcal{A}$ для $h = 1, 2, 3$, откуда $\dim \mathcal{L}_{i+1}(\mathcal{S}) \geqslant \dim \mathcal{L}_i(\mathcal{S}) + 1$ для $h = 1, 2, 3$. Значит,

$$6 \geqslant \dim \mathcal{L}_4(\mathcal{S}) \geqslant \dim \mathcal{L}_1(\mathcal{S}) + 3 \geqslant 3 + 3 = 6,$$

т.е.

$$\dim \mathcal{L}_1(\mathcal{S}) = 3, \ \dim \mathcal{L}_2(\mathcal{S}) = 4, \ \dim \mathcal{L}_3(\mathcal{S}) = 5, \ \dim \mathcal{L}_4(\mathcal{S}) = 6.$$

В силу первого из этих равенств, можно считать, что $m = 2$ согласно предложению 3.5.

Положим $\mathcal{B} = \mathcal{A}/J(\mathcal{A})$ и рассмотрим канонический гомоморфизм алгебр $\pi : \mathcal{A} \to \mathcal{B}$. Множество $\mathcal{S}_B = \{B_1 = \pi(A_1), B_2 = \pi(A_2)\} \subseteq \mathcal{B}$ является системой порождающих для алгебры $\mathcal{B}$. Поскольку $\dim \mathcal{B} = 2$ (согласно предложению 3.12), то длина алгебры $\mathcal{B}$ равна 1. Следовательно, $\dim \mathcal{L}_1(\mathcal{S}_B) = \dim \mathcal{B} = 2$. Не ограничивая общности, можно считать, что элементы $1_{\mathcal{B}} = 1_{\mathcal{A}} + J(\mathcal{A})$ и B_1 образуют базис алгебры $\mathcal{B}$, $B_2 = \beta B_1 + \gamma 1_{\mathcal{B}}$ и $B_1^2 = B_1$. Тогда, согласно предложениям 3.3 и 3.4, множество $\mathcal{S}_2 = \{A_1, A_2 - \beta A_1 - \gamma 1_{\mathcal{A}}\}$ является системой порождающих алгебры $\mathcal{A}$ длины $l(\mathcal{S}_2) = l(\mathcal{S}) = 4$. Без ограничения общности можем считать, что $A_1^2 - A_1, A_2 \in J(\mathcal{A})$.

Мы знаем, что $\dim \mathcal{L}_{\mu+1}(\mathcal{S}) = \dim \mathcal{L}_\mu(\mathcal{S}) + 1$, $\mu = 1, 2, 3$. Поэтому существует несократимое слово $v_4 = A_i A_j A_k A_r \in \mathcal{S}^4$, где $i, j, k, r \in \{1, 2\}$. Тогда множество $\{1_{\mathcal{A}},\ A_1,\ A_2,\ v_2 = A_i A_j,\ v_3 = A_i A_j A_k,\ v_4\}$ является базисом алгебры $\mathcal{A}$, причём $\mathcal{L}_\mu(\mathcal{S}) = \mathcal{L}_{\mu-1}(\mathcal{S}) \oplus \langle v_\mu \rangle$, $\mu = 2, 3, 4$.

Отдельно рассмотрим следующие случаи.

(1) Пусть $A_2 A_s \notin \mathcal{L}_1(\mathcal{S})$ для некоторого $s \in \{1, 2\}$. Тогда $v_2 = \alpha_0 A_2 A_s + w_0$, $A_s A_k = \alpha_1 A_2 A_s + w_1$, $A_s A_r = \alpha_2 A_2 A_s + w_2$, $\alpha_0, \alpha_1, \alpha_2 \in \mathbb{F}$, $w_0, w_1, w_2 \in \mathcal{L}_1(\mathcal{S})$. В этом случае,

$$\begin{aligned} v_4 = (\alpha_0 A_2 A_s + w_0) A_k A_r &= \alpha_0 A_2 (\alpha_1 A_2 A_s + w_1) A_r + w_3 \\ &= \alpha_0 \alpha_1 A_2^2 A_s A_r + w_4 = \alpha_0 \alpha_1 A_2^2 (\alpha_2 A_2 A_s + w_2) + w_4 \\ &= \alpha_0 \alpha_1 \alpha_2 A_2^3 A_s + w_5, \end{aligned}$$

где $w_3, w_4, w_5 \in \mathcal{L}_3(\mathcal{S})$. С другой стороны, $A_2^3 = 0$, так как $A_2 \in J(\mathcal{A})$ и $N(J(\mathcal{A})) = 3$ (согласно предложению 3.10). Таким образом, $v_4 = w_5 \in \mathcal{L}_3(\mathcal{S})$ – противоречие с несократимостью слова v_4.

(2) Случай $A_s A_2 \notin \mathcal{L}_1(\mathcal{S})$ рассматривается аналогично с использованием представлений $A_k A_r$, $A_j A_s$ и $A_i A_s$ через $A_s A_2$ и элементов из $\mathcal{L}_1(\mathcal{S})$. Тогда v_4 выражается через $A_s A_2^3$ и элемент из $\mathcal{L}_3(\mathcal{S})$, что противоречит несократимости слова v_4, поскольку $A_2^3 = 0$.

(3) Остаётся случай, когда $A_1 A_2,\ A_2 A_1,\ A_2^2 \in \mathcal{L}_1(\mathcal{S})$. Эти слова сократимы, поэтому не могут быть подсловами несократимых

слов v_2, v_3, v_4, значит, $v_2 = A_1^2$, $v_3 = A_1^3$, $v_4 = A_1^4$. Покажем, что эта ситуация не реализуется для базиса алгебры $\mathcal{A}$.

Рассмотрим произвольный элемент $x \in J(\mathcal{A}) \cap \mathcal{L}_1(\mathcal{S})$. Тогда $x = \alpha' 1_{\mathcal{A}} + \beta' A_1 + \gamma' A_2$, $\alpha', \beta', \gamma' \in \mathbb{F}$, но $A_2 \in J(\mathcal{A})$, а $\pi(1_{\mathcal{A}})$ и $\pi(A_1)$ образуют базис алгебры $\mathcal{B} = \mathcal{A}/J(\mathcal{A})$. Следовательно, $\alpha' = \beta' = 0$, откуда $J(\mathcal{A}) \cap \mathcal{L}_1(\mathcal{S}) = \langle A_2 \rangle$.

Имеем $A_1A_2,\ A_2A_1, A_2^2 \in J(\mathcal{A}) \cap \mathcal{L}_1(\mathcal{S})$, поэтому $A_2^2 = \gamma A_2$, $A_1A_2 = \alpha A_2,\ A_2A_1 = \beta A_2$, где $\alpha, \beta, \gamma \in \mathbb{F}$. Заметим, что $\gamma = 0$, так как $A_2^3 = 0$, и $\alpha \neq \beta$, так как порождающие A_1 и A_2 не могут коммутировать, поскольку алгебра $\mathcal{A}$ некоммутативна.

Пусть $\alpha \notin \{0, 1\}$. Тогда элемент $B_1 - \alpha 1_{\mathcal{B}}$ обратим в алгебре $\mathcal{B}$, поскольку оператор умножения на B_1 в алгебре $\mathcal{B}$ является идемпотентным и поэтому не имеет собственных чисел, кроме 0 и 1. Значит, существуют элементы $x \in \mathcal{A}$ и $y \in J(\mathcal{A})$ такие, что $(A_1 - \alpha 1_{\mathcal{A}})x = 1_{\mathcal{A}} + y$, но элемент $1_{\mathcal{A}} + y$, обратим в алгебре $\mathcal{A}$, откуда получаем, что $A_1 - \alpha 1_{\mathcal{A}}$ обратим. Тогда из равенства $A_1A_2 = \alpha A_2$ следует, что $A_2 = 0$. Полученное противоречие показывает, что $\alpha \in \{0, 1\}$. Аналогично, получаем, что $\beta \in \{0, 1\}$. Таким образом, $\{\alpha, \beta\} = \{0, 1\}$. Не ограничивая общности, можем считать, что $\alpha = 0$, $\beta = 1$. Рассмотрим элементы $1_{\mathcal{A}},\ A_1^i - A_1, i = 2, 3, 4$. Поскольку слова $1_{\mathcal{A}}, A_1, A_2, v_2 = A_1^2, v_3 = A_1^3, v_4 = A_1^4$ образуют базис $\mathcal{L}_4(\mathcal{S})$, то элементы $1_{\mathcal{A}},\ A_1^i - A_1, i = 2, 3, 4$, линейно независимы. Также заметим, что

$$(A_1^i - A_1)A_2 = A_1^i A_2 - A_1A_2 = 0$$

и

$$A_2(A_1^i - A_1) = A_2A_1^i - A_2A_1 = A_2 - A_2 = 0,$$

т.е. элементы $A_1^i - A_1, i = 2, 3, 4$, принадлежат центру $Z(\mathcal{A})$ алгебры $\mathcal{A}$ и $\dim Z(\mathcal{A}) \geqslant 4$. С другой стороны, известно, что размерность центра групповой алгебры совпадает с числом различных классов сопряжённости в группе [9, глава 4, §1, лемма 1.1] и, в частности, $\dim Z(\mathbb{F}S_3) = 3$. Противоречие. $\square$

Доказательство теоремы 3.1 получается объединением лемм 3.2, 3.9, 3.11 и 3.13: из леммы 3.2 получается нижняя оценка, а леммы 3.9, 3.11 и 3.13 дают совпадающую с ней верхнюю оценку длины в случаях полей характеристики, отличной от 2 и 3, полей характеристики 2 и полей характеристики 3 соответственно. $\square$

Список литературы

1. L. Babai, Á. Seress, *On the diameter of permutation groups.* — Eur. J. Combin. **13**, No. 4 (1992), 231–243.
2. Э. Б. Винберг, *Курс алгебры.* 3-е изд. М., Факториал Пресс, 2002.
3. М. М. Глухов, А. Ю. Зубов, *О длинах симметрических и знакопеременных групп подстановок в различных системах образующих (обзор).* — Мат. вопр. кибернетики **8** (1999), 5–32.
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.* Preprint, 2018.
5. A. E. Guterman, O. V. Markova, M. A. Khrystik, *On the lengths of group algebras of finite Abelian groups in the modular case.* Preprint, 2018.
6. О. В. Маркова, *Верхняя оценка длины коммутативных алгебр.* — Мат. сборник **200**, No. 12 (2009), 41–62.
7. О. В. Маркова, *Функция длины и матричные алгебры.* — Фундам. прикл. матем. **17**, No. 6 (2012), 65–173.
8. C. J. Pappacena, *An upper bound for the length of a finite-dimensional algebra.* — J. Algebra **197** (1997), 535–545.
9. D. S. Passman, *The Algebraic Structure of Group Rings.* Wiley-Interscience, New York, 1977.
10. Р. Пирс, *Ассоциативные алгебры.* М., Мир, 1986.
11. R. K. Sharma, J. B. Srivastava, M. Khan, *The unit group of* $\mathbb{F}S_3$. — Acta Math. Acad. Paedagog. Nyházi **23**, No. 2 (2007), 129–142.

Guterman A. E., Markova O. V. The length of group algebras of small-order groups.

The paper evaluates the lengths of group algebras of all groups of orders at most 7 over an arbitrary field.

Московский государственный университет
им. М. В. Ломоносова, 119991 Москва;
Московский физико-технический институт
(Университет), 141701 Долгопрудный, Россия

E-mail: guterman@list.ru

E-mail: ov_markova@mail.ru

Поступило 30 октября 2018 г.