Записки научных
семинаров ПОМИ
Том 524, 2023 г.

**О. В. Маркова**

# КОММУТАТИВНЫЕ МАТРИЧНЫЕ АЛГЕБРЫ, ПОРОЖДЁННЫЕ ЦИКЛИЧЕСКИМИ МАТРИЦАМИ

## §1. Введение

Описание коммутативных матричных подалгебр и изучение их числовых характеристик является классической областью исследований в теории матриц. Данная работа посвящена изучению коммутативных матричных алгебр, содержащих циклические матрицы. Напомним, что матрица называется *циклической*, если её минимальный многочлен совпадает с характеристическим (известно множество других содержательных эквивалентных определений и интересных свойств циклических матриц, см., например, [11, 15]).

Обозначим через $M_n(\mathbb{F})$ алгебру квадратных $n \times n$ матриц над полем $\mathbb{F}$. Как принято в задачах, связанных с описанием семейств матриц, решение предполагается получить с точностью до подобия (напомним, что матрицы $A, B \in M_n(\mathbb{F})$ подобны, если существует обратимая матрица $C \in M_n(\mathbb{F})$ такая, что $C^{-1}AC = B$). Поэтому здесь и далее, говоря о различных матрицах и алгебрах, мы будем иметь в виду различные с точностью до подобия. Отметим, что задачу подсчёта самих циклических матриц имеет смысл рассматривать только для конечных полей, поскольку для любого бесконечного поля количество различных циклических матриц тоже заведомо всегда бесконечно за счёт бесконечности количества вариантов выбора собственных чисел. Естественным образом аналогичный вопрос возникает и для алгебр.

**Вопрос 1.1.** *Для заданных поля коэффициентов $\mathbb{F}$ и порядка матриц $n$ определить, сколько существует различных подалгебр алгебры матриц $M_n(\mathbb{F})$, порождённых циклическими матрицами. В частности, если их конечное число, то вычислить его как функцию от порядка матриц $n$.*

---

*Ключевые слова*: коммутативная матричная подалгебра, циклическая матрица, разбиения натурального числа, длина алгебры.

Исследование выполнено за счет гранта Российского научного фонда (проект No. 22-21-00267).

Данная работа посвящена исследованию вышеозначенного вопроса над различными полями. Будет показано существование бесконечных полей, для которых количество различных алгебр бесконечно для всех значений $n \geqslant 2$. В общем случае будет установлен критерий подобия матричных алгебр указанного типа в терминах изоморфизма факторалгебр алгебры многочленов. С помощью него будет показана конечность количества алгебр для всех алгебраически замкнутых полей и поля вещественных чисел. Для этих полей, а также для достаточно больших по мощности конечных полей, будет получен ответ на вторую часть вопроса 1.1. В частности, будет показано, что в случае алгебраически замкнутых полей ответ на этот вопрос в явном виде получается благодаря использованию матричных методов, а именно жордановой нормальной формы матриц. Как следствие, будет предложен канонический вид исследуемых алгебр. Для поля вещественных чисел и конечных полей задача о количестве алгебр будет решена с привлечением методов теории многочленов и целочисленных последовательностей.

Ранее многократно подтверждалось, что наличие циклических матриц в системах порождающих матричных подалгебр является сильным условием, которое позволяет решить те или иные задачи, связанные с системами порождающих и алгебрами, см., например, работы [4–7, 12–14, 17, 21] и их библиографию. Так, например, в статье А. Гутермана, Т. Лаффи, О. Марковой и Х. Шмигоц [12] в случае, когда система содержит циклическую матрицу, доказана справедливость гипотезы А. Паза 1984 года [22] об оценке длины порождающей системы алгебры матриц порядка $n$ числом $2n-2$. При этом в общем случае эта гипотеза до сих пор является открытой. В работе [7] Д. Новочадовым установлено, что в точности для этого класса систем порождающих задачу о совпадении алгебры, порождённой данным множеством, с полной матричной алгеброй можно решить в терминах графа Бернсайда. В работе [6] для указанных систем порождающих матричной алгебры решены некоторые алгоритмические задачи теории матриц. В этом контексте коммутативные алгебры, порождённые циклическими матрицами, являются алгебрами максимальной длины в классе всех коммутативных матричных алгебр [4, 13]. Поэтому как следствие результатов данной работы удаётся установить количество коммутативных алгебр максимальной длины.

Работа построена следующим образом. В §2 вводится система обозначений, там же представлены некоторые вспомогательные результаты относительно матричных подалгебр, порождённых циклическими матрицами. В §3 показано, что, в случае алгебраически замкнутых полей, для произвольного $n$ количество различных с точностью до подобия коммутативных подалгебр алгебры $M_n(\mathbb{F})$, порождённых циклическими матрицами, конечно и совпадает с числом разбиений числа $n$. Более того, получено описание рассматриваемых алгебр. В §4 приведён критерий подобия матричных алгебр, порождённых циклическими матрицами, формулируемый в терминах изоморфизма факторалгебр алгебры многочленов. С помощью него показано существование бесконечных полей, для которых количество различных алгебр бесконечно для всех значений порядка матриц. Также найдено количество алгебр, порождённых циклическими матрицами, над полем вещественных чисел и над достаточно большими по мощности конечными полями, для чего используются известные целочисленные последовательности.

## §2. Общие свойства алгебр, порождённых циклическими матрицами

Понятия из теории колец и алгебр, использованные в статье, можно найти, например, в [8]. Все рассматриваемые в работе алгебры – **ассоциативные конечномерные алгебры с единицей над полями**. Для конечного множества $\mathcal{S}$ алгебры $\mathcal{A}$ через $\mathcal{L}(\mathcal{S})$ будем обозначать подалгебру с единицей в алгебре $\mathcal{A}$, порожденную множеством $\mathcal{S}$. В том случае, когда $\mathcal{S} = \{A\}$, для $\mathcal{L}(\{A\})$ будем использовать более простое обозначение $\mathcal{L}(A)$.

Пусть далее $M_n(\mathbb{F})$ обозначает алгебру матриц порядка $n$ над полем $\mathbb{F}$, $T_n(\mathbb{F})$ – подалгебру верхнетреугольных матриц в $M_n(\mathbb{F})$. Через $E_{i,j}$ будем обозначать матричную единицу, т.е. матрицу с 1 на позиции $(i, j)$ и нулями на остальных местах. Единичную матрицу в $M_n(\mathbb{F})$ обозначим символом $E_n$ или просто $E$, если размер ясен из контекста.

Пусть $C \in M_n(\mathbb{F})$ – циклическая матрица. Напомним эквивалентные определения цикличности матрицы, которые будут использованы в статье. В случае, когда поле $\mathbb{F}$ алгебраически замкнуто, цикличность матрицы равносильна тому, что каждое собственное число имеет геометрическую кратность 1, т.е. каждому собственному числу в жордановой нормальной форме соответствует ровно одна жорданова клетка.

Другое условие сформулируем через сопровождающие матрицы.

**Определение 2.1.** *Пусть* $\mathbb{F}$ *– произвольное поле,* $n \in \mathbb{N}$ *и* $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{F}[x]$ *(многочлен со старшим коэффициентом* 1 *будем называть* унитарным). Сопровождающей матрицей многочлена $f(x)$ *называется матрица*

$$C(f) = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \dots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix} \in M_n(\mathbb{F}).$$

**Теорема 2.2** ( [15, теорема 3.3.15]). *Пусть* $\mathbb{F}$ *– произвольное поле,* $n \in \mathbb{N}$ *и* $A \in M_n(\mathbb{F})$. *Матрица* $A$ *является циклической тогда и только тогда, когда она подобна сопровождающей матрице своего характеристического многочлена.*

**Следствие 2.3.** *Пусть* $\mathbb{F}$ *– произвольное поле,* $n \in \mathbb{N}$. *Циклические матрицы* $A, B \in M_n(\mathbb{F})$ *с одинаковыми характеристическими многочленами подобны.*

**Теорема 2.4** (**Теорема Герштенхабера** [23, теорема 1]). *Пусть* $\mathbb{F}$ *– произвольное поле, матрицы* $A$, $B \in M_n(\mathbb{F})$ *таковы, что* $AB = BA$. *Пусть* $\mathcal{L}(A, B)$ *– подалгебра* $M_n(\mathbb{F})$, *порождённая матрицами* $A$ *и* $B$. *Тогда* $\dim_{\mathbb{F}} \mathcal{L}(A, B) \leqslant n$.

Как следствие получаем следующий результат.

**Лемма 2.5** ( [13, лемма 6.3]). *Пусть* $\mathbb{F}$ *– произвольное поле и* $\mathcal{A}$ *– коммутативная подалгебра в* $M_n(\mathbb{F})$. *Если существует циклическая матрица* $A \in \mathcal{A}$, *то* $\mathcal{A}$ *является подалгеброй, порождённой матрицей* $A$.

Таким образом, если коммутативная матричная подалгебра может быть порождена циклической матрицей, то любая содержащаяся в ней циклическая матрица будет образующим элементом.

**Лемма 2.6** ([5, лемма 4.21]). *Пусть* $\mathbb{F}$ *– произвольное поле и* $C \in M_n(\mathbb{F})$ *– циклическая матрица. Тогда матрица* $C + \alpha E$ *является циклической для любого* $\alpha \in \mathbb{F}$.

**Следствие 2.7.** *Пусть поле* $\mathbb{F}$ *бесконечно, и* $\mathcal{A}$ *– коммутативная подалгебра в* $M_n(\mathbb{F})$, *порождённая циклической матрицей. Тогда в алгебре* $\mathcal{A}$ *содержится бесконечно много различных порождающих её циклических матриц.*

**Определение 2.8.** Длиной конечной системы $\mathcal{S}$ порождающих *конечномерной ассоциативной алгебры $\mathcal{A}$ над произвольным полем называется наименьшее натуральное число $l(\mathcal{S})$, такое что слова длины не большей $l(\mathcal{S})$ порождают данную алгебру как векторное пространство.* Длиной алгебры *называется наибольшая из длин её систем порождающих, обозначим её через $l(\mathcal{A})$.*

Длина является важной числовой характеристикой алгебры, трудность вычисления которой даже для классических алгебр обусловлена необходимостью рассмотрения всех систем образующих в данной алгебре.

Исследование длины коммутативных подалгебр алгебры матриц также восходит к работе А. Паза [22], в которой было установлено, что длина любой коммутативной подалгебры алгебры матриц порядка $n$ над полем комплексных чисел $\mathbb{C}$ не превосходит $n-1$. Поэтому для комплексных коммутативных подалгебр была получена линейная относительно порядка матриц верхняя оценка длины. В работе [13] (совместно с А. Э. Гутерманом) показано, что эта оценка справедлива в случае произвольного поля и является точной.

**Теорема 2.9** ([13, теорема 6.1])**.** *Пусть $\mathbb{F}$ – произвольное поле и $\mathcal{A}$ – коммутативная подалгебра в $M_n(\mathbb{F})$. Тогда $l(\mathcal{A}) \leqslant n-1$.*

Связь этой характеристики с циклическими матрицами установлена в следующей теореме.

**Теорема 2.10** ([4, теорема 3])**.** *Пусть $\mathbb{F}$ – произвольное поле. Коммутативная подалгебра $\mathcal{A}$ в $M_n(\mathbb{F})$ имеет максимально возможную длину $n-1$ тогда и только тогда, когда она порождена циклической матрицей.*

## §3. Алгебры, порождённые циклическими матрицами, в случае алгебраически замкнутых полей

В этом параграфе показано, что, в случае алгебраически замкнутых полей, для произвольного $n$ количество различных с точностью до подобия коммутативных подалгебр алгебры $M_n(\mathbb{F})$, порождённых циклическими матрицами, конечно и совпадает с числом разбиений $n$. Более того, удаётся дать описание вышеозначенных алгебр.

Напомним необходимые сведения из теории чисел.

**Определение 3.1.** Разбиение *натурального числа $n$ – это представление $n$ в виде суммы положительных целых чисел, называемых частями, так что порядок следования частей не учитывается,* (*т.е. разбиения, отличающиеся только порядком частей, считаются равными*). *В канонической записи разбиения части перечисляются в невозрастающем порядке.*

*Число разбиений* $P(n)$ натурального числа $n$ является одним из фундаментальных объектов изучения в теории чисел. Нахождение его выражения в виде функции от $n$ остаётся открытой проблемой. Асимптотическое равенство для числа разбиений найдено Г. Х. Харди и С. Рамануджаном (см., например, [9, глава 5] и последовательность A000041 в энциклопедии целочисленных последовательностей OEIS [20]): при $n \to \infty$

$$P(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}.$$

**Обозначение 3.2.** Рассмотрим циклическую матрицу $C \in M_n(\mathbb{F})$. В жордановой нормальной форме матрицы $C$ каждому собственному значению $\gamma_j$ соответствует единственная жорданова клетка размера $n_j$, причем $\sum\limits_j n_j = n$. Известно, что жорданова нормальная форма матрицы единственна с точностью до порядка клеток. Таким образом, жордановой нормальной форме матрицы $C$ можно сопоставить разбиение числа $n$. Обозначим его символом $p_J(C)$.

**Лемма 3.3.** *Пусть $\mathbb{F}$ – алгебраически замкнутое поле и $n \in \mathbb{N}$, $n \geqslant 2$. Рассмотрим коммутативную подалгебру $\mathcal{A} \subset M_n(\mathbb{F})$, порождённую циклической матрицей $A$. Если $C \in \mathcal{A}$ – циклическая матрица, то $p_J(C) = p_J(A)$.*

**Доказательство.** Из условия $C \in \mathcal{A}$ следует, что существует многочлен $Q(x) \in \mathbb{F}[x]$ степени $\deg Q \leqslant n-1$ такой, что $C = Q(A)$.

Пусть $\gamma_1, \ldots, \gamma_k$ – все различные собственные значения матрицы $A$ кратностей $s_1, \ldots, s_k$ соответственно.

Тогда, согласно [2, глава VI, §7, теорема 9], собственными значениями матрицы $Q(A)$ будут числа $Q(\gamma_1), \ldots, Q(\gamma_k)$, причём $Q(\gamma_i)$ может соответствовать одна жорданова клетка размера $s_i$, либо несколько клеток, сумма размеров которых также равна $s_i$.

Поскольку матрица $C = Q(A)$ по условию циклическая, то каждому её собственному значению соответствует ровно одна жорданова клетка, значит, все числа $Q(\gamma_1), \ldots, Q(\gamma_k)$ попарно различны, им соответствуют клетки размеров $s_1, \ldots, s_k$.

Таким образом, $p_J(C) = p_J(Q(A)) = p_J(A)$. □

**Обозначение 3.4.** Пусть $\mathbb{F}$ – алгебраически замкнутое поле и $n \in \mathbb{N}$, $n \geqslant 2$. Рассмотрим коммутативную подалгебру $\mathcal{A} \subset M_n(\mathbb{F})$, порождённую циклической матрицей. Тогда через $p_J(\mathcal{A})$ обозначим разбиение, соответствующее произвольной циклической матрице в алгебре $\mathcal{A}$.

Обозначим через $J_k = \sum\limits_{i=1}^{k-1} E_{i,i+1} \in T_k(\mathbb{F})$ жорданову клетку размера $k$ с собственным числом 0 и возьмём порождённую ею алгебру $\mathcal{N}_k$. Она совпадает с линейной оболочкой $\langle E_k,\ J_k^i | i = 1, \ldots, k-1\rangle \subset T_k(\mathbb{F})$.

**Обозначение 3.5.** Пусть дано разбиение $\mathbf{p} = (n_1, \ldots, n_m)$ числа $n$, где $n \geqslant n_1 \geqslant \ldots \geqslant n_m \geqslant 0$, $1 \leqslant m \leqslant n$, $\sum_{i=1}^m n_i = n$. Сопоставим ему алгебру $\mathcal{T}_{\mathbf{p}} = \bigoplus\limits_{j=1}^{m} \mathcal{N}_{n_j} \subset T_n(\mathbb{F})$, где прямая сумма понимается как алгебра блочно-диагональных матриц.

**Теорема 3.6.** *Пусть $\mathbb{F}$ – алгебраически замкнутое поле, $n \in \mathbb{N}$, $n \geqslant 2$. Рассмотрим коммутативные подалгебры $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{F})$, порождённые циклическими матрицами. Тогда*

(1) *подалгебры $\mathcal{A}$ и $\mathcal{B}$ подобны в $M_n(\mathbb{F})$ тогда и только тогда, когда $p_J(\mathcal{A}) = p_J(\mathcal{B})$;*
(2) *в $M_n(\mathbb{F})$ содержится ровно $P(n)$ различных с точностью до подобия подалгебр, порождённых циклическими матрицами;*
(3) *подалгебра $\mathcal{A}$ подобна верхнетреугольной подалгебре $\mathcal{T}_{p_J(\mathcal{A})}$.*

**Доказательство.** Утверждение (2), очевидно, следует из утверждения (1). Докажем (1). *Необходимость.* Пусть $A \in \mathcal{A}$, $B \in \mathcal{B}$ – циклические матрицы. Допустим, найдётся невырожденная матрица $T \in M_n(\mathbb{F})$ такая, что $\mathcal{B} = T\mathcal{A}T^{-1}$. Тогда, по лемме 2.5, алгебра $\mathcal{B}$ порождена циклической матрицей $B_T = TAT^{-1}$. Существует многочлен $Q(x) \in \mathbb{F}[x]$ степени $\deg Q \leqslant n-1$ такой, что $B = Q(B_T)$.

Применяя лемму 3.3, в итоге получаем:

$$p_J(\mathcal{A}) = p_J(A) = p_J(TAT^{-1}) = p_J(\mathcal{B}).$$

*Достаточность.* Пусть $p_J(A) = p_J(B) = (n_1, \dots, n_m)$, где $n \geqslant n_1 \geqslant \dots \geqslant n_m \geqslant 0$, $1 \leqslant m \leqslant n$, $\sum_{i=1}^m n_i = n$.

Тогда существуют такие невырожденные матрицы $U, V \in M_n(\mathbb{F})$, что матрицы $U^{-1}AU$ и $V^{-1}BV$ жордановы, причём размеры их клеток упорядочены по убыванию. Из того, что каждой жордановой клетке соответствует своё собственное число, получаем

$$\mathcal{A} = U(\bigoplus_{i=1}^{m} \mathcal{N}_{n_i})U^{-1}, \quad \mathcal{B} = V(\bigoplus_{i=1}^{m} \mathcal{N}_{n_i})V^{-1},$$

откуда

$$\mathcal{B} = VU^{-1}\mathcal{A}(VU^{-1})^{-1}.$$

Из последних равенств сразу получается и утверждение (3). □

## §4. Количество алгебр, порождённых циклическими матрицами, над другими полями

Поскольку любую конечномерную однопорождённую алгебру естественно рассматривать как факторалгебру алгебры многочленов по некоторому главному идеалу, вопрос подобия алгебр, порождённых циклическими матрицами, можно также свести к вопросу о взаимосвязи многочленов, порождающих соответствующие идеалы.

Сначала докажем общий критерий подобия матричных алгебр указанного типа в терминах изоморфизма факторалгебр алгебры многочленов.

**Теорема 4.1.** *Пусть $\mathbb{F}$ – призвольное поле, $n \in \mathbb{N}$. Рассмотрим циклические матрицы $A, B \in M_n(\mathbb{F})$ и порождённые ими подалгебры $\mathcal{A} = \mathcal{L}(A)$, $\mathcal{B} = \mathcal{L}(B)$. Пусть $\mu_A(x), \mu_B(x) \in \mathbb{F}[x]$ – минимальные многочлены матриц $A, B$ и пусть $\mathfrak{A} = \mathbb{F}[x]/(\mu_A(x))$, $\mathfrak{B} = \mathbb{F}[x]/(\mu_B(x))$. Тогда подалгебры $\mathcal{A}$ и $\mathcal{B}$ сопряжены в $M_n(\mathbb{F})$ тогда и только тогда, когда алгебры $\mathfrak{A}$ и $\mathfrak{B}$ изоморфны.*

**Доказательство.** В одну сторону утверждение очевидно, так как подобные алгебры изоморфны.

Пусть $\mathfrak{A} \cong \mathfrak{B}$. Тогда в алгебре $\mathfrak{A}$ найдётся элемент $a$ с минимальным многочленом равным $\mu_B(x)$. Соответственно, в изоморфной ей алгебре $\mathcal{A}$ найдётся матрица $M$ с минимальным многочленом равным $\mu_B(x)$. В частности, $M$ будет циклической. Из условия $M \in \mathcal{A}$ следует, что $M = f(A)$ для некоторого многочлена $f(x) \in \mathbb{F}[x]$ степени не выше

$n-1$. По лемме 2.5 получаем, что $\mathcal{A} = \mathcal{L}(M)$. Из следствия 2.3 заключаем, что матрицы $M$ и $B$ подобны над $\mathbb{F}$, откуда сразу получаем, что порождённые ими алгебры тоже подобны. $\square$

**Замечание 4.2.** Заметим, что, в силу китайской теоремы об остатках и основной структурной теоремы для модулей над кольцами главных идеалов [1, глава 9, §3, теорема 5], вопрос об изоморфизме факторалгебр $\mathfrak{A}$ и $\mathfrak{B}$ сводится к случаю неприводимых многочленов. С одной стороны, здесь очевидно, что алгебры, построенные по различным неприводимым многочленам, часто оказываются изоморфными. Это видно даже на примере неприводимых многочленов первой степени, $\mathbb{F}[x]/(x-a) \cong \mathbb{F}$ для любого элемента $a \in \mathbb{F}$. Однако, насколько известно автору, в общем случае вопрос описания многочленов, приводящих к изоморфным факторалгебрам, является открытым вопросом теорий колец и полей.

Поэтому в данной работе мы применим критерий из теоремы 4.1 к некоторым полям, для которых ответ на вопрос об изоморфизме факторалгебр известен, – к полям рациональных и действительных чисел и к конечным полям.

Сперва с помощью данного критерия покажем, что существуют поля, для которых количество различных алгебр, порождённых циклическими матрицами, бесконечно для всех значений $n \geqslant 2$.

**Теорема 4.3.** *Для любого $n \geqslant 2$ в алгебре $M_n(\mathbb{Q})$ матриц над полем рациональных чисел найдётся бесконечно много различных алгебр, порождённых циклическими матрицами.*

**Доказательство.** Докажем сначала утверждение теоремы при $n = 2$.

Для каждого простого $p$ возьмём многочлен $f_p(x) = x^2 - p$. Он является неприводимым унитарным многочленом, поэтому каждая из факторалгебр $\mathcal{A}_p = \mathbb{Q}[x]/(f_p(x))$ является двумерным расширением поля $\mathbb{Q}$. Для различных простых чисел $p$ и $q$ алгебры $\mathcal{A}_p$ и $\mathcal{A}_q$, очевидно, неизоморфны, поскольку $\sqrt{p}$ и $\sqrt{q}$ линейно независимы над $\mathbb{Q}$. Следовательно, по теореме 4.1, все алгебры, порождённые циклическими сопровождающими матрицами $C(f_p)$, будут различны с точностью до подобия.

Для всех $n \geqslant 3$ каждый из многочленов $f_p(x)$ можно домножить на произведение $(x-1)\ (x-2)\cdots\ (x-(n-2))$ различных линейных множителей. $\square$

Теперь перейдём к действительным алгебрам.

**Теорема 4.4.** *В алгебре $M_n(\mathbb{R})$ матриц над полем действительных чисел содержится $P_2(n) = P(n) + \sum_{j=1}^{[\frac{n}{2}]} P(j)P(n-2j)$ различных с точностью до подобия подалгебр, порождённых циклическими матрицами.*

**Доказательство.** Над полем действительных чисел неприводимые многочлены исчерпываются многочленами первой степени и квадратичными многочленами с отрицательным дискриминантом. При этом для любого унитарного неприводимого многочлена $p_1(x)$ первой степени имеем $\mathbb{R}[x]/(p_1(x)) \cong \mathbb{R}$, а для унитарного неприводимого многочлена $p_2(x)$ второй степени имеем $\mathbb{R}[x]/(p_2(x)) \cong \mathbb{C}$. Тогда для фиксированного $n$ и произвольного унитарного многочлена $f(x) \in \mathbb{R}[x]$ степени $n$ факторалгебра $\mathfrak{A} = \mathbb{R}[x]/(f(x))$ определяется количествами и наборами кратностей неприводимых множителей степеней 1 и 2: если $f(x) = (x^2 + b_1x + c_1)^{k_1} \cdots (x^2 + b_rx + c_r)^{k_r}(x - a_1)^{m_1} \cdots (x - a_s)^{m_s}$ – каноническое разложение многочлена на неприводимые множители, то алгебра $\mathfrak{A}$ определяется набором $\mathbf{p}_2 = (k_1, \ldots, k_r | m_1, \ldots, m_s)$ и не зависит от чисел $a_j, b_j, c_j$. Набору $\mathbf{p}_2$ соответствует разбиение числа $n$ вида $(2k_1, \ldots, 2k_r, m_1, \ldots, m_s)$, поэтому количество таких наборов $P_2(n)$ можно найти через обычное число разбиений:

$$P_2(n) = P(n) + \sum_{j=1}^{[\frac{n}{2}]} P(j)P(n-2j). \qquad \square$$

**Замечание 4.5.** Известны и другие свойства числовой последовательности $P_2(n)$, она же последовательность A002513 в энциклопедии целочисленных последовательностей [20]. Например, её асимптотика определена в работе [16]: при $n \to \infty$

$$P_2(n) \sim \frac{e^{\pi\sqrt{n}}}{8n^{\frac{5}{4}}} \cdot \left(1 - \frac{\frac{\pi}{16} + \frac{15}{8\pi}}{\sqrt{n}}\right).$$

Далее перейдём к случаю больших конечных полей. Сначала определим необходимую числовую последовательность (A006171 в энциклопедии целочисленных последовательностей [20]).

**Обозначение 4.6.** Для $n \in \mathbb{N}$ через $P_g(n)$ обозначим количество возможных способов разложения многочлена степени $n$ на неприводимые множители над кольцом целых чисел, т.е. в предположении, что степени сомножителей могут принимать все значения от 1 до $n$, а для любой степени количество неприводимых многочленов неограничено. Это число также совпадает с числом таких разбиений числа $n$ на составные части, в которых имеется неограниченное количество различимых, но немаркированных составных частей каждого размера. Например, разбивая $n = 2$ на две части размера 1, мы различаем, используется ли для каждой части одна и та же составная часть, или две разные.

Асимптотика последовательности $P_g(n)$ определена в работе [10]: при $n \to \infty$

$$\log(P_g(n)) \sim \pi \cdot \sqrt{\frac{n \cdot \log n}{3}}.$$

**Теорема 4.7.** *Пусть $n \in \mathbb{N}$, $q \geqslant n$ – степень простого числа. В алгебре $M_n(\mathbb{F}_q)$ матриц над конечным полем из $q$ элементов содержится $P_g(n)$ различных с точностью до подобия подалгебр, порождённых циклическими матрицами.*

**Доказательство.** Для произвольного унитарного неприводимого многочлена $g(x) \in \mathbb{F}_q[x]$ степени $m$ верно, что $\mathbb{F}_q[x]/(g(x)) \cong \mathbb{F}_{q^m}$ (см. [3, глава 1, теорема 1.86; глава 2, теоремы 2.5 и 2.10]). Поэтому для фиксированного значения $n$ и произвольного унитарного многочлена $f(x) \in \mathbb{F}_q[x]$ степени $n$ факторалгебра $\mathfrak{A} = \mathbb{F}_q[x]/(f(x))$ определяется количествами и наборами кратностей неприводимых множителей степеней от 1-ой до $n$-ой и не зависит от выбора самих неприводимых множителей: если $f(x) = p_{1,n}(x)^{k_{1,n}} \cdots p_{1,1}(x)^{k_{l_1,1}}$ – каноническое разложение многочлена на неприводимые множители, где множитель вида $p_{i,j}(x)$ имеет степень $j$, то алгебра $\mathfrak{A}$ определяется набором $\mathbf{p}_g = (k_{1,n}, \ldots, k_{l_n,n}| \ldots |k_{1,1}, \ldots, k_{l_1,1})$ и не зависит от коэффициентов многочленов $p_{i,j}(x)$.

Теперь посчитаем количество способов разложить многочлен на неприводимые множители. Для количества $N_q(m)$ унитарных неприводимых многочленов степени $m$ над полем $\mathbb{F}_q$ справедлива следующая оценка (см. [3, глава 3, замечание после примера 3.26]):

$$N_q(m) \geqslant \frac{1}{m}\left(q^m - \frac{q^m - q}{q-1}\right) \geqslant \frac{1}{m}\left(q^m - \frac{q^m - q}{1}\right) = \frac{q}{m} \geqslant \frac{n}{m}.$$

Следовательно, любое из $P_g(n)$ возможных разложений на множители реализуется для многочлена степени $n$ над $\mathbb{F}_q$ при $q \geqslant n$. $\square$

**Замечание 4.8.** Отметим, что первая часть доказательства предыдущей теоремы справедлива для любого конечного поля, в то время как количество способов разложения на множители для малых конечных полей будет меньше. Например, уже разложений на линейные множители будет меньше, чем $P(n)$, поскольку над малым полем есть всего $q < n$ унитарных линейных многочленов.

Объединяя результаты о количестве алгебр с теоремой 2.10, получаем следующее утверждение.

**Следствие 4.9.** *Теоремы* 3.6, 4.3, 4.4 и 4.7 *справедливы, если их условия сформулировать для количества различных коммутативных подалгебр максимальной длины в матричной алгебре.*

Автор выражает благодарность Н. А. Колегову и Д. Ю. Новочадову за полезные обсуждения.

## Список литературы

1. Э. Б. Винберг, *Курс алгебры.* 3-е изд., Факториал Пресс, М., 2002.
2. Ф. Р. Гантмахер, *Теория Матриц.* 4-е изд., Наука, М., 1988.
3. Р. Лидл, Г. Нидеррайтер, *Конечные поля.* В 2-х томах, Мир, М., 1988.
4. О. В. Маркова, *Характеризация коммутативных матричных подалгебр максимальной длины над произвольным полем.* — Вестн. Моск. ун-та. Сер.1. Математика. Механика **5** (2009), 53–55.
5. О. В. Маркова, *Функция длины и матричные алгебры.* — Фундам. прикл. матем. **17**, No. 6 (2012), 65–173.
6. О. В. Маркова, *Функция длины и одновременная триангулизуемость пар матриц.* — Зап. научн. семин. ПОМИ **514** (2022), 126–137.
7. О. В. Маркова, Д. Ю. Новочадов, *Системы порождающих полной матричной алгебры, содержащие циклические матрицы.* — Зап. научн. семин. ПОМИ **504** (2021), 157–171.
8. Р. Пирс, *Ассоциативные алгебры.* Мир, М., 1986.
9. Г. Эндрюс, *Теория разбиений.* Наука, М., 1982.
10. N. A. Brigham, *A general asymptotic formula for partition functions.* — Proc. Amer. Math. Soc. **1** (1950), 182–191.
11. G. Dolinar, A. Guterman, B. Kuzma, P. Oblak, *Extremal matrix centralizers.* — Linear Algebra Appl. **438**, No. 7 (2013), 2904–2910.
12. A. E. Guterman, T. Laffey, O. V. Markova, H. Šmigoc, *A resolution of Paz's conjecture in the presence of a nonderogatory matrix.* — Linear Algebra Appl. **543** (2018), 234–250.
13. A. E. Guterman, O. V. Markova, *Commutative matrix subalgebras and length function.* — Linear Algebra Appl. **430** (2009), 1790–1805.
14. A. E. Guterman, O. V. Markova, V. Mehrmann, *Lengths of quasi-commutative pairs of matrices.* — Linear Algebra Appl. **498** (2016), 450–470.

15. R. Horn, C. Johnson, *Matrix Analysis.* 2nd edition, Cambridge University Press, 2013.
16. V. Kotesovec, *Asymptotics of Sequence A002513.* 2019,
17. W. E. Longstaff, *Burnside's theorem: irreducible pairs of transformations.* — Linear Algebra Appl. **382** (2004), 247–269.
18. W. E. Longstaff, *On minimal sets of* $(0,1)$*-matrices whose pairwise products form a basis for* $M_n(\mathbb{F})$. — Bull. Austral. Math. Soc. **98**, No. 3 (2018), 402–413.
19. W. E. Longstaff, *Irreducible families of complex matrices containing a rank-one matrix.* — Bull. Austral. Math. Soc. **102**, No. 2 (2020), 226–236.
20. *On-Line Encyclopedia of Integer Sequences (OEIS).*
21. C. J. Pappacena, *An upper bound for the length of a finite-dimensional algebra.* — J. Algebra **197** (1997), 535–545.
22. A. Paz, *An application of the Cayley–Hamilton theorem to matrix polynomials in several variables.* — Linear Multilinear Algebra **15** (1984), 161–170.
23. A. Wadsworth, *The algebra generated by two commuting matrices.* — Linear Multilinear Algebra **27** (1990), 159–162.

Markova O. V. Commutative matrix subalgebras generated by nonderogatory matrices.

The paper is devoted to studying the question on the number of subalgebras in the matrix algebra that generated by nonderogatory matrices and are distinct up to similarity. A criterion for similarity of matrix algebras of the type indicated is established in terms of isomorphisms of quotient algebras of the algebra of polynomials. The existence of infinite fields for which the number of distinct algebras is infinite for all values of the matrix order is established. For algebraically closed fields, for the field of real numbers, and for finite fields of sufficiently large cardinality, the number of distinct algebras generated by nonderogatory matrices is determined as a function of the matrix order.

Московский государственный
университет имени М. В. Ломоносова,
119991, Москва;
Петербургский государственный
университет путей сообщения
императора Александра I,
С.-Петербург, Россия
*E-mail*: ov_markova@mail.ru

Поступило 3 октября 2023 г.