Math-Net.Ru

Общероссийский математический портал

О. В. Маркова, Верхняя оценка длины коммутативных алгебр, *Матем. сб.*, 2009, том 200, номер 12, 41–62

DOI: <https://doi.org/10.4213/sm7531>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.224.135.184

26 апреля 2023 г., 16:23:09

УДК 512.552

О. В. Маркова

Верхняя оценка длины коммутативных алгебр

Длиной конечной системы порождающих конечномерной ассоциативной алгебры над произвольным полем называется наименьшее натуральное число k такое, что слова длины не большей k порождают эту алгебру как векторное пространство. Длиной алгебры называется максимум длин ее систем порождающих. В настоящей работе получена верхняя оценка длины коммутативной алгебры в терминах функции двух ее инвариантов – размерности и максимальной степени минимального многочлена элементов алгебры. В качестве следствия этого результата получена формула для длины алгебры диагональных матриц над произвольным полем.

Библиография: 8 названий.

Ключевые слова: длина алгебры, теория матриц, коммутативные алгебры, алгебра диагональных матриц.

§ 1. Основные определения

Кольцо $\mathcal{A}$, являющееся также векторным пространством над полем $\mathbb{F}$, называется *алгеброй* над $\mathbb{F}$ или $\mathbb{F}$ -*алгеброй*, если для любого $\lambda \in \mathbb{F}$ и любых $a, b \in \mathcal{A}$ выполняется равенство $\lambda(ab) = (\lambda a)b = a(\lambda b)$. Алгебра называется *конечномерной*, если соответствующее векторное пространство имеет конечную размерность над $\mathbb{F}$. Алгебра называется *конечнопорожденной*, если все ее элементы могут быть представлены в виде конечных линейных комбинаций (с коэффициентами из $\mathbb{F}$) конечных произведений некоторого конечного множества ее элементов, называемого *системой порождающих*. Легко видеть, что любая конечномерная алгебра порождается своим базисом, т.е. является конечнопорожденной. Обозначим через $\mathcal{S} = \{a_1, \dots, a_k\}$ конечную систему порождающих алгебры $\mathcal{A}$.

ОПРЕДЕЛЕНИЕ 1.1. Обозначим через $\langle S \rangle$ линейную оболочку (множество всех конечных линейных комбинаций с коэффициентами из $\mathbb{F}$) множества S .

ОПРЕДЕЛЕНИЕ 1.2. Пусть $B = \{b_1, \dots, b_m\}$ – непустое конечное множество (алфавит). Конечные последовательности букв из B назовем *словами*. Обозначим через B^* множество всех слов в алфавите B , а через F_B – свободную полугруппу над алфавитом B .

ОПРЕДЕЛЕНИЕ 1.3. Длина слова $b_{i_1} \dots b_{i_t}$, где $b_{i_j} \in B$, $b_{i_j} \neq 1$, равна t . Будем считать единицу словом от элементов B длины нуль.

ОПРЕДЕЛЕНИЕ 1.4. Обозначим через B^i множество всех слов в алфавите B длины не большей $i \geq 0$, а через $B^{=i}$ – множество всех слов в алфавите B длины $i \geq 1$.

ЗАМЕЧАНИЕ 1.5. Произведения элементов из порождающего множества $\mathcal{S}$ можно рассматривать как образы элементов свободной полугруппы $F_{\mathcal{S}}$ при естественном гомоморфизме и их также можно называть словами от образующих.

Пусть алгебра $\mathcal{A}$ также содержит единицу $1_{\mathcal{A}}$.

ОПРЕДЕЛЕНИЕ 1.6. Обозначим через $\mathcal{L}_i(\mathcal{S})$ линейную оболочку слов из $\mathcal{S}^i$. Заметим, что $\mathcal{L}_0(\mathcal{S}) = \langle 1_{\mathcal{A}} \rangle = \mathbb{F}$. Пусть $\mathcal{L}(\mathcal{S}) = \bigcup_{i=0}^{\infty} \mathcal{L}_i(\mathcal{S})$ – это линейная оболочка всех слов в алфавите $\{a_1, \dots, a_k\}$.

ЗАМЕЧАНИЕ 1.7. Так как $\mathcal{S}$ является системой порождающих для $\mathcal{A}$, то любой элемент $\mathcal{A}$ можно представить в виде конечной линейной комбинации слов от $\{a_1, \dots, a_k\}$, т.е. $\mathcal{A} = \mathcal{L}(\mathcal{S})$. Из определения $\mathcal{S}^i$ и наличия в алгебре $\mathcal{A}$ единицы следует, что

$$\mathcal{S}^{i+j} = \mathcal{S}^i \mathcal{S}^j, \quad (1)$$

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

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

Тогда в силу конечномерности $\mathcal{A}$ получаем, что найдется такой номер h , что $\mathcal{L}_h(\mathcal{A}) = \mathcal{L}_{h+1}(\mathcal{A})$.

ОПРЕДЕЛЕНИЕ 1.8. Наименьшее целое число $k \geq 0$, для которого $\mathcal{L}_k(\mathcal{S}) = \mathcal{L}_{k+1}(\mathcal{S})$, называется *длиной системы порождающих* $\mathcal{S}$. Обозначим длину системы порождающих $\mathcal{S}$ через $l(\mathcal{S})$.

ЗАМЕЧАНИЕ 1.9. Если для некоторого $h \geq 0$ выполнено условие $\mathcal{L}_h(\mathcal{S}) = \mathcal{L}_{h+1}(\mathcal{S})$, то

$$\begin{aligned} \mathcal{L}_{h+2}(\mathcal{S}) &= \langle \mathcal{L}_1(\mathcal{S}) \mathcal{L}_{h+1}(\mathcal{S}) \rangle = \langle \mathcal{L}_1(\mathcal{S}) \mathcal{L}_h(\mathcal{S}) \rangle = \mathcal{L}_{h+1}(\mathcal{S}), \\ \mathcal{L}_i(\mathcal{S}) &= \mathcal{L}_h(\mathcal{S}), \quad i \geq h. \end{aligned}$$

Следовательно, $l(\mathcal{S})$ определена корректно. Поскольку $\mathcal{S}$ является системой порождающих для $\mathcal{A}$, то $\mathcal{L}_h(\mathcal{S}) = \mathcal{L}(\mathcal{S}) = \mathcal{A}$.

ОПРЕДЕЛЕНИЕ 1.10. Число $l(\mathcal{A}) = \max_{\mathcal{S}} l(\mathcal{S})$, где максимум берется по всем системам порождающих этой алгебры, называется *длиной алгебры* $\mathcal{A}$.

ОПРЕДЕЛЕНИЕ 1.11. Слово $v \in \mathcal{S}^j$ называется *сократимым над $\mathcal{S}$* , если найдется такой номер $i < j$, что $v \in \mathcal{L}_i(\mathcal{S})$, (т.е. v представляется в виде линейной комбинации слов меньшей длины).

ОПРЕДЕЛЕНИЕ 1.12. Слово $v \in \mathcal{S}^j$ называется *несократимым над $\mathcal{S}$* , если оно не является сократимым.

ОПРЕДЕЛЕНИЕ 1.13. Назовем слова $v = a_{i_1} a_{i_2} \dots a_{i_p}$, $w = a_{j_1} a_{j_2} \dots a_{j_q} \in \mathcal{S}^*$ *формально равными*, если $p = q$ и для каждого $1 \leq s \leq p$ выполнено $i_s = j_s$; в противном случае назовем слова *формально различными*.

ОПРЕДЕЛЕНИЕ 1.14. Пусть $j \in \{1, \dots, k\}$ и $v \in \mathcal{S}^*$. Обозначим через $\#_j(v)$ число вхождений буквы a_j в слово v .

ОПРЕДЕЛЕНИЕ 1.15. Пусть $I: \mathcal{S}^* \rightarrow \mathbb{Z}_+^k$ – отображение, сопоставляющее слову $v \in \mathcal{S}^*$ строку $(\#_1(v), \dots, \#_k(v))$.

ПРЕДЛОЖЕНИЕ 1.16. *Отображение I порождает отношение эквивалентности $\wp_I$ на множестве $\mathcal{S}^*$:*

$$(v, w) \in \wp_I \iff I(v) = I(w).$$

ДОКАЗАТЕЛЬСТВО. Проверим, что отношение $\wp_I$ является эквивалентностью. Действительно,

- 1) для любого $v \in \mathcal{S}^*$ верно равенство $I(v) = I(v)$, поэтому $(v, v) \in \wp_I$;
- 2) для любых $v, w \in \mathcal{S}^*$ равенство $I(v) = I(w)$ симметрично, поэтому $(v, w) \in \wp_I \iff (w, v) \in \wp_I$;
- 3) если $(u, v) \in \wp_I$ и $(v, w) \in \wp_I$, то $I(u) = I(v)$, $I(v) = I(w)$ и, следовательно, $I(u) = I(w)$ для $(u, w) \in \wp_I$.

Обозначим через $\wp_I(v) = \{w \in \mathcal{S}^* \mid (v, w) \in \wp_I\}$ класс эквивалентности слова $v \in \mathcal{S}^*$.

ОПРЕДЕЛЕНИЕ 1.17. Для каждого $v \in \mathcal{S}^*$ существует подстановка $\varphi_v \in S_k$, упорядочивающая координаты вектора $I(v)$, т.е.

$$x_1 = \#_{\varphi_v(1)}(v) \geq x_2 = \#_{\varphi_v(2)}(v) \geq \dots \geq x_k = \#_{\varphi_v(k)}(v).$$

Через $I_0: \mathcal{S}^* \rightarrow \mathbb{Z}_+^k$ обозначим отображение, сопоставляющее слову $v \in \mathcal{S}^*$ упорядоченную строку $(x_1, \dots, x_k)$.

ПРЕДЛОЖЕНИЕ 1.18. *Отображение I_0 порождает отношение эквивалентности $\wp_{I_0}$ на множестве $\mathcal{S}^*$:*

$$(v, w) \in \wp_{I_0} \iff I_0(v) = I_0(w).$$

ДОКАЗАТЕЛЬСТВО аналогично доказательству предложения 1.16. .

Обозначим через $\wp_{I_0}(v) = \{w \in \mathcal{S}^* \mid (v, w) \in \wp_{I_0}\}$ класс эквивалентности слова $v \in \mathcal{S}^*$.

ЗАМЕЧАНИЕ 1.19. Поскольку множество $\mathbb{Z}_+^k$ является линейно упорядоченным относительно лексикографического порядка, то его непустое подмножество $I_0(\mathcal{S}^*)$ также является линейно упорядоченным относительно лексикографического порядка. Далее будем использовать следующее обозначение:

$$v \stackrel{I_0}{\leq} w \iff I_0(v) \stackrel{\text{lex}}{\leq} I_0(w) \quad \forall v, w \in \mathcal{S}^*.$$

Отметим, что равенство $v \stackrel{I_0}{=} w$ равносильно условию $(v, w) \in \wp_{I_0}$ для любых $v, w \in \mathcal{S}^*$.

ОПРЕДЕЛЕНИЕ 1.20. Пусть $a \in \mathcal{A}$ и $\deg a$ обозначает степень минимального многочлена элемента a над полем $\mathbb{F}$.

Из конечномерности алгебры $\mathcal{A}$ следует, что для любого $a \in \mathcal{A}$ справедлива оценка $\deg a \leq \dim \mathcal{A}$.

Положим

$$m(\mathcal{S}) = \max\{\deg w, w \in \mathcal{S}^*\}, \quad m = m(\mathcal{A}) = \max_{\mathcal{S}} m(\mathcal{S}) = \max_{a \in \mathcal{A}} \{\deg a\}.$$

ОПРЕДЕЛЕНИЕ 1.21. Пусть $M_{m,n}(\mathbb{F})$ – линейное пространство матриц размера $m \times n$ над полем $\mathbb{F}$, $M_n(\mathbb{F})$ – алгебра матриц порядка n над полем $\mathbb{F}$, $T_n(\mathbb{F})$ – алгебра верхнетреугольных матриц порядка n над полем $\mathbb{F}$, $D_n(\mathbb{F})$ – алгебра диагональных матриц порядка n над полем $\mathbb{F}$, а $N_n(\mathbb{F})$ – подалгебра нильпотентных матриц в $T_n(\mathbb{F})$.

Обозначим через E единичную матрицу, а через $E_{i,j}$ – (i, j) -ю матричную единицу, т.е. матрицу с единицей на (i, j) -ом месте и нулями на остальных.

ОПРЕДЕЛЕНИЕ 1.22. Пусть $x \in \mathbb{R}$. Через $[x]$ обозначим целую часть числа x , т.е. наибольшее целое число, не превосходящее x , а через $\lceil x \rceil$ – наименьшее целое число z такое, что $z \geq x$. Через $\{x\}$ обозначим дробную часть числа x , т.е. $\{x\} = x - [x]$.

§ 2. Введение

Задача вычисления длины алгебры матриц как функции порядка матриц была поставлена в 1984 году в работе [1] и до сих пор не решена. Случай, когда порядок матриц равен трем, изучали Спенсер и Ривлин [2], [3] в связи с возможным применением в механике. Существует гипотеза, состоящая в том, что зависимость между длиной и порядком матриц линейная.

ГИПОТЕЗА 2.1 (Паз; см. [1]). Пусть $\mathbb{F}$ – произвольное поле. Тогда $l(M_n(\mathbb{F})) = 2n - 2$.

Известно, что эта гипотеза верна при $n = 2, 3, 4$. Однако существующие верхние оценки длины алгебры матриц, найденные в работах Пазы [1] и Паппачены [4], не являются линейными.

ТЕОРЕМА 2.2 (Паз; см. [1; теорема 1, замечание 1]). Пусть $\mathbb{F}$ – произвольное поле. Тогда $l(M_n(\mathbb{F})) \leq \lceil (n^2 + 2)/3 \rceil$.

Вопрос о связи длины алгебры $\mathcal{A}$ с ее инвариантами $d = \dim \mathcal{A}$ и $m = m(\mathcal{A})$ рассматривается в работе Паппачены [4], где получена следующая оценка.

ТЕОРЕМА 2.3 (см. [4; теорема 3.1]). Пусть $\mathbb{F}$ – произвольное поле и

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

Тогда для произвольной системы порождающих $\mathcal{S}$ алгебры $\mathcal{A}$ выполнены неравенства

$$l(\mathcal{S}) < f(d, m(\mathcal{S})), \quad l(\mathcal{A}) < f(d, m).$$

Отметим, что если $\mathcal{A} \subseteq M_n(\mathbb{F})$, то $d \leq n^2$ и $m \leq n$.

В работе Константайна и Дарнолла [5] оценивается длина систем матриц из $M_n(\mathbb{F})$, обладающих следующим свойством.

ОПРЕДЕЛЕНИЕ 2.4 (см. [5; определение 2.1]). Говорят, что подмножество $\mathcal{S} = \{X_1, \dots, X_t\}$ в алгебре $\mathcal{A}$ обладает *модифицированным свойством Пуанкаре–Биркгофа–Вита* (сокращенно *ПБВ-свойством*), если любое произведение $u = X_{i_1} X_{i_2} \cdots X_{i_m}$ может быть записано по модулю $\mathcal{L}_{m-1}(\mathcal{S})$ в виде

$$\sum_{j_1 + j_2 + \cdots + j_t = m} c_{(j_1, \dots, j_t)} X_t^{j_t} X_{t-1}^{j_{t-1}} \cdots X_1^{j_1},$$

где $c_{(j_1, \dots, j_t)} = 0$, когда $X_t^{j_t} X_{t-1}^{j_{t-1}} \cdots X_1^{j_1} < u$ относительно лексикографического порядка.

ТЕОРЕМА 2.5 (см. [5; теорема 2.7]). Пусть $\mathbb{F}$ – произвольное поле, $\mathcal{S} \subset M_n(\mathbb{F})$ – множество матриц, обладающее модифицированным ПБВ-свойством. Тогда $l(\mathcal{S}) \leq 2n - 2$.

Отметим, что при доказательстве указанных выше результатов из работ [1], [4] и [5] используется похожая комбинаторная техника подсчета линейно независимых подслов.

В §3 настоящей работы получена оценка, являющаяся более точной, чем оценка из теоремы 2.3 в случае, когда алгебра $\mathcal{A}$ коммутативна. Пусть

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

В работе показано, что для любой системы порождающих $\mathcal{S} \subseteq \mathcal{A}$ выполнено $l(\mathcal{S}) \leq g(d, m(\mathcal{S}))$ и $l(\mathcal{A}) \leq g(d, m(\mathcal{A}))$.

Как следствие, в §5 вычислена длина алгебры диагональных матриц $D_n(\mathbb{F})$ над произвольным полем $\mathbb{F}$.

§3. Верхняя оценка длины для коммутативных алгебр

В этом параграфе получена верхняя оценка длины коммутативной $\mathbb{F}$ -алгебры $\mathcal{A}$ в терминах функции двух ее инвариантов – размерности $d = \dim_{\mathbb{F}} \mathcal{A}$ и максимальной степени минимального многочлена элементов из $\mathcal{A}$. Пусть

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

Покажем, что для любой системы порождающих $\mathcal{S} \subseteq \mathcal{A}$ выполнено $l(\mathcal{S}) \leq g(d, m(\mathcal{S}))$ и $l(\mathcal{A}) \leq g(d, m(\mathcal{A}))$.

Сначала укажем некоторые свойства функции $g(d, m)$.

ЛЕММА 3.1. Пусть $d, m \in \mathbb{N}$, $d \geq m \geq 2$. Тогда для любых $k, r_0, r, s \in \mathbb{N}$, $1 \leq k \leq m-1$, $0 \leq r_0 < m^r$, выполнены равенства

$$g(m^{r+s}, m) = g(m^r, m) + g(m^s, m), \quad (4)$$

$$g(km^r, m) = g(k, m) + g(m^r, m), \quad (5)$$

$$g(km^r + r_0, m) = g(km^r, m). \quad (6)$$

ДОКАЗАТЕЛЬСТВО. 1) Сначала проверим равенство (4). Имеем

$$\begin{aligned}
 g(m^{r+s}, m) &= (m-1)[\log_m m^{r+s}] + [m^{\{\log_m m^{r+s}\}}] - 1 = (m-1)(r+s) + 1 - 1 \\
 &= ((m-1)r + 1 - 1) + ((m-1)s + 1 - 1) \\
 &= ((m-1)[\log_m m^r] + [m^{\{\log_m m^r\}}] - 1) \\
 &\quad + ((m-1)[\log_m m^s] + [m^{\{\log_m m^s\}}] - 1) \\
 &= g(m^r, m) + g(m^s, m).
 \end{aligned}$$

2) Теперь проверим равенство (5). Так как $\log_m k \in [0, 1)$, $\log_m m^r \in \mathbb{N}$, то

$$\begin{aligned}
 [\log_m km^r] &= [\log_m k + \log_m m^r] = \log_m m^r = r, \\
 [m^{\{\log_m km^r\}}] &= [m^{\{\log_m k\}}] = [m^{\log_m k}] = k.
 \end{aligned}$$

Получаем

$$\begin{aligned}
 g(km^r, m) &= (m-1)[\log_m km^r] + [m^{\{\log_m km^r\}}] - 1 = (m-1)r + k - 1 \\
 &= (k-1+1-1) + ((m-1)r + 1 - 1) \\
 &= ((k-1)\log_k k + [k^{\{\log_k k\}}] - 1) + ((m-1)[\log_m m^r] + [m^{\{\log_m m^r\}}] - 1) \\
 &= g(k, k) + g(m^r, m).
 \end{aligned}$$

3) Поскольку $km^r \leq km^r + r_0 < m^{r+1}$, то

$$\begin{aligned}
 [\log_m (km^r + r_0)] &= [\log_m km^r] = r, \\
 [m^{\{\log_m (km^r + r_0)\}}] &= \left\lfloor \frac{km^r + r_0}{m^r} \right\rfloor = k = \left\lfloor \frac{km^r}{m^r} \right\rfloor = [m^{\{\log_m km^r\}}].
 \end{aligned}$$

Следовательно, $g(km^r + r_0, m) = g(km^r, m)$.

ТЕОРЕМА 3.2. При фиксированном значении $m \geq 2$ функция $g(d, m)$ является неубывающей по d .

ДОКАЗАТЕЛЬСТВО. Пусть $m \geq 2$ – некоторое натуральное число и $d_1, d_2 \in \mathbb{N}$, $m \leq d_1 < d_2$. Проверим, что $g(d_1, m) \leq g(d_2, m)$. Числа d_1 и d_2 единственным образом представляются в виде $d_i = q_i m^{l_i} + r_i$, где $l_i \geq 1$, $1 \leq q_i \leq m-1$, $0 \leq r_i < m^{l_i}$, $i = 1, 2$. При этом $[\log_m d_i] = l_i$, $[m^{\{\log_m d_i\}}] = q_i$. Следовательно, $g(d_i, m) = (m-1)l_i + q_i - 1$, $i = 1, 2$. Из соотношения между числами d_1 и d_2 получаем, что

$$m^{l_1} \leq d_1 < d_2 \leq m^{l_2+1} - 1.$$

Тогда $m^{l_1} < m^{l_2+1}$. Используя монотонность показательной функции, получаем соотношение $l_1 < l_2 + 1$ или, что равносильно для целых чисел, неравенство $l_1 \leq l_2$. Рассмотрим отдельно два случая: $l_1 < l_2$ и $l_1 = l_2$.

1) Пусть $l_1 < l_2$. Имеем

$$g(d_2, m) - g(d_1, m) = (m-1)(l_2 - l_1) + (q_2 - q_1).$$

При этом по условию $l_2 - l_1 > 0$. Следовательно, $l_2 - l_1 \geq 1$ и $q_2 - q_1 \geq 1 - (m - 1) = 2 - m$. Итак,

$$g(d_2, m) - g(d_1, m) \geq m - 1 + 2 - m = 1 > 0, \quad g(d_2, m) > g(d_1, m).$$

2) Пусть $l_1 = l_2$. Снова воспользуемся соотношением между числами d_1 и d_2 . Имеем

$$d_2 - d_1 = m^{l_1}(q_2 - q_1) + r_2 - r_1 > 0.$$

По условию $r_2 - r_1 \leq m^{l_1} - 1$. Следовательно,

$$m^{l_1}(q_2 - q_1) + m^{l_1} - 1 \geq d_2 - d_1 > 0$$

или

$$m^{l_1}(q_2 - q_1 + 1) > 1.$$

Поскольку $m^{l_1} > 0$, то также и $q_2 - q_1 + 1 > 0$. Заметим, что $q_2 - q_1 + 1 \in \mathbb{Z}$, поэтому $q_2 - q_1 + 1 \geq 1$. Таким образом, $q_2 \geq q_1$. Получаем, что

$$g(d_2, m) - g(d_1, m) = q_2 - q_1 \geq 0, \quad g(d_2, m) \geq g(d_1, m).$$

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

ДОКАЗАТЕЛЬСТВО. При $d = 2$ множество $[2, d] \cap \mathbb{N}$ состоит из одной точки и утверждение теоремы очевидно.

Пусть $d \geq 3$ – некоторое натуральное число и $m_1, m_2 \in \mathbb{N}$, $2 \leq m_1 < m_2 \leq d$. Докажем, что $g(d, m_1) \leq g(d, m_2)$. Доказательство проведем индукцией по d .

База индукции. Пусть $d = 3$ и $2 \leq m \leq 3$. Имеем $3 = 1 \cdot 2^1 + 1 = 1 \cdot 3^1$. Следовательно,

$$g(3, 2) = (2 - 1) \cdot 1 + 1 - 1 = 1 < 2 = (3 - 1) \cdot 1 + 1 - 1 = g(3, 3).$$

Шаг индукции. Пусть $d > 3$ и для всех $h < d$ утверждение теоремы выполнено.

I. Пусть $m_1, m_2 \in \mathbb{N}$, $2 \leq m_1 < m_2 \leq d$, такие, что $[\log_{m_1} d] = [\log_{m_2} d] = l$. Так как $m_2 \leq d$, то $l \geq 1$. Рассмотрим функцию $f: (1, +\infty) \rightarrow \mathbb{R}$, $f(x) = l(x - 1) + d/x^l$. Функция f непрерывна и дифференцируема на области определения и

$$f'(x) = l - \frac{ld}{x^{l+1}} = \frac{l(x^{l+1} - d)}{x^{l+1}}.$$

Поскольку для $x \in [m_1, m_2]$ выполнено $[\log_x d] = l$, то $x^{l+1} > d$. Следовательно, $f'(x) > 0$ на $[m_1, m_2]$, т.е. на отрезке $[m_1, m_2]$ функция $f(x)$ возрастает. Тогда для $n_1, n_2 \in \mathbb{N} \cap [m_1, m_2]$, $n_1 < n_2$, получаем, что

$$\begin{aligned} f(n_1) &< f(n_2), & [f(n_1)] &\leq [f(n_2)], \\ g(d, n_1) &= (n_1 - 1)l + \left\lceil \frac{d}{n_1^l} \right\rceil = \left\lceil (n_1 - 1)l + \frac{d}{n_1^l} \right\rceil = [f(n_1)] \\ &\leq [f(n_2)] = \left\lceil (n_2 - 1)l + \frac{d}{n_2^l} \right\rceil = (n_2 - 1)l + \left\lceil \frac{d}{n_2^l} \right\rceil = g(d, n_2). \end{aligned}$$

II. Таким образом, осталось доказать, что для $2 \leq m < d$ таких, что $[\log_m d] > [\log_{m+1} d]$, выполнено $g(d, m) \leq g(d, m+1)$. Обозначим $l = [\log_m d]$, $s = [\log_{m+1} d]$, $l > s \geq 1$. Число d единственным образом представляется в виде

$$d = qm^l + r = q_1(m+1)^s + r_1,$$

где $q, q_1 \in \mathbb{N}$, $r, r_1 \in \mathbb{Z}_+$ и $1 \leq q \leq m-1$, $1 \leq q_1 \leq m$, $0 \leq r < m^l$, $0 \leq r_1 < (m+1)^s$. Заметим, что $\text{НОД}(m, m+1) = 1$, поэтому qm^l делится на m^2 , а $q_1(m+1)^s$ не делится на m^2 , поэтому $r \neq r_1$. Следовательно, хотя бы один из остатков r и r_1 строго положителен. Рассмотрим следующие случаи.

1. Случай $s = 1$.

i. Пусть $r > 0$, $r_1 > 0$.

Положим $r_0 = \min\{r, r_1\} > 0$, $d_0 = d - r_0$. Имеем $d > d_0 \geq qm^l \geq m^l \geq 2^2 = 4$, $d_0 \geq m+1$. Тогда по предположению индукции

$$g(d_0, m) \leq g(d_0, m+1).$$

Из равенства (6) заключаем, что $g(d, m) = g(d_0, m)$ и $g(d, m+1) = g(d_0, m+1)$. Следовательно,

$$g(d, m) \leq g(d, m+1).$$

ii. Пусть $r > 0$, $r_1 = 0$.

Если $d = m+1$, то $m+1 > qm^l \geq m^l \geq m^2$. Это неравенство не выполняется при $m \geq 2$, поэтому можно считать, что $d > m+1$, $d-1 \geq m+1$ и $q_1 > 1$. Тогда по предположению индукции

$$g(d-1, m) \leq g(d-1, m+1).$$

Из равенства (6) заключаем, что $g(d, m) = g(d-1, m)$. Также

$$d-1 = (q_1-1)(m+1) + m, \quad g(d-1, m+1) = m + (q_1-1) - 1.$$

Поэтому

$$g(d, m+1) = m + q_1 - 1 = g(d-1, m+1) + 1.$$

Следовательно, получаем неравенство

$$g(d, m) = g(d-1, m) \leq g(d-1, m+1) = g(d, m+1) - 1 < g(d, m+1).$$

iii. Пусть $r = 0$, $r_1 > 0$.

Если $d = m^2$, то $d = (m-1)(m+1) + 1$. Следовательно,

$$g(d, m) = (m-1) \cdot 2 + 1 - 1 = 2m - 2 = m \cdot 1 + m - 1 - 1 = g(d, m+1).$$

Пусть $d > m^2$. Напомним, что $r_1 \leq m < m^l$ и при $l \geq 3$ также $r_1 < m^{l-1}$. Имеем

$$\begin{aligned} d - r_1 - 1 &= \begin{cases} (q-1)m^l + (m^l - r_1 - 1) & \text{при } q > 1, \\ (m-1)m^{l-1} + (m^{l-1} - r_1 - 1) & \text{при } q = 1, l \geq 3, \end{cases} \\ g(d - r_1 - 1, m) &= (m-1)l + (q-1) - 1 & \text{при } q > 1, \\ g(d - r_1 - 1, m) &= (m-1)(l-1) + m - 1 - 1 \\ &= (m-1)l + (q-1) - 1 & \text{при } q_1 = 1. \end{aligned}$$

Таким образом,

$$g(d, m) = (m - 1)l + q - 1 = g(d - r_1 - 1, m) + 1.$$

При доказательстве п. 1, ii было показано, что $g(d - r_1, m + 1) = g(d - r_1 - 1, m + 1) + 1$. Используя равенство (6), получаем, что

$$g(d, m + 1) = g(d - r_1, m + 1) = g(d - r_1 - 1, m + 1) + 1.$$

По предположению индукции $g(d - r_1 - 1, m) \leq g(d - r_1 - 1, m + 1)$. Следовательно, получаем неравенство

$$g(d, m) = g(d - r_1 - 1, m) + 1 \leq g(d - r_1 - 1, m + 1) + 1 = g(d, m + 1).$$

2. Случай $s \geq 2$.

i. Пусть $r > 0, r_1 > 0$.

Положим $r_0 = \min\{r, r_1\} > 0, d_0 = d - r_0$. Имеем

$$d > d_0 \geq qm^l \geq m^l \geq 2^2 = 4, d_0 \geq \max\{m^l, (m + 1)^s\} \geq m + 1.$$

Тогда по предположению индукции $g(d_0, m) \leq g(d_0, m + 1)$. Из равенства (6) заключаем, что

$$g(d, m) = g(d_0, m) \text{ и } g(d, m + 1) = g(d_0, m + 1).$$

Следовательно,

$$g(d, m) \leq g(d, m + 1).$$

ii. Пусть $r > 0, r_1 = 0$. При $s \geq 2$ верно, что $d > m + 1, d - 1 \geq m + 1$. Тогда по предположению индукции $g(d - 1, m) \leq g(d - 1, m + 1)$. Из равенства (6) заключаем, что $g(d, m) = g(d - 1, m)$. Также

$$d - 1 = \begin{cases} (q_1 - 1)(m + 1)^s + ((m + 1)^s - 1) & \text{при } q_1 > 1, \\ m(m + 1)^{s-1} + ((m + 1)^{s-1} - 1) & \text{при } q_1 = 1, \end{cases}$$

$$g(d - 1, m + 1) = \begin{cases} ms + (q_1 - 1) - 1 & \text{при } q_1 > 1, \\ m(s - 1) + m - 1 = ms + (q_1 - 1) - 1 & \text{при } q_1 = 1. \end{cases}$$

Поэтому

$$g(d, m + 1) = ms + q_1 - 1 = g(d - 1, m + 1) + 1.$$

Следовательно, получаем неравенство

$$g(d, m) = g(d - 1, m) \leq g(d - 1, m + 1) = g(d, m + 1) - 1 < g(d, m + 1).$$

iii. Пусть $r = 0, r_1 > 0$.

Обозначим $d_0 = d/m \in \mathbb{N}$. Поскольку в данном случае $d > (m + 1)^2$, то $d_0 > m + 1$. Кроме того, число d_0 представляется в виде

$$d_0 = qm^{l-1} = q_0(m + 1)^t + r_0,$$

где $q_0, t \in \mathbb{N}$, $r_0 \in \mathbb{Z}_+$, $1 \leq q_0 \leq m$, $0 \leq r_0 < (m+1)^t$. Тогда по предположению индукции

$$g(d_0, m) = (m-1)(l-1) + q - 1 \leq mt + q_0 - 1 = g(d_0, m+1). \quad (7)$$

Прибавляя $m-1$ к обеим частям неравенства (7), получаем следующее неравенство:

$$(m-1)l + q - 1 \leq m(t+1) + (q_0 - 1) - 1,$$

или, что эквивалентно,

$$g(d, m) \leq m(t+1) + (q_0 - 1) - 1. \quad (8)$$

По определению чисел d_0 и d имеем

$$d = md_0 = q_0 m(m+1)^t + mr_0$$

и, таким образом,

$$d \geq q_0 m(m+1)^t.$$

Как показано в теореме 3.2, при фиксированном значении $m+1$ справедлива оценка

$$g(q_0 m(m+1)^t, m+1) \leq g(d, m+1). \quad (9)$$

Непосредственно вычислим значение $g(q_0 m(m+1)^t, m+1)$. При $q_0 = 1$ имеем

$$\begin{aligned} q_0 m(m+1)^t &= m(m+1)^t, \\ g(q_0 m(m+1)^t, m+1) &= mt + m - 1 = m(t+1) + (q_0 - 1) - 1. \end{aligned}$$

При $2 \leq q_0 \leq m$, разделив $q_0 m$ на $m+1$ с остатком, получаем

$$\begin{aligned} q_0 m &= (q_0 - 1)(m+1) + (m+1 - q_0), \\ q_0 m(m+1)^t &= (q_0 - 1)(m+1)^{t+1} + (m+1 - q_0)(m+1)^t, \\ g(q_0 m(m+1)^t, m+1) &= m(t+1) + (q_0 - 1) - 1. \end{aligned}$$

Таким образом, при любом значении q_0 справедливо равенство

$$g(q_0 m(m+1)^t, m+1) = m(t+1) + (q_0 - 1) - 1,$$

т.е. значение функции $g(q_0 m(m+1)^t, m+1)$ совпадает с правой частью неравенства (8).

Тогда из неравенств (8) и (9) получаем требуемую оценку

$$g(d, m) \leq g(q_0 m(m+1)^t, m+1) \leq g(d, m+1).$$

Теперь докажем вспомогательные комбинаторные результаты.

ЛЕММА 3.4. Пусть $l, m, q \in \mathbb{N}$, $m \geq 2$, $1 \leq q \leq m - 1$. Положим $N = (m - 1)l + q$. Рассмотрим множество $\mathcal{X} \subseteq \mathbb{Z}^N$, состоящее из всех строк $X = (x_1, \dots, x_N)$ таких, что

$$0 \leq x_N \leq x_{N-1} \leq \dots \leq x_2 \leq x_1 \leq m - 1, \quad \sum_{i=1}^N x_i = N.$$

Рассмотрим функцию $F: \mathcal{X} \rightarrow \mathbb{Z}$,

$$F(X) = \prod_{i=1}^N (x_i + 1).$$

Тогда для любого $X \in \mathcal{X}$ справедливо неравенство

$$F(X) \geq (q + 1)m^l,$$

причем минимум достигается на наборе $X = (x_1, \dots, x_n)$ следующего вида

$$x_1 = \dots = x_l = m - 1, \quad x_{l+1} = q, \quad x_{l+2} = \dots = x_N = 0.$$

ДОКАЗАТЕЛЬСТВО. При $m = 2$ множество $\mathcal{X}$ состоит из одной строки $X = (1, 1, \dots, 1)$, $q = 1$, $N = l + 1$ и

$$F(X) = 2^N = 2^{l+1} = (q + 1)m^l.$$

Пусть $m > 2$. Так как множество $\mathcal{X}$ конечно, то существует строка $Y = (y_1, \dots, y_N) \in \mathcal{X}$ такая, что $F(Y) = \min_{X \in \mathcal{X}} F(X)$.

Покажем, что Y не может содержать двух координат y_p и y_q , $1 \leq p < q \leq N$, одновременно удовлетворяющих неравенству $0 < y_i < m - 1$.

Предположим противное. Пусть для некоторых $1 \leq p < q \leq N$ выполнено

$$0 < y_p < m - 1, \quad 0 < y_q < m - 1.$$

Обозначим $s = y_p + y_q$. Имеем $1 < s < 2m - 3$. Рассмотрим функцию

$$F_0(y) = (y + 1)(s - y + 1) \prod_{\substack{i=1 \\ i \neq p, q}}^N (y_i + 1) = (y + 1)(s - y + 1)P'.$$

При фиксированном значении s произведение P' не зависит от y .

1. Пусть $1 < s \leq m - 1$. Рассмотрим функцию $F_0(y)$ при $0 \leq y \leq s$. Для любого $y \in \mathbb{Z}$, $0 \leq y \leq s$, строка $X(y)$, состоящая из чисел

$$y, \quad s - y, \quad y_i, \quad i \in \{1, \dots, N\} \setminus \{p, q\},$$

упорядоченных по убыванию, принадлежит множеству $\mathcal{X}$ и $F(X(y)) = F_0(y)$. Квадратичная функция $z(y) = (y + 1)(s - y + 1)$ строго возрастает при $0 \leq y \leq [s/2]$, при этом $0 < y_q \leq [s/2]$. Поэтому $z(0) < z(y_q)$. Следовательно, получаем, что

$$F(Y) = F_0(y_q) = z(y_q)P' > z(0)P' = F_0(0) = F(X(0)),$$

что противоречит выбору Y .

2. Пусть $m - 1 \leq s < 2m - 3$. Рассмотрим функцию $F_0(y)$ при $s - (m - 1) \leq y \leq m - 1$. Для любого $y \in \mathbb{Z}$, $s - (m - 1) \leq y \leq m - 1$, строка $X(y)$, состоящая из чисел

$$y, \quad s - y, \quad y_i, \quad i \in \{1, \dots, N\} \setminus \{p, q\},$$

упорядоченных по убыванию, принадлежит множеству $\mathcal{X}$ и $F(X(y)) = F_0(y)$. Квадратичная функция $z(y) = (y + 1)(s - y + 1)$ строго убывает при $[(s + 1)/2] \leq y \leq m - 1$, при этом $[(s + 1)/2] \leq y_p < m - 1$. Поэтому $z(m - 1) < z(y_p)$. Следовательно, получаем, что

$$F(Y) = F_0(y_p) = z(y_p)P' > z(m - 1)P' = F_0(m - 1) = F(X(m - 1)),$$

что противоречит выбору Y .

Таким образом, для некоторых $\varepsilon, r, y \in \mathbb{Z}$, где $0 \leq r \leq N$, $1 \leq y \leq m - 2$, $\varepsilon = 0, 1$, строка Y удовлетворяет условию $y_1 = \dots = y_r = m - 1$, $y_{r+1} = \varepsilon y$, $y_{r+2} = \dots = y_N = 0$. Так как $Y \in \mathcal{X}$, то

$$N = l(m - 1) + q = r(m - 1) + \varepsilon y.$$

Откуда при $q \leq m - 2$ получаем, что $\varepsilon y = q$, $r = l$. Поэтому $y = q$. При $q = m - 1$ получаем $\varepsilon y = 0$ и $r = l + 1$. Следовательно, в обоих случаях $y_1 = \dots = y_l = m - 1$, $y_{l+1} = q$, $y_{l+2} = \dots = y_N = 0$.

Тогда

$$F(Y) = (m - 1 + 1)^l (q + 1)^1 (0 + 1)^{N-l-1} = (q + 1)m^l.$$

ПРЕДЛОЖЕНИЕ 3.5. Пусть $k \in \mathbb{N}$, $X = (x_1, \dots, x_k) \in \mathbb{Z}_+^k$, $X \neq (0, \dots, 0)$ и $x_1 \geq x_2 \geq \dots \geq x_k$. Пусть существуют такие $X' = (x'_1, \dots, x'_k)$, $X'' = (x''_1, \dots, x''_k) \in \mathbb{Z}_+^k$, что $X', X'' \neq (0, \dots, 0)$ и $X = X' + X''$. Пусть $Y'' = (y''_1, \dots, y''_k) \in \mathbb{Z}_+^k$ и $Y'' \stackrel{\text{lex}}{>} X''$. Положим $Y = X' + Y''$. Пусть $\varphi \in S_k$ такая, что $y_{\varphi(1)} \geq y_{\varphi(2)} \geq \dots \geq y_{\varphi(k)}$. Обозначим $Y_\varphi = (y_{\varphi(1)}, y_{\varphi(2)}, \dots, y_{\varphi(k)})$. Тогда $X \stackrel{\text{lex}}{<} Y_\varphi$.

ДОКАЗАТЕЛЬСТВО. По условию $X'' \stackrel{\text{lex}}{<} Y''$. Прибавив X' к обеим частям сравнения, получим $X = X' + X'' \stackrel{\text{lex}}{<} X' + Y'' = Y$. При упорядочивании справедливо $Y \stackrel{\text{lex}}{\leq} Y_\varphi$. Следовательно, $X \stackrel{\text{lex}}{<} Y_\varphi$.

ЗАМЕЧАНИЕ 3.6. Из коммутативности алгебры $\mathcal{A}$ следует, что для произвольных слов $v, w \in \mathcal{S}^*$ условие $w \in \wp_I(v)$ влечет равенство $v = w$ как элементов алгебры. Поэтому в дальнейшем, говоря о слове $v \in \mathcal{S}^*$, будем рассматривать класс эквивалентности $\wp_I(v)$, заданный представителем вида

$$a_1^{\#_1(v)} a_2^{\#_2(v)} \dots a_k^{\#_k(v)}.$$

ОПРЕДЕЛЕНИЕ 3.7. Пусть слово $v = a_1^{i_1} a_2^{i_2} \dots a_k^{i_k} \in \mathcal{S}^*$. Подсловом слова v называется любое слово $w = a_1^{j_1} a_2^{j_2} \dots a_k^{j_k} \in \mathcal{S}^*$, удовлетворяющее условиям $j_s \leq i_s$ для любого $s = 1, \dots, k$.

ЛЕММА 3.8. Пусть $\mathbb{F}$ – произвольное поле, $k, M \in \mathbb{N}$ и $k, M \geq 2$. Пусть $\mathcal{A}$ – ассоциативная конечномерная коммутативная $\mathbb{F}$ -алгебра и $\mathcal{S} = \{a_1, \dots, a_k\} \subseteq \mathcal{A}$ – некоторое ее подмножество. Пусть $v \in \mathcal{S}^M$ – несократимое слово и множество всех подслов v длины не большей $M-1$ линейно независимо. Тогда существуют

$$n \in \mathbb{N}, \quad w \in \mathcal{L}_{M-1}(\mathcal{S}), \quad u_1, \dots, u_n \in \mathcal{S}^M \quad \alpha_1, \dots, \alpha_n \in \mathbb{F}$$

такие, что

- 1) для всех $1 \leq s \leq n$ слово u_s несократимо;
- 2) для всех $1 \leq s \leq n$ выполнено $v \stackrel{I_0}{<} u_s$;
- 3) $v = \sum_{i=1}^n \alpha_i u_i + w$.

ДОКАЗАТЕЛЬСТВО. В силу линейной зависимости существуют $v_1, \dots, v_p$ (подслова v) и $\beta_1, \dots, \beta_p \in \mathbb{F}$, не все равные нулю, для которых

$$\sum_{j=1}^p \beta_j v_j = 0. \quad (10)$$

Если $p = 1$, то $v_1 = 0$. Тогда $v = 0$, что противоречит несократимости v . Следовательно, $p \geq 2$. Не ограничивая общности, можно считать, что подслова $v_1, \dots, v_p$ упорядочены так, что их длины не возрастают.

Пусть t – это максимум из длин $v_1, \dots, v_p$, $1 \leq t \leq M-1$ и $v_1, \dots, v_r$ имеют длину t , $v_{r+1}, \dots, v_p$ имеют длину не более $t-1$. Если $r = 1$, то из равенства (10) получаем

$$v_1 = -\beta_1^{-1} \sum_{j=2}^p \beta_j v_j \in \mathcal{L}_{t-1}(\mathcal{S}),$$

т.е. v_1 сократимо. Но тогда и v было бы сократимо. Получаем противоречие. Значит, $r \geq 2$.

Положим $I_0(v) = (x_1, \dots, x_k)$, $\tau \in S_k$ и $v = a_{\tau(1)}^{x_1} \dots a_{\tau(k)}^{x_k}$.

Упорядочим переменные следующим образом: $a_{\tau(1)} > a_{\tau(2)} > \dots > a_{\tau(k)}$. Тогда слова из множества $\mathcal{S}^t$ будут упорядочены лексикографически. Существует такая подстановка $\sigma \in S_r$, что

$$v_{\sigma(1)} \stackrel{\text{lex}}{<} v_{\sigma(2)} \stackrel{\text{lex}}{<} \dots \stackrel{\text{lex}}{<} v_{\sigma(r)}.$$

Тогда из равенства (10) получаем

$$v_{\sigma(1)} = -\beta_{\sigma(1)}^{-1} \sum_{\substack{j=1 \\ j \neq \sigma(1)}}^p \beta_j v_j = \sum_{\substack{j=1 \\ j \neq \sigma(1)}}^r \beta'_j v_j + V_{t-1}, \quad (11)$$

где $\beta'_j = -\beta_{\sigma(1)}^{-1} \beta_j$, $V_{t-1} \in \mathcal{L}_{t-1}(\mathcal{S})$.

По определению 3.7 существует $v' \in \mathcal{S}^{(M-t)}$, для которого

$$v = v' \cdot v_{\sigma(1)}. \quad (12)$$

Подставив выражение для $v_{\sigma(1)}$, полученное в (11), в равенство (12), получаем

$$v = \sum_{\substack{j=1 \\ j \neq \sigma(1)}}^r \beta'_j v' v_j + V_{M-1}, \quad (13)$$

где $V_{M-1} \in \mathcal{L}_{M-1}(\mathcal{S})$.

Пусть $K = \{1, \dots, r\} \setminus \{\sigma(1)\}$, $K_1 \subseteq K$ – подмножество индексов s , для которых $v' v_s$ несократимы, $K_2 = K \setminus K_1$.

Допустим, что множество K_1 пусто. В этом случае $\sum_{j \in K} \beta'_j v' v_j \in \mathcal{L}_{M-1}(\mathcal{S})$ и из равенства (13) следует, что $v \in \mathcal{L}_{M-1}(\mathcal{S})$, т.е. сократимо. Получаем противоречие.

Положим $n = |K_1|$, $K_1 = \{k_1, \dots, k_n\}$, $u_j = v' v_{k_j}$, $\alpha_j = \beta'_{k_j}$, $j = 1, \dots, n$, и $w = \sum_{s \in K_2} \beta'_s v' v_s + V_{M-1}$. По лемме 3.5 при всех j получаем $I_0(v) < I_0(u_j)$.

ЛЕММА 3.9. Пусть $\mathbb{F}$ – произвольное поле, $\mathcal{A}$ – ассоциативная конечномерная коммутативная $\mathbb{F}$ -алгебра с единицей, $\mathcal{S} = \{a_1, \dots, a_k\} \subseteq \mathcal{A}$ – система порождающих. Пусть $m(\mathcal{S}) = m \geq 2$, $d(\mathcal{A}) = qm^l + r$, $l \in \mathbb{N}$, $0 \leq r < m^l$, $1 \leq q \leq m - 1$. Положим $N = (m - 1)l + q$. Тогда любое слово $v \in \mathcal{S}^N$ сократимо.

ДОКАЗАТЕЛЬСТВО. Предположим противное, т.е. что существует несократимое слово $v' \in \mathcal{S}^N$.

Рассмотрим отображение $T: I_0(\mathcal{S}^N) \rightarrow \mathbb{Z}_+^N$ такое, что

$$T((x_1, \dots, x_k)) = \begin{cases} (x_1, \dots, x_k, 0, \dots, 0) & \text{при } k < N, \\ (x_1, \dots, x_k) & \text{при } k = N, \\ (x_1, \dots, x_N) & \text{при } k > N. \end{cases}$$

Любое слово v длины N в k -буквенном алфавите содержит не более $\min(k, N)$ различных букв. Поэтому при $k > N$ у вектора $I_0(v)$ координаты с $(N + 1)$ -ой по k -ю нулевые. Следовательно, отображение T биективно.

Пусть $\mathcal{T}_2$ – подмножество тех строк $(y_1, \dots, y_N)$ из $\text{Im } T$, у которых $y_1 \geq m$. Положим $\mathcal{T}_1 = \text{Im } T \setminus \mathcal{T}_2$. Если $T(I_0(v)) \in \mathcal{T}_2$, то v содержит m -ю степень элемента из $\mathcal{S}$ и будет сократимо по определению m . Следовательно, $T(I_0(v')) \in \mathcal{T}_1$. Заметим, что $\mathcal{T}_1 \subseteq \mathcal{X}$, где $\mathcal{X}$ – множество, определенное в лемме 3.4, $(\mathcal{X}, \leq^{\text{lex}})$ – конечное линейно упорядоченное множество. Поэтому существует несократимое слово $v'' \in \mathcal{S}^N$ такое, что любое $w \in \mathcal{S}^N$, удовлетворяющее $w \stackrel{I_0}{>} v''$, сократимо.

Получаем, что v'' – несократимое слово и для него не выполнено утверждение леммы 3.8. Это означает, что оно не удовлетворяет условию леммы 3.8, касающегося линейной зависимости подслов. Следовательно, множество всех подслов слова v'' длины не большей $N - 1$ линейно независимо.

Пусть M – число всех подслов слова v'' , $T(I_0(v'')) = (x''_1, \dots, x''_N)$; число всех подслов слова v'' длины не большей $N - 1$ равно $M - 1$. Имеем

$$M = \prod_{i=1}^k (\#_i(v'') + 1) = \prod_{j=1}^N (x''_j + 1) = F(T(I_0(v''))), \quad (14)$$

где F – функция, определенная в лемме 3.4. Соотношение (14) и лемма 3.4 приводят к такой оценке:

$$\dim \mathcal{L}_{N-1}(\mathcal{S}) \geq M - 1 \geq (q + 1)m^l - 1 = qm^l + (m^l - 1) \geq qm^l + r = \dim \mathcal{A}.$$

С другой стороны, из несократимости слова v'' следует, что

$$\dim \mathcal{L}_{N-1}(\mathcal{S}) < \dim \mathcal{A}.$$

Полученное противоречие доказывает лемму.

Как следствие, получаем верхнюю оценку для длины системы порождающих.

СЛЕДСТВИЕ 3.10. Пусть $\mathbb{F}$ – произвольное поле, $\mathcal{A}$ – ассоциативная конечномерная коммутативная $\mathbb{F}$ -алгебра с единицей, $\mathcal{S}$ – система порождающих алгебры $\mathcal{A}$. Пусть

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

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

ДОКАЗАТЕЛЬСТВО. Пусть $m(\mathcal{S}) = m$, $d = \dim \mathcal{A}$.

При $m = 1$ любой элемент из $\mathcal{S}$ имеет вид $\alpha \cdot 1_{\mathcal{A}}$, $\alpha \in \mathbb{F}$, алгебра $\mathcal{A} \cong \mathbb{F}$ и $l(\mathcal{S}) = l(\mathcal{A}) = l(\mathbb{F}) = 0$.

Пусть $m \geq 2$. Обозначим $l = [\log_m d] \geq 1$. Тогда $m^l \leq d < m^{l+1}$ и после деления с остатком d на m^l получим, что $d = qm^l + r$, где $0 \leq r < m^l$, $1 \leq q \leq m - 1$. Имеем

$$[m^{\{\log_m d\}}] = [m^{\log_m d - [\log_m d]}] = \left\lfloor \frac{d}{m^l} \right\rfloor = q, \quad g(d, m) = (m - 1)l + q - 1.$$

Из леммы 3.9 получаем, что все слова из $\mathcal{S}^{=(g(d, m)+1)}$ сократимы. Следовательно, $l(\mathcal{S}) \leq g(d, m)$.

Докажем основную теорему.

ТЕОРЕМА 3.11. Пусть $\mathbb{F}$ – произвольное поле, $\mathcal{A}$ – ассоциативная конечномерная коммутативная $\mathbb{F}$ -алгебра с единицей. Пусть

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

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

ДОКАЗАТЕЛЬСТВО. Пусть $m(\mathcal{A}) = m$, $d = \dim \mathcal{A}$.

При $m = 1$ алгебра $\mathcal{A} \cong \mathbb{F}$ и $l(\mathcal{A}) = l(\mathbb{F}) = 0$.

Пусть $m \geq 2$. Пусть $\mathcal{S}$ – произвольная система порождающих алгебры $\mathcal{A}$. По определению $m(\mathcal{S}) \leq m$. Следовательно, по теореме 3.3

$$g(d, m(\mathcal{S})) \leq g(d, m). \quad (15)$$

Оценка (15) справедлива для любой системы порождающих. Таким образом,

$$l(\mathcal{A}) = \max_{\mathcal{S}} l(\mathcal{S}) \leq \max_{\mathcal{S}} g(d, m(\mathcal{S})) \leq \max_{\mathcal{S}} g(d, m) = g(d, m).$$

СЛЕДСТВИЕ 3.12. Пусть $\mathbb{F}$ – произвольное поле, $\mathcal{A}$ – ассоциативная конечномерная $\mathbb{F}$ -алгебра с единицей, $\mathcal{S} = \{a_1, \dots, a_k\}$ – такая система порождающих алгебры $\mathcal{A}$, что

$$a_i a_j - a_j a_i \in \mathcal{L}_1(\mathcal{S}), \quad 1 \leq i < j \leq k.$$

Пусть

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

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

§ 4. Сравнение с общей оценкой

Покажем, что для коммутативных алгебр оценка длины, полученная в теореме 3.11, лучше общей оценки длины из теоремы 2.3.

ТЕОРЕМА 4.1. Пусть $d, m \in \mathbb{N}$, $d \geq m \geq 2$, и

$$g(d, m) = (m-1)[\log_m d] + [m^{\{\log_m d\}}] - 1, \quad f(d, m) = m\sqrt{\frac{2d}{m-1} + \frac{1}{4}} + \frac{m}{2} - 2.$$

Тогда справедливо неравенство

$$g(d, m) < f(d, m). \quad (16)$$

ДОКАЗАТЕЛЬСТВО. Число d единственным образом представляется в виде $d = qm^l + r$, где $l \in \mathbb{N}$, $0 \leq r < m^l$, $1 \leq q \leq m-1$. При этом

$$g(d, m) = (m-1)l + q - 1, \quad f(d, m) = m\sqrt{\frac{2(qm^l + r)}{m-1} + \frac{1}{4}} + \frac{m}{2} - 2.$$

Рассмотрим два случая.

1. Случай $l = 1$. Имеем $g(d, m) = m + q - 2$ и

$$f(d, m) = m\sqrt{\frac{2(qm + r)}{m-1} + \frac{1}{4}} + \frac{m}{2} - 2 \geq m\sqrt{\frac{2qm}{m-1} + \frac{1}{4}} + \frac{m}{2} - 2. \quad (17)$$

Из неравенства (17) следует, что для проверки условия $g(d, m) < f(d, m)$ достаточно доказать, что

$$m\sqrt{\frac{2qm}{m-1} + \frac{1}{4}} + \frac{m}{2} - 2 > m + q - 2,$$

или, после вычитания из обеих частей $m/2 - 2$, что

$$m\sqrt{\frac{2qm}{m-1} + \frac{1}{4}} > \frac{m}{2} + q.$$

Выражения в обеих частях неравенства положительны, т.е. неравенство сохранится и после возведения их в квадрат. Следовательно,

$$m^2 \left(\frac{2qm}{m-1} + \frac{1}{4} \right) > \frac{m^2}{4} + qm + q^2$$

или

$$\frac{q}{m-1}(m^3 - m^2 + (1-q)m + q^2) > 0. \quad (18)$$

Таким образом, осталось доказать, что выполнено неравенство (18).

Рассмотрим функцию $h: \mathbb{R} \rightarrow \mathbb{R}$, $h(x) = x^3 - x^2 + (1-q)x + q$. Имеем

$$h'(x) = 3x^2 - 2x + 1 - q,$$

при $q \in \mathbb{N}$ верно неравенство $3q - 2 > 0$, $h'(x) = 0$ при $x_{1,2} = (1 \pm \sqrt{3q-2})/3$ и $h'(x) > 0$ при $x > (1 + \sqrt{3q-2})/3$. Следовательно, функция $h(x)$ возрастает на интервале $((1 + \sqrt{3q-2})/3, +\infty)$. Отметим, что при $q \in \mathbb{N}$ $(1 + \sqrt{3q-2})/3 < q$, поэтому $h(x)$ возрастает и на $[q, +\infty)$. Поскольку при этом $h(q) = q^3 - 2q^2 + 2q = q((q-1)^2 + 1) > 0$ при $q > 0$, то $h(x) > 0$ при $x \geq q$. По условию $q \leq m-1$, $q > 0$ и $m-1 > 0$. Поэтому $h(m) > h(q) > 0$ и

$$\frac{q}{m-1}h(m) > 0.$$

Итак, неравенство (18) выполнено.

2. Случай $l \geq 2$. Оценим $f(d, m)$ снизу. Имеем

$$f(d, m) > m\sqrt{\frac{2(qm^l + r)}{m-1}} + \frac{m}{2} - 2 > m\sqrt{\frac{2(qm^l)}{m}} + \frac{m}{2} - 2 \geq \sqrt{2}m^{\frac{l+1}{2}} - 1. \quad (19)$$

Оценим $g(d, m)$ сверху. Получаем

$$g(d, m) \leq l(m-1) + m - 1 - 1 = (l+1)(m-1) - 1. \quad (20)$$

Рассмотрим функцию $\delta: [2, +\infty) \rightarrow \mathbb{R}$, $\delta(x) = \sqrt{2}x^{(l+1)/2} - (l+1)(x-1)$. Найдем $\delta'(x)$:

$$\delta'(x) = \frac{\sqrt{2}(l+1)}{2}x^{(l-1)/2} - (l+1).$$

Кроме того, поскольку $x \geq 2$ и $l \geq 2$, то $x^{(l-1)/2} \geq x^{1/2} \geq \sqrt{2}$. Следовательно,

$$\delta'(x) \geq \frac{\sqrt{2}(l+1)}{2} \sqrt{2} - (l+1) = 0,$$

т.е. функция $\delta(x)$ возрастает на области определения и для всех $x > 2$ выполнено $\delta(x) \geq \delta(2)$.

Теперь рассмотрим функцию $h: [2, +\infty) \rightarrow \mathbb{R}$, $h(l) = \sqrt{2} \cdot 2^{(l+1)/2} - (l+1) = 2 \cdot 2^{l/2} - (l+1)$. Имеем

$$h'(l) = 2 \cdot \frac{1}{2} \ln 2 \cdot 2^{l/2} - 1.$$

Так как $l \geq 2$, то $2^{l/2} \geq 2$ и $2 \ln 2 > 1$. Следовательно, $h'(l) \geq 0$, т.е. функция $h(l)$ возрастает на области определения и для всех $l > 2$ выполнено $h(l) \geq h(2) = 1$.

Следовательно, из неравенств (19) и (20) получаем, что

$$f(d, m) - g(d, m) > \sqrt{2} m^{(l+1)/2} - (l+1)(m-1) \geq 2 \cdot 2^{l/2} - (l+1) \geq 1.$$

§ 5. О длине алгебры диагональных матриц

Теорема 3.11 позволяет точно вычислить длину алгебры диагональных матриц $D_n(\mathbb{F})$ над произвольным полем $\mathbb{F}$.

Нам понадобится нижняя оценка длины тензорного произведения алгебр.

ЛЕММА 5.1. Пусть $\mathbb{F}$ – произвольное поле, $\mathcal{A}$ и $\mathcal{B}$ – конечномерные алгебры с единицами над $\mathbb{F}$. Тогда $l(\mathcal{A} \otimes_{\mathbb{F}} \mathcal{B}) \geq l(\mathcal{A}) + l(\mathcal{B})$.

ДОКАЗАТЕЛЬСТВО. Обозначим $m = l(\mathcal{A})$, $n = l(\mathcal{B})$. Построим систему порождающих алгебры $\mathcal{A} \otimes \mathcal{B}$ длины $m + n$.

Пусть $\mathcal{S}_{\mathcal{A}} = \{a_1, \dots, a_p\}$ – система порождающих для $\mathcal{A}$ длины m и $\mathcal{S}_{\mathcal{B}} = \{b_1, \dots, b_q\}$ – система порождающих для $\mathcal{B}$ длины n . Рассмотрим множество

$$\mathcal{S} = \{a_i \otimes 1, 1 \otimes b_j, i = 1, \dots, p, j = 1, \dots, q\} \subset \mathcal{A} \otimes_{\mathbb{F}} \mathcal{B}.$$

Покажем, что $\mathcal{S}$ является системой порождающих для алгебры $\mathcal{A} \otimes \mathcal{B}$ длины $m + n$.

Поскольку $\mathcal{L}_m(\mathcal{S}_{\mathcal{A}}) = \mathcal{A}$ и $\mathcal{L}_n(\mathcal{S}_{\mathcal{B}}) = \mathcal{B}$, то

$$\mathcal{L}_m(\mathcal{S}_{\mathcal{A}}) \otimes \mathcal{L}_n(\mathcal{S}_{\mathcal{B}}) = \mathcal{A} \otimes \mathcal{B}.$$

Пусть $N \in \mathbb{N}$. По определению

$$\mathcal{L}_N(\mathcal{S}) = \left\langle a_{i_1} \dots a_{i_s} \otimes b_{j_1} \dots b_{j_t} \mid \begin{array}{l} s, t \in \mathbb{Z}_+, \\ 0 \leq s + t \leq N \end{array} \right\rangle.$$

Заметим, что если $s \geq m+1$ или $t \geq n+1$, то любое слово $a_{i_1} \dots a_{i_s} \otimes b_{j_1} \dots b_{j_t}$ сократимо, так как сократимо $a_{i_1} \dots a_{i_s}$ или $b_{j_1} \dots b_{j_t}$, т.е.

$$\mathcal{L}_N(\mathcal{S}) = \left\langle a_{i_1} \dots a_{i_s} \otimes b_{j_1} \dots b_{j_t} \mid \begin{array}{l} s, t \in \mathbb{Z}_+, s \leq m, t \leq n, \\ 0 \leq s + t \leq N \end{array} \right\rangle. \quad (21)$$

Следовательно,

$$\begin{aligned}\mathcal{L}_{m+n}(\mathcal{S}) &= \left\langle a_{i_1} \dots a_{i_s} \otimes b_{j_1} \dots b_{j_t} \mid \begin{array}{l} s, t \in \mathbb{Z}_+, \\ 0 \leq s + t \leq m + n \end{array} \right\rangle \\ &= \left\langle a_{i_1} \dots a_{i_s} \otimes b_{j_1} \dots b_{j_t} \mid \begin{array}{l} s, t \in \mathbb{Z}_+, \\ s \leq m, t \leq n, \end{array} \right\rangle \\ &= \mathcal{L}_m(\mathcal{S}_{\mathcal{A}}) \otimes \mathcal{L}_n(\mathcal{S}_{\mathcal{B}}) = \mathcal{A} \otimes \mathcal{B}.\end{aligned}$$

Таким образом, $\mathcal{S}$ является системой порождающих для алгебры $\mathcal{A} \otimes \mathcal{B}$ и $l(\mathcal{S}) \leq m + n$.

Для доказательства равенства $l(\mathcal{S}) = m + n$ достаточно показать, что

$$\mathcal{L}_{m+n-1}(\mathcal{S}) \neq \mathcal{A} \otimes \mathcal{B}.$$

Действительно, из равенства (21) следует, что

$$\begin{aligned}\mathcal{L}_{m+n-1}(\mathcal{S}) &= \left\langle a_{i_1} \dots a_{i_s} \otimes b_{j_1} \dots b_{j_t} \mid \begin{array}{l} s, t \in \mathbb{Z}_+, s \leq m, t \leq n, \\ 0 \leq s + t \leq m + n - 1 \end{array} \right\rangle \\ &= \mathcal{L}_{m-1}(\mathcal{S}_{\mathcal{A}}) \otimes \mathcal{L}_n(\mathcal{S}_{\mathcal{B}}) + \mathcal{L}_m(\mathcal{S}_{\mathcal{A}}) \otimes \mathcal{L}_{n-1}(\mathcal{S}_{\mathcal{B}}).\end{aligned}$$

Пусть $v_1, \dots, v_d$ – базис пространства $\mathcal{L}_{m-1}(\mathcal{S}_{\mathcal{A}})$, $v_{d+1}, \dots, v_M$ – его дополнение до базиса пространства $\mathcal{L}_m(\mathcal{S}_{\mathcal{A}}) = \mathcal{A}$. Пусть также $w_1, \dots, w_r$ – базис пространства $\mathcal{L}_{n-1}(\mathcal{S}_{\mathcal{B}})$, $w_{r+1}, \dots, w_K$ – его дополнение до базиса пространства $\mathcal{L}_n(\mathcal{S}_{\mathcal{B}}) = \mathcal{B}$. Тогда по определению элементы $v_i \otimes w_j$ при $i = 1, \dots, M$, $j = 1, \dots, K$ образуют базис пространства $\mathcal{L}_m(\mathcal{S}_{\mathcal{A}}) \otimes \mathcal{L}_n(\mathcal{S}_{\mathcal{B}}) = \mathcal{A} \otimes \mathcal{B}$, элементы $v_i \otimes w_j$ при $i = 1, \dots, d$, $j = 1, \dots, K$ образуют базис пространства $\mathcal{L}_{m-1}(\mathcal{S}_{\mathcal{A}}) \otimes \mathcal{L}_n(\mathcal{S}_{\mathcal{B}})$ и элементы $v_i \otimes w_j$ при $i = 1, \dots, M$, $j = 1, \dots, r$ образуют базис пространства $\mathcal{L}_m(\mathcal{S}_{\mathcal{A}}) \otimes \mathcal{L}_{n-1}(\mathcal{S}_{\mathcal{B}})$. Таким образом, элементы $v_i \otimes w_j$ при $i = d + 1, \dots, M$, $j = r + 1, \dots, K$ лежат в $\mathcal{A} \otimes \mathcal{B} = \mathcal{L}_{m+n}(\mathcal{S})$, но не лежат в $\mathcal{L}_{m+n-1}(\mathcal{S})$.

Далее будем использовать следующий результат, ранее полученный автором.

ТЕОРЕМА 5.2 (см. [6; теорема 2]). Пусть $\mathcal{A}$ и $\mathcal{B}$ – конечномерные алгебры над полем $\mathbb{F}$ длины $l_{\mathcal{A}}$ и $l_{\mathcal{B}}$ соответственно. Тогда выполнено следующее неравенство:

$$\max\{l_{\mathcal{A}}, l_{\mathcal{B}}\} \leq l(\mathcal{A} \oplus \mathcal{B}) \leq l_{\mathcal{A}} + l_{\mathcal{B}} + 1. \quad (22)$$

ЛЕММА 5.3. Пусть $\mathbb{F}$ – произвольное поле и $\mathcal{A}$ – алгебра с единицей над $\mathbb{F}$. Равенство $l(\mathcal{A}) = \dim \mathcal{A} - 1$ выполняется тогда и только тогда, когда существует элемент $A \in \mathcal{A}$ степени $\deg A = \dim \mathcal{A}$, порождающий алгебру $\mathcal{A}$. Как следствие, алгебра $\mathcal{A}$ коммутативна.

ДОКАЗАТЕЛЬСТВО. *Достаточность.* Если алгебра $\mathcal{A}$ порождена одним элементом A степени $\deg A = \dim \mathcal{A}$, то возьмем в $\mathcal{A}$ систему порождающих $\mathcal{S} = \{A\}$. Получаем, что для любого $k \geq 0$ выполнено $\mathcal{L}_k(\mathcal{S}) = \langle 1_{\mathcal{A}}, A, A^2, \dots, A^k \rangle$ и, следовательно, $l(\mathcal{A}) \geq l(\mathcal{S}) = \deg A - 1 = \dim \mathcal{A} - 1$.

Необходимость. Положим $n = \dim \mathcal{A}$. При $n = 1$ алгебра $\mathcal{A} = \mathbb{F}$, $l(\mathcal{A}) = l(\mathbb{F}) = 0$ и требуемым порождающим элементом является единица.

Рассмотрим случай $n \geq 2$. Пусть $l(\mathcal{A}) = n - 1$. Рассмотрим систему порождающих $\mathcal{S}$ для $\mathcal{A}$ длины $l(\mathcal{S}) = l(\mathcal{A})$. Предположим, что $\dim \mathcal{L}_1(\mathcal{S}) \geq 3$. Тогда

$$\begin{aligned} \dim \mathcal{L}_{n-2}(\mathcal{S}) &= \dim \mathcal{L}_0(\mathcal{S}) + \sum_{k=1}^{n-2} (\dim \mathcal{L}_k(\mathcal{S}) - \dim \mathcal{L}_{k-1}(\mathcal{S})) \\ &= \dim \mathcal{L}_1(\mathcal{S}) + \sum_{k=2}^{n-2} (\dim \mathcal{L}_k(\mathcal{S}) - \dim \mathcal{L}_{k-1}(\mathcal{S})) \\ &\geq \dim \mathcal{L}_1(\mathcal{S}) + \sum_{k=2}^{n-2} 1 = \dim \mathcal{L}_1(\mathcal{S}) + n - 3 \geq n = \dim \mathcal{A}. \end{aligned}$$

Поэтому $\mathcal{L}_{n-2}(\mathcal{S}) = \mathcal{A}$ и $l(\mathcal{S}) \leq n - 2$. Получаем противоречие.

Если $\dim \mathcal{L}_1(\mathcal{S}) = 1$, то $\dim \mathcal{L}_0(\mathcal{S}) = \dim \mathcal{L}_1(\mathcal{S})$ и $l(\mathcal{S}) = 0 < n - 1$. Следовательно, $\dim \mathcal{L}_1(\mathcal{S}) = 2$, т.е. существует элемент $A \in \mathcal{S}$ такой, что $\mathcal{L}_1(\mathcal{S}) = \langle 1_{\mathcal{A}}, A \rangle$. Тогда по определению длины

$$\dim \mathcal{A} = n = \dim \mathcal{L}_{n-1}(\mathcal{S}) = \dim \langle 1_{\mathcal{A}}, A, A^2, \dots, A^{n-1} \rangle.$$

Следовательно, $\deg A = \dim \mathcal{A}$ и алгебра $\mathcal{A}$ порождена элементом A .

ТЕОРЕМА 5.4. Пусть $\mathbb{F}$ – произвольное поле.

1. Если $\mathbb{F}$ – бесконечно, то $l(D_n(\mathbb{F})) = n - 1$.

$$2. l(D_n(\mathbb{F}_q)) = \begin{cases} n - 1 & \text{при } q \geq n, \\ (q - 1)[\log_q n] + [q^{\{\log_q n\}}] - 1 & \text{при } q < n. \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Заметим, что если поле $\mathbb{F}$ бесконечно, то $m(D_n(\mathbb{F})) = n = \dim D_n(\mathbb{F})$ и утверждение 1 теоремы следует из леммы 5.3.

Пусть $\mathbb{F} = \mathbb{F}_q$. В этом случае $\dim D_n(\mathbb{F}_q) = n$ и $m(D_n(\mathbb{F}_q)) = \min(n, q)$. Также $g(n, n) = n - 1$ и $g(n, q) = (q - 1)[\log_q n] + [q^{\{\log_q n\}}] - 1$ при $q < n$.

Верхняя оценка

$$l(D_n(\mathbb{F}_q)) \leq g(\dim D_n(\mathbb{F}_q), m(D_n(\mathbb{F}_q)))$$

следует из теоремы 3.11.

Докажем нижнюю оценку $l(D_n(\mathbb{F}_q)) \geq g(n, \min(n, q))$ индукцией по n .

База индукции. При $n = 1, \dots, q$ утверждение следует из леммы 5.3.

Шаг индукции. Допустим, что $n > q$ и для всех $n' < n$ утверждение доказано. Заметим, что для любых $a, b \in \mathbb{N}$ верно

$$D_{ab}(\mathbb{F}) \cong D_a(\mathbb{F}) \otimes_{\mathbb{F}} D_b(\mathbb{F}), \quad D_{a+b}(\mathbb{F}) \cong D_a(\mathbb{F}) \oplus D_b(\mathbb{F}). \quad (23)$$

Тогда по теореме 5.2 для любых $t > s$ получаем

$$\begin{aligned} l(D_t(\mathbb{F})) &= l(D_{s+(t-s)}(\mathbb{F})) = l(D_s(\mathbb{F}) \oplus D_{t-s}(\mathbb{F})) \\ &\geq \max\{l(D_s(\mathbb{F})), l(D_{t-s}(\mathbb{F}))\} \geq l(D_s(\mathbb{F})). \end{aligned} \quad (24)$$

1) Пусть $n = q^l$, $l \geq 2$. Из равенства (23) и леммы 5.1 получаем

$$l(D_{q^l}(\mathbb{F}_q)) = l(D_q(\mathbb{F}_q) \otimes D_{q^{l-1}}(\mathbb{F}_q)) \geq l(D_q(\mathbb{F}_q)) + l(D_{q^{l-1}}(\mathbb{F}_q)). \quad (25)$$

Тогда, используя предположение индукции и равенство (4), заключаем, что

$$l(D_q(\mathbb{F}_q)) + l(D_{q^{l-1}}(\mathbb{F}_q)) \geq g(q, q) + g(q^{l-1}, q) = g(q^l, q).$$

2) Пусть $n = kq^l$, где $2 \leq k \leq q-1$, $l \geq 1$. Из равенств (5) и (23), неравенства (25) и леммы 5.1 получаем оценку

$$\begin{aligned} l(D_{kq^l}(\mathbb{F}_q)) &= l(D_k(\mathbb{F}_q) \otimes D_{q^l}(\mathbb{F}_q)) \geq l(D_k(\mathbb{F}_q)) + l(D_{q^l}(\mathbb{F}_q)) \\ &\geq g(k, k) + g(q^l, q) = g(kq^l, q). \end{aligned} \quad (26)$$

3) Пусть $n = kq^l + r$, где $0 < r < q^l$, $1 \leq k \leq q-1$, $l \geq 1$. Используя равенство (6), неравенства (24) и (26), получаем

$$l(D_{kq^l+r}(\mathbb{F}_q)) \geq l(D_{kq^l}(\mathbb{F}_q)) \geq g(kq^l, q) = g(kq^l + r, q).$$

СЛЕДСТВИЕ 5.5. *Верхняя оценка длины коммутативной алгебры в теореме 3.11 является точной.*

С другой стороны, в следующем примере будет показано, что существует коммутативная $\mathbb{F}$ -алгебра $\mathcal{A}$ произвольной размерности $\dim \mathcal{A} \geq 4$, для которой $l(\mathcal{A}) < g(\dim \mathcal{A}, m(\mathcal{A}))$.

ПРИМЕР 5.6. Пусть $\mathbb{F}$ – произвольное поле. Рассмотрим подалгебру $\mathcal{A}_1 \subseteq M_n(\mathbb{F})$, $n \geq 2$, состоящую из всех матриц вида

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{11} & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & a_{11} \end{pmatrix}.$$

В [7; пример 2] и [8; пример 7.2] доказано, что $\mathcal{A}_1$ – максимальная коммутативная подалгебра в $M_n(\mathbb{F})$, $\dim \mathcal{A}_1 = n$, $m(\mathcal{A}_1) = 2$ и $l(\mathcal{A}_1) = 1$.

Следовательно, при $n \geq 4$ получаем, что

$$l(\mathcal{A}_1) = 1 < [\log_2 n] = g(n, 2) = g(\dim \mathcal{A}_1, m(\mathcal{A}_1)).$$

Автор выражает особую благодарность своему научному руководителю А. Э. Гутерману за внимание к работе и полезные обсуждения.

Список литературы

- [1] A. Paz, “An application of the Cayley–Hamilton theorem to matrix polynomials in several variables”, *Linear and Multilinear Algebra*, **15:2** (1984), 161–170.
- [2] A. J. M. Spencer, R. S. Rivlin, “The theory of matrix polynomials and its application to the mechanics of isotropic continua”, *Arch. Rational Mech. Anal.*, **2:1** (1958), 309–336.

- [3] A. J. M. Spencer, R. S. Rivlin, “Further results in the theory of matrix polynomials”, *Arch. Rational Mech. Anal.*, **4**:1 (1959), 214–230.
- [4] Ch. J. Pappacena, “An upper bound for the length of a finite-dimensional algebra”, *J. Algebra*, **197**:2 (1997), 535–545.
- [5] D. Constantine, M. Darnall, “Lengths of finite dimensional representations of PBW algebras”, *Linear Algebra Appl.*, **395** (2005), 175–181.
- [6] О. В. Маркова, “О длине алгебры верхнетреугольных матриц”, *УМН*, **60**:5 (2005), 177–178; англ. пер.: O. V. Markova, “On the length of the algebra of upper-triangular matrices”, *Russian Math. Surveys*, **60**:5 (2005), 984–985.
- [7] W. C. Brown, F. W. Call, “Maximal commutative subalgebras of $n \times n$ matrices”, *Comm. Algebra*, **21**:12 (1993), 4439–4460.
- [8] О. В. Маркова, “Вычисление длин матричных подалгебр специального вида”, *Фундамент. и прикл. матем.*, **13**:4 (2007), 165–197; англ. пер.: O. V. Markova, “Length computation of matrix subalgebras of special type”, *J. Math. Sci. (N. Y.)*, **155**:6 (2008), 908–931.

О. В. Маркова (O. V. Markova)

Механико-математический факультет Московского
государственного университета им. М. В. Ломоносова
E-mail: ov_markova@mail.ru

Поступила в редакцию
28.01.2009