Функция длины и матричные алгебры*

О. В. МАРКОВА
Московский государственный университет
им. М. В. Ломоносова
e-mail: ov_markova@mail.ru

УДК 512.552+512.643

Ключевые слова: функция длины, матричные подалгебры, коммутативные алгебры.

Аннотация

Длиной конечной системы порождающих конечномерной ассоциативной алгебры над произвольным полем называется наименьшее натуральное число k, такое что слова длины, не большей k, порождают данную алгебру как векторное пространство. Длиной алгебры называется максимум длин её систем порождающих. В настоящей работе исследованы основные теоретико-кольцевые свойства функции длины: поведение длины при присоединение единицы к алгебре, при взятии прямой суммы алгебр, при переходе к подалгебрам, при гомоморфизмах. Получена верхняя оценка длины алгебры как функция индекса нильпотентности её радикала Джекобсона и размерности фактора по радикалу. Также вычислены функции длины отдельных алгебр, в частности следующих классических матричных подалгебр: алгебры верхнетреугольных матриц, алгебры диагональных матриц, алгебры Шура, алгебры Куртера и классов алгебр: локальных, коммутативных.

Abstract

O. V. Markova, The length function and matrix algebras, Fundamentalnaya i prikladnaya matematika, vol. 17 (2011/2012), no. 6, pp. 65—173.

By the length of a finite system of generators for a finite-dimensional associative algebra over an arbitrary field we mean the least positive integer k such that the words of length not exceeding k span this algebra (as a vector space). The maximum length for the systems of generators of an algebra is referred to as the length of the algebra. In the present paper, we study the main ring-theoretical properties of the length function: the behavior of the length under unity adjunction, direct sum of algebras, passing to subalgebras and homomorphic images. We give an upper bound for the length of the algebra as a function of the nilpotency index of its Jacobson radical and the length of the quotient algebra. We also provide examples of the length computation for certain algebras, in particular, for the following classical matrix subalgebras: the algebra of upper triangular matrices, the algebra of diagonal matrices, the Schur algebra, Courter's algebra, and for the classes of local and commutative algebras.

*Работа выполнена при финансовой поддержке грантом МД-2502.2012.1 и грантом РФФИ 12-01-00140-а.

Фундаментальная и прикладная математика, 2011/2012, том 17, № 6, с. 65—173.

1. Введение

Классическим направлением исследований в теории матриц является изучение различных числовых характеристик матричных подалгебр. Для функции размерности эти исследования восходят к работе И. Шура 1905 г. [32], в которой получена верхняя оценка размерности $[n^2/4]+1$ коммутативных подалгебр алгебры матриц порядка n над полем комплексных чисел, где $[x]$ обозначает наибольшее целое число, не превосходящее x. Эта область активно развивается в течение XX века, достаточно упомянуть работу Н. Джекобсона 1944 г. [22], в которой оценка И. Шура была перенесена на случай произвольного поля, статью М. Герштенхабера 1961 г. [19], в которой получена оценка размерности коммутативной алгебры, порождённой двумя матрицами, работу А. Паза 1984 г. [30], результаты которого описаны ниже, монографию Д. А. Супруненко и Р. И. Тышкевич 1966 г. [12], а также работы [16, 18, 23, 25, 33, 36].

Важную роль в изучении конечномерных алгебр играет такой инвариант алгебры, как длина (длина понимается в смысле определения 2.11). Задача вычисления длины впервые возникла в работах А. Спенсера и Р. Ривлина 1959—1960 гг. [34, 35] для полной алгебры матриц порядка 3 в связи с возможным применением в механике сплошных сред. В общей формулировке проблема вычисления длины полной алгебры матриц $\mathrm{M}_n(\mathbb{F})$ как функции порядка матриц была поставлена А. Пазом в 1984 году в работе [30] и до сих пор является открытой. Существует гипотеза, состоящая в том, что зависимость между длиной и порядком матриц линейная и задаётся следующей формулой.

Гипотеза 1.1 [30]. Пусть $\mathbb{F}$ — произвольное поле. Тогда $l\big(\mathrm{M}_n(\mathbb{F})\big)=2n-2$.

Известно, что эта гипотеза верна при $n=2,3,4$ (см. [30, пример]). Однако существующие верхние оценки длины алгебры матриц не являются линейными.

Оценка, полученная в работе А. Паза, является квадратичной относительно порядка матриц.

Теорема 1.2 [30, теорема 1, замечание 1]. *Пусть $\mathbb{F}$ — произвольное поле. Тогда*

$$l\big(\mathrm{M}_n(\mathbb{F})\big)\leqslant\left\lceil\frac{n^2+2}{3}\right\rceil,$$

где $\lceil\cdot\rceil$ обозначает наименьшее целое число, большее или равное данному.

В работе 1997 г. [29] К. Паппачена предложил обобщение метода комбинаторного подсчёта линейно независимых слов, использованного А. Пазом и с его помощью получил верхнюю оценку длины произвольной ассоциативной алгебры $\mathcal{A}$ как функцию двух её инвариантов: размерности и максимальной степени минимального многочлена элементов алгебры $m(\mathcal{A})$.

Теорема 1.3 [29, теорема 3.1]. *Пусть $\mathbb{F}$ — произвольное поле, и пусть*

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

Тогда

$$l(\mathcal{A}) < f\big(\dim \mathcal{A}, m(\mathcal{A})\big).$$

Для матричной алгебры эта теорема даёт верхнюю оценку асимптотики $O(n^{3/2})$.

Теорема 1.4 [29, следствие 3.2]. *Пусть* $\mathbb{F}$ — *произвольное поле. Тогда*

$$l\big(\mathrm{M}_n(\mathbb{F})\big) < n\sqrt{\frac{2n^2}{n-1}+\frac{1}{4}}+\frac{n}{2}-2.$$

Некоторые системы порождающих, длины которых не превосходят $2n-2$, рассмотрены в [17, 26, 27]. Пример системы порождающих длины $2n-2$ в случае, когда основное поле является алгебраически замкнутым характеристики 0, построен в [24, раздел 4].

В работе А. Паза [30, теорема 2] также было доказано, что верхняя оценка длины коммутативной матричной подалгебры над полем комплексных чисел $\mathbb{C}$ равна $n-1$, т. е. для коммутативных подалгебр получена линейная относительно порядка матриц точная верхняя оценка длины.

Приложения разрабатываемой теории возникают в следующем классе задач вычислительных методов теории матриц (см., например, [1, 15]): рассматривается подалгебра в полной алгебре матриц $\mathrm{M}_n(\mathbb{F})$ порядка n над полем $\mathbb{F}$ (обычно полем комплексных или действительных чисел), заданная порождающим множеством $A_1, \ldots, A_k$, и требуется проверить, обладает ли данная алгебра некоторым заданным свойством. При этом процедура проверки должна быть *рациональной*, т. е. использующей конечное число арифметических операций с элементами матриц. Такие процедуры, как правило, включают в себя рациональную процедуру вычисления базиса алгебры. Длина порождающего множества $A_1, \ldots, A_k$ ограничивает сверху число матриц, участвующих в рассматриваемых произведениях матриц, т. е. является мерой сложности этой процедуры. Также длина определяет сложность рациональной процедуры проверки, является ли некоторое множество системой порождающих для заданной алгебры.

Отметим, что в ряде вычислительных задач требуется оценить длину произвольного подмножества $\mathcal{S}'$ в алгебре $\mathcal{A}$, которое может порождать не всю алгебру, а её собственную подалгебру $\mathcal{A}' \subset \mathcal{A}$, или найти такое число $M \in \mathbb{N}$, что для любой подалгебры $\mathcal{A}' \subseteq \mathcal{A}$ будет справедлива оценка $l(\mathcal{A}') \leqslant M$. Ввиду тривиальной оценки длины $l(\mathcal{A}') \leqslant \dim \mathcal{A}' - 1$ всегда можно положить $M = \dim \mathcal{A} - 1$. Однако, как показывает, например, оценка в теореме 1.4, тривиальная оценка может не быть точной.

Таким образом, вопросы, связанные с вычислением и оцениванием длин различных матричных подалгебр, мотивированы приложениями и активно разрабатываются. Поэтому построение общей теории функции длины представляет не только самостоятельный теоретический интерес, но и является эффективным инструментом работы с различными классами вычислительных задач в прикладной и теоретической алгебре.

Цель настоящей работы — изучение основных алгебраических свойств функции длины и применение этих результатов к вычислению или оцениванию длин классических матричных подалгебр.

Раздел 3 посвящён изучению основных теоретико-кольцевых свойств функции длины.

В разделе 3.1 показано, что длина системы порождающих не меняется при обратимых линейных заменах этой системы.

В разделе 3.2 показано, что длина алгебры не меняется при присоединении к алгебре внешней единицы.

В разделе 3.3 получены точные оценки длины прямой суммы алгебр. В качестве следствия вычислена длина алгебры верхнетреугольных матриц, найдены оценки для длин подалгебр данной алгебры.

Основной результат раздела 3.5 заключается в том, что длина алгебры не уменьшается при переходе к алгебраическому расширению основного поля. Построен пример строгого возрастания длины алгебры при переходе к алгебраическому замыканию поля.

В разделе 3.6 исследуется поведение длины при переходе от алгебры к её фактор-алгебрам.

В разделе 3.8 длина произвольной конечномерной алгебры оценена сверху функцией от индекса нильпотентности её радикала Джекобсона и длины фактор-алгебры по радикалу.

В разделе 4 исследуется длина коммутативных алгебр. Получено обобщение результата А. Паза о длине коммутативных матричных подалгебр на случай произвольного поля. Показана точность этой оценки. Более того, охарактеризован класс коммутативных матричных подалгебр длины $n-1$ в терминах порождающих элементов. Как следствие установлено, что максимальные по длине коммутативные подалгебры в $\mathrm{M}_n(\mathbb{F})$ являются также максимальными по включению.

В разделе 4.2 приведены примеры вычисления длин таких классических коммутативных матричных подалгебр, как алгебра Шура, алгебра Куртера и др. Эти примеры также показывают, что длины максимальных по включению коммутативных подалгебр в $\mathrm{M}_n(\mathbb{F})$ могут принимать любое натуральное значение в отрезке от 1 до $n-1$, т. е. максимальные по включению коммутативные подалгебры не обязательно имеют максимальную длину.

В разделе 4.4 получена точная верхняя оценка длины коммутативной алгебры как функция таких инвариантов алгебры, как размерность алгебры и максимальная степень минимального многочлена элементов алгебры. Эта оценка существенно сильнее общей оценки К. Паппачены из теоремы 1.3: в последнюю входит квадратный корень из размерности алгебры, а в полученную автором — логарифм размерности.

Раздел 5 посвящён изучению вопроса о связи длины подалгебры с длиной содержащей её алгебры. В алгебре матриц любого порядка, превышающего 3, построены примеры, показывающие, что функция длины может расти при переходе к подалгебрам. Для матричных подалгебр порядков 2 и 3 установлено, что длина подалгебры не превосходит длины содержащей её алгебры.

Полностью решён вопрос о возможных значениях разности длины подалгебры и длины содержащей её алгебры: показано, что длина подалгебры может превышать длину содержащей её алгебры на любое натуральное число.

Рассмотрены специальные конструкции двух- и трёхблочных верхнетреугольных матричных подалгебр. Заметим, что до настоящего времени существовало не много примеров алгебр с явно вычисленной длиной, поэтому вычисление длин подалгебр данного вида представляет непосредственный интерес. Помимо этого, представленные конструкции дают пример того, что отношение длины подалгебры к длине алгебры может быть любым рациональным числом из отрезка $[1, 2]$.

Некоторые из этих результатов с другими доказательствами содержатся в работах автора [6—10, 20].

2. Основные определения и обозначения

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 *конечно порождённой*, если в ней существует такое конечное подмножество $\mathcal{S} = \{a_1, \ldots, a_k\}$, называемое *системой порождающих*, что каждый элемент алгебры является линейной комбинацией конечного числа произведений элементов из $\mathcal{S}$; пустое произведение равно единичному элементу. Легко убедиться, что любая конечномерная алгебра порождается своим базисом, т. е. является конечно порождённой. Понятия теории колец и алгебр, использованные в статье, можно найти, например, в [11].

Важную роль в изучении конечномерных алгебр играет такой инвариант алгебры, как *длина*, определим её согласно [29].

Обозначение 2.1. Через $\langle S \rangle$ будем обозначать линейную оболочку (множество всех конечных линейных комбинаций с коэффициентами из $\mathbb{F}$) подмножества S некоторого векторного пространства над $\mathbb{F}$.

Обозначение 2.2. Пусть $B = \{b_1, \ldots, b_m\}$ — непустое конечное множество (алфавит). Конечные последовательности букв из B назовём словами. Пусть B^* обозначает множество всех слов в алфавите B, F_B — свободную полугруппу над алфавитом B, т. е. B^* с операцией конкатенации.

Определение 2.3. *Длина* слова $b_{i_1} \cdots b_{i_t}$, где $b_{i_j} \in B$, равна t. Будем считать 1 (пустое слово) словом от элементов B *длины* 0.

Обозначение 2.4. Пусть B^i обозначает множество всех слов в алфавите B длины, не большей i, $i \geqslant 0$. Тогда через $B^i \setminus B^{i-1}$ обозначим множество всех слов в алфавите B длины, равной i, $i \geqslant 1$.

Замечание 2.5. Произведения элементов из порождающего множества $\mathcal{S}$ можно рассматривать как образы элементов свободной полугруппы $F_{\mathcal{S}}$ при естественном гомоморфизме, их также можно называть словами от образующих и использовать естественные обозначения $\mathcal{S}^i$ и $\mathcal{S}^i \setminus \mathcal{S}^{i-1}$.

Обозначение 2.6. Положим $\mathcal{S}^0 = \{1_{\mathcal{A}}\}$, если алгебра $\mathcal{A}$ содержит единицу $1_{\mathcal{A}}$, иначе положим $\mathcal{S}^0 = \varnothing$.

Обозначение 2.7. Обозначим через $\mathcal{L}_i(\mathcal{S})$ линейную оболочку слов из $\mathcal{S}^i$. Заметим, что $\mathcal{L}_0(\mathcal{S}) = \langle 1_{\mathcal{A}} \rangle = \mathbb{F}$ для алгебр с единицей и $\mathcal{L}_0(\mathcal{S}) = 0$ иначе. Пусть также $\mathcal{L}(\mathcal{S}) = \bigcup\limits_{i=0}^{\infty} \mathcal{L}_i(\mathcal{S})$ обозначает линейную оболочку всех слов в алфавите $\{a_1, \ldots, a_k\}$.

Замечание 2.8. Так как $\mathcal{S}$ является системой порождающих для $\mathcal{A}$, то $\mathcal{A} = \mathcal{L}(\mathcal{S})$. Из определения $\mathcal{S}^i$ для $i, j > 0$ получаем, что

$$\mathcal{S}^{i+j} = \mathcal{S}^i \mathcal{S}^j \cup \mathcal{S}^1, \tag{2.1}$$

$$\mathcal{L}_{i+j}(\mathcal{S}) = \langle \mathcal{L}_i(\mathcal{S}) \mathcal{L}_j(\mathcal{S}) + \mathcal{L}_1(\mathcal{S}) \rangle \tag{2.2}$$

и

$$\mathcal{L}_0(\mathcal{S}) \subseteq \mathcal{L}_1(\mathcal{S}) \subseteq \ldots \subseteq \mathcal{L}_h(\mathcal{S}) \subseteq \ldots \subseteq \mathcal{L}(\mathcal{S}) = \mathcal{A}. \tag{2.3}$$

В дальнейшем все рассматриваемые алгебры имеют конечную размерность.

Определение 2.9. *Длиной системы порождающих* $\mathcal{S}$ алгебры $\mathcal{A}$ называется наименьшее неотрицательное целое число k, для которого $\mathcal{L}_k(\mathcal{S}) = \mathcal{A}$. Обозначим длину системы порождающих $\mathcal{S}$ через $l(\mathcal{S})$.

Замечание 2.10. В случае алгебр с единицей равенства (2.1) и (2.2) можно упростить:

$$\mathcal{S}^{i+j} = \mathcal{S}^i \mathcal{S}^j, \tag{2.4}$$

$$\mathcal{L}_{i+j}(\mathcal{S}) = \langle \mathcal{L}_i(\mathcal{S}) \mathcal{L}_j(\mathcal{S}) \rangle. \tag{2.5}$$

Определение 2.11. *Длиной алгебры* $\mathcal{A}$ называется число $l(\mathcal{A}) = \max\limits_{\mathcal{S}} l(\mathcal{S})$, где максимум берётся по всем системам порождающих этой алгебры.

Определение 2.12. Слово $v \in \mathcal{S}^j \setminus \mathcal{S}^{j-1}$ 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).

Определение 2.13. Слово $v \in \mathcal{S}^j$ называется *несократимым над* $\mathcal{S}$, если оно не является сократимым.

Определение 2.14. Назовём слова $v = a_{i_1} a_{i_2} \cdots a_{i_p},\ w = a_{j_1} a_{j_2} \cdots a_{j_q} \in \mathcal{S}^*$ *формально равными*, если $p = q$ и для каждого $1 \leqslant s \leqslant p$ выполнено $i_s = j_s$; в противном случае назовём эти слова *формально различными*.

Обозначение 2.15. Пусть $j \in \{1, \ldots, k\}$ и $v \in \mathcal{S}^*$. Через $\#_j(v)$ обозначим число вхождений буквы a_j в слово v.

Обозначение 2.16. Пусть $I \colon \mathcal{S}^* \to \mathbb{Z}_+^k$ обозначает отображение, ставящее в соответствие слову $v \in \mathcal{S}^*$ строку $\big(\#_1(v), \ldots, \#_k(v)\big)$.

Предложение 2.17. *Отображение I порождает отношение эквивалентности $\wp_I$ на множестве $\mathcal{S}^*$:*

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

Пусть

$$\wp_I(v) = \{w \in \mathcal{S}^* \mid (v, w) \in \wp_I\} \text{ —}$$

класс эквивалентности слова $v \in \mathcal{S}^*$.

Доказательство. Проверим, что отношение $\wp_I$ является эквивалентностью. Действительно, для любого $v \in \mathcal{S}^*$ верно равенство $I(v) = I(v)$, поэтому $(v, v) \in \wp_I$. Для любых $v, w \in \mathcal{S}^*$ равенство $I(v) = I(w)$ симметрично, поэтому $(v, w) \in \wp_I$ тогда и только тогда, когда $(w, v) \in \wp_I$. Если $(u, v) \in \wp_I$ и $(v, w) \in \wp_I$, то $I(u) = I(v)$, $I(v) = I(w)$, следовательно, $I(u) = I(w)$, и $(u, w) \in \wp_I$. □

Обозначение 2.18. Для каждого $v \in \mathcal{S}^*$ существует подстановка $\varphi_v \in \mathrm{S}_k$, упорядочивающая координаты вектора $I(v)$, т. е.

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

Через $I_0 \colon \mathcal{S}^* \to \mathbb{Z}_+^k$ обозначим отображение, ставящее в соответствие слову $v \in \mathcal{S}^*$ упорядоченную строку $(x_1, \ldots, x_k)$.

Предложение 2.19. *Отображение I_0 порождает отношение эквивалентности $\wp_{I_0}$ на множестве $\mathcal{S}^*$:*

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

Пусть

$$\wp_{I_0}(v) = \{w \in \mathcal{S}^* \mid (v, w) \in \wp_{I_0}\} \text{ —}$$

класс эквивалентности слова $v \in \mathcal{S}^*$.

Доказательство. Доказательство аналогично доказательству предложения 2.17. □

Определение 2.20. *Лексикографическим порядком* на числовых наборах из $\mathbb{Z}_+^k$ мы будем называть порядок, при котором набор $X = (x_1, \ldots, x_k)$ предшествует набору $Y = (y_1, \ldots, y_k)$, если для некоторого $s \in \{0, \ldots, k-1\}$ и для всех $i = 1, \ldots, s$ выполнено $x_i = y_i$ и $x_{s+1} < y_{s+1}$. Обозначим это как $X \overset{\mathrm{lex}}{<} Y$.

Замечание 2.21. 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. В дальнейшем будем использовать следующее обозначение:

$$v \overset{I_0}{\leqslant} w \iff \forall\, v, w \in \mathcal{S}^*\ I_0(v) \overset{\mathrm{lex}}{\leqslant} I_0(w).$$

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

Обозначение 2.22. 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 положим

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

Обозначение 2.23. Обозначим через $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_+$ множества натуральных, целых, неотрицательных целых чисел соответственно. Через $\mathbb{R}$ и $\mathbb{C}$ обозначим поля действительных и комплексных чисел, через $\mathbb{F}_q$ — конечное поле мощности q.

Обозначение 2.24. Пусть $x \in \mathbb{R}$. Через $[x]$ будем обозначать целую часть числа x, т. е. наибольшее целое число, не превосходящее x. Через $\lceil x \rceil$ будем обозначать наименьшее целое число z, такое что $z \geqslant x$. Через $\{x\}$ будем обозначать дробную часть числа x, т. е. $\{x\} = x - [x]$.

Обозначение 2.25. Обозначим через $\mathrm{M}_{m,n}(\mathbb{F})$ линейное пространство матриц размера $m \times n$ над полем $\mathbb{F}$, через $\mathrm{M}_n(\mathbb{F})$ — алгебру матриц порядка n над полем $\mathbb{F}$, через $\mathrm{T}_n(\mathbb{F})$ — алгебру верхнетреугольных матриц порядка n над полем $\mathbb{F}$, через $\mathrm{D}_n(\mathbb{F})$ — алгебру диагональных матриц порядка n над полем $\mathbb{F}$, через $\mathrm{N}_n(\mathbb{F})$ — подалгебру нильпотентных матриц в $\mathrm{T}_n(\mathbb{F})$, через E, E_n — единичную матрицу в $\mathrm{M}_n(\mathbb{F})$, через O, O_n, $O_{m\times n}$ — нулевые матрицы в $\mathrm{M}_n(\mathbb{F})$ и $\mathrm{M}_{m,n}(\mathbb{F})$ соответственно, через $E_{i,j}$ — (i,j)-ю матричную единицу, т. е. матрицу с 1 на (i,j)-м месте и 0 на остальных.

3. Базовые алгебраические свойства функции длины

3.1. Поведение длины системы образующих при преобразованиях этой системы

В данном разделе приведены примеры преобразований систем порождающих, сохраняющих длину. В частности, показано, что длина системы порождающих не меняется при обратимых линейных заменах этой системы.

Предложение 3.1. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — конечномерная алгебра над $\mathbb{F}$. Если $\mathcal{S} = \{a_1, \ldots, a_k\}$ — система порождающих этой алгебры и $C = \{c_{i,j}\} \in \mathrm{M}_k(\mathbb{F})$ — невырожденная матрица, то множество координат вектора*

$$C \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix} = \begin{pmatrix} c_{1,1}a_1 + c_{1,2}a_2 + \ldots + c_{1,k}a_k \\ \vdots \\ c_{k,1}a_1 + c_{k,2}a_2 + \ldots + c_{k,k}a_k \end{pmatrix}, \tag{3.1}$$

т. е. множество

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

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

Доказательство. Докажем равенство $\mathcal{L}_n(\mathcal{S}) = \mathcal{L}_n(\mathcal{S}_c)$ индукцией по n.

База индукции. При $n = 0$ утверждение верно по определению. Пусть $n = 1$. По определению любая линейная комбинация $\gamma_1 a_1 + \ldots + \gamma_k a_k$, $\gamma_1, \ldots, \gamma_k \in \mathbb{F}$, принадлежит $\mathcal{L}_1(\mathcal{S})$. Следовательно, $\mathcal{L}_1(\mathcal{S}_c) \subseteq \mathcal{L}_1(\mathcal{S})$. Из невырожденности матрицы C следует, что существует обратная матрица $C^{-1} = (d_{i,j})$. Тогда в силу соотношения (3.1)

$$a_i = (d_{i,1}, d_{i,2}, \ldots, d_{i,k}) \begin{pmatrix} c_{1,1}a_1 + c_{1,2}a_2 + \ldots + c_{1,k}a_k \\ \vdots \\ c_{k,1}a_1 + c_{k,2}a_2 + \ldots + c_{k,k}a_k \end{pmatrix} \in \mathcal{L}_1(\mathcal{S}_c)$$

для всех $i = 1, \ldots, k$ по определению линейной оболочки. Следовательно, $\mathcal{L}_1(\mathcal{S}) \subseteq \mathcal{L}_1(\mathcal{S}_c)$. А значит, $\mathcal{L}_1(\mathcal{S}_c) = \mathcal{L}_1(\mathcal{S})$.

Шаг индукции. Допустим, что $n > 1$ и для всех $m < n$ утверждение доказано. Тогда с учётом равенства (2.2) получаем

$$\mathcal{L}_n(\mathcal{S}) = \langle \mathcal{L}_1(\mathcal{S})\mathcal{L}_{n-1}(\mathcal{S}) + \mathcal{L}_1(\mathcal{S}) \rangle = \langle \mathcal{L}_1(\mathcal{S}_c)\mathcal{L}_{n-1}(\mathcal{S}_c) + \mathcal{L}_1(\mathcal{S}_c) \rangle = \mathcal{L}_n(\mathcal{S}_c). \quad \square$$

Предложение 3.2. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — конечномерная алгебра с единицей над $\mathbb{F}$. Пусть $\mathcal{S} = \{a_1, \ldots, a_k\}$ — система порождающих этой алгебры, такая что $1_\mathcal{A} \notin \langle a_1, \ldots, a_k \rangle$. Тогда для любых $\gamma_1, \ldots, \gamma_k \in \mathbb{F}$ множество $\mathcal{S}_1 = \{a_1 + \gamma_1 1_\mathcal{A}, \ldots, a_k + \gamma_k 1_\mathcal{A}\}$ — система порождающих алгебры $\mathcal{A}$ и $l(\mathcal{S}_1) = l(\mathcal{S})$.*

Доказательство. Как и в предыдущем утверждении, докажем равенство $\mathcal{L}_n(\mathcal{S}) = \mathcal{L}_n(\mathcal{S}_1)$ для всех n, используя индукцию по n.

База индукции. Так как $1_\mathcal{A} \in \mathcal{L}_0(\mathcal{S}) = \mathcal{L}_0(\mathcal{S}_1)$, то $\mathcal{L}_1(\mathcal{S}_1) = \mathcal{L}_1(\mathcal{S})$.

Шаг индукции. Допустим, что $n > 1$ и для всех $m < n$ утверждение доказано. Тогда, пользуясь равенством (2.5), получаем

$$\mathcal{L}_n(\mathcal{S}) = \langle \mathcal{L}_1(\mathcal{S})\mathcal{L}_{n-1}(\mathcal{S}) \rangle = \langle \mathcal{L}_1(\mathcal{S}_1)\mathcal{L}_{n-1}(\mathcal{S}_1) \rangle = \mathcal{L}_n(\mathcal{S}_1). \quad \square$$

Предложение 3.3. *Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{A}$ — конечномерная $\mathbb{F}$-алгебра без единицы и $\mathcal{S} = \{a_1, \ldots, a_k\}$ — система порождающих для алгебры $\mathcal{A}$. Тогда существует система порождающих $\mathcal{S}'$ для $\mathcal{A}$, удовлетворяющая следующим условиям*:

1) $\mathcal{S}' \subseteq \mathcal{S}$;
2) $\dim \mathcal{L}_1(\mathcal{S}') = |\mathcal{S}'|$;
3) $l(\mathcal{S}') = l(\mathcal{S})$.

Доказательство. Для любой системы порождающих по определению выполнены равенства $\mathcal{L}_0(\mathcal{S}) = 0$ и $\mathcal{L}_1(\mathcal{S}) = \langle \mathcal{S} \rangle$. Пусть $a_{i_1}, \ldots, a_{i_m}$ — элементы $\mathcal{S}$, образующие базис $\langle \mathcal{S} \rangle$. Тогда положим $\mathcal{S}' = \{a_{i_1}, \ldots, a_{i_m}\}$. Получаем, что множество $\mathcal{S}'$ удовлетворяет условиям 1) и 2).

Как и в предыдущем утверждении, докажем равенство $\mathcal{L}_n(\mathcal{S}) = \mathcal{L}_n(\mathcal{S}')$ для всех n, используя индукцию по n.

База индукции. Поскольку $\mathcal{L}_0(\mathcal{S}) = 0 = \mathcal{L}_0(\mathcal{S}')$, то

$$\mathcal{L}_1(\mathcal{S}) = \langle \mathcal{S} \rangle = \langle \mathcal{S}' \rangle = \mathcal{L}_1(\mathcal{S}').$$

Шаг индукции. Допустим, что $n > 1$ и для всех $r < n$ утверждение доказано. Тогда, снова пользуясь равенством (2.2), получаем

$$\mathcal{L}_n(\mathcal{S}) = \langle \mathcal{L}_1(\mathcal{S})\mathcal{L}_{n-1}(\mathcal{S}) + \mathcal{L}_1(\mathcal{S}) \rangle = \langle \mathcal{L}_1(\mathcal{S}')\mathcal{L}_{n-1}(\mathcal{S}') + \mathcal{L}_1(\mathcal{S}') \rangle = \mathcal{L}_n(\mathcal{S}'),$$

следовательно, условие 3) также выполнено. □

Предложение 3.4. *Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{A}$ — конечномерная $\mathbb{F}$-алгебра с единицей $1_\mathcal{A}$ и $\mathcal{S} = \{a_1, \ldots, a_k\}$ — система порождающих для алгебры $\mathcal{A}$. Тогда существует система порождающих $\mathcal{S}'$ для $\mathcal{A}$, удовлетворяющая следующим условиям*:

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

Доказательство. Для любой системы порождающих по определению выполнены равенства $\mathcal{L}_0(\mathcal{S}) = \langle 1_\mathcal{A} \rangle$ и $\mathcal{L}_1(\mathcal{S}) = \langle \mathcal{S} \cup \{1_\mathcal{A}\} \rangle$. Рассмотрим множество $\mathcal{S}_1 = \{1_\mathcal{A}, a_1, a_2, \ldots, a_k\}$. Последовательно удаляя из $\mathcal{S}_1$ те элементы, которые линейно выражаются через элементы с меньшими значениями индексов, получаем множество $\mathcal{S}_2 = \{1_\mathcal{A}, a_{j_1}, a_{j_2}, \ldots, a_{j_m}\}$. По построению элементы из $\mathcal{S}_2$ образуют базис $\mathcal{L}_1(\mathcal{S})$. Положим $\mathcal{S}' = \mathcal{S}_2 \setminus \{1_\mathcal{A}\} = \{a_{j_1}, a_{j_2}, \ldots, a_{j_m}\}$. Получаем, что $1_\mathcal{A} \notin \langle \mathcal{S}' \rangle$ и

$$\mathcal{L}_1(\mathcal{S}) = \langle \mathcal{S} \cup \{1_\mathcal{A}\} \rangle = \langle \mathcal{S}' \cup \{1_\mathcal{A}\} \rangle = \langle \mathcal{S}' \rangle + \langle 1_\mathcal{A} \rangle = \langle \mathcal{S}' \rangle \oplus \langle 1_\mathcal{A} \rangle = \mathcal{L}_1(\mathcal{S}'). \quad (3.2)$$

Значит, условия 1)—3) выполнены.

Как и в предыдущем утверждении, докажем равенство $\mathcal{L}_n(\mathcal{S}) = \mathcal{L}_n(\mathcal{S}')$ для всех n, используя индукцию по n.

База индукции доказана в (3.2).

Шаг индукции. Допустим, что $n > 1$ и для всех $r < n$ утверждение доказано. Тогда воспользуемся равенством (2.5):

$$\mathcal{L}_n(\mathcal{S}) = \langle \mathcal{L}_1(\mathcal{S})\mathcal{L}_{n-1}(\mathcal{S}) \rangle = \langle \mathcal{L}_1(\mathcal{S}')\mathcal{L}_{n-1}(\mathcal{S}') \rangle = \mathcal{L}_n(\mathcal{S}'),$$

Как следствие, условие 4) также выполнено. □

Следствие 3.5. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — конечномерная $\mathbb{F}$-алгебра, возможно без единицы. Тогда без ограничения общности можно считать, что система порождающих алгебры $\mathcal{A}$ является линейно независимой системой элементов.*

3.2. Поведение длины при присоединении к алгебре единицы

В данном разделе показано, что длина алгебры не меняется при присоединении к ней внешней единицы.

Теорема 3.6. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — конечномерная алгебра без единицы над полем $\mathbb{F}$. Определим $\mathbb{F}$-алгебру $\mathcal{A}_1 = \mathcal{A} \oplus \mathbb{F}$ со следующими операциями*:

$$\begin{gathered}(a_1, f_1) + (a_2, f_2) = (a_1 + a_2, f_1 + f_2),\\ f_1(a, f_2) = (f_1 a, f_1 f_2),\\ (a_1, f_1)(a_2, f_2) = (a_1 a_2 + f_2 a_1 + f_1 a_2, f_1 f_2),\\ a, a_1, a_2 \in \mathcal{A}, \quad f_1, f_2 \in \mathbb{F}.\end{gathered}$$

Тогда $\mathcal{A}_1$ — конечномерная $\mathbb{F}$-алгебра с единичным элементом $(0, 1)$ и $l(\mathcal{A}) = l(\mathcal{A}_1)$.

Доказательство. Из построения видно, что $\mathcal{A}_1$ является $\mathbb{F}$-алгеброй, её конечномерность следует из равенства $\dim_{\mathbb{F}} \mathcal{A}_1 = \dim_{\mathbb{F}} \mathcal{A} + 1$.

Элемент $(0, 1)$ является единицей в алгебре $\mathcal{A}_1$, поскольку для любых $a \in \mathcal{A}$, $f \in \mathbb{F}$ выполнено

$$\begin{gathered}(a, f)(0, 1) = (a0 + f0 + 1a, f1) = (a, f),\\ (0, 1)(a, f) = (0a + 1a + f0, 1f) = (a, f).\end{gathered}$$

Теперь докажем равенство длин $l(\mathcal{A}) = l(\mathcal{A}_1)$.

1. Сначала докажем оценку $l(\mathcal{A}_1) \leqslant l(\mathcal{A})$. Для этого возьмём в $\mathcal{A}_1$ систему порождающих $\mathcal{S}_1 = \{b_1, \ldots, b_k\}$ длины $l(\mathcal{S}_1) = l(\mathcal{A}_1)$. По определению каждый b_i имеет вид (a_i, f_i), где $a_i \in \mathcal{A}$ и $f_i \in \mathbb{F}$, $i = 1, \ldots, k$. Согласно предложению 3.4 можно считать, что $\dim \mathcal{L}_1(\mathcal{S}_1) = |\mathcal{S}_1| + 1 = k + 1$. Тогда по предложению 3.2 множество $\mathcal{S}_0 = \{(a_1, 0), \ldots, (a_k, 0)\}$ будет системой порождающих для $\mathcal{A}_1$, $l(\mathcal{S}_1) = l(\mathcal{S}_0)$ и $\dim \mathcal{L}_1(\mathcal{S}_0) = \dim \mathcal{L}_1(\mathcal{S}_1) = k + 1$, т. е. элементы $a_1, \ldots, a_k$ линейно независимы в $\mathcal{A}$. Обозначим $\mathcal{S} = \{a_1, \ldots, a_k\}$. Получаем, что для любого $m \geqslant 1$

$$\mathcal{L}_m(\mathcal{S}) = \langle \mathcal{S}^m \rangle \cong \langle \{(v, 0),\ v \in \mathcal{S}^m\} = \langle \mathcal{S}_0^m \setminus \mathcal{S}_0^0 \rangle. \tag{3.3}$$

По условию на $\mathcal{S}_0$

$$\mathcal{L}_m(\mathcal{S}_0) = \langle \mathcal{S}_0^m \setminus \mathcal{S}_0^0 \rangle \oplus \langle \mathcal{S}_0^0 \rangle. \tag{3.4}$$

Следовательно, для любого $m \geqslant 1$

$$\dim \mathcal{L}_m(\mathcal{S}_0) = \dim \mathcal{L}_m(\mathcal{S}) + 1. \tag{3.5}$$

При $m = l(\mathcal{S}_1)$ получаем, что

$$\dim \mathcal{L}_m(\mathcal{S}) = \dim \mathcal{L}_m(\mathcal{S}_0) - 1 = \dim \mathcal{A}_1 - 1 = \dim \mathcal{A}.$$

Значит, множество $\mathcal{S}$ является системой порождающих для $\mathcal{A}$, и из равенства размерностей получаем, что

$$l(\mathcal{A}_1) = l(\mathcal{S}_0) = l(\mathcal{S}) \leqslant \max_{\mathcal{S}} l(\mathcal{S}) = l(\mathcal{A}).$$

2. Докажем обратное неравенство $l(\mathcal{A}) \leqslant l(\mathcal{A}_1)$. Для этого возьмём в $\mathcal{A}$ систему порождающих $\mathcal{S} = \{a_1, \ldots, a_k\}$ длины $l(\mathcal{S}) = l(\mathcal{A})$. Согласно предложению 3.3 можно считать, что $\dim \mathcal{L}_1(\mathcal{S}) = |\mathcal{S}| = k$. Рассмотрим подмножество $\mathcal{S}_0 = \{(a_1, 0), \ldots, (a_k, 0)\}$ в $\mathcal{A}_1$. По построению $\dim \mathcal{L}_1(\mathcal{S}_0) = k + 1$, т. е. для любого $m \geqslant 1$ $\mathcal{S}$ и $\mathcal{S}_0$ удовлетворяют соотношениям (3.3)—(3.5). При $m = l(\mathcal{S})$ получаем, что

$$\dim \mathcal{L}_m(\mathcal{S}_0) = \dim \mathcal{L}_m(\mathcal{S}) + 1 = \dim \mathcal{A} + 1 = \dim \mathcal{A}_1.$$

Значит, множество $\mathcal{S}_0$ является системой порождающих для $\mathcal{A}_1$, и из равенства размерностей получаем, что

$$l(\mathcal{A}) = l(\mathcal{S}) = l(\mathcal{S}_0) \leqslant \max_{\mathcal{S}_{\mathcal{A}_1}} l(\mathcal{S}_{\mathcal{A}_1}) = l(\mathcal{A}_1). \qquad \square$$

Следствие 3.7. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — такая подалгебра $\mathrm{M}_n(\mathbb{F})$, что $E \notin \mathcal{A}$. Если $\mathcal{A}_1 = \langle E, A \mid A \in \mathcal{A} \rangle$, то $l(\mathcal{A}_1) = l(\mathcal{A})$.*

Таким образом, без ограничения общности мы можем считать далее, что все рассматриваемые в этой работе алгебры содержат единицу.

3.3. Длина прямой суммы алгебр

В данном разделе получены точные верхняя и нижняя оценки длины прямых сумм алгебр.

Пусть $\mathcal{A}$ и $\mathcal{B}$ — конечномерные алгебры над одним полем $\mathbb{F}$. Через $\mathcal{A} \oplus \mathcal{B}$ обозначим алгебру, элементами которой являются пары (a, b), $a \in \mathcal{A}$, $b \in \mathcal{B}$, с покоординатными сложением, умножением на числа и умножением, т. е. для любых (a_1, b_1), (a_2, b_2), $(a, b) \in \mathcal{A} \oplus \mathcal{B}$ и для любого $\alpha \in \mathbb{F}$ выполнено

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$
$$\alpha(a, b) = (\alpha a, \alpha b),$$
$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2).$$

Замечание 3.8. Отметим, что если $\mathcal{A}$ и $\mathcal{B}$ — алгебры с единицами $1_{\mathcal{A}}$ и $1_{\mathcal{B}}$ соответственно, то алгебра $\mathcal{A} \oplus \mathcal{B}$ содержит единицу $1_{\mathcal{A} \oplus \mathcal{B}} = (1_{\mathcal{A}}, 1_{\mathcal{B}})$. В случае, когда в прямую сумму входят слагаемые как с единицами, так и без, обязательно дополним их единицами внешним образом.

Теорема 3.9. *Пусть $\mathcal{A}$ и $\mathcal{B}$ — конечномерные ассоциативные алгебры над полем $\mathbb{F}$ длин $l_{\mathcal{A}}$ и $l_{\mathcal{B}}$ соответственно. Тогда выполнены следующие неравенства*:

$$\max\{l_{\mathcal{A}}, l_{\mathcal{B}}\} \leqslant l(\mathcal{A} \oplus \mathcal{B}) \leqslant l_{\mathcal{A}} + l_{\mathcal{B}} + 1. \qquad (3.6)$$

Доказательство. Обозначим $p = l_{\mathcal{A}}$, $q = l_{\mathcal{B}}$.

Для того чтобы доказать нижнюю оценку, возьмём системы порождающих $\{a_1, \ldots, a_k\}$ и $\{b_1, \ldots, b_m\}$ для $\mathcal{A}$ и $\mathcal{B}$ с длинами p и q соответственно. Тогда множество $\{(a_1, 0), \ldots, (a_k, 0), (0, b_1), \ldots, (0, b_m)\}$ будет системой порождающих в $\mathcal{A} \oplus \mathcal{B}$ длины, не меньшей $\max\{p, q\}$.

Возьмём в $\mathcal{A}\oplus\mathcal{B}$ произвольную систему порождающих $\mathcal{S}=\{(c_1,d_1),\ldots,(c_n,d_n)\}$ и докажем, что всякое слово от элементов $\mathcal{S}$ длины $p+q+2$ сократимо. Заметим, что множество $c_1,\ldots,c_n$ является системой порождающих для алгебры $\mathcal{A}$, множество $d_1,\ldots,d_n$ является системой порождающих для алгебры $\mathcal{B}$. Обозначим $N=p+q+2$. Пусть

$$v=(c_{i_1},d_{i_1})\cdots(c_{i_N},d_{i_N})=(c_{i_1}\cdots c_{i_N},d_{i_1}\cdots d_{i_N}),\;\; i_j\in\{1,\ldots,n\},\;\; j=1,\ldots,N.$$

Так как длина алгебры $\mathcal{A}$ равна p, то слово $c_{i_1}\cdots c_{i_{p+1}}$ сократимо, т. е.

$$c_{i_1}\cdots c_{i_{p+1}}=\alpha_1 c_{i_1}\cdots c_{i_p}+\ldots+\alpha_{M-1}c_n+\alpha_M 1_{\mathcal{A}}.$$

Так как длина алгебры $\mathcal{B}$ равна q, то слово $d_{i_{p+2}}\cdots d_{i_N}$ сократимо, т. е.

$$d_{i_{p+2}}\cdots d_{i_N}=\beta_1 d_{i_{p+2}}\cdots d_{i_{N-1}}+\ldots+\beta_{K-1}d_n+\beta_K 1_{\mathcal{B}}.$$

Подставляя выражения для $c_{i_1}\cdots c_{i_{p+1}}$ и $d_{i_{p+2}}\cdots d_{i_N}$ в v, получим

$$\begin{aligned}&\{(c_{i_1}\cdots c_{i_{p+1}},\, d_{i_1}\cdots d_{i_{p+1}})-\alpha_1(c_{i_1}\cdots c_{i_p},\, d_{i_1}\cdots d_{i_p})-\ldots-\\&\quad-\alpha_{M-1}(c_n,d_n)-\alpha_M(1_A,1_B)\}\{(c_{i_{p+2}}\cdots c_{i_N},\, d_{i_{p+2}}\cdots d_{i_N})-\\&\quad-\beta_K(1_A,1_B)-\beta_{K-1}(c_n,d_n)-\ldots-\beta_1(c_{i_{p+2}}\cdots c_{i_{N-1}},\; d_{i_{p+2}}\cdots d_{i_{N-1}})\}=\\&\quad=(0,x)(y,0)=0.\end{aligned}$$

Значит, слово v представляется в виде линейной комбинации слов меньшей длины. Так как v было выбрано произвольно, то $l(\mathcal{A}\oplus\mathcal{B})\leqslant p+q+1$. □

По индукции оценки в предыдущей теореме обобщаются на произвольное число слагаемых.

Следствие 3.10. *Пусть $\mathbb{F}$ — произвольное поле и $k\in\mathbb{N}$, $k\geqslant 2$. Пусть $\mathcal{A}_1,\ldots,\mathcal{A}_k$ — конечномерные ассоциативные алгебры над полем $\mathbb{F}$ длин $l_1,\ldots,l_k$ соответственно. Пусть $\mathcal{A}=\bigoplus\limits_{j=1}^{k}\mathcal{A}_j$. Тогда выполнены следующие неравенства:*

$$\max\{l_1,\ldots,l_k\}\leqslant l(\mathcal{A})\leqslant\sum_{j=1}^{k}l_j+k-1.$$

Следствие 3.11. *Пусть $\mathcal{A}$ — подалгебра блочно-треугольных матриц, т. е. все матрицы из $\mathcal{A}$ имеют вид*

$$A=\left(\begin{array}{c|c|c|c}A_{1,1}&A_{1,2}&\ldots&A_{1,k}\\\hline 0&A_{2,2}&\ldots&A_{2,k}\\\hline &&\ddots&\\\hline 0&0&\ldots&A_{k,k}\end{array}\right),$$

где $A_{i,j}\in\mathrm{M}_{n_i,n_j}(\mathbb{F})$, $n_1+n_2+\ldots+n_k=n$, причём все матрицы $A_{i,i}$ образуют подалгебру в $\mathrm{M}_{n_i}(\mathbb{F})$ длины l_i, $i=1,\ldots,k$. Тогда для $l(\mathcal{A})$ выполнены следующие неравенства:

$$\max\{l_1,\ldots,l_k\}\leqslant l(\mathcal{A})\leqslant\sum_{j=1}^{k}l_j+k-1. \tag{3.7}$$

Отсюда легко вытекает следующий результат.

Следствие 3.12. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — произвольная подалгебра алгебры $\mathrm{T}_n(\mathbb{F})$. Тогда $l(\mathcal{A}) \leqslant n-1$.*

Доказательство. Любая подалгебра треугольной матричной алгебры является блочно-треугольной алгеброй, все блоки которой имеют единичный размер. Так как $l(\mathbb{F}) = 0$, имеем оценку $l(\mathcal{A}) \leqslant 0 + n - 1 = n - 1$. □

Теорема 3.13. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{D}$ — произвольная подалгебра в $\mathrm{D}_n(\mathbb{F})$. Положим $\mathcal{A} = \mathcal{D} + \mathrm{N}_n(\mathbb{F})$. Тогда $l(\mathcal{A}) = n-1$. В частности, $l\big(\mathrm{T}_n(\mathbb{F})\big) = n-1$.*

Доказательство. Верхняя оценка $l(\mathcal{A}) \leqslant n-1$ доказана в следствии 3.12. Пусть $D_1, \ldots, D_k$ — базис $\mathcal{D}$. Рассмотрим следующую систему порождающих для $\mathcal{A}$:

$$\mathcal{S} = \{E_{i,i+1},\ i = 1, \ldots, n-1\} \cup \{D_1, \ldots, D_k\}.$$

Для любых $1 \leqslant i < j \leqslant n$ и $r, s = 1, \ldots, k$ выполнено $D_r E_{i,j} = (D_r)_{i,i} E_{i,j}$, $E_{i,j} D_r = (D_r)_{j,j} E_{i,j}$ и $D_r D_s \in \langle D_1, \ldots, D_k \rangle$. Также $E_{1,n} = E_{1,2} E_{2,3} \cdots E_{n-1,n}$ не может быть представлена как произведение меньшего, чем $n-1$, числа элементов $\mathcal{S}$. Таким образом, $l(\mathcal{S}) = n-1$, и следовательно, $l(\mathcal{A}) \geqslant n-1$. □

Отметим, что обе оценки (3.6) являются точными. Это следует из теорем 3.15 и 5.24 ниже.

Приведём пример алгебры, длина которой не совпадает с оценками из теоремы 3.9 и лежит строго между ними.

Пример 3.14. Пусть $\mathcal{A} = \mathcal{B} = \mathrm{D}_n(\mathbb{F}_2)$, $n \geqslant 2$. Согласно теореме 4.60 $l(\mathcal{A}) = l(\mathcal{B}) = [\log_2 n] > 0$. Также

$$\begin{aligned} l(\mathcal{A} \oplus \mathcal{B}) &= l\big(\mathrm{D}_{2n}(\mathbb{F}_2)\big) = \\ &= [\log_2 2n] = [\log_2 n + \log_2 2] = [\log_2 n + 1] = [\log_2 n] + 1 = l(\mathcal{A}) + 1. \end{aligned}$$

Следовательно,

$$\max\{l(\mathcal{A}), l(\mathcal{B})\} = l(\mathcal{A}) < l(\mathcal{A}) + 1 = l(\mathcal{A} \oplus \mathcal{B}) < 2l(\mathcal{A}) + 1 = l(\mathcal{A}) + l(\mathcal{B}) + 1.$$

3.4. Примеры вычисления длины прямых сумм матричных подалгебр

Для некоторых прямых сумм матричных подалгебр удаётся точно вычислить длину.

Теорема 3.15. *Пусть $\mathbb{F}$ — произвольное поле. Тогда $l(\mathrm{T}_n(\mathbb{F}) \oplus \mathbb{F}) = n$.*

Доказательство. По теоремам 3.9 и 3.13

$$l(\mathrm{T}_n(\mathbb{F}) \oplus \mathbb{F}) \leqslant l\big(\mathrm{T}_n(\mathbb{F})\big) + l(\mathbb{F}) + 1 = n - 1 + 0 + 1 = n.$$

Рассмотрим следующую систему порождающих для $\mathrm{T}_n(\mathbb{F})\oplus\mathbb{F}$:

$$\mathcal{S}=\{A_i=E_{i,i}+E_{i,i+1},\, E_{n,n},\, E_{n+1},\ i=1,\ldots,n-1\}.$$

Заметим, что все A_i — идемпотенты и $A_jA_k=0$ при $j>k$ и $k-j>2$, а $A_jA_{j+1}\cdots A_{j+t}=E_{j,j+t}+E_{j,j+t+1}$ и $A_{n-s}A_{n-s+1}\cdots A_{n-1}E_{n,n}=E_{n-s,n}$, $1\leqslant t\leqslant n-2$, $1\leqslant s\leqslant n-1$, т. е. у матриц в $\mathcal{L}_1(\mathcal{S})$ ненулевые элементы могут находиться на главной диагонали и на первой наддиагонали, у матриц в $\mathcal{L}_2(\mathcal{S})$ — также на второй наддиагонали, у матриц в $\mathcal{L}_k(\mathcal{S})$ — также на k-й наддиагонали. Тогда $\dim\mathcal{L}_1(\mathcal{S})=n+1$, $\dim\mathcal{L}_{k+1}(\mathcal{S})=\dim\mathcal{L}_k(\mathcal{S})+n-k$, $1\leqslant k\leqslant n-1$. Отсюда получаем, что при $2\leqslant k\leqslant n$

$$\dim\mathcal{L}_k(\mathcal{S})=(n+1)+(n-1)+(n-2)+\ldots+(n-k+1).$$

Значит,

$$\dim\mathcal{L}_{n-1}(\mathcal{S})=\frac{n(n+1)}{2}<\frac{n(n+1)}{2}+1=\dim\mathcal{L}_n(\mathcal{S})=\dim\left(\mathrm{T}_n(\mathbb{F})\oplus\mathbb{F}\right)$$

и $l(\mathcal{S})=n$. □

Теорема 3.16. *Пусть $\mathbb{F}$ — произвольное поле. Тогда $l\big(\mathrm{T}_2(\mathbb{F})\oplus\mathrm{T}_2(\mathbb{F})\big)=3$.*

Доказательство. По теореме 3.9

$$l\big(\mathrm{T}_2(\mathbb{F})\oplus\mathrm{T}_2(\mathbb{F})\big)\leqslant 2l\big(\mathrm{T}_2(\mathbb{F})\big)+1=3.$$

Рассмотрим следующую систему порождающих для $\mathrm{T}_2(\mathbb{F})\oplus\mathrm{T}_2(\mathbb{F})$:

$$\mathcal{S}=\{A=E_{1,1}+E_{1,2}+E_{3,3}+E_{3,4},\, B=E_{2,2}+E_{3,3},\, E_4\}.$$

Видно, что $\dim\mathcal{L}_1(\mathcal{S})=3$. Так как $B^2=B$, $A^2=A$, $AB=E_{1,2}+E_{3,3}$ и $BA=E_{3,3}+E_{3,4}$, то

$$\dim\mathcal{L}_2(\mathcal{S})=5<6=\dim\mathrm{T}_2(\mathbb{F})\oplus\mathrm{T}_2(\mathbb{F}).$$

Поскольку $BAB=E_{3,3}$, то $\dim\mathcal{L}_3(\mathcal{S})=6$ и $l\big(\mathrm{T}_2(\mathbb{F})\oplus\mathrm{T}_2(\mathbb{F})\big)\geqslant l(\mathcal{S})=3$. □

Лемма 3.17. *Пусть $\mathbb{F}$ — произвольное поле. Тогда $l\big(\mathbb{F}\oplus\mathrm{M}_2(\mathbb{F})\big)=2$.*

Доказательство. Обозначим $\mathcal{A}=\mathbb{F}\oplus\mathrm{M}_2(\mathbb{F})$. Так как $\mathcal{A}$ изоморфна блочной подалгебре в $\mathrm{M}_3(\mathbb{F})$, то по теореме Гамильтона—Кэли $m(\mathcal{A})=3$. При этом $\dim\mathcal{A}=5$. Значит, $\mathcal{A}$ удовлетворяет условиям леммы 5.62, и следовательно, мы получаем верхнюю оценку $l(\mathcal{A})\leqslant 2$.

Нижняя оценка получается по теореме 3.9 и лемме 5.52:

$$l(\mathcal{A})\geqslant\max\big\{l(\mathbb{F}),l\big(\mathrm{M}_2(\mathbb{F})\big)\big\}\geqslant l\big(\mathrm{M}_2(\mathbb{F})\big)=2.$$ □

Лемма 3.18. *Пусть $\mathbb{F}$ — произвольное поле. Тогда $l\big(\mathrm{M}_2(\mathbb{F})\oplus\mathrm{D}_2(\mathbb{F})\big)=3$.*

Доказательство. Обозначим $\mathcal{A}=\mathrm{M}_2(\mathbb{F})\oplus D_2(\mathbb{F})$.

Верхняя оценка длины получается по теореме 3.9 и лемме 3.17:

$$l(\mathcal{A})=l(\mathrm{M}_2(\mathbb{F})\oplus\mathbb{F}\oplus\mathbb{F})\leqslant l(\mathrm{M}_2(\mathbb{F})\oplus\mathbb{F})+l(\mathbb{F})+1=2+0+1=3.$$

Нижняя оценка достигается на следующей системе порождающих алгебры $\mathcal{A}$:
$$\mathcal{S} = \left\{A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}.$$
Действительно,
$$A^2 = A, \quad B^2 = 0, \quad AB = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad BA = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$
$$ABA = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$
Таким образом, $\dim \mathcal{L}_2(\mathcal{S}) = 5 < 6 = \dim \mathcal{A}$, но $\mathcal{L}_3(\mathcal{S}) = \mathcal{A}$. Следовательно, $l(\mathcal{A}) \geqslant l(\mathcal{S}) = 3$. □

3.5. Поведение длины алгебры при переходе к расширению поля

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 $\mathcal{A}_{\mathbb{F}} \otimes_{\mathbb{F}} \mathbb{K}$.

Предложение 3.19. *Пусть $\mathcal{A}$ — конечномерная алгебра с единицей над полем $\mathbb{F}$. Тогда для любого расширения $\mathbb{K}$ поля $\mathbb{F}$ выполняется неравенство $l(\mathcal{A}_{\mathbb{F}}) \leqslant l(\mathcal{A}_{\mathbb{K}})$.*

Доказательство. Обозначим $l = l(\mathcal{A}_{\mathbb{F}})$. Тогда по определению длины алгебры существует система порождающих $\mathcal{S} = \{a_1, \ldots, a_k\}$ алгебры $\mathcal{A}_{\mathbb{F}}$ длины l. Очевидно, что $\mathcal{S}' = \{a_1 \otimes 1, \ldots, a_k \otimes 1\}$ является системой порождающих алгебры $\mathcal{A}_{\mathbb{K}}$. Покажем, что $l(\mathcal{S}') = l$.

Так как $l(\mathcal{S}) = l$, существует слово $v = v(a_1, \ldots, a_k)$ длины l, несократимое в $\mathcal{L}_l(\mathcal{S})$. Предположим, что $v \otimes 1$ сократимо в $\mathcal{L}_l(\mathcal{S}')$. Тогда существуют такие слова $v'_1, \ldots, v'_m \in (\mathcal{S}')^{l-1}$ и элементы $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$, что $v \otimes 1 = \sum\limits_{i=1}^{m} \alpha_i v'_i$. Однако в силу выбора множества образующих $\mathcal{S}'$ каждое слово v'_i имеет вид
$$v'_i = (a_{i_1} \otimes 1) \cdots (a_{i_j} \otimes 1) = (a_{i_1} \cdots a_{i_j}) \otimes 1,$$
т. е. каждое слово v'_i имеет вид $v'_i = v_i \otimes 1$ для некоторого $v_i \in \mathcal{S}^{l-1}$. Тогда $v \otimes 1 = \sum\limits_{i=1}^{m} v_i \otimes \alpha_i$, откуда следует, что $\alpha_i \in \mathbb{F}$ и $v = \sum\limits_{i=1}^{m} \alpha_i v_i$. Противоречие с несократимостью слова v показывает, что v' несократимо в $\mathcal{L}_l(\mathcal{S}')$, т. е. $l = l(\mathcal{S}) \leqslant l(\mathcal{S}')$. Обратное неравенство следует из того, что любой элемент алгебры $\mathcal{A}_{\mathbb{K}}$ — это линейная комбинация элементов вида $a \otimes 1$, $a \in \mathcal{A}_{\mathbb{F}}$, а каждый такой элемент — линейная комбинация слов из $(\mathcal{S}')^l$.

Следовательно, $l(\mathcal{A}_{\mathbb{K}}) \geqslant l(\mathcal{S}') = l = l(\mathcal{A}_{\mathbb{F}})$. □

Отметим, что это неравенство может быть строгим. Это следует из теоремы 4.60 ниже.

3.6. Связь между длиной алгебры и длиной её гомоморфных образов

Теорема 3.20. *Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{A}$ и $\mathcal{B}$ — алгебры над $\mathbb{F}$ и $\varphi\colon \mathcal{A} \to \mathcal{B}$ — эпиморфизм. Тогда $l(\mathcal{B}) \leqslant l(\mathcal{A})$.*

Доказательство. Обозначим $K = \ker\varphi$. Тогда по теореме о гомоморфизме $\mathcal{B} \cong \mathcal{A}/K$. Рассмотрим систему порождающих $\mathcal{S}_\mathcal{B} = \{b_1, \ldots, b_m\}$ алгебры $\mathcal{B}$ длины $l(\mathcal{S}_\mathcal{B}) = l(\mathcal{B})$. Пусть $a_1, \ldots, a_m$ — такие элементы $\mathcal{A}$, что $\varphi(a_j) = b_j$, $j = 1, \ldots, m$, и пусть $e_1, \ldots, e_k \in K$ образуют базис K. Тогда $\mathcal{S}_\mathcal{A} = \{a_1, \ldots, a_m, e_1, \ldots, e_k\}$ является системой порождающих для $\mathcal{A}$.

Пусть $N = l(\mathcal{S}_\mathcal{A})$. Покажем, что $l(\mathcal{S}_\mathcal{B}) \leqslant N$. Для этого покажем, что для произвольного элемента $w \in \mathcal{L}_{N+1}(\mathcal{S}_\mathcal{B})$ верно $w \in \mathcal{L}_N(\mathcal{S}_\mathcal{B})$. По определению w найдётся такой многочлен $P_{N+1} \in \mathbb{F}\langle x_1, \ldots, x_m\rangle$ степени, не большей $N+1$, что $w = P_{N+1}(b_1, \ldots, b_m)$. Тогда если положить $v = P_{N+1}(a_1, \ldots, a_m)$, то $\varphi(v) = w$. По построению $v \in \mathcal{L}_{N+1}(\mathcal{S}_\mathcal{A})$, следовательно, $v \in \mathcal{L}_N(\mathcal{S}_\mathcal{A})$, т. е. найдётся такой многочлен $P_N \in \mathbb{F}\langle x_1, \ldots, x_{m+k}\rangle$ степени, не большей N, что $v = P_N(a_1, \ldots, a_m, e_1, \ldots, e_k)$. Поскольку K — идеал в $\mathcal{A}$, то найдётся такой многочлен $Q_N \in \mathbb{F}\langle x_1, \ldots, x_m\rangle$ степени, не большей N, что $v = Q_N(a_1, \ldots, a_m) + r$, $r \in K \subseteq \mathcal{L}_1(\mathcal{S}_\mathcal{A})$. Значит,

$$w = \varphi(v) = \varphi(Q_N(a_1, \ldots, a_m) + r) = \varphi\big(Q_N(a_1, \ldots, a_m)\big) = \\ = Q_N(b_1, \ldots, b_m) \in \mathcal{L}_N(\mathcal{S}_\mathcal{B}).$$

Следовательно, $l(\mathcal{B}) = l(\mathcal{S}_\mathcal{B}) \leqslant l(\mathcal{S}_\mathcal{A}) \leqslant l(\mathcal{A})$. □

Следующий пример показывает, что из равенства длин в теореме 3.20, вообще говоря, не следует, что φ — изоморфизм алгебр.

Пример 3.21. Пусть $\mathcal{A} = \mathrm{T}_n(\mathbb{R})$, $\mathcal{B} = \mathrm{D}_n(\mathbb{R})$. Существует естественный гомоморфизм $\pi\colon \mathcal{A} \to \mathcal{B}$, действующий следующим образом:

$$\pi\colon \begin{pmatrix} a_{1,1} & & * \\ & \ddots & \\ 0 & & a_{n,n} \end{pmatrix} \mapsto \begin{pmatrix} a_{1,1} & & 0 \\ & \ddots & \\ 0 & & a_{n,n} \end{pmatrix}.$$

При этом

$$\dim\mathcal{A} = \frac{n(n+1)}{2} > n = \dim\mathcal{B}$$

и $\mathcal{A} \ncong \mathcal{B}$, однако из теорем 3.13 и 4.60 получаем, что $l(\mathcal{A}) = l(\mathcal{B}) = n-1$.

Следующий пример показывает, что неравенство в теореме 3.20 может быть строгим.

Пример 3.22. Пусть $\mathcal{A} = \mathrm{T}_n(\mathbb{F}_2)$, $\mathcal{B} = \mathrm{D}_n(\mathbb{F}_2)$, $n > 2$. Существует естественный гомоморфизм $\pi\colon \mathcal{A} \to \mathcal{B}$, описанный в примере 3.21. Из теорем 3.13 и 4.60 получаем, что $l(\mathcal{A}) = n - 1 > [\log_2(n)] = l(\mathcal{B})$.

3.7. Нижняя оценка длины тензорного произведения

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

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

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

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

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

$$\mathcal{L}_N(\mathcal{S}) = \left\langle a_{i_1} \cdots a_{i_s} \otimes b_{j_1} \cdots b_{j_t} \;\middle|\; \begin{matrix} s, t \in \mathbb{Z}_+, \\ 0 \leqslant s + t \leqslant N \end{matrix} \right\rangle.$$

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

$$\mathcal{L}_N(\mathcal{S}) = \left\langle a_{i_1} \cdots a_{i_s} \otimes b_{j_1} \cdots b_{j_t} \;\middle|\; \begin{matrix} s, t \in \mathbb{Z}_+,\ s \leqslant m,\ t \leqslant n \\ 0 \leqslant s + t \leqslant N \end{matrix} \right\rangle. \tag{3.8}$$

Следовательно,

$$\mathcal{L}_{m+n}(\mathcal{S}) = \left\langle a_{i_1} \cdots a_{i_s} \otimes b_{j_1} \cdots b_{j_t} \;\middle|\; \begin{matrix} s, t \in \mathbb{Z}_+, \\ 0 \leqslant s + t \leqslant m + n \end{matrix} \right\rangle =$$
$$= \left\langle a_{i_1} \cdots a_{i_s} \otimes b_{j_1} \cdots b_{j_t} \;\middle|\; \begin{matrix} s, t \in \mathbb{Z}_+, \\ s \leqslant m,\ t \leqslant n \end{matrix} \right\rangle = \mathcal{L}_m(\mathcal{S}_\mathcal{A}) \otimes \mathcal{L}_n(\mathcal{S}_\mathcal{B}) = \mathcal{A} \otimes \mathcal{B}.$$

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

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 (3.8) следует, что

$$\mathcal{L}_{m+n-1}(\mathcal{S}) = \left\langle a_{i_1} \cdots a_{i_s} \otimes b_{j_1} \cdots b_{j_t} \;\middle|\; \begin{matrix} s, t \in \mathbb{Z}_+,\ s \leqslant m,\ t \leqslant n, \\ 0 \leqslant s + t \leqslant m + n - 1 \end{matrix} \right\rangle =$$
$$= \mathcal{L}_{m-1}(\mathcal{S}_\mathcal{A}) \otimes \mathcal{L}_n(\mathcal{S}_\mathcal{B}) + \mathcal{L}_m(\mathcal{S}_\mathcal{A}) \otimes \mathcal{L}_{n-1}(\mathcal{S}_\mathcal{B}).$$

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

3.8. Верхняя оценка длины алгебры как функция от индекса нильпотентности её радикала Джекобсона и длины фактора по радикалу

В данном разделе получена верхняя оценка длины алгебры как функция двух инвариантов этой алгебры: индекса нильпотентности её радикала Джекобсона и длины фактора по радикалу. В частности, в случае локальных алгебр (локальность понимается в смысле определения 3.24) предлагаемая верхняя оценка длины является усовершенствованием ранее полученной автором оценки из работы [10].

Определение 3.24. Ассоциативная алгебра называется *локальной*, если она обладает единственным максимальным правым идеалом.

Определение 3.25. *Радикалом Джекобсона* ассоциативного кольца называется пересечение всех его максимальных правых идеалов.

Замечание 3.26. Известно, что множество всех необратимых элементов локальной алгебры содержится в её радикале Джекобсона. Радикал Джекобсона J артинова кольца нильпотентен, т. е. существует такое натуральное число N, что $J^N = (0)$, а $J^{N-1} \neq (0)$, здесь через J^N обозначено множество всех произведений элементов из J длины N, число N называют *индексом нильпотентности* идеала J (см., например, [11, § 4.4]. В частности, радикал Джекобсона конечномерной алгебры нильпотентен.

Согласно основной теореме об эквивалентности различных определений локальности (см. [11, § 5.2]), определение 3.24 эквивалентно следующему.

Определение 3.27. Ассоциативная алгебра называется *локальной*, если фактор-алгебра $\mathcal{A}/J(\mathcal{A})$ является алгеброй с делением.

Сперва докажем вспомогательные утверждения относительно длин сократимых слов от элементов произвольного подмножества в данной алгебре и от элементов её систем порождающих.

Лемма 3.28. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — конечномерная $\mathbb{F}$-алгебра. Положим $\mathcal{B} = \mathcal{A}/J(\mathcal{A})$, где $J(\mathcal{A})$ обозначает радикал Джекобсона алгебры $\mathcal{A}$, и $Q = l(\mathcal{B}) + 1$. Пусть $\mathcal{S} = \{A_1,\ldots,A_k\} \subseteq \mathcal{A}$ — произвольная система порождающих алгебры $\mathcal{A}$. Тогда для любого набора $\mathbf{i} = (i_1,\ldots,i_Q) \in \mathbb{N}^Q$, $1 \leqslant i_s \leqslant k$,*

$s=1,\ldots,k$, существует такой многочлен $P_{\mathbf{i}} \in \mathbb{F}\langle x_1,\ldots,x_k\rangle$ степени, не большей $Q-1$, что $A_{i_1}A_{i_2}\cdots A_{i_Q} - P_{\mathbf{i}}(A_1,\ldots,A_k) \in J(\mathcal{A})$.

Доказательство. Если хотя бы один из элементов $A_{i_1},\ldots,A_{i_Q}$ принадлежит $J(\mathcal{A})$, то лемма выполняется тривиально.

Рассмотрим естественный гомоморфизм алгебр

$$\pi\colon \mathcal{A} \to \mathcal{B}, \quad A \mapsto A + J(\mathcal{A}), \quad A \in \mathcal{A},$$

ядром которого является идеал $J(\mathcal{A})$. Поскольку множество $\mathcal{S}$ выбрано как система порождающих для алгебры $\mathcal{A}$, то множество

$$\mathcal{S}_B = \{B_1 = \pi(A_1),\ldots,B_k = \pi(A_k)\} \subseteq \mathcal{B}$$

является системой порождающих для фактор-алгебры $\mathcal{B}$. По определению длины получаем, что $l(\mathcal{S}_B) \leqslant Q-1$. Таким образом, любое слово от элементов $\mathcal{S}_B$ длины Q сократимо в смысле определения 2.12. Следовательно, найдётся такой многочлен $P_{\mathbf{i}} \in \mathbb{F}\langle x_1,\ldots,x_k\rangle$ степени, не большей $Q-1$, что

$$B_{i_1}\cdots B_{i_Q} = P_{\mathbf{i}}(B_1,\ldots,B_k). \tag{3.9}$$

Пользуясь линейностью и мультипликативностью отображения π, из равенства (3.9) получаем соотношения

$$\pi(A_{i_1}\cdots A_{i_Q}) = \pi\big(P_{\mathbf{i}}(A_1,\ldots,A_k)\big), \quad \pi\big(A_{i_1}\cdots A_{i_Q} - P_{\mathbf{i}}(A_1,\ldots,A_k)\big) = 0,$$

это и означает, что

$$A_{i_1}\cdots A_{i_Q} - P_{\mathbf{i}}(A_1,\ldots,A_k) \in J(\mathcal{A}). \qquad \square$$

Следствие 3.29. *Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{A}$ — конечномерная $\mathbb{F}$-алгебра и $J(\mathcal{A})$ — её радикал Джекобсона, $\mathcal{B} = \mathcal{A}/J(\mathcal{A})$ и $D = \dim_{\mathbb{F}}\mathcal{B}$. Пусть $A_1,\ldots,A_D \in \mathcal{A}$ — произвольные элементы. Тогда существует такой многочлен $P \in \mathbb{F}\langle x_1,\ldots,x_D\rangle$ степени, не большей $D-1$, что $A_1A_2\cdots A_D - P(A_1,\ldots,A_D) \in J(\mathcal{A})$.*

Доказательство. Как и при доказательстве леммы 3.28, рассмотрим естественный гомоморфизм алгебр $\pi\colon \mathcal{A} \to \mathcal{B}$. Множество

$$\mathcal{S} = \{B_1 = \pi(A_1),\ldots,B_D = \pi(A_D)\} \subseteq \mathcal{B}$$

является системой порождающих для некоторой подалгебры $\mathcal{B}' \subseteq \mathcal{B}$. Используя тривиальную оценку длины, получаем, что

$$l(\mathcal{S}) \leqslant l(\mathcal{B}') \leqslant \dim\mathcal{B}' - 1 \leqslant \dim\mathcal{B} - 1 = D-1.$$

Далее рассуждая как в доказательстве лемме 3.28, получим требуемое утверждение. $\square$

Теорема 3.30. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — конечномерная $\mathbb{F}$-алгебра с единицей. Пусть $J(\mathcal{A})$ — радикал Джекобсона алгебры $\mathcal{A}$, через N обозначим индекс нильпотентности $J(A)$. Пусть также $\mathcal{B} = \mathcal{A}/J(\mathcal{A})$. Тогда $l(\mathcal{A}) \leqslant (l(\mathcal{B})+1)N-1$.*

Доказательство. Обозначим $Q = l(\mathcal{B}) + 1$, $q = QN$. Пусть $\mathcal{S} = \{S_1, \ldots, S_k\}$ — произвольная система порождающих алгебры $\mathcal{A}$. Покажем, что любое слово длины q от элементов $\mathcal{S}$ сократимо в смысле определения 2.12.

Зафиксируем слово $W = S_{i_1} \cdots S_{i_q}$. Найдётся число $0 \leqslant t \leqslant q$, такое что t сомножителей в W лежат в $J(\mathcal{A})$ (обозначим их $B_1, \ldots, B_t$), а остальные $q - t$ сомножителей в W не лежат в $J(\mathcal{A})$ (их обозначим $A_1, \ldots, A_{q-t}$).

Пусть $K_1, \ldots, K_{t+1} \subseteq \{1, \ldots, q-t\}$, $K_i \cap K_j = \varnothing$, $\bigcup\limits_{i=1}^{t+1} K_i = \{1, \ldots, q-t\}$, и если $K_i \neq \varnothing$, то $K_i = \{k_i, k_i + 1, \ldots, k_i + |K_i| - 1\}$. Положим

$$V_i = \begin{cases} \prod\limits_{r \in K_i} A_r, & \text{если } K_i \neq \varnothing, \\ 1_{\mathcal{A}}, & \text{если } K_i = \varnothing. \end{cases}$$

Тогда слово W можно представить в виде

$$W = \prod_{i=1}^{t} (V_i B_i) \cdot V_{t+1}.$$

Рассмотрим три случая.

1. Пусть $t \geqslant N$. Так как $J(\mathcal{A})$ — идеал в $\mathcal{A}$, то $V_i \cdot B_i \in J(\mathcal{A})$, для всех $i = 1, \ldots, t$. Тогда $\prod\limits_{i=1}^{N} (V_i B_i) = 0$ по определению N. Следовательно,

$$W = \prod_{i=1}^{t} (V_i B_i) \cdot V_{t+1} = 0 \cdot \left(\prod_{i=N+1}^{t} (V_i B_i) \cdot V_{t+1} \right) = 0,$$

т. е. в этом случае $W = 0$, а значит, слово W сократимо.

2. Пусть $t = 0$. В этом случае имеем

$$W = \prod_{j=0}^{N-1} (A_{jQ+1} A_{jQ+2} \cdots A_{jQ+Q}).$$

По лемме 3.28 для каждого $j = 0, \ldots, N-1$ найдётся многочлен $P_j \in \mathbb{F}\langle x_1, \ldots, x_k \rangle$ степени, не большей $Q - 1$, такой что

$$A_{jQ+1} A_{jQ+2} \cdots A_{jQ+Q} - P_j(S_1, \ldots, S_k) = R_j \in J(\mathcal{A}).$$

По определению индекса нильпотентности радикала $R_0 R_1 \cdots R_N = 0$, т. е.

$$\prod_{j=0}^{N-1} \big(A_{jQ+1} A_{jQ+2} \cdots A_{jQ+Q} - P_j(S_1, \ldots, S_k) \big) = 0.$$

Раскрывая скобки, получаем, что единственный одночлен старшей степени совпадает с W, а все остальные слагаемые лежат в $\mathcal{L}_{q-1}(\mathcal{S})$. Поэтому, перенося все слагаемые, кроме первого, в правую часть равенства, получим, что $W \in \mathcal{L}_{q-1}(\mathcal{S})$, т. е. слово W сократимо.

3. Пусть $0 < t < N$. Пусть $\mathcal{T}_1$ — множество таких K_i, что $|K_i| < Q$, $\mathcal{T}_2$ — множество таких K_i, что $|K_i| \geqslant Q$. Если $s_1 = |\mathcal{T}_1|$, то $|\mathcal{T}_2| = t+1-s_1$. Заметим, что $s_1 < t+1$, так как иначе

$$\sum_{j=1}^{t+1} |K_j| \leqslant (t+1)(Q-1) \leqslant N(Q-1) < NQ - t,$$

противоречие.

Если $K_i \in \mathcal{T}_2$, то $|K_i| = q_i Q + r_i$, и если $K_j \in \mathcal{T}_1$, то $|K_j| = Q - r_j$ для $q_i, r_j \in \mathbb{N}$, $r_i \in \mathbb{Z}_+$, $r_i \leqslant Q-1$, $r_j \leqslant Q$.

Покажем, что $\sum\limits_{i\colon K_i \in \mathcal{T}_2} q_i \geqslant N - t$. Действительно, если $\sum\limits_{i\colon K_i \in \mathcal{T}_2} q_i \leqslant N-t-1$, то

$$\begin{aligned} QN - t &= \sum_{i\colon K_i \in \mathcal{T}_1} |K_i| + \sum_{j\colon K_j \in \mathcal{T}_2} |K_j| = \\ &= \biggl(\sum_{j\colon K_j \in \mathcal{T}_2} q_j + s_1\biggr) Q + \sum_{j\colon K_j \in \mathcal{T}_2} r_j - \sum_{i\colon K_i \in \mathcal{T}_1} r_i \leqslant \\ &\leqslant (N - t - 1 + s_1)Q + (t+1-s_1)(Q-1) - s_1 = QN - t - 1. \end{aligned}$$

Противоречие.

Пусть i такое, что $K_i \in \mathcal{T}_2$. Снова применяя лемму 3.28 и рассуждая как в пункте 2, получаем, что существуют элементы $R_{i,1}, R_{i,2}, \ldots, R_{i,q_i-1}, R'_{i,q_i} \in J(\mathcal{A})$ и многочлен $P_i \in \mathbb{F}\langle x_1, \ldots, x_k\rangle$ степени, не большей $q_i Q - 1$, такие что

$$\begin{multline} V_i = \bigl(R_{i,1}R_{i,2}\cdots R_{i,q_i-1}R'_{i,q_i} + P_i(S_1, \ldots, S_k)\bigr) A_{k_i+q_iQ} \cdots A_{k_i+|K_i|-1} = \\ = R_{i,1}R_{i,2}\cdots R_{i,q_i-1}R_{i,q_i} + P'_i, \quad (3.10) \end{multline}$$

где

$$R_{i,q_i} = R'_{i,q_i} \cdot (A_{k_i+q_iQ} \cdots A_{k_i+|K_i|-1}) \in J(\mathcal{A})$$

и P'_i — многочлен от $S_1, \ldots, S_k$ степени, не большей $|K_i| - 1$.

Пусть $i < t+1$ такое, что $K_i \in \mathcal{T}_1$. В этом случае заметим, что $B'_i = V_i B_i \in J(\mathcal{A})$. Если $K_{t+1} \in \mathcal{T}_1$, то положим

$$B'_t = \begin{cases} B_t V_{t+1}, & \text{если } K_t \in \mathcal{T}_2, \\ V_t B_t V_{t+1}, & \text{если } K_t \in \mathcal{T}_1. \end{cases}$$

Подставляя представления для V_i из равенства (3.10) в слово W и раскрывая скобки, получим, что существует многочлен P от элементов $S_1, \ldots, S_k$ степени, не большей $q-1$, такой что

$$W - P = \prod_k \biggl(\prod_{a_k} \biggl(\prod_{j=1}^{q_{a_k}} R_{a_k,j} B_{a_k}\biggr) \prod_{c_k} B'_{c_k}\biggr)$$

есть произведение не менее N радикальных элементов $R_{i,j}$, B_i и B'_i, следовательно, $W - P = 0$, т. е. слово W сократимо.

Таким образом, мы получили, что любое слово длины QN от элементов системы $\mathcal{S}$ сократимо в смысле определения 2.12. Это означает, что $l(\mathcal{S}) \leqslant QN-1$.

Следовательно,

$$l(\mathcal{A}) = \max_{\mathcal{S}} l(\mathcal{S}) \leqslant \max_{\mathcal{S}}\{QN-1\} = QN-1. \qquad \square$$

Следствие 3.31. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — конечномерная $\mathbb{F}$-алгебра с единицей. Пусть $J(\mathcal{A})$ — радикал Джекобсона алгебры $\mathcal{A}$, через N обозначен индекс нильпотентности $J(A)$. Пусть также $\mathcal{B} = \mathcal{A}/J(\mathcal{A})$. Тогда для длины любой подалгебры $\mathcal{A}' \subseteq \mathcal{A}$ справедлива верхняя оценка $l(\mathcal{A}') \leqslant N \dim \mathcal{B} - 1$.*

Доказательство. Из теоремы получим, что $l(\mathcal{A}') \leqslant N(l(\mathcal{B}')+1)-1$, где $\mathcal{B}' = \mathcal{A}'/J(\mathcal{A})$ — подалгебра в $\mathcal{B}$. Как в доказательстве следствия 3.29, имеем оценку $l(\mathcal{B}') \leqslant \dim \mathcal{B}' - 1 \leqslant \dim \mathcal{B} - 1$. $\square$

Следствие 3.32. *Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{A}$ — конечномерная локальная $\mathbb{F}$-алгебра и $J(\mathcal{A})$ — её радикал Джекобсона, через N обозначен индекс нильпотентности $J(A)$. Пусть $\mathcal{A} = \mathbb{F}1_{\mathcal{A}} + J(\mathcal{A})$. Тогда $l(\mathcal{A}) \leqslant N-1$.*

Следующий пример показывает, что эта оценка является точной.

Пример 3.33. Рассмотрим алгебру $\mathcal{A}$ матриц вида

$$\begin{pmatrix} \alpha & \beta_1 & \dots & \beta_{n-1} \\ 0 & \alpha & \ddots & \beta_{n-2} \\ \dots & \dots & \ddots & \dots \\ 0 & 0 & 0 & \alpha \end{pmatrix}, \quad \alpha, \beta_j \in \mathbb{F}.$$

Эта алгебра является локальной, её радикал Джекобсона равен

$$J = \left\langle \begin{pmatrix} 0 & \beta_1 & \dots & \beta_{n-1} \\ 0 & 0 & \ddots & \beta_{n-2} \\ \dots & \dots & \ddots & \dots \\ 0 & 0 & 0 & 0 \end{pmatrix} \;\middle|\; \beta_j \in \mathbb{F} \right\rangle.$$

Следовательно, $N = N(J) = n$. Имеем $l(\mathcal{A}) = N-1 = n-1$ по лемме 4.5.

Замечание 3.34. С другой стороны, в теореме 4.11 будет дан пример такой локальной алгебры $\mathcal{A} = \mathbb{F}1_{\mathcal{A}} + J(\mathcal{A})$ с индексом нильпотентности радикала N, что $l(\mathcal{A}) = N-2 < N-1$.

Определение 3.35. Пусть $\mathbb{F}$ — произвольное поле, $n \in \mathbb{N}$ и $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in \mathbb{F}[x]$. *Сопровождающей матрицей многочлена* $f(x)$ называется матрица

$$A = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \dots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix} \in \mathrm{M}_n(\mathbb{F}).$$

Лемма 3.36. *Пусть $p \in \mathbb{N}$ — простое число, $D \in \mathbb{N}$, $D \geqslant 2$. Рассмотрим поле $\mathbb{F}_{p^D}$ как $\mathbb{F}_p$-алгебру. Тогда $l(\mathbb{F}_{p^D}) = D - 1 = \dim_{\mathbb{F}_p} \mathbb{F}p^D - 1$.*

Доказательство. Согласно [4, гл. 2, § 5] существуют $f(x) \in \mathbb{F}_p[x]$ — нормированный неприводимый многочлен степени D, $A \in \mathrm{M}_D(\mathbb{F}_p)$ — сопровождающая матрица многочлена $f(x)$, такие что алгебра $\mathbb{F}_{p^D}$ изоморфна подалгебре $\mathcal{A} \subset \mathrm{M}_D(\mathbb{F}_p)$, порождённой матрицей A.

Согласно [4, теорема 2.14] многочлен $f(x)$ имеет ровно D различных корней в алгебраическом замыкании поля $\mathbb{F}_p$. Поэтому жорданова нормальная форма матрицы A состоит из D клеток размера 1 с попарно различными собственными значениями. Следовательно, матрица A циклическая (см. определение 4.2, лемму 4.5). Тогда

$$l(\mathbb{F}p^D) = l(\mathcal{A}) = D - 1. \qquad \square$$

Следующая лемма показывает, что оценка из теоремы 3.30 является точной для любых N и Q.

Лемма 3.37. *Пусть $p \in \mathbb{N}$ — простое число, $N, D \in \mathbb{N}$, $N, D \geqslant 2$. Рассмотрим $\mathbb{F}_p$-алгебру $\mathcal{A}$, состоящую из всех матриц вида*

$$\begin{pmatrix} b_1 & b_2 & b_3 & \dots & b_{N-1} & b_N \\ 0 & b_1 & b_2 & \dots & b_{N-2} & b_{N-1} \\ 0 & 0 & b_1 & \dots & b_{N-3} & b_{N-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & b_1 \end{pmatrix} \in \mathrm{M}_N(\mathbb{F}_{p^D}).$$

Тогда

1) *$\mathcal{A}$ — коммутативная локальная алгебра*;
2) *радикал Джекобсона $J(\mathcal{A})$ состоит из тех матриц, у которых $b_1 = 0$, и $N(J) = N$*;
3) *$\mathcal{B} = \mathcal{A}/J(\mathcal{A}) \cong \mathbb{F}_{p^D}$*;
4) *$l(\mathcal{B}) = D - 1$*;
5) *$l(\mathcal{A}) = DN - 1$.*

Доказательство. Утверждения 1)—3) верны по построению.

Утверждение 4) доказано в лемме 3.36.

Докажем утверждение 5). $\dim \mathcal{A} = DN$, поэтому нам нужно проверить равенство

$$l(\mathcal{A}) = DN - 1 = \dim \mathcal{A} - 1.$$

Для этого достаточно предъявить элемент, порождающий алгебру $\mathcal{A}$.

Согласно [4, гл. 2, § 5] существуют $f(x) \in \mathbb{F}_p[x]$ — нормированный неприводимый многочлен степени D, $A \in \mathrm{M}_D(\mathbb{F}_p)$ — сопровождающая матрица многочлена $f(x)$, такие что алгебра $\mathcal{A}$ изоморфна коммутативной алгебре $\mathcal{B}$ блочно-треугольных матриц вида

$$\begin{pmatrix} h_1(A) & h_2(A) & h_3(A) & \ldots & h_{N-1}(A) & h_N(A) \\ O_D & h_1(A) & h_2(A) & \ldots & h_{N-2}(A) & h_{N-1}(A) \\ O_D & O_D & h_1(A) & \ldots & h_{N-3}(A) & h_{N-2}(A) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ O_D & O_D & O_D & \ldots & O_D & h_1(A) \end{pmatrix} \in \mathrm{M}_{DN}(F_p),$$

где $h_i(x) \in \mathbb{F}_p[x]$ — многочлен степени, меньшей D, $i = 1, \ldots, N$. Поэтому по лемме 4.5 достаточно доказать, что алгебра $\mathcal{B}$ содержит циклическую матрицу.

Покажем, что циклической является матрица

$$B = \begin{pmatrix} A & I_D & O_D & \ldots & O_D & O_D \\ O_D & A & I_D & \ldots & O_D & O_D \\ O_D & O_D & A & \ddots & O_D & O_D \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ O_D & O_D & O_D & \ldots & O_D & A \end{pmatrix} \in \mathcal{B}.$$

Действительно, любое конечное поле совершенно, значит, к матрице B применима лемма 4 из [5, гл. 4, § 15.6]. Согласно [4, теорема 2.14] многочлен $h(x)$ имеет ровно D различных корней в алгебраическом замыкании поля $\mathbb{F}_p$, поэтому жорданова нормальная форма матрицы B состоит из D клеток размера N с попарно различными собственными значениями. Следовательно, матрица B циклическая. □

4. Длина коммутативных алгебр

В [30] было установлено, что длина любой коммутативной подалгебры алгебры матриц порядка n над полем комплексных чисел $\mathbb{C}$ не больше $n-1$, т. е. для коммутативных подалгебр получена линейная относительно порядка матриц верхняя оценка длины. В разделе 4.1 показано, что эта оценка справедлива в случае произвольного поля и является точной. Таким образом, можно говорить о коммутативных подалгебрах в $\mathrm{M}_n(\mathbb{F})$ длины $n-1$ как о коммутативных подалгебрах *максимальной длины*. Здесь возникают следующие естественные вопросы: получить описание коммутативных подалгебр максимальной длины и установить связь между максимальными по длине и максимальными по включению коммутативными матричными подалгебрами.

В настоящем разделе показано, что максимальными по длине являются подалгебры, порождённые циклическими матрицами (см. определение 4.2), и только они. Как следствие получено, что максимальные по длине коммутативные подалгебры в $\mathrm{M}_n(\mathbb{F})$ являются также максимальными по включению. С другой стороны, как показано в примерах из раздела 4.2, длины максимальных по включению коммутативных подалгебр в $\mathrm{M}_n(\mathbb{F})$ могут принимать любое натуральное значение в отрезке от 1 до $n-1$, т. е. максимальные по включению коммутативные подалгебры не обязательно имеют максимальную длину.

В разделе 4.4 получена точная верхняя оценка длины коммутативной алгебры как функция таких инвариантов алгебры, как размерность алгебры и максимальная степень минимального многочлена элементов алгебры. Эта оценка является улучшением общей оценки, полученной в [29, теорема 3.1] в коммутативном случае. Этот результат применяется для вычисления длины алгебры диагональных матриц над произвольным полем.

4.1. Верхняя оценка длины коммутативных матричных алгебр

Теорема 4.1. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — коммутативная подалгебра в $\mathrm{M}_n(\mathbb{F})$. Тогда $l(\mathcal{A}) \leqslant n-1$.*

Доказательство. Заметим, что в доказательстве теоремы 2 из [30] используется только алгебраическая замкнутость поля комплексных чисел. Следовательно, утверждение теоремы справедливо для произвольного алгебраически замкнутого поля. Тогда, взяв в предложении 3.19 в качестве расширения поля $\mathbb{F}$ его алгебраическое замыкание $\bar{\mathbb{F}}$, получаем оценку $l(\mathcal{A}) \leqslant l(\mathcal{A}_{\bar{\mathbb{F}}}) \leqslant n-1$. □

Нам потребуется следующий специальный класс матриц, который будет использоваться и в дальнейшем.

Определение 4.2. Пусть $\mathbb{F}$ — произвольное поле. Матрица $C \in \mathrm{M}_n(\mathbb{F})$ называется *циклической*, если

$$\dim_{\mathbb{F}}(\langle E, C, C^2, \ldots, C^{n-1}\rangle) = n.$$

Предложение 4.3 [21, теорема 4.4.17]. *Пусть $\mathbb{F}$ — произвольное поле. Матрица $C \in \mathrm{M}_n(\mathbb{F})$ является циклической тогда и только тогда, когда её минимальный многочлен совпадает с характеристическим.*

Лемма 4.5 показывает точность оценки в теореме 4.1; её доказательство основано на следующем результате Герштенхабера.

Теорема 4.4 (теорема Герштенхабера [36, теорема 1]). *Пусть $\mathbb{F}$ — произвольное поле, матрицы $A, B \in \mathrm{M}_n(\mathbb{F})$ такие, что $AB = BA$. Пусть $\mathcal{A}(A, B)$ — подалгебра $\mathrm{M}_n(\mathbb{F})$, порождённая матрицами A и B. Тогда $\dim_{\mathbb{F}} \mathcal{A}(A, B) \leqslant n$.*

Лемма 4.5. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — коммутативная подалгебра в $\mathrm{M}_n(\mathbb{F})$. Если существует циклическая матрица $A \in \mathcal{A}$, то $\mathcal{A}$ является подалгеброй, порождённой матрицей A, и $l(\mathcal{A}) = n-1$.*

Доказательство. Сначала покажем, что A порождает $\mathcal{A}$.

Поскольку матрицы $E, A, A^2, \ldots, A^{n-1}$ линейно независимы (по определению циклической матрицы), то $\dim_{\mathbb{F}} \mathcal{A} \geqslant n$. Рассмотрим произвольную матрицу $B \in \mathcal{A}$. Имеем $AB = BA$. Обозначим через $\mathcal{L}(A)$ подалгебру $\mathrm{M}_n(\mathbb{F})$, порождённую матрицей A, и через $\mathcal{L}(A, B)$ — подалгебру $\mathrm{M}_n(\mathbb{F})$, порождённую матрицами A, B. По построению $\mathcal{L}(A) \subseteq \mathcal{L}(A, B) \subseteq \mathcal{A}$.

По теореме 4.4 получаем $\dim_{\mathbb{F}} \mathcal{L}(A, B) \leqslant n$. Следовательно, $\mathcal{L}(A, B) = \mathcal{L}(A)$, поэтому $B \in \langle E, A, A^2, \ldots, A^{n-1}\rangle$, значит, B — значение некоторого многочлена от A, $\mathcal{A} = \mathcal{L}(A)$ и $\mathcal{A}$ — максимальная коммутативная подалгебра.

Из линейной независимости матриц $E, A, A^2, \ldots, A^{n-1}$ следует, что множество $\{A\}$ является системой порождающих для $\mathcal{A}$ длины $n-1$. Значит, $l(\mathcal{A}) = n - 1$. □

Следствие 4.6. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — коммутативная подалгебра в $\mathrm{M}_n(\mathbb{F})$. Если $m(\mathcal{A}) = n$, то $\dim \mathcal{A} = n$.*

4.2. Длина классических коммутативных подалгебр алгебры $\mathrm{M}_n(\mathbb{F})$

Приведём примеры вычисления длин некоторых коммутативных матричных подалгебр.

Во всех следующих примерах поле $\mathbb{F}$ произвольное.

Пример 4.7. Рассмотрим подалгебру $\mathcal{A}_1 \subseteq \mathrm{M}_n(\mathbb{F})$, состоящую из всех матриц вида

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

В [16, пример 2] доказано, что $\mathcal{A}_1$ — максимальная коммутативная подалгебра в $\mathrm{M}_n(\mathbb{F})$ с индексом нильпотентности радикала $N = 2$. Тогда по следствию 3.32 получаем, что $l(\mathcal{A}_1) = 1$.

Пример 4.8 (алгебра Шура [32]). Алгебра Шура — пример коммутативной подалгебры алгебры $\mathrm{M}_n(\mathbb{F})$ максимальной возможной размерности.

Пусть $n = k + m$, $k, m \in \mathbb{N}$ и $|k - m| \leqslant 1$. Рассмотрим следующую коммутативную подалгебру $\mathcal{A}_S \subseteq \mathrm{M}_n(\mathbb{F})$:

$$\mathcal{A}_S = \left\{ \left(\begin{array}{c|c} xI_k & Z \\ \hline 0 & xI_m \end{array} \right) \,\middle|\, x \in \mathbb{F},\ Z \in \mathrm{M}_{k,m}(\mathbb{F}) \right\}.$$

Её размерность $\dim_{\mathbb{F}}(\mathcal{A}_S) = 1 + km = [n^2/4] + 1$ является максимально возможной для коммутативной подалгебры матричной алгебры, следовательно, $\mathcal{A}_S$ — максимальная коммутативная подалгебра $\mathrm{M}_n(\mathbb{F})$. $J(\mathcal{A}_S)$ состоит из тех матриц, у которых $x = 0$. Получаем, что $N\big(J(\mathcal{A}_S)\big) = 2$ и $l(\mathcal{A}_S) = 1$.

Пример 4.9 (алгебра Куртера [18]). Алгебра Куртера — коммутативная подалгебра алгебры $\mathrm{M}_{14}(\mathbb{F})$ — знаменита тем, что $\dim(\mathcal{A}_C) = 13$. Она была построена Р. Куртером как контрпример к гипотезе Герштенхабера, утверждающей, что размерность максимальной коммутативной подалгебры алгебры $\mathrm{M}_n(\mathbb{F})$ не меньше числа n (порядка матриц) (см. [16,18,19]. Отметим, что этот пример является минимальным относительно размера матриц.

Рассмотрим множество J всех матриц порядка 14 вида

$$\left(\begin{array}{cc|cccccccccc|cc}
0 & 0 & \multicolumn{10}{c|}{} & \multicolumn{2}{c}{} \\
0 & 0 & \multicolumn{10}{c|}{O_{2\times 10}} & \multicolumn{2}{c}{O_2} \\
\hline
x_{11} & 0 & \multicolumn{10}{c|}{} & \multicolumn{2}{c}{} \\
0 & x_{11} & \multicolumn{10}{c|}{} & \multicolumn{2}{c}{} \\
x_{12} & 0 & \multicolumn{10}{c|}{} & \multicolumn{2}{c}{} \\
0 & x_{12} & \multicolumn{10}{c|}{} & \multicolumn{2}{c}{} \\
x_{21} & 0 & \multicolumn{10}{c|}{O_{10}} & \multicolumn{2}{c}{O_{10\times 2}} \\
0 & x_{21} & \multicolumn{10}{c|}{} & \multicolumn{2}{c}{} \\
x_{22} & 0 & \multicolumn{10}{c|}{} & \multicolumn{2}{c}{} \\
0 & x_{22} & \multicolumn{10}{c|}{} & \multicolumn{2}{c}{} \\
z_{11} & z_{12} & \multicolumn{10}{c|}{} & \multicolumn{2}{c}{} \\
z_{21} & z_{22} & \multicolumn{10}{c|}{} & \multicolumn{2}{c}{} \\
\hline
y_{11} & y_{12} & z_{11} & z_{12} & z_{21} & z_{22} & 0 & 0 & 0 & 0 & x_{11} & x_{12} & 0 & 0 \\
y_{21} & y_{22} & 0 & 0 & 0 & 0 & z_{11} & z_{12} & z_{21} & z_{22} & x_{21} & x_{22} & 0 & 0
\end{array}\right),$$

где x_{ij}, y_{ij} и z_{ij} — произвольные элементы поля F. Из определения множества J следует, что оно замкнуто относительно умножения и состоит из попарно коммутирующих матриц. Пусть $\delta \in J$. Матрица δ представляется в следующем блочном виде:

$$\delta = \begin{pmatrix} O_2 & O & O \\ A & O_{10} & O \\ Y & B & O_2 \end{pmatrix}.$$

Пусть

$$\delta' = \begin{pmatrix} O_2 & O & O \\ A' & O_{10} & O \\ Y' & B' & O_2 \end{pmatrix}$$

также матрица из J. Тогда

$$\delta'\delta = \begin{pmatrix} O_2 & O & O \\ O & O_{10} & O \\ B'A & O & O_2 \end{pmatrix}.$$

Следовательно, произведение любых трёх матриц из J равно нулю. Тогда $\mathcal{A}_C = \mathbb{F}E_{14} \oplus J$ — коммутативная подалгебра $\mathrm{M}_{14}(\mathbb{F})$ размерности 13 с радикалом индекса нильпотентности 3. В [16, пример 4] показано, что $\mathcal{A}_C$ является максимальной коммутативной подалгеброй.

Предложение 4.10. *Пусть $\mathcal{A}_C$ — алгебра Куртера, определённая в примере* 4.9. *Тогда $l(A_C) = 2$.*

Доказательство. Из следствия 3.32 вытекает, что $l(\mathcal{A}_C) \leqslant 2$.

Возьмём в $\mathcal{A}_C$ множество $\mathcal{S}$, состоящее из матриц

$$X_{11} = E_{3,1} + E_{4,2} + E_{13,11}, \quad X_{12} = E_{5,1} + E_{6,2} + E_{13,12},$$
$$X_{21} = E_{7,1} + E_{8,2} + E_{14,11}, \quad X_{22} = E_{9,1} + E_{10,2} + E_{14,12},$$

$$Z_{11} = E_{11,1} + E_{13,3} + E_{14,7}, \quad Z_{12} = E_{11,2} + E_{13,4} + E_{14,8},$$
$$Z_{21} = E_{12,1} + E_{13,5} + E_{14,9}, \quad Z_{22} = E_{12,2} + E_{13,6} + E_{14,10}$$

и единичной матрицы. У всех этих матриц элементы левого нижнего угла (стоящие на пересечении 13-й и 14-й строк с первым и вторым столбцами) равны нулю. Значит, $\mathcal{L}_1(\mathcal{S}) \neq \mathcal{A}_C$. На втором шаге эти элементы можно получить, например, так:

$$E_{13,1} = X_{11}Z_{11}, \quad E_{13,2} = X_{11}Z_{12}, \quad E_{13,1} = X_{21}Z_{11}, \quad E_{13,1} = X_{22}Z_{22}.$$

Следовательно, $\mathcal{S}$ является системой порождающих для $\mathcal{A}_C$ и $l(\mathcal{S}) = 2$. А значит, и $l(\mathcal{A}_C) = 2$. □

Теорема 4.11. *Пусть $n \in \mathbb{N}$, $n \geqslant 4$. Пусть $\mathbb{F}$ — произвольное поле. Пусть $A = E_{1,2} + \ldots + E_{n-2,n-1} \in \mathrm{M}_n(\mathbb{F})$ и $\mathcal{A}_\alpha \subseteq \mathrm{M}_n(\mathbb{F})$ — подалгебра, порождённая матрицами E, $E_{1,n} + \alpha E_{n,n-1}$, $\alpha \neq 0$, и A. Тогда $l(\mathcal{A}_\alpha) = 2$ при $n = 4$ и $l(A_\alpha) = n - 3$ при $n \geqslant 5$.*

Доказательство. По построению $\mathcal{A}_\alpha$ является локальной алгеброй. Как показано в [12, гл. 3, теорема 1], индекс нильпотентности её радикала Джекобсона равен $N = N\big(J(\mathcal{A}_\alpha)\big) = n - 1$. Следовательно, $l(\mathcal{A}_\alpha) \leqslant n - 2$ согласно следствию 3.32.

Рассмотрим систему порождающих $\mathcal{S} = \{A,\, B = E_{1,n} + \alpha E_{n,n-1}\}$. Имеем

$$AB = BA = 0, \quad B^2 = \alpha E_{1,n-1} = \alpha A^{n-2}, \quad B^3 = 0. \tag{4.1}$$

Значит, при $n = 4$ $\mathcal{L}_2(\mathcal{S}) = \mathcal{A}_\alpha$ и $l(\mathcal{A}_\alpha) = 2$.

При $n \geqslant 5$ и при $2 \leqslant k \leqslant n - 3$ верно

$$\dim \mathcal{L}_k(\mathcal{S}) = \dim\langle E, B, B^2, A, A^2, \ldots, A^k\rangle = k + 3,$$

следовательно, $l(\mathcal{S}) = n - 3$ и $l(\mathcal{A}_\alpha) \geqslant n - 3$.

Осталось показать, что при $n \geqslant 5$ справедлива оценка $l(\mathcal{A}_\alpha) \leqslant n-3$. Рассмотрим произвольную систему порождающих $\mathcal{S}$ для $\mathcal{A}_\alpha$ и докажем, что $l(\mathcal{S}) \leqslant n-3$.

По лемме 4.34 $\dim \mathcal{L}_1(\mathcal{S}) \geqslant 3$.

I. Если $\dim \mathcal{L}_1(\mathcal{S}) \geqslant 4$, то

$$\begin{aligned}\dim \mathcal{L}_{n-3}(\mathcal{S}) &= \dim \mathcal{L}_0(\mathcal{S}) + \sum_{k=1}^{n-3}\big(\dim \mathcal{L}_k(\mathcal{S}) - \dim \mathcal{L}_{k-1}(\mathcal{S})\big) = \\ &= \dim \mathcal{L}_1(\mathcal{S}) + \sum_{k=2}^{n-3}\big(\dim \mathcal{L}_k(\mathcal{S}) - \dim \mathcal{L}_{k-1}(\mathcal{S})\big) \geqslant \dim \mathcal{L}_1(\mathcal{S}) + \sum_{k=2}^{n-3} 1 = \\ &= \dim \mathcal{L}_1(\mathcal{S}) + n - 4 \geqslant n = \dim \mathcal{A}_\alpha,\end{aligned}$$

и $l(\mathcal{S}) \leqslant n - 3$.

II. Пусть $\dim \mathcal{L}_1(\mathcal{S}) = 3$. Согласно предложению 3.4 без ограничения общности можно считать, что $\mathcal{S} = \{A_1, A_2\}$, где

$$A_1 = \sum_{j=1}^{n-2} \gamma_{1,j} A^j + \delta_1 B, \quad A_2 = \sum_{j=1}^{n-2} \gamma_{2,j} A^j + \delta_2 B.$$

Из равенств (4.1) следует, что при $k \geqslant 2$ $\mathcal{S}^k \setminus \mathcal{S}^{k-1} \subseteq \langle A^2, A^3, \dots, A^{n-2}\rangle$. Поэтому если $\mathcal{S}$ — система порождающих, то A_1 и A_2 линейно независимы по модулю пространства $\langle A^2, A^3, \dots, A^{n-2}\rangle$, т. е.

$$\det \begin{pmatrix} \gamma_{1,1} & \delta_1 \\ \gamma_{2,1} & \delta_2 \end{pmatrix} \neq 0.$$

Пусть матрица $C = \{c_{i,j}\} \in \mathrm{M}_2(\mathbb{F})$ такая, что

$$C = \begin{pmatrix} \gamma_{1,1} & \delta_1 \\ \gamma_{2,1} & \delta_2 \end{pmatrix}^{-1}.$$

По предложению 3.1 множество

$$\mathcal{S}_c = \{A_1' = c_{1,1}A_1 + c_{1,2}A_2,\ A_2' = c_{2,1}A_1 + c_{2,2}A_2\}$$

является системой порождающих для $\mathcal{A}_\alpha$ и $l(\mathcal{S}_c) = l(\mathcal{S})$. Покажем, что $l(\mathcal{S}_c) \leqslant \leqslant n-3$.

По построению

$$A_1' = A + \sum_{j=2}^{n-2} \gamma_{1,j}' A^j, \quad A_2' = \sum_{j=2}^{n-2} \gamma_{2,j}' A^j + B.$$

Обозначим

$$C_2 = \sum_{j=2}^{n-2} \gamma_{2,j}' A^j.$$

При $m \geqslant 1$ рассмотрим матрицы

$$(A_1')^m = A^m + \sum_{t=m+1}^{n-2} \varepsilon_{m,t} A^t.$$

Получаем, что для некоторых $\mu, \lambda_1, \dots, \lambda_{n-3} \in \mathbb{F}$

$$\langle A_2', A_1', (A_1')^2, \dots, (A_1')^{n-3}\rangle =$$
$$= \langle B+\mu E_{1,n-1},\ A+\lambda_1 E_{1,n-1},\ A^2+\lambda_2 E_{1,n-1}, \dots,\ A^{n-3}+\lambda_{n-3}E_{1,n-1}\rangle \subseteq \mathcal{L}_{n-3}(\mathcal{S}_c).$$

Теперь осталось проверить, что $E_{1,n-1} \in \mathcal{L}_{n-3}(\mathcal{S}_c)$. Рассмотрим два случая.

1. Пусть $C_2^2 = 0$. Тогда из равенства (4.1) следует, что

$$(A_2')^2 = C_2^2 + 2BC_2 + B^2 = B^2 = \alpha E_{1,n-1}.$$

Поскольку $\alpha \neq 0$, то $E_{1,n-1} \in \mathcal{L}_2(\mathcal{S}_c) \subseteq \mathcal{L}_{n-3}(\mathcal{S}_c)$.

2. Пусть $C_2^2 \neq 0$. Положим $k = \min\limits_{2 \leqslant j \leqslant n-2} \{\gamma_{2,j}' \neq 0\}$. В данном случае k существует и $k \leqslant (n-2)/2$. Тогда $n-2-k \leqslant n-4$. Следовательно,

$$(A_1')^{n-k-2} \cdot A_2' = (A_1')^{n-k-2} \cdot C_2 = \gamma_{2,k}' E_{1,n-1} \in \mathcal{L}_{n-3}(\mathcal{S}_c).$$

Значит, $\mathcal{A}_\alpha = \langle E, B, E_{1,n-1}, A, A^2, \dots, A^{n-3}\rangle \subseteq \mathcal{L}_{n-3}(\mathcal{S}_c)$ и $l(\mathcal{S}_c) \leqslant n-3$. $\square$

Предложение 4.12. *Пусть $m, n \in \mathbb{N}$, $k \in \mathbb{Z}_+$ и $k + m + 1 \leqslant n$. Рассмотрим подалгебру $\mathcal{B}_{k,m} \subseteq \mathrm{M}_n(\mathbb{F})$, порождённую матрицами*

$$E,\ B = E_{m,m+1} + E_{m+1,m+2} + \ldots + E_{m+k,m+k+1},\ E_{i,j}, \qquad 1 \leqslant i \leqslant m, \quad m+k+1 \leqslant j \leqslant n.$$

Тогда $\mathcal{B}_{k,m}$ — максимальная коммутативная подалгебра в $\mathrm{M}_n(\mathbb{F})$ длины $l(\mathcal{B}_{k,m}) = k + 1$.

Доказательство. В [13] доказано, что $\mathcal{B}_{k,m}$ — максимальная коммутативная подалгебра в $\mathrm{M}_n(\mathbb{F})$ с индексом нильпотентности радикала $N = k + 2$.

Согласно следствию 3.32 получаем, что $l(\mathcal{B}_{k,m}) \leqslant k + 1$.

Для доказательства нижней оценки $l(\mathcal{B}_{k,m}) \geqslant k + 1$ рассмотрим следующую систему порождающих в $\mathcal{B}_{k,m}$:

$$\mathcal{S} = \{B,\ E_{i,j} \mid 1 \leqslant i \leqslant m,\ m + k + 1 \leqslant j \leqslant n,\ (i, j) \neq (m, m + k + 1)\}.$$

Имеем, что $BE_{i,j} = 0$, $E_{i,j}E_{p,q} = 0$ для любых $E_{i,j}, E_{p,q} \in \mathcal{S}$. Также по построению для любого $s = 2, \ldots, k + 1$ выполнено

$$B^s = \sum_{h=0}^{k-s+1} E_{m+h,m+h+s} \in \mathcal{L}_s(\mathcal{S}), \quad B^s \notin \mathcal{L}_{s-1}(\mathcal{S}).$$

Значит, $l(\mathcal{S}) = k + 1$.

Таким образом, $l(\mathcal{B}_{k,m}) = k + 1$. □

Следствие 4.13. *Пусть $n \in \mathbb{N}$, $n \geqslant 2$, и пусть $\mathbb{F}$ — произвольное поле. Тогда для любого $k \in \mathbb{N}$, $1 \leqslant k \leqslant n - 1$, алгебра $\mathrm{M}_n(\mathbb{F})$ содержит максимальную коммутативную подалгебру длины k.*

Следствие 4.14. *Пусть $n \in \mathbb{N}$, $n \geqslant 2$, и пусть $\mathbb{F}$ — произвольное поле. Тогда для любого $k \in \mathbb{Z}_+$, $0 \leqslant k \leqslant n - 2$, алгебра $\mathrm{M}_n(\mathbb{F})$ содержит коммутативную подалгебру длины k, не являющуюся максимальной по включению.*

Определение 4.15. Матрица $C \in \mathrm{M}_n(\mathbb{F})$ называется *циркулянтной матрицей* или *циркулянтом*, если она имеет вид

$$\begin{pmatrix} c_0 & c_{n-1} & c_{n-2} & \cdots & c_1 \\ c_1 & c_0 & c_{n-1} & \cdots & c_2 \\ c_2 & c_1 & c_0 & \cdots & c_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & c_{n-2} & c_{n-3} & \cdots & c_0 \end{pmatrix}.$$

Замечание 4.16. Подмножество циркулянтных матриц в $\mathrm{M}_n(\mathbb{F})$ является коммутативной подалгеброй, порождённой матрицей

$$P_n = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

(см., например, [2, гл. 1, § 3]). Подалгебру циркулянтных матриц в $\mathrm{M}_n(\mathbb{F})$ будем обозначать $\mathrm{C}_n(\mathbb{F})$.

Теорема 4.17. *Пусть $\mathbb{F}$ — произвольное поле. Тогда $l\big(\mathrm{C}_n(\mathbb{F})\big) = n - 1$.*

Доказательство. Поскольку

$$P_n^m = \sum_{i=1}^{n-m} E_{i+m,i} + \sum_{j=1}^{m} E_{j,j+n-m}$$

при $m = 1, \dots, n-1$, то $\dim\langle E, P_n, P_n^2, \dots, P_n^{n-1}\rangle = n$ и матрица P_n является циклической. Следовательно, применяя лемму 4.5, получаем утверждение теоремы. □

Следующая конструкция является обобщением конструкции циркулянтных матриц.

Определение 4.18. Пусть $\varphi \in \mathbb{F}$, $\varphi \neq 0$. Матрица $C \in \mathrm{M}_n(\mathbb{F})$ называется *φ-косоциркулянтом*, если она имеет вид

$$\begin{pmatrix} c_0 & \varphi c_{n-1} & \varphi c_{n-2} & \dots & \varphi c_1 \\ c_1 & c_0 & \varphi c_{n-1} & \dots & \varphi c_2 \\ c_2 & c_1 & c_0 & \dots & \varphi c_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & c_{n-2} & c_{n-3} & \dots & c_0 \end{pmatrix}.$$

Замечание 4.19. Подмножество φ-косоциркулянтных матриц в $\mathrm{M}_n(\mathbb{F})$ является коммутативной подалгеброй, порождённой матрицей

$$Q_n = \begin{pmatrix} 0 & 0 & \dots & 0 & \varphi \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

(см., например, [2, гл. 1, § 3]). Подалгебру φ-косоциркулянтных матриц в $\mathrm{M}_n(\mathbb{F})$ будем обозначать $\mathrm{C}_n(\mathbb{F}, \varphi)$.

Теорема 4.20. *Пусть $\mathbb{F}$ — произвольное поле. Тогда $l\big(\mathrm{C}_n(\mathbb{F}, \varphi)\big) = n - 1$.*

Доказательство. Поскольку

$$Q_n^m = \sum_{i=1}^{n-m} E_{i+m,i} + \sum_{j=1}^{m} \varphi E_{j,j+n-m}$$

при $m = 1, \ldots, n-1$, то $\dim\langle E, Q_n, Q_n^2, \ldots, Q_n^{n-1}\rangle = n$ и матрица Q_n является циклической. Следовательно, применяя лемму 4.5, получаем утверждение теоремы. $\square$

4.3. Коммутативные матричные алгебры максимальной длины

4.3.1. Коммутативные матричные алгебры максимальной длины над алгебраически замкнутыми полями

Лемма 4.21. *Пусть $\mathbb{F}$ — произвольное поле и $C \in \mathrm{M}_n(\mathbb{F})$ — циклическая матрица. Тогда матрица $C + \alpha E$ является циклической для любого $\alpha \in \mathbb{F}$.*

Доказательство. При $n = 1$ имеем, что $\mathrm{M}_1(\mathbb{F}) = \mathbb{F}$, $C = \gamma \in \mathbb{F}$ и для любого $\alpha \in \mathbb{F}$ выполнено $\dim\langle E, C + \alpha E\rangle = \dim\langle 1, \gamma + \alpha\rangle = 1$.

При $n \geqslant 2$ рассмотрим алгебру $\mathcal{A} \subset \mathrm{M}_n(\mathbb{F})$, порождённую матрицами E и C. В этом случае множество $\mathcal{S} = \{C\}$ является системой порождающих для алгебры $\mathcal{A}$ и $E \notin \langle C\rangle$. Тогда, применяя к $\mathcal{S}$ предложение 3.2, получим, что множество $\mathcal{S}(\alpha) = \{C + \alpha E\}$ является системой порождающих для алгебры $\mathcal{A}$ и $\mathcal{L}_{n-1}(\mathcal{S}) = \mathcal{L}_{n-1}\big(\mathcal{S}(\alpha)\big)$. Следовательно,

$$n = \dim\langle E, C, C^2, \ldots, C^{n-1}\rangle = \dim \mathcal{L}_{n-1}(\mathcal{S}) = \dim \mathcal{L}_{n-1}\big(\mathcal{S}(\alpha)\big) = \\ = \dim\langle E, C + \alpha E, (C+\alpha E)^2, \ldots, (C+\alpha E)^{n-1}\rangle,$$

т. е. матрица $C + \alpha E$ циклическая. $\square$

Следствие 4.22. *Не содержащая единицу алгебра $\mathcal{A}$ порождается циклической матрицей тогда и только тогда, когда алгебра $\mathcal{A}_1 = \langle E, A \mid A \in \mathcal{A}\rangle$ с присоединённой единицей порождается циклической матрицей. Поэтому тот факт, что алгебра порождается некоторой циклической матрицей, не зависит от наличия в алгебре единицы, и мы без ограничения общности можем считать, что $E \in \mathcal{A}$.*

Лемма 4.23. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A} \subseteq \mathrm{M}_n(\mathbb{F})$ — коммутативная подалгебра блочно-диагональных матриц с блоками $\mathcal{A}_i \subseteq \mathrm{M}_{n_i}(\mathbb{F})$, $i = 1, \ldots, k$. Тогда из равенства $l(\mathcal{A}) = n-1$ следует, что $l(\mathcal{A}_i) = n_i - 1$ для всех $i = 1, \ldots, k$.*

Доказательство. Из коммутативности $\mathcal{A}$ следует, что все $\mathcal{A}_i$ коммутативны. Значит, для каждого i справедливо $l(\mathcal{A}_i) \leqslant n_i - 1$. Предположим, что найдётся номер $i_0 \in \{1, \ldots, k\}$, такой что $l(\mathcal{A}_{i_0}) < n_{i_0} - 1$. Тогда по следствию 3.11

$$l(\mathcal{A}) \leqslant \sum_{j=1}^{k} l(\mathcal{A}_j) + k - 1 < \sum_{j=1}^{k} (n_j - 1) + k - 1 = n - 1.$$

Полученное противоречие доказывает лемму. $\square$

Предложение 4.24. *Пусть $\mathbb{F}$ — произвольное поле. Коммутативная подалгебра $\mathcal{A}$ в $\mathrm{M}_2(\mathbb{F})$ имеет максимальную длину тогда и только тогда, когда она порождена циклической матрицей.*

Доказательство. Пусть $A \in \mathcal{A}$ — некоторая матрица. Если матрица A не является циклической, т. е. $\dim(\langle E, A\rangle) = 1$, то $A = aE$, $a \in \mathbb{F}$. Следовательно, если найдётся $A \in \mathcal{A}$, $A \neq aE$, то $\mathcal{A}$ порождена циклической матрицей A. В этом случае $l(\mathcal{A}) = 1$, т. е. алгебра $\mathcal{A}$ максимальна по включению. Подалгебра, порождённая только единичной матрицей, имеет длину 0. □

Предложение 4.25. *Пусть $\mathbb{F}$ — поле, в котором есть по крайней мере n различных ненулевых элементов, V — подпространство в $\mathbb{F}^n$ и для каждого $i = 1, \ldots, n$ найдётся такой $v^i \in V$, что $v_i^i \neq 0$. Тогда найдётся такой $v \in V$, что $v_i \neq 0$ для всех $i = 1, \ldots, n$.*

Доказательство. Доказательство проведём индукцией по n.

База индукции. При $n = 1$ утверждение верно.

Шаг индукции. Допустим, что $n > 1$ и для $n - 1$ утверждение доказано. Это означает, что существует такой $v^0 \in V$, что $v_i^0 \neq 0$, $i = 1, \ldots, n-1$. Если $v_n^0 \neq 0$, то положим $v = v^0$. В противном случае найдётся $v^1 \in V$, $v_n^1 \neq 0$. Рассмотрим $v^0 + av^1$, $a \in \mathbb{F}$, $a \neq 0$. Пусть $y_i(x) = v_i^1 x + v_i^0$, $i = 1, \ldots, n-1$. При каждом i $v_i^0 \neq 0$, значит, уравнение $y_i(x) = 0$ имеет в $\mathbb{F}$ не более одного решения. Следовательно, если

$$X = \{x \in \mathbb{F} \mid \text{найдётся такой } i \in \{1, \ldots, n-1\}, \text{ что } y_i(x) = 0\},$$

то $|X| \leqslant n-1$. Из условия на число элементов поля следует, что найдётся такой $a \in \mathbb{F}$, $a \neq 0$, что $v_i^0 + av_i^1 \neq 0$, $i = 1, \ldots, n$. Вектор $v^0 + av^1$ и есть искомый. □

Предложение 4.26. *Пусть $k, m, n \in N$, $n = k + m$, $\mathbb{F}$ — поле, содержащее не менее $[n^2/4] + 1$ различных элементов ($[\cdot]$ обозначает целую часть числа). Рассмотрим подалгебры $\mathcal{A} \subseteq \mathrm{M}_k(\mathbb{F})$, $\mathcal{B} \subseteq \mathrm{M}_m(\mathbb{F})$, порождённые циклическими матрицами. Обозначим через $\mathcal{C} = \mathcal{A} \oplus \mathcal{B}$ блочно-диагональную подалгебру в $\mathrm{M}_n(\mathbb{F})$. Тогда $\mathcal{C}$ порождена циклической матрицей.*

Доказательство. Рассмотрим циклические матрицы $A_k \in \mathcal{A}$, $B_m \in \mathcal{B}$. Тогда

$$A = \begin{pmatrix} A_k & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{C}, \quad B = \begin{pmatrix} 0 & 0 \\ 0 & B_m \end{pmatrix} \in \mathcal{C}, \quad E' = \begin{pmatrix} 0 & 0 \\ 0 & E \end{pmatrix} \in \mathcal{C}.$$

Обозначим $C(\alpha) = A + B + \alpha E'$. Покажем, что существует такое $\alpha \in \mathbb{F}$, что множества собственных значений матриц A и $B + \alpha E'$ не пересекаются, и соответственно, матрица $C(\alpha)$ циклическая.

Действительно, пусть $\bar{\mathbb{F}}$ — алгебраическое замыкание поля $\mathbb{F}$. Обозначим через $\gamma_1, \ldots, \gamma_k$ множество собственных значений матрицы A и через $\beta_1, \ldots, \beta_m$ множество собственных значений матрицы B. Положим

$$\bar{X} = \{\beta_j - \gamma_i \mid i = 1, \ldots, k, \ j = 1, \ldots, m\} \subseteq \bar{\mathbb{F}}$$

и $X = \bar{X} \cap \mathbb{F}$. Имеем

$$|X| \leqslant |\bar{X}| \leqslant k \cdot m = k(n-k) \leqslant \left[\frac{n^2}{4}\right].$$

Тогда по условию на мощность поля $\mathbb{F}$ найдётся $\alpha_0 \in \mathbb{F}$, $\alpha_0 \notin X$, и в таком случае множество собственных чисел матрицы A не пересекается с множеством собственных чисел матрицы $B + \alpha_0 E'$. Следовательно,

$$\chi_{C(\alpha_0)}(t) = \chi_A(t)\chi_{(B+\alpha_0 E')}(t) = \mu_A(t)\mu_{(B+\alpha_0 E')}(t) = \mu_{C(\alpha_0)}(t)$$

и матрица $C(\alpha_0) \in \mathcal{C}$ циклическая.

Таким образом, по лемме 4.5 алгебра $\mathcal{C}$ порождена матрицей C. □

Для доказательства основной теоремы нам понадобятся следующие классические понятия теории колец и алгебр.

Определение 4.27. Конечномерная $\mathbb{F}$-алгебра называется *полупростой*, если её радикал Джекобсона равен нулю, $J(\mathcal{A}) = 0$.

Предложение 4.28 [3, § 2.1, предложение 9]. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — конечномерная $\mathbb{F}$-алгебра. Тогда фактор-алгебра по радикалу Джекобсона $\mathcal{A}/J(\mathcal{A})$ является полупростой.*

Теорема 4.29 (теорема Веддербарна—Артина [11, § 3.5, с. 69]). *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — конечномерная полупростая $\mathbb{F}$-алгебра. Тогда существуют такие числа $n_1, \ldots, n_r \in \mathbb{N}$ и конечномерные тела $\mathbb{D}_1, \ldots, \mathbb{D}_r$ над $\mathbb{F}$, что*

$$\mathcal{A} \cong \bigoplus_{i=1}^{r} \mathrm{M}_{n_i}(\mathbb{D}_i).$$

В частности, если $\mathcal{A}$ — коммутативная полупростая алгебра, то

$$\mathcal{A} \cong \bigoplus_{i=1}^{r} \mathbb{F}_i,$$

где $\mathbb{F}_i$ — конечномерные поля над $\mathbb{F}$.

Предложение 4.30. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — коммутативная конечномерная $\mathbb{F}$-алгебра с единицей $1_{\mathcal{A}}$, не являющаяся локальной. Рассмотрим фактор-алгебру по радикалу Джекобсона $\mathcal{B} = \mathcal{A}/J(\mathcal{A})$. Тогда алгебра $\mathcal{B}$ содержит нетривиальное множество ортогональных идемпотентов $B_1, \ldots, B_k$, $k \geqslant 2$, т. е. $B_i \neq 0, 1_{\mathcal{B}}$ и $B_i B_j = \delta_{ij} B_j$,*

$$\delta_{ij} = \begin{cases} 1, & \text{если } i = j, \\ 0, & \text{если } i \neq j. \end{cases}$$

Доказательство. Согласно предложению 4.28 алгебра $\mathcal{B}$ является коммутативной полупростой алгеброй, при этом по условию данная алгебра не является алгеброй с делением. Следовательно, применяя к алгебре $\mathcal{B}$ теорему 4.29, получаем, что

$$\mathcal{B} \cong \bigoplus_{i=1}^{r} \mathbb{F}_i,$$

где $\mathbb{F}_i$ — конечномерные поля над $\mathbb{F}$ и $r \geqslant 2$. Тогда элементы

$$B_1 = (1, 0, \ldots, 0),\ B_2 = (0, 1, \ldots, 0), \ldots,\ B_r = (0, \ldots, 1)$$

и будут искомыми. □

Предложение 4.31 [3, § 3.6, предложения 1, 2]. *Пусть N — ниль-идеал кольца $\mathcal{R}$. В этом случае любое конечное или счётное ортогональное множество отличных от нуля идемпотентов может быть поднято по модулю N до ортогонального множества отличных от нуля идемпотентов кольца $\mathcal{R}$, т. е. если $R_1, R_2, \ldots$ — такие элементы кольца $\mathcal{R}$, что $R_i \notin N$ и $R_iR_j - \delta_{ij}R_j \in N$, то найдутся такие элементы $U_1, U_2, \ldots$, что $U_i \neq 0$, $U_i - R_i \in N$ и $U_iU_j = \delta_{ij}U_j$.*

Теорема 4.32. *Пусть $\mathbb{F}$ — алгебраически замкнутое поле. Коммутативная подалгебра $\mathcal{A}$ в $\mathrm{M}_n(\mathbb{F})$ имеет максимальную длину тогда и только тогда, когда она порождена циклической матрицей.*

Доказательство. Достаточность следует из леммы 4.5.

Докажем необходимость. Пусть $l(\mathcal{A}) = n - 1$. Покажем, что в этом случае $\mathcal{A}$ порождена циклической матрицей. Доказательство проведём индукцией по порядку матриц n.

База индукции. При $n = 1$ любая подалгебра с единицей $\mathcal{A}$ в $\mathrm{M}_1(\mathbb{F})$ совпадает с $\mathrm{M}_1(\mathbb{F}) = \mathbb{F}$ и порождена циклическим элементом 1. При $n = 2$ утверждение следует из предложения 4.24.

Шаг индукции. Предположим, что для коммутативных подалгебр в $\mathrm{M}_k(\mathbb{F})$, $k < n$, выполнено утверждение теоремы. Рассмотрим два случая.

1. Пусть алгебра $\mathcal{A}$ не является локальной. Согласно предложениям 4.30 и 4.31 в алгебре $\mathcal{A}$ найдётся нетривиальный идемпотент — матрица A. Тогда $A^2 = A$ и $A \neq 0, E$, следовательно, A имеет ровно два различных собственных значения: 0 и 1, причём в жордановой форме матрицы A все клетки размера 1×1. Пусть 1 как собственное число A имеет кратность s, $1 \leqslant s \leqslant n - 1$. Тогда по теореме о жордановой нормальной форме найдётся такая невырожденная матрица $V \in \mathrm{M}_n(\mathbb{F})$, что

$$E_s' = V^{-1}AV = \begin{pmatrix} E_s & 0 \\ 0 & 0_{n-s} \end{pmatrix}.$$

По теореме об общем виде матрицы, коммутирующей с данной (см. [5, § 16.6]), все матрицы, перестановочные с E_s' также являются блочно-диагональными и состоят из двух блоков.

Обозначим

$$\mathcal{A}_V = V^{-1}\mathcal{A}V = \{V^{-1}AV \mid A \in \mathcal{A}\}.$$

Очевидно, что $l(\mathcal{A}) = l(\mathcal{A}_V)$, и $\mathcal{A}$ порождена циклической матрицей тогда и только тогда, когда $\mathcal{A}_V$ порождена циклической матрицей.

Имеем

$$E'_{n-s} = \begin{pmatrix} 0_s & 0 \\ 0 & E_{n-s} \end{pmatrix} = E - E'_s \in \mathcal{A}_V.$$

Получаем, что $\mathcal{A}_V = E'_s\mathcal{A}_V \oplus E'_{n-s}\mathcal{A}_V$ — блочно-диагональная подалгебра $\mathrm{M}_n(\mathbb{F})$ с двумя ненулевыми блоками.

Из леммы 4.23 получаем, что блоки $\mathcal{A}_V$ имеют длины $s-1$ и $n-s-1$. Тогда по предположению индукции они порождены циклическими матрицами. Алгебраически замкнутое поле $\mathbb{F}$ бесконечно, алгебры $E'_s\mathcal{A}_V$ и $E'_{n-s}\mathcal{A}_V$ удовлетворяют условию предложения 4.26, следовательно, существует циклическая матрица $C \in \mathcal{A}_V$. Тогда алгебра $\mathcal{A}$ порождена циклической матрицей VCV^{-1}.

2. Пусть алгебра $\mathcal{A}$ локальна. Так как у конечного множества коммутирующих матриц над алгебраически замкнутым полем есть общий собственный вектор (см. [14, гл. 1, § 1.3, лемма 1.3.17]), то найдётся такая невырожденная матрица $V \in \mathrm{M}_n(\mathbb{F})$, что $\mathcal{A}_V = V^{-1}\mathcal{A}V \subseteq \mathrm{T}_n(\mathbb{F})$. По построению алгебра $\mathcal{A}_V$ также является локальной. Пусть J — радикал Джекобсона алгебры $\mathcal{A}_V$. Идеал J нильпотентен (см. замечание 3.26), следовательно, $J \subseteq \mathrm{N}_n(\mathbb{F})$. Поскольку поле $\mathbb{F}$ алгебраически замкнуто, то $\mathcal{A}/J = \mathbb{F}$, и любая матрица $C \in \mathcal{A}_V$ представляется в виде $C = \gamma E + C_N$, $C_N \in J$.

Если для любого $k = 1, \ldots, n$ в J есть матрица $C_k = \{c_{ij}^{(k)}\}$, для которой $c_{k,k+1}^{(k)} \neq 0$, то из предложения 4.25 получаем, что существует линейная комбинация матриц C_k — матрица $C = \{c_{ij}\}$, такая что все элементы $c_{k,k+1}$ отличны от 0. Матрицы $E, C, \ldots, C^n - 1$ линейно независимы, поскольку при $m < n$ для $C^m = \{c_{ij}^{(m)}\}$ выполнено $c_{ij}^{(m)} = 0$, $j < i + m$, и $c_{i,i+m}^{(m)}$ равны некоторым произведениям $c_{i,i+1}^{(1)} = c_{i,i+1} \neq 0$. Значит, матрица C циклическая, она порождает алгебру $\mathcal{A}_V$. Следовательно, $\mathcal{A}$ порождена циклической матрицей VCV^{-1}.

Предположим, что существует $l \in \{1, \ldots, n-1\}$, такое что для любой $B = \{b_{ij}\} \in J$ выполнено $b_{l,l+1} = 0$. Пусть $B_k = \{b_{ij}^{(k)}\} \in J$, $k = 1, \ldots, n-1$. Тогда у матрицы $B_1 B_2 \cdots B_{n-1}$ отличным от нуля может быть только последний элемент в первой строке, он равен $b_{12}^{(1)} b_{23}^{(2)} \cdots b_{n-1,n}^{(n-1)}$. Но по нашему предположению какой-то из сомножителей всегда равен нулю. Это означает, что произведение любых $n-1$ матриц в J равно 0. Тогда согласно следствию 3.32 $l(\mathcal{A}) = l(\mathcal{A}_V) \leqslant n-2$, что противоречит максимальности $\mathcal{A}$. □

Следствие 4.33. *Пусть $\mathbb{F}$ — алгебраически замкнутое поле. Если коммутативная подалгебра $\mathcal{A}$ в $\mathrm{M}_n(\mathbb{F})$ имеет длину $n-1$, то она является максимальной по включению.*

Доказательство. По теореме 4.32 если $l(\mathcal{A}) = n-1$, то $\mathcal{A}$ порождена циклической матрицей. Тогда из теоремы Герштенхабера 4.4 следует, что $\mathcal{A}$ — максимальная по включению коммутативная подалгебра. □

4.3.2. Коммутативные подалгебры максимальной длины над произвольными полями

Лемма 4.34. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — алгебра с единицей над $\mathbb{F}$. Тогда $l(\mathcal{A}) = \dim\mathcal{A} - 1$ 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. Докажем достаточность. Если алгебра $\mathcal{A}$ порождена одним элементом A степени $\deg A = \dim\mathcal{A}$, то возьмём в $\mathcal{A}$ систему порождающих $\mathcal{S} = \{A\}$. Получаем, что для любого $k \geqslant 0$ выполнено $\mathcal{L}_k(\mathcal{S}) = \langle 1_{\mathcal{A}}, A, A^2, \ldots, A^k\rangle$, и следовательно, $l(\mathcal{A}) \geqslant l(\mathcal{S}) = \deg A - 1 = \dim\mathcal{A} - 1$.

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

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

$$\begin{aligned}\dim\mathcal{L}_{n-2}(\mathcal{S}) &= \dim\mathcal{L}_0(\mathcal{S}) + \sum_{k=1}^{n-2}\bigl(\dim\mathcal{L}_k(\mathcal{S}) - \dim\mathcal{L}_{k-1}(\mathcal{S})\bigr) = \\ &= \dim\mathcal{L}_1(\mathcal{S}) + \sum_{k=2}^{n-2}\bigl(\dim\mathcal{L}_k(\mathcal{S}) - \dim\mathcal{L}_{k-1}(\mathcal{S})\bigr) \geqslant \dim\mathcal{L}_1(\mathcal{S}) + \sum_{k=2}^{n-2} 1 = \\ &= \dim\mathcal{L}_1(\mathcal{S}) + n - 3 \geqslant n = \dim\mathcal{A}. \end{aligned} \tag{4.2}$$

Следовательно, $\mathcal{L}_{n-2}(\mathcal{S}) = \mathcal{A}$ и $l(\mathcal{S}) \leqslant n - 2$. 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

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

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

Следствие 4.35. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — коммутативная подалгебра в $\mathrm{M}_n(\mathbb{F})$ размерности $\dim\mathcal{A} = n$. Тогда $l(\mathcal{A}) = n - 1$ тогда и только тогда, когда $\mathcal{A}$ порождена циклической матрицей.*

Следствие 4.36. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — некоммутативная алгебра с единицей над $\mathbb{F}$. Тогда $l(\mathcal{A}) \leqslant \dim\mathcal{A} - 2$.*

Теорема 4.37. *Пусть $\mathbb{F}$ — произвольное поле. Коммутативная подалгебра $\mathcal{A}$ в $\mathrm{M}_n(\mathbb{F})$ имеет максимальную длину тогда и только тогда, когда она порождена циклической матрицей.*

Доказательство. Достаточность следует из леммы 4.5.

Пусть $l(\mathcal{A}) = n - 1$. Рассмотрим подалгебру $\mathcal{A}_{\bar{\mathbb{F}}} \subseteq \mathrm{M}_n(\bar{\mathbb{F}})$. По предложению 3.19 и теореме 4.1

$$n - 1 = l(\mathcal{A}) \leqslant l(\mathcal{A}_{\bar{\mathbb{F}}}) \leqslant n - 1,$$

т. е. $l(\mathcal{A}_{\bar{\mathbb{F}}}) = n-1$. Тогда по теореме 4.32 подалгебра $\mathcal{A}_{\bar{\mathbb{F}}}$ порождена циклической матрицей. Следовательно, $\dim_{\bar{\mathbb{F}}} \mathcal{A}_{\bar{\mathbb{F}}} = n$.

По построению $\dim_{\mathbb{F}} \mathcal{A} = \dim_{\bar{\mathbb{F}}} \mathcal{A}_{\bar{\mathbb{F}}}$, т. е. $\dim_{\mathbb{F}} \mathcal{A} = n$. Согласно следствию 4.35 алгебра $\mathcal{A}$ порождена циклической матрицей. $\square$

Следствие 4.38. *Пусть $\mathbb{F}$ — произвольное поле. Если коммутативная подалгебра $\mathcal{A}$ в $\mathrm{M}_n(\mathbb{F})$ имеет длину $n-1$, то она является максимальной по включению.*

Следствие 4.39. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — коммутативная подалгебра в $\mathrm{M}_n(\mathbb{F})$. Если максимальная степень минимальных многочленов элементов алгебры $m(\mathcal{A})$ не превосходит $n-1$, то $l(\mathcal{A}) \leqslant n-2$.*

4.4. Верхняя оценка длины для коммутативных алгебр как функция от двух инвариантов

Вопрос о связи длины алгебры $\mathcal{A}$ с её инвариантами $\dim \mathcal{A}$ и максимальной степенью $m(\mathcal{A})$ минимального многочлена элементов алгебры был впервые поставлен в работе К. Паппачены [29], а именно получена верхняя оценка длины (см. теорему 1.3).

В [17] оценивается длина систем матриц из $\mathrm{M}_n(\mathbb{F})$, обладающих следующим свойством.

Определение 4.40 [17, определение 2.1]. Подмножество $\mathcal{S} = \{X_1, \ldots, X_t\}$ в алгебре $\mathcal{A}$ обладает *модифицированным свойством Пуанкаре—Биркгофа—Витта* (сокращённо *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

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

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

Теорема 4.41 [17, теорема 2.7]. *Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{S} \subset \mathrm{M}_n(\mathbb{F})$ — множество матриц, обладающее модифицированным ПБВ-свойством. Тогда $l(\mathcal{S}) \leqslant 2n-2$.*

Отметим, что в [17, 29, 30] используются схожие комбинаторные методы подсчёта линейно независимых подслов.

В данном разделе предлагается улучшение оценки из теоремы 1.3 в случае, когда алгебра $\mathcal{A}$ коммутативна.

Пусть

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

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

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

Лемма 4.42. *Пусть $d, m \in \mathbb{N}$, $d \geqslant m \geqslant 2$. Тогда для любых $k, r_0, r, s \in \mathbb{N}$, $1 \leqslant k \leqslant m-1$, $0 \leqslant r_0 < m^r$, выполнены равенства*

$$g(m^{r+s}, m) = g(m^r, m) + g(m^s, m), \tag{4.3}$$

$$g(km^r, m) = g(k, k) + g(m^r, m), \tag{4.4}$$

$$g(km^r + r_0, m) = g(km^r, m). \tag{4.5}$$

Доказательство. 1. Сначала проверим равенство (4.3):

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

2. Теперь проверим равенство (4.4). Так как $\log_m k \in [0, 1)$, $\log_m m^r \in \mathbb{N}$, то

$$[\log_m km^r] = [\log_m k + \log_m m^r] = \log_m m^r = r,$$

$$[m^{\{\log_m km^r\}}] = [m^{\{\log_m k\}}] = [m^{\log_m k}] = k.$$

Получаем

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

3. Поскольку $km^r \leqslant km^r + r_0 < m^{r+1}$, то $[\log_m(km^r + r_0)] = [\log_m km^r] = r$ и

$$[m^{\{\log_m(km^r + r_0)\}}] = \left[\frac{km^r + r_0}{m^r}\right] = k = \left[\frac{km^r}{m^r}\right] = [m^{\{\log_m km^r\}}],$$

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

Теорема 4.43. *При фиксированном значении $m \geqslant 2$ функция $g(d, m)$ является неубывающей по d.*

Доказательство. Пусть $m \geqslant 2$ — некоторое натуральное число, $d_1, d_2 \in \mathbb{N}$, $m \leqslant d_1 < d_2$. Проверим, что $g(d_1, m) \leqslant g(d_2, m)$. Числа d_1 и d_2 единственным образом представляются в виде $d_i = q_i m^{l_i} + r_i$, $l_i \geqslant 1$, $1 \leqslant q_i \leqslant m-1$, $0 \leqslant r_i < m^{l_i}$, $i = 1, 2$. 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

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

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, $l_1 \leqslant l_2$. Рассмотрим отдельно два случая.

1. $l_1 < l_2$. Имеем

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

при этом по условию $l_2 - l_1 > 0$, значит, $l_2 - l_1 \geqslant 1$, и $q_2 - q_1 \geqslant 1-(m-1) = 2-m$. Следовательно,

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

и

$$g(d_2, m) > g(d_1, m).$$

2. $l_1 = l_2$. 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 $r_2 - r_1 \leqslant m^{l_1} - 1$, значит,

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

или

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

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

$$g(d_2, m) - g(d_1, m) = q_2 - q_1 \geqslant 0$$

и

$$g(d_2, m) \geqslant g(d_1, m). \qquad \square$$

Теорема 4.44. *При фиксированном значении $d \geqslant 2$ 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 $d \geqslant 3$ — некоторое натуральное число, и пусть $m_1, m_2 \in \mathbb{N}$, $2 \leqslant m_1 < m_2 \leqslant d$. Докажем, что $g(d, m_1) \leqslant g(d, m_2)$. Доказательство проведём индукцией по d.

База индукции. Пусть $d = 3$, $2 \leqslant m \leqslant 3$. 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 выполнено.

I. Пусть $m_1, m_2 \in \mathbb{N}$, $2 \leqslant m_1 < m_2 \leqslant d$, такие, что $[\log_{m_1} d] = [\log_{m_2} d] = l$. Так как $m_2 \leqslant d$, то $l \geqslant 1$. Рассмотрим функцию

$$f\colon (1, +\infty) \to \mathbb{R}, \quad f(x) = l(x-1) + \frac{d}{x^l}.$$

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

$$f(n_1) < f(n_2), \quad [f(n_1)] \leqslant [f(n_2)]$$

и

$$g(d, n_1) = (n_1 - 1)l + \left[\frac{d}{n_1^l}\right] = \left[(n_1 - 1)l + \frac{d}{n_1^l}\right] = [f(n_1)] \leqslant$$
$$\leqslant [f(n_2)] = \left[(n_2 - 1)l + \frac{d}{n_2^l}\right] = (n_2 - 1)l + \left[\frac{d}{n_2^l}\right] = g(d, n_2).$$

II. Таким образом, осталось доказать, что для $2 \leqslant m < d$, таких что $[\log_m d] > [\log_{m+1} d]$, выполнено $g(d, m) \leqslant g(d, m+1)$. Обозначим $l = [\log_m d]$, $s = [\log_{m+1} d]$, $l > s \geqslant 1$. 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 $1 \leqslant q \leqslant m - 1$, $1 \leqslant q_1 \leqslant m$, $0 \leqslant r < m^l$, $0 \leqslant r_1 < (m+1)^s$. Заметим, что НОД$(m, m+1) = 1$, поэтому qm^l делится на m^2, а $q_1(m+1)^s$ не делится на m^2, следовательно, $r \neq r_1$. Значит, хотя бы один из остатков r и r_1 строго положителен. Рассмотрим случаи.

1. $s = 1$.

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

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

По равенству (4.5) имеем, что $g(d, m) = g(d_0, m)$ и $g(d, m+1) = g(d_0, m+1)$. Следовательно,

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

б) $r > 0$, $r_1 = 0$. Если $d = m+1$, то $m + 1 > qm^l \geqslant m^l \geqslant m^2$, это неравенство не выполняется при $m \geqslant 2$, поэтому можно считать, что $d > m+1$, $d - 1 \geqslant m+1$ и $q_1 > 1$. Тогда по предположению индукции

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

По равенству (4.5) имеем, что $g(d, m) = g(d-1, m)$. Также

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

значит,

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

Следовательно, получаем неравенство

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

в) $r = 0$, $r_1 > 0$.

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 $r_1 \leqslant m < m^l$ и при $l \geqslant 3$ также $r_1 < m^{l-1}$. Имеем

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

$$g(d - r_1 - 1, m) = (m-1)l + (q-1) - 1 \ \text{ при } \ q > 1,$$

$$g(d - r_1 - 1, m) = (m-1)(l-1) + m - 1 - 1 = (m-1)l + (q-1) - 1 \ \text{ при } \ q_1 = 1.$$

Значит,

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

В доказательстве пункта 1б) было получено, что $g(d - r_1, m + 1) = g(d - r_1 - 1, m+1) + 1$. Используя равенство (4.5), получаем, что

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

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

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

2. $s \geqslant 2$.

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

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

Тогда по предположению индукции $g(d_0, m) \leqslant g(d_0, m+1)$. Из равенства (4.5) выводим, что

$$g(d,m) = g(d_0, m), \quad g(d, m+1) = g(d_0, m+1).$$

Следовательно,

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

б) $r > 0$, $r_1 = 0$. При $s \geqslant 2$ верно, что $d > m+1$, $d - 1 \geqslant m+1$. Тогда по предположению индукции $g(d-1, m) \leqslant g(d-1, m+1)$. Из равенства (4.5) выводим, что $g(d,m) = g(d-1, m)$. Также имеем

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

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

значит,

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

Следовательно, получаем неравенство

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

в) $r = 0$, $r_1 > 0$. Обозначим $d_0 = d/m \in \mathbb{N}$. Поскольку в данном случае $d > (m+1)^2$, то $d_0 > m+1$. Число d_0 представляется в виде

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

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

$$g(d_0,m) = (m-1)(l-1) + q - 1 \leqslant mt + q_0 - 1 = g(d_0, m+1). \tag{4.6}$$

Прибавим $m-1$ к обеим частям неравенства (4.6), получаем неравенство

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

или, что эквивалентно,

$$g(d,m) \leqslant m(t+1) + (q_0-1) - 1. \tag{4.7}$$

По определению чисел d_0 и d имеем

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

и

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

Как показано в теореме 4.43, при фиксированном значении $m+1$ справедлива оценка

$$g(q_0 m(m+1)^t, m+1) \leqslant g(d, m+1). \tag{4.8}$$

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

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

при $2 \leqslant q_0 \leqslant m$ разделим $q_0 m$ на $m+1$ с остатком, получим

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

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 (4.7). Теперь из неравенств (4.7) и (4.8) получаем требуемую оценку

$$g(d,m) \leqslant g(q_0 m(m+1)^t, m+1) \leqslant g(d, m+1). \qquad \square$$

Теперь сформулируем вспомогательные комбинаторные результаты, которые понадобятся нам в дальнейшем.

Лемма 4.45. *Пусть* $l, m, q \in \mathbb{N}$, $m \geqslant 2$, $1 \leqslant q \leqslant m-1$. *Положим* $N = (m-1)l + q$. *Рассмотрим множество* $\mathcal{X} \subseteq \mathbb{Z}^N$, *состоящее из всех строк* $X = (x_1, \ldots, x_N)$, *удовлетворяющих условиям*

$$0 \leqslant x_N \leqslant x_{N-1} \leqslant \ldots \leqslant x_2 \leqslant x_1 \leqslant m-1$$

и

$$\sum_{i=1}^{N} x_i = N.$$

Рассмотрим функцию

$$F\colon \mathcal{X} \to \mathbb{Z}, \quad F(X) = \prod_{i=1}^{N} (x_i + 1).$$

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

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

причём минимум достигается на наборе $X = (x_1, \ldots, x_n)$ *вида*

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

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

Пусть $m > 2$. Поскольку множество $\mathcal{X}$ конечно, существует строка $Y = (y_1, \ldots, y_N) \in \mathcal{X}$, такая что $F(Y) = \min\limits_{X \in \mathcal{X}} F(X)$. Покажем, что Y не может содержать двух координат y_p и y_t, $1 \leqslant p < t \leqslant N$, одновременно удовлетворяющих неравенству $0 < y_i < m-1$.

Предположим противное. Пусть для некоторых $1 \leqslant p < t \leqslant N$ выполнено

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

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

$$F_0(y) = (y+1)(s-y+1) \prod_{\substack{i=1,\\ i \neq p,t}}^{N} (y_i+1) = (y+1)(s-y+1) \cdot P'.$$

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

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

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

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

$$F(Y) = F_0(y_t) = z(y_t)P' > z(0)P' = F_0(0) = F\bigl(X(0)\bigr),$$

что противоречит выбору Y.

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

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

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

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

что противоречит выбору Y. Следовательно, для некоторых $\varepsilon, r, y \in \mathbb{Z}$, $0 \leqslant r \leqslant \leqslant N$, $1 \leqslant y \leqslant m-2$, $\varepsilon = 0, 1$, строка Y удовлетворяет соотношениям

$$y_1 = \ldots = y_r = m-1, \quad y_{r+1} = \varepsilon y, \quad y_{r+2} = \ldots = y_N = 0.$$

Из условия $Y \in \mathcal{X}$ выводим, что

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

откуда при $q \leqslant m-2$ получаем, что $\varepsilon y = q$, $r = l$, значит, $y = q$. При $q = m-1$ получаем, что $\varepsilon y = 0$ и $r = l+1$. Значит, в обоих случаях справедливы соотношения

$$y_1 = \ldots = y_l = m-1, \quad y_{l+1} = q, \quad y_{l+2} = \ldots = y_N = 0.$$

Тогда

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

Здесь и далее лексикографический порядок понимается в смысле определения 2.20.

Предложение 4.46. *Пусть* $k \in \mathbb{N}$, $X = (x_1,\dots,x_k) \in \mathbb{Z}_+^k$, $X \neq (0,\dots,0)$ *и* $x_1 \geqslant x_2 \geqslant \ldots \geqslant x_k$. *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* $Y'' \overset{\text{lex}}{>} X''$. *Положим* $Y = X' + Y''$. *Пусть перестановка* $\varphi \in \mathrm{S}_k$ *такая, что* $y_{\varphi(1)} \geqslant y_{\varphi(2)} \geqslant \ldots \geqslant y_{\varphi(k)}$. *Обозначим* $Y_\varphi = \big(y_{\varphi(1)}, y_{\varphi(2)},\dots,y_{\varphi(k)}\big)$. *Тогда* $X \overset{\text{lex}}{<} Y_\varphi$.

Доказательство. По условию $X'' \overset{\text{lex}}{<} Y''$. Прибавим X' к обеим частям сравнения, получим $X = X' + X'' \overset{\text{lex}}{<} X' + Y'' = Y$. При упорядочивании справедливо $Y \overset{\text{lex}}{\leqslant} Y_\varphi$. Следовательно, $X \overset{\text{lex}}{<} Y_\varphi$. $\square$

Замечание 4.47. Из коммутативности алгебры $\mathcal{A}$ следует, что для произвольных слов $v, w \in \mathcal{S}^*$ свойство $w \in \wp_I(v)$ влечёт равенство элементов v и w как элементов алгебры. Поэтому в дальнейшем, говоря о слове $v \in \mathcal{S}^*$, будем рассматривать класс эквивалентности $\wp_I(v)$, заданный представителем вида

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

Определение 4.48. Пусть $v = a_1^{i_1} a_2^{i_2} \cdots a_k^{i_k} \in \mathcal{S}^*$. *Подсловом* слова v называется любое слово $w = a_1^{j_1} a_2^{j_2} \cdots a_k^{j_k} \in \mathcal{S}^*$, удовлетворяющее условиям $j_s \leqslant i_s$ для любого $s = 1, \ldots, k$.

Лемма 4.49. *Пусть $\mathbb{F}$ — произвольное поле, $k, M \in \mathbb{N}$, $k, M \geqslant 2$. Пусть $\mathcal{A}$ — ассоциативная конечномерная коммутативная $\mathbb{F}$-алгебра и $\mathcal{S} = \{a_1, \ldots, a_k\} \subseteq \subseteq \mathcal{A}$ — некоторое подмножество. Пусть $v \in \mathcal{S}^M \setminus \mathcal{S}^{M-1}$ — несократимое слово и множество всех подслов v длины, не большей $M-1$, линейно зависимо. Тогда существуют $n \in \mathbb{N}$, $w \in \mathcal{L}_{M-1}(\mathcal{S})$, $u_1, \ldots, u_n \in \mathcal{S}^M \setminus \mathcal{S}^{M-1}$ и $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$, такие что*

1) *для всех $1 \leqslant s \leqslant n$ слово u_s несократимо;*
2) *для всех $1 \leqslant s \leqslant n$ выполнено $v \overset{I_0}{<} u_s$;*
3) $v = \sum\limits_{i=1}^{n} \alpha_i u_i + w$.

Доказательство. По условию о линейной зависимости существуют такие подслова $v_1, \ldots, v_p$ слова v и $\beta_1, \ldots, \beta_p \in \mathbb{F}$, все неравные нулю, что

$$\sum_{j=1}^{p} \beta_j v_j = 0. \tag{4.9}$$

Если $p = 1$, то $v_1 = 0$. Тогда $v = 0$ — противоречие с несократимостью v. Следовательно, $p \geqslant 2$. Не ограничивая общности, можно считать, что подслова $v_1, \ldots, v_p$ упорядочены так, что их длины не возрастают.

Пусть t обозначает максимум из длин $v_1, \ldots, v_p$, $1 \leqslant t \leqslant M-1$, и $v_1, \ldots, v_r$ имеют длину t, $v_{r+1}, \ldots, v_p$ — длины не более $t-1$. Если $r = 1$, то из равенства (4.9) получаем, что

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

т. е. v_1 сократимо. Тогда и v сократимо — противоречие. Значит, $r \geqslant 2$.

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

Упорядочим переменные следующим образом: $a_{\tau(1)} > a_{\tau(2)} > \ldots > a_{\tau(k)}$. Тогда слова из множества $\mathcal{S}^t \setminus \mathcal{S}^{t-1}$ упорядочим лексикографически. Существует такая подстановка $\sigma \in \mathrm{S}_r$, что

$$v_{\sigma(1)} \overset{\text{lex}}{<} v_{\sigma(2)} \overset{\text{lex}}{<} \ldots \overset{\text{lex}}{<} v_{\sigma(r)}.$$

Тогда ввиду равенства (4.9)

$$v_{\sigma(1)} = -\beta_{\sigma(1)}^{-1} \sum_{\substack{j=1,\\ j \neq \sigma(1)}}^{p} \beta_j v_j = \sum_{\substack{j=1,\\ j \neq \sigma(1)}}^{r} \beta'_j v_j + V_{t-1}, \tag{4.10}$$

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

По определению 4.48 существует $v' \in \mathcal{S}^{(M-t)} \setminus \mathcal{S}^{(M-t)-1}$, для которого
$$v = v' \cdot v_{\sigma(1)}. \tag{4.11}$$
Подставив в равенство (4.11) выражение для $v_{\sigma(1)}$, найденное в (4.10), получим
$$v = \sum_{\substack{j=1,\\ j\neq\sigma(1)}}^{r} \beta'_j v' v_j + V_{M-1}, \tag{4.12}$$
где $V_{M-1} \in \mathcal{L}_{M-1}(\mathcal{S})$.

Обозначим $K = \{1,\ldots,r\} \setminus \{\sigma(1)\}$. Пусть $K_1 \subseteq K$ — 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 (4.12) следует, что $v \in \mathcal{L}_{M-1}(\mathcal{S})$, т. е. v сократимо. Противоречие.

Положим $n = |K_1|$, $K_1 = \{k_1,\ldots,k_n\}$, $u_j = v'v_{k_j}$, $\alpha_j = \beta'_{k_j}$, $j = 1,\ldots,n$, и $w = \sum\limits_{s\in K_2} \beta'_s v' v_s + V_{M-1}$. По лемме 4.46 при всех j получаем $I_0(v) < I_0(u_j)$. $\square$

Лемма 4.50. *Пусть $\mathbb{F}$ — произвольное поле. Пусть $\mathcal{A}$ — ассоциативная конечномерная коммутативная $\mathbb{F}$-алгебра с единицей и $\mathcal{S} = \{a_1,\ldots,a_k\} \subseteq \mathcal{A}$ — система порождающих. Пусть также $m(\mathcal{S}) = m \geqslant 2$ и $\dim\mathcal{A} = qm^l + r$, $l \in \mathbb{N}$, $0 \leqslant r < m^l$, $1 \leqslant q \leqslant m-1$. Положим $N = (m-1)l + q$. Тогда любое слово $v \in \mathcal{S}^N \setminus \mathcal{S}^{N-1}$ сократимо.*

Доказательство. Предположим, что существует несократимое слово $v' \in \mathcal{S}^N \setminus \mathcal{S}^{N-1}$. Приведём это утверждение к противоречию.

Рассмотрим отображение $T\colon I_0(\mathcal{S}^N \setminus \mathcal{S}^{N-1}) \to \mathbb{Z}_+^N$, такое что
$$T\bigl((x_1,\ldots,x_k)\bigr) = \begin{cases} (x_1,\ldots,x_k,0,\ldots,0) & \text{при } k < N,\\ (x_1,\ldots,x_k) & \text{при } k = N,\\ (x_1,\ldots,x_N) & \text{при } k > N. \end{cases}$$

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 $(N+1)$-й по k-ю нулевые. Следовательно, отображение T биективно.

Обозначим через $\mathcal{T}_2$ подмножество тех строк $(y_1,\ldots,y_N)$ из $\operatorname{Im}T$, у которых $y_1 \geqslant m$, положим $\mathcal{T}_1 = \operatorname{Im}T \setminus \mathcal{T}_2$.

Если $T\bigl(I_0(v)\bigr) \in \mathcal{T}_2$, то v содержит m-ю степень элемента из $\mathcal{S}$ и будет сократимо по определению m.

Следовательно, $T\bigl(I_0(v')\bigr) \in \mathcal{T}_1$. Заметим, что $\mathcal{T}_1 \subseteq \mathcal{X}$, где $\mathcal{X}$ — множество, определённое в лемме 4.45. $(\mathcal{X}, \overset{\mathrm{lex}}{\leqslant})$ — конечное линейно упорядоченное множество. Значит, существует несократимое слово $v'' \in \mathcal{S}^N \setminus \mathcal{S}^{N-1}$, такое что любое слово $w \in \mathcal{S}^N \setminus \mathcal{S}^{N-1}$, удовлетворяющее условию $w \overset{I_0}{>} v''$, сократимо.

Получаем, что v'' — несократимое слово и для него не выполнено утверждение леммы 4.49. Это означает, что оно не удовлетворяет условию леммы 4.49 о линейной зависимости подслов. Следовательно, множество всех подслов слова v'' длины, не большей $N-1$, линейно независимо.

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

$$M = \prod_{i=1}^{k} (\#_i(v'') + 1) = \prod_{j=1}^{N} (x''_j + 1) = F\Big(T\big(I_0(v'')\big)\Big), \tag{4.13}$$

где F — функция, определённая в лемме 4.45. Соотношение (4.13) и лемма 4.45 дают оценку

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

С другой стороны, из несократимости слова v'' выводим оценку

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

Полученное противоречие доказывает лемму. □

Как следствие получаем верхнюю оценку для длины системы порождающих.

Следствие 4.51. *Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{A}$ — ассоциативная конечномерная коммутативная $\mathbb{F}$-алгебра с единицей и $\mathcal{S}$ — система порождающих алгебры $\mathcal{A}$. Пусть*

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

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

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

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

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

$$[m^{\{\log_m d\}}] = [m^{\log_m d - [\log_m d]}] = \left[\frac{d}{m^l}\right] = q$$

и

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

По лемме 4.50 получаем, что все слова из $\mathcal{S}^{(g(d,m)+1)} \setminus \mathcal{S}^{(g(d,m)+1)-1}$ сократимы, следовательно, $l(\mathcal{S}) \leqslant g(d,m)$. □

Докажем основную теорему.

Теорема 4.52. *Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{A}$ — ассоциативная конечномерная коммутативная $\mathbb{F}$-алгебра с единицей. Пусть*

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

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

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 $m\geqslant 2$. Пусть $\mathcal{S}$ — произвольная система порождающих алгебры $\mathcal{A}$. По определению $m(\mathcal{S})\leqslant m$, и значит, по теореме 4.5

$$g\big(d,m(\mathcal{S})\big)\leqslant g(d,m). \tag{4.14}$$

Оценка (4.14) справедлива для любой системы порождающих, следовательно,

$$l(\mathcal{A})=\max_{\mathcal{S}} l(\mathcal{S})\leqslant\max_{\mathcal{S}} g\big(d,m(\mathcal{S})\big)\leqslant\max_{\mathcal{S}} g(d,m)=g(d,m). \qquad \square$$

Следствие 4.53. *Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{A}$ — ассоциативная конечномерная $\mathbb{F}$-алгебра с единицей. Пусть $\mathcal{S}=\{a_1,\ldots,a_k\}$ — такая система порождающих алгебры $\mathcal{A}$, что для всех $1\leqslant i<j\leqslant k$ верно*

$$a_ia_j-a_ja_i\in\mathcal{L}_1(\mathcal{S}).$$

Пусть

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

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

4.5. Сравнение с другими оценками

Покажем, что для коммутативных алгебр оценка длины, полученная в теореме 4.52, лучше общей оценки длины из теоремы 1.3.

Теорема 4.54. *Пусть $d,m\in\mathbb{N}$, $d\geqslant m\geqslant 2$ 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

$$g(d,m)<f(d,m). \tag{4.15}$$

Доказательство. Число d единственным образом представляется в виде $d=qm^l+r$, где $l\in\mathbb{N}$, $0\leqslant r<m^l$, $1\leqslant q\leqslant m-1$. 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. $l = 1$. Имеем $g(d, m) = m + q - 2$ и

$$f(d, m) = m\sqrt{\frac{2(qm + r)}{m - 1}} + \frac{m}{2} - 2 \geqslant m\sqrt{\frac{2qm}{m - 1} + \frac{1}{4}} + \frac{m}{2} - 2. \tag{4.16}$$

Из неравенства (4.16) следует, что для проверки условия $g(d, m) < f(d, m)$ достаточно показать, что

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

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

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

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

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

или

$$\frac{q}{m - 1}(m^3 - m^2 + (1 - q)m + q^2) > 0. \tag{4.17}$$

Таким образом, осталось доказать, что выполнено неравенство (4.17).

Рассмотрим функцию

$$h\colon \mathbb{R} \to \mathbb{R}, \quad h(x) = x^3 - x^2 + (1 - q)x + q.$$

Имеем

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

при $q \in \mathbb{N}$ верно $3q - 2 > 0$, $h'(x) = 0$ 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 $\big((1 + \sqrt{3q - 2})/3, +\infty\big)$. Отметим, что при $q \in \mathbb{N}$ выполнено неравенство $(1 + \sqrt{3q - 2})/3 < q$, поэтому $h(x)$ возрастает и на $[q, +\infty)$. Поскольку при этом $h(q) = q^3 - 2q^2 + 2q = q\big((q - 1)^2 + 1\big) > 0$ при $q > 0$, то $h(x) > 0$ при $x \geqslant q$. По условию $q \leqslant m - 1$, $q > 0$ и $m - 1 > 0$, значит, $h(m) > h(q) > 0$ и

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

Таким образом, неравенство (4.17) выполнено.

2. $l \geqslant 2$. Оценим $f(d, m)$ снизу:

$$f(d, m) > m\sqrt{\frac{2(qm^l + r)}{m - 1}} + \frac{m}{2} - 2 > m\sqrt{\frac{2(qm^l)}{m}} + \frac{m}{2} - 2 \geqslant \sqrt{2}m^{(l+1)/2} - 1. \tag{4.18}$$

Оценим $g(d, m)$ сверху:

$$g(d, m) \leqslant l(m - 1) + m - 1 - 1 = (l + 1)(m - 1) - 1. \tag{4.19}$$

Рассмотрим функцию

$$\delta\colon [2,+\infty)\to\mathbb{R},\quad \delta(x)=\sqrt{2}x^{(l+1)/2}-(l+1)(x-1).$$

Имеем

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

Поскольку $x\geqslant 2$ и $l\geqslant 2$, то $x^{(l-1)/2}\geqslant x^{1/2}\geqslant\sqrt{2}$. Следовательно,

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

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

Теперь рассмотрим функцию

$$h\colon [2,+\infty)\to\mathbb{R},\quad h(l)=\sqrt{2}\cdot 2^{(l+1)/2}-(l+1)=2\cdot 2^{l/2}-(l+1).$$

Имеем

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

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

Из неравенств (4.18) и (4.19) получаем, что

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

Точность оценки из теоремы 4.52 будет показана в разделе 4.6. С другой стороны, неравенство в теореме 4.52 может быть строгим.

Предложение 4.55. *Над произвольным полем $\mathbb{F}$ существуют коммутативная $\mathbb{F}$-алгебра $\mathcal{A}$ произвольной размерности $\dim\mathcal{A}\geqslant 4$, для которой $l(\mathcal{A})<g\big(\dim\mathcal{A},m(\mathcal{A})\big)$.*

Доказательство. Рассмотрим подалгебру $\mathcal{A}=\mathcal{A}_1\subseteq \mathrm{M}_n(\mathbb{F})$, $n\geqslant 2$, из примера 4.7. Для неё справедливы равенства $\dim\mathcal{A}_1=n$, $m(\mathcal{A}_1)=2$ и $l(\mathcal{A}_1)=1$. Следовательно, при $n\geqslant 4$ получаем, что

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

Покажем, что при некоторых ограничениях на значения размерности оценка длины для коммутативных подалгебр в $\mathrm{M}_n(\mathbb{F})$, полученная в теореме 4.52, также лучше общей оценки длины из следствия 4.39.

Предложение 4.56. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}\subset\mathrm{M}_n(\mathbb{F})$ — коммутативная подалгебра. Тогда*

1) *если $m(\mathcal{A})=n$, то $l(\mathcal{A})=g\big(\dim\mathcal{A},m(\mathcal{A})\big)=n-1$;*
2) *если $m(\mathcal{A})=n-1$ и $\dim\mathcal{A}\leqslant 2n-3$, то $l(\mathcal{A})\leqslant g\big(\dim\mathcal{A},m(\mathcal{A})\big)\leqslant n-2$;*
3) *если $m(\mathcal{A})\leqslant n-2$ и $\dim\mathcal{A}\leqslant 2n-5$, то $l(\mathcal{A})\leqslant g\big(\dim\mathcal{A},m(\mathcal{A})\big)\leqslant n-3$.*

Доказательство. При $m(\mathcal{A}) = n$ равенства $\dim \mathcal{A} = n$ и $l(\mathcal{A}) = n-1$ следуют из леммы 4.5. В этом случае также $g\big(\dim \mathcal{A}, m(\mathcal{A})\big) = g(n,n) = n-1 = l(\mathcal{A})$.

При $m(\mathcal{A}) = n-1$ и $\dim \mathcal{A} \leqslant 2n-3$ по теореме 4.43 получаем оценку

$$l(\mathcal{A}) \leqslant g\big(\dim(\mathcal{A}), m(\mathcal{A})\big) \leqslant g(2n-3, n-1) = (n-2)\cdot 1 + 1 - 1 = n-2.$$

При $m(\mathcal{A}) \leqslant n-2$ и $\dim \mathcal{A} \leqslant 2n-5$ по теоремам 4.43 и 4.44 получаем оценку

$$l(\mathcal{A}) \leqslant g\big(\dim(\mathcal{A}), m(\mathcal{A})\big) \leqslant g\big(2n-5, m(\mathcal{A})\big) \leqslant \\ \leqslant g(2n-5, n-2) = (n-3)\cdot 1 + 1 - 1 = n-3. \quad \square$$

Замечание 4.57. Отметим, что множества алгебр из пунктов 2) и 3) не пусты. Например, рассмотрим следующее семейство алгебр: пусть

$$C_k = \sum_{i=1}^{k-1} E_{i,i+1} \in \mathrm{M}_k(\mathbb{F}),$$

$r, n \in \mathbb{N}$, $r \geqslant 3$, $n_1 \geqslant n_2 \geqslant \ldots \geqslant n_r \in \mathbb{N}$, $n = n_1 + \ldots + n_r$, $\mathcal{C}_j \subset \mathrm{M}_{n_j}(\mathbb{F})$ — подалгебра, порождённая матрицами E, C_{n_j}, $j = 1, \ldots, r$. Положим

$$\mathcal{C} = \bigoplus_{j=1}^{r} \mathcal{C}_j \subset \mathrm{M}_n(\mathbb{F}).$$

Тогда

1) $m(\mathcal{C}) = n$ при $|\mathbb{F}| \geqslant r$,
2) $m(\mathcal{C}) = n-1$ при $|\mathbb{F}| = r-1$ и $n_r = 1$,
3) $m(\mathcal{C}) \leqslant n-2$ при $|\mathbb{F}| \leqslant r-2$.

Для локальных алгебр теорема 4.52 не даёт существенных улучшений относительно следствия 3.32, как показывает следующее утверждение.

Предложение 4.58. *Пусть $N \in \mathbb{N}$, $\mathbb{F}$ — поле характеристики $p > N$ или характеристики 0. Пусть $\mathcal{A}$ — конечномерная коммутативная локальная $\mathbb{F}$-алгебра с единицей. Пусть $J(\mathcal{A})$ — радикал Джекобсона алгебры $\mathcal{A}$, индекс нильпотентности $J(\mathcal{A})$ равен N. Тогда $l(\mathcal{A}) \leqslant N-1 \leqslant g\big(\dim \mathcal{A}, m(\mathcal{A})\big)$, причём при $\dim \mathcal{A} \geqslant 2N$ неравенство строгое: $N-1 < g\big(\dim \mathcal{A}, m(\mathcal{A})\big)$.*

Доказательство. По определению индекса нильпотентности радикала и согласно основной теореме об эквивалентности различных определений локальности (см. [11, § 5.2]) $m(\mathcal{A}) \leqslant N$. С другой стороны, при данных ограничениях на поле существует элемент $a \in \mathcal{A}$, такой что $\deg a = N$ (см., например, [12, гл. 1, следствие предложения 5]). Следовательно, $m(\mathcal{A}) = N$.

Из явного вида функции $g(d,m)$ видно, что $g(\dim \mathcal{A}, N) = N-1$ при $N \leqslant \dim \mathcal{A} \leqslant 2N-1$ и $g(2N,N) = N$. Тогда по теореме 4.43 при $\dim \mathcal{A} \geqslant 2N$ получаем оценку

$$g(\dim \mathcal{A}, N) \geqslant g(2N, N) = N > N-1. \quad \square$$

Пример 4.59. Пусть $\mathbb{F}$ — поле характеристики $p > 0$, и пусть $k \in \mathbb{N}$, $k > p$. Пусть $\mathbb{F}[X_1, \ldots, X_k]$ — алгебра многочленов от k коммутирующих переменных. Положим $I_p = (X_1^p, \ldots, X_k^p) \lhd \mathbb{F}[X_1, \ldots, X_k]$ и рассмотрим фактор-алгебру $\mathcal{A} = \mathbb{F}[X_1, \ldots, X_k]/I_p$. В алгебре $\mathcal{A}$ возьмём идеал $I = (X_1^{p-1} \cdots X_k^{p-1} + I_p)$ и положим $\mathcal{B}_{p,k} = \mathcal{A}/I$. По построению $\mathcal{B}_{p,k}$ является коммутативной локальной алгеброй с единицей размерности $\dim \mathcal{B}_{p,k} = p^k - 1$, $m(\mathcal{B}_{p,k}) = p$, индекс нильпотентности радикала равен $N = k(p-1) > p = m(\mathcal{B}_{p,k})$. Таким образом,

$$\dim \mathcal{B}_{p,k} - 1 > N - 1 = (p-1)k - 1 = (p-1)\log_p p^{k-1} + (p-1) - 1 = \\ = g\big((p-1)p^{k-1} + p^{k-1} - 1, p\big) = g\big(\dim \mathcal{B}_{p,k}, m(\mathcal{B}_{p,k})\big).$$

Следовательно, для алгебры $\mathcal{B}_{p,k}$ оценки длины из теоремы 4.52 и следствия 3.32 совпадают и улучшают тривиальную оценку $l(\mathcal{B}_{p,k}) \leqslant \dim \mathcal{B}_{p,k} - 1$.

4.6. О длине алгебры диагональных матриц

Теорема 4.60. *Пусть $\mathbb{F}$ — произвольное поле.*

1. *Если $\mathbb{F}$ бесконечно, то $l\big(\mathrm{D}_n(\mathbb{F})\big) = n - 1$.*
2. *Справедливо*

$$l\big(\mathrm{D}_n(\mathbb{F}_q)\big) = \begin{cases} n-1 & \text{при } q \geqslant n, \\ (q-1)[\log_q n] + [q^{\{\log_q n\}}] - 1 & \text{при } q < n. \end{cases}$$

Доказательство. Заметим, что если поле $\mathbb{F}$ бесконечно, то $m\big(\mathrm{D}_n(\mathbb{F})\big) = n = \dim \mathrm{D}_n(\mathbb{F})$, и утверждение 1 теоремы следует из леммы 4.34.

Пусть $\mathbb{F} = \mathbb{F}_q$. В этом случае $\dim \mathrm{D}_n(\mathbb{F}_q) = n$ и $m\big(\mathrm{D}_n(\mathbb{F}_q)\big) = \min(n, q)$. 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

$$l\big(\mathrm{D}_n(\mathbb{F}_q)\big) \leqslant g\Big(\dim \mathrm{D}_n(\mathbb{F}_q), m\big(\mathrm{D}_n(\mathbb{F}_q)\big)\Big)$$

следует из теоремы 4.52.

Докажем нижнюю оценку

$$l\big(\mathrm{D}_n(\mathbb{F}_q)\big) \geqslant g\big(n, \min(n,q)\big)$$

индукцией по n.

База индукции. При $n = 1, \ldots, q$ утверждение следует из леммы 4.34.

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

$$\mathrm{D}_{ab}(\mathbb{F}) \cong \mathrm{D}_a(\mathbb{F}) \otimes_{\mathbb{F}} \mathrm{D}_b(\mathbb{F}), \quad \mathrm{D}_{a+b}(\mathbb{F}) \cong \mathrm{D}_a(\mathbb{F}) \oplus \mathrm{D}_b(\mathbb{F}). \tag{4.20}$$

Тогда по теореме 3.9 для любых $t > s$ получаем

$$l\big(\mathrm{D}_t(\mathbb{F})\big) = l\big(\mathrm{D}_{s+(t-s)}(\mathbb{F})\big) = l\big(\mathrm{D}_s(\mathbb{F}) \oplus \mathrm{D}_{t-s}(\mathbb{F})\big) \geqslant \\ \geqslant \max\big\{l\big(\mathrm{D}_s(\mathbb{F})\big), l\big(\mathrm{D}_{t-s}(\mathbb{F})\big)\big\} \geqslant l\big(\mathrm{D}_s(\mathbb{F})\big). \tag{4.21}$$

1. Пусть $n = q^l$, $l \geqslant 2$. Из равенства (4.20) и предложения 3.23 получаем

$$l\big(\mathrm{D}_{q^l}(\mathbb{F}_q)\big) = l\big(\mathrm{D}_q(\mathbb{F}_q) \otimes \mathrm{D}_{q^{l-1}}(\mathbb{F}_q)\big) \geqslant l\big(\mathrm{D}_q(\mathbb{F}_q)\big) + l\big(\mathrm{D}_{q^{l-1}}(\mathbb{F}_q)\big). \qquad (4.22)$$

Тогда, используя предположение индукции и (4.3), получаем

$$l\big(\mathrm{D}_q(\mathbb{F}_q)\big) + l\big(\mathrm{D}_{q^{l-1}}(\mathbb{F}_q)\big) \geqslant g(q,q) + g(q^{l-1},q) = g(q^l,q).$$

2. Пусть $n = kq^l$, где $2 \leqslant k \leqslant q-1$, $l \geqslant 1$. Из равенств (4.4) и (4.20), неравенства (4.22) и предложения 3.23 получаем

$$l\big(\mathrm{D}_{kq^l}(\mathbb{F}_q)\big) = l\big(\mathrm{D}_k(\mathbb{F}_q) \otimes \mathrm{D}_{q^l}(\mathbb{F}_q)\big) \geqslant l\big(\mathrm{D}_k(\mathbb{F}_q)\big) + l\big(\mathrm{D}_{q^l}(\mathbb{F}_q)\big) \geqslant$$
$$\geqslant g(k,k) + g(q^l,q) = g(kq^l,q). \qquad (4.23)$$

3. Пусть $n = kq^l + r$, где $0 < r < q^l$, $1 \leqslant k \leqslant q-1$, $l \geqslant 1$. Используя равенство (4.5), неравенства (4.21) и (4.23), получаем

$$l\big(\mathrm{D}_{kq^l+r}(\mathbb{F}_q)\big) \geqslant l\big(\mathrm{D}_{kq^l}(\mathbb{F}_q)\big) \geqslant g(kq^l,q) = g(kq^l+r,q). \qquad \square$$

Следствие 4.61. *Верхняя оценка длины коммутативной алгебры в теореме 4.52 является точной для любого значения* $\dim \mathcal{A}$ *и бесконечного множества значений* $m(\mathcal{A})$.

Следствие 4.62. *Пусть* $\mathbb{F}$ *— произвольное поле и* $\mathcal{A}$ *— такая подалгебра алгебры* $\mathrm{T}_n(\mathbb{F})$, *что* $\{\mathrm{diag}(a_{1,1},\ldots,a_{n,n}) \mid A = (a_{i,j}) \in \mathcal{A}\} = \mathrm{D}_n(\mathbb{F})$. *Тогда* $l(\mathcal{A}) \geqslant l\big(\mathrm{D}_n(\mathbb{F})\big)$, *в частности, если* $|\mathbb{F}| \geqslant n$, *то* $l(\mathcal{A}) = n-1$.

Доказательство. Пусть $\mathcal{S}$ — система порождающих алгебры $\mathrm{D}_n(\mathbb{F})$ длины $l(\mathcal{S}) = l\big(\mathrm{D}_n(\mathbb{F})\big)$, и пусть $N_1,\ldots,N_t$ — базис для $\mathcal{A} \cap \mathrm{N}_n(\mathbb{F})$. Пусть $\mathcal{S}_{\mathcal{A}} = \mathcal{S} \cup \{N_1,\ldots,N_t\}$. Так как для любых матриц $D \in \mathrm{D}_n(\mathbb{F})$ и $N \in \mathrm{N}_n(\mathbb{F})$ справедливо $DN, ND \in \mathrm{N}_n(\mathbb{F})$, то $l(\mathcal{S}_{\mathcal{A}}) = l(\mathcal{S}) = l\big(\mathrm{D}_n(\mathbb{F})\big)$. Следовательно, $l(\mathcal{A}) \geqslant l(\mathcal{S}_{\mathcal{A}}) = l\big(\mathrm{D}_n(\mathbb{F})\big)$. $\square$

Следствие 4.63. *Пусть* $\mathbb{F}$ *— конечное поле. Тогда существуют алгебра* $\mathcal{A}_{\mathbb{F}}$ *и расширение* $\mathbb{K}$ *поля* $\mathbb{F}$ *такие, что* $l(\mathcal{A}_{\mathbb{F}} \otimes \mathbb{K}) > l(\mathcal{A}_{\mathbb{F}})$.

Доказательство. Пусть $|\mathbb{F}| = q$. Положим $n = q^2$, $\mathcal{A}_{\mathbb{F}} = \mathrm{D}_n(\mathbb{F})$. Тогда $l(\mathcal{A}_{\mathbb{F}}) = 2(q-1) < q^2 - 1 = n-1$, поскольку $q+1 > 2$.

Если степень расширения $\mathbb{K}$ больше или равна 2, то $|\mathbb{K}| \geqslant q^2 = n$ и $l(\mathcal{A}_{\mathbb{K}}) = l\big(\mathrm{D}_n(\mathbb{K})\big) = n-1 > l(\mathcal{A}_{\mathbb{F}})$. $\square$

Следствие 4.63 показывает, что неравенство из предложения 3.19 может быть строгим.

5. Связь длины алгебры с длиной её подалгебр

Пусть $\mathcal{A}$ — конечномерная ассоциативная алгебра над произвольным полем $\mathbb{F}$. В ряде вычислительных задач требуется оценить длину произвольного подмножества $\mathcal{S}'$ в алгебре $\mathcal{A}$, которое может порождать не всю алгебру, а её собственную подалгебру $\mathcal{A}' \subset \mathcal{A}$, или, что эквивалентно, найти такое число $M \in \mathbb{N}$, что для любой подалгебры $\mathcal{A}' \subseteq \mathcal{A}$ будет справедлива оценка $l(\mathcal{A}') \leqslant M$.

Заметим, что такие характеристики алгебры $\mathcal{A}$, как размерность и максимальная степень минимального многочлена элемента, не возрастают при переходе к подалгебрам. Поэтому ввиду тривиальной оценки длины $l(\mathcal{A}') \leqslant \dim \mathcal{A}' - 1$ всегда можно взять $M = \dim \mathcal{A} - 1$. В более общем случае, если удаётся получить верхнюю оценку длины алгебры вида $l(\mathcal{A}) \leqslant h\big(\dim \mathcal{A}, m(\mathcal{A})\big)$, где функция $h(x, y)\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ является неубывающей по каждой переменной, также для любой подалгебры $\mathcal{A}' \subseteq \mathcal{A}$ верно $l(\mathcal{A}') \leqslant h\big(\dim \mathcal{A}', m(\mathcal{A}')\big) \leqslant h\big(\dim \mathcal{A}, m(\mathcal{A})\big)$.

Но тривиальная оценка может не быть точной. Например, если взять $\mathcal{A} = \mathrm{T}_n(\mathbb{F})$, то согласно теореме 3.12 для любой подалгебры $\mathcal{A}' \subseteq \mathcal{A}$ справедлива оценка $l(\mathcal{A}') \leqslant n - 1 = l(\mathcal{A})$, при этом $\dim \mathcal{A} = n(n+1)/2$, т. е. тривиальную оценку можно улучшить на порядок.

С другой стороны, произвольное подмножество всегда можно вложить в систему порождающих всей алгебры, поэтому естественно было бы предположить, что длину подалгебры можно оценить длиной любой содержащей её алгебры. Однако, как будет показано в этом разделе (пример 5.9), уже в алгебре матриц порядка 4 можно построить пример, показывающий, что функция длины может расти при переходе к подалгебрам.

Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — конечномерная ассоциативная $\mathbb{F}$-алгебра. Пусть действительнозначная функция f определена на всех подалгебрах алгебры $\mathcal{A}$.

Определение 5.1. Будем говорить, что функция f *монотонна на алгебре* $\mathcal{A}$, если для любой подалгебры $\mathcal{B} \subseteq \mathcal{A}$ выполнено $f(\mathcal{B}) \leqslant f(\mathcal{A})$.

Определение 5.2. Будем говорить, что функция f *строго монотонна на алгебре* $\mathcal{A}$, если для любой подалгебры $\mathcal{B} \subsetneq \mathcal{A}$ выполнено $f(\mathcal{B}) < f(\mathcal{A})$.

Определение 5.3. Будем говорить, что функция f *монотонна на подалгебрах алгебры* $\mathcal{A}$, если f монотонна на каждой подалгебре $\mathcal{B} \subseteq \mathcal{A}$, т. е. для любых подалгебр $\mathcal{B}' \subseteq \mathcal{B} \subseteq \mathcal{A}$ выполнено $f(\mathcal{B}') \leqslant f(\mathcal{B})$.

Определение 5.4. Будем говорить, что функция f *строго монотонна на подалгебрах алгебры* $\mathcal{A}$, если f строго монотонна на каждой подалгебре $\mathcal{B} \subseteq \mathcal{A}$, т. е. для любых подалгебр $\mathcal{B}' \subsetneq \mathcal{B} \subseteq \mathcal{A}$ выполнено $f(\mathcal{B}') < f(\mathcal{B})$.

Замечание 5.5. Заметим, что функция размерности монотонна в смысле определений 5.1—5.4, а максимальная степень минимального многочлена элемента монотонна в смысле определений 5.1 и 5.3, но не строго монотонна.

Покажем, что существует алгебра $\mathcal{A}$, такая что функция длины монотонна на $\mathcal{A}$, но не строго монотонна.

Пример 5.6. Пусть $\mathbb{F}$ — произвольное поле, $n \in \mathbb{N}$, $n \geqslant 2$, $\mathcal{A} = \mathrm{T}_n(\mathbb{F})$ и $\mathcal{B} \subseteq \mathcal{A}$ — произвольная подалгебра. По лемме 3.12 справедлива оценка $l(\mathcal{B}) \leqslant n-1$, и $n-1 = l(\mathcal{A})$ по теореме 3.13. Следовательно, функция длины монотонна на $\mathcal{A}$ в смысле определения 5.1. Рассмотрим подалгебру $\mathcal{C} \subseteq \mathcal{A}$, порождённую циклической матрицей

$$C = E + \sum_{i=1}^{n-1} E_{i,i+1}.$$

Заметим, что

$$\dim \mathcal{C} = n < \frac{n(n+1)}{2} = \dim \mathcal{A}$$

и $\mathcal{C} \neq \mathcal{A}$, но по лемме 4.5 имеем $l(\mathcal{C}) = n - 1 = l(\mathcal{A})$.

Покажем, что существует матричная подалгебра $\mathcal{A}$, такая что функция длины не монотонна на $\mathcal{A}$.

Предложение 5.7. *Пусть $\mathbb{F}$ — произвольное поле. Рассмотрим алгебру $\mathcal{A}_4 \subset \subset \mathrm{T}_4(\mathbb{F})$, порождённую как векторное пространство матрицами E, $E_{4,4}$, $E_{1,2}$, $E_{1,3}$ и $E_{2,3}$. Тогда $l(\mathcal{A}_4) = 2$.*

Доказательство. Согласно следствию 3.12 $l(\mathcal{A}_4) \leqslant 3$.

Размерность подалгебры $\mathrm{M}_4(\mathbb{F})$, порождённой одной матрицей, не больше 4, а $\dim_{\mathbb{F}} \mathcal{A}_4 = 5$. Значит, для любой системы порождающих $\mathcal{S} = \{A_1, \ldots, A_k\}$ в $\mathcal{A}_4$ справедливо $k \geqslant 2$, и если $\mathcal{S} = \{A_1, A_2\}$, то $E \notin \langle A_1, A_2 \rangle$. Рассмотрим возможные случаи.

1. Допустим, что в системе порождающих $\mathcal{S}$ найдутся три матрицы A_1, A_2, A_3, такие что $E \notin \langle A_1, A_2, A_3 \rangle$. Тогда $\dim_{\mathbb{F}} \mathcal{L}_1(\mathcal{S}) \geqslant 4$. Так как $\mathcal{S}$ — система порождающих, имеем $\dim_{\mathbb{F}} \mathcal{L}_2(\mathcal{S}) > \dim_{\mathbb{F}} \mathcal{L}_1(\mathcal{S}) \geqslant 4$. Следовательно, $\dim_{\mathbb{F}} \mathcal{L}_2(\mathcal{S}) = 5$, т. е. $l(\mathcal{S}) \leqslant 2$.

2. Рассмотрим случай $\mathcal{S} = \{A, B\}$, $E \notin \langle A, B \rangle$. По предложению 3.2 можно считать, что

$$A = \begin{pmatrix} 0 & a_{12} & a_{13} & 0 \\ 0 & 0 & a_{23} & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_{44} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & b_{12} & b_{13} & 0 \\ 0 & 0 & b_{23} & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & b_{44} \end{pmatrix}.$$

Так как $\mathcal{S}$ — система порождающих, то хотя бы один из элементов a_{44} и b_{44} отличен от нуля. Без ограничения общности можно считать, что $a_{44} \neq 0$. По предложению 3.1, рассматривая преобразование

$$A \to A, \quad B \to B - \frac{b_{44}}{a_{44}} A$$

системы порождающих алгебры $\mathcal{A}_4$ с обратимой матрицей

$$\begin{pmatrix} 1 & -b_{44}/a_{44} \\ 0 & 1 \end{pmatrix},$$

можно считать, что $b_{44} = 0$. Тогда

$$A^2 = a_{12}a_{23}E_{1,3} + a_{44}^2 E_{4,4}, \quad AB = a_{12}b_{23}E_{1,3}, \quad BA = a_{23}b_{12}E_{1,3},$$
$$B^2 = b_{12}b_{23}E_{1,3}, \quad A^3 = a_{44}^3 E_{4,4}.$$

Другие произведения матриц A и B большей или равной 3 длины равны нулю. Если $AB = BA = 0$, то $\mathcal{L}(A, B)$ — коммутативная алгебра. Следовательно, $\{A, B\}$ не является системой порождающих некоммутативной алгебры $\mathcal{A}_4$.

Следовательно, или $AB \neq 0$, или $BA \neq 0$, или выполнены оба неравенства одновременно. Тогда $E_{1,3} \in \mathcal{L}_2(\mathcal{S})$. В этом случае

$$E_{4,4} = a_{44}^{-2}(A^2 - a_{12}a_{23}E_{1,3}) \in \mathcal{L}_2(\mathcal{S}), \quad E_{1,2}, E_{1,3} \in \langle A, B, E_{1,3}, E_{4,4}\rangle \subseteq \mathcal{L}_2(\mathcal{S}).$$

Следовательно, $\mathcal{L}_2(\mathcal{S}) = \mathcal{A}_4$ и $l(\mathcal{S}) = 2$. Значит, и $l(\mathcal{A}_4) = 2$. □

Следствие 5.8. *Рассмотрим подалгебру $\mathcal{A}' \subset \mathcal{A}_4$, порождённую матрицей $A = E_{1,2} + E_{2,3} + E_{4,4}$. Тогда $l(\mathcal{A}') = 3$.*

Доказательство. Непосредственная проверка показывает, что матрица A циклическая. Тогда по лемме 3.12 имеем $l(A') = 4 - 1 = 3$. □

Пример 5.9. Пусть $\mathbb{F}$ — произвольное поле. Рассмотрим алгебру $\mathcal{A}_4 \subset \mathrm{T}_4(\mathbb{F})$, порождённую как векторное пространство матрицами E, $E_{4,4}$, $E_{1,2}$, $E_{1,3}$ и $E_{2,3}$, и подалгебру $\mathcal{A}' \subset \mathcal{A}_4$, порождённую матрицей $A = E_{1,2} + E_{2,3} + E_{4,4}$. По доказанному в предложении 5.7 и следствии 5.8 $l(\mathcal{A}_4) = 2 < 3 = l(\mathcal{A}')$.

Обобщим следствие 5.8 на случай произвольного $n \geqslant 4$.

Следствие 5.10. *Для всех $n \geqslant 4$ и для любого поля $\mathbb{F}$, в котором больше $n-4$ элементов, существуют такие подалгебры $\mathcal{A}'_n \subset \mathcal{A}_n \subset \mathrm{M}_n(\mathbb{F})$, что $l(\mathcal{A}'_n) > l(\mathcal{A}_n)$.*

Доказательство. Пусть $f_4, \ldots, f_n \in \mathbb{F}$ — различные ненулевые элементы. Рассмотрим в $\mathrm{M}_n(\mathbb{F})$ подалгебры

$$\mathcal{A}'_n = \langle\{E_{1,1} + E_{2,2} + E_{3,3}, E_{1,2}, E_{1,3}, E_{2,3}, E_{4,4}, \ldots, E_{n,n}\}\rangle,$$
$$\mathcal{A}_n = \left\langle E_{1,2} + E_{1,3} + \sum_{i=4}^{n} f_i E_{i,i}\right\rangle.$$

Тогда $\mathcal{A}'_n \subset \mathcal{A}_n$ и $l(\mathcal{A}'_n) = n - 1$, так как $E_{1,2} + E_{1,3} + \sum\limits_{i=4}^{n} f_i E_{i,i}$ — циклическая матрица. По теореме 4.60 $l\big(\mathrm{D}_{n-4}(\mathbb{F})\big) = n - 5$. Последовательное применение утверждения примера 5.9 и теоремы 3.9 о прямой сумме даёт

$$l(\mathcal{A}_n) = l\big(\mathcal{A}_4 \oplus \mathrm{D}_{n-4}(\mathbb{F})\big) \leqslant 2 + (n-5) + 1 = n - 2.$$ □

Таким образом пример 5.9 и следствие 5.8 дают положительный ответ на вопрос, может ли длина подалгебры превосходить длину содержащей её алгебры. Возникает следующий естественный вопрос: какие значения могут принимать разность и отношение длины подалгебры и длины содержащей её алгебры?

Пусть $\mathbb{F}$ — произвольное поле и $(\mathcal{A}, \mathcal{A}')$ — пара, состоящая из $\mathbb{F}$-алгебры $\mathcal{A}$ и её подалгебры $\mathcal{A}' \subseteq \mathcal{A}$. В следующей теореме будет доказано, что существуют семейства пар данного вида, такие что $l(\mathcal{A}') \geqslant l(\mathcal{A})$, и разность длин может принимать сколь угодно большое значение. Таким образом будет получен ответ на первый вопрос. Вопрос о значениях отношения длин будет рассмотрен в следующих двух разделах.

Теорема 5.11. *Пусть $k \in \mathbb{N}$ — произвольное натуральное число, $n = 4k$. Тогда существуют такие алгебры $\mathcal{A}' \subset \mathcal{A} \subset \mathrm{M}_n(\mathbb{F})$, что $l(\mathcal{A}') - l(\mathcal{A}) = k$.*

Доказательство. Явная конструкция пары $(\mathcal{A}, \mathcal{A}')$ алгебр над $\mathbb{F}$, таких что $\mathcal{A}' \subseteq \mathcal{A}$ и $l(\mathcal{A}') - l(\mathcal{A}) = k$, приведена в примере 5.12 и предложении 5.13. Данная конструкция также использует утверждение примера 5.9. $\square$

Пример 5.12. Пусть $\mathbb{F}$ — достаточно большое поле, k — фиксированное положительное число, $n = 4k$. Пусть

$$\mathcal{A} = \underbrace{\mathcal{A}_4 \oplus \ldots \oplus \mathcal{A}_4}_{k \text{ раз}} \subset \mathrm{M}_n(\mathbb{F}),$$

$$A_i = E_{4i-3,4i-3} + E_{4i-3,4i-2} + E_{4i-2,4i-2} + E_{4i-2,4i-1} + E_{4i-1,4i-1}, \quad i = 1, \ldots, k.$$

Положим

$$\mathcal{A}' = \left\langle \sum_{i=1}^{k} (a_i A_i + b_i E_{4i,4i}) \right\rangle \subset \mathcal{A},$$

здесь a_i, b_i, $i = 1, \ldots, k$, — различные ненулевые элементы $\mathbb{F}$.

Как будет показано в следующем предложении, $l(\mathcal{A}) = 3k - 1$, в то время как $l(\mathcal{A}') = n - 1 = 4k - 1$ согласно предложению 4.3.

Предложение 5.13. *Пусть k — фиксированное положительное число, $\mathbb{F}$ — такое поле, что $|\mathbb{F}| \geqslant 2k + 1$. Пусть*

$$\mathcal{A} = \underbrace{\mathcal{A}_4 \oplus \ldots \oplus \mathcal{A}_4}_{k \text{ раз}} \subset \mathrm{M}_n(\mathbb{F}).$$

Тогда $l(\mathcal{A}) = 3k - 1$.

Доказательство. Из теоремы 3.9 о прямой сумме и примера 5.9 следует, что $l(\mathcal{A}) \leqslant 2k + k - 1 = 3k - 1$. Рассмотрим систему порождающих

$$\mathcal{S}_{\mathcal{A}} = \left\{ A = \sum_{i=1}^{k} (\alpha_i (A_i - E_{4i-2,4i-1}) + \beta_i E_{4i,4i}),\ E_{4j-2,4j-1},\ j = 1, \ldots, k \right\},$$

где α_i, β_i, $i = 1, \ldots, k$, — различные ненулевые элементы $\mathbb{F}$,

$$A_i = E_{4i-3,4i-3} + E_{4i-3,4i-2} + E_{4i-2,4i-2} + E_{4i-2,4i-1} + E_{4i-1,4i-1}, \quad i = 1, \ldots, k.$$

Поскольку

$$AE_{4j-2,4j-1} = \alpha_j (E_{4j-3,4j-1} + E_{4j-2,4j-1}), \quad E_{4j-2,4j-1} A = \alpha_j E_{4j-2,4j-1}$$

и степень минимального многочлена A равна $3k$, то $l(\mathcal{S}_{\mathcal{A}}) = 3k - 1 = l(\mathcal{A})$. $\square$

5.1. Блочные подалгебры в алгебре верхнетреугольных матриц

5.1.1. Алгебры с двумя блоками

Отметим, что в примере 5.12 величина $m = l(\mathcal{A}') - l(\mathcal{A})$ — произвольное натуральное число, однако отношение $r = l(\mathcal{A}') : l(\mathcal{A}) = 3 : 2$ постоянно. Этот и следующий раздел посвящены доказательству того факта, что для любого рационального числа $r \in [1,2]$ можно так подобрать $\mathbb{F}$-алгебру $\mathcal{A}$ и её подалгебру $\mathcal{A}'$, что $l(\mathcal{A}')/l(\mathcal{A}) = r$.

В данном разделе рассмотрены двухпараметрические семейства алгебр $\mathcal{A}_{n,m}$ вида

$$\mathcal{A}_{n,m} = \left\langle E,\ \sum_{i=1}^{n} E_{i,i},\ E_{i,j} \ \middle|\ \begin{array}{l} 1 \leqslant i < j \leqslant n \\ \text{или} \\ n+1 \leqslant i < j \leqslant n+m \end{array} \right\rangle \subset \mathrm{T}_{m+n}(\mathbb{F}),$$

где $n \geqslant m$ — натуральные числа, над произвольным полем $\mathbb{F}$. Удалось явно вычислить их длины и подобрать в каждой алгебре из этого семейства подалгебру $\mathcal{A}'_{n,m}$, для которой $l(\mathcal{A}'_{n,m}) > l(\mathcal{A}_{n,m})$. Подбирая нужные значения параметров n и m, получаем требуемые значения отношения $l(\mathcal{A}'_{n,m})/l(\mathcal{A}_{n,m})$ (см. следствия 5.25—5.26).

Замечание 5.14. Данные конструкции обобщают пример 5.9, а именно получается серия алгебр $\mathcal{A}(n) = \mathcal{A}_{n,m}$ и их подалгебр $\mathcal{A}'(n)$ с фиксированной разностью длин m, для которых отношение длин $r = r(n)$ является непостоянной дробно-линейной функцией.

Замечание 5.15. Алгебра $\mathcal{A}_4$, описанная в примере 5.9, в обозначениях данного раздела совпадает с $\mathcal{A}_{3,1}$.

Обозначение 5.16. Любая матрица $A \in \mathcal{A}_{n,m}$ имеет вид

$$A = \begin{pmatrix} A' & 0 \\ 0 & A'' \end{pmatrix},$$

где $A' \in \mathrm{T}_n(\mathbb{F})$, $A'' \in \mathrm{T}_m(\mathbb{F})$. Далее будем использовать обозначение $A = A' \oplus A''$.

В следующих двух леммах будет показано, что в системах порождающих можно выбрать элементы специального вида, которые нужны для дальнейшего вычисления длин алгебр $\mathcal{A}_{n,m}$.

Лемма 5.17. *Пусть $n \in \mathbb{N}$, $n \geqslant 3$, и пусть $\mathcal{S}$ — произвольная система порождающих для $\mathcal{A}_{n,m}$. Тогда существует система порождающих $\tilde{\mathcal{S}}$ для алгебры $\mathcal{A}_{n,m}$, такая что выполнены следующие условия*:

1) $\dim \mathcal{L}_1(\tilde{\mathcal{S}}) = |\tilde{\mathcal{S}}| + 1$;
2) *существует матрица $A_0 = A_0' \oplus A_0'' \in \tilde{\mathcal{S}}$, такая что*

$$A_0' = \sum_{1 \leqslant i < j \leqslant n} a_{i,j} E_{i,j}, \quad A_0'' = \sum_{1 \leqslant i < j \leqslant m} a_{i+n,j+n} E_{i+n,j+n} + E;$$

3) *для всех $S \in \tilde{\mathcal{S}}$, $S \neq A_0$, выполнено $(S)_{i,i} = 0$, $i = 1, \ldots, n+m$;*
4) *существуют матрицы $B_1, \ldots, B_{n-1} \in \tilde{\mathcal{S}}$ и индекс $k \in \{1, \ldots, n-1\}$, такие что*

а) *для всех* $r = 1, \ldots, n-1$

$$B'_r = E_{r,r+1} + \sum_{i=1}^{n} \sum_{j=i+2}^{n} b_{i,j;r} E_{i,j}, \quad B''_r \in \mathrm{N}_m(\mathbb{F}),$$

$$A'_0 = \sum_{2 \leqslant j-i \leqslant n-1} \hat{a}_{i,j} E_{i,j}, \quad A''_0 = \sum_{1 \leqslant i<j \leqslant m} \hat{a}_{i+n,j+n} E_{i+n,j+n} + E,$$

либо

б) *для всех* $r = 1, \ldots, n-1$, $r \neq k$,

$$B'_r = E_{r,r+1} + b_r E_{k,k+1} + \sum_{i=1}^{n} \sum_{j=i+2}^{n} b_{i,j;r} E_{i,j}, \quad B''_r \in \mathrm{N}_m(\mathbb{F}),$$

$$B'_k = A'_0 = a_k E_{k,k+1} + \sum_{i=1}^{n} \sum_{j=i+2}^{n} \hat{a}_{i,j} E_{i,j}, \quad a_k \neq 0,$$

$$B''_k = A''_0 = \sum_{1 \leqslant i<j \leqslant m} \hat{a}_{i+n,j+n} E_{i+n,j+n} + E;$$

5) $l(\tilde{\mathcal{S}}) = l(\mathcal{S})$.

Доказательство. Будем последовательно преобразовывать $\mathcal{S}$ до системы порождающих, удовлетворяющей условиям 1)—5).

Условие 1. Данное условие можно считать выполненным согласно предложению 3.4

Условие 2. Предположим, что для всех элементов $S \in \mathcal{S}$ выполнено $(S)_{i,i} = (S)_{i+1,i+1}$, $i = 1, \ldots, n+m-1$, и приведём это утверждение к противоречию. Действительно, данное условие означает, что множество $\mathcal{S}$ лежит в алгебре $\mathbb{F}E \oplus N_{n+m}(\mathbb{F})$ и, соответственно, алгебра $\mathcal{A}_{n,m}$, порождённая множеством $\mathcal{S}$, является подалгеброй в $\mathbb{F}E \oplus N_{n+m}(\mathbb{F})$. С другой стороны,

$$D = \sum_{i=1}^{n} E_{i,i} \in \mathcal{A}_{n,m},$$

но при этом $D \notin \mathbb{F}E \oplus N_{n+m}(\mathbb{F})$. Противоречие. Следовательно, найдётся матрица $A = A' \oplus A'' \in \mathcal{S}$, такая что

$$A' = \alpha_1 E + \sum_{1 \leqslant i<j \leqslant n} a_{i,j} E_{i,j}, \quad A'' = \alpha_2 E + \sum_{1 \leqslant i<j \leqslant m} a_{i+n,j+n} E_{i+n,j+n},$$

где $\alpha_1 \neq \alpha_2$. Положим $A_0 = (\alpha_2 - \alpha_1)^{-1}(A - \alpha_1 E)$.

По предложению 3.2 с сохранением длины перейдём к системе порождающих

$$\mathcal{S}_0 = \{A_0,\, S \mid S \in \mathcal{S},\ S \neq A\}.$$

Условие 3. По предложению 3.2 с сохранением длины перейдём к системе порождающих

$$\mathcal{S}' = \{S - (S)_{1,1} E \mid S \in \mathcal{S}_0\},$$

затем по предложению 3.1 с сохранением длины перейдём к системе порождающих

$$\mathcal{S}'' = \{A_0,\ S - (S)_{n+1,n+1}A_0 \mid S \in \mathcal{S}',\ S \neq A_0\}.$$

Для простоты дальнейшего изложения обозначим $\mathcal{S}''$ снова через $\mathcal{S}$.

Условие 4. Поскольку $E_{i,i+1} \in \mathcal{A}_{n,m}$, но для любых $t \geqslant 2$ и $S \in \mathcal{S}^t \backslash \mathcal{S}^{t-1}$ коэффициент $(S)_{i,i+1}$, $i = 1, \ldots, n-1$, равен 0, то найдутся матрицы $B_1, \ldots, B_{n-1} \in \mathcal{S}$, такие что векторы

$$u_i = \big((B_i)_{1,2},\ (B_i)_{2,3}, \ldots,\ (B_i)_{n-1,n}\big), \quad i = 1, \ldots, n-1,$$

линейно независимы.

Теперь выполним преобразование $\mathcal{F}$ системы $\mathcal{S}$ (по предложению 3.1 $\mathcal{F}$ сохраняет длину $\mathcal{S}$), которое на всех элементах $S \in \mathcal{S}$, $S \neq B_i$, $i = 1, \ldots, n-1$, и $S \neq A_0$, действует тождественно, т. е. $\mathcal{F}(S) = S$, а действие $\mathcal{F}$ на множестве матриц $\{B_j \mid j = 1, \ldots, n-1\}$ и на матрице A_0 зависит от принадлежности матрицы A_0 этому множеству и определяется следующим образом.

а) Пусть $A_0 \notin \{B_1, \ldots, B_{n-1}\}$. Невырожденным линейным преобразованием $F = \{f_{i,j}\} \in \mathrm{M}_{n-1}(\mathbb{F})$ можно перевести набор векторов $\{u_i \mid i = 1, \ldots, n-1\}$ в набор

$$\{e_1 = (1, 0, \ldots, 0),\ e_2 = (0, 1, \ldots, 0), \ldots,\ e_{n-1} = (0, 0, \ldots, 1)\} \subset \mathbb{F}^{n-1},$$

т. е.

$$e_i = \sum_{j=1}^{n-1} f_{i,j} u_j.$$

Тогда положим

$$\mathcal{F}(B_r) = \sum_{j=1}^{n-1} f_{r,j} B_j.$$

При этом

$$\mathcal{F}(B_r)' = E_{r,r+1} + \sum_{i=1}^{n} \sum_{j=i+2}^{n} b_{i,j;r} E_{i,j}.$$

Также положим

$$\mathcal{F}(A_0) = A_0 - \sum_{i=1}^{n-1} (A_0)_{i,i+1} \mathcal{F}(B_i).$$

б) Пусть $A_0 \in \{B_1, \ldots, B_{n-1}\}$, т. е. $A_0 = B_p$ для некоторого $p \in \{1, \ldots, n-1\}$. Так как у любой матрицы в $\mathrm{M}_{n-1,n-2}(\mathbb{F})$ ранга $n-2$ существует невырожденная подматрица порядка $n-2$, то в этом случае найдётся индекс $k \in \{1, \ldots, n-1\}$, такой что векторы

$$v_i = \big((B_i)_{1,2}, \ldots,\ (B_i)_{k-1,k},\ (B_i)_{k+1,k+2}, \ldots,\ (B_i)_{n-1,n}\big), \quad i = 1, \ldots, n-1,\ \ i \neq p,$$

линейно независимы. Поскольку упорядочивание матриц B_j произвольно, можно считать, что $p = k$. Невырожденным линейным преобразованием $G = \{g_{i,j}\} \in \in \mathrm{M}_{n-2}(\mathbb{F})$ можно перевести набор векторов $\{v_i \mid i = 1, \ldots, n-1,\ i \neq k\}$ в набор

$$\{e_1 = (1, 0, \ldots, 0),\ e_2 = (0, 1, \ldots, 0), \ldots,\ e_{n-2} = (0, 0, \ldots, 1)\} \subset \mathbb{F}^{n-2},$$

т. е.

$$e_i = \sum_{j=1}^{k-1} g_{i,j} v_j + \sum_{j=k}^{n-2} g_{i,j} v_{j+1}.$$

Тогда положим

$$\mathcal{F}(B_r) = \sum_{j=1}^{k-1} f_{r,j} B_j + \sum_{j=k}^{n-2} f_{r,j} B_{j+1}, \quad r < k,$$

$$\mathcal{F}(B_r) = \sum_{j=1}^{k-1} f_{r-1,j} B_j + \sum_{j=k}^{n-2} f_{r-1,j} B_{j+1}, \quad r > k,$$

$$\mathcal{F}(A_0) = A_0 - \sum_{\substack{i=1,\\ i\neq k}}^{n-1} (A_0)_{i,i+1} \mathcal{F}(B_i),$$

т. е.

$$\mathcal{F}(B_r)' = E_{r,r+1} + b_r E_{k,k+1} + \sum_{i=1}^{n} \sum_{j=i+2}^{n} b_{i,j;r} E_{i,j} \quad \text{для} \quad r \neq k,$$

$$\mathcal{F}(A_0)' = a_k E_{k,k+1} + \sum_{i=1}^{n} \sum_{j=i+2}^{n} \hat{a}_{i,j} E_{i,j}, \quad a_k \neq 0,$$

$$\mathcal{F}(A_0)'' = \sum_{1 \leqslant i < j \leqslant m} \hat{a}_{i+n,j+n} E_{i+n,j+n} + E.$$

Для простоты дальнейшего изложения обозначим $\mathcal{F}(A_0)$ и $\mathcal{F}(B_r)$ снова через A_0 и B_r соответственно. Тогда система порождающих $\tilde{\mathcal{S}} = \mathcal{F}(\mathcal{S})$ и будет искомой.

Условие 5. Преобразования системы $\mathcal{S}$ из пунктов 1—4 не меняли её длины, следовательно, длина полученной системы порождающих $\tilde{\mathcal{S}}$ равна длине исходной системы. □

Лемма 5.18. *Пусть $n \geqslant 3$, $m \geqslant 2$, и пусть $\mathcal{S}$ — система порождающих для $\mathcal{A}_{n,m}$, удовлетворяющая условиям* 1)—4) *леммы* 5.17. *Тогда выполнено одно из следующих условий*:

а) *существуют такие матрицы $C, C_1, \ldots, C_{m-1} \in \langle \mathcal{S} \setminus A_0 \rangle$, что*

$$C_r'' = E_{r+n,r+n+1} + \sum_{i=1}^{m} \sum_{j=i+2}^{m} c_{i+n,j+n;r} E_{i+n,j+n}, \quad r = 1, \ldots, m-1,$$

и если $\tilde{A}_0 = E - A_0 + C$, *то*

$$\tilde{A}_0'' = \sum_{i=1}^{m} \sum_{j=i+2}^{m} \tilde{a}_{i+n,j+n} E_{i+n,j+n},$$

б) *существуют индекс* $s \in \{1, \dots, m-1\}$ *и такие матрицы* $C, C_r \in \langle \mathcal{S} \setminus A_0 \rangle$, $r = 1, \dots, m-1$, $r \neq s$, $C_s \in \langle \mathcal{S} \rangle$, *что*

$$C_r'' = E_{r+n,r+n+1} + c_r E_{s+n,s+n+1} + \sum_{i=1}^{m} \sum_{j=i+2}^{m} c_{i+n,j+n;r} E_{i+n,j+n}$$

при $r = 1, \dots, m-1$, $r \neq s$, *и если* $C_s = \tilde{A}_0 = E - A_0 + C$, *то*

$$\tilde{A}_0'' = \tilde{a}_s E_{s+n,s+n+1} + \sum_{i=1}^{m} \sum_{j=i+2}^{m} \tilde{a}_{i+n,j+n} E_{i+n,j+n}, \quad \tilde{a}_s \neq 0.$$

Доказательство. Поскольку для любых $S_1, S_2 \in \mathcal{S}$ и для любого $i = n+1, \dots, n+m-1$ справедливо $(S_1 S_2)_{i,i+1} = 0$ при $S_1 \neq A_0$, $S_2 \neq A_0$, а также

$$(S_1 A_0)_{i,i+1} = (S_1)_{i,i+1}, \quad (A_0 S_2)_{i,i+1} = (S_2)_{i,i+1}, \quad (A_0^2)_{i,i+1} = 2(A_0)_{i,i+1},$$

то найдутся такие $\tilde{C}_1, \dots, \tilde{C}_{m-1} \in \mathcal{S}$, что векторы

$$w_i = \big((\tilde{C}_i)_{n+1,n+2}, (\tilde{C}_i)_{n+2,n+3}, \dots, (\tilde{C}_i)_{n+m-1,n+m}\big), \quad i = 1, \dots, m-1,$$

линейно независимы.

Условие а). Пусть $A_0 \notin \{\tilde{C}_1, \dots, \tilde{C}_{m-1}\}$. Невырожденным линейным преобразованием $F_c = \{f_{i,j}\} \in \mathrm{M}_{m-1}(\mathbb{F})$ можно перевести набор векторов $\{w_i \mid i = 1, \dots, m-1\}$ в набор

$$\{e_1 = (1, 0, \dots, 0),\ e_2 = (0, 1, \dots, 0), \dots,\ e_{m-1} = (0, 0, \dots, 1)\} \subset \mathbb{F}^{m-1},$$

т. е.

$$e_i = \sum_{j=1}^{m-1} f_{i,j} w_j.$$

Положим

$$C_r = \sum_{j=1}^{m-1} f_{r,j} \tilde{C}_j.$$

Тогда

$$C_r \in \langle \tilde{C}_1, \dots, \tilde{C}_{m-1} \rangle \subset \langle \mathcal{S} \setminus A_0 \rangle, \quad r = 1, \dots, m-1,$$

и

$$C_r'' = E_{r+n,r+n+1} + \sum_{i=1}^{m} \sum_{j=i+2}^{m} c_{i+n,j+n;r} E_{i+n,j+n}.$$

Теперь положим
$$C=\sum_{i=1}^{m-1}\hat a_{i+n,i+n+1}C_i,$$
т. е.
$$(C)_{i+n,i+n+1}=(A_0)_{i+n,i+n+1}$$
для любого $i=1,\dots,m-1$. Тогда
$$\tilde A_0''=E-A_0''+C''=\sum_{i=1}^{m}\sum_{j=i+2}^{m}\tilde a_{i+n,j+n}E_{i+n,j+n}.$$

Условие б). Пусть $\tilde C_p=A_0$ для некоторого $p\in\{1,\dots,m-1\}$.

При $m=2$ положим $\tilde A_0=E-A_0$ и $C_1=\tilde A_0$.

Пусть $m\geqslant 3$. У любой матрицы в $\mathrm{M}_{m-1,m-2}(\mathbb F)$ ранга $m-2$ существует невырожденная подматрица порядка $m-2$. Следовательно, найдётся индекс $s\in\{1,\dots,m-1\}$, такой что векторы
$$x_i=\big((\tilde C_i)_{1,2},\,\dots,\,(\tilde C_i)_{s-1,s},\,(\tilde C_i)_{s+1,s+2},\,\dots,\,(\tilde C_i)_{m-1,m}\big),\qquad i=1,\dots,m-1,\quad i\neq p,$$
линейно независимы. Поскольку порядок матриц $\tilde C_j$ произволен, можно считать, что $p=s$. Невырожденным линейным преобразованием $G_c=\{g_{i,j}\}\in\mathrm{M}_{m-2}(\mathbb F)$ можно перевести набор $\{x_i\mid i=1,\dots,m-1,\ i\neq s\}$ в набор
$$\{e_1=(1,0,\dots,0),\,e_2=(0,1,\dots,0),\,\dots,\,e_{m-2}=(0,0,\dots,1)\}\subset\mathbb F^{m-2},$$
т. е.
$$e_i=\sum_{j=1}^{s-1}g_{i,j}x_j+\sum_{j=s}^{m-2}g_{i,j}x_{j+1}.$$
Положим
$$C_r=\sum_{j=1}^{s-1}g_{r,j}\tilde C_j+\sum_{j=s}^{m-2}g_{r,j}\tilde C_{j+1},\quad r<s,$$
$$C_r=\sum_{j=1}^{s-1}g_{r-1,j}\tilde C_j+\sum_{j=s}^{m-2}g_{r-1,j}\tilde C_{j+1},\quad r>s.$$
Тогда
$$C_r\in\langle\tilde C_1,\dots,\tilde C_{s-1},\tilde C_{s+1},\dots,\tilde C_{m-1}\rangle\subset\langle\mathcal S\setminus A_0\rangle,\quad r=1,\dots,m-1,\ \ r\neq s,$$
$$C_r''=E_{r+n,r+n+1}+c_rE_{s+n,s+n+1}+\sum_{i=1}^{m}\sum_{j=i+2}^{m}c_{i+n,j+n;r}E_{i+n,j+n}.$$
Теперь положим
$$C=\sum_{\substack{i=1,\\ i\neq s}}^{m-1}\hat a_{i+n,i+n+1}C_i$$

и $C_s = \tilde{A}_0 = E - A_0 + C$, т. е. $(C)_{i+n,i+n+1} = (A_0)_{i+n,i+n+1}$ для любого $i = 1, \ldots, m-1$, $i \neq s$. Тогда

$$\tilde{A}_0'' = I - A_0'' + C'' = \tilde{a}_s E_{s+n,s+n+1} + \sum_{i=1}^{m} \sum_{j=i+2}^{m} \tilde{a}_{i+n,j+n} E_{i+n,j+n},$$

где $\tilde{a}_s \neq 0$. □

Вычислим длину алгебр $\mathcal{A}_{n,m}$ отдельно для различных значений n и m.

Лемма 5.19. *Пусть $\mathbb{F}$ — произвольное поле. Тогда $l(\mathcal{A}_{1,1}) = 1$ и $l(\mathcal{A}_{2,2}) = 3$.*

Доказательство. Так как $\mathcal{A}_{1,1} = \mathrm{D}_2(\mathbb{F})$, по теореме 4.60 $l(\mathcal{A}_{1,1}) = 1$.

Алгебра $\mathcal{A}_{2,2}$ порождается циклической матрицей $E_{1,1} + E_{1,2} + E_{2,2} + E_{3,4}$. Следовательно, по лемме 4.5 $l(\mathcal{A}_{2,2}) = 3$. □

Лемма 5.20. *Пусть $\mathbb{F}$ — произвольное поле. Тогда $l(\mathcal{A}_{2,1}) = 2$ и $l(\mathcal{A}_{3,2}) = 3$.*

Доказательство. Алгебра $\mathcal{A}_{2,1}$ порождается циклической матрицей $E_{1,1} + E_{1,2} + E_{2,2}$. Следовательно, по лемме 4.5 $l(\mathcal{A}_{2,1}) = 2$.

2. Пусть $\mathcal{S}$ — произвольная система порождающих для $\mathcal{A}_{3,2}$. Не ограничивая общности, можно считать, что $\mathcal{S}$ удовлетворяет условиям 1)—4) леммы 5.17 и, значит, одному из условий леммы 5.18. Покажем, что $\mathcal{L}_3(\mathcal{S}) = \mathcal{A}_{3,2}$. Имеем

$$B_1 B_2 (E - A_0) = a E_{1,3}, \quad a \neq 0,$$
$$B_1 (E - A_0)^2 = b_{11} E_{1,2} + b_{12} E_{2,3} + b_{13} E_{1,3},$$
$$B_2 (E - A_0)^2 = b_{21} E_{1,2} + b_{22} E_{2,3} + b_{23} E_{1,3},$$

где векторы (b_{11}, b_{12}) и (b_{21}, b_{22}) линейно независимы,

$$C_1 A_0^2 = b E_{4,5} + c E_{1,3}, \quad b \neq 0.$$

Также

$$E_{4,4} + E_{5,5} = (A_0 - (A_0)_{1,2} E_{1,2} - (A_0)_{1,3} E_{1,3} - (A_0)_{2,3} E_{2,3} - (A_0)_{4,5} E_{4,5}) \in \mathcal{L}_3(\mathcal{S}).$$

Возьмём

$$\mathcal{S} = \{A = E_{1,2},\ B = E_{2,3} + E_{4,4} + E_{4,5} + E_{5,5},\ E\}.$$

Из равенств $A^2 = 0$, $AB = E_{1,3}$, $BA = 0$, $B^2 = E_{4,4} + 2E_{4,5} + E_{5,5}$ и $B^3 - B^2 = E_{4,5}$ выводим, что $l(\mathcal{S}) = 3 = l(\mathcal{A}_{3,2})$. □

Лемма 5.21. *Пусть $\mathbb{F}$ — произвольное поле, $n, m \in \mathbb{N}$ и $n - m \geqslant 2$. Тогда $l(\mathcal{A}_{n,m}) = n - 1$.*

Доказательство. I. Сначала докажем верхнюю оценку $l(\mathcal{A}_{n,m}) \leqslant n - 1$. Для этого рассмотрим произвольную систему порождающих $\mathcal{S}$ для $\mathcal{A}_{n,m}$. Не ограничивая общности, можно считать, что $\mathcal{S}$ удовлетворяет условиям 1)—4) леммы 5.17.

1. Индукцией по $p = n-(j-i)$ докажем, что $E_{i,j} \in \mathcal{L}_{n-1}(\mathcal{S})$ при $1 \leqslant i < j \leqslant n$, $j - i \geqslant 2$.

База индукции. При $p = 1$ рассмотрим произведение $B_1 B_2 \cdots B_{n-1} \in \mathcal{L}_{n-1}(\mathcal{S})$. Заметим, что $B_1' B_2' \cdots B_{n-1}' = (a_k)^t E_{1,n}$, $t \in \{0,1\}$, и $B_1'' B_2'' \cdots B_{n-1}'' = 0$ как произведение $n-1$ нильпотентной матрицы B_r'' порядка $m \leqslant n-2$ при $t = 0$ и как произведение $n-2$ нильпотентных матриц B_r'', $r \neq k$, и одной унитреугольной матрицы B_k'' порядка $m \leqslant n-2$ при $t = 1$. Следовательно,

$$E_{1,n} = (a_k)^{-t} B_1 B_2 \cdots B_{n-1} \in \mathcal{L}_{n-1}(\mathcal{S}).$$

Шаг индукции. Предположим, что утверждение верно для всех q, $1 < q < p$. Рассмотрим произведения матриц

$$B_{j,j+n-p-1} = B_j B_{j+1} \cdots B_{j+n-p-1} (E - A_0)^{p-1} \in \mathcal{L}_{n-1}(\mathcal{S}), \quad j = 1, \ldots, p.$$

Имеем

$$B'_{j,j+n-p-1} = (a_k)^t E_{j,j+n-p} + \sum_{h=1}^{n} \sum_{i=h+n-p+1}^{n} d_{h,i;j,p} E_{h,i}, \quad t \in \{0,1\},$$

при этом $B''_{j,j+n-p-1} = 0$ как произведение $n-1$ нильпотентной матрицы B_r'' и $(E - A_0)''$ порядка $m \leqslant n-2$ при $t = 0$ и как произведение $n-2$ нильпотентных матриц B_r'', $r \neq k$, $(E - A_0)''$ и одной унитреугольной матрицы B_k'' порядка $m \leqslant n-2$ при $t = 1$.

По предположению индукции $E_{i,i+n-q-1} \in \mathcal{L}_{n-1}(\mathcal{S})$ для любых $q = 1, \ldots, p-1$, $i = 1, \ldots, q$. Значит, $B_{j,j+n-p-1} - (a_k)^t E_{j,j+n-p} \in \mathcal{L}_{n-1}(\mathcal{S})$. Поскольку $B_{j,j+n-p-1} \in \mathcal{L}_{n-1}(\mathcal{S})$ по построению, получаем, что

$$E_{j,j+n-p-1} = (a_k)^{-t} \big(B_{j,j+n-p-1} - (B_{j,j+n-p-1} - (a_k)^t E_{j,j+n-p}) \big) \in \mathcal{L}_{n-1}(\mathcal{S}), \quad j = 1, \ldots, p.$$

2. Теперь рассмотрим матрицы $B_{j,j} = B_j (E - A_0)^{n-2} \in \mathcal{L}_{n-1}(\mathcal{S})$, $j = 1, \ldots, n-1$. По построению

$$(B_{j,j})_{r,r+1} = (B_j)_{r,r+1}, \quad j, r = 1, \ldots, n-1,$$

т. е.

$$B'_{j,j} = E_{j,j+1} + \gamma_j E_{k,k+1} + \sum_{h=1}^{n} \sum_{i=h+2}^{n} d_{h,i;j} E_{h,i}, \quad j \neq k,$$

$$B'_{k,k} = a_k^t E_{k,k+1} + \sum_{h=1}^{n} \sum_{i=h+2}^{n} d_{h,i;k} E_{h,i}, \quad t \in \{0,1\},$$

при этом $(E'' - A_0'')^{n-2} = 0$ как произведение $n-2$ нильпотентных матриц порядка $m \leqslant n-2$, значит, $B''_{r,r} = B_r'' (E'' - A_0'')^{n-2} = 0$.

По доказанному в пункте 1

$$\sum_{h=1}^{n} \sum_{i=h+2}^{n} d_{h,i;j} E_{h,i} \in \mathcal{L}_{n-1}(\mathcal{S}), \quad j = 1, \ldots, n.$$

Значит,

$$E_{k,k+1} = a_k^{-t}\left(B_{k,k} - \sum_{h=1}^{n}\sum_{i=h+2}^{n} d_{h,i;k}E_{h,i}\right) \in \mathcal{L}_{n-1}(\mathcal{S}).$$

Тогда

$$E_{j,j+1} = B_{j,j} - \sum_{h=1}^{n}\sum_{i=h+2}^{n} d_{h,i;j}E_{h,i} - \gamma_j E_{k,k+1} \in \mathcal{L}_{n-1}(\mathcal{S}).$$

Следовательно, $E_{i,j} \in \mathcal{L}_{n-1}(\mathcal{S})$, $1 \leqslant i < j \leqslant n$. Тогда для любой матрицы $N \in \mathrm{N}_n(\mathbb{F})$ выполнено $N \oplus 0 \in \mathcal{L}_{n-1}(\mathcal{S})$.

3. Пусть $S_1, \ldots, S_n \in \mathcal{S}$. Пусть $\mathcal{B} \subseteq \mathrm{T}_m(\mathbb{F})$ — подалгебра, порождённая матрицами $S_1'', \ldots, S_{n-1}''$. Согласно следствию 3.12 $l(\mathcal{B}) \leqslant m-1$, значит, найдётся элемент $V'' \in \mathcal{L}_{m-1}(\{S_1'', \ldots, S_{n-1}''\})$, такой что $S_1'' \cdots S_{n-1}'' - V'' = 0$. Положим $W'' = V'' \cdot S_n'' \in \mathcal{L}_m(\{S_1'', \ldots, S_n''\}$ и заметим, что W'' — линейная комбинация слов положительной длины от элементов $S_1'', \ldots, S_n''$. Пусть $W \in \mathcal{L}_m(\mathcal{S}) \subseteq \mathcal{L}_{n-1}(\mathcal{S})$ — прообраз W''. Тогда $S_1 \cdots S_n + W = S' \oplus 0$, $S' \in N_n(\mathbb{F})$, но $S' \oplus 0 \in \mathcal{L}_{n-1}(\mathcal{S})$ по доказанному в пунктах 1 и 2. Значит, слово $S_1 \cdots S_n$ сократимо.

Таким образом, мы получили, что любое слово длины n от элементов $\mathcal{S}$ сократимо, $\mathcal{L}_n(\mathcal{S}) = \mathcal{L}_{n-1}(\mathcal{S})$ и $l(\mathcal{S}) \leqslant n-1$.

II. Из теоремы 3.9 о прямой сумме получаем нижнюю оценку

$$l(\mathcal{A}_{n,m}) \geqslant \max\{n-1, m-1\} = n-1.$$

Следовательно, $l(\mathcal{A}_{n,m}) = n-1$. □

Лемма 5.22. *Пусть $\mathbb{F}$ — произвольное поле, $n \in \mathbb{N}$ и $n > 3$. Тогда $l(\mathcal{A}_{n,n-1}) = n-1$.*

Доказательство. I. Сначала докажем верхнюю оценку $l(\mathcal{A}_{n,n-1}) \leqslant n-1$. Для этого рассмотрим произвольную систему порождающих $\mathcal{S}$ для $\mathcal{A}_{n,n-1}$. Не ограничивая общности, можно считать, что $\mathcal{S}$ удовлетворяет условиям 1)—4) леммы 5.17 и, значит, одному из условий леммы 5.18.

1. Индукцией по $p = n-(j-i)$ докажем, что $E_{i,j} \in \mathcal{L}_{n-1}(\mathcal{S})$ при $1 \leqslant i < j \leqslant n$, $j-i \geqslant 2$.

База индукции. Рассмотрим случай $p = 1$.

а) Предположим, что нет такого k, что $A_0 = B_k$. Тогда $B_1 B_2 \cdots B_{n-1} = E_{1,n} \in \mathcal{L}_{n-1}(\mathcal{S})$, поскольку $B_1'' B_2'' \cdots B_{n-1}'' = 0$ как произведение $n-1$ нильпотентной матрицы порядка $n-1$. Также $C_1 \cdots C_{n-2} A_0 = aE_{n+1,2n-1} + bE_{1,n}$, $a \neq 0$, т. е. $E_{n+1,2n-1} \in \mathcal{L}_{n-1}(\mathcal{S})$.

б) Теперь предположим, что есть k, для которого $A_0 = B_k$. Тогда

$$B_1 B_2 \cdots B_{n-1} = a_k E_{1,n} + \alpha E_{n+1,2n-1}.$$

Пусть $\alpha = 0$. Рассмотрим произведение $C_1 \cdots C_{n-2} \in \mathcal{L}_{n-2}(\mathcal{S})$. Имеем

$$(C_1 \cdots C_{n-2})'' = aE_{n+1,2n-1}, \quad a \neq 0,$$

и

$$(C_1 \cdots C_{n-2})' = \\ = \beta_1 E_{1,n-2} + \beta_2 E_{1,n-1} + \beta_3 E_{1,n} + \beta_4 E_{2,n-1} + \beta_5 E_{2,n} + \beta_6 E_{3,n} \in \mathrm{N}_n(\mathbb{F}).$$

Заметим, что

$$(C_1 \cdots C_{n-2} A_0)'' = (A_0 C_1 \cdots C_{n-2})'' = (C_1 \cdots C_{n-2})'',$$

при $k > 2$ справедливо $(A_0 C_1 \cdots C_{n-2})' = \beta E_{1,n}$, а при $k < n-2$ справедливо $(C_1 \cdots C_{n-2} A_0)' = \beta E_{1,n}$.

Следовательно, если хотя бы одно из неравенств $k > 2$ и $k < n-2$ выполнено, то $E_{1,n}, E_{n+1,2n-1} \in \mathcal{L}_{n-1}(\mathcal{S})$.

Если система порождающих $\mathcal{S}$ удовлетворяет условию а) леммы 5.18, то $\beta_1 = \beta_4 = \beta_6 = 0$, значит, $(A_0 C_1 \cdots C_{n-2})' = \beta E_{1,n}$. Таким образом, в этом случае также $E_{1,n}, E_{n+1,2n-1} \in \mathcal{L}_{n-1}(\mathcal{S})$.

Пусть $n-2 \leqslant k \leqslant 2$ и система порождающих $\mathcal{S}$ удовлетворяет условию б) леммы 5.18. По условию леммы $n \geqslant 4$, следовательно, $n = 4$ и $k = 2$.

Если коэффициент c_{3-s}, определённый в пункте б) леммы 5.18, не равен нулю, то получаем, что $(C_{3-s})' \in \mathrm{N}_4(\mathbb{F})$,

$$(C_{3-s}^2)'' = c_{3-s} E_{5,7}, \quad (A_0 C_{3-s}^2)' = \beta' E_{1,4}, \quad (A_0 C_{3-s}^2)'' = c_{3-s} E_{5,7},$$

значит, $E_{1,n}, E_{n+1,2n-1} \in \mathcal{L}_{n-1}(\mathcal{S})$.

Пусть $c_{3-s} = 0$. Имеем

$$(C_2 C_1)'' = 0, \quad (C_2 C_1)'_{i,i+1} = (C_1 C_2)'_{i,i+1}, \quad i = 1,2,3,$$
$$\big(A_0(C_1 C_2 - C_2 C_1)\big)' = \beta E_{1,4}, \quad \big(A_0(C_1 C_2 - C_2 C_1)\big)'' = a E_{5,7}.$$

Таким образом, в этом случае также $E_{1,n}, E_{n+1,2n-1} \in \mathcal{L}_{n-1}(\mathcal{S})$.

Пусть теперь $\alpha \neq 0$. Это означает, что

$$(B_1 \cdots B_{k-1} B_{k+1} \cdots B_{n-1})'' = \alpha E_{1,n-1}$$

и

$$(B_1 \cdots B_{k-1} B_{k+1} \cdots B_{n-1})' = \beta_1 E_{1,n-1} + \beta_2 E_{1,n} + \beta_3 E_{2,n}.$$

Поскольку $n > 3$, то $k \neq 1$ или $k \neq n-1$. При $k \neq 1$ получаем, что

$$A_0 B_1 \cdots B_{k-1} B_{k+1} \cdots B_{n-1} = \alpha E_{n+1,2n-1},$$

а при $k \neq n-1$ получаем, что

$$B_1 \cdots B_{k-1} B_{k+1} \cdots B_{n-1} A_0 = \alpha E_{n+1,2n-1},$$

следовательно, $E_{1,n}, E_{n+1,2n-1} \in \mathcal{L}_{n-1}(\mathcal{S})$.

Таким образом, во всех случаях $E_{1,n} \in \mathcal{L}_{n-1}(\mathcal{S})$, а также $E_{n+1,2n-1} \in \mathcal{L}_{n-1}(\mathcal{S})$.

Шаг индукции. Предположим, что утверждение верно для всех q, $1 < q < p$. Рассмотрим произведения

$$B_{j,j+n-p-1} = B_j B_{j+1} \cdots B_{j+n-p-1} (E - A_0)^{p-1} \in \mathcal{L}_{n-1}(\mathcal{S}), \quad j = 1, \ldots, p.$$

Тогда

$$B'_{j,j+n-p-1} = (a_k)^t E_{j,j+n-p} + \sum_{\substack{1\leqslant h<i\leqslant n,\\ i-h>n-p}} d_{h,i;j,p} E_{h,i},\ t \in \{0,1\},$$

$B''_{j,j+n-p-1} = b(j,p)E_{1,n-1}$, $b(j,p) \in \mathbb{F}$, как произведение $n-1$ нильпотентной матрицы порядка $n-1$ при $t=0$ и как произведение $n-2$ нильпотентных и одной унитреугольной матрицы порядка $n-1$ при $t=1$.

По предположению индукции $E_{i,i+n-q-1} \in \mathcal{L}_{n-1}(\mathcal{S})$ для любых $q = 2,\ldots,p-1$, $i=1,\ldots,q$, и, как показано ранее, $E_{1,n}, E_{n+1,2n-1} \in \mathcal{L}_{n-1}(\mathcal{S})$. Значит, $B_{j,j+n-p-1} - (a_k)^t E_{j,j+n-p} \in \mathcal{L}_{n-1}(\mathcal{S})$. Поскольку $B_{j,j+n-p-1} \in \mathcal{L}_{n-1}(\mathcal{S})$ по определению, получаем, что

$$E_{j,j+n-p-1} = (a_k)^{-t}\big(B_{j,j+n-p-1} - (B_{j,j+n-p-1} - (a_k)^t E_{j,j+n-p})\big) \in \mathcal{L}_{n-1}(\mathcal{S}),\quad j=1,\ldots,p.$$

2. Теперь рассмотрим матрицы

$$B_{j,j} = B_j(E-A_0)^{n-2} \in \mathcal{L}_{n-1}(\mathcal{S}),\quad j=1,\ldots,n-1.$$

По построению

$$(B_{j,j})_{r,r+1} = (B_j)_{r,r+1},\quad j,r=1,\ldots,n-1,$$

т. е.

$$B'_{j,j} = E_{j,j+1} + \gamma_j E_{k,k+1} + \sum_{h=1}^{n}\sum_{i=h+2}^{n} d_{h,i;j}E_{h,i},\quad j\neq k,$$

$$B'_{k,k} = a_k^t E_{k,k+1} + \sum_{h=1}^{n}\sum_{i=h+2}^{n} d_{h,i;k}E_{h,i},\quad t\in\{0,1\},$$

при этом $B''_{r,r} = b(r)E_{n+1,2n-1}$, $b(r) \in \mathbb{F}$, как произведение $n-1$ нильпотентной матрицы порядка $n-1$ при $r \neq k$ либо $r=k$ и $t=0$ и как произведение $n-2$ нильпотентных и одной унитреугольной матрицы порядка $n-1$ при $r=k$ и $t=1$.

По доказанному в пункте 1

$$\sum_{h=1}^{n}\sum_{i=h+2}^{n} d_{h,i;j}E_{h,i} + b(r)E_{n+1,2n-1} \in \mathcal{L}_{n-1}(\mathcal{S}),\quad j=1,\ldots,n.$$

Значит,

$$E_{k,k+1} = a_k^{-t}(B_{k,k} - \sum_{h=1}^{n}\sum_{i=h+2}^{n} d_{h,i;k}E_{h,i} - b(r)E_{n+1,2n-1}) \in \mathcal{L}_{n-1}(\mathcal{S}).$$

Тогда

$$E_{j,j+1} = B_{j,j} - \sum_{h=1}^{n}\sum_{i=h+2}^{n} d_{h,i;j}E_{h,i} - \gamma_j E_{k,k+1} - b(j)E_{n+1,2n-1} \in \mathcal{L}_{n-1}(\mathcal{S}).$$

Следовательно, $E_{i,j} \in \mathcal{L}_{n-1}(\mathcal{S})$, $1 \leqslant i < j \leqslant n$. Тогда для любой матрицы $N \in \mathrm{N}_n(\mathbb{F})$ выполнено $N \oplus 0 \in \mathcal{L}_{n-1}(\mathcal{S})$.

3. Пусть $S_1, \ldots, S_n \in \mathcal{S}$. Пусть $\mathcal{B} \subseteq \mathrm{T}_{n-1}(\mathbb{F})$ — подалгебра, порождённая матрицами $S_1'', \ldots, S_{n-1}''$. Согласно следствию 3.12 $l(\mathcal{B}) \leqslant n-2$, значит, найдётся элемент $V'' \in \mathcal{L}_{n-2}(\{S_1'', \ldots, S_{n-1}''\})$, такой что $S_1'' \cdots S_{n-1}'' - V'' = 0$. Положим $W'' = V'' \cdot S_n'' \in \mathcal{L}_{n-1}(\{S_1'', \ldots, S_n''\}$ и заметим, что W'' — линейная комбинация слов положительной длины от элементов $S_1'', \ldots, S_n''$. Пусть $W \in \mathcal{L}_{n-1}(\mathcal{S})$ — прообраз W''. Тогда $S_1 \cdots S_n + W = S' \oplus 0$, $S' \in \mathrm{N}_n(\mathbb{F})$, но $S' \oplus 0 \in \mathcal{L}_{n-1}(\mathcal{S})$ по доказанному в пунктах 1 и 2. Значит, слово $S_1 \cdots S_n$ сократимо.

Таким образом, мы получили, что любое слово длины n от элементов $\mathcal{S}$ сократимо, $\mathcal{L}_n(\mathcal{S}) = \mathcal{L}_{n-1}(\mathcal{S})$ и $l(\mathcal{S}) \leqslant n-1$.

II. Из теоремы 3.9 о прямой сумме получаем

$$l(\mathcal{A}_{n,n-1}) \geqslant \max\{n-1, n-2\} = n-1.$$

Следовательно, $l(\mathcal{A}_{n,n-1}) = n-1$. □

Лемма 5.23. *Пусть $\mathbb{F}$ — произвольное поле, $n \in \mathbb{N}$ и $n > 2$. Тогда $l(\mathcal{A}_{n,n}) = n$.*

Доказательство. I. Сначала докажем верхнюю оценку $l(\mathcal{A}_{n,n}) \leqslant n$. Для этого рассмотрим произвольную систему порождающих $\mathcal{S}$ для $\mathcal{A}_{n,n}$. Не ограничивая общности, можно считать, что $\mathcal{S}$ удовлетворяет условиям 1)—4) леммы 5.17 и, значит, одному из условий леммы 5.18.

1. Индукцией по $p = n - (j - i)$ докажем, что $E_{i,j}, E_{i+n,j+n} \in \mathcal{L}_n(\mathcal{S})$ при $1 \leqslant i < j \leqslant n$, $j - i \geqslant 2$.

База индукции. Рассмотрим случай $p = 1$.

а) Предположим, что нет такого k, что $A_0 = B_k$. Тогда

$$B_1 B_2 \cdots B_{n-1}(E - A_0) = E_{1,n} \in \mathcal{L}_n(\mathcal{S}),$$

поскольку $B_1'' B_2'' \cdots B_{n-1}''(E - A_0)'' = 0$ как произведение n нильпотентных матриц порядка n.

б) Пусть $A_0 = B_k$. Тогда

$$B_1 B_2 \cdots B_{n-1} = a_k E_{1,n} + \alpha_1 E_{n+1,2n-1} + \alpha_2 E_{n+1,2n} + \alpha_3 E_{n+2,2n}.$$

Если система порождающих $\mathcal{S}$ удовлетворяет условию а) леммы 5.18, то $(\tilde{A}_0)_{n+1,n+2} = (\tilde{A}_0)_{2n-1,2n} = 0$. Если система порождающих $\mathcal{S}$ удовлетворяет условию б) леммы 5.18, то, поскольку $n = m > 2$, для введённого там индекса $s \in \{1, \ldots, n-1\}$ выполняется хотя бы одно из неравенств $s \neq 1$ или $s \neq n-1$. При $s \neq 1$ верно $(\tilde{A}_0)_{n+1,n+2} = 0$, а при $s \neq n-1$ верно $(\tilde{A}_0)_{2n-1,2n} = 0$. Также если $(\tilde{A}_0)_{n+1,n+2} = 0$, то $\tilde{A}_0 B_1 B_2 \cdots B_{n-1} = E_{1,n}$, и если $(\tilde{A}_0)_{n+1,n+2} = 0$, то $B_1 B_2 \cdots B_{n-1} \tilde{A}_0 = E_{1,n}$. Значит, $E_{1,n} \in \mathcal{L}_n(\mathcal{S})$. Также $C_1 \cdots C_{n-1} A_0 = a E_{1,n} + b E_{n+1,2n} \in \mathcal{L}_n(\mathcal{S})$, $b \neq 0$, следовательно, $E_{n+1,2n} = b^{-1}(C_1 \cdots C_{n-1} A_0 - a E_{1,n}) \in \mathcal{L}_n(\mathcal{S})$.

Шаг индукции. Предположим, что утверждение верно для всех q, $1 < q < p$. Рассмотрим произведения

$$B_{j,j+n-p-1} = B_j B_{j+1} \cdots B_{j+n-p-1}(E - A_0)^p \in \mathcal{L}_n(\mathcal{S}), \quad j = 1, \ldots, p.$$

Имеем

$$B'_{j,j+n-p-1} = a_k^t E_{j,j+n-p} + \sum_{h=1}^{n} \sum_{i=h+n-p+1}^{n} b_{h,i;j,p} E_{h,i}, \quad t \in \{0,1\},$$

и $B''_{j,j+n-p-1} = b(j,p)E_{n+1,2n}$, $b(j,p) \in \mathbb{F}$, как произведение n нильпотентных матриц порядка n при $t=0$ и как произведение $n-1$ нильпотентной и одной унитреугольной матрицы порядка n при $t=1$.

Также рассмотрим произведения

$$C_{j,j+n-p-1} = C_j C_{j+1} \cdots C_{j+n-p-1} A_0^p \in \mathcal{L}_n(\mathcal{S}), \quad j=1,\ldots,p.$$

Имеем

$$C''_{j,j+n-p-1} = (\tilde{a}_s)^t E_{j+n,j+2n-p} + \sum_{h=1}^{n} \sum_{i=h+n-p+1}^{n} c_{h,i;j,p} E_{h+n,i+n}, \quad t \in \{0,1\},$$

и $C'_{j,j+n-p-1} = c(j,p)E_{1,n}$ как произведение n нильпотентных матриц порядка n при $t=0$ и как произведение $n-1$ нильпотентной и одной унитреугольной матрицы порядка n при $t=1$.

По предположению индукции $E_{i,i+n-q-1}, E_{i+n,i+2n-q-1} \in \mathcal{L}_n(\mathcal{S})$ для любых $q=2,\ldots,p-1$, $i=1,\ldots,q$, и, как показано ранее, $E_{1,n}, E_{n+1,2n} \in \mathcal{L}_n(\mathcal{S})$. Значит,

$$B_{j,j+n-p-1} - (a_k)^t E_{j,j+n-p}, C_{j,j+n-p-1} - (a_s)^t E_{j+n,j+2n-p} \in \mathcal{L}_n(\mathcal{S}).$$

Поскольку $B_{j,j+n-p-1}, C_{j,j+n-p-1} \in \mathcal{L}_n(\mathcal{S})$ по определению, получаем, что

$$E_{j,j+n-p-1} = (a_k)^{-t}\big(B_{j,j+n-p-1} - (B_{j,j+n-p-1} - (a_k)^t E_{j,j+n-p})\big) \in \mathcal{L}_n(\mathcal{S}),$$

$$E_{j+n,j+2n-p-1} =$$
$$= (a_s)^{-t}\big(C_{j,j+n-p-1} - (C_{j,j+n-p-1} - (a_s)^t E_{j+n,j+2n-p})\big) \in \mathcal{L}_n(\mathcal{S}), \quad j=1,\ldots,p.$$

2. Теперь рассмотрим матрицы

$$B_{j,j} = B_j(E-A_0)^{n-1} \in \mathcal{L}_n(\mathcal{S}), \quad C_{j,j} = C_j A_0^{n-1} \in \mathcal{L}_n(\mathcal{S}), \quad j=1,\ldots,n-1.$$

По построению

$$(B_{j,j})_{r,r+1} = (B_j)_{r,r+1}, \quad j,r=1,\ldots,n-1,$$

и

$$(C_{j,j})_{r+n,r+n+1} = (C_j)_{r+n,r+n+1}, \quad j,r=1,\ldots,n-1,$$

т. е.

$$B'_{j,j} = E_{j,j+1} + \beta_j E_{k,k+1} + \sum_{h=1}^{n} \sum_{i=h+2}^{n} b_{h,i;j,n-1} E_{h,i}, \quad j \neq k,$$

$$B'_{k,k} = (a_k)^t E_{k,k+1} + \sum_{h=1}^{n} \sum_{i=h+2}^{n} b_{h,i;k,n-1} E_{h,i}, \quad t \in \{0,1\},$$

$$C''_{j,j} = E_{j+n,j+n+1} + \gamma_j E_{s+n,s+n+1} + \sum_{h=1}^{n} \sum_{i=h+2}^{n} c_{h,i;j,n-1} E_{h+n,i+n}, \quad j \neq s,$$

$$C''_{s,s} = (\tilde{a}_s)^u E_{s+n,s+n+1} + \sum_{h=1}^{n} \sum_{i=h+2}^{n} c_{h,i;s,n-1} E_{h,i}, \quad u \in \{0,1\}.$$

При этом $B''_{r,r} = b(j)E_{1,n}$ как произведение n нильпотентных матриц порядка n при $r \neq k$ либо при $r = k$ и $t = 0$ и как произведение $n-1$ нильпотентной и одной унитреугольной матрицы порядка n при $r = k$ и $t = 1$; аналогично $C'_{r,r} = c(r)E_{1,n}$.

По доказанному в пункте 1

$$B_{k,k} - (a_k)^t E_{k,k+1}, C_{s,s} - (a_s)^t E_{s+n,s+n+1} \in \mathcal{L}_n(\mathcal{S}).$$

Значит, и $E_{k,k+1}, E_{s+n,s+n+1} \in \mathcal{L}_n(\mathcal{S})$. Тогда

$$E_{j,j+1} = B_{j,j} - \sum_{h=1}^{n} \sum_{i=h+2}^{n} b_{h,i;j,n-1} E_{h,i} - \beta_j E_{k,k+1} - b(j) E_{n+1,2n} \in \mathcal{L}_{n-1}(\mathcal{S}),$$

$$E_{j+n,j+n+1} = C_{j,j} - \sum_{h=1}^{n} \sum_{i=h+2}^{n} c_{h,i;j,n-1} E_{h,i} - \gamma_j E_{s+n,s+n+1} - c(j) E_{1,n} \in \mathcal{L}_{n-1}(\mathcal{S}).$$

Следовательно, $E_{i,j}, E_{i+n,j+n} \in \mathcal{L}_{n-1}(\mathcal{S})$, $1 \leqslant i < j \leqslant n$.

3. Из соотношения

$$0 \oplus E'' = A_0 - (A_0)_{k,k} E_{k,k+1} - \sum_{1 \leqslant i < j \leqslant n} (\hat{a}_{i,j} E_{i,j} + \hat{a}_{i+n,j+n} E_{i+n,j+n})$$

получаем, что $0 \oplus E'' \in \mathcal{L}_n(\mathcal{S})$.

Значит, для любой системы порождающих $\mathcal{S}$ верно $\mathcal{L}_n(\mathcal{S}) = \mathcal{A}_{n,n}$, т. е. $l(\mathcal{A}_{n,n}) \leqslant n$.

II. Построим систему порождающих для алгебры $\mathcal{A}_{n,n}$ длины n. Пусть

$$\mathcal{S}_n = \left\{ A_i = E_{i,i+1} + E_{n+i,n+i+1},\ i = 1, \ldots, n-1,\ E,\ E_n = \sum_{j=1}^{n} E_{j,j} \right\}.$$

Так как $A_i A_j = 0$ при $j \neq i+1$ и $E_n A_i = A_i E_n = E_{i,i+1}$, то $E_{1,n} \notin \mathcal{L}_{n-1}(\mathcal{S}_n)$, где

$$\mathcal{L}_{n-1}(\mathcal{S}_n) = \left\langle E,\ E_n,\ E_{i,j},\ E_{i+n,j+n},\ E_{1,n} + E_{n+1,2n} \;\middle|\; \begin{array}{l} 1 \leqslant i < j \leqslant n, \\ j - i \leqslant n-2 \end{array} \right\rangle,$$

но $E_{1,n} = A_1 \cdots A_{n-1} E_n \in \mathcal{L}_n(\mathcal{S}_n)$, и значит, $\mathcal{L}_n(\mathcal{S}_n) = \mathcal{A}_{n,n}$. Следовательно, $l(\mathcal{A}_{n,n}) = n$. □

Объединяя леммы 5.19—5.23, получаем следующую теорему.

Теорема 5.24. *Пусть $\mathbb{F}$ — произвольное поле, $n \geqslant m$ — натуральные числа,*

$$\mathcal{A}_{n,m} = \left\langle E,\ \sum_{i=1}^{n} E_{i,i},\ E_{i,j} \;\middle|\; \begin{array}{l} 1 \leqslant i < j \leqslant n \\ \text{или} \\ n+1 \leqslant i < j \leqslant n+m \end{array} \right\rangle \subset \mathrm{T}_{m+n}(\mathbb{F}).$$

Тогда

$$l(\mathcal{A}_{n,m}) = \begin{cases} n-1 & \text{при } \; n-m \geqslant 2, \\ n-1 & \text{при } \; n = m+1, \; n > 3, \\ n+1 & \text{при } \; n = m = 2, \\ n & \text{при } \; n = m \neq 2, \\ n & \text{при } \; n = m+1, \; m = 1, 2. \end{cases}$$

Следствие 5.25. *Пусть* $\mathbb{F}$ *— произвольное поле,* $n \geqslant m$ *— фиксированные натуральные числа. Пусть*

$$C_{n,m} = \sum_{i=1}^{n-1} E_{i,i+1} + \sum_{j=1}^{m-1} (E_{j+n,j+n} + E_{j+n,j+n+1}) + E_{n+m,n+m} \in \mathcal{A}_{n,m} \; -$$

циклическая матрица,

$$\mathcal{A}'_{n,m} = \langle C_{n,m}^j \mid 0 \leqslant j \leqslant n+m-1 \rangle \subseteq \mathcal{A}_{n,m}.$$

Тогда

1) $l(\mathcal{A}'_{n,m}) = n+m-1$ *по лемме* 4.5;
2) *при* $n = m = 1, 2$ *и* $n = 2$, $m = 1$ $\mathcal{A}_{n,m} = \mathcal{A}'_{n,m}$ *и* $l(\mathcal{A}_{n,m}) = l(\mathcal{A}'_{n,m})$;
3) *при* $n \geqslant 3$

$$l(\mathcal{A}'_{n,m}) - l(\mathcal{A}_{n,m}) = \begin{cases} m & \text{при } \; n-m \geqslant 2 \text{ или } n = m+1, \; n > 3, \\ m-1 & \text{при } \; n = m \geqslant 3 \text{ или } n = 3, \; m = 2 \end{cases}$$

и

$$\frac{l(\mathcal{A}'_{n,m})}{l(\mathcal{A}_{n,m})} = \begin{cases} 1 + m/(n-1) & \text{при } \; n-m \geqslant 2 \text{ или } n = m+1, \; n > 3, \\ 1 + (m-1)/n & \text{при } \; n = m \geqslant 3 \text{ или } n = 3, \; m = 2. \end{cases}$$

Следствие 5.26. *Отношение длины подалгебры двухблочной алгебры к длине алгебры может быть любым рациональным числом из отрезка* $[1, 2]$.

5.1.2. Алгебры с тремя блоками

В данном разделе рассмотрены трёхпараметрические семейства алгебр

$$\mathcal{A}_{n_1,n_2,n_3} \subset \mathrm{T}_{n_1}(\mathbb{F}) \oplus \mathrm{T}_{n_2}(\mathbb{F}) \oplus \mathrm{T}_{n_3}(\mathbb{F}),$$

$$\mathcal{A}_{n_1,n_2,n_3} = \left\langle E, \; \sum_{i=1}^{n_1} E_{i,i}, \; \sum_{i=n_1+1}^{n_1+n_2} E_{i,i}, \; E_{i,j} \;\middle|\; \begin{array}{l} 1 \leqslant i < j \leqslant n_1, \text{ или} \\ n_1+1 \leqslant i < j \leqslant n_1+n_2, \text{ или} \\ n_1+n_2+1 \leqslant i < j \leqslant n_1+n_2+n_3 \end{array} \right\rangle$$

над произвольным полем $\mathbb{F}$. При некоторых ограничениях на значения параметров n_1, n_2, n_3 длины таких алгебр вычислены явно. При $\mathbb{F} \neq \mathbb{F}_2$ подобраны подалгебры $\mathcal{A}'_{n_1,n_2,n_3} \subset \mathcal{A}_{n_1,n_2,n_3}$, для которых $l(\mathcal{A}'_{n_1,n_2,n_3}) > l(\mathcal{A}_{n_1,n_2,n_3})$, отношение длин

$$r = \frac{l(\mathcal{A}'_{n_1,n_2,n_3})}{l(\mathcal{A}_{n_1,n_2,n_3})}$$

принадлежит интервалу $(1,3)$ (см. следствия 5.36, 5.37 и 5.41. В частности, построена серия алгебр с отношением длин $r > 2$.

Обозначение 5.27. Любая матрица $A \in \mathcal{A}_{n_1,n_2,n_3}$ имеет вид

$$A = \begin{pmatrix} A' & 0 & 0 \\ 0 & A'' & 0 \\ 0 & 0 & A''' \end{pmatrix}, \quad \text{где} \quad A' \in \mathrm{T}_{n_1}(\mathbb{F}), \quad A'' \in \mathrm{T}_{n_2}(\mathbb{F}), \quad A''' \in \mathrm{T}_{n_3}(\mathbb{F}).$$

Далее будем использовать обозначение $A = A' \oplus A'' \oplus A'''$.

В следующих четырёх леммах будет показано, что в системах порождающих можно выбрать элементы специального вида, которые нужны для дальнейшего вычисления длин алгебр $\mathcal{A}_{n_1,n_2,n_3}$.

Лемма 5.28. *Пусть $\mathcal{S}$ — произвольная система порождающих для алгебры $\mathcal{A}_{n_1,n_2,n_3}$. Тогда существует система порождающих $\tilde{\mathcal{S}}$ для $\mathcal{A}_{n_1,n_2,n_3}$, такая что выполнены следующие условия*:

1) $\dim \mathcal{L}_1(\tilde{\mathcal{S}}) = |\tilde{\mathcal{S}}| + 1$;
2) *для любой матрицы $S \in \tilde{\mathcal{S}}$ выполнено $(S)_{i,i} = 0$, $i = 1, \ldots, n_1$;*
3) а) *либо существуют такие матрицы $A_1 = (a_{i,j;1})$, $A_2 = (a_{i,j;2}) \in \tilde{\mathcal{S}}$, что*

$$\begin{aligned} A_1'' &= E + N_1, \quad N_1 \in \mathrm{N}_{n_2}(\mathbb{F}), \quad A_1''' \in \mathrm{N}_{n_3}(\mathbb{F}), \\ A_2'' &\in \mathrm{N}_{n_2}(\mathbb{F}), \quad A_2''' = E + N_2, \quad N_2 \in \mathrm{N}_{n_3}(\mathbb{F}), \end{aligned}$$

и для всех $S \in \tilde{\mathcal{S}}$, $S \neq A_1, A_2$, выполнено $(S)_{i,i} = 0$, $i = 1, \ldots, n_1 + n_2 + n_3$,

б) *либо существует такая матрица $A_0 = (a_{i,j;0})$, что*

$$A_0'' = E + N, \quad N \in \mathrm{N}_{n_2}(\mathbb{F}), \quad A_0''' = aE + M, \quad M \in \mathrm{N}_{n_3}(\mathbb{F}), \quad a \notin \{0,1\},$$

и для всех $S \in \mathcal{S}$, $S \neq A_0$, выполнено $(S)_{i,i} = 0$, $i = 1, \ldots, n_1 + n_2 + n_3$;

4) $l(\tilde{\mathcal{S}}) = l(\mathcal{S})$.

Доказательство. Будем последовательно преобразовывать $\mathcal{S}$ до системы порождающих, удовлетворяющей условиям 1)—4).

Условие 1). Данное условие можно считать выполненным согласно предложению 3.4.

Условие 2). По предложению 3.2 с сохранением длины перейдём к системе порождающих

$$\mathcal{S}_1 = \{S - (S)_{1,1}E \mid S \in \mathcal{S}\}.$$

Условие 3а). Пусть существуют такие матрицы $C_1, C_2 \in \mathcal{S}_1$, что векторы

$$\begin{aligned} c_1 &= \big((C_1)_{n_1+1,n_1+1},\, (C_1)_{n_1+n_2+1,n_1+n_2+1}\big), \\ c_2 &= \big((C_2)_{n_1+1,n_1+1},\, (C_2)_{n_1+n_2+1,n_1+n_2+1}\big) \end{aligned}$$

линейно независимы. В этом случае существует невырожденная матрица $F = (f_{i,j}) \in \mathrm{M}_2(\mathbb{F})$, такая что

$$(1,0) = f_{1,1}c_1 + f_{1,2}c_2, \quad (0,1) = f_{2,1}c_1 + f_{2,2}c_2.$$

Положим
$$A_i = f_{i,1}C_1 + f_{i,2}C_2, \quad i = 1, 2,$$
и по предложению 3.1 с сохранением длины перейдём к системе порождающих
$$\mathcal{S}_2 = \{A_1,\, A_2,\, S \mid S \in \mathcal{S}_1,\ S \neq C_1, C_2\}.$$
Затем по предложению 3.1 с сохранением длины перейдём к системе порождающих
$$\mathcal{S}_3 = \{A_1,\, A_2,\, S - (S)_{n_1+1,n_1+1}A_1 - (S)_{n_1+n_2+1,n_1+n_2+1}A_2 \mid S \in \mathcal{S}_2,\ S \neq A_1, A_2\}.$$
Положим $\tilde{\mathcal{S}} = \mathcal{S}_3$.

Условие 3б). Если не выполнено условие предыдущего пункта, то в $\mathcal{S}_1$ есть такая матрица A, что векторы
$$\big((A)_{n_1+1\ n_1+1},\, (A)_{n_1+n_2+1\ n_1+n_2+1}\big), \quad \big((A^2)_{n_1+1\ n_1+1},\, (A^2)_{n_1+n_2+1\ n_1+n_2+1}\big)$$
линейно независимы и вектор
$$\big((A)_{n_1+1\ n_1+1},\, (A)_{n_1+n_2+1\ n_1+n_2+1}\big)$$
образует базис пространства
$$\big\langle \big((S)_{n_1+1,n_1+1},\, (S)_{n_1+n_2+1,n_1+n_2+1}\big) \bigm| S \in \mathcal{S}_1 \big\rangle.$$
По условию собственные числа матрицы A, отвечающие второму и третьему блокам, различны и отличны от нуля. Значит, с сохранением длины можно заменить в $\mathcal{S}_1$ матрицу A на матрицу $A_0 = (A)^{-1}_{n_1+1,n_1+1}A$. Тогда по предложению 3.1 с сохранением длины перейдём к системе порождающих
$$\mathcal{S}_2 = \{A_0,\, S - (S)_{n_1+1,n_1+1}A_0 \mid S \in \mathcal{S}_1,\ S \neq A_0\}.$$
Положим $\tilde{\mathcal{S}} = \mathcal{S}_2$.

Условие 4). Преобразования системы $\mathcal{S}$ из пунктов 1)—3) не меняли её длины, следовательно, длина полученной системы порождающих $\tilde{\mathcal{S}}$ равна длине исходной системы. □

Лемма 5.29. *Пусть $n_1 \geqslant 3$, и пусть $\mathcal{S}$ — система порождающих для $\mathcal{A}_{n_1,n_2,n_3}$, удовлетворяющая условиям* 1), 2 *и* 3а) *леммы* 5.28. *Тогда существует система порождающих $\tilde{\mathcal{S}}$ для $\mathcal{A}_{n_1,n_2,n_3}$ с условием $l(\tilde{\mathcal{S}}) = l(\mathcal{S})$ и существуют такие $B_1, \ldots, B_{n_1-1} \in \tilde{\mathcal{S}}$ и $k_1, k_2 \in \{1, \ldots, n_1 - 1\}$, что выполнено одно из следующих условий*:

1)
$$B'_r = E_{r,r+1} + \sum_{i=1}^{n_1} \sum_{j=i+2}^{n_1} b_{i,j;r}E_{i,j}, \quad B''_r \in \mathrm{N}_{n_2}(\mathbb{F}),$$
$$B'''_r \in \mathrm{N}_{n_3}(\mathbb{F}), \quad r = 1, \ldots, n-1,$$
$$A'_s = \sum_{h=1}^{n_1} \sum_{i=h+2}^{n_1} a_{h,i;s}E_{h,i}, \quad s = 1, 2;$$

2) *найдётся* $j \in \{1,2\}$, *для которого*

$$B'_r = E_{r,r+1} + b_{rj}E_{k_j,k_j+1} + \sum_{h=1}^{n_1}\sum_{i=h+2}^{n_1} b_{h,i;r}E_{h,i},$$

$$B''_r \in \mathrm{N}_{n_2}(\mathbb{F}),\quad B'''_r \in \mathrm{N}_{n_3}(\mathbb{F}),\quad r = 1,\ldots,n_1-1,\quad r \neq k_j,$$

$$A'_j = B'_{k_j} = a(k_j,j)E_{k_j,k_j+1} + \sum_{h=1}^{n_1}\sum_{i=h+2}^{n_1} a_{h,i;j}E_{h,i},\quad a(k_j,j) \neq 0,$$

$$B''_{k_j} = A''_j,\quad B'''_{k_j} = A'''_j,$$

$$A'_{3-j} = a(k_j,3-j)E_{k_j,k_j+1} + \sum_{h=1}^{n_1}\sum_{i=h+2}^{n_1} a_{h,i;3-j}E_{h,i};$$

3)
$$B'_r = E_{r,r+1} + b_{r1}E_{k_1,k_1+1} + b_{r2}E_{k_2,k_2+1} + \sum_{h=1}^{n_1}\sum_{i=h+2}^{n_1} b_{h,i;r}E_{h,i},$$

$$B''_r \in \mathrm{N}_{n_2}(\mathbb{F}),\quad B'''_r \in \mathrm{N}_{n_3}(\mathbb{F}),\quad r = 1,\ldots,n_1-1,\quad r \neq k_1,k_2,$$

$$A'_j = B'_{k_j} = a(k_1,j)E_{k_1,k_1+1} + a(k_2,j)E_{k_2,k_2+1} + \sum_{h=1}^{n_1}\sum_{i=h+2}^{n_1} a_{h,i;j}E_{h,i},$$

$$a(k_j,j) \neq 0,\quad a(k_1,1)a(k_2,2) - a(k_2,1)a(k_1,2) \neq 0,$$

$$B''_{k_j} = A''_j,\quad B'''_{k_j} = A'''_j,\quad j = 1,2.$$

Доказательство. Поскольку $E_{i,i+1} \in \mathcal{A}_{n_1,n_2,n_3}$, но для любых $t \geqslant 2$ и $S \in \mathcal{S}^t \setminus \mathcal{S}^{t-1}$ коэффициент $(S)_{i,i+1}$ равен 0, $i = 1,\ldots,n_1-1$, то найдутся такие $B_1,\ldots,B_{n_1-1} \in \mathcal{S}$, что векторы $\big((B_i)_{1,2},(B_i)_{2,3},\ldots,(B_i)_{n_1-1,n_1}\big)$, $i = 1,\ldots,n_1-1$, линейно независимы.

Теперь выполним следующее преобразование $\mathcal{F}$ системы $\mathcal{S}$ (по предложению 3.1 оно сохраняет длину $\mathcal{S}$): все элементы $S \in \mathcal{S}$, $S \neq B_i$, $i = 1,\ldots,n_1-1$, $S \neq A_1,A_2$, оно оставляет на месте, а его действие на множество матриц B_j, $j = 1,\ldots,n_1-1$, и на матрицах A_1, A_2 зависит от принадлежности матриц A_1 и A_2 этому множеству.

Если $|\{B_1,\ldots,B_{n_1-1}\}\cap\{A_1,A_2\}| \leqslant 1$, то преобразование $\mathcal{F}$ строится так же, как в пункте 4) леммы 5.17.

Пусть существуют различные p и q, для которых $A_1 = B_p$ и $A_2 = B_q$. Тогда существуют $k_1,\ k_2 \in \{1,\ldots,n_1-1\}$, $k_1 < k_2$, такие что векторы

$$v_i = \big((B_i)_{1,2},\ldots,(B_i)_{k_1-1,k_1},(B_i)_{k_1+1,k_1+2},\ldots,\\ (B_i)_{k_2-1,k_2},(B_i)_{k_2+1,k_2+2}(B_i)_{n_1-1,n_1}\big),\quad i = 1,\ldots,n_1-1,\quad i \neq p,q,$$

линейно независимы. Поскольку порядок матриц B_j произволен, можно считать, что $p = k_1$, $q = k_2$. Невырожденным линейным преобразованием $G = \{g_{i,j}\} \in \mathrm{M}_{n_1-3}(\mathbb{F})$ можно перевести набор $\{v_i\}$ в набор

$$\{e_1 = (1,0,\ldots,0),\ e_2 = (0,1,\ldots,0),\ldots,\ e_{n_1-3} = (0,0,\ldots,1)\} \subset \mathbb{F}^{n_1-3},$$

т. е.

$$e_i = \sum_{j=1}^{k_1-1} g_{i,j} v_j + \sum_{j=k_1}^{k_2-1} g_{i,j} v_{j+1} + \sum_{j=k_2}^{n_1-1} g_{i,j} v_{j+2}.$$

Тогда положим

$$\mathcal{F}(B_r) = \sum_{j=1}^{k_1-1} g_{r,j} B_j + \sum_{j=k_1}^{k_2-1} g_{r,j} B_{j+1} + \sum_{j=k_2}^{n_1-1} g_{r,j} B_{j+2}, \quad r < k_1,$$

$$\mathcal{F}(B_r) = \sum_{j=1}^{k_1-1} g_{r-1,j} B_j + \sum_{j=k_1}^{k_2-1} g_{r-1,j} B_{j+1} + \sum_{j=k_2}^{n_1-1} g_{r-1,j} B_{j+2}, \quad k_1 < r < k_2,$$

$$\mathcal{F}(B_r) = \sum_{j=1}^{k_1-1} g_{r-2,j} B_j + \sum_{j=k_1}^{k_2-1} g_{r-2,j} B_{j+1} + \sum_{j=k_2}^{n_1-1} g_{r-2,j} B_{j+2}, \quad r > k_2,$$

$$\mathcal{F}(A_s) = A_s - \sum_{\substack{i=1,\\ i\neq k_1,k_2}}^{n_1-1} (A_s)_{i,i+1} \mathcal{F}(B_i), \quad s = 1, 2.$$

Имеем

$$\mathcal{F}(B_r)' = E_{r,r+1} + b_{r1} E_{k_1,k_1+1} + b_{r2} E_{k_2,k_2+1} + \sum_{h=1}^{n_1} \sum_{i=h+2}^{n_1} b_{h,i;r} E_{h,i},$$

$$\mathcal{F}(B_r)'' \in \mathrm{N}_{n_2}(\mathbb{F}), \quad \mathcal{F}(B_r)''' \in \mathrm{N}_{n_3}(\mathbb{F}), \quad r = 1, \ldots, n_1 - 1, \quad r \neq k_1, k_2,$$

$$\mathcal{F}(A_j)' = \mathcal{F}(B_{k_j})' = a(k_1, j) E_{k_1,k_1+1} + a(k_2, j) E_{k_2,k_2+1} + \sum_{h=1}^{n_1} \sum_{i=h+2}^{n_1} a_{h,i;j} E_{h,i},$$

$$a(k_j, j) \neq 0, \quad a(k_1,1)a(k_2,2) - a(k_2,1)a(k_1,2) \neq 0,$$

$$\mathcal{F}(B_{k_j})'' = \mathcal{F}(A_j)'', \quad \mathcal{F}(B_{k_j})''' = \mathcal{F}(A_j)''', \quad j = 1, 2.$$

Положим $\tilde{\mathcal{S}} = \mathcal{F}(\mathcal{S})$. □

Лемма 5.30. *Пусть $n_1 \geqslant 3$, и пусть $\mathcal{S}$ — система порождающих для $\mathcal{A}_{n_1,n_2,n_3}$, удовлетворяющая условиям* 1), 2) *и* 3б) *леммы* 5.28. *Тогда существует система порождающих $\tilde{\mathcal{S}}$ для $\mathcal{A}_{n_1,n_2,n_3}$ с условием $l(\tilde{\mathcal{S}}) = l(\mathcal{S})$ и существуют такие матрицы $B_1, \ldots, B_{n_1-1} \in \tilde{\mathcal{S}}$ и индекс $k_0 \in \{1, \ldots, n_1 - 1\}$, что выполнено одно из следующих условий*:

1) $$B'_r = E_{r,r+1} + \sum_{i=1}^{n_1} \sum_{j=i+2}^{n_1} b_{i,j;r} E_{i,j}, \quad B''_r \in \mathrm{N}_{n_2}(\mathbb{F}),$$

$$B'''_r \in \mathrm{N}_{n_3}(\mathbb{F}), \quad r = 1, \ldots, n - 1,$$

$$A'_0 = \sum_{h=1}^{n_1} \sum_{i=h+2}^{n_1} a_{h,i;0} E_{h,i};$$

2)
$$B'_r = E_{r,r+1} + b_{r0}E_{k_0,k_0+1} + \sum_{h=1}^{n_1}\sum_{i=h+2}^{n_1} b_{h,i;r}E_{h,i},$$
$$B''_r \in \mathrm{N}_{n_2}(\mathbb{F}),\quad B'''_r \in \mathrm{N}_{n_3}(\mathbb{F}),\quad r = 1,\ldots,n_1-1,\quad r \neq k_0,$$
$$A'_0 = B'_{k_0} = a(k_0,0)E_{k_0,k_0+1} + \sum_{h=1}^{n_1}\sum_{i=h+2}^{n_1} a_{h,i;0}E_{h,i},\quad a(k_0,0)\neq 0,$$
$$B''_{k_0} = A''_0,\quad B'''_{k_0} = A'''_0.$$

Доказательство. По условию матричные единицы $E_{i,i+1}$ принадлежат $\mathcal{A}_{n_1,n_2,n_3}$, но для любых $t \geqslant 2$ и $S \in \mathcal{S}^t \setminus \mathcal{S}^{t-1}$ коэффициент $(S)_{i,i+1}$ равен 0, $i = 1,\ldots,n_1-1$, следовательно, найдутся матрицы $B_1,\ldots,B_{n_1-1} \in \mathcal{S}$, такие что векторы
$$u_i = \big((B_i)_{1,2},(B_i)_{2,3},\ldots,(B_i)_{n_1-1,n_1}\big),\quad i = 1,\ldots,n_1-1,$$
линейно независимы.

Теперь выполним преобразование $\mathcal{F}$ системы порождающих $\mathcal{S}$ (по предложению 3.1 $\mathcal{F}$ сохраняет длину $\mathcal{S}$), которое на всех элементах $S \in \mathcal{S}$, $S \neq B_i$, $i = 1,\ldots,n_1-1$, и $S \neq A_0$, действует тождественно, т. е. $\mathcal{F}(S) = S$, а действие $\mathcal{F}$ на множестве матриц $\{B_j \mid j = 1,\ldots,n_1-1\}$ и на матрице A_0 в зависимости от принадлежности матрицы A_0 этому множеству определяется следующим образом.

Условие 1). Пусть $A_0 \notin \{B_1,\ldots,B_{n_1-1}\}$. Невырожденным линейным преобразованием $F = \{f_{i,j}\} \in \mathrm{M}_{n_1-1}(\mathbb{F})$ можно перевести набор векторов $\{u_i \mid i = 1,\ldots,n_1-1\}$ в набор
$$\{e_1 = (1,0,\ldots,0),\, e_2 = (0,1,\ldots,0),\ldots,\, e_{n_1-1} = (0,0,\ldots,1)\} \subset \mathbb{F}^{n_1-1},$$
т. е.
$$e_i = \sum_{j=1}^{n_1-1} f_{i,j}u_j.$$
Тогда положим
$$\mathcal{F}(B_r) = \sum_{j=1}^{n_1-1} f_{r,j}B_j.$$
При этом
$$\mathcal{F}(B_r)' = E_{r,r+1} + \sum_{i=1}^{n_1}\sum_{j=i+2}^{n_1} b_{i,j;r}E_{i,j},$$
$$\mathcal{F}(B_r)'' \in \mathrm{N}_{n_2}(\mathbb{F}),\quad \mathcal{F}(B_r)''' \in \mathrm{N}_{n_3}(\mathbb{F}),\quad r = 1,\ldots,n_1-1.$$
Также положим
$$\mathcal{F}(A_0) = A_0 - \sum_{i=1}^{n_1-1}(A_0)_{i,i+1}\mathcal{F}(B_i).$$

Условие 2). Пусть $A_0 \in \{B_1, \ldots, B_{n_1-1}\}$, т. е. $A_0 = B_p$ для некоторого $p \in \{1, \ldots, n_1 - 1\}$. Так как у любой матрицы в $\mathrm{M}_{n_1-1,n_1-2}(\mathbb{F})$ ранга $n_1 - 2$ существует невырожденная подматрица порядка $n_1 - 2$, то найдётся индекс $k_0 \in \in \{1, \ldots, n_1 - 1\}$, такой что векторы

$$v_i = \big((B_i)_{1,2}, \ldots, (B_i)_{k_0-1,k_0}, (B_i)_{k_0+1,k_0+2}, \ldots, (B_i)_{n_1-1,n_1}\big),\\ i = 1, \ldots, n_1 - 1, \quad i \neq p,$$

линейно независимы. Поскольку упорядочивание матриц B_j произвольно, можно считать, что $p = k_0$. Невырожденным линейным преобразованием $G = \{g_{i,j}\} \in \mathrm{M}_{n_1-2}(\mathbb{F})$ можно перевести набор векторов $\{v_i \mid i = 1, \ldots, n_1 - 1, i \neq k_0\}$ в набор

$$\{e_1 = (1, 0, \ldots, 0),\ e_2 = (0, 1, \ldots, 0),\ \ldots,\ e_{n_1-2} = (0, 0, \ldots, 1)\} \subset \mathbb{F}^{n_1-2},$$

т. е.

$$e_i = \sum_{j=1}^{k_0-1} g_{i,j} v_j + \sum_{j=k_0}^{n_1-2} g_{i,j} v_{j+1}.$$

Тогда положим

$$\mathcal{F}(B_r) = \sum_{j=1}^{k_0-1} f_{r,j} B_j + \sum_{j=k_0}^{n_1-2} f_{r,j} B_{j+1}, \quad r < k_0,$$

$$\mathcal{F}(B_r) = \sum_{j=1}^{k_0-1} f_{r-1,j} B_j + \sum_{j=k_0}^{n_1-2} f_{r-1,j} B_{j+1}, \quad r > k_0,$$

$$\mathcal{F}(A_0) = A_0 - \sum_{\substack{i=1,\\ i\neq k_0}}^{n_1-1} (A_0)_{i,i+1} \mathcal{F}(B_i).$$

Имеем

$$\mathcal{F}(B_r)' = E_{r,r+1} + b_{r0} E_{k_0,k_0+1} + \sum_{i=1}^{n_1} \sum_{j=i+2}^{n_1} b_{i,j;r} E_{i,j} \quad \text{для} \quad r \neq k_0,$$

$$\mathcal{F}(A_0)' = a(k_0, 0) E_{k_0,k_0+1} + \sum_{i=1}^{n_1} \sum_{j=i+2}^{n_1} a_{i,j;0} E_{i,j}, \quad a(k_0, 0) \neq 0.$$

Также для всех $1 \leqslant i \leqslant n_1 + n_2 + n_3$ и $r = 1, \ldots, n_1$, $r \neq k_0$, выполнено

$$\big(\mathcal{F}(B_r)\big)_{i,i} = (B_r)_{i,i} = 0, \quad \big(\mathcal{F}(A_0)\big)_{i,i} = (A_0)_{i,i}.$$

Для простоты дальнейшего изложения обозначим $\mathcal{F}(A_0)$ и $\mathcal{F}(B_r)$ снова через A_0 и B_r соответственно. Тогда система порождающих $\tilde{\mathcal{S}} = \mathcal{F}(\mathcal{S})$ и будет искомой. □

Лемма 5.31. *Пусть $n_1 \geqslant 3$, $n_2 \geqslant n_3 \geqslant 2$, и пусть $\mathcal{S}$ — система порождающих для $\mathcal{A}_{n_1,n_2,n_3}$, удовлетворяющая условиям леммы* 5.30. *Тогда выполнены следующие условия*:

1) *найдётся индекс* $c \in \{n_1+1, \ldots, n_1+n_2-1\}$, *такой что*

   а) *либо существуют такие матрицы* $C, B_{n_1+1}, \ldots, B_{n_1+n_2-1} \in \langle \mathcal{S} \setminus A_0 \rangle$, *что*

   $$B_r'' = E_{r,r+1} + \sum_{i=n_1+1}^{n_1+n_2} \sum_{j=i+2}^{n_1+n_2} c_{i,j;r} E_{i,j}, \quad r = n_1+1, \ldots, n_1+n_2-1,$$

   и если $\tilde{A}_0 = E - A_0 + C$, *то*

   $$\tilde{A}_0'' = \sum_{i=n_1+1}^{n_1+n_2} \sum_{j=i+2}^{n_1+n_2} \tilde{a}_{i,j} E_{i,j},$$

   б) *либо существуют такие матрицы* $C, B_r \in \langle \mathcal{S} \setminus A_0 \rangle$, $r = n_1+1, \ldots, n_1+n_2-1$, $r \neq c$, *что*

   $$B_r'' = E_{r,r+1} + c_r E_{c,c+1} + \sum_{i=n_1+1}^{n_1+n_2} \sum_{j=i+2}^{n_1+n_2} c_{i,j;r} E_{i,j},$$

   и если $\tilde{A}_0 = E - A_0 + C$, *то*

   $$\tilde{A}_0'' = \tilde{a}_c E_{c,c+1} + \sum_{i=n_1+1}^{n_1+n_2} \sum_{j=i+2}^{n_1+n_2} \tilde{a}_{i,j} E_{i,j}, \quad \tilde{a}_c \neq 0$$

   (*в этом случае положим* $B_c = \tilde{A}_0$);

2) *найдётся индекс* $d \in \{n_1+n_2+1, \ldots, n_1+n_2+n_3-1\}$, *такой что*

   а) *либо существуют такие матрицы* $D, B_{n_1+n_2+1}, \ldots, B_{n_1+n_2+n_3-1} \in$ $\in \langle \mathcal{S} \setminus A_0 \rangle$, *что*

   $$B_r''' = E_{r,r+1} + \sum_{i=n_1+n_2+1}^{n_1+n_2+n_3} \sum_{j=i+2}^{n_1+n_2+n_3} d_{i,j;r} E_{i,j},$$
   $$r = n_1+n_2+1, \ldots, n_1+n_2+n_3-1,$$

   и если $\hat{A}_0 = E - a^{-1} A_0 + D$, *то*

   $$\hat{A}_0''' = \sum_{i=n_1+n_2+1}^{n_1+n_2+n_3} \sum_{j=i+2}^{n_1+n_2+n_3} \hat{a}_{i,j} E_{i,j},$$

   б) *либо существуют такие матрицы* $D, B_r \in \langle \mathcal{S} \setminus A_0 \rangle$, $r = n_1+n_2+1, \ldots,$ $n_1+n_2+n_3-1$, $r \neq d$, *что*

   $$B_r''' = E_{r,r+1} + d_r E_{d,d+1} + \sum_{i=n_1+n_2+1}^{n_1+n_2+n_3} \sum_{j=i+2}^{n_1+n_2+n_3} d_{i,j;r} E_{i,j},$$

и если $\hat{A}_0 = E - a^{-1}A_0 + D$, *то*

$$\hat{A}_0''' = \hat{a}_d E_{d,d+1} + \sum_{i=n_1+n_2+1}^{n_1+n_2+n_3} \sum_{j=i+2}^{n_1+n_2+n_3} \hat{a}_{i,j} E_{i,j}, \quad \hat{a}_d \neq 0$$

(*в этом случае положим* $B_d = \hat{A}_0$).

Доказательство. По условию матричные единицы $E_{h,h+1}$ принадлежат $\mathcal{A}_{n_1,n_2,n_3}$, но для любых $S_1, S_2 \in \mathcal{S}$ и для любых $i = n_1+1, \ldots, n_1+n_2-1$, $j = n_1+n_2+1, \ldots, n_1+n_2+n_3-1$ справедливо

$$(S_1S_2)_{i,i+1} = (S_1S_2)_{j,j+1} = 0$$

при $S_1 \neq A_0$, $S_2 \neq A_0$, а также

$$\begin{aligned} (S_1A_0)_{i,i+1} &= (S_1)_{i,i+1}, \quad (S_1A_0)_{j,j+1} = a(S_1)_{j,j+1}, \\ (A_0S_2)_{i,i+1} &= (S_2)_{i,i+1}, \quad (A_0S_2)_{j,j+1} = a(S_2)_{j,j+1}, \\ (A_0^2)_{i,i+1} &= 2(A_0)_{i,i+1}, \quad (A_0^2)_{j,j+1} = 2a(A_0)_{j,j+1}. \end{aligned}$$

Следовательно, найдутся матрицы $\tilde{B}_{n_1+1}, \ldots, \tilde{B}_{n_1+n_2-1} \in \mathcal{S}$, такие что векторы

$$w_i = \big((\tilde{B}_i)_{n_1+1,n_1+2}, (\tilde{B}_i)_{n_1+2,n_1+3}, \ldots, (\tilde{B}_i)_{n_1+n_2-1,n_1+n_2}\big), \qquad i = n_1+1, \ldots, n_1+n_2-1,$$

линейно независимы, и найдутся матрицы $\tilde{B}_{n_1+n_2+1}, \ldots, \tilde{B}_{n_1+n_2+n_3-1} \in \mathcal{S}$, такие что векторы

$$w_i = \big((\tilde{B}_i)_{n_1+n_2+1,n_1+n_2+2}, (\tilde{B}_i)_{n_1+n_2+2,n_1+n_2+3}, \ldots, (\tilde{B}_i)_{n_1+n_2+n_3-1,n_1+n_2+n_3}\big), \qquad i = n_1+n_2+1, \ldots, n_1+n_2+n_3-1,$$

линейно независимы.

Пусть $N = 1, 2$. Обозначим $M = n_1 + (N-1)n_2 + 1$.

Условие Na). Предположим, что $A_0 \notin \{\tilde{B}_M, \ldots, \tilde{B}_{M+n_{N+1}-2}\}$. Невырожденным линейным преобразованием $F_N = \{f_{i,j;N}\} \in \mathrm{M}_{n_{N+1}-1}(\mathbb{F})$ можно перевести набор векторов $\{w_i \mid i = M, \ldots, M+n_{N+1}-2\}$ в набор

$$\{e_1 = (1,0,\ldots,0),\, e_2 = (0,1,\ldots,0), \ldots,\, e_{n_{N+1}-1} = (0,0,\ldots,1)\} \subset \mathbb{F}^{n_{N+1}-1},$$

т. е.

$$e_h = \sum_{j=1}^{n_{N+1}-1} f_{h,j;N} w_{j+M-1}.$$

Положим

$$B_{h+M-1} = \sum_{j=1}^{n_{N+1}-1} f_{h,j;M} \tilde{B}_{j+M-1}, \quad h = 1, \ldots, n_{N+1}-1.$$

Тогда

$$B_{h+M-1} \in \langle \tilde{B}_M, \ldots, \tilde{B}_{M+n_{N+1}-2} \rangle \subset \langle \mathcal{S} \setminus A_0 \rangle, \quad h = 1, \ldots, n_{N+1}-1.$$

Если $N = 1$, то

$$B_r'' = E_{r,r+1} + \sum_{i=n_1+1}^{n_1+n_2} \sum_{j=i+2}^{n_1+n_2} c_{i,j;r} E_{i,j}, \quad r = n_1+1, \ldots, n_1+n_2-1.$$

Положим

$$C = \sum_{i=n_1+1}^{n_1+n_2-1} (A_0)_{i,i+1} B_i,$$

т. е. $(C)_{h,h+1} = (A_0)_{h,h+1}$ для любого $h = n_1+1, \ldots, n_1+n_2-1$, и

$$\tilde{A}_0'' = E - A_0'' + C'' = \sum_{i=1}^{n_2} \sum_{j=i+2}^{n_2} \tilde{a}_{i+n_1,j+n_1} E_{i+n_1,j+n_1}.$$

Если $N = 2$, то

$$B_r''' = E_{r,r+1} + \sum_{i=1}^{n_1+n_2+n_3} \sum_{j=i+2}^{n_1+n_2+n_3} d_{i,j;r} E_{i,j},$$
$$r = n_1+n_2+1, \ldots, n_1+n_2+n_3-1.$$

Положим

$$D = a^{-1} \sum_{i=n_1+n_2+1}^{n_1+n_2+n_3-1} (A_0)_{i,i+1} B_i,$$

т. е. $a(D)_{h,h+1} = (A_0)_{h,h+1}$ для любого $h = n_1+n_2+1, \ldots, n_1+n_2+n_3-1$, и

$$\hat{A}_0''' = E - a^{-1}A_0''' + D''' = \sum_{i=1}^{n_3} \sum_{j=i+2}^{n_3} \hat{a}_{i+n_1+n_2,j+n_1+n_2} E_{i+n_1+n_2,j+n_1+n_2}.$$

Условие Nб). Пусть $\tilde{B}_p = A_0$ для некоторого $p \in \{M, \ldots, M+n_{N+1}-2\}$.

При $n_2 = 2$ положим $\tilde{A}_0 = E - A_0$ и $B_{n_1+1} = \tilde{A}_0$.

При $n_3 = 2$ положим $\hat{A}_0 = E - a^{-1}A_0$ и $B_{n_1+n_2+1} = \hat{A}_0$.

Пусть $n_2 \geqslant n_3 \geqslant 3$. У любой матрицы в $\mathrm{M}_{n_{N+1}-1,n_{N+1}-2}(\mathbb{F})$ ранга $n_{N+1}-2$ существует невырожденная подматрица порядка $n_{N+1}-2$. Следовательно, найдётся индекс $q \in \{M, \ldots, M+n_{N+1}-2\}$, такой что векторы

$$x_i = \big((\tilde{B}_i)_{M,M+1}, \ldots, (\tilde{B}_i)_{q-1,q}, (\tilde{B}_i)_{q+1,q+2}, \ldots, (\tilde{B}_i)_{M+n_{N+1}-2,M+n_{N+1}-1}\big),$$
$$i = M, \ldots, M+n_{N+1}-2, \quad i \neq p,$$

линейно независимы. Поскольку порядок матриц $\tilde{B}_j$ произволен, можно считать, что $p = q$. Невырожденным линейным преобразованием $G_N = \{g_{i,j;N}\} \in \mathrm{M}_{n_{N+1}-2}(\mathbb{F})$ можно перевести набор $\{x_i \mid i = M, \ldots, M+n_{N+1}-2,\ i \neq q\}$ в набор

$$\{e_1 = (1,0,\ldots,0),\, e_2 = (0,1,\ldots,0), \ldots,\, e_{n_{N+1}-2} = (0,0,\ldots,1)\} \subset \mathbb{F}^{n_{N+1}-2},$$

т. е.

$$e_h = \sum_{j=1}^{q-M} g_{h,j;N} x_{j+M-1} + \sum_{j=q-M+1}^{n_{N+1}-1} g_{h,j;N} x_{j+M}, \quad h = 1, \ldots, n_{N+1} - 2.$$

Положим

$$B_{h+M-1} = \sum_{j=1}^{q-M} g_{h,j;N} \tilde{B}_{j+M-1} + \sum_{j=q-M+1}^{n_{N+1}-2} g_{h,j;N} \tilde{B}_{j+M}, \quad h < q - M + 1,$$

$$B_{h+M-1} = \sum_{j=1}^{q-M} g_{h-1,j;N} \tilde{B}_{j+M-1} + \sum_{j=q-M+1}^{n_{N+1}-2} g_{h-1,j;N} \tilde{B}_{j+M}, \quad h > q - M + 1.$$

Тогда

$$B_r \in \langle \tilde{B}_M, \ldots, \tilde{B}_{q-1}, \tilde{B}_{q+1}, \ldots, \tilde{B}_{M+n_{N+1}-2} \rangle \subset \langle \mathcal{S} \setminus A_0 \rangle,$$
$$r = M, \ldots, M + n_{N+1} - 2, \quad r \neq q.$$

При $N = 1$ положим $c = q$. Получаем

$$B_r'' = E_{r,r+1} + c_r E_{c,c+1} + \sum_{i=n_1+1}^{n_1+n_2} \sum_{j=i+2}^{n_1+n_2} c_{i,j;r} E_{i,j}, \quad r = n_1+1, \ldots, n_1+n_2-1, \ \ r \neq c.$$

Также пусть

$$C = \sum_{\substack{i=n_1+1,\\ i \neq c}}^{n_1+n_2-1} (A_0)_{i,i+1} B_i,$$

т. е. $(C)_{i,i+1} = (A_0)_{i,i+1}$ для любого $i = n_1 + 1, \ldots, n_1 + n_2 - 1$, $i \neq c$, и $B_c = \tilde{A}_0 = E - A_0 + C$. Тогда

$$\tilde{A}_0'' = E'' - A_0'' + C'' = \tilde{a}_c E_{c,c+1} + \sum_{i=n_1+1}^{n_1+n_2} \sum_{j=i+2}^{n_1+n_2} \tilde{a}_{i,j} E_{i,j},$$

где $\tilde{a}_c \neq 0$.

При $N = 2$ положим $d = q$. Получаем

$$B_r''' = E_{r,r+1} + d_r E_{d,d+1} + \sum_{i=n_1+n_2+1}^{n_1+n_2+n_3} \sum_{j=i+2}^{n_1+n_2+n_3} d_{i,j;r} E_{i,j},$$
$$r = n_1 + n_2 + 1, \ldots, n_1 + n_2 + n_3 - 1, \quad r \neq d.$$

Также пусть

$$D = a^{-1} \sum_{\substack{i=n_1+n_2+1,\\ i \neq d}}^{n_1+n_2+n_3-1} (A_0)_{i,i+1} B_i,$$

т. е. $a(D)_{i,i+1} = (A_0)_{i,i+1}$ для любого $i = n_1+n_2+1,\ldots,n_1+n_2+n_3-1$, $i \neq d$, и $B_d = \hat{A}_0 = E - a^{-1}A_0 + D$. Тогда

$$\hat{A}_0''' = E''' - a^{-1}A_0''' + D''' = \hat{a}_d E_{d,d+1} + \sum_{i=n_1+n_2+1}^{n_1+n_2+n_3} \sum_{j=i+2}^{n_1+n_2+n_3} \hat{a}_{i,j} E_{i,j},$$

где $\hat{a}_d \neq 0$. $\square$

Дальнейшее вычисление длин $\mathcal{A}_{n_1,n_2,n_3}$ проводится отдельно для различных значений параметров n_1, n_2 и n_3.

Лемма 5.32. *Пусть $n_1, n_2, n_3 \in \mathbb{N}$, $n_1 \geqslant 3$, $n_1 \geqslant n_2+2$, $n_2 \geqslant n_3$. Пусть $\mathbb{F}$ — произвольное поле. Пусть $\mathcal{S}$ — система порождающих для алгебры $\mathcal{A}_{n_1,n_2,n_3}$, удовлетворяющая условиям леммы* 5.29. *Тогда $l(\mathcal{S}) \leqslant n_1 - 1$.*

Доказательство. 1. Индукцией по $p = n_1 - (j-i)$ докажем, что $E_{i,j} \in \in \mathcal{L}_{n_1-1}(\mathcal{S})$ при $1 \leqslant i < j \leqslant n_1$, $j - i \geqslant 2$.

База индукции. Заметим, что

$$B_1B_2\cdots B_{n_1-1} = a(k_1,1)^{t_1}a(k_2,2)^{t_2}E_{1,n_1} \in \mathcal{L}_{n_1-1}(\mathcal{S}), \quad t_1,t_2 \in \{0,1\},$$

поскольку $(B_1B_2\cdots B_{n_1-1})'' = 0$ и $(B_1B_2\cdots B_{n_1-1})''' = 0$ как произведения n_1-1 нильпотентной матрицы порядка $n_{s+1} \leqslant n_1-2$, если не существует k_s, и как произведение n_1-2 нильпотентной и одной унитреугольной матрицы порядка $n_{s+1} \leqslant n_1-2$, если k_s существует, $s=1,2$.

Шаг индукции. Предположим, что утверждение верно для всех q, $1 < q < p$. Рассмотрим

$$B_{j,j+n_1-p-1} = B_jB_{j+1}\cdots B_{j+n_1-p-1}(E-A_1-A_2)^{p-1} \in \mathcal{L}_{n_1-1}(\mathcal{S}), \quad j=1,\ldots,p.$$

Получаем, что

$$B'_{j,j+n_1-p-1} = a(k_1,1)^{t_{1,j}}a(k_2,2)^{t_{2,j}}E_{j,j+n_1-p} + \sum_{h=1}^{n_1}\sum_{i=h+n_1-p+1}^{n_1} c_{h,i;j}E_{h,i}, \qquad t_{1,j}, t_{2,j} \in \{0,1\},$$

$B''_{j,j+n_1-p-1} = 0$ и $B'''_{j,j+n_1-p-1} = 0$ как произведения n_1-1 нильпотентной матрицы порядка $n_{s+1} \leqslant n_1-2$, если $k_s \notin \{j,\ldots,j+n_1-p-1\}$ или k_s не существует, и как произведение n_1-2 нильпотентной и одной унитреугольной матрицы порядка $n_{s+1} \leqslant n_1-2$, если $k_s \in \{j,\ldots,j+n_1-p-1\}$, $s=1,2$. По предположению индукции $E_{i,i+n_1-q-1} \in \mathcal{L}_{n_1-1}(\mathcal{S})$ для любых $q=1,\ldots,p-1$, $i=1,\ldots,q$. Значит, $B_{j,j+n_1-p-1} - E_{j,j+n-p} \in \mathcal{L}_{n_1-1}(\mathcal{S})$. Тогда

$$\begin{aligned} E_{j,j+n_1-p-1} &= a(k_1,1)^{-t_{1,j}}a(k_2,2)^{-t_{2,j}} \times \\ &\times \bigl(B_{j,j+n_1-p-1} - (B_{j,j+n_1-p-1} - E_{j,j+n_1-p})\bigr) \in \mathcal{L}_{n_1-1}(\mathcal{S}), \quad j=1,\ldots,p. \end{aligned}$$

2. Теперь рассмотрим матрицы $B_{j,j} = B_j(E-A_1-A_2)^{n_1-2} \in \mathcal{L}_{n_1-1}(\mathcal{S})$, $j=1,\ldots,n_1-1$. По построению

$$(B_{j,j})_{r,r+1} = (B_j)_{r,r+1}, \quad r=1,\ldots,n_1-1,$$

$B''_{j,j} = 0$ и $B'''_{j,j} = 0$ как произведение $n_1 - 1$ нильпотентной матрицы порядка $n_{s+1} \leqslant n_1 - 2$, если $k_s \neq j$ или k_s не существует, и как произведение $n_1 - 2$ нильпотентных и одной унитреугольной матрицы порядка $n_{s+1} \leqslant n_1 - 2$, если $k_s = j$, $s = 1, 2$. Следовательно, $B_{j,j} = B'_{j,j} \oplus 0 \oplus 0$, $j = 1, \ldots, n_1 - 1$.

По лемме 5.29 из равенств $(B_{j,j})_{r,r+1} = (B_j)_{r,r+1}$ следует, что

$$(E_{r,r+1} + N_r) \oplus 0 \oplus 0 \in \langle B'_{j,j} \oplus 0 \oplus 0 \mid j = 1, \ldots, n_1 - 1\rangle = \\ = \langle B_{j,j} \mid j = 1, \ldots, n_1 - 1\rangle \subseteq \mathcal{L}_{n_1-1}(\mathcal{S}), \quad N_r \in \mathrm{N}^2_{n_1}(\mathbb{F}), \quad r = 1, \ldots, n_1 - 1.$$

Учитывая пункт 1, получаем, что

$$E_{r,r+1} = (E_{r,r+1} + N_r) \oplus 0 \oplus 0 - N_r \oplus 0 \oplus 0 \in \mathcal{L}_{n_1-1}(\mathcal{S}), \quad r = 1, \ldots, n_1 - 1.$$

Следовательно, $E_{i,j} \in \mathcal{L}_{n_1-1}(\mathcal{S})$, $1 \leqslant i < j \leqslant n_1$.

3. Из пунктов 1 и 2 получаем, что

$$(E - A_1 - A_2)^{n_2} = \sum_{i=1}^{n_1} E_{i,i} + \sum_{1 \leqslant h < i \leqslant n_1} \lambda_{h,i} E_{h,i} \in \mathcal{L}_{n_2}(\mathcal{S})$$

и

$$\sum_{i=1}^{n_1} E_{i,i} \in \mathcal{L}_{n_1-1}(\mathcal{S}).$$

4. Пусть $S_1, \ldots, S_{n_1} \in \mathcal{S}$. Множество $\mathcal{S}_{2,3} = \{S'' \oplus S''', \ S \in \mathcal{S}\}$ является системой порождающих для $\mathcal{A}_{n_2,n_3}$. По теореме 5.24 $\mathcal{A}_{n_2,n_3} = \mathcal{L}_{n_2+1}(\mathcal{S}_{2,3})$. Следовательно, найдётся такой элемент $S_0 \in \mathcal{L}_{n_2+1}(\mathcal{S}_{2,3})$, что $(S_1 \cdots S_{n_1})'' \oplus \oplus (S_1 \cdots S_{n_1})''' - S_0 = 0$. Возьмём $T_0 \in \mathcal{L}_{n_2+1}(\mathcal{S})$ — прообраз S_0. По условию теоремы $n_1 - 1 \geqslant n_2 + 1$. Тогда $S_1 \cdots S_{n_1} - T_0 = S' \oplus 0 \oplus 0 \in \mathcal{L}_{n_1-1}(\mathcal{S})$. Значит, любое слово длины n_1 от элементов $\mathcal{S}$ сократимо, $\mathcal{L}_{n_1}(\mathcal{S}) = \mathcal{L}_{n_1-1}(\mathcal{S})$ и $l(\mathcal{S}) \leqslant n_1 - 1$. □

Лемма 5.33. *Пусть $\mathbb{F}$ — произвольное поле, $|\mathbb{F}| \geqslant 3$ и $n_1, n_2, n_3 \in \mathbb{N}$, $n_1 \geqslant \geqslant n_2 + n_3 + 2$. Пусть $\mathcal{S}$ — система порождающих для $\mathcal{A}_{n_1,n_2,n_3}$, удовлетворяющая условиям леммы* 5.30. *Тогда $l(\mathcal{S}) \leqslant n_1 - 1$.*

Доказательство. 1. Индукцией по $p = n_1 - (j - i)$ докажем, что $E_{i,j} \in \in \mathcal{L}_{n_1-1}(\mathcal{S})$ при $1 \leqslant i < j \leqslant n_1$, $j - i \geqslant 2$. Обозначим $m = n_1 + n_2 + 1$.

База индукции. При $p = 1$ рассмотрим произведение $B_1 \cdots B_{n_1-1} \in \in \mathcal{L}_{n_1-1}(\mathcal{S})$. Имеем

$$(B_1 \cdots B_{n_1-1})' = bE_{1,n_1}, \quad b \neq 0,$$

при этом $(B_1 \cdots B_{n_1-1})'' = 0$ и $(B_1 \cdots B_{n_1-1})''' = 0$ как произведения $n_1 - 1$ нильпотентной матрицы порядков $n_2 \leqslant n_1 - 2$ и $n_3 \leqslant n_1 - 2$, если $\mathcal{S}$ удовлетворяет условию 1) леммы 5.30, или $n_1 - 2$ нильпотентных и одной унитреугольной в противном случае. Таким образом,

$$E_{1,n_1} = b^{-1}(B_1 \cdots B_{n_1-1}) \in \mathcal{L}_{n_1-1}(\mathcal{S}).$$

Шаг индукции. Предположим, что утверждение верно для всех q, $1 < q < p$.

При $p \leqslant n_1 - n_3 - 2$ и $j = 1, \ldots, p$ рассмотрим матрицы

$$B_{j,j+n_1-p-1} = B_j \cdots B_{j+n_1-p-1}(E - A_0)^{p-1} \in \mathcal{L}_{n_1-1}(\mathcal{S}).$$

Имеем

$$B'_{j,j+n_1-p-1} = a(k_0,0)^t E_{j,j+n_1-p} + \sum_{h=1}^{n_1} \sum_{i=h+n_1-p+1}^{n_1} c_{h,i;j} E_{h,i}, \quad t \in \{0,1\},$$

$B''_{j,j+n_1-p-1} = 0$ и $B''_{j,j+n_1-p-1} = 0$ как произведения нильпотентных матриц длины, не меньшей порядков матриц.

При $n_1 - n_3 - 1 \leqslant p < n_1 - 1$ и $j = 1, \ldots, p$ рассмотрим матрицы

$$B_{j,j+n_1-p-1} = B_j \cdots B_{j+n_1-p-1}(E - a^{-1}A_0)^{n_3-n_1+p}(E - A_0)^{n_1-n_3-1},$$

$B_{j,j+n_1-p-1} \in \mathcal{L}_{n_1-1}(\mathcal{S})$,

$$B'_{j,j+n_1-p-1} = a(k_0,0)^t E_{j,j+n_1-p} + \sum_{h=1}^{n_1} \sum_{i=h+n_1-p+1}^{n_1} c_{h,i;j} E_{h,i}, \quad t \in \{0,1\},$$

$B''_{j,j+n_1-p-1} = 0$ и $B''_{j,j+n_1-p-1} = 0$ как произведения нильпотентных матриц длины, не меньшей порядков матриц.

По предположению индукции $E_{i,i+n_1-q-1} \in \mathcal{L}_{n_1-1}(\mathcal{S})$ для любых $q = 2, \ldots, p-1$, $i = 1, \ldots, q$, и, как показано ранее, $E_{1,n_1} \in \mathcal{L}_{n_1-1}(\mathcal{S})$. Значит,

$$B_{j,j+n_1-p-1} - a(k_0,0)^t E_{j,j+n_1-p} \in \mathcal{L}_{n_1-1}(\mathcal{S}).$$

Получаем, что

$$E_{j,j+n_1-p-1} = \\ = \bigl(a(k_0,0)\bigr)^{-t}\Bigl(B_{j,j+n_1-p-1} - \bigl(B_{j,j+n_1-p-1} - \bigl(a(k_0,0)\bigr)^t E_{j,j+n_1-p}\bigr)\Bigr) \in \mathcal{L}_{n_1-1}(\mathcal{S})$$

при всех $j = 1, \ldots, p$.

2. При $j = 1, \ldots, n_1 - 1$ рассмотрим матрицы

$$B_{j,j} = B_j(E - a^{-1}A_0)^{n_3-1}(E - A_0)^{p-n_3}, \quad j \neq k_0,$$
$$B_{k_0,k_0} = B_{k_0}(E - a^{-1}A_0)^{n_3}(E - A_0)^{p-n_3-1},$$

$B_{j,j} \in \mathcal{L}_{n_1-1}(\mathcal{S})$. Имеем, что

$$B'_{j,j} = E_{j,j+1} + \gamma_j E_{k_0,k_0+1} + \sum_{h=1}^{n_1} \sum_{i=h+2}^{n_1} c_{h,i;j} E_{h,i}, \quad j \neq k_0,$$
$$B'_{k_0,k_0} = a(k_0,0) E_{k_0,k_0+1} + \sum_{h=1}^{n_1} \sum_{i=h+2}^{n_1} c_{h,i;k_0} E_{h,i},$$

$B''_{r,r} = 0$, $B'''_{r,r} = 0$ как произведения нильпотентных матриц длины, не меньшей порядков матриц. Учитывая пункт 1, получаем, что $E_{j,j+n_1-p} \in \mathcal{L}_{n_1-1}(\mathcal{S})$, $j = 1, \ldots, p$.

3. Имеем

$$(E - A_0)^{n_2}(E - a^{-1}A_0)^{n_3} = \sum_{i=1}^{n_1} E_{i,i} + \sum_{1 \leqslant h < i \leqslant n_1} \lambda_{h,i} E_{h,i} \in \mathcal{L}_{n_2+n_3}(\mathcal{S}),$$

$$\sum_{i=1}^{n_1} E_{i,i} \in \mathcal{L}_{n_1-1}(\mathcal{S}).$$

4. Пусть $S_1, \ldots, S_{n_1} \in \mathcal{S}$. Множество $\mathcal{S}_{2,3} = \{S'' \oplus S'',\ S \in \mathcal{S}\}$ является системой порождающих для $\mathcal{A}_{n_2,n_3}$. По теореме 5.24 $\mathcal{A}_{n_2,n_3} = \mathcal{L}_{n_2+1}(\mathcal{S}')$. Следовательно, найдётся элемент $S_0 \in \mathcal{L}_{n_2+1}(\mathcal{S}_{2,3})$, такой что $(S_1 \cdots S_{n_1})'' \oplus \oplus (S_1 \cdots S_{n_1})'' - S_0 = 0$. Возьмём $T_0 \in \mathcal{L}_{n_2+1}(\mathcal{S}) \subseteq \mathcal{L}_{n_1-1}(\mathcal{S})$ — прообраз S_0. Тогда $S_1 \cdots S_{n_1} - T_0 = S'' \oplus 0 \oplus 0 \in \mathcal{L}_{n_1-1}(\mathcal{S})$. Значит, любое слово длины n_1 от элементов $\mathcal{S}$ сократимо, $\mathcal{L}_{n_1}(\mathcal{S}) = \mathcal{L}_{n_1-1}(\mathcal{S})$ и $l(\mathcal{S}) \leqslant n_1 - 1$. □

Теорема 5.34. *Пусть $\mathbb{F} = \mathbb{F}_2$. Пусть $n_1, n_2, n_3 \in \mathbb{N}$, $n_1 \geqslant 3$, $n_1 \geqslant n_2 + 2$, $n_2 \geqslant n_3$. Тогда $l(\mathcal{A}_{n_1,n_2,n_3}) = n_1 - 1$.*

Доказательство. Сначала докажем верхнюю оценку $l(\mathcal{A}_{n_1,n_2,n_3}) \leqslant n_1 - 1$. Для этого рассмотрим произвольную систему порождающих $\mathcal{S}$ для алгебры $\mathcal{A}_{n_1,n_2,n_3}$. Из данного условия на поле следует, что без ограничения общности можно считать, что $\mathcal{S}$ удовлетворяет условиям леммы 5.29 и, соответственно, условиям леммы 5.32, откуда получаем, что $l(\mathcal{S}) \leqslant n_1 - 1$. Тогда

$$l(\mathcal{A}_{n_1,n_2,n_3}) = \max_{\mathcal{S}} l(\mathcal{S}) \leqslant \max_{\mathcal{S}} (n_1 - 1) = n_1 - 1.$$

Нижняя оценка следует из теорем 3.9 и 5.24:

$$l(\mathcal{A}_{n_1,n_2,n_3}) \geqslant \max\bigl\{l(\mathcal{A}_{n_1,n_2}), l\bigl(\mathrm{N}_{n_3}(\mathbb{F}_2)\bigr)\bigr\} \geqslant l(\mathcal{A}_{n_1,n_2}) \geqslant n_1 - 1.$$ □

Теорема 5.35. *Пусть $\mathbb{F}$ — произвольное поле. Пусть $n_1, n_2, n_3 \in \mathbb{N}$, $n_1 \geqslant \geqslant n_2 + n_3 + 2$. Тогда $l(\mathcal{A}_{n_1,n_2,n_3}) = n_1 - 1$.*

Доказательство. Сначала докажем верхнюю оценку $l(\mathcal{A}_{n_1,n_2,n_3}) \leqslant n_1 - 1$. Для этого рассмотрим произвольную систему порождающих $\mathcal{S}$ для алгебры $\mathcal{A}_{n_1,n_2,n_3}$. Без ограничения общности можно считать, что $\mathcal{S}$ удовлетворяет условиям леммы 5.28. Тогда из лемм 5.32 и 5.33 получаем, что $l(\mathcal{S}) \leqslant n_1 - 1$. Следовательно,

$$l(\mathcal{A}_{n_1,n_2,n_3}) = \max_{\mathcal{S}} l(\mathcal{S}) \leqslant \max_{\mathcal{S}} (n_1 - 1) = n_1 - 1.$$

Нижняя оценка следует из теорем 3.9 и 5.24:

$$l(\mathcal{A}_{n_1,n_2,n_3}) \geqslant \max\bigl\{l(\mathcal{A}_{n_1,n_2}), l\bigl(\mathrm{N}_{n_3}(\mathbb{F}_2)\bigr)\bigr\} \geqslant l(\mathcal{A}_{n_1,n_2}) \geqslant n_1 - 1.$$ □

Следствие 5.36. *Пусть $\mathbb{F} \neq \mathbb{F}_2$ — произвольное поле, и пусть $n_1, n_2, n_3 \in \mathbb{N}$, $n_1 \geqslant n_2 + n_3 + 2$, $n_2 \geqslant n_3 \geqslant 3$. Пусть $a \in \mathbb{F}$, $a \neq 0, 1$, и*

$$C_{n_1,n_2,n_3} = \sum_{i=1}^{n_1-1} E_{i,i+1} + \sum_{j=n_1+1}^{n_1+n_2-1} (E_{j,j} + E_{j,j+1}) + E_{n_1+n_2,n_1+n_2} +$$
$$+ \sum_{k=n_1+n_2+1}^{n_1+n_2+n_3-1} (aE_{k,k} + E_{k,k+1}) + aE_{n_1+n_2+n_3,n_1+n_2+n_3} \in \mathcal{A}_{n_1,n_2,n_3} -$$

циклическая матрица. Положим

$$\mathcal{A}'_{n_1,n_2,n_3} = \langle C^j_{n_1,n_2,n_3} \mid 0 \leqslant j \leqslant n_1 + n_2 + n_3 - 1 \rangle \subseteq \mathcal{A}_{n_1,n_2,n_3}.$$

Тогда

1) $l(\mathcal{A}'_{n_1,n_2,n_3}) = n_1 + n_2 + n_3 - 1$;
2) $l(\mathcal{A}'_{n_1,n_2,n_3}) - l(\mathcal{A}_{n_1,n_2,n_3}) = n_2 + n_3$;
3) $l(\mathcal{A}'_{n_1,n_2,n_3})/l(\mathcal{A}_{n_1,n_2,n_3}) = 1+(n_2+n_3)/(n_1-1) \leqslant 1+(n_1-2)/(n_1-1) < 2$.

Следствие 5.37. *Отношение длины подалгебры трёхблочной алгебры к длине алгебры принимает все рациональные значения из интервала* $(1, 2)$.

Доказательство. Согласно следствию 5.37 достаточно показать, что при условиях $n_1, n_2, n_3 \in \mathbb{N}$, $n_1 \geqslant n_2+n_3+2$, $n_2 \geqslant n_3 \geqslant 3$ отношение $(n_2+n_3)/(n_1-1)$ принимает все рациональные значения из интервала $(0, 1)$. Для этого подберём значение параметров n_1, n_2, n_3 так, что

$$\frac{n_2 + n_3}{n_1 - 1} = \frac{p}{q},$$

где $p < q \in \mathbb{N}$ — взаимно простые числа.

Положим $n_3 = 3$. Поскольку $q - p \in \mathbb{N}$, то существует число $k \in \mathbb{N}$, такое что $k \cdot \min\{(q - p), p\} \geqslant 6$. Положим $n_1 = kq + 1$ и $n_2 = kp - 3$.

По условию $kq-kp \geqslant 6$ и $kp \geqslant 6$, т. е. $n_2 = kp-3 \geqslant 3 = n_3$ и $n_1-(n_2+n_3) = kq+1-(kp-3+3) = k(q-p)+1 \geqslant 7 > 2$. Значит, условия на параметры n_1, n_2, n_3 выполнены. Также получаем, что

$$\frac{n_2 + n_3}{n_1 - 1} = \frac{n_2 + 3}{n_1 - 1} = \frac{kp}{kq} = \frac{p}{q}. \qquad \square$$

Лемма 5.38. *Пусть* $\mathbb{F}$ *— произвольное поле,* $n \in \mathbb{N}$ *и* $n > 2$*. Пусть* $\mathcal{S}$ *— система порождающих для алгебры* $\mathcal{A}_{n,n,n}$*, удовлетворяющая условиям леммы* 5.29*. Тогда* $l(\mathcal{S}) \leqslant n + 1$.

Доказательство. 1. Индукцией по $p = n-(j-i)$ докажем, что $E_{i,j} \in \mathcal{L}_{n+1}(\mathcal{S})$ при $1 \leqslant i < j \leqslant n$, $j - i \geqslant 2$.

База индукции. Рассмотрим произведение $B_1B_2\cdots B_{n-1}(E - A_1 - A_2)^2 \in \mathcal{L}_{n+1}(\mathcal{S})$. Заметим, что

$$(B_1B_2\cdots B_{n-1}(E - A_1 - A_2)^2)' = a(k_1, 1)^{t_1}a(k_2, 2)^{t_2}E_{1,n}, \quad t_1, t_2 \in \{0, 1\},$$

при этом

$$(B_1B_2\cdots B_{n-1}(E - A_1 - A_2)^2)'' = 0$$

и

$$(B_1 B_2 \cdots B_{n-1}(E - A_1 - A_2)^2)''' = 0$$

как произведения $n{+}1$ нильпотентной матрицы порядка n, если $\mathcal{S}$ удовлетворяет условию 1) леммы 5.29, или одной унитреугольной и n нильпотентных матриц порядка n иначе. Следовательно, получаем, что

$$E_{1,n} = a(k_1, 1)^{-t_1} a(k_2, 2)^{-t_2} (B_1 B_2 \cdots B_{n-1}(E - A_1 - A_2)^2) \in \mathcal{L}_{n+1}(\mathcal{S}).$$

Шаг индукции. Рассмотрим матрицы

$$B_{j,j+n-p-1} = B_j B_{j+1} \cdots B_{j+n-p-1}(E - A_1 - A_2)^{p+1} \in \mathcal{L}_{n+1}(\mathcal{S}), \quad j = 1, \ldots, p.$$

Имеем

$$B'_{j,j+n-p-1} = a(k_1, 1)^{t_1} a(k_2, 2)^{t_2} E_{j,j+n-p} + \sum_{h=1}^{n} \sum_{i=h+n-p+1}^{n} c_{h,i;j} E_{h,i}, \qquad t_1, t_2 \in \{0, 1\},$$

$B''_{j,j+n-p-1} = 0$ и $B'''_{j,j+n-p-1} = 0$ как произведения $n{+}1$ нильпотентной матрицы порядка n, если $t_r = 0$, или одной унитреугольной и n нильпотентных матриц порядка n иначе.

По предположению индукции $E_{i,i+n-q-1} \in \mathcal{L}_{n+1}(\mathcal{S})$ для любых $q = 1, \ldots, p-1$, $i = 1, \ldots, q$. Значит,

$$B_{j,j+n-p-1} - E_{j,j+n-p} \in \mathcal{L}_{n+1}(\mathcal{S}).$$

Отсюда получаем, что

$$E_{j,j+n-p-1} = \bigl(B_{j,j+n-p-1} - (B_{j,j+n-p-1} - E_{j,j+n-p})\bigr) \in \mathcal{L}_{n+1}(\mathcal{S}), \quad j = 1, \ldots, p.$$

2. Теперь рассмотрим матрицы

$$B_{j,j} = B_j (E - A_1 - A_2)^n \in \mathcal{L}_{n+1}(\mathcal{S}), \quad j = 1, \ldots, n-1.$$

Имеем

$$B'_{j,j} = E_{j,j+1} + \gamma_{j,1} E_{k_1,k_1+1} + \gamma_{j,2} E_{k_2,k_2+1} + \sum_{h=1}^{n} \sum_{i=h+2}^{n} c_{h,i;j} E_{h,i}, \quad j \neq k_1, k_2,$$

$$B'_{k_r,k_r} = a_{k_1,r} E_{k_1,k_1+1} + a_{k_2,r} E_{k_2,k_2+1} + \sum_{h=1}^{n} \sum_{i=h+2}^{n} c_{h,i;r} E_{h,i}, \quad r = 1, 2,$$

$B''_{j,j} = 0$ и $B'''_{j,j} = 0$ как произведения n нильпотентных и одной унитреугольной или $n+1$ нильпотентной матрицы порядка n. Учитывая пункт 1, получаем, что

$$E_{j,j+1} + \gamma_{j,1} E_{k_1,k_1+1} + \gamma_{j,2} E_{k_2,k_2+1},\ a_{k_1,r} E_{k_1,k_1+1} + a_{k_2,r} E_{k_2,k_2+1} \in \mathcal{L}_{n+1}(\mathcal{S}), \qquad j \neq k_1, k_2, \quad r = 1, 2.$$

а значит, $E_{j,j+1} \in \mathcal{L}_{n+1}(\mathcal{S})$, $j = 1, \ldots, n-1$. Следовательно, $E_{i,j} \in \mathcal{L}_{n+1}(\mathcal{S})$, $1 \leqslant i < j \leqslant n$.

3. Из пунктов 1 и 2 получаем, что

$$(E - A_1 - A_2)^n = \sum_{i=1}^{n} E_{i,i} + \sum_{1 \leqslant h < i \leqslant n} \lambda_{h,i} E_{h,i} \in \mathcal{L}_n(\mathcal{S}),$$

следовательно,

$$\sum_{i=1}^{n} E_{i,i} \in \mathcal{L}_{n+1}(\mathcal{S}).$$

4. Пусть $S_1, \ldots, S_{n+2} \in \mathcal{S}$. Множество $\mathcal{S}_{2,3} = \{S'' \oplus S'',\ S \in \mathcal{S}\}$ является системой порождающих для $\mathcal{A}_{n,n}$. По теореме 5.24 $\mathcal{A}_{n,n} = \mathcal{L}_{n+1}(\mathcal{S}_{2,3})$. Следовательно, найдётся элемент $S_0 \in \mathcal{L}_{n+1}(\mathcal{S}_{2,3})$, такой что

$$(S_1 \cdots S_{n+2})'' \oplus (S_1 \cdots S_{n+2})''' - S_0 = 0.$$

Возьмём $T_0 \in \mathcal{L}_{n+1}(\mathcal{S})$ — прообраз S_0. Тогда

$$S_1 \cdots S_{n+2} - T_0 = S' \oplus 0 \oplus 0 \in \mathcal{L}_{n+1}(\mathcal{S}).$$

Значит, любое слово длины $n+2$ от элементов $\mathcal{S}$ сократимо, $\mathcal{L}_{n+2}(\mathcal{S}) = \mathcal{L}_{n+1}(\mathcal{S})$ и $l(\mathcal{S}) \leqslant n + 1$. □

Лемма 5.39. *Пусть $\mathbb{F}$ — произвольное поле, $|\mathbb{F}| \geqslant 3$, $n \in \mathbb{N}$ и $n \geqslant 5$. Пусть $\mathcal{S}$ — система порождающих для алгебры $\mathcal{A}_{n,n,n}$, удовлетворяющая условиям леммы* 5.31. *Тогда $l(\mathcal{S}) \leqslant n + 1$.*

Доказательство. 1. Индукцией по $p = n-(j-i)$ докажем, что $E_{i,j}, E_{i+n,j+n}, E_{i+2n,j+2n} \in \mathcal{L}_{n+1}(\mathcal{S})$ при $1 \leqslant i < j \leqslant n$.

База индукции. а) Пусть $p = 1$. Рассмотрим произведение $B_1 B_2 \cdots B_{n-1} \in \mathcal{L}_{n-1}(\mathcal{S})$. Имеем

$$(B_1 B_2 \cdots B_{n-1})' = a(k_0, 0)^{t_0} E_{1,n}, \quad t_0 \in \{0, 1\},$$
$$(B_1 B_2 \cdots B_{n-1})'' = \beta_{2,1} E_{n+1,2n-1} + \beta_{2,2} E_{n+1,2n} + \beta_{2,3} E_{n+2,2n},$$
$$(B_1 B_2 \cdots B_{n-1})''' = \beta_{3,1} E_{2n+1,3n-1} + \beta_{3,2} E_{2n+1,3n} + \beta_{3,3} E_{2n+2,3n}.$$

Отметим, что поскольку $n > 2$, то для введённого в лемме 5.31 индекса $c \in \{n+1, \ldots, 2n-1\}$ справедливо хотя бы одно из неравенств $c \neq n+1$ и $c \neq 2n-1$.

При $c \neq n+1$ верно $(\tilde{A}_0)_{n+1,n+2} = 0$,

$$(\tilde{A}_0 B_1 B_2 \cdots B_{n-1})'' = 0, \quad (\tilde{A}_0 B_1 B_2 \cdots B_{n-1})' = (B_1 B_2 \cdots B_{n-1})',$$
$$(\tilde{A}_0 B_1 B_2 \cdots B_{n-1})''' = \tilde{\beta}_{3,1} E_{2n+1,3n-1} + \tilde{\beta}_{3,2} E_{2n+1,3n} + \tilde{\beta}_{3,3} E_{2n+2,3n},$$

в этом случае обозначим $\tilde{B} = \tilde{A}_0 B_1 B_2 \cdots B_{n-1}$.

При $c \neq 2n-1$ верно $(\tilde{A}_0)_{2n-1,2n} = 0$,

$$(B_1 B_2 \cdots B_{n-1} \tilde{A}_0)'' = 0, \quad (B_1 B_2 \cdots B_{n-1} \tilde{A}_0)' = (B_1 B_2 \cdots B_{n-1})',$$
$$(B_1 B_2 \cdots B_{n-1} \tilde{A}_0)''' = \tilde{\beta}_{3,1} E_{2n+1,3n-1} + \tilde{\beta}_{3,2} E_{2n+1,3n} + \tilde{\beta}_{3,3} E_{2n+2,3n},$$

в этом случае обозначим $\tilde{B} = B_1 B_2 \cdots B_{n-1} \tilde{A}_0$.

Также заметим, что поскольку $n > 2$, то для введённого в лемме 5.31 индекса $d \in \{2n+1, \ldots, 3n-1\}$ справедливо хотя бы одно из неравенств $d \neq 2n+1$ и $d \neq 3n-1$.

При $d \neq 2n+1$ верно $(\hat{A}_0)_{2n+1,2n+2} = 0$,

$$(\hat{A}_0\tilde{B})''' = 0, \quad (\hat{A}_0\tilde{B})'' = 0, \quad (\hat{A}_0\tilde{B})' = (B_1B_2\cdots B_{n-1})',$$

а при $d \neq 3n-1$ верно $(\hat{A}_0)_{3n-1,3n} = 0$,

$$(\tilde{B}\hat{A}_0)''' = 0, \quad (\tilde{B}\hat{A}_0)'' = 0, \quad (\tilde{B}\hat{A}_0)' = (B_1B_2\cdots B_{n-1})'.$$

Таким образом, $E_{1,n} \in \mathcal{L}_{n+1}(\mathcal{S})$.

Имеем

$$(B_{n+1}\cdots B_{2n-1}A_0)' = bE_{1,n},$$
$$(B_{n+1}\cdots B_{2n-1}A_0)'' = \tilde{a}_c^t E_{n+1,2n}, \quad t \in \{0,1\},$$
$$(B_{n+1}\cdots B_{2n-1}A_0)''' = \beta_{3,1}E_{2n+1,3n-1} + \beta_{3,2}E_{2n+1,3n} + \beta_{3,3}E_{2n+2,3n}.$$

Тогда

$$(B_{n+1}\cdots B_{2n-1}A_0\hat{A}_0)' = (\hat{A}_0B_{n+1}\cdots B_{2n-1}A_0)' = bE_{1,n},$$
$$(B_{n+1}\cdots B_{2n-1}A_0\hat{A}_0)'' = (\hat{A}_0B_{n+1}\cdots B_{2n-1}A_0)'' = (1-a^{-1})\tilde{a}_c^t E_{n+1,2n}, \quad t \in \{0,1\}.$$

При $d \neq 2n+1$ верно

$$(\hat{A}_0B_{n+1}\cdots B_{2n-1}A_0)''' = 0,$$

а при $d \neq 3n-1$ верно

$$(B_{n+1}\cdots B_{2n-1}A_0\hat{A}_0)''' = 0.$$

Значит, либо

$$(1-a^{-1})^{-1}\tilde{a}_c^{-t}(B_{n+1}\cdots B_{2n-1}A_0\hat{A}_0 - bE_{1,n}) = E_{n+1,2n},$$

либо

$$(1-a^{-1})^{-1}\tilde{a}_c^{-t}(\hat{A}_0B_{n+1}\cdots B_{2n-1}A_0 - bE_{1,n}) = E_{n+1,2n},$$

т. е. $E_{n+1,2n} \in \mathcal{L}_{n+1}(\mathcal{S})$.

Имеем

$$(B_{2n+1}\cdots B_{3n-1}A_0\tilde{A}_0)' = b_1E_{1,n},$$
$$(B_{2n+1}\cdots B_{3n-1}A_0\tilde{A}_0)'' = b_2E_{n+1,2n},$$
$$(B_{2n+1}\cdots B_{3n-1}A_0\tilde{A}_0)''' = a(1-a)\hat{a}_d^t E_{2n+1,3n}, \quad t \in \{0,1\}.$$

Значит,

$$E_{2n+1,3n} = a^{-1}(1-a)^{-1}\hat{a}_d^{-t}(B_{2n+1}\cdots B_{3n-1}A_0\tilde{A}_0 - b_1E_{1,n} - b_2E_{n+1,2n}) \in \mathcal{L}_{n+1}(\mathcal{S}).$$

Таким образом, мы получили, что $E_{1,n}, E_{n+1,2n}, E_{2n+1,3n} \in \mathcal{L}_{n+1}(\mathcal{S})$.

б) Рассмотрим случай $p = 2$. Пусть $j \in \{1, 2\}$. Рассмотрим произведения $B_j B_{j+1} \cdots B_{j+n-3} \hat{A}_0^2 \in \mathcal{L}_n(\mathcal{S})$. Имеем

$$(B_j B_{j+1} \cdots B_{j+n-3} \hat{A}_0^2)' = a(k_0, 0)^{t_0} E_{j,j+n-2} + b E_{1,n}, \quad t_0 \in \{0, 1\},$$

$$(B_j B_{j+1} \cdots B_{j+n-3} \hat{A}_0^2)'' = \begin{pmatrix} 0 & 0 & \dots & \beta_{2,1} & \beta_{2,2} & \beta_{2,3} \\ 0 & 0 & \dots & 0 & \beta_{2,4} & \beta_{2,5} \\ 0 & 0 & \dots & 0 & 0 & \beta_{2,6} \\ 0 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 \end{pmatrix},$$

$$(B_j B_{j+1} \cdots B_{j+n-3} \hat{A}_0^2)''' = \beta_3 E_{2n+1,3n}.$$

Отметим, что поскольку $n > 4$, то для введённого в лемме 5.31 индекса $c \in \{n+1, \dots, 2n-1\}$ справедливо хотя бы одно из неравенств $c > n+2$ и $c < 2n-2$.

При $c > n+2$ имеем

$$\tilde{A}_0'' = \begin{pmatrix} 0 & 0 & * & * & \dots & * \\ 0 & 0 & 0 & * & \dots & * \\ 0 & 0 & 0 & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & * \\ 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix},$$

$$(\tilde{A}_0 B_j B_{j+1} \cdots B_{j+n-3} \hat{A}_0^2)' = a(k_0, 0)^{t_0} E_{j,j+n-2} + \beta_1 E_{1,n}, \quad t_0 \in \{0, 1\},$$

$$(\tilde{A}_0 B_j B_{j+1} \cdots B_{j+n-3} \hat{A}_0^2)'' = \beta_2 E_{n+1,2n},$$

$$(\tilde{A}_0 B_j B_{j+1} \cdots B_{j+n-3} \hat{A}_0^2)''' = \tilde{\beta}_3 E_{2n+1,3n}.$$

При $c < 2n-2$ имеем

$$\tilde{A}_0'' = \begin{pmatrix} 0 & * & \dots & * & * & * \\ 0 & 0 & \dots & * & * & * \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & 0 & * \\ 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 \end{pmatrix},$$

$$(B_j B_{j+1} \cdots B_{j+n-3} \hat{A}_0^2 \tilde{A}_0)' = a(k_0, 0)^{t_0} E_{j,j+n-2} + \beta_1 E_{1,n}, \quad t_0 \in \{0, 1\},$$

$$(B_j B_{j+1} \cdots B_{j+n-3} \hat{A}_0^2 \tilde{A}_0)'' = \beta_2 E_{n+1,2n},$$

$$(B_j B_{j+1} \cdots B_{j+n-3} \hat{A}_0^2 \tilde{A}_0)''' = \tilde{\beta}_3 E_{2n+1,3n}.$$

Значит, либо

$$a(k_0, 0)^{-t_0} (\tilde{A}_0 B_j B_{j+1} \cdots B_{j+n-3} \hat{A}_0^2 - \beta_1 E_{1,n} - \beta_2 E_{n+1,2n} - \tilde{\beta}_3 E_{2n+1,3n}) = E_{j,j+n-2},$$

либо

$$a(k_0,0)^{-t_0}(B_jB_{j+1}\cdots B_{j+n-3}\hat{A}_0^2\tilde{A}_0-\beta_1E_{1,n}-\beta_2E_{n+1,2n}-\tilde{\beta}_3E_{2n+1,3n})=E_{j,j+n-2},$$

т. е. $E_{1,n-1}, E_{2,n}\in\mathcal{L}_{n+1}(\mathcal{S})$.

При $j\in\{1,2\}$ имеем

$$\begin{aligned}&(B_{j+n}B_{j+n+1}\cdots B_{j+2n-3}A_0\hat{A}_0^2)'=\beta_{1,1}E_{1,n-1}+\beta_{1,2}E_{1,n}+\beta_{1,3}E_{2,n},\\&(B_{j+n}B_{j+n+1}\cdots B_{j+2n-3}A_0\hat{A}_0^2)''=\\&\quad=\tilde{a}_c^t(1-a^{-1})^2E_{j+n,j+2n-2}+\beta_2E_{n+1,2n},\quad t\in\{0,1\},\\&(B_{j+n}B_{j+n+1}\cdots B_{j+2n-3}A_0\hat{A}_0^2)'''=\beta_3E_{2n+1,3n}.\end{aligned}$$

Тогда

$$\begin{aligned}E_{j+n,j+2n-2}=\tilde{a}_c^{-t}(1-a^{-1})^{-2}(B_{j+n}B_{j+n+1}\cdots B_{j+2n-3}A_0\hat{A}_0^2-\\-\beta_{1,1}E_{1,n-1}-\beta_{1,2}E_{1,n}-\beta_{1,3}E_{2,n}-\beta_2E_{n+1,2n}-\beta_3E_{2n+1,3n}),\end{aligned}$$

т. е. $E_{n+1,2n-1}, E_{n+2,2n}\in\mathcal{L}_{n+1}(\mathcal{S})$.

Также при $j\in\{1,2\}$ имеем

$$\begin{aligned}&(B_{j+2n}B_{j+2n+1}\cdots B_{j+3n-3}A_0\tilde{A}_0^2)'=\beta_{1,1}E_{1,n-1}+\beta_{1,2}E_{1,n}+\beta_{1,3}E_{2,n},\\&(B_{j+2n}B_{j+2n+1}\cdots B_{j+3n-3}A_0\tilde{A}_0^2)''=\beta_2E_{n+1,2n},\\&(B_{j+2n}B_{j+2n+1}\cdots B_{j+3n-3}A_0\tilde{A}_0^2)'''=\\&\quad=\hat{a}_d^t(1-a)^2E_{j+2n,j+3n-2}+\beta_3E_{2n+1,3n},\quad t\in\{0,1\}.\end{aligned}$$

Тогда

$$\begin{aligned}E_{j+2n,j+3n-2}=\hat{a}_d^{-t}(1-a)^{-2}(B_{j+2n}B_{j+2n+1}\cdots B_{j+3n-3}A_0\tilde{A}_0^2-\\-\beta_{1,1}E_{1,n-1}-\beta_{1,2}E_{1,n}-\beta_{1,3}E_{2,n}-\beta_2E_{n+1,2n}-\beta_3E_{2n+1,3n}),\end{aligned}$$

т. е. $E_{2n+1,3n-1}, E_{2n+2,3n}\in\mathcal{L}_{n+1}(\mathcal{S})$.

Таким образом, мы получили, что

$$E_{1,n-1},\ E_{2,n},\ E_{n+1,2n-1},\ E_{n+2,2n},\ E_{2n+1,3n-1},\ E_{2n+2,3n}\in\mathcal{L}_{n+1}(\mathcal{S}).$$

Шаг индукции. а) Пусть $3\leqslant p\leqslant n-2$ и $j\in\{1,\ldots,p\}$. Рассмотрим произведения

$$\begin{aligned}&B_{j,j+n-p-1}=B_jB_{j+1}\cdots B_{j+n-p-1}\tilde{A}_0^2\hat{A}_0^2\in\mathcal{L}_{n-p+4}(\mathcal{S}),\\&B_{j+n,j+2n-p-1}=B_{j+n}B_{j+n+1}\cdots B_{j+2n-p-1}A_0^2\hat{A}_0^2\in\mathcal{L}_{n-p+4}(\mathcal{S}),\\&B_{j+2n,j+3n-p-1}=B_{j+2n}B_{j+2n+1}\cdots B_{j+3n-p-1}\tilde{A}_0^2A_0^2\in\mathcal{L}_{n-p+4}(\mathcal{S}).\end{aligned}$$

Отметим, что поскольку $p\geqslant 3$, то $n-p+4\leqslant n+1$ и $\mathcal{L}_{n-p+4}(\mathcal{S})\subseteq\mathcal{L}_{n+1}(\mathcal{S})$.

Имеем

$$B'_{j,j+n-p-1}=a(k_0,0)^{t_1}E_{j,j+n-p}+\sum_{h=1}^{n}\sum_{i=h+n-p+1}^{n}b_{h,i;j,p}E_{h,i},\quad t_1\in\{0,1\},$$

$$B''_{j,j+n-p-1} = \sum_{h=n+1}^{2n} \sum_{i=h+2n-p+1}^{2n} b_{h,i;j,p} E_{h,i},$$

$$B'''_{j,j+n-p-1} = \sum_{h=2n+1}^{3n} \sum_{i=h+2n-p+1}^{3n} b_{h,i;j,p} E_{h,i},$$

$$B'_{j+n,j+2n-p-1} = \sum_{h=1}^{n} \sum_{i=h+n-p+1}^{n} b_{h,i;j+n,p} E_{h,i},$$

$$B''_{j+n,j+2n-p-1} = (1-a^{-1})^2 \tilde{a}_c^{t_2} E_{j+n,j+2n-p} + \\ + \sum_{h=n+1}^{2n} \sum_{i=h+2n-p+1}^{2n} b_{h,i;j+n,p} E_{h,i}, \quad t_2 \in \{0,1\},$$

$$B'''_{j+n,j+2n-p-1} = \sum_{h=2n+1}^{3n} \sum_{i=h+2n-p+1}^{3n} b_{h,i;j+n,p} E_{h,i},$$

$$B'_{j+2n,j+3n-p-1} = \sum_{h=1}^{n} \sum_{i=h+n-p+1}^{n} b_{h,i;j+2n,p} E_{h,i},$$

$$B''_{j+2n,j+3n-p-1} = \sum_{h=n+1}^{2n} \sum_{i=h+2n-p+1}^{2n} b_{h,i;j+2n,p} E_{h,i},$$

$$B'''_{j+2n,j+3n-p-1} = a^2(1-a)^2 \hat{a}_d^{t_3} E_{j+2n,j+3n-p} + \\ + \sum_{h=2n+1}^{3n} \sum_{i=h+2n-p+1}^{3n} b_{h,i;j+2n,p} E_{h,i}, \quad t_3 \in \{0,1\}.$$

По предположению индукции $E_{i,i+n-q}$, $E_{i+n,i+2n-q}$, $E_{i+2n,i+3n-q} \in \mathcal{L}_{n+1}(\mathcal{S})$ для любых $q = 1, \ldots, p-1$, $i = 1, \ldots, q$. Значит,

$$B_{j,j+n-p-1} - a(k_0,0)^{t_1} E_{j,j+n-p} \in \mathcal{L}_{n+1}(\mathcal{S}),$$
$$B_{j+n,j+2n-p-1} - (1-a^{-1})^2 \tilde{a}_c^{t_2} E_{j+n,j+2n-p} \in \mathcal{L}_{n+1}(\mathcal{S}),$$
$$B_{j+2n,j+3n-p-1} - a^2(1-a)^2 \hat{a}_d^{t_3} E_{j+2n,j+3n-p} \in \mathcal{L}_{n+1}(\mathcal{S}).$$

Следовательно, получаем, что

$$E_{j,j+n-p} = \\ = a(k_0,0)^{-t_1} \Big(B_{j,j+n-p-1} - \big(B_{j,j+n-p-1} - \big(a(k_0,0)\big)^{t_1} E_{j,j+n-p} \big) \Big) \in \mathcal{L}_{n+1}(\mathcal{S}),$$

$$E_{j+n,j+2n-p} = (1-a^{-1})^{-2} \tilde{a}_c^{-t_2} \big(B_{j+n,j+2n-p-1} - \\ - (B_{j+n,j+2n-p-1} - (1-a^{-1})^2 \tilde{a}_c^{t_2} E_{j+n,j+2n-p}) \big) \in \mathcal{L}_{n+1}(\mathcal{S}),$$

$$E_{j+2n,j+3n-p} = a^{-2}(1-a)^{-2}\hat{a}_d^{-t_3}\big(B_{j+2n,j+3n-p-1} -$$
$$- (B_{j+2n,j+3n-p-1} - a^2(1-a)^2\hat{a}_d^{t_3}E_{j+2n,j+3n-p})\big) \in \mathcal{L}_{n+1}(\mathcal{S}).$$

б) Пусть $p = n-1$. Рассмотрим

$$B_j\tilde{A}_0^2\hat{A}_0^2,\ B_{j+n}A_0^2\hat{A}_0^2,\ B_{j+2n}\tilde{A}_0^2A_0^2 \in \mathcal{L}_5(\mathcal{S}) \subseteq \mathcal{L}_{n+1}(\mathcal{S}), \quad j = 1,\dots,n-1.$$

По построению

$$B_j\tilde{A}_0^2\hat{A}_0^2,\ B_{j+n}A_0^2\hat{A}_0^2,\ B_{j+2n}\tilde{A}_0^2A_0^2 \in \mathrm{N}_{3n}(\mathbb{F})$$

и

$$(B_j\tilde{A}_0^2\hat{A}_0^2)_{r,r+1} = (B_j)_{r,r+1},$$
$$(B_j\tilde{A}_0^2\hat{A}_0^2)_{r+n,r+n+1} = 0, \quad (B_j\tilde{A}_0^2\hat{A}_0^2)_{r+2n,r+2n+1} = 0,$$
$$(B_{j+n}A_0^2\hat{A}_0^2)_{r+n,r+n+1} = (B_{j+n})_{r+n,r+n+1},$$
$$(B_{j+n}A_0^2\hat{A}_0^2)_{r,r+1} = 0, \quad (B_{j+n}A_0^2\hat{A}_0^2)_{r+2n,r+2n+1} = 0,$$
$$(B_{j+2n}\tilde{A}_0^2A_0^2)_{r+2n,r+2n+1} = (B_{j+2n})_{r+2n,r+2n+1},$$
$$(B_{j+2n}\tilde{A}_0^2A_0^2)_{r,r+1} = 0, \quad (B_{j+2n}\tilde{A}_0^2A_0^2)_{r+n,r+n+1} = 0, \quad j,r = 1,\dots,n-1.$$

По доказанному получаем, что

$$B_j\tilde{A}_0^2\hat{A}_0^2 - \sum_{r=1}^{n-1}(B_j)_{r,r+1}E_{r,r+1} \in \mathcal{L}_{n+1}(\mathcal{S}),$$
$$B_{j+n}A_0^2\hat{A}_0^2 - \sum_{r=n+1}^{2n-1}(B_{j+n})_{r+n,r+n+1}E_{r+n,r+n+1} \in \mathcal{L}_{n+1}(\mathcal{S}),$$
$$B_{j+2n}\tilde{A}_0^2A_0^2 - \sum_{r=2n+1}^{3n-1}(B_{j+2n})_{r+2n,r+2n+1}E_{r+2n,r+2n+1} \in \mathcal{L}_{n+1}(\mathcal{S}).$$

Следовательно,

$$E_{k_0,k_0+1},\ E_{c,c+1},\ E_{d,d+1},$$
$$E_{r_1,r_1+1} + \gamma_{r_1}E_{k_0,k_0+1},\ E_{r_2,r_2+1} + \gamma_{r_2}E_{c,c+1},\ E_{r_3,r_3+1} + \gamma_{r_3}E_{d,d+1} \in \mathcal{L}_{n+1}(\mathcal{S}),$$
$$r_1 \in \{1,\dots,n-1\} \setminus \{k_0\}, \quad r_2 \in \{n+1,\dots,2n-1\} \setminus \{c\},$$
$$r_3 \in \{2n+1,\dots,3n-1\} \setminus \{d\}.$$

Значит,

$$E_{j,j+1},\ E_{j+n,j+n+1},\ E_{j+2n,j+2n+1} \in \mathcal{L}_{n+1}(\mathcal{S}), \quad j = 1,\dots,n-1.$$

2. Заметим, что

$$0 \oplus 0 \oplus E = (a^2 - a)^{-1}(A_0^2 - A_0) + N_1, \quad N_1 \in \mathcal{A}_{n,n,n} \cap \mathrm{N}_{3n}(\mathbb{F}),$$
$$0 \oplus E \oplus 0 = (a^{-1} - 1)^{-1}(a^{-1}A_0^2 - A_0) + N_2, \quad N_2 \in \mathcal{A}_{n,n,n} \cap \mathrm{N}_{3n}(\mathbb{F}),$$

и $N_1, N_2 \in \mathcal{L}_{n+1}(\mathcal{S})$ по доказанному выше. Следовательно, $0 \oplus E \oplus 0$, $0 \oplus 0 \oplus E \in \mathcal{L}_{n+1}(\mathcal{S})$.

Таким образом, $\mathcal{L}_{n+1}(\mathcal{S}) = \mathcal{A}_{n,n,n}$, т. е. $l(\mathcal{S}) \leqslant n+1$. □

Теорема 5.40. *Пусть $\mathbb{F} \neq \mathbb{F}_2$ — произвольное поле, $n \in \mathbb{N}$ и $n \geqslant 5$. Тогда $l(\mathcal{A}_{n,n,n}) = n+1$.*

Доказательство. Сначала докажем верхнюю оценку $l(\mathcal{A}_{n,n,n}) \leqslant n+1$. Для этого рассмотрим произвольную систему порождающих $\mathcal{S}$ для алгебры $\mathcal{A}_{n,n,n}$. Без ограничения общности можно считать, что $\mathcal{S}$ удовлетворяет условиям леммы 5.28. Тогда из лемм 5.39 и 5.38 получаем, что $l(\mathcal{S}) \leqslant n+1$. Следовательно,

$$l(\mathcal{A}_{n,n,n}) = \max_{\mathcal{S}} l(\mathcal{S}) \leqslant \max_{\mathcal{S}} (n+1) = n+1.$$

Построим систему порождающих для $\mathcal{A}_{n,n,n}$ длины $n+1$. Пусть

$$\mathcal{S}_{n+1} = \Biggl\{ A = \sum_{j=1}^{n} (E_{j,j} + aE_{j+n,j+n}),\ a \neq 0, 1, \\ A_i = E_{i,i+1} + E_{n+i,n+i+1} + E_{2n+i,2n+i+1} \Biggm| i = 1, \ldots, n-1 \Biggr\}.$$

Так как $A_i A_j = 0$ при $j \neq i+1$,

$$AA_i = A_i A = E_{i,i+1} + aE_{i+n,i+n+1}, \quad A^2 A_i = A_i A^2 = E_{i,i+1} + a^2 E_{i+n,i+n+1}$$

для $i = 1, \ldots, n-1$ и

$$A^3 = (a+1)A^2 - aA,$$

то

$$\dim \mathcal{L}_{n+1}(\mathcal{S}) = 3 + 3\sum_{k=1}^{n-1} (n-k) = \dim \mathcal{A}_{n,n,n},$$

но $\dim \mathcal{L}_{n+1}(\mathcal{S}) - \dim \mathcal{L}_n(\mathcal{S}) = 1$, т. е. $\dim \mathcal{L}_n(\mathcal{S}) < \dim \mathcal{A}_{n,n,n}$. Следовательно, $l(\mathcal{S}) = n+1$ и $l(\mathcal{A}_{n,n,n}) \geqslant l(\mathcal{S}) = n+1$. □

Следствие 5.41. *Пусть $\mathbb{F} \neq \mathbb{F}_2$ — произвольное поле, $n \in \mathbb{N}$ и $n \geqslant 5$. Пусть $a \in \mathbb{F}$, $a \neq 0, 1$, и*

$$C_{n,n,n} = \sum_{i=1}^{n-1} E_{i,i+1} + \sum_{j=n+1}^{2n-1} (E_{j,j} + E_{j,j+1}) + E_{2n,2n} + \\ + \sum_{k=2n+1}^{3n-1} (aE_{k,k} + E_{k,k+1}) + aE_{3n,3n} \in \mathcal{A}_{n,n,n} -$$

циклическая матрица. Положим

$$\mathcal{A}'_{n,n,n} = \langle C_{n,n,n}^j \mid 0 \leqslant j \leqslant 3n-1 \rangle \subseteq \mathcal{A}_{n,n,n}.$$

Тогда

1) $l(\mathcal{A}'_{n,n,n}) = 3n-1$;

2) $l(\mathcal{A}'_{n,n,n}) - l(\mathcal{A}_{n,n,n}) = 2n-2$;
3) $2 < l(\mathcal{A}'_{n,n,n})/l(\mathcal{A}_{n,n,n}) = 2 + (n-3)/(n+1) < 3$.

Замечание 5.42. Пусть

$$\mathcal{A}_{n_1} = \langle E^{(n_1)}, E_{i,j},\ 1 \leqslant i < j \leqslant n_1 \rangle \subset \mathrm{T}_{n_1}(\mathbb{F}).$$

Заметим, что $\mathcal{A}_{n_1,n_2,n_3} = \mathcal{A}_{n_1} \oplus \mathcal{A}_{n_2,n_3}$ и

$$l(\mathcal{A}_{n_1,n_2,n_3}) = l(\mathcal{A}_{n_1}) = \max\big(l(\mathcal{A}_{n_1}), l(\mathcal{A}_{n_2,n_3})\big).$$

Таким образом, мы получили ещё один пример точности нижней оценки в неравенствах (3.6).

5.2. Монотонность функции длины

В этом подразделе приведём примеры алгебр, для которых длина подалгебры может быть оценена длиной всей алгебры.

Следствие 5.43. *Пусть $\mathbb{F}$ — произвольное поле, $n, m \in \mathbb{N}$, $n \geqslant m-2$, $\mathcal{A}_{n,m}$ — алгебра, описанная в теореме 5.24. Пусть*

$$\mathcal{B} = \left\langle E_{i,j},\ 1 \leqslant i < j \leqslant n,\ E,\ \sum_{i=1}^{n} E_{i,i},\ N_1, \ldots, N_p \in 0 \oplus \mathrm{N}_m(\mathbb{F}) \right\rangle \subseteq \mathcal{A}_{n,m}.$$

Тогда $l(\mathcal{B}) = n-1 = l(\mathcal{A}_{n,m})$.

Предложение 5.44. *Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{A}$ — конечномерная алгебра над $\mathbb{F}$ и $\mathcal{B} \subseteq \mathcal{A}$, причём существуют такие $a_1, \ldots, a_n \in \mathcal{A}$, что $\langle \mathcal{B}, a_1, \ldots, a_n \rangle = \mathcal{A}$ и для любого $b \in \mathcal{B}$ выполнено $a_i b, b a_i \in \langle a_1, \ldots, a_n \rangle$. Тогда $l(\mathcal{B}) \leqslant l(\mathcal{A})$.*

Доказательство. Пусть $\mathcal{S}_\mathcal{B}$ — произвольная система порождающих алгебры $\mathcal{B}$. Тогда $\mathcal{S}_\mathcal{A} = \mathcal{S}_\mathcal{B} \cup \{a_1, \ldots, a_n\}$ будет системой порождающих для $\mathcal{A}$ длины $l(\mathcal{S}_\mathcal{B})$. Следовательно, $l(\mathcal{A}) \geqslant l(\mathcal{S}_\mathcal{A}) = l(\mathcal{S}_\mathcal{B})$, и значит, $l(\mathcal{A}) \geqslant \max\limits_{\mathcal{S}_\mathcal{B}} l(\mathcal{S}_\mathcal{B}) = l(\mathcal{B})$. □

Приведём примеры таких алгебр.

Пример 5.45. Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{A} \subseteq \mathrm{T}_n(\mathbb{F})$ — произвольная подалгебра верхнетреугольной матричной алгебры и $\mathcal{B} = \mathcal{A} \cap \mathrm{D}_n(\mathbb{F})$. Тогда $l(\mathcal{B}) \leqslant l(\mathcal{A})$.

Пример 5.46. Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{A}$, $\mathcal{B}$ — конечномерные алгебры над $\mathbb{F}$. Тогда $\mathcal{A} \subset \mathcal{A} \oplus \mathcal{B}$ и $l(\mathcal{A}) \leqslant l(\mathcal{A} \oplus \mathcal{B})$.

Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — конечномерная ассоциативная $\mathbb{F}$-алгебра с единицей $1_\mathcal{A}$.

Покажем, что на подалгебрах алгебр длины 1 функция длины монотонна.

Лемма 5.47. *Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{A}$ — алгебра с единицей $1_\mathcal{A}$ над $\mathbb{F}$ и $\mathcal{A}'$ — произвольная подалгебра в $\mathcal{A}$. Если $l(\mathcal{A}) = 1$, то $l(\mathcal{A}') \leqslant 1$.*

Доказательство. Предположим, что существует подалгебра $\mathcal{B} \subset \mathcal{A}$ длины $l(\mathcal{B}) \geqslant 2$. Обозначим $n = \dim \mathcal{A}$, $m = \dim \mathcal{B}$ и $k = l(\mathcal{B})$. Пусть $\mathcal{S}_1$ — система порождающих для алгебры $\mathcal{B}$ длины $l(\mathcal{S}_1) = k$. Из условия $k > 1$ получаем, что $\dim \mathcal{L}_1(\mathcal{S}_1) < m$. Пусть $B_1, \ldots, B_m \in \mathcal{S}_1^k$ — базис $\mathcal{B}$. Существуют элементы $B_{m+1}, \ldots, B_n \in \mathcal{A}$, такие что $B_1, \ldots, B_n$ образуют базис $\mathcal{A}$. Тогда множество $\mathcal{S}_2 = \{B_{m+1}, \ldots, B_n, S \mid S \in \mathcal{S}_1\}$ будет системой порождающих алгебры $\mathcal{A}$. Также получаем, что $\dim \mathcal{L}_1(\mathcal{S}_2) \leqslant \dim \mathcal{L}_1(\mathcal{S}_1) + n - m < m + n - m = n$, т. е. $l(\mathcal{A}) \geqslant l(\mathcal{S}_2) > 1$. Противоречие. □

Следствие 5.48. *Пусть $\mathbb{F}$ — произвольное поле, $\mathcal{A}$ — алгебра с единицей $1_{\mathcal{A}}$ над $\mathbb{F}$. Если $l(\mathcal{A}) = 1$, то для любого элемента $A \in \mathcal{A}$ справедливо $\deg A \leqslant 2$.*

Доказательство. Предположим, что существует такой элемент $A \in \mathcal{A}$, что $\deg A = k \geqslant 3$. Пусть $\mathcal{A}' \subseteq \mathcal{A}$ — подалгебра, порождённая элементом A. По построению $l(\mathcal{A}') = k - 1 \geqslant 2$. Но $l(\mathcal{A}') \leqslant 1$ по лемме 5.47. Противоречие. □

Предложение 5.49. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — подалгебра в $\mathrm{M}_n(\mathbb{F})$, содержащая единичную матрицу E. Если для любой подалгебры $\mathcal{A}' \subseteq \mathcal{A}$ с $E \in \mathcal{A}'$ выполнено $l(\mathcal{A}') \leqslant l(\mathcal{A})$, то для всех подалгебр $\mathcal{B} \subseteq \mathcal{A}$ выполнено $l(\mathcal{B}) \leqslant l(\mathcal{A})$.*

Доказательство. Пусть $\mathcal{B}$ — подалгебра в $\mathcal{A}$ и $E \notin B$. Положим $\mathcal{B}_1 = \langle E, B \mid B \in \mathcal{B} \rangle$. По построению $\mathcal{B} \subseteq \mathcal{B}_1 \subseteq \mathcal{A}$. Тогда по условию предложения $l(\mathcal{B}_1) \leqslant l(\mathcal{A})$. Согласно следствию 3.7 $l(\mathcal{B}) = l(\mathcal{B}_1)$. Следовательно, $l(\mathcal{B}) \leqslant l(\mathcal{A})$. □

Предложение 5.50. *Пусть $\mathbb{F}$ — произвольное поле и $\mathcal{A}$ — подалгебра в $\mathrm{M}_n(\mathbb{F})$, не содержащая единичную матрицу E. Пусть*

$$\mathcal{A}_1 = \langle E, A \mid A \in \mathcal{A} \rangle \subseteq \mathrm{M}_n(\mathbb{F}).$$

Тогда если для любой подалгебры $\mathcal{A}' \subseteq \mathcal{A}_1$ выполнено $l(\mathcal{A}') \leqslant l(\mathcal{A}_1)$, то для всех подалгебр $\mathcal{B} \subseteq \mathcal{A}$ выполнено $l(\mathcal{B}) \leqslant l(\mathcal{A})$.

Доказательство. Пусть $\mathcal{B}$ — подалгебра в $\mathcal{A}$. В этом случае $\mathcal{B}$ также является подалгеброй в $\mathcal{A}_1$. Следовательно, по условию $l(\mathcal{B}) \leqslant l(\mathcal{A}_1)$, но согласно следствию 3.7 $l(\mathcal{A}_1) = l(\mathcal{A})$. Следовательно, $l(\mathcal{B}) \leqslant l(\mathcal{A})$. □

Следствие 5.51. *В классе матричных подалгебр монотонность длины достаточно проверять на подалгебрах, содержащих единичную матрицу.*

5.3. Подалгебры матриц порядков 2 и 3

Мы показываем, что для $n = 2, 3$ функция длины монотонна на подалгебрах $\mathrm{M}_n(\mathbb{F})$, т. е. для произвольных подалгебр $\mathcal{A}' \subseteq \mathcal{A} \subseteq \mathrm{M}_n(\mathbb{F})$ выполнено $l(\mathcal{A}') \leqslant l(\mathcal{A})$. Таким образом, пример 5.9 является минимальным в классе матричных подалгебр.

Ввиду следствия 5.51 в дальнейшем будем предполагать, что все рассматриваемые подалгебры содержат единичную матрицу.

5.3.1. Длина подалгебр в $\mathrm{M}_2(\mathbb{F})$

Лемма 5.52. *Пусть $\mathbb{F}$ — произвольное поле. Тогда $l\big(\mathrm{M}_2(\mathbb{F})\big) = 2$.*

Доказательство. Поскольку алгебра матриц $\mathrm{M}_2(\mathbb{F})$ не является коммутативной, то из следствия 4.36 получаем верхнюю оценку

$$l\big(\mathrm{M}_2(\mathbb{F})\big) \leqslant \dim \mathrm{M}_2(\mathbb{F}) - 2 = 2.$$

Эта оценка достигается на системе порождающих, состоящей из матриц $E_{1,2}$ и $E_{2,1}$. □

Теорема 5.53. *Пусть $\mathbb{F}$ — произвольное поле. Тогда для произвольных подалгебр $\mathcal{A}' \subseteq \mathcal{A} \subseteq \mathrm{M}_2(\mathbb{F})$ выполнено $l(\mathcal{A}') \leqslant l(\mathcal{A}) \leqslant l\big(\mathrm{M}_2(\mathbb{F})\big) = 2$.*

Доказательство. Пусть $\mathcal{A}' \subseteq \mathcal{A} \subseteq \mathrm{M}_2(\mathbb{F})$. Имеем

$$1 \leqslant \dim \mathcal{A}' \leqslant \dim \mathcal{A} \leqslant \dim \mathrm{M}_2(\mathbb{F}) = 4.$$

Заметим, что если $\dim \mathcal{A} \geqslant 2$, то $l(\mathcal{A}) \geqslant 1$. Рассмотрим случаи.

1. $\dim \mathcal{A} = 1$. Тогда $\mathcal{A} = \mathbb{F}E$, $l(\mathcal{A}) = 0$ и не существует $\mathcal{A}' \neq \mathcal{A}$.

2. $\dim \mathcal{A} = 2$. В этом случае $1 \leqslant l(\mathcal{A}) \leqslant \dim \mathcal{A} - 1 = 1$, т. е. $l(\mathcal{A}) = 1$, и по лемме 5.47 также получаем оценку $l(\mathcal{A}') \leqslant 1 = l(\mathcal{A})$.

3. $\dim \mathcal{A} = 3$. Покажем, что $l(\mathcal{A}) = 1$. Ввиду тривиальных оценок $1 \leqslant l(\mathcal{A}) \leqslant 2$. Пусть $l(\mathcal{A}) = 2 = \dim \mathcal{A} - 1$. Тогда по лемме 4.34 существует элемент $A \in \mathcal{A}$ степени $\deg A = 3$. Противоречие с теоремой Гамильтона—Кэли.

Таким образом, $l(\mathcal{A}) = 1$. Также если $\mathcal{A}' \subset \mathcal{A}$, то $\dim \mathcal{A}' \leqslant 2$, и по доказанному в пунктах 1 и 2 справедлива оценка $l(\mathcal{A}') \leqslant 1$. Получаем, что $l(\mathcal{A}') \leqslant 1 = l(\mathcal{A})$.

4. $\dim \mathcal{A} = 4 = \dim \mathrm{M}_2(\mathbb{F})$. Тогда $\mathcal{A} = \mathrm{M}_2(\mathbb{F})$ и $l(\mathcal{A}) = 2$ по лемме 5.52. Если $\mathcal{A}' \subset \mathcal{A}$, то $\dim \mathcal{A}' \leqslant 3$, следовательно, $l(\mathcal{A}') \leqslant \dim \mathcal{A}' - 1 \leqslant 2 = l(\mathcal{A})$. □

Следствие 5.54. *Пусть $\mathbb{F}$ — произвольное поле. Тогда функция длины строго монотонна на алгебре $\mathrm{M}_2(\mathbb{F})$.*

5.3.2. Длина подалгебр в $\mathrm{M}_3(\mathbb{F})$

Лемма 5.55. *Пусть $\mathbb{F}$ — произвольное поле. Тогда $l\big(\mathrm{M}_3(\mathbb{F})\big) = 4$.*

Доказательство. Пусть $\mathcal{S} = \{A_1, \ldots, A_k\}$ — система порождающих алгебры $\mathrm{M}_3(\mathbb{F})$. По предложению 3.4 можно считать, что все элементы $\mathcal{S}$ линейно независимы и $\dim \mathcal{L}_1(\mathcal{S}) = |\mathcal{S}| + 1 = k + 1$.

Если $\dim \mathcal{L}_1(\mathcal{S}) \leqslant 2$, то $\mathcal{S} = \{A_1\}$, и по теореме Гамильтона—Кэли $\dim \mathcal{L}(\mathcal{S}) \leqslant 3 < 9 = \dim \mathrm{M}_3(\mathbb{F})$, т. е. $\mathcal{S}$ не является системой порождающих. Значит, $\dim \mathcal{L}_1(\mathcal{S}) \geqslant 3$.

Заметим, что если $\dim \mathcal{L}_i(\mathcal{S}) < \dim \mathrm{M}_3(\mathbb{F})$, то $\dim \mathcal{L}_{i+1}(\mathcal{S}) \geqslant \dim \mathcal{L}_i(\mathcal{S}) + 1$. Следовательно, если $\dim \mathcal{L}_1(\mathcal{S}) \geqslant 6$ и $l(\mathcal{S}) \geqslant 4$, то $\dim \mathcal{L}_2(\mathcal{S}) \geqslant 7$, $\dim \mathcal{L}_3(\mathcal{S}) \geqslant 8$ и $\dim \mathcal{L}_4(\mathcal{S}) = 9$, т. е. $l(\mathcal{S}) = 4$. Значит, для систем порождающих $\mathcal{S}$ с $|\mathcal{S}| \geqslant 5$ справедлива оценка $l(\mathcal{S}) \leqslant 4$.

Пусть $3 \leqslant \dim L_1(\mathcal{S}) \leqslant 5$. Предположим, что $l(\mathcal{S}) \geqslant 5$, и приведём это утверждение к противоречию.

Если $l(\mathcal{S}) > 4$, то в $\mathcal{S}^5 \backslash \mathcal{S}^{5-1}$ найдётся несократимое слово $B = A_{i_1} \ldots A_{i_5}$. Из несократимости B следует, что и его подслова $A_{i_1}A_{i_2}$, $A_{i_1}A_{i_2}A_{i_3}$ и $A_{i_1}A_{i_2}A_{i_3}A_{i_4}$ несократимы, и значит, $\dim \mathcal{L}_4(\mathcal{S}) \geqslant \dim \mathcal{L}_1(\mathcal{S}) + 3$.

I. Допустим, что $\dim \mathcal{L}_2(\mathcal{S}) = \dim \mathcal{L}_1(\mathcal{S}) + 1$. В этом случае все слова в $\mathcal{L}_2(\mathcal{S})$ представляются в виде линейной комбинации $A_{i_1}A_{i_2}$ и слов длины, меньшей 2. Но тогда слово B — линейная комбинация сократимого по теореме Гамильтона—Кэли слова $A_{i_1}^3 A_{i_2} A_{i_5}$ и слов длины, меньшей 5, т. е. B сократимо. Противоречие.

II. Пусть теперь $\dim \mathcal{L}_2(\mathcal{S}) \geqslant \dim \mathcal{L}_1(\mathcal{S}) + 2$. В этом случае $\dim \mathcal{L}_4(\mathcal{S}) \geqslant \dim \mathcal{L}_1(\mathcal{S}) + 4$.

При $\dim L_1(\mathcal{S}) = 5$ получаем, что $\dim \mathcal{L}_4(\mathcal{S}) = 9 = \dim \mathrm{M}_3(\mathbb{F})$, $\mathcal{L}_4(\mathcal{S}) = \mathrm{M}_3(\mathbb{F})$, а значит, B сократимо. Противоречие.

Пусть $\dim L_1(\mathcal{S}) \leqslant 4$.

1. Предположим, что все слова в $\mathcal{L}_3(\mathcal{S})$ представляются в виде линейной комбинации слова $A_{i_1}A_{i_2}A_{i_3}$ и слов длины, меньшей 3. Тогда получим, что слово B представляется в виде линейной комбинации сократимого слова $A_{i_1}^3 A_{i_2} A_{i_3}$ и слов длины, меньшей 5, т. е. B сократимо. Противоречие.

2. Пусть в $\mathcal{L}_3(\mathcal{S})$ есть несократимое слово, не представляющееся в виде линейной комбинации слова $A_{i_1}A_{i_2}A_{i_3}$ и слов длины, меньшей 3. Следовательно, $\dim \mathcal{L}_4(\mathcal{S}) \geqslant \dim \mathcal{L}_1(\mathcal{S}) + 5$.

При $\dim L_1(\mathcal{S}) = 4$ получаем, что $\dim \mathcal{L}_4(\mathcal{S}) = 9 = \dim \mathrm{M}_3(\mathbb{F})$, $\mathcal{L}_4(\mathcal{S}) = \mathrm{M}_3(\mathbb{F})$, а значит, B сократимо. Противоречие.

Пусть $\dim L_1(\mathcal{S}) = 3$. Возможны два случая: либо $i_1 = i_2$, либо $i_1 \neq i_2$.

а) Если $i_1 = i_2$, то либо все слова в $\mathcal{L}_4(\mathcal{S})$ представляются в виде линейной комбинации слова $A_{i_1}^2 A_{i_3} A_{i_4}$ и слов длины, меньшей 4, либо $\dim \mathcal{L}_4(\mathcal{S}) = 9$. Тогда слово B либо представляется в виде линейной комбинации сократимого слова $A_{i_1}^3 A_{i_3} A_{i_4}$ и слов длины, меньшей 5, либо $B \in \mathcal{L}_4(\mathcal{S})$, поскольку $\mathcal{L}_4(S) = \mathrm{M}_3(\mathbb{F})$, т. е. B не может быть несократимо. Противоречие.

б) Если $i_1 \neq i_2$, то либо $\dim \mathcal{L}_4(\mathcal{S}) = 9$ и $B \in \mathcal{L}_4(\mathcal{S}) = \mathrm{M}_3(\mathbb{F})$, либо слово B представляется линейной комбинацией сократимого по пункту а) слова $A_{i_1}^2 A_{i_2} A_{i_3} A_{i_4}$ и слов меньшей длины, т. е. также получается, что B сократимо. Противоречие.

Следовательно, все слова в $\mathcal{S}^5 \setminus \mathcal{S}^{5-1}$ сократимы и $l(\mathcal{S}) \leqslant 4$. Тогда получаем оценку

$$l\big(\mathrm{M}_3(\mathbb{F})\big) = \max_{\mathcal{S}} l(\mathcal{S}) \leqslant 4.$$

Эта оценка достигается на системе порождающих, состоящей из матриц $E_{1,2}$ и $E_{1,2} + E_{2,3} + E_{3,1}$. $\square$

Теорема 5.56 [31, теорема 1.5.1]. *Пусть $\mathbb{F}$ — алгебраически замкнутое поле, $\mathcal{A}$ — подалгебра с единицей в $\mathrm{M}_n(\mathbb{F})$. Тогда существует базис пространства $\mathbb{F}^n$, в котором любая матрица $A \in \mathcal{A}$ представляется в блочно-верхнетреугольном* *виде*

$$A = \begin{pmatrix} A_{11} & A_{12} & \dots & & A_{1k} \\ 0 & A_{22} & \dots & & A_{2k} \\ 0 & 0 & A_{33} & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & & A_{kk} \end{pmatrix},$$

где $\mathcal{A}_{ii} \in \mathrm{M}_{n_i}(\mathbb{F})$, $i = 1, \dots, k$, $n_1 + \dots + n_k = n$, *и множество* $\{1, \dots, k\}$ *есть объединение попарно непересекающихся множеств* $J_1, J_2, \dots, J_l$, *причём*

1) $\{A_{ii} \mid A \in \mathcal{A}\} = \mathrm{M}_{n_i}(\mathbb{F})$, $i = 1, \dots, k$;
2) *если* $i, j \in J_s$, *то* $A_{ii} = A_{jj}$ *для всех* $A \in \mathcal{A}$;
3) *если* $i \in J_r$, $j \in J_s$ *и* $r \neq s$, *то* $\{(A_{ii}, A_{jj}) \mid A \in \mathcal{A}\} = \mathrm{M}_{n_i}(\mathbb{F}) \oplus \mathrm{M}_{n_j}(\mathbb{F})$;
4) *если* $i \in J_s$, *то существует такая матрица* $A \in \mathcal{A}$, *что* $A_{ii} = E$ *и* $A_{jj} = 0$ *для всех* $j \notin J_s$.

Предложение 5.57. *Пусть* $\mathbb{F}$ *— произвольное поле. Пусть* $\mathcal{A}$ *— подалгебра в* $\mathrm{M}_3(\mathbb{F})$ *и* $\mathcal{A} \neq \mathrm{M}_3(\mathbb{F})$. *Тогда* $\dim \mathcal{A} \leqslant 7$.

Доказательство. I. Пусть поле $\mathbb{F}$ алгебраически замкнуто. Тогда по теореме 5.56 существуют блочно-верхнетреугольная подалгебра $\mathcal{B} \subset \mathrm{M}_3(\mathbb{F})$ и невырожденная матрица $T \in \mathrm{M}_3(\mathbb{F})$, такие что $T^{-1}\mathcal{A}T = \mathcal{B}$. Пусть k — число диагональных блоков в $\mathcal{B}$. Очевидно, что k ограничено сверху размером матриц, т. е. $k \leqslant 3$.

1. Если $k = 1$, то $\mathcal{B} = \mathrm{M}_3(\mathbb{F})$, и следовательно, $\mathcal{A} = \mathrm{M}_3(\mathbb{F})$ — противоречие с условием предложения.

2. Если $k = 3$, то $\mathcal{B} \subseteq \mathrm{T}_3(\mathbb{F})$ и $\dim \mathcal{A} = \dim \mathcal{B} \leqslant \dim \mathrm{T}_3(\mathbb{F}) = 6$.

3. Пусть $k = 2$. Тогда $n_1, n_2 \in \mathbb{N}$ и $n_1 + n_2 = 3$. Следовательно, либо $n_1 = 2$, $n_2 = 1$, либо $n_1 = 1$, $n_2 = 2$. Значит, все матрицы $B \in \mathcal{B}$ либо имеют вид

$$B = \begin{pmatrix} b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,1} & b_{2,2} & b_{2,3} \\ 0 & 0 & b_{3,3} \end{pmatrix},$$

либо имеют вид

$$B = \begin{pmatrix} b_{1,1} & b_{1,2} & b_{1,3} \\ 0 & b_{2,2} & b_{2,3} \\ 0 & b_{3,2} & b_{3,3} \end{pmatrix}.$$

В обоих случаях получаем, что в двух фиксированных позициях в каждой матрице из $\mathcal{B}$ стоят нули, т. е. число ненулевых координат не более 7, следовательно, $\dim \mathcal{A} = \dim \mathcal{B} \leqslant 7$.

II. Пусть поле $\mathbb{F}$ не является алгебраически замкнутым и $\bar{\mathbb{F}}$ — его алгебраическое замыкание. Рассмотрим подалгебру $\mathcal{A}_{\bar{\mathbb{F}}} = (\mathcal{A}_{\mathbb{F}} \otimes_{\mathbb{F}} \bar{\mathbb{F}})_{\bar{\mathbb{F}}} \subseteq \mathrm{M}_3(\bar{\mathbb{F}})$. По доказанному выше $\dim_{\bar{\mathbb{F}}} \mathcal{A}_{\bar{\mathbb{F}}} \leqslant 7$. По построению $\dim_{\mathbb{F}} \mathcal{A} = \dim_{\bar{\mathbb{F}}} \mathcal{A}_{\bar{\mathbb{F}}}$, следовательно, $\dim \mathcal{A} \leqslant 7$. □

Предложение 5.58. *Пусть* $\mathbb{F}$ — *алгебраически замкнутое поле. Пусть* $\mathcal{A}$ — *подалгебра в* $\mathrm{M}_3(\mathbb{F})$ *и* $\dim\mathcal{A} = 6$. *Тогда существует невырожденная матрица* $T \in \mathrm{M}_3(\mathbb{F})$, *такая что* $T^{-1}\mathcal{A}T = \mathrm{T}_3(\mathbb{F})$.

Доказательство. По теореме 5.56 существуют блочно-верхнетреугольная подалгебра $\mathcal{B} \subset \mathrm{M}_3(\mathbb{F})$ и невырожденная матрица $T \in \mathrm{M}_3(\mathbb{F})$, такие что $T^{-1}\mathcal{A}T = \mathcal{B}$. Пусть k — число диагональных блоков в $\mathcal{B}$, $k \leqslant 3$.

I. Если $k = 1$, то $\mathcal{B} = \mathrm{M}_3(\mathbb{F})$, и следовательно, $\mathcal{A} = \mathrm{M}_3(\mathbb{F})$ — противоречие с условием предложения.

II. Если $k = 3$, то $\mathcal{B} \subseteq \mathrm{T}_3(\mathbb{F})$, при этом $\dim\mathcal{B} = \dim\mathcal{A} = 6 = \dim\mathrm{T}_3(\mathbb{F})$, значит, $\mathcal{B} = \mathrm{T}_3(\mathbb{F})$.

III. Пусть $k = 2$. Покажем, что в этом случае $\dim\mathcal{B} \neq 6$. Имеем, что $n_1, n_2 \in \mathbb{N}$ и $n_1 + n_2 = 3$. Следовательно, либо $n_1 = 2$, $n_2 = 1$, либо $n_1 = 1$, $n_2 = 2$.

1. Пусть $n_1 = 2$, $n_2 = 1$. В этом случае все матрицы $B \in \mathcal{B}$ имеют вид

$$B = \begin{pmatrix} b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,1} & b_{2,2} & b_{2,3} \\ 0 & 0 & b_{3,3} \end{pmatrix},$$

причём из теоремы 5.56 следует, что $\mathcal{B}$ содержит матрицы

$$B_{i,j} = E_{i,j} + b_{i,j;1}E_{1,3} + b_{i,j;2}E_{2,3}, \quad 1 \leqslant i, j \leqslant 2,$$

и

$$B_{3,3} = E_{3,3} + b_{3,3;1}E_{1,3} + b_{3,3;2}E_{2,3}.$$

Матрицы $B_{i,j}$ линейно независимы, поэтому существует матрица $C = \{c_{i,j}\} \in \mathcal{B}$, дополняющая множество матриц $B_{i,j}$ до базиса алгебры $\mathcal{B}$. Рассматривая преобразование

$$B_{i,j} \to B_{i,j}, \quad i,j = 1,2, \quad C \to C - \sum_{i,j=1}^{2} c_{i,j}B_{i,j} - c_{3,3}B_{3,3}$$

базиса алгебры $\mathcal{B}$ с обратимой матрицей

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -c_{1,1} \\ 0 & 1 & 0 & 0 & 0 & -c_{1,2} \\ 0 & 0 & 1 & 0 & 0 & -c_{2,1} \\ 0 & 0 & 0 & 1 & 0 & -c_{2,2} \\ 0 & 0 & 0 & 0 & 1 & -c_{3,3} \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

можно считать, что $C = c_{1,3}E_{1,3} + c_{2,3}E_{2,3}$. Поскольку $C \neq 0$, то $c_{1,3}$ и $c_{2,3}$ не равны нулю одновременно.

Если $c_{1,3} \neq 0$, то

$$c_{1,3}^{-1}B_{1,1}C = E_{1,3},\ c_{1,3}^{-1}B_{2,1}C = E_{2,3} \in \mathcal{B}.$$

Если $c_{2,3} \neq 0$, то

$$c_{2,3}^{-1} B_{1,2} C = E_{1,3},\ c_{2,3}^{-1} B_{2,2} C = E_{2,3} \in \mathcal{B}.$$

Следовательно,

$$\dim \mathcal{B} \geqslant \dim \langle B_{1,1}, B_{1,2}, \ldots, B_{3,3}, E_{1,3}, E_{2,3} \rangle = 7.$$

2. Пусть $n_1 = 1$, $n_2 = 2$. Пусть

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Тогда отображение φ, ставящее в соответствие каждой матрице $B \in \mathcal{B}$ матрицу $\varphi(B) = (A^{-1} B A)^{\mathrm{T}}$, является антиизоморфизмом алгебры $\mathcal{B}$. Следовательно, $\dim \mathcal{B} = \dim \varphi(\mathcal{B})$. Алгебра $\varphi(\mathcal{B})$ имеет блочную структуру, рассмотренную в пункте 1 доказательства, поэтому $\dim \varphi(\mathcal{B}) \neq 6$. Значит, и $\dim \mathcal{B} \neq 6$. □

Предложение 5.59. *Пусть $\mathbb{F}$ — произвольное поле. Пусть $\mathcal{A}$ — подалгебра в $\mathrm{M}_3(\mathbb{F})$ и $\dim \mathcal{A} = 6$. Тогда $l(\mathcal{A}) \leqslant 2$.*

Доказательство. Пусть $\bar{\mathbb{F}}$ — алгебраическое замыкание поля $\mathbb{F}$. Рассмотрим подалгебру $\mathcal{A}_{\bar{\mathbb{F}}} = (\mathcal{A}_{\mathbb{F}} \otimes_{\mathbb{F}} \bar{\mathbb{F}})_{\bar{\mathbb{F}}} \subseteq \mathrm{M}_3(\bar{\mathbb{F}})$. Последовательно применяя предложение 3.19, следствие 3.12 и лемму 5.58, получаем оценку

$$l(\mathcal{A}) \leqslant l(\mathcal{A}_{\bar{\mathbb{F}}}) = l\big(\mathrm{T}_3(\mathbb{F})\big) = 2. \qquad \square$$

Лемма 5.60. *Пусть $\mathbb{F}$ — произвольное поле. Пусть $\mathcal{B}_{2,1}$ — подалгебра в $\mathrm{M}_3(\mathbb{F})$, состоящая из всех матриц вида*

$$B = \begin{pmatrix} b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,1} & b_{2,2} & b_{2,3} \\ 0 & 0 & b_{3,3} \end{pmatrix},$$

и пусть $\mathcal{B}_{1,2}$ — подалгебра в $\mathrm{M}_3(\mathbb{F})$, состоящая из всех матриц вида

$$C = \begin{pmatrix} c_{1,1} & c_{1,2} & c_{1,3} \\ 0 & c_{2,2} & c_{2,3} \\ 0 & c_{3,2} & c_{3,3} \end{pmatrix}.$$

Тогда $l(\mathcal{B}_{1,2}) = l(\mathcal{B}_{2,1}) = 3$.

Доказательство. 1. Из следствия 3.11 о длине блочно-треугольных матричных алгебр получаем верхние оценки

$$l(\mathcal{B}_{1,2}) \leqslant l(\mathbb{F}) + l\big(\mathrm{M}_2(\mathbb{F})\big) + 1 = 2 + 0 + 1 = 3,$$
$$l(\mathcal{B}_{2,1}) \leqslant l\big(\mathrm{M}_2(\mathbb{F})\big) + l(\mathbb{F}) + 1 = 0 + 2 + 1 = 3.$$

2. Рассмотрим множество

$$\mathcal{S}_1 = \{B_1 = E_{1,2} + E_{2,3},\ B_2 = E_{2,1}\} \subset \mathcal{B}_{2,1}.$$

Имеем

$$B_1^2 = E_{1,3}, \quad B_2^2 = 0, \quad B_1B_2 = E_{1,1}, \quad B_2B_1 = E_{2,2}, \quad B_2B_1^2 = E_{2,3}.$$

Таким образом, $\mathcal{L}_3(\mathcal{S}_1) = \mathcal{B}_{2,1}$, $\dim \mathcal{L}_2(\mathcal{S}) = 6 < \dim \mathcal{B}_{2,1}$, следовательно, $\mathcal{S}_1$ является системой порождающих для алгебры $\mathcal{B}_{2,1}$ длины $l(\mathcal{S}_1) = 3$ и $l(\mathcal{B}_{2,1}) = 3$.

3. Рассмотрим множество

$$\mathcal{S}_2 = \{C_1 = E_{1,2} + E_{2,3},\, C_2 = E_{3,2}\} \subset \mathcal{B}_{1,2}.$$

Имеем

$$C_1^2 = E_{1,3}, \quad C_2^2 = 0, \quad C_1C_2 = E_{2,2}, \quad C_2C_1 = E_{3,3}, \quad C_1^2C_2 = E_{1,2}.$$

Следовательно, $\mathcal{L}_3(\mathcal{S}_2) = \mathcal{B}_{1,2}$, $\dim \mathcal{L}_2(\mathcal{S}) = 6 < \dim \mathcal{B}_{1,2}$, $\mathcal{S}_2$ является системой порождающих для алгебры $\mathcal{B}_{1,2}$ длины $l(\mathcal{S}_1) = 3$ и $l(\mathcal{B}_{1,2}) = 3$. $\square$

Предложение 5.61. *Пусть $\mathbb{F}$ — произвольное поле. Пусть $\mathcal{A}$ — подалгебра в $\mathrm{M}_3(\mathbb{F})$ и $\dim \mathcal{A} = 7$. Тогда $l(\mathcal{A}) \leqslant 3$.*

Доказательство. Пусть $\bar{\mathbb{F}}$ — алгебраическое замыкание поля $\mathbb{F}$. Рассмотрим подалгебру $\mathcal{A}_{\bar{\mathbb{F}}} = (\mathcal{A}_{\mathbb{F}} \otimes_{\mathbb{F}} \bar{\mathbb{F}})_{\bar{\mathbb{F}}} \subseteq \mathrm{M}_3(\bar{\mathbb{F}})$. По теореме 5.56 существует невырожденная матрица $T \in \mathrm{M}_3(\bar{\mathbb{F}})$, такая что либо $T^{-1}\mathcal{A}_{\bar{\mathbb{F}}}T = B_{2,1}$, либо $T^{-1}\mathcal{A}_{\bar{\mathbb{F}}}T = B_{1,2}$. Следовательно, по лемме 5.60 $l(\mathcal{A}_{\bar{\mathbb{F}}}) = 3$. Из предложения 3.19 получаем требуемую оценку $l(\mathcal{A}) \leqslant l(\mathcal{A}_{\bar{\mathbb{F}}}) = 3$. $\square$

Лемма 5.62. *Пусть $\mathbb{F}$ — произвольное поле. Пусть $\mathcal{A}$ — $\mathbb{F}$-алгебра с единицей $1_{\mathcal{A}}$, $\dim \mathcal{A} = 5$ и $m(\mathcal{A}) \leqslant 3$. Тогда $l(\mathcal{A}) \leqslant 2$.*

Доказательство. Пусть $\mathcal{S} = \{A_1, \ldots, A_k\}$ — произвольная система порождающих алгебры $\mathcal{A}$. Покажем, что $l(\mathcal{S}) \leqslant 2$. По предложению 3.4 можно считать, что все элементы $\mathcal{S}$ линейно независимы и $\dim \mathcal{L}_1(\mathcal{S}) = |\mathcal{S}| + 1 = k + 1$. Если $\dim \mathcal{L}_1(\mathcal{S}) \leqslant 2$, то $\mathcal{S} = \{A_1\}$ и

$$\dim \mathcal{L}(\mathcal{S}) \leqslant \deg A_1 \leqslant m(\mathcal{A}) \leqslant 3 < 5 = \dim \mathcal{A},$$

т. е. $\mathcal{S}$ не является системой порождающих. Значит, $\dim \mathcal{L}_1(\mathcal{S}) \geqslant 3$. Рассмотрим случаи.

I. Если $\dim \mathcal{L}_1(\mathcal{S}) = 5 = \dim \mathcal{A}$, то $\mathcal{L}_1(\mathcal{S}) = \mathcal{A}$ и $l(\mathcal{S}) = 1$.

II. Если $\dim \mathcal{L}_1(\mathcal{S}) = 4$, то $\dim \mathcal{L}_2(\mathcal{S}) \geqslant \dim \mathcal{L}_1(\mathcal{S}) + 1 = 5 = \dim \mathcal{A}$, значит, $\mathcal{L}_2(\mathcal{S}) = \mathcal{A}$ и $l(\mathcal{S}) = 2$.

III. Пусть $\dim \mathcal{L}_1(\mathcal{S}) = 3$, $\mathcal{S} = \{A_1, A_2\}$. При этом $\dim \mathcal{L}_2(\mathcal{S}) \geqslant \dim \mathcal{L}_1(\mathcal{S}) + 1 = 4$.

1. Если $\dim \mathcal{L}_2(\mathcal{S}) = 5 = \dim \mathcal{A}$, то $\mathcal{L}_2(\mathcal{S}) = \mathcal{A}$ и $l(\mathcal{S}) = 2$.

2. Предположим, что $\dim \mathcal{L}_2(\mathcal{S}) = 4$. Приведём это утверждение к противоречию. Рассмотрим множество

$$\mathcal{S}^3 \setminus \mathcal{S}^{3-1} = \{A_1^3,\, A_2^3,\, A_1^2A_2,\, A_1A_2^2,\, A_2A_1^2,\, A_2^2A_1,\, A_1A_2A_1,\, A_2A_1A_2\}.$$

Слова A_1^3 и A_2^3 сократимы по определению $m(\mathcal{A})$.

а) Предположим, что оба слова A_1^2 и A_2^2 сократимы. Тогда все слова в $\mathcal{S}^3 \setminus \mathcal{S}^{3-1}$, содержащие квадрат, также сократимы. В этом случае найдётся такая перестановка $\pi \in \mathrm{S}_2$, что

$$\mathcal{L}_2(\mathcal{S}) = \big\langle 1_{\mathcal{A}},\, A_1,\, A_2,\, A_{\pi(1)}A_{\pi(2)} \big\rangle.$$

Поскольку $A_{\pi(2)}A_{\pi(1)} \in \mathcal{L}_2(\mathcal{S})$, то $A_{\pi(2)}A_{\pi(1)} = \alpha A_{\pi(1)}A_{\pi(2)} + U$, где $\alpha \in \mathbb{F}$, $U \in \mathcal{L}_1(\mathcal{S})$. Получаем, что

$$A_{\pi(1)}A_{\pi(2)}A_{\pi(1)} = A_{\pi(1)}(\alpha A_{\pi(1)}A_{\pi(2)} + U) = \alpha A_{\pi(1)}^2 A_{\pi(2)} + V,$$
$$A_{\pi(2)}A_{\pi(1)}A_{\pi(2)} = (\alpha A_{\pi(1)}A_{\pi(2)} + U)A_{\pi(2)} = \alpha A_{\pi(1)}A_{\pi(2)}^2 + W,$$

где $V, W \in \mathcal{L}_2(\mathcal{S})$, т. е. слова $A_1A_2A_1$ и $A_2A_1A_2$ сократимы. Таким образом, все слова в $\mathcal{S}^3 \setminus \mathcal{S}^{3-1}$ сократимы, $\mathcal{L}_3(\mathcal{S}) = \mathcal{L}_2(\mathcal{S})$, но $\mathcal{L}_2(\mathcal{S}) \neq \mathcal{A}$. Противоречие.

б) Пусть хотя бы одно из слов A_1^2 и A_2^2 несократимо. Без ограничения общности можно считать, что A_1^2 несократимо. В этом случае

$$\mathcal{L}_2(\mathcal{S}) = \langle 1_{\mathcal{A}},\, A_1,\, A_2,\, A_1^2 \rangle.$$

Поскольку $A_1A_2, A_2A_1, A_2^2 \in \mathcal{L}_2(\mathcal{S})$, то

$$A_1A_2 = \alpha_1 A_1^2 + U_1, \quad A_2A_1 = \alpha_2 A_1^2 + U_2, \quad A_2^2 = \alpha_3 A_1^2 + U_3,$$

где $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}$, $U_1, U_2, U_3 \in \mathcal{L}_1(\mathcal{S})$. Получаем, что

$$A_1^2A_2 = A_1(\alpha_1 A_1^2 + U_1) = \alpha_1 A_1^3 + V_1,$$
$$A_1A_2^2 = A_1(\alpha_3 A_1^2 + U_3) = \alpha_3 A_1^3 + V_2,$$
$$A_2A_1^2 = (\alpha_2 A_1^2 + U_2)A_1 = \alpha_2 A_1^3 + V_3,$$
$$A_2^2A_1 = (\alpha_3 A_1^2 + U_3)A_1 = \alpha_3 A_1^3 + V_4,$$
$$A_1A_2A_1 = A_1(\alpha_2 A_1^2 + U_2) = \alpha_2 A_1^3 + V_5,$$
$$A_2A_1A_2 = A_2(\alpha_1 A_1^2 + U_1) = \alpha_1 A_2A_1^2 + V_6 = \alpha_1\alpha_2 A_1^3 + \alpha_1 V_3 + V_6 = \alpha_1\alpha_2 A_1^3 + V_7,$$

где $V_1, \ldots, V_7 \in \mathcal{L}_2(\mathcal{S})$. Таким образом, все слова в $\mathcal{S}^3 \setminus \mathcal{S}^{3-1}$ сократимы, $\mathcal{L}_3(\mathcal{S}) = \mathcal{L}_2(\mathcal{S})$, но $\mathcal{L}_2(\mathcal{S}) \neq \mathcal{A}$. Противоречие. $\square$

Теорема 5.63. *Пусть $\mathbb{F}$ — произвольное поле. Тогда для произвольных подалгебр $\mathcal{A}' \subseteq \mathcal{A} \subseteq \mathrm{M}_3(\mathbb{F})$ выполнено $l(\mathcal{A}') \leqslant l(\mathcal{A}) \leqslant l\big(\mathrm{M}_3(\mathbb{F})\big) = 4$.*

Доказательство. Пусть $\mathcal{A}' \subseteq \mathcal{A} \subseteq \mathrm{M}_3(\mathbb{F})$. Согласно следствию 5.51 можно считать, что $E \in \mathcal{A}'$, поэтому

$$1 \leqslant \dim \mathcal{A}' \leqslant \dim \mathcal{A} \leqslant \dim \mathrm{M}_3(\mathbb{F}) = 9.$$

Заметим, что если $\dim \mathcal{A} \geqslant 2$, то $l(\mathcal{A}) \geqslant 1$. Рассмотрим случаи.

1. $\dim \mathcal{A} = 1$. Тогда $\mathcal{A} = \mathbb{F}E$, $l(\mathcal{A}) = 0$ и не существует $\mathcal{A}' \neq \mathcal{A}$.

2. $\dim \mathcal{A} = 2$. В этом случае $1 \leqslant l(\mathcal{A}) \leqslant \dim \mathcal{A} - 1 = 1$, т. е. $l(\mathcal{A}) = 1$, и по лемме 5.47 также получаем оценку $l(\mathcal{A}') \leqslant 1 = l(\mathcal{A})$.

3. $\dim \mathcal{A} = 3$. Если $\mathcal{A}' \subset \mathcal{A}$, то $\dim \mathcal{A}' \leqslant 2$, и по доказанному в пунктах 1 и 2 справедлива оценка $l(\mathcal{A}') \leqslant 1$. Получаем, что $l(\mathcal{A}') \leqslant 1 \leqslant l(\mathcal{A})$.

4. $\dim \mathcal{A} = 4$.

Если $l(\mathcal{A}) = 3$, то по лемме 4.34 $\mathcal{A}$ порождена одной матрицей A и $\deg A = 4$, но по теореме Гамильтона—Кэли для любой матрицы $A \in \mathrm{M}_3(\mathbb{F})$ выполнено $\deg A \leqslant 3$. Противоречие. Следовательно, $l(\mathcal{A}) \leqslant 2$.

Если $l(\mathcal{A}) = 1$, то по лемме 5.47 получаем оценку $l(\mathcal{A}') \leqslant 1 = l(\mathcal{A})$.

Пусть $l(\mathcal{A}) = 2$. Если $\mathcal{A}' \subset \mathcal{A}$, то $\dim \mathcal{A}' \leqslant 3$, следовательно, $l(\mathcal{A}') \leqslant \dim \mathcal{A}' - 1 \leqslant 2 = l(\mathcal{A})$.

5. $\dim \mathcal{A} = 5$. По лемме 5.62 $l(\mathcal{A}) \leqslant 2$.

Если $l(\mathcal{A}) = 1$, то по лемме 5.47 получаем оценку $l(\mathcal{A}') \leqslant 1 = l(\mathcal{A})$.

Пусть $l(\mathcal{A}) = 2$. Если $\mathcal{A}' \subset \mathcal{A}$, то $\dim \mathcal{A}' \leqslant 4$, и по доказанному в пунктах 1—4, $l(\mathcal{A}') \leqslant 2 = l(\mathcal{A})$.

6. $\dim \mathcal{A} = 6$. По предложению 5.59 $l(\mathcal{A}) \leqslant 2$.

Если $l(\mathcal{A}) = 1$, то по лемме 5.47 получаем оценку $l(\mathcal{A}') \leqslant 1 = l(\mathcal{A})$.

Пусть $l(\mathcal{A}) = 2$. Если $\mathcal{A}' \subset \mathcal{A}$, то $\dim \mathcal{A}' \leqslant 5$, и по доказанному в пунктах 1—5 $l(\mathcal{A}') \leqslant 2 = l(\mathcal{A})$.

7. $\dim \mathcal{A} = 7$. По предложению 5.61 $l(\mathcal{A}) \leqslant 3$.

Если $l(\mathcal{A}) = 1$, то по лемме 5.47 получаем оценку $l(\mathcal{A}') \leqslant 1 = l(\mathcal{A})$.

Пусть $l(\mathcal{A}) \geqslant 2$.

Если $\mathcal{A}' \subset \mathcal{A}$, то $\dim \mathcal{A}' \leqslant 6$, и по доказанному в пунктах 1—6 $l(\mathcal{A}') \leqslant 2 \leqslant l(\mathcal{A})$.

8. $\dim \mathcal{A} = 9 = \dim \mathrm{M}_3(\mathbb{F})$. Тогда $\mathcal{A} = \mathrm{M}_3(\mathbb{F})$ и $l(\mathcal{A}) = 4$ по лемме 5.55. Если $\mathcal{A}' \subset \mathcal{A}$, то $\dim \mathcal{A}' \leqslant 7$, и по доказанному в пунктах 1—7 $l(\mathcal{A}') \leqslant 3 < 4 = l(\mathcal{A})$. □

Следствие 5.64. *Пусть $\mathbb{F}$ — произвольное поле. Тогда функция длины строго монотонна на алгебре* $\mathrm{M}_3(\mathbb{F})$.

Автор выражает глубокую благодарность А. Э. Гутерману и А. В. Михалёву за постановку задачи, постоянное внимание к работе и всестороннюю поддержку.

Литература

[1] Альпин Ю. А., Икрамов Х. Д. Об унитарном подобии матричных семейств // Мат. заметки. — 2003. — Т. 74, № 6. — С. 815—826.

[2] Воеводин В. В., Тыртышников Е. Е. Вычислительные процессы с теплицевыми матрицами. — М.: Наука, 1987.

[3] Ламбек И. Кольца и модули. — М.: Мир, 1971.

[4] Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1. — М.: Мир, 1988.

[5] Мальцев А. И. Основы линейной алгебры. — М.: Наука, 1975.

[6] Маркова О. В. О длине алгебры верхнетреугольных матриц // Успехи мат. наук. — 2005. — Т. 60, № 3. — С. 177—178.

[7] Маркова О. В. Вычисление длин матричных подалгебр специального вида // Фундамент. и прикл. мат. — 2007. — Т. 13, вып. 4. — С. 165—197.

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

[9] Маркова О. В. Характеризация коммутативных матричных подалгебр максимальной длины над произвольным полем // Вестн. Моск. ун-та. Сер. 1. Математика, механика. — 2009. — № 5. — С. 53—55.

[10] Маркова О. В. О некоторых свойствах функции длины // Мат. заметки. — 2010. — Т. 87, № 1. — С. 83—91.

[11] Пирс Р. Ассоциативные алгебры. — М.: Мир, 1986.

[12] Супруненко Д. А., Тышкевич Р. И. Перестановочные матрицы. — М.: УРСС, 2003.

[13] Фам Вьет Хунг. Верхняя граница для размерности коммутативных нильпотентных подалгебр алгебры матриц // Изв. Акад. наук БССР. Сер. физ.-мат. наук. — 1987. — Т. 3. — С. 110—111.

[14] Хорн Р., Джонсон Ч. Матричный анализ. — М.: Мир, 1989.

[15] Al'pin Yu. A., Ikramov Kh. D. Reducibility theorems for pairs of matrices as rational criteria // Linear Algebra Appl. — 2000. — Vol. 313. — P. 155—161.

[16] Brown W. C., Call F. W. Maximal commutative subalgebras of $n \times n$ matrices // Commun. Algebra. — 1993. — Vol. 21, no. 12. — P. 4439—4460.

[17] Constantine D., Darnall M. Lengths of finite dimensional representations of PWB algebras // Linear Algebra Appl. — 2005. — Vol. 395. — P. 175—181.

[18] Courter R. C. The dimension of maximal commutative subalgebras of K_n // Duke Math. J. — 1965. — Vol. 32. — P. 225—232.

[19] Gerstenhaber M. On dominance and varieties of commuting matrices // Ann. Math. — 1961. — Vol. 73, no. 2. — P. 324—348.

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

[21] Horn R. A., Johnson C. R. Topics in Matrix Analysis. — Cambridge: Cambridge Univ. Press, 1991.

[22] Jacobson N. Schur's theorems on commutative matrices // Bull. Am. Math. Soc. — 1944. — Vol. 50. — P. 431—436.

[23] Laffey T. J. The minimal dimension of maximal commutative subalgebras of full matrix algebras // Linear Algebra Appl. — 1985. — Vol. 71. — P. 199—212.

[24] Laffey T. J. Simultaneous reduction of sets of matrices under similarity // Linear Algebra Appl. — 1986. — Vol. 84. — P. 123—138.

[25] Laffey T. J., Lazarus S. Two-generated commutative matrix subalgebras // Linear Algebra Appl. — 1991. — Vol. 147. — P. 249—273.

[26] Longstaff W. E. Burnside's theorem: irreducible pairs of transformations // Linear Algebra Appl. — 2004. — Vol. 382. — P. 247—269.

[27] Longstaff W. E., Rosenthal P. On the lengths of irreducible pairs of complex matrices // Proc. Am. Math. Soc. — 2011. — Vol. 139, no. 11. — P. 3769—3777.

[28] Markova O. V. Matrix algebras and their length // Matrix Methods: Theory, Algorithms, Applications. — World Scientific, 2010. — P. 116—139.

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

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

[31] Radjavi H., Rosenthal P. Simultaneous Triangularization. — New York: Springer, 2000.

[32] Schur I. Zur Theorie der vertauschbären Matrizen // J. Reine Angew. Math. — 1905. — B. 130. — S. 66—76.

[33] Song Y. A construction of maximal commutative subalgebra of matrix algebras // J. Korean Math. Soc. — 2003. — Vol. 40, no. 2. — P. 241—250.

[34] Spencer A. J. M., Rivlin R. S. The theory of matrix polynomials and its applications to the mechanics of isotropic continua // Arch. Ration. Mech. Anal. — 1959. — Vol. 2. — P. 309—336.

[35] Spencer A. J. M., Rivlin R. S. Further results in the theory of matrix polynomials // Arch. Ration. Mech. Anal. — 1960. — Vol. 4. — P. 214—230.

[36] Wadsworth A. The algebra generated by two commuting matrices // Linear and Multilinear Algebra. — 1990. — Vol. 27. — P. 159—162.