МАТЕМАТИКА И ТЕОРЕТИЧЕСКИЕ КОМПЬЮТЕРНЫЕ НАУКИ

Издается с 2023 года
Выходит 4 раза в год
ISSN 2949-3919

Том 4
Выпуск 2

Казань
2026

МАТЕМАТИКА И ТЕОРЕТИЧЕСКИЕ КОМПЬЮТЕРНЫЕ НАУКИ

Издается с 2023 года
Выходит 4 раза в год
ISSN 2949-3919

Том 4
Выпуск 2

Казань
2026

Учредитель: ФГАОУ ВО КПФУ
Адрес редакции: 420008, Республика Татарстан, г. Казань, Казанский федеральный университет, Институт математики и механики, ул. Кремлевская, д. 35, комн. 501.
Тел. +7 843 233-70-60
E-mail: mathematics.tcs@gmail.com
URL: https://mathtcs.ru/

Издается с 2023 года.
Выходит 4 раза в год.
ISSN 2949-3919
Регистрационный номер СМИ: Эл № ФС77-84704

Сетевое издание «Математика и теоретические компьютерные науки» основано в 2023 году Научно-образовательным математическим центром Приволжского федерального округа (НОМЦ ПФО). Его учредителем является ФГАОУ ВО «Казанский (Приволжский) федеральный университет». Издание ориентировано на публикацию научных статей по следующим направлениям фундаментальной и прикладной математики, теоретической информатики и компьютерных наук:

- вещественный, комплексный и функциональный анализ;
- дифференциальные уравнения, динамические системы и оптимальное управление;
- математическая физика;
- геометрия и топология;
- теория вероятностей и математическая статистика;
- математическая логика, алгебра и теория чисел;
- вычислительная математика;
- теория вычислимости и сложности вычислений;
- дискретная математика и математическая кибернетика;
- теоретическая информатика;
- математические методы в искусственном интеллекте.

Также принимаются к печати обзоры, научно-популярные статьи, статьи о математической жизни. Все статьи проходят процедуру рецензирования. Все опубликованные статьи находятся в открытом доступе. Языки журнала – русский и английский.

СОДЕРЖАНИЕ

МАТЕМАТИЧЕСКАЯ ЖИЗНЬ

Том 4, Выпуск 2
Стр. 4–75 (2026)

УДК 512.55
MSC 18G05

Квадратичный закон взаимности и его обобщения

А.Н. Абызов, П.Н. Буутай

Аннотация. Статья носит обзорно-методический характер и посвящена развитию идей Е.И. Золотарёва, заложенных в его подходе к доказательству квадратичного закона взаимности (1872 г.). Мы рассматриваем расширения подхода Золотарёва на абстрактные числовые кольца, приведенные в работе А. Бруньята и П.Л. Кларка (2015 г.), и на конечные группы, изученные в статье У. Дьюка и К. Хопкинс (2005 г.). Также обсуждаются связи этих исследований с некоторыми классическими результатами и различными подходами к доказательству квадратичного закона взаимности.

Ключевые слова: квадратичный закон взаимности, групповой символ, таблица характеров, определитель Вандермонда, результант.

DOI: 10.26907/2949-3919.2026.2.4-75

Введение

Вопросы из теории чисел, связанные с квадратичным законом взаимности, впервые встречаются в труде Диофанта Александрийского “Арифметика”, где рассматриваются задачи о представимости натуральных чисел в виде суммы двух квадратов. На основе анализа текста “Арифметики” авторы важной монографии [1] делают следующий вывод: “Диофант умел доказывать, что целое число N, не делящееся ни на какой квадрат и имеющее простой делитель вида $4n-1$, не может быть представлено формой a^2+b^2. Диофант открыл, но, по-видимому, не умел доказывать, что всякое простое число p вида $4n+1$ представимо формой a^2+b^2”. Заметим, что первое из приведенных утверждений о числах вида $4n-1$ несложно доказывается с помощью пифагорейской теории четных и нечетных чисел, изложенной в IX книге “Начал” Евклида (предложения 21–34), о которой Диофант хорошо знал.

Пьер Ферма был первым математиком, который систематически изучал вопросы, связанные с квадратичным законом взаимности. Интерес к этим проблемам у него возник при чтении “Арифметики” Диофанта. Ферма изучал вопросы о виде целых чисел, представимых формами: $x^2+y^2, x^2+2y^2, x^2+3y^2, x^2+xy+y^2$. Им без доказательства

Благодарности. Работа А.Н. Абызова выполнена в рамках реализации программы развития Научно-образовательного математического центра Приволжского федерального округа (соглашение № 075-02-2026-1328/1).

Поступила: 09.06.2026. Принята: 30.06.2026. Опубликована: 07.07.2026.

в переписке или в пометках, сделанных на полях, принадлежащему Ферма экземпляра Диофанта, были сформулированы следующие утверждения, лежащие в основе последующих исследований по законам взаимности:

a) Если $p = 4n + 1$ – простое число, то уравнение $p = x^2 + y^2$ имеет решение в натуральных числах. Ни одно простое число вида $p = 4n + 3$ не представимо суммой двух квадратов.

b) Если $p = 8n + 1$ или $p = 8n + 3$ – простое число, то уравнение $p = x^2 + 2y^2$ имеет решение в натуральных числах. Ни одно простое число вида $8n + 5$ или $8n + 7$ не представимо в виде $x^2 + 2y^2$.

c) Если $p = 8n + 1$ или $p = 8n + 7$ – простое число, то уравнение $p = x^2 - 2y^2$ имеет решение в натуральных числах. Ни одно простое число вида $8n + 3$ или $8n + 5$ не представимо в виде $x^2 - 2y^2$.

d) Если $p = 3n + 1$ – простое число, то уравнения $p = x^2 + 3y^2$, $x^2 + xy + y^2$ имеют решения в натуральных числах. Ни одно простое число вида $3n + 2$ не может быть представлено ни одной из форм $x^2 + 3y^2$, $x^2 + xy + y^2$.

В этих утверждениях прослеживается содержание Артиновского закона взаимности для квадратичных полей. А именно, закономерности, обнаруженные Ферма, показывают, что число выписанных выше прогрессий, в которых все простые числа представимы рассмотренными выше формами, равно числу прогрессий, в которых отсутствуют представимые простые числа.

Исследования Ферма по теории чисел были продолжены Леонардом Эйлером. Катализатором этих исследований послужила переписка Эйлера с Христианом Гольдбахом, начавшаяся в 1729 году. В своих письмах Гольдбах обратил внимание Эйлера на труды Ферма, и впоследствии Эйлер сумел доказать многие утверждения своего предшественника. Подробный обзор исследований Эйлера по различным вопросам теории чисел представлен в книге [2], подготовленной на основе его архивных рукописей и записных книжек коллективом историков математики – Г.П. Матвиевской, Е.П. Ожиговой и другими. На основании исследований простых чисел, представимых формами ax^2+by^2, и многочисленных вычислений Эйлер в 1744 году представил эквивалентную формулировку классического квадратичного закона взаимности в работе [3]. Согласно этой формулировке, если использовать современные обозначения, для различных простых нечетных чисел p, q и натурального числа a из сравнения $p \equiv \pm q \pmod{4a}$ следует равенство $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. В частности, свойство числа a быть квадратичным вычетом простого числа p полностью определяется остатком от деления p на $4a$. Формулировка, близкая к современной, но все еще без доказательства, была дана Эйлером в 1783 году в работе [4] . Несколько позже, в 1785 году, квадратичный закон взаимности был независимо сформулирован Адриеном Мари Лежандром в труде [5], где впервые встречается само название закон взаимности (loi de réciprocité). Доказательство квадратичного закона взаимности, приведенное Лежандром в этой работе, не является полным, так как оно опирается на известную теорему о простых числах

в арифметических прогрессиях, доказанную в 1837 году П.Г.Л. Дирихле. В первом издании известного сочинения «Essai sur la théorie des nombres»[6] Лежандр вводит символ, носящий его имя, и вместе с тем он формулирует квадратичный закон взаимности в виде хорошо известного изящного равенства $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

Первое полное доказательство квадратичного закона взаимности принадлежит Карлу Фридриху Гауссу. В предисловии к статье [7] Гаусс описывает историю своих первых исследований в области законов взаимности. Гаусс пришел к квадратичному закону взаимности самостоятельно эмпирическим путем в марте 1795 года, когда ему было 18 лет, в это время он ничего не знал о работах своих предшественников. Попытки Гаусса доказать общий квадратичный закон взаимности оставались тщетными в течение целого года. Наконец, 8 апреля 1796 года ему удалось найти полное доказательство. Первое доказательство, которое было достаточно сложным и использовало метод математической индукции, было опубликовано в 1801 году в его знаменитом труде “Арифметические исследования” (Disquisitiones Arithmeticae). В этой же работе Гаусс дает второе доказательство квадратичного закона взаимности с помощью им же созданной теории бинарных квадратичных форм. Всего Гауссу принадлежит восемь различных доказательств квадратичного закона взаимности. На сегодняшний день известно более 300 различных доказательств квадратичного закона взаимности, хронологический список которых поддерживается в актуальном состоянии в электронном архиве [9].

Гаусс первым осознал, что правильное обобщение квадратичного закона взаимности глубоко связано с арифметикой в числовых полях. В связи со своими исследованиями по кубическому и биквадратичному законам взаимности в работе “Теория биквадратичных вычетов” [8, с. 655] Гаусс пишет: “После того как мы начали исследовать эти вопросы в 1805 г., ... мы скоро пришли к убеждению, что применявшиеся до сих пор арифметические принципы ни в коем случае не достаточны для обоснования общей теории, а что эта теория с необходимостью требует в некотором смысле бесконечно расширить область высшей арифметики; а как это следует понимать, будет показано в процессе настоящих исследований”. Работы Гаусса были продолжены Якоби и Эйзенштейном. Последующее развитие этих исследований привели к работам Куммера, Гильберта, Фуртвенглера, Такаги и в конечном счете привело к формулировке общего закона взаимности Артина. В работе [10] Э. Артин отмечает, что ключевой идеей доказательства закона взаимности явилось присоединение полей деления круга, заимствованной из работы Н.Г. Чеботарева, где он доказывает свою знаменитую теорему плотности. В своей математической автобиографии Н.Г. Чеботарев пишет: “Летом 1927 г., изучая теорию полей классов, я пришел к убеждению, что можно доказать закон Артина, воспользовавшись моим приемом присоединения полей деления круга” ([11, с. 155]).

В 1872 году Е.И. Золотарёв в работе [12] предложил новое доказательство квадратичного закона взаимности, основанное на обнаруженной им новой интерпретации символа Лежандра. Согласно ей, для произвольного нечетного простого числа p и целого

числа a, взаимно простого с p, значение символа Лежандра $\left(\frac{a}{p}\right)$ совпадает со знаком перестановки на конечном поле $\mathbb{Z}/p\mathbb{Z}$, действующей по правилу $x \mapsto ax$. Этот классический результат ныне широко известен как лемма Золотарёва. В статье [7], где Гаусс приводит свое третье доказательство квадратичного закона взаимности на основе леммы Гаусса, которая, по существу, эквивалентна лемме Золотарёва, он следующим образом комментирует предложенный подход: "... Поэтому я, не колеблясь, утверждаю, что *естественное* доказательство до сих пор отсутствовало; знатоки смогут судить, заслуживает ли такого наименования доказательство, которое нам недавно посчастливилось открыть и которое излагается на следующих ниже страницах" [8, с. 588]. Представляется обоснованным, что подход Золотарёва удовлетворяет этому требованию естественности, поскольку он дает достаточно прозрачное доказательство квадратичного закона взаимности и, что не менее важно, имеет естественные обобщения. Обобщение леммы Золотарёва на случай символа Якоби было получено в 1896 году М. Лерхом [18] и независимо в 1914 году Ф.Г. Фробениусом в работе [17]. В 2005 году У. Дьюк и К. Хопкинс в статье [19], опираясь на идеи Золотарёва, получили аналог квадратичного закона взаимности для конечных групп. В недавней работе [14] А. Бруньят и П.Л. Кларк обобщили подход Золотарёва на случай абстрактных числовых колец, т. е. дедекиндовых колец, факторкольца по максимальным идеалам которых конечны.

Цель нашей работы – представить обзор развития идей Е.И. Золотарёва, заложенных в его классическом подходе к доказательству квадратичного закона взаимности. В статье рассмотрены расширения данного метода на абстрактные числовые кольца, приведенные в работе [14], а также на конечные группы, изученные в статье [19]. Обсуждаются связи этих исследований с некоторыми классическими результатами и подходами к доказательству квадратичного закона взаимности. Работа состоит из шести параграфов. В первом параграфе рассматривается расширение подхода Золотарёва к доказательству квадратичного закона взаимности на произвольные абстрактные числовые области. Изложение в основном следует ключевым идеям работы Золотарёва [12] и опирается на материал статьи [14]. Второй параграф посвящен групповым символам, изученным в статьях [19, 20]. В рамках подхода Золотарёва они являются естественным обобщением символов Лежандра и Якоби. В данном разделе рассматриваются различные способы доказательства квадратичного закона для конечных групп. В качестве приложения, в частности, рассматриваются методы доказательства квадратичного закона взаимности с помощью определителей Вандермонда. Четвертый параграф посвящен символу Картье, который является естественным обобщением группового символа для случая конечных абелевых групп. Рассматриваются их основные свойства, многие из которых были получены в работе [15]. Также приводится формула, обобщающая известные выражения символа Картье через определители. Заключительный параграф работы посвящен законам взаимности для многочленов. В первой его части доказывается квадратичный закон взаимности для многочленов на основе подхода Золотарёва. Вторая часть посвящена доказательству степенного закона взаимности для многочленов с использованием результантов. В заключительной части обсуждают-

ся различные способы доказательства классического квадратичного закона с помощью результанта.

1. Квадратичный закон взаимности по Золотарёву

Напомним, что область целостности R называется дедекиндовым кольцом, если для произвольных ее идеалов A и B выполнено условие:

$$A \subseteq B \Leftrightarrow B \mid A.$$

Примерами дедекиндовых колец служат кольца главных идеалов и кольца целых конечных расширений поля рациональных чисел $\mathbb{Q}$. Хорошо известно, что область целостности R является дедекиндовой в точности тогда, когда каждый его ненулевой идеал (однозначно) представим в виде произведения простых идеалов (см., например, [13, теорема 2.11]).

Для конечного поля $\mathbb{F}_q$ нечетного порядка и произвольного ненулевого элемента $a \in \mathbb{F}_q$ символ Лежандра определяется классическим образом:

$$\left(\frac{a}{\mathbb{F}_q}\right) := \begin{cases} 1, & \text{если } a \in \mathbb{F}_q^{*2}; \\ -1, & \text{если } a \notin \mathbb{F}_q^{*2}. \end{cases}$$

Дедекиндово кольцо R, в котором факторкольцо R/A конечно для любого ненулевого идеала A, называется абстрактным числовым кольцом [14]. Важными примерами таких колец являются кольца целых конечных расширений поля $\mathbb{Q}$ и кольца многочленов $\mathbb{F}_q[x]$.

Если A – идеал кольца R и $a \in R$, то смежный класс $a + A$ обозначается $[a]_A$. Если $b \in R$, то через $[a]_b$ обозначим смежный класс $a + (b)$.

Пусть R – абстрактное числовое кольцо. Ненулевой собственный идеал $A \subset R$ назовем нечетным, если порядок факторкольца $|R/A|$ – нечетное число. Если P – нечетный простой идеал кольца R и $a \notin P$, то следуя [14], определим символ Лежандра элемента a по модулю идеала P согласно правилу:

$$\left(\frac{a}{P}\right) := \left(\frac{[a]_P}{R/P}\right).$$

Пусть A – нечетный идеал кольца R, $A = P_1 \dots P_k$, где $P_1, \dots, P_k$ – простые идеалы кольца R, и a – элемент из R, для которого выполнено равенство $(a)+A = R$, т. е. в разложения идеалов A и (a) входят различные простые идеалы. Следуя [14], определим символ Якоби элемента a по модулю идеала A согласно правилу:

$$\left(\frac{a}{A}\right) := \prod_{i=1}^{k} \left(\frac{a}{P_i}\right).$$

Рассмотрим отображение $m_a : R/A \to R/A$, действующее согласно правилу $[r]_A \mapsto [ar]_A$. Ясно, что m_a является биективным отображением. Символ Золотарёва элемента a по модулю идеала A определяется как знак этой перестановки [14]:

$$\left[\frac{a}{A}\right] := \operatorname{sgn}(m_a).$$

В случае, если идеал A является главным и порождается элементом b, для краткости будем использовать обозначения $\left(\frac{a}{b}\right)$ и $\left[\frac{a}{b}\right]$ вместо $\left(\frac{a}{(b)}\right)$ и $\left[\frac{a}{(b)}\right]$ соответственно.

Пусть G – группа и X – G-множество, где X – конечное множество. Представление группы G перестановками множества X, соответствующее G-множеству X, будем обозначать через $\pi_X \colon G \to \operatorname{Sym}(X)$, где $\operatorname{Sym}(X)$ – группа всех перестановок X. Гомоморфизм из группы G в группу $\{\pm 1\}$, который каждому элементу $g \in G$ сопоставляет знак перестановки $\pi_X(g)$, обозначим через π'_X. Следующее утверждение проверяется непосредственно.

Лемма 1.

a) *Если конечное G-множество X является дизъюнктным объединением своих G-подмножеств $X_1, \dots, X_k$, то $\pi'_X(g) = \pi'_{X_1}(g) \dots \pi'_{X_k}(g)$ для каждого $g \in G$.*

b) *Если $X_1, \dots, X_k$ – конечные G-множества, $|X_1| = n_1, \dots, |X_k| = n_k$ и $n = n_1 \cdots n_k$, то $\pi'_{X_1 \times \dots \times X_k}(g) = \pi'_{X_1}(g)^{\frac{n}{n_1}} \cdots \pi'_{X_k}(g)^{\frac{n}{n_k}}$ для каждого $g \in G$. В частности, если все натуральные числа $n_1, \dots, n_k$ нечетны, то $\pi'_{X_1 \times \dots \times X_k}(g) = \pi'_{X_1}(g) \cdots \pi'_{X_k}(g)$ для каждого $g \in G$.*

Через ε_G будем обозначать представление Кэли группы G, т. е. гомоморфизм $G \to \operatorname{Sym}(G)$, действующий по правилу $g \mapsto (a \mapsto ga)$.

Доказательство следующего утверждения основано на идеях из работы [14] и является обобщением рассуждений, приведенных в работе [24] при доказательстве леммы Золотарёва–Фробениуса.

Теорема 2 (Обобщенная лемма Золотарёва–Фробениуса; см. Картье [15] и [14])**.** *Пусть R – абстрактное числовое кольцо и I – нечетный идеал R. Если a – элемент из R, для которого выполнено равенство $(a) + I = R$, то*

$$\left[\frac{a}{I}\right] = \left(\frac{a}{I}\right).$$

Доказательство. Рассмотрим сначала случай, когда $I = Q^m$, где Q – простой идеал кольца R. Положим $G = U(R/Q^m)$. Для каждого натурального числа $k \le m$ факторкольцо R/Q^k имеет естественную структуру R/Q^m-модуля. Этот модуль индуцирует на R/Q^k структуру G-множества, которое, как несложно заметить, является дизъюнктным объединением своих G-подмножеств $U(R/Q^k)$ и Q/Q^k. Так как R/Q^m-модули Q/Q^k и R/Q^{k-1} изоморфны, они изоморфны и как G-множества. Следовательно, имеет место изоморфизм G-множеств $R/Q^k \cong U(R/Q^k) \sqcup R/Q^{k-1}$. Тогда с помощью индукции получаем

изоморфизм G-множеств $R/Q^m \cong U(R/Q) \sqcup \ldots \sqcup U(R/Q^m)$. Для некоторого нечетного простого числа p и $n \in \mathbb{N}$ имеет место изоморфизм $R/Q \cong \mathbb{F}_{p^n}$. Положим $q = p^n$. Согласно [16, теорема XVIII.2], для произвольного натурального числа $k \leq m$ имеет место разложение $U(R/Q^k) = C_{q-1} \times U$, где C_{q-1} – циклическая группа порядка $q-1$, а U – p-группа. Образ $\varepsilon_{U(R/Q^k)}(g)$ порождающего элемента g циклической группы C_{q-1} является произведением $|U|$ циклов четной длины $q-1$. Следовательно, гомоморфизм $\pi'_{U(R/Q^k)} \colon G \to \{\pm 1\}$ является неединичным.

Заметим, что символ Лежандра $\left(\frac{\cdot}{Q}\right)$ индуцирует неединичный гомоморфизм из G в $\{\pm 1\}$, действующий согласно правилу $a + Q^m \mapsto \left(\frac{a}{Q}\right)$, который мы будем обозначать также через $\left(\frac{\cdot}{Q}\right)$. Поскольку, очевидно, группа G обладает единственной подгруппой индекса два, то существует единственный неединичный гомоморфизм из G в $\{\pm 1\}$. Таким образом, имеют место равенства:

$$\left(\frac{\cdot}{Q}\right) = \pi'_{U(R/Q^m)} = \ldots = \pi'_{U(R/Q)}.$$

Тогда, согласно лемме 1 a), для каждого элемента $a \in R$, удовлетворяющего условию $(a) + Q = R$, получаем:

$$\left[\frac{a}{Q^m}\right] = \pi'_{R/Q^m}(a + Q^m) = \pi'_{U(R/Q^m)}(a + Q^m) \cdots \pi'_{U(R/Q)}(a + Q^m) = \left(\frac{a}{Q}\right)^m = \left(\frac{a}{Q^m}\right).$$

Рассмотрим общий случай. Пусть $I = Q_1^{m_1} \cdots Q_k^{m_k}$, где $Q_1, \ldots, Q_k$ – различные простые нечетные идеалы кольца R, и $G = U(R/I)$. Согласно китайской теореме об остатках, диагональный кольцевой гомоморфизм из R в $R/Q_1^{m_1} \times \cdots \times R/Q_k^{m_k}$, действующий по правилу $a \mapsto (a + Q_1^{m_1}, \ldots, a + Q_k^{m_k})$, индуцирует изоморфизм R/I-модулей

$$R/I \cong R/Q_1^{m_1} \times \cdots \times R/Q_k^{m_k},$$

который также является изоморфизмом G-множеств. Тогда, согласно лемме 1 b), для каждого элемента $a \in R$, для которого выполнено равенство $(a) + I = R$, имеют место равенства:

$$\left[\frac{a}{I}\right] = \pi'_{R/I}(a + I) = \pi'_{R/Q_1^{m_1}}(a + I) \cdots \pi'_{R/Q_k^{m_k}}(a + I) = \left(\frac{a}{Q_1^{m_1}}\right) \cdots \left(\frac{a}{Q_k^{m_k}}\right) = \left(\frac{a}{I}\right). \quad \square$$

Следствие 3 (лемма Золотарёва–Фробениуса; Фробениус, 1914 г., [17], Лерх, 1896 г., [18])**.** *Для произвольного целого нечетного числа $n > 1$ и целого числа m, взаимно простого с n, имеет место равенство*

$$\left[\frac{m}{n}\right] = \left(\frac{m}{n}\right).$$

До конца этого параграфа будем предполагать, что R – абстрактное числовое кольцо. Также будем придерживаться следующих обозначений: $a, b \in R$ – ненулевые и необратимые взаимно простые элементы из R, $A = \{a_1, \ldots, a_n\}$ – полная система представителей классов смежности для факторкольца $R/(a)$ и $B = \{b_1, \ldots, b_m\}$ – полная система представителей для $R/(b)$. Для некоторых $t_1, t_2 \in R$ имеет место равенство $1 = bt_1 + at_2$. Через e_1, e_2 обозначим соответственно bt_1 и at_2. Естественный изоморфизм, действующий из $R/(ab)$ в $R/(a) \times R/(b)$ согласно правилу $r_1e_1 + e_2r_2 + (ab) \mapsto (r_1 + (a), r_2 + (b))$, обозначим ψ.

Следующее утверждение доказывается с помощью стандартных рассуждений.

Лемма 4. *Множества*

$$S = \{a_i + b_j a \mid 1 \leq i \leq n,\ 1 \leq j \leq m\}, \qquad S' = \{a_i b + b_j \mid 1 \leq i \leq n,\ 1 \leq j \leq m\}$$

и $E = \{e_1 a_i + e_2 b_j \mid a_i \in A,\ b_j \in B\}$ *образуют полные системы представителей для факторкольца* $R/(ab)$.

Лемма 5. *Если* $b \in R$ *– нечетный элемент, то*:

1) *для любого элемента* $c \in R/(b)$ *знак биективного отображения* $S_c \colon R/(b) \to R/(b)$, *действующего согласно правилу* $S_c(x) = x + c$, *равен* 1;
2) *для любого элемента* $c \in R/(b)$ *знак биективного отображения* $L \colon R/(b) \to R/(b)$, *действующего согласно правилу* $L(x) = ax + c$, *равен* $\left[\dfrac{a}{b}\right]$.

Доказательство. 1) Так как $|R/(b)|$ – нечетное натуральное число, порядок k элемента c в аддитивной группе кольца $R/(b)$ является нечетным числом. Следовательно, перестановка S_c является произведением независимых циклов, длина каждого из которых равна k. Таким образом, $\operatorname{sgn}(S_c) = 1$.

2) Следует из первого пункта и определения символа Золотарёва. □

Теорема 6 (вторая лемма Золотарёва; [14])**.**
Пусть $\alpha \colon R/(ab) \to R/(ab)$ *и* $\beta \colon R/(ab) \to R/(ab)$ *– отображения, действующие для каждых* $1 \leq i \leq n$ *и* $1 \leq j \leq m$ *согласно правилам:*

$$\alpha \colon [e_1 a_i + e_2 b_j]_{ab} \mapsto [a_i + ab_j]_{ab},$$
$$\beta \colon [e_1 a_i + e_2 b_j]_{ab} \mapsto [a_i b + b_j]_{ab}.$$

Тогда α, β *– биекции, и имеют место равенства:*

$$\operatorname{sgn}(\alpha) = \left[\frac{a}{b}\right], \qquad \operatorname{sgn}(\beta) = \left[\frac{b}{a}\right].$$

Доказательство. Так как $e_1 + e_2 = 1$ и $e_2 \equiv 0 \pmod{a}$, то справедливо равенство

$$\alpha([e_1 a_i + e_2 b_j]_{ab}) = [a_i + ab_j]_{ab} = [e_1 a_i + e_2(a_i + ab_j)]_{ab}.$$

Следовательно, отображение α индуцирует биективное отображение $\alpha' = \psi\alpha\psi^{-1}$ множества $R/(a) \times R/(b)$ в себя, которое действует по правилу:

$$\alpha' \colon ([a_i]_a, [b_j]_b) \mapsto ([a_i]_a, [a_i + ab_j]_b).$$

Поскольку множество $R/(a) \times R/(b)$ является дизъюнктным объединением подмножеств $X_1, \ldots, X_n$, где $X_i = \{([a_i]_a, [b_1]_b), \ldots, ([a_i]_a, [b_m]_b)\}$ для каждого $1 \leq i \leq n$, и при этом $\alpha'(X_i) = X_i$, то

$$\operatorname{sgn}(\alpha) = \operatorname{sgn}(\alpha') = \prod_{i=1}^{n} \operatorname{sgn}(\alpha'_{|X_i}).$$

Так как сужение $\alpha'_{|X_i}$ для каждого i оставляет первые компоненты элементов множества X_i без изменений, а вторые компоненты преобразует согласно правилу $[b_j]_b \mapsto [a_i]_b + [a]_b[b_j]_b$, то из леммы 5 следует равенство $\operatorname{sgn}(\alpha'_{|X_i}) = \left[\frac{a}{b}\right]$. Поскольку порядок $n = |R/(a)|$ является нечетным (так как a – нечетный элемент), получаем:

$$\operatorname{sgn}(\alpha) = \left(\left[\frac{a}{b}\right]\right)^n = \left[\frac{a}{b}\right].$$

Аналогично доказывается равенство

$$\operatorname{sgn}(\beta) = \left[\frac{b}{a}\right]. \qquad \square$$

Следуя работе [14], определим знак Золотарёва для произвольных взаимно простых нечетных элементов $a, b \in R$:

$$\mathrm{Z}_R(a, b) := \operatorname{sgn}\left(\beta\alpha^{-1}\right).$$

Биективное отображение $\beta\alpha^{-1} \colon R/(ab) \to R/(ab)$ действует для каждых $1 \leq i \leq n$ и $1 \leq j \leq m$ согласно правилу $[a_i + b_j a]_{ab} \mapsto [a_i b + b_j]_{ab}$. При этом, согласно теореме 6, значение $\mathrm{Z}_R(a, b)$ не зависит от выбора полных систем представителей A и B.

Следующая теорема непосредственно вытекает из теоремы 2 и теоремы 6.

Теорема 7 (квадратичный закон взаимности Золотарёва; см. [14])**.**
Пусть $a, b \in R$ – нечетные взаимно простые элементы. Тогда

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \mathrm{Z}_R(a, b).$$

Теорема 8 (лемма Эйзенштейна; [14])**.** *Пусть m, n – натуральные взаимно простые нечетные числа и $m, n > 1$. Тогда*

$$\mathrm{Z}_{\mathbb{Z}}(m, n) = (-1)^{\frac{(m-1)(n-1)}{4}}.$$

Доказательство. Положим $A = \{0, 1, \ldots, mn-1\}$. Ясно, что

$$A = \{i + jm \mid 0 \leq i \leq m-1,\ 0 \leq j \leq n-1\} = \{in + j \mid 0 \leq i \leq m-1,\ 0 \leq j \leq n-1\}.$$

Тогда $\mathrm{Z}_{\mathbb{Z}}(m,n)$ – знак биективного отображения $\alpha\colon A \to A$, которое для произвольных $0 \leq i \leq m-1$ и $0 \leq j \leq n-1$ действует согласно правилу $\alpha(i+jm) = in + j$.

Несложно заметить, что неравенство $i_1 + j_1 m < i_2 + j_2 m$, где $0 \leq i_1, i_2 \leq m-1$ и $0 \leq j_1, j_2 \leq n-1$, выполнено в точности тогда, когда либо $j_1 < j_2$, либо $j_1 = j_2$ и $i_1 < i_2$. Аналогично, неравенство $i_1 n + j_1 < i_2 n + j_2$, где $0 \leq i_1, i_2 \leq m-1$ и $0 \leq j_1, j_2 \leq n-1$, имеет место в точности тогда, когда либо $i_1 < i_2$, либо $i_1 = i_2$ и $j_1 < j_2$.

Таким образом, для произвольных $0 \leq i_1, i_2 \leq m-1$ и $0 \leq j_1, j_2 \leq n-1$ неравенства $i_1 + j_1 m < i_2 + j_2 m$ и $ni_1 + j_1 > ni_2 + j_2$ одновременно выполнены в точности тогда, когда $i_1 > i_2$ и $j_1 < j_2$. Следовательно, общее число инверсий перестановки, индуцированной биекцией α, относительно естественного порядка на A равно

$$\binom{m}{2}\binom{n}{2} = \frac{m(m-1)}{2} \cdot \frac{n(n-1)}{2}.$$

Тогда, учитывая нечетность чисел m и n, получаем:

$$\mathrm{Z}_{\mathbb{Z}}(m,n) = (-1)^{\frac{m(m-1)}{2} \cdot \frac{n(n-1)}{2}} = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} = (-1)^{\frac{(m-1)(n-1)}{4}}. \qquad \square$$

Из теоремы 7 и теоремы 8 непосредственно вытекает классический закон взаимности для символа Якоби.

Теорема 9. *Пусть m, n – натуральные взаимно простые нечетные числа и $m, n > 1$. Тогда*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}.$$

2. Групповые символы и квадратичный закон взаимности для них

2.1. Символ Дьюка–Хопкинс. Развивая теоретико-групповой подход Золотарёва к квадратичному закону взаимности, У. Дьюк и К. Хопкинс [19] ввели его обобщение для произвольной конечной группы.

Определение 10 (символ Дьюка–Хопкинс)**.** Пусть G – конечная группа порядка n. Пусть $C_1 = \{1\}, C_2, \ldots, C_m$ – классы сопряженности группы G. Для произвольного целого числа a рассмотрим отображение $g \mapsto g^a$. Если $(a,n) = 1$, оно индуцирует перестановку φ_a на множестве классов сопряженности $\{C_1, \ldots, C_m\}$: $\varphi_a(C_j) = C_j^a = \{g^a \mid g \in C_j\}$. Символ Дьюка–Хопкинс определяется как:

$$\left(\frac{a}{G}\right)_{\mathrm{DH}} = \begin{cases} \operatorname{sgn}(\varphi_a), & \text{если } (a,n) = 1; \\ 0, & \text{если } (a,n) \neq 1. \end{cases}$$

Из определения символа Дьюка–Хопкинс непосредственно вытекает следующее утверждение:

Лемма 11. *Пусть G – конечная группа порядка n и $a, b \in \mathbb{Z}$. Тогда*:

1) *если* $a \equiv b \pmod{n}$, *то* $\left(\frac{a}{G}\right)_{\mathrm{DH}} = \left(\frac{b}{G}\right)_{\mathrm{DH}}$;

2) $\left(\frac{ab}{G}\right)_{\mathrm{DH}} = \left(\frac{a}{G}\right)_{\mathrm{DH}} \left(\frac{b}{G}\right)_{\mathrm{DH}}$.

Поскольку в абелевой группе каждый класс сопряженности состоит из одного элемента, перестановка классов сопряженности совпадает с перестановкой самих элементов. Тогда из леммы Золотарёва–Фробениуса (следствие 3) следует, что если $n > 1$ – нечетное натуральное число, $m \in \mathbb{Z}$ и $(m, n) = 1$, то для аддитивной группы кольца вычетов $\mathbb{Z}_n$ имеет место равенство:

$$\left(\frac{m}{\mathbb{Z}_n}\right)_{\mathrm{DH}} = \left(\frac{m}{n}\right).$$

Символ Дьюка–Хопкинс наследует ряд важных свойств классических символов Лежандра и Якоби. В частности, как будет показано ниже (в разд. 2.3), для него выполняется аналог квадратичного закона взаимности.

Для символа Дьюка–Хопкинс в случае конечных абелевых групп также имеют место аналоги первого и второго дополнений к квадратичному закону взаимности. Поскольку для $\mathbb{Z}_n$ символ Дьюка–Хопкинс совпадает с символом Якоби, приведем комбинаторные доказательства этих дополнений, опирающиеся на лемму Золотарёва–Фробениуса.

Предложение 12. *Пусть n – натуральное нечетное число. Тогда*:

1) $\left(\frac{-1}{\mathbb{Z}_n}\right)_{\mathrm{DH}} = (-1)^{\frac{n-1}{2}}$;

2) $\left(\frac{2}{\mathbb{Z}_n}\right)_{\mathrm{DH}} = (-1)^{\frac{n^2-1}{8}}$.

Доказательство. Для любого $a \in \mathbb{Z}$ такого, что $(a, n) = 1$, перестановку на множестве элементов кольца вычетов $\mathbb{Z}_n$, действующую согласно правилу $x \mapsto ax$, будем обозначать через φ_a.

1) Рассмотрим циклическое разложение перестановки φ_{-1}, действующей на кольце вычетов $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Так как n нечетно, то для каждого ненулевого элемента $x \in \mathbb{Z}_n$ выполнены условия: $x \neq -x$, $\varphi_{-1}(x) = -x$ и $\varphi_{-1}(-x) = x$. Таким образом, перестановка φ_{-1} раскладывается в произведение $(n-1)/2$ независимых циклов длины два, следовательно,

$$\left(\frac{-1}{\mathbb{Z}_n}\right)_{\mathrm{DH}} = (-1)^{\frac{n-1}{2}}.$$

2) Разобьем множество элементов $\mathbb{Z}_n$ на две части:

$$A = \left\{0, 1, \ldots, \frac{n-1}{2}\right\} \quad \text{и} \quad B = \left\{\frac{n+1}{2}, \ldots, n-1\right\}.$$

Тогда $\varphi_2(A) = \{0, 2, 4, \ldots, n-1\}$ и

$$\varphi_2(B) = \left\{2 \cdot \frac{n+1}{2}, \ldots, 2(n-1)\right\} = \left\{2 \cdot \frac{n+1}{2} - n, \ldots, 2(n-1) - n\right\} = \{1, 3, 5, \ldots, n-2\}.$$

Заметим, что все арифметические операции в выписанном выше равенстве осуществляются в кольце вычетов $\mathbb{Z}_n$. Тогда

$$(\varphi_2(0), \ldots, \varphi_2(n-1)) = \left(\underbrace{0, 2, \ldots, n-1}_{\text{элементы } \varphi_2(A)}, \underbrace{1, 3, \ldots, n-2}_{\text{элементы } \varphi_2(B)}\right).$$

Найдем количество инверсий в перестановке последовательности $0, 1, 2, \ldots, n-1$, выписанной выше. Для каждого $a = 2k \in \varphi_2(A)$ посчитаем элементы

$$b \in \varphi_2(B) = \left\{2j - 1 \mid 1 \leq j \leq \frac{n-1}{2}\right\}$$

такие, что $2k > 2j - 1$. Это неравенство эквивалентно условию $j \leq k$. Для фиксированного k таких значений j ровно k штук. Следовательно, общее число инверсий перестановки φ_2 равно:

$$\sum_{k=1}^{(n-1)/2} k = \frac{\frac{n-1}{2}\left(\frac{n-1}{2} + 1\right)}{2} = \frac{\frac{n-1}{2} \cdot \frac{n+1}{2}}{2} = \frac{n^2 - 1}{8}.$$

Таким образом,

$$\left(\frac{2}{\mathbb{Z}_n}\right)_{\text{DH}} = (-1)^{\frac{n^2-1}{8}}. \qquad \square$$

Лемма 13. *Пусть G_1 и G_2 – конечные абелевы группы нечетного порядка n_1 и n_2 соответственно, причем $a \in \mathbb{Z}$ удовлетворяет условию $(a, n_1 n_2) = 1$. Тогда*

$$\left(\frac{a}{G_1 \times G_2}\right)_{\text{DH}} = \left(\frac{a}{G_1}\right)_{\text{DH}} \left(\frac{a}{G_2}\right)_{\text{DH}}.$$

Доказательство. Пусть $x \in G_1$ и $y \in G_2$. Элементы группы $G_1 \times G_2$ имеют вид (x, y). Отображение $g \mapsto g^a$ индуцирует перестановку φ_a на элементах группы $G_1 \times G_2$: $\varphi_a((x, y)) = (x^a, y^a)$. Обозначим через π_a перестановку $x \mapsto x^a$ на элементах группы G_1, а через σ_a – перестановку $y \mapsto y^a$ на элементах группы G_2. Тогда по определению символа Дьюка–Хопкинс имеем:

$$\left(\frac{a}{G_1}\right)_{\text{DH}} = \operatorname{sgn}(\pi_a) \quad \text{и} \quad \left(\frac{a}{G_2}\right)_{\text{DH}} = \operatorname{sgn}(\sigma_a).$$

Следовательно, согласно лемме 1 b), имеют место равенства:

$$\left(\frac{a}{G_1 \times G_2}\right)_{\mathrm{DH}} = \mathrm{sgn}(\varphi_a) = (\mathrm{sgn}(\pi_a))^{n_2}(\mathrm{sgn}(\sigma_a))^{n_1} = \mathrm{sgn}(\pi_a)\,\mathrm{sgn}(\sigma_a) = \left(\frac{a}{G_1}\right)_{\mathrm{DH}}\left(\frac{a}{G_2}\right)_{\mathrm{DH}}.$$

□

Предложение 14. *Пусть G – конечная абелева группа нечетного порядка n. Тогда*:

1) $\left(\dfrac{-1}{G}\right)_{\mathrm{DH}} = (-1)^{\frac{n-1}{2}}$;

2) $\left(\dfrac{2}{G}\right)_{\mathrm{DH}} = (-1)^{\frac{n^2-1}{8}}$.

Доказательство. Согласно основной теореме о строении конечных абелевых групп, группу G можно разложить в прямое произведение циклических групп H_i:

$$G \cong H_1 \times H_2 \times \cdots \times H_k.$$

Поскольку порядок группы G нечетен, порядки $m_i = |H_i|$ также нечетны. При этом $H_i \cong \mathbb{Z}_{m_i}$, а порядок всей группы равен $n = m_1 m_2 \dots m_k$.

1) Из предложения 12 1) следует, что для каждого i имеет место равенство $\left(\dfrac{-1}{\mathbb{Z}_{m_i}}\right)_{\mathrm{DH}} = (-1)^{\frac{m_i-1}{2}}$. Тогда, согласно лемме 13, получаем:

$$\left(\frac{-1}{G}\right)_{\mathrm{DH}} = \prod_{i=1}^{k}(-1)^{\frac{m_i-1}{2}} = (-1)^{\sum\limits_{i=1}^{k}\frac{m_i-1}{2}}.$$

Таким образом, из несложно проверяемого сравнения $\sum\limits_{i=1}^{k}\frac{m_i-1}{2} \equiv \frac{(\prod m_i)-1}{2} \pmod 2$ вытекает, что:

$$\left(\frac{-1}{G}\right)_{\mathrm{DH}} = (-1)^{\frac{n-1}{2}}.$$

2) Из предложения 12 2) следует, что для каждого i имеет место равенство $\left(\dfrac{2}{\mathbb{Z}_{m_i}}\right)_{\mathrm{DH}} = (-1)^{\frac{m_i^2-1}{8}}$. Тогда

$$\left(\frac{2}{G}\right)_{\mathrm{DH}} = \prod_{i=1}^{k}(-1)^{\frac{m_i^2-1}{8}} = (-1)^{\sum\limits_{i=1}^{k}\frac{m_i^2-1}{8}}.$$

Таким образом, из несложно проверяемого сравнения $\sum\limits_{i=1}^{k}\frac{m_i^2-1}{8} \equiv \frac{(\prod m_i)^2-1}{8} \pmod 2$ следует, что

$$\left(\frac{2}{G}\right)_{\mathrm{DH}} = (-1)^{\frac{n^2-1}{8}}.$$

□

Заметим, что предыдущее предложение не имеет место для произвольных конечных групп нечетного порядка. Пусть p – нечетное простое число. Рассмотрим группу Фробе-

ниуса $G = \mathrm{Aff}(\mathbb{F}_p)$, состоящую из всех преобразований поля $\mathbb{F}_p$ вида $x \mapsto ax + b$, где $a \in \mathbb{F}_p^*$ и $b \in \mathbb{F}_p$. Порядок группы $|G| = p(p-1)$ является четным. Покажем, что

$$\left(\frac{-1}{G}\right)_{\mathrm{DH}} = (-1)^{\frac{p-3}{2}}.$$

Известно, что аффинная группа $\mathrm{Aff}(\mathbb{F}_p)$ разбивается на $m = p$ классов сопряженности: тождественное преобразование, нетривиальные параллельные переносы $x \mapsto x+b$, они все образуют один класс, и преобразования растяжения с фиксированной точкой $x \mapsto ax + b$ для каждого $a \neq 1$, таких классов $p-2$. Определим количество вещественных классов r_1. Тождественный класс вещественен тривиально. Для любого переноса $f(x) = x + b$ обратным является перенос $f^{-1}(x) = x - b$, который принадлежит тому же классу сопряженности нетривиальных переносов; следовательно, этот класс также вещественен. Для любого элемента $g(x) = ax + b$, $a \neq 1$, обратный элемент имеет коэффициент при x, равный a^{-1}. Класс сопряженности такого элемента будет вещественным тогда и только тогда, когда $a = a^{-1}$, что равносильно $a^2 = 1$. В поле $\mathbb{F}_p$ единственным корнем этого уравнения, отличным от единицы, является $a = -1$. Таким образом, класс преобразований вида $x \mapsto -x+b$ является вещественным, а все остальные $p-3$ классов образуют комплексно-сопряженные пары. Итого, группа содержит $r_1 = 3$ вещественных класса. Поскольку $m = r_1 + 2r_2$, получаем $r_2 = \dfrac{p-3}{2}$. Таким образом, $\left(\dfrac{-1}{G}\right)_{\mathrm{DH}} = (-1)^{\frac{p-3}{2}}$.

Предложение 15. *Пусть G – конечная абелева группа нечетного порядка n, причем $a \in \mathbb{Z}$ удовлетворяет условию $(a, n) = 1$. Тогда*

$$\left(\frac{a}{G}\right)_{\mathrm{DH}} = \left(\frac{a}{n}\right).$$

В частности, если G_1, G_2 – конечные абелевы группы одного и того же нечетного порядка n, то для всякого целого числа a, взаимно простого с n, имеет место равенство:

$$\left(\frac{a}{G_1}\right)_{\mathrm{DH}} = \left(\frac{a}{G_2}\right)_{\mathrm{DH}}.$$

Доказательство. Пусть группа G изоморфна прямому произведению циклических групп:

$$G \cong H_1 \times H_2 \times \cdots \times H_k,$$

где каждая $H_i \cong \mathbb{Z}_{m_i}$ является циклической группой.

Согласно лемме 13 о мультипликативности символа Дьюка–Хопкинс, применяя ее итеративно, получаем:

$$\left(\frac{a}{G}\right)_{\mathrm{DH}} = \left(\frac{a}{H_1 \times H_2 \times \cdots \times H_k}\right)_{\mathrm{DH}} = \prod_{i=1}^{k} \left(\frac{a}{H_i}\right)_{\mathrm{DH}}.$$

Так как $H_i \cong \mathbb{Z}_{m_i}$ и m_i – нечетное натуральное число, по лемме Золотарёва–Фробениуса (см. следствие 3) имеем:

$$\left(\frac{a}{H_i}\right)_{\mathrm{DH}} = \left(\frac{a}{\mathbb{Z}_{m_i}}\right)_{\mathrm{DH}} = \left(\frac{a}{m_i}\right).$$

Подставляя это в предыдущее выражение, получаем:

$$\left(\frac{a}{G}\right)_{\mathrm{DH}} = \prod_{i=1}^{k} \left(\frac{a}{m_i}\right).$$

Используя свойство полной мультипликативности символа Якоби по второму аргументу, находим:

$$\prod_{i=1}^{k} \left(\frac{a}{m_i}\right) = \left(\frac{a}{m_1 m_2 \cdots m_k}\right).$$

Поскольку $n = m_1 m_2 \cdots m_k$, окончательно получаем:

$$\left(\frac{a}{G}\right)_{\mathrm{DH}} = \left(\frac{a}{n}\right). \qquad \square$$

Это утверждение показывает, что хотя определение символа Дьюка–Хопкинс учитывает структуру группы, для конечных абелевых групп нечетного порядка его итоговое значение зависит только от порядка этой группы n (и числа a), а не от конкретного типа изоморфизма группы.

Этот исчерпывающий результат для конечных абелевых групп нечетного порядка естественно ставит вопрос: существует ли аналогичная простая связь для групп четного порядка? Первым кандидатом на обобщение символа Якоби является символ Кронекера, однако, как мы увидим, прямого аналога не наблюдается.

Проанализируем поведение символа $\left(\frac{m}{\mathbb{Z}_n}\right)_{\mathrm{DH}}$ для четного порядка n, где $m \in \mathbb{Z}$. Естественным объектом для сравнения выступает символ Кронекера $\left(\frac{m}{n}\right)$, который является обобщением символа Якоби и, в частности, определен для четных значений второго аргумента, включая $n = 2$.

Рассмотрим простейший случай четного порядка: $n = 2$. Символ Дьюка–Хопкинс $\left(\frac{m}{\mathbb{Z}_2}\right)_{\mathrm{DH}}$ для нечетных m постоянен и равен единице. С другой стороны, символ Кронекера $\left(\frac{m}{2}\right)$ для нечетных m определяется как $\left(\frac{m}{2}\right) = (-1)^{(m^2-1)/8}$.

Сравнение этих двух величин для $n = 2$ уже на начальном этапе выявляет существенное различие между $\left(\frac{m}{\mathbb{Z}_n}\right)_{\mathrm{DH}}$ и $\left(\frac{m}{n}\right)$ для нечетного целого m. Это наблюдение указывает на то, что ожидаемая аналогия между поведением символа Дьюка–Хопкинс для циклических групп четного порядка (в сопоставлении с символом Кронекера) и ранее установленной связью для групп нечетного порядка (с символом Якоби) не является прямой

и требует более детального изучения специфики четных порядков. Более того, оказывается, что для четного натурального числа n в общем случае символ $\left(\frac{m}{\mathbb{Z}_n}\right)_{\text{DH}}$ определяется только его значением для максимальной степени двойки, делящей n.

Предложение 16. *Пусть $n = 2^k t$, где $k \geq 1$, t – нечетное натуральное число, а $m \in \mathbb{Z}$ взаимно просто с n. Тогда*

$$\left(\frac{m}{\mathbb{Z}_n}\right)_{\text{DH}} = \left(\frac{m}{\mathbb{Z}_{2^k}}\right)_{\text{DH}}.$$

Доказательство. Поскольку $n = 2^k t$, где t – нечетное натуральное число, по китайской теореме об остатках группа $\mathbb{Z}_n$ изоморфна прямому произведению групп $\mathbb{Z}_{2^k} \times \mathbb{Z}_t$:

$$\mathbb{Z}_n \cong \mathbb{Z}_{2^k} \times \mathbb{Z}_t\,.$$

Перестановка $\varphi_m\colon x \mapsto mx \pmod n$ на $\mathbb{Z}_n$ индуцирует соответствующую перестановку на элементах $\mathbb{Z}_{2^k} \times \mathbb{Z}_t$. Если элемент $x \in \mathbb{Z}_n$ соответствует паре (x_1, x_2), где $x_1 \in \mathbb{Z}_{2^k}$ и $x_2 \in \mathbb{Z}_t$, то $mx \pmod n$ соответствует паре $\big(mx_1 \big(\mathrm{mod}\ 2^k\big), mx_2 \pmod t\big)$.

Обозначим через π_m перестановку $x_1 \mapsto mx_1\big(\mathrm{mod}\ 2^k\big)$ на $\mathbb{Z}_{2^k}$, а через σ_m – перестановку $x_2 \mapsto mx_2 \pmod t$ на $\mathbb{Z}_t$. По определению символа Дьюка–Хопкинс $\left(\frac{m}{\mathbb{Z}_{2^k}}\right)_{\text{DH}} = \operatorname{sgn}(\pi_m)$ и $\left(\frac{m}{\mathbb{Z}_t}\right)_{\text{DH}} = \operatorname{sgn}(\sigma_m)$. Согласно лемме 1 b), знак перестановки φ_m, действующей на прямом произведении $\mathbb{Z}_{2^k} \times \mathbb{Z}_t$, равен:

$$\left(\frac{m}{\mathbb{Z}_n}\right)_{\text{DH}} = \operatorname{sgn}(\varphi_m) = (\operatorname{sgn}(\pi_m))^t (\operatorname{sgn}(\sigma_m))^{2^k}.$$

Так как t – нечетное число, а 2^k – четное, имеем $(\operatorname{sgn}(\pi_m))^t = \operatorname{sgn}(\pi_m)$ и $(\operatorname{sgn}(\sigma_m))^{2^k} = 1$. Следовательно,

$$\left(\frac{m}{\mathbb{Z}_n}\right)_{\text{DH}} = \operatorname{sgn}(\pi_m) = \left(\frac{m}{\mathbb{Z}_{2^k}}\right)_{\text{DH}}. \qquad \square$$

2.2. Символ Хабличека–Мантиллы-Солера. Символ Дьюка–Хопкинс является обобщением подхода Золотарёва, зависящим только от классов сопряженности конечной группы. В работе [20] М. Хабличек и Г. Мантилла-Солер изучают "более прямое обобщение" подхода Золотарёва, рассматривая перестановку на элементах группы, индуцированную степенным отображением.

Определение 17 (символ Хабличека–Мантиллы-Солера)**.** Пусть G – конечная группа порядка n. Для целого числа a, взаимно простого с n, отображение $g \mapsto g^a$ индуцирует перестановку ρ_a на множестве элементов группы. Символ Хабличека–Мантиллы-Солера определяется как:

$$\left(\frac{a}{G}\right)_{\text{el}} = \begin{cases} \operatorname{sgn}(\rho_a), & \text{если } (a,n) = 1; \\ 0, & \text{если } (a,n) \neq 1. \end{cases}$$

Ясно, что в абелевом случае символы $\left(\frac{\cdot}{G}\right)_{\mathrm{DH}}$ и $\left(\frac{\cdot}{G}\right)_{\mathrm{el}}$ совпадают, а для неабелевых групп ситуация совершенно иная. Хабличек и Мантилла-Солер отмечают, что для групп S_3, S_4 (симметрические группы порядка 6 и 24), D_8 (диэдральная группа порядка 8) и Q_8 (группа кватернионов) символ Дьюка–Хопкинс тривиален. С другой стороны, вычисления показывают, что символ $\left(\frac{\cdot}{G}\right)_{\mathrm{el}}$ для этих групп нетривиален.

Однако Хабличеком и Мантиллой-Солером доказано, что символы $\left(\frac{\cdot}{G}\right)_{\mathrm{DH}}$ и $\left(\frac{\cdot}{G}\right)_{\mathrm{el}}$ совпадают для любой конечной группы нечетного порядка, даже если она неабелева. Для доказательства они вводят понятие сопряженно-эквивариантных отображений.

Определение 18 (сопряженно-эквивариантное отображение)**.** Пусть G – конечная группа. Инъективное отображение $f\colon G \to G$ называется сопряженно-эквивариантным, если для всех $x, g \in G$ выполняется равенство:

$$g^{-1}f(x)g = f(g^{-1}xg).$$

Множество всех сопряженно-эквивариантных отображений на G обозначается как $\mathrm{Sym}(G)^G$.

Заметим, что степенное отображение $\rho_a\colon g \mapsto g^a$ для $(a, |G|) = 1$ является примером сопряженно-эквивариантного отображения, так как $g^{-1}(x^a)g = (g^{-1}xg)^a$.

Любое сопряженно-эквивариантное отображение $f \in \mathrm{Sym}(G)^G$ индуцирует две перестановки:

1) перестановку $\rho_{\mathrm{el}}(f)$ на элементах группы G.

2) перестановку $\psi_{\mathcal{C}}(f)$ на множестве классов сопряженности G.

Их знаки порождают два гомоморфизма из $\mathrm{Sym}(G)^G$ в $\{-1, 1\}$, которые мы обозначим как $\left(\frac{f}{G}\right)_{\mathrm{El}}$ и $\left(\frac{f}{G}\right)_{\mathcal{C}}$ соответственно. В этих обозначениях $\left(\frac{a}{G}\right)_{\mathrm{el}} = \left(\frac{\rho_a}{G}\right)_{\mathrm{El}}$ и $\left(\frac{a}{G}\right)_{\mathrm{DH}} = \left(\frac{\rho_a}{G}\right)_{\mathcal{C}}$.

Ключевым результатом, связывающим эти два символа для групп нечетного порядка, является следующая

Теорема 19 (см. [20])**.** *Пусть G – конечная группа нечетного порядка. Тогда для любого сопряженно-эквивариантного отображения $f \in \mathrm{Sym}(G)^G$ справедливо равенство:*

$$\left(\frac{f}{G}\right)_{\mathrm{El}} = \left(\frac{f}{G}\right)_{\mathcal{C}}.$$

Доказательство. Пусть $f \in \mathrm{Sym}(G)^G$. Перестановка $\psi_{\mathcal{C}}(f)$ на множестве классов сопряженности разлагается в произведение независимых циклов. Рассмотрим один такой цикл

$\sigma = (C_1, C_2, \ldots, C_j)$. Обозначим через C_σ объединение элементов всех классов сопряженности, входящих в этот цикл: $C_\sigma = \bigcup_{i=1}^{j} C_i$.

Поскольку f сопряженно-эквивариантно, оно переводит классы сопряженности в классы сопряженности. Следовательно, f действует как биекция на множестве C_σ. Обозначим ограничение f на C_σ как f_σ. Тогда полная перестановка элементов $\rho_{\text{el}}(f)$ является произведением таких частичных перестановок f_σ по всем циклам σ в разложении $\psi_{\mathcal{C}}(f)$.

Таким образом, $\operatorname{sgn}(\rho_{\text{el}}(f)) = \prod_\sigma \operatorname{sgn}(f_\sigma)$. Для доказательства теоремы достаточно показать, что для каждого цикла σ выполняется равенство $\operatorname{sgn}(f_\sigma) = \operatorname{sgn}(\sigma)$.

Все классы сопряженности C_i в цикле σ имеют одинаковый размер, который мы обозначим $|C_1|$. Тогда мощность множества C_σ равна $|C_\sigma| = j|C_1|$.

Перестановка f_σ на множестве C_σ разлагается в произведение независимых циклов. Из сопряженной эквивариантности следует, что $f^m(g^{-1}xg) = g^{-1}f^m(x)g$. Значит, условие $f^a(x) = x$ равносильно $f^a(g^{-1}xg) = g^{-1}xg$, поэтому все элементы одного класса имеют циклы одинаковой длины. Поскольку f последовательно переставляет классы

$$C_1 \to C_2 \to \cdots \to C_j \to C_1,$$

эта длина совпадает для всех элементов C_σ. Обозначим ее за a. Элемент может вернуться в свой исходный класс сопряженности только за число шагов, кратное j, откуда $a = jk$ для некоторого целого k. Если в разложении f_σ ровно r таких циклов, то общее число элементов в C_σ равно $|C_\sigma| = ar = jkr$.

Сравнивая два выражения для $|C_\sigma|$, получаем $j|C_1| = jkr$, откуда следует, что $|C_1| = kr$. По условию порядок группы $|G|$ нечетен. Так как $|C_1|$ является делителем $|G|$, то $|C_1|$ также нечетно. Следовательно, числа k и r оба должны быть нечетными.

Теперь вычислим знак перестановки f_σ. Она состоит из r циклов длины $a = jk$. Знак такой перестановки равен

$$\operatorname{sgn}(f_\sigma) = ((-1)^{a-1})^r = ((-1)^{jk-1})^r.$$

Поскольку k и r нечетны, $jk-1$ имеет ту же четность, что и $j-1$, а возведение в нечетную степень r не меняет знак. Таким образом,

$$\operatorname{sgn}(f_\sigma) = (-1)^{j-1} = \operatorname{sgn}(\sigma).$$

Это равенство выполняется для каждого цикла σ в разложении $\psi_{\mathcal{C}}(f)$, что и завершает доказательство. □

Следствие 20. *Для любой конечной группы G нечетного порядка символы Дьюка–Хопкинс и Хабличека–Мантиллы-Солера совпадают:*

$$\left(\frac{a}{G}\right)_{\text{DH}} = \left(\frac{a}{G}\right)_{\text{el}}.$$

Доказательство. Рассмотрим степенное отображение $\rho_a\colon g \mapsto g^a$, где $(a, |G|) = 1$. Это отображение является сопряженно-эквивариантным. По определению, $\left(\frac{a}{G}\right)_{\mathrm{DH}} = \left(\frac{\rho_a}{G}\right)_{\mathcal{C}}$ и $\left(\frac{a}{G}\right)_{\mathrm{el}} = \left(\frac{\rho_a}{G}\right)_{\mathrm{El}}$. Поскольку $|G|$ нечетно, по теореме 19 имеем $\left(\frac{\rho_a}{G}\right)_{\mathcal{C}} = \left(\frac{\rho_a}{G}\right)_{\mathrm{El}}$. Отсюда и следует доказываемое равенство. □

Этот результат показывает, что для групп нечетного порядка, несмотря на различие в определениях (перестановка классов сопряженности и перестановка элементов), оба символа несут одинаковую информацию.

2.3. Квадратичный закон взаимности в конечной группе. Для формулировки закона взаимности для конечных групп, полученного в работе [19] У. Дьюка и К. Хопкинс, нам понадобится символ Кронекера. Он является естественным расширением символа Якоби на произвольные целые числа с сохранением его важнейшего свойства – бимультипликативности. Приведем формальное определение.

Определение 21 (символ Кронекера)**.** Пусть a и n – целые числа. Символ Кронекера $\left(\frac{a}{n}\right)$ определяется следующим образом:

1) Если $n = 0$, то
$$\left(\frac{a}{0}\right) = \begin{cases} 1, & \text{если } a = \pm 1; \\ 0, & \text{в противном случае.} \end{cases}$$

2) Если $n \neq 0$, пусть $n = u \cdot \prod\limits_{i=1}^{k} p_i^{e_i}$ – разложение n на простые множители, где $u = \pm 1$ – знак числа n, а p_i – простые числа. Тогда
$$\left(\frac{a}{n}\right) := \left(\frac{a}{u}\right) \prod_{i=1}^{k} \left(\left(\frac{a}{p_i}\right)\right)^{e_i}.$$

Здесь значения $\left(\frac{a}{u}\right)$ и $\left(\frac{a}{p_i}\right)$ определяются так:

- Для $u = -1$:
$$\left(\frac{a}{-1}\right) = \begin{cases} -1, & \text{если } a < 0; \\ 1, & \text{если } a \geq 0 \end{cases}$$
(для $u = 1$ множитель $\left(\frac{a}{1}\right)$ всегда равен 1 и не влияет на произведение).
- Для нечетного простого p: значение $\left(\frac{a}{p}\right)$ совпадает с символом Лежандра.

- Для $p = 2$:

$$\left(\frac{a}{2}\right) = \begin{cases} 0, & \text{если } a \text{ четно;} \\ (-1)^{\frac{a^2-1}{8}}, & \text{если } a \text{ нечетно.} \end{cases}$$

Важным свойством символа Кронекера, приведенным в следующем утверждении, является его мультипликативность по обоим аргументам. Это свойство непосредственно вытекает из приведенного выше определения.

Предложение 22 (бимультипликативность символа Кронекера)**.** *Для любых целых чисел* a, b, m, n *справедливы следующие равенства*:

1) *Мультипликативность по верхнему аргументу*:

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$

2) *Мультипликативность по нижнему аргументу* (*если* m *и* n *не равны нулю одновременно*):

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right).$$

Пусть G – конечная группа, а $C_1, \ldots, C_m$ – все ее попарно различные классы сопряженности, где $m = r_1 + 2r_2$. Упорядочим их таким образом, чтобы $C_1, \ldots, C_{r_1}$ были всеми классами сопряженности, для которых выполнено условие $C = C^{-1}$, так называемые вещественные классы, а оставшиеся $2r_2$ комплексных классов разбивались на пары взаимно обратных: $C_{r_1+i} = C^{-1}_{r_1+r_2+i}$ для каждого $1 \leq i \leq r_2$. Следуя работе [19], определим дискриминант $D(G)$ группы G согласно равенству:

$$D(G) = (-1)^{r_2} \prod_{j=1}^{r_1} \frac{|G|}{|C_j|}. \tag{1}$$

Заметим, что $D(G)$ – ненулевое целое число, так как для любого $g \in C_j$ отношение $|G|/|C_j|$ равно порядку централизатора $|C_G(g)|$ и, следовательно, является целым. Кроме того, $D(G)$ имеет те же простые делители, что и $|G|$.

Лемма 23. *Пусть* p *– простое число,* $\mathbb{F}$ *– алгебраически замкнутое поле,* G *– конечная группа, порядок которой обратим в поле* $\mathbb{F}$, *и*

$$A = \begin{pmatrix} \chi_1(C_1) & \cdots & \chi_1(C_m) \\ \vdots & \ddots & \vdots \\ \chi_m(C_1) & \cdots & \chi_m(C_m) \end{pmatrix},$$

где $\chi_1, \ldots, \chi_m$ *– все неприводимые характеры* $\mathbb{F}$*-представлений группы* G. *Тогда имеют место следующие утверждения*:

1) $|A|^2 = l^2 D(G)$, *где* $l = \prod\limits_{i=r_1+1}^{r_1+r_2} \frac{|G|}{|C_i|}$;

2) $D(G) \equiv 0 \pmod 4$, *если* G *– группа четного порядка, и* $D(G) \equiv 1 \pmod 4$, *если* G *– группа нечетного порядка;*

3) *если* $\mathbb{F}$ *– поле характеристики* p, *то*

$$|A|^p = \left(\frac{p}{G}\right)_{\mathrm{DH}} |A|;$$

4) *если* $\mathbb{F} = \mathbb{C}$ *и* $\zeta_n = e^{2\pi i/n}$, *где* $n = |G|$, *то*

$$|A|^p \equiv \left(\frac{p}{G}\right)_{\mathrm{DH}} |A| \pmod{p\mathbb{Z}[\zeta_n]}.$$

Доказательство. 1) Из соотношений ортогональности для неприводимых характеров следует матричное равенство:

$$\begin{pmatrix} \chi_1(C_1) & \cdots & \chi_1(C_m) \\ \vdots & \ddots & \vdots \\ \chi_m(C_1) & \cdots & \chi_m(C_m) \end{pmatrix} \begin{pmatrix} |C_1|\chi_1(C_1^{-1}) & \cdots & |C_1|\chi_m(C_1^{-1}) \\ \vdots & \ddots & \vdots \\ |C_m|\chi_1(C_m^{-1}) & \cdots & |C_m|\chi_m(C_m^{-1}) \end{pmatrix} = \begin{pmatrix} |G| & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & |G| \end{pmatrix}.$$

Переходя к определителям обеих частей, заметим, что вторая матрица получается из транспонированной матрицы A путем умножения ее i-й строки на $|C_i|$ и перестановки столбцов в соответствии с отображением $C_j \mapsto C_j^{-1}$. По определению символа Дьюка–Хопкинс знак этой перестановки равен $\left(\frac{-1}{G}\right)_{\mathrm{DH}}$. Следовательно, определитель второй матрицы равен $\left(\frac{-1}{G}\right)_{\mathrm{DH}} |C_1| \cdots |C_m|\,|A|$.

Из определения группового символа также вытекает, что $\left(\frac{-1}{G}\right)_{\mathrm{DH}} = (-1)^{r_2}$. Тогда получаем:

$$|A|^2 (-1)^{r_2} |C_1| \cdots |C_m| = |G|^m,$$

и, следовательно,

$$\begin{aligned} |A|^2 &= (-1)^{r_2} |G|^m \prod_{i=1}^{m} |C_i|^{-1} = (-1)^{r_2} |G|^m \prod_{j=1}^{r_1} |C_j|^{-1} \left(\prod_{i=r_1+1}^{r_1+r_2} |C_i|^{-1} \right)^2 \\ &= (-1)^{r_2} |G|^{r_1} \prod_{j=1}^{r_1} |C_j|^{-1} \left(|G|^{r_2} \prod_{i=r_1+1}^{r_1+r_2} |C_i|^{-1} \right)^2 = D(G) l^2. \end{aligned}$$

2) С помощью стандартных рассуждений, которые используются при доказательстве теоремы Штикельбергера о дискриминанте (см., например, [21, с. 15]), несложно показать, что $|A|^2 \equiv 0$ или $1 \pmod 4$. Тогда, если G – группа нечетного порядка, то $l^2 \equiv 1 \pmod 4$,

и, следовательно, согласно равенству из первого пункта $D(G) \equiv 1 \pmod 4$. Если G – группа четного порядка, то по теореме Коши G содержит элемент a порядка 2. Для класса сопряженности C, который содержит a, выполнено равенство $C = C^{-1}$. Тогда порядок централизатора элемента a входит в разложение (1) и делится на 2, поскольку этот централизатор содержит подгруппу второго порядка $\langle a \rangle$. Следовательно, так как порядок централизатора нейтрального элемента G, совпадающий с G, также входит в разложение (1) дискриминанта $D(G)$, то $D(G) \equiv 0 \pmod 4$.

3) Так как характеристика алгебраически замкнутого поля $\mathbb{F}$ равна p, то отображение возведения в степень p является автоморфизмом поля $\mathbb{F}$. Тогда для произвольного $g \in G$ и характера χ имеет место равенство $\chi(g)^p = \chi(g^p)$ и $|A|^p$ равен определителю матрицы, элементы которой суть $\chi_i(C_j^p)$. Эта матрица получается из матрицы A перестановкой столбцов, соответствующей отображению $C_j \mapsto C_j^p$. По определению символа Дьюка–Хопкинс знак этой перестановки равен $\left(\frac{p}{G}\right)_{\mathrm{DH}}$, поэтому:

$$|A|^p = \begin{vmatrix} \chi_1(C_1^p) & \cdots & \chi_1(C_m^p) \\ \vdots & \ddots & \vdots \\ \chi_m(C_1^p) & \cdots & \chi_m(C_m^p) \end{vmatrix} = \left(\frac{p}{G}\right)_{\mathrm{DH}} |A|.$$

4) Так как $(n, p) = 1$, существует однозначно определенный автоморфизм $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, для которого выполнено равенство $\sigma_p(\zeta_n) = \zeta_n^p$. Поскольку $\sigma_p(\chi(g)) = \chi(g^p)$, то

$$\sigma_p(|A|) = \left(\frac{p}{G}\right)_{\mathrm{DH}} |A|.$$

Ясно, что $|A|$ лежит в кольце целых $\mathbb{Z}[\zeta_n]$ поля $\mathbb{Q}(\zeta_n)$. Так как для любого элемента $\alpha \in \mathbb{Z}[\zeta_n]$ выполнено сравнение $\sigma_p(\alpha) \equiv \alpha^p \pmod{p\mathbb{Z}[\zeta_n]}$, получаем:

$$\sigma_p(|A|) \equiv |A|^p \pmod{p\mathbb{Z}[\zeta_n]},$$

и, следовательно,

$$\left(\frac{p}{G}\right)_{\mathrm{DH}} |A| \equiv |A|^p \pmod{p\mathbb{Z}[\zeta_n]}. \qquad \square$$

Приведем основной результат работы Дьюка и Хопкинс [19]:

Теорема 24 (квадратичный закон взаимности в конечной группе; [19])**.** *Пусть G – конечная группа с дискриминантом $D(G)$, определенным выше. Тогда $D(G) \equiv 0$ или $1 \pmod 4$, и для любого целого a справедливо равенство*:

$$\left(\frac{a}{G}\right)_{\mathrm{DH}} = \left(\frac{D(G)}{a}\right), \tag{2}$$

где справа стоит символ Кронекера. В частности, символ $\left(\frac{\cdot}{G}\right)$ *тривиален тогда и только тогда, когда* $D(G)$ *является квадратом целого числа.*

Доказательство. Пусть $|G| = n$. Если $(a, n) > 1$, то, очевидно, обе части равенства (2) равны нулю. Далее будем предполагать, что $(a, n) = 1$. Ввиду бимультипликативности символа Кронекера равенство (2) достаточно доказать в случае, когда либо a – простое число, либо $a = -1$. Предположим, что $a = p$ – простое число. Так как $(p, n) = 1$, то имеет место автоморфизм σ_p поля $\mathbb{Q}(\varepsilon_n)$, действующий согласно правилу $\varepsilon_n \mapsto \varepsilon_n^p$. Из определения символа Дьюка–Хопкинс, следует, что $\sigma_p(|A|) = \left(\frac{p}{G}\right)_{\mathrm{DH}} |A|$, где A матрица, рассмотренная в лемме 23. Тогда согласно лемме 23 1) $\mathbb{Q}\left(\sqrt{D(G)}\right)$ – подполе поля $\mathbb{Q}(\varepsilon_n)$ и имеет место равенство

$$\sigma_p\left(\sqrt{D(G)}\right) = \left(\frac{p}{G}\right)_{\mathrm{DH}} \sqrt{D(G)}. \tag{3}$$

Дискриминант $D(G)$ представим в виде $D(G) = d_0 t^2$, где $t \in \mathbb{N}$, а d_0 – бесквадратное целое число. Если $d_0 = 1$, то в силу равенства (3) имеем $\left(\frac{p}{G}\right)_{\mathrm{DH}} = \left(\frac{D(G)}{p}\right) = 1$. Таким образом, без ограничения общности можно считать, что $d_0 \neq 1$, т. е. $\sqrt{D(G)} \notin \mathbb{Q}$. Ясно, что σ_p является автоморфизмом Фробениуса соответствующим идеалу (p) кольца $\mathbb{Z}$. Согласно [22, теорема 68; свойство 2.2, с. 112] ограничение σ_p на $\mathbb{Q}\left(\sqrt{D(G)}\right)$ является тождественным автоморфизмом в точности тогда, когда простое число p разложимо по отношению к полю $\mathbb{Q}\left(\sqrt{D(G)}\right)$. Тогда согласно равенству (3) имеет место эквивалентность

$$\left(\frac{p}{G}\right)_{\mathrm{DH}} = 1 \quad \Leftrightarrow \quad p \text{ – разложимо по отношению к полю } \mathbb{Q}\left(\sqrt{D(G)}\right).$$

Если $p = 2$, то n – нечетное число и из леммы 23 1) следует, что $D(G) \equiv 1 \pmod 4$. Тогда из фундаментального свойства символа Кронекера [23, теорема 32, с. 356] следует, что для произвольного простого числа p, взаимно простого с n, имеет место эквивалентность

$$\left(\frac{D(G)}{p}\right) = 1 \quad \Leftrightarrow \quad p \text{ – разложимо по отношению к полю } \mathbb{Q}(\sqrt{D(G)}).$$

Таким образом, для произвольного простого числа p имеет место равенство $\left(\frac{p}{G}\right)_{\mathrm{DH}} = \left(\frac{D(G)}{p}\right)$. Равенство $\left(\frac{-1}{G}\right)_{\mathrm{DH}} = \left(\frac{D(G)}{-1}\right) = (-1)^{r_2}$ непосредственно следует из определений дискриминанта группы G и символов Кронекера и Дьюка–Хопкинс. □

В случае, когда группа G имеет нечетный порядок, получается прямое обобщение классической квадратичной взаимности:

Следствие 25. *Если* G *имеет нечетный порядок* n, *то* $D(G) = n^* = (-1)^{\frac{n-1}{2}} n$. *Для лю-*

бого целого числа a:

$$\left(\frac{a}{G}\right)_{\mathrm{DH}} = \left(\frac{n^*}{a}\right).$$

Кроме того, $(\frac{\cdot}{G})$ тривиально тогда и только тогда, когда n является квадратом целого числа.

Дьюк и Хопкинс доказали теорему 24 с использованием теории характеров и важных арифметических свойств числовых полей. Ниже рассмотрены два доказательства теоремы 24 в рамках теории характеров в случае, когда a – нечетное натуральное число. В первом доказательстве используются базовые факты из теории конечных полей, во втором – элементарная арифметика в кольцах целых циклотомических полей. Заметим, что, как будет показано ниже, этой версии теоремы 24 достаточно, чтобы доказать в качестве следствий классические квадратичные законы взаимности.

Теорема 26. *Пусть G – конечная группа порядка n, а a – нечетное натуральное число. Тогда*

$$\left(\frac{a}{G}\right)_{\mathrm{DH}} = \left(\frac{D(G)}{a}\right),$$

где справа стоит символ Якоби.

Первое доказательство [24]. В силу мультипликативности обоих символов по нижнему аргументу (соответственно, по числу a), достаточно показать, что для произвольного нечетного простого числа p, взаимно простого с n, имеет место равенство:

$$\left(\frac{p}{G}\right)_{\mathrm{DH}} = \left(\frac{D(G)}{p}\right).$$

Будем рассматривать все характеры группы G относительно представлений группы G над алгебраическим замыканием $\overline{\mathbb{F}}_p$ поля из p элементов. Так как $(n,p)=1$, то из леммы 23 1) следует, что $|A| \in \overline{\mathbb{F}}_p^*$. Также согласно лемме 23 1) имеет место эквивалентность

$$|A| \in \mathbb{F}_p \Leftrightarrow \left(\frac{D(G)}{p}\right) = 1.$$

С другой стороны, согласно лемме 23 2) справедливы эквивалентности

$$|A| \in \mathbb{F}_p \Leftrightarrow |A| = |A|^p \Leftrightarrow \left(\frac{p}{G}\right)_{\mathrm{DH}} = 1.$$

Поскольку значения символов могут быть равны только ± 1, получаем требуемое:

$$\left(\frac{p}{G}\right)_{\mathrm{DH}} = \left(\frac{D(G)}{p}\right). \qquad \square$$

Второе доказательство. Пусть p – простое нечетное число, взаимно простое с $|G|$. Будем рассматривать все характеры группы G относительно комплексных представлений. Ясно,

что $|A| \in \mathbb{Z}[\zeta_n]$, и из леммы 23 1) следует, что $|A|$ обратим по модулю идеала $p\mathbb{Z}[\zeta_n]$. Тогда из леммы 23 4) вытекает сравнение

$$\left(\frac{p}{G}\right)_{\mathrm{DH}} \equiv |A|^{p-1} \pmod{p\mathbb{Z}[\zeta_n]}.$$

С другой стороны, $|A|^{p-1} = \left(|A|^2\right)^{\frac{p-1}{2}} = \left(l^2 D(G)\right)^{\frac{p-1}{2}}$. Согласно критерию Эйлера имеют место сравнения

$$\left(l^2 D(G)\right)^{\frac{p-1}{2}} \equiv \left(\frac{l^2 D(G)}{p}\right) \equiv \left(\frac{D(G)}{p}\right) \pmod{p}.$$

Следовательно,

$$\left(\frac{p}{G}\right)_{\mathrm{DH}} \equiv \left(\frac{D(G)}{p}\right) \pmod{p\mathbb{Z}[\zeta_n]}.$$

Так как $\mathbb{Z} \cap p\mathbb{Z}[\zeta_n] = p\mathbb{Z}$, то

$$\left(\frac{p}{G}\right)_{\mathrm{DH}} \equiv \left(\frac{D(G)}{p}\right) \pmod{p}.$$

Наконец, поскольку $p > 2$, а разность значений символов может быть равна лишь $0, 2$ или -2, из сравнения по модулю p следует строгое равенство:

$$\left(\frac{p}{G}\right)_{\mathrm{DH}} = \left(\frac{D(G)}{p}\right). \qquad \square$$

Напомним, что лемма Золотарёва–Фробениуса в терминах символа Дьюка–Хопкинс выражается как:

$$\left(\frac{m}{\mathbb{Z}_n}\right)_{\mathrm{DH}} = \left(\frac{m}{n}\right),$$

где $n > 1$ – нечетное натуральное число, $m \in \mathbb{Z}$ и $(m, n) = 1$.

Первая публикация, содержащая доказательство леммы Золотарёва–Фробениуса, это статья М. Лерха 1896 года [18]. Авторский же вариант Фробениуса был опубликован лишь в 1914 году [17], хотя, согласно [15, с. 37], само обобщение было сделано им “немедленно” после ознакомления с работой Золотарёва. Фактически Лерх доказал более сильный результат:

Теорема 27 (М. Лерх, 1896 г., [18])**.** *Пусть $n > 1$ – натуральное число, $m \in \mathbb{Z}$.*

Если $(m, 2n) = 1$, то

$$\left(\frac{m}{\mathbb{Z}_{2n}}\right)_{\mathrm{DH}} = (-1)^{\frac{(m-1)(n-1)}{2}}.$$

Если n – нечетно и $(m, n) = 1$, то

$$\left(\frac{m}{\mathbb{Z}_n}\right)_{\mathrm{DH}} = \left(\frac{m}{n}\right).$$

Обобщение предыдущего результата на произвольные абелевы группы дает следующее утверждение.

Теорема 28 ([19])**.** *Пусть G – конечная абелева группа четного порядка n, а $G_2 = \{g \in G \mid g^2 = 1\}$ – ее подгруппа, состоящая из единицы и элементов порядка два. Обозначим порядок этой подгруппы через 2^t. Тогда для любого целого числа m, взаимно простого с n, справедливо равенство:*

$$\left(\frac{m}{G}\right)_{\mathrm{DH}} = \begin{cases} 1, & \text{если } n \equiv 2 \pmod 4 \text{ или } t > 1; \\ (-1)^{\frac{m-1}{2}}, & \text{если } n \equiv 0 \pmod 4 \text{ и } t = 1. \end{cases}$$

Доказательство. Вычислим дискриминант группы G. Количество вещественных классов совпадает с порядком подгруппы G_2. Остальные $n - 2^t$ элементов образуют комплексные классы, поэтому получаем

$$D(G) = (-1)^{\frac{n-2^t}{2}} n^{2^t}.$$

Согласно теореме 24 и свойствам символа Кронекера

$$\left(\frac{m}{G}\right)_{\mathrm{DH}} = \left(\frac{-1}{m}\right)^{\frac{n-2^t}{2}} \left(\frac{n^{2^t}}{m}\right) = \left(\frac{-1}{m}\right)^{\frac{n-2^t}{2}}.$$

Если $t > 1$, то так как подгруппа G_2 имеет порядок 2^t, то n делится на 4. Разность $n - 2^t$ является кратной 4, поэтому $\left(\frac{-1}{m}\right)^{\frac{n-2^t}{2}} = 1$ для любого m, взаимно простого с n.

Если $t = 1$, то подгруппа G_2 состоит только из единицы и единственного элемента порядка 2

$$\left(\frac{m}{G}\right)_{\mathrm{DH}} = \left(\frac{-1}{m}\right)^{\frac{n-2}{2}}.$$

Если $n \equiv 2 \pmod 4$, то $\dfrac{n-2}{2}$ – четное число. В этом случае $\left(\frac{-1}{m}\right)^{\frac{n-2}{2}} = 1$. Если $n \equiv 0 \pmod 4$, то $\frac{n-2}{2}$ – нечетное число. Символ Кронекера сводится к:

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}.$$

Отметим, что эта формула остается справедливой и для отрицательных m. □

Напомним, что согласно теореме 19 для конечных групп нечетного порядка символ $\left(\frac{\cdot}{G}\right)_{\mathrm{el}}$ совпадает с символом Дьюка–Хопкинс $\left(\frac{\cdot}{G}\right)_{\mathrm{DH}}$ и, следовательно, в этом случае для символа Хабличека–Мантиллы-Солера квадратичный закон взаимности выполняется в той же форме, как в теореме 24. Однако в случае групп четного порядка ситуация усложняется, так как перестановочная структура на элементах начинает проявлять более

высокую чувствительность к инволюциям, нежели структура классов сопряженности.

Для формулировки аналога закона взаимности М. Хабличек и Г. Мантилла-Солер [20] выделяют обширный класс конечных групп, удовлетворяющих одному из двух условий:

1) группа G представима в виде прямого произведения группы нечетного порядка и 2-группы;
2) группа G имеет порядок $2n$, где n нечетно, и все элементы четного порядка в ней являются инволюциями.

Заметим, что под эти условия автоматически подпадают все конечные нильпотентные группы, а также группы нечетного порядка. Главный результат авторов для данного класса формулируется следующим образом:

Теорема 29 (см. [20]). *Пусть конечная группа G удовлетворяет указанным выше условиям. Тогда для любого целого m, $(m, |G|) = 1$, справедливо равенство*:

$$\left(\frac{m}{G}\right)_{\text{el}} = \left(\frac{d_G}{m}\right),$$

где справа стоит символ Кронекера, а d_G – аналог дискриминанта группы, вычисляемый через количество решений уравнения $x^2 = 1$, обозначаемое как $|f_2(G)|$, и число силовских 2-подгрупп $n_2(G)$:

$$d_G := (-1)^{\frac{|G|-|f_2(G)|}{2}} \frac{|G|^{|f_2(G)|}}{n_2(G)^{\epsilon(G)}}.$$

Здесь $\epsilon(G)$ является индикаторной функцией, которая определяется структурным соотношением между порядком группы и количеством ее силовских 2-подгрупп:

$$\epsilon(G) = \begin{cases} 1, & \text{если } |G| = 2n_2(G); \\ 0, & \text{иначе.} \end{cases}$$

Авторы подчеркивают, что данные структурные требования к группе являются достаточными, но не необходимыми. Например, закон взаимности в форме $\left(\frac{m}{G}\right)_{\text{el}} = \left(\frac{d_G}{m}\right)$ выполняется для всех существующих групп порядка 24, хотя не все они удовлетворяют условиям теоремы. Более того, проведенный авторами компьютерный анализ всех 148 неизоморфных групп порядка не выше 35 показал, что исключение составляют всего четыре группы: две порядка 30, одна порядка 20 и одна порядка 18.

Для преодоления этих ограничений и построения общего закона взаимности для символа авторы разрабатывают комбинаторный метод – метод симметрических разностей на группах. Они доказывают, что любая конечная группа может быть единственным образом (с точностью до порядка) разложена в симметрическую разность своих циклических подгрупп. Ограничивая действие степенного отображения на эти подгруппы, они получают обобщение:

Теорема 30 (см. [20]). *Для любой конечной группы G существует такое целое число d_G^*, что для всех a, удовлетворяющих условию $(a, |G|) = 1$, выполняется*:

$$\left(\frac{a}{G}\right)_{\text{el}} = \left(\frac{d_G^*}{a}\right).$$

Здесь инвариант d_G^* определяется как произведение базовых инвариантов $d_{\langle g_i\rangle}$ для циклических подгрупп, составляющих редуцированное разложение группы G. Поиск явной и легко вычислимой формулы для d_G^* в общем случае остается открытой математической задачей. Для малых групп порядка < 36 авторы эмпирически устанавливают связь $d_G^* = n_2(G)^{v(G)} d_G$, где $v(G) \in \{0, 1\}$.

3. Приложение к классическому квадратичному закону взаимности

3.1. Приложения к закону взаимности для символа Якоби. Первое доказательство теоремы 26, примененное к случаю, когда G – циклическая группа нечетного порядка, дает короткое доказательство квадратичного закона взаимности для символа Якоби.

Пусть p – простое нечетное число, $m > 1$ – нечетное натуральное число, взаимно простое с p, а $\varepsilon \in \overline{\mathbb{F}}_p$ – примитивный корень степени m из единицы. Положим

$$A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \varepsilon & \dots & \varepsilon^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \varepsilon^{m-1} & \dots & \varepsilon^{(m-1)^2} \end{pmatrix}. \tag{4}$$

Рассмотрим произведение матриц:

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \varepsilon & \dots & \varepsilon^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \varepsilon^{m-1} & \dots & \varepsilon^{(m-1)^2} \end{pmatrix} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \varepsilon^{-1} & \dots & \varepsilon^{-(m-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \varepsilon^{-(m-1)} & \dots & \varepsilon^{-(m-1)^2} \end{pmatrix} = \begin{pmatrix} m & 0 & \dots & 0 \\ 0 & m & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & m \end{pmatrix}.$$

Переходя к определителям обеих частей и учитывая лемму Золотарёва–Фробениуса получаем следующие равенства:

$$\left(|A|\, m^{-\frac{m-1}{2}}\right)^2 = (-1)^{\frac{m-1}{2}} m, \tag{5}$$

$$|A|^p = \left(\frac{p}{m}\right)|A|. \tag{6}$$

Из равенства (5) следует эквивалентность:

$$|A| \in \mathbb{F}_p \quad \Leftrightarrow \quad \left(\frac{(-1)^{\frac{m-1}{2}}m}{p}\right) = 1.$$

С другой стороны, принадлежность элемента $|A|$ полю $\mathbb{F}_p$ равносильна тому факту, что он является корнем уравнения $x^p = x$. Следовательно, из равенства (6) следует эквивалентность:

$$|A| \in \mathbb{F}_p \quad \Leftrightarrow \quad |A| = |A|^p \quad \Leftrightarrow \quad \left(\frac{p}{m}\right) = 1.$$

Таким образом, имеет место равенство

$$\left(\frac{p}{m}\right) = \left(\frac{(-1)^{\frac{m-1}{2}}m}{p}\right).$$

Квадратичный закон взаимности для символа Якоби теперь непосредственно следует из свойства бимультипликативности этого символа.

Отметим, что изложение первого доказательства теоремы 26 и ее специального случая, приведенного выше, основано на работе [24].

3.2. Приложения к закону взаимности для символа Кронекера. В данном подразделе мы докажем квадратичный закон взаимности для символа Кронекера. Для этого нам потребуется выразить символ Кронекера в терминах групповых символов.

Предложение 31. *Пусть Q_{16} – группа обобщенных кватернионов порядка* 16. *Тогда для любого целого числа a справедливо равенство:*

$$\left(\frac{a}{Q_{16}}\right)_{\mathrm{DH}} = \left(\frac{a}{2}\right).$$

Доказательство. По определению символа Дьюка–Хопкинс, квадратичный символ $\left(\frac{a}{G}\right)_{\mathrm{DH}}$ для целого числа a, взаимно простого с порядком группы n, равен знаку перестановки классов сопряженности группы G, индуцированной возведением элементов в степень a. Если $(a, n) \neq 1$, то символ равен нулю.

Рассмотрим группу обобщенных кватернионов Q_{16} порядка $n = 16$. Зададим ее стандартным копредставлением:

$$Q_{16} = \langle x, y \mid x^8 = 1,\ y^2 = x^4,\ y^{-1}xy = x^{-1}\rangle.$$

Если a – четное число, то $(a, 16) \neq 1$, и по определению $\left(\frac{a}{Q_{16}}\right)_{\mathrm{DH}} = 0$. С другой стороны, по определению символа Кронекера для четного a имеем $\left(\frac{a}{2}\right) = 0$. В этом случае равенство выполняется.

Пусть теперь a – нечетное число. Найдем классы сопряженности Q_{16}. Всего их $m = 7$:

$$C_1 = \{1\}, \quad C_2 = \{x^4\},$$
$$C_3 = \{x, x^7\}, \quad C_4 = \{x^2, x^6\}, \quad C_5 = \{x^3, x^5\},$$
$$C_6 = \{y, x^2y, x^4y, x^6y\}, \quad C_7 = \{xy, x^3y, x^5y, x^7y\}.$$

Порядок элемента x равен 8. Для элементов вида x^ky их квадрат равен

$$\left(x^ky\right)^2 = x^kyx^ky = x^kx^{-k}y^2 = x^4$$

(поскольку $yx^k = x^{-k}y$), следовательно, их порядок равен 4. Таким образом, отображение $g \mapsto g^a$ полностью определяется остатком от деления a на 8. Рассмотрим 4 возможных случая для нечетного $a \pmod 8$:

1) $a \equiv 1 \pmod 8$**:**
   Отображение $g \mapsto g$ оставляет все классы на своих местах. Следовательно, перестановка является тождественной, и $\left(\dfrac{a}{Q_{16}}\right)_{\text{DH}} = 1$.
2) $a \equiv 3 \pmod 8$**:**
   Возведение в куб дает следующие переходы:

   $$C_3 \to \{x^3, x^{21}\} = C_5, \quad C_4 \to \{x^6, x^{18}\} = C_4, \quad C_5 \to \{x^9, x^{15}\} = C_3.$$

   Для классов C_6 и C_7 элементы остаются внутри своих классов. Перестановка является одной транспозицией ($C_3 \leftrightarrow C_5$) – это нечетная перестановка, поэтому $\left(\dfrac{a}{Q_{16}}\right)_{\text{DH}} = -1$.
3) $a \equiv 5 \pmod 8$**:**
   Возведение в 5-ю степень дает:

   $$C_3 \to \{x^5, x^{35}\} = C_5, \quad C_5 \to \{x^{15}, x^{25}\} = C_3.$$

   Элементы из C_6 и C_7 имеют порядок 4, поэтому $g^5 = g^4g = g$, и они остаются на своих местах. Снова получаем ровно одну транспозицию ($C_3 \leftrightarrow C_5$), значит $\left(\dfrac{a}{Q_{16}}\right)_{\text{DH}} = -1$.
4) $a \equiv 7 \pmod 8 \equiv -1 \pmod 8$**:**
   Переход к обратным элементам дает:

   $$C_3 \to \{x^{-1}, x^{-7}\} = \{x^7, x\} = C_3, \quad C_5 \to C_5.$$

   Для C_6 и C_7 имеем $(x^ky)^{-1} = y^{-1}x^{-k} = x^4yx^{-k} = x^{k+4}y$. Поскольку числа k и $k+4$

имеют одинаковую четность, элементы класса C_6 переходят в элементы C_6, а элементы C_7 – в элементы C_7. Все классы переходят в себя, перестановка тождественная, $\left(\dfrac{a}{Q_{16}}\right)_{\mathrm{DH}} = 1$.

Итак, мы получили, что:

$$\left(\frac{a}{Q_{16}}\right)_{\mathrm{DH}} = \begin{cases} 1, & \text{если } a \equiv \pm 1 \pmod 8; \\ -1, & \text{если } a \equiv \pm 3 \pmod 8. \end{cases}$$

Теперь обратимся к определению символа Кронекера для нечетного a:

$$\left(\frac{a}{2}\right) = (-1)^{\frac{a^2-1}{8}}.$$

Оба символа полностью совпадают на всех целых числах a, что и требовалось доказать. □

Замечание 32. Аналогичный результат достигается для диэдральной группы D_{16} порядка 16:

$$\left(\frac{a}{D_{16}}\right)_{\mathrm{DH}} = \left(\frac{a}{2}\right).$$

Лемма 33. *Пусть a, b – целые ненулевые числа. Тогда:*

$$\left(\frac{a}{\mathrm{sgn}(b)}\right) = (-1)^{\frac{\mathrm{sgn}(a)-1}{2}\cdot\frac{\mathrm{sgn}(b)-1}{2}}.$$

Доказательство. Если $b > 0$, то $\mathrm{sgn}(b) = 1$, и по определению символа Кронекера $\left(\dfrac{a}{1}\right) = 1$. В правой части формулы показатель степени содержит множитель $\dfrac{\mathrm{sgn}(b)-1}{2} = 0$, поэтому она также равна $(-1)^0 = 1$. Левая и правая части совпадают.

Если $b < 0$, то $\mathrm{sgn}(b) = -1$. Левая часть принимает вид $\left(\dfrac{a}{-1}\right)$, что по определению равно 1 при $a > 0$ и -1 при $a < 0$. В правой части множитель $\dfrac{\mathrm{sgn}(b)-1}{2} = \dfrac{-1-1}{2} = -1$. Тогда правая часть принимает вид:

$$(-1)^{-\frac{\mathrm{sgn}(a)-1}{2}}.$$

Если $a > 0$, то $\mathrm{sgn}(a) = 1$, и показатель степени равен 0, что дает $(-1)^0 = 1$. Если $a < 0$, то $\mathrm{sgn}(a) = -1$, и показатель степени равен 1, что дает $(-1)^1 = -1$.

В обоих случаях результат формулы в точности совпадает со значением $\left(\dfrac{a}{-1}\right)$ из определения. □

Теорема 34 (закон взаимности для символа Кронекера)**.** *Пусть a, b – любые ненулевые целые числа. Представим их в виде $a = \operatorname{sgn}(a)2^{\alpha}a_1$ и $b = \operatorname{sgn}(b)2^{\beta}b_1$, где $\alpha, \beta \geq 0$, а a_1, b_1 – натуральные нечетные числа. Тогда*

$$\left(\frac{a}{b}\right) = (-1)^{\frac{a_1-1}{2}\cdot\frac{b_1-1}{2}+\frac{\operatorname{sgn}(a)-1}{2}\cdot\frac{b_1-1}{2}+\frac{a_1-1}{2}\cdot\frac{\operatorname{sgn}(b)-1}{2}}\left(\frac{b}{a}\right).$$

Доказательство. Если $(a, b) > 1$, то по определению символа Кронекера $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) = 0$, и требуемое равенство выполняется. Поэтому далее без ограничения общности считаем, что a и b взаимно просты.

По свойству мультипликативности символа Кронекера:

$$\left(\frac{a}{b}\right) = \left(\frac{a}{\operatorname{sgn}(b)}\right)\cdot\left(\frac{a}{2}\right)^{\beta}\cdot\left(\frac{a}{b_1}\right).$$

Согласно предложению 31, лемме 33 и в силу того, что символ Якоби выражается через групповой символ $\left(\frac{a}{b_1}\right) = \left(\frac{a}{\mathbb{Z}_{b_1}}\right)_{\text{DH}}$, получим:

$$\left(\frac{a}{b}\right) = (-1)^{\frac{\operatorname{sgn}(a)-1}{2}\cdot\frac{\operatorname{sgn}(b)-1}{2}}\cdot\left(\frac{a}{Q_{16}}\right)^{\beta}_{\text{DH}}\cdot\left(\frac{a}{\mathbb{Z}_{b_1}}\right)_{\text{DH}}.$$

Воспользуемся теоремой Дьюка–Хопкинс для групповых символов:

$$\left(\frac{a}{b}\right) = (-1)^{\frac{\operatorname{sgn}(a)-1}{2}\cdot\frac{\operatorname{sgn}(b)-1}{2}}\cdot\left(\frac{D(Q_{16})}{a}\right)^{\beta}\cdot\left(\frac{D(\mathbb{Z}_{b_1})}{a}\right).$$

Известно, что $D(\mathbb{Z}_{b_1}) = (-1)^{\frac{b_1-1}{2}}b_1$. Вычислим дискриминант группы обобщенных кватернионов Q_{16}:

$$D(Q_{16}) = (-1)^0\cdot 16^7\cdot\frac{1}{1\cdot 1\cdot 2\cdot 2\cdot 2\cdot 4\cdot 4} = 2^{21}.$$

Тогда

$$\left(\frac{D(Q_{16})}{a}\right) = \left(\frac{2^{21}}{a}\right) = \left(\frac{2}{a}\right).$$

Подставим получившиеся выражения в исходное произведение:

$$\left(\frac{a}{b}\right) = (-1)^{\frac{\operatorname{sgn}(a)-1}{2}\cdot\frac{\operatorname{sgn}(b)-1}{2}}\cdot\left(\frac{2^{\beta}}{a}\right)\cdot\left(\frac{(-1)^{\frac{b_1-1}{2}}}{a}\right)\cdot\left(\frac{b_1}{a}\right).$$

Заметим, что $2^\beta b_1 = \mathrm{sgn}(b)b$, и, пользуясь мультипликативностью, получим:

$$\left(\frac{a}{b}\right) = (-1)^{\frac{\mathrm{sgn}(a)-1}{2}\cdot\frac{\mathrm{sgn}(b)-1}{2}} \cdot \left(\frac{(-1)^{\frac{b_1-1}{2}}}{a}\right) \cdot \left(\frac{\mathrm{sgn}(b)}{a}\right) \cdot \left(\frac{b}{a}\right).$$

Преобразуем первые множители, содержащие a в нижней части:

$$\left(\frac{(-1)^{\frac{b_1-1}{2}}}{a}\right) \cdot \left(\frac{\mathrm{sgn}(b)}{a}\right) = \left(\frac{-1}{a}\right)^{\frac{b_1-1}{2}} \cdot \left(\frac{-1}{a}\right)^{\frac{\mathrm{sgn}(b)-1}{2}} = \left(\frac{-1}{a}\right)^{\frac{b_1-1}{2}+\frac{\mathrm{sgn}(b)-1}{2}}.$$

Отдельно рассмотрим значение $\left(\frac{-1}{a}\right)$:

$$\left(\frac{-1}{a}\right) = \left(\frac{-1}{\mathrm{sgn}(a)}\right) \cdot \left(\frac{-1}{2}\right)^{\alpha} \cdot \left(\frac{-1}{a_1}\right).$$

Пользуясь леммой 33 и свойством символа Якоби $\left(\frac{-1}{a_1}\right)$, получим

$$\left(\frac{-1}{a}\right) = (-1)^{\frac{\mathrm{sgn}(a)-1}{2}\cdot\frac{-1-1}{2}} \cdot 1^\alpha \cdot (-1)^{\frac{a_1-1}{2}} = (-1)^{\frac{\mathrm{sgn}(a)-1}{2}+\frac{a_1-1}{2}}.$$

Подставляя это обратно, находим показатель степени при -1:

$$\left(\frac{\mathrm{sgn}(a)-1}{2} + \frac{a_1-1}{2}\right)\left(\frac{b_1-1}{2} + \frac{\mathrm{sgn}(b)-1}{2}\right).$$

Раскрывая скобки и складывая с начальным множителем $\frac{\mathrm{sgn}(a)-1}{2}\cdot\frac{\mathrm{sgn}(b)-1}{2}$ (учитывая, что по модулю 2 знак слагаемого не важен), исходное произведение примет вид

$$\left(\frac{a}{b}\right) = (-1)^{\frac{a_1-1}{2}\cdot\frac{b_1-1}{2}+\frac{\mathrm{sgn}(a)-1}{2}\cdot\frac{b_1-1}{2}+\frac{a_1-1}{2}\cdot\frac{\mathrm{sgn}(b)-1}{2}}\left(\frac{b}{a}\right),$$

что и требовалось доказать. □

3.3. Шестое доказательство Гаусса квадратичного закона. Определитель Вандермонда находит применение в различных доказательствах закона квадратичной взаимности (см., например, [25–29]). В данном подразделе мы исследуем тесную связь между доказательствами квадратичной взаимности, опирающимися на свойства определителя Вандермонда, и классическими методами, использующими квадратичные суммы Гаусса.

Пусть p – нечетное простое число, $\zeta = e^{\frac{2\pi i}{p}}$ – примитивный корень p-й степени из единицы, а $\chi\colon \mathbb{F}_p^* \to \mathbb{C}^*$ – характер мультипликативной группы поля $\mathbb{F}_p$. Из теории характеров конечных групп известно, что группа мультипликативных характеров является цикли-

ческой группой порядка $p-1$ относительно операции поточечного умножения. Введем в рассмотрение матрицу Вандермонда V и вектор-столбец значений характера $\boldsymbol{\chi}$:

$$V = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta^1 & (\zeta^1)^2 & \dots & (\zeta^1)^{p-1} \\ 1 & \zeta^2 & (\zeta^2)^2 & \dots & (\zeta^2)^{p-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{p-1} & (\zeta^{p-1})^2 & \dots & (\zeta^{p-1})^{p-1} \end{pmatrix}, \quad \boldsymbol{\chi} = \begin{pmatrix} 0 \\ \chi(1) \\ \chi(2) \\ \vdots \\ \chi(p-1) \end{pmatrix} = \Big(0, \ \ \chi(1), \ \ \dots, \ \ \chi(p-1)\Big)^T.$$

По своей сути матрица V является таблицей характеров аддитивной группы поля $\mathbb{F}_p$, а вектор $\boldsymbol{\chi}$ состоит из значений характера мультипликативной группы с добавлением нуля на первой позиции.

В работе К. Мотосе [27] важные свойства сумм Гаусса были получены на основе изучения связей между матрицей V и вектор-столбцами вида $\boldsymbol{\chi}$. Отметим, что в указанной работе для анализа сумм Гаусса использовалась усеченная матрица характеров размера $(p-1)\times(p-1)$, индексы которой пробегали только по ненулевым элементам поля.

Напомним, что для произвольного характера $\chi\colon \mathbb{F}_p^* \to \mathbb{C}^*$ *сумма Гаусса* определяется равенством

$$\tau_\chi := \sum_{k=1}^{p-1} \chi(k)\zeta^k.$$

Если в качестве характера χ выбрать символ Лежандра $\left(\frac{\cdot}{p}\right)$, мы приходим к понятию *квадратичной суммы Гаусса*:

$$\tau_p := \tau_{\left(\frac{\cdot}{p}\right)} = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k.$$

Лемма 35. *Пусть χ – некоторый нетривиальный характер мультипликативной группы поля $\mathbb{F}_p$, а $\overline{\chi}$ – сопряженный ему характер. Тогда*

1) $V\boldsymbol{\chi} = \tau_\chi \overline{\boldsymbol{\chi}}$;
2) $V^2\boldsymbol{\chi} = \tau_\chi \tau_{\overline{\chi}} \boldsymbol{\chi}$;
3) $\tau_\chi \tau_{\overline{\chi}} = p\chi(-1)$. *В частности, для квадратичной суммы Гаусса имеет место равенство:*

$$\tau_p^2 = (-1)^{\frac{p-1}{2}} p. \tag{7}$$

Доказательство. Будем индексировать строки и столбцы матриц от 0 до $p-1$. Тогда j,k-я компонента матрицы V имеет вид $V_{j,k} = \zeta^{jk}$.

1) Для каждого $j \in \{1,\dots,p-1\}$ имеет место равенство:

$$(V\boldsymbol{\chi})_j = \sum_{k=0}^{p-1} V_{j,k}\boldsymbol{\chi}_k = \sum_{k=1}^{p-1} \chi(k)\zeta^{jk}.$$

Сделаем замену переменной $m = jk \pmod p$. Поскольку $j \not\equiv 0 \pmod p$, при пробегании k всех ненулевых элементов поля индекс m также пробегает все ненулевые элементы. Учитывая, что $k \equiv j^{-1}m \pmod p$, получаем

$$\sum_{m=1}^{p-1} \chi(j^{-1}m)\zeta^m = \chi(j^{-1}) \sum_{m=1}^{p-1} \chi(m)\zeta^m = \overline{\chi}(j)\tau_\chi = (\tau_\chi \overline{\boldsymbol{\chi}})_j.$$

Если же $j = 0$, то, так как сумма нетривиального характера по всей группе равна нулю, имеем

$$(V\boldsymbol{\chi})_0 = \sum_{k=1}^{p-1} \chi(k) = 0 = (\tau_\chi \overline{\boldsymbol{\chi}})_0.$$

Таким образом, $V\boldsymbol{\chi} = \tau_\chi \overline{\boldsymbol{\chi}}$.

2) Согласно первому пункту, применяя матрицу V дважды, получаем

$$V^2\boldsymbol{\chi} = V(V\boldsymbol{\chi}) = V(\tau_\chi \overline{\boldsymbol{\chi}}) = \tau_\chi (V\overline{\boldsymbol{\chi}}) = \tau_\chi \tau_{\overline{\chi}} \boldsymbol{\chi}.$$

3) Вычислим элементы матрицы V^2:

$$(V^2)_{j,l} = \sum_{k=0}^{p-1} V_{j,k}V_{k,l} = \sum_{k=0}^{p-1} \zeta^{jk}\zeta^{kl} = \sum_{k=0}^{p-1} \zeta^{k(j+l)} = \begin{cases} p, & \text{если } j \equiv -l \pmod p; \\ 0, & \text{если } j \not\equiv -l \pmod p. \end{cases}$$

Тогда j-я компонента вектора $V^2\boldsymbol{\chi}$ равна:

$$(V^2\boldsymbol{\chi})_j = \sum_{l=0}^{p-1} (V^2)_{j,l}\boldsymbol{\chi}_l = \begin{cases} 0, & \text{если } j = 0; \\ p\chi(-j), & \text{если } j > 0. \end{cases}$$

Поскольку $p\chi(-j) = p\chi(-1)\chi(j)$, можно записать это в векторном виде:

$$V^2\boldsymbol{\chi} = p\chi(-1)\boldsymbol{\chi}.$$

Сопоставляя это с результатом второго пункта, имеем

$$\tau_\chi \tau_{\overline{\chi}} \boldsymbol{\chi} = p\chi(-1)\boldsymbol{\chi}.$$

Поскольку $\boldsymbol{\chi}$ – ненулевой вектор, отсюда следует, что

$$\tau_\chi \tau_{\overline{\chi}} = p\chi(-1).$$

Наконец, для вывода равенства (7) применим этот результат к символу Лежандра $\chi = \left(\frac{\cdot}{p}\right)$. Так как этот характер принимает только действительные значения ± 1, он

совпадает со своим сопряженным: $\overline{\chi} = \chi$. Кроме того, $\chi(-1) = \left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Следовательно, $\tau_p^2 = (-1)^{\frac{p-1}{2}} p$. □

В работе [27] лемма 35 лежит в основе доказательства квадратичного закона взаимности, приведенного ниже. Рассмотрим вектор $\boldsymbol{\eta} = (0, \eta(1), \ldots, \eta(p-1))^T$, где $\eta(k) = \left(\dfrac{k}{p}\right)$ – символ Лежандра. Поскольку символ Лежандра принимает только вещественные значения, сопряженный вектор $\overline{\boldsymbol{\eta}}$ совпадает с $\boldsymbol{\eta}$. Тогда, согласно лемме 35, для вектора $\boldsymbol{\eta}$ имеют место равенства:

$$V\boldsymbol{\eta} = \tau_p \boldsymbol{\eta}, \qquad V^2\boldsymbol{\eta} = p\eta(-1)\boldsymbol{\eta} = p(-1)^{\frac{p-1}{2}}\boldsymbol{\eta}. \tag{8}$$

Пусть q – нечетное простое число, отличное от p. Рассмотрим действие оператора V^{q-1} на вектор $\boldsymbol{\eta}$ в кольце $\mathbb{Z}[\zeta]$ по модулю идеала $q\mathbb{Z}[\zeta]$. Вычислим этот результат двумя способами.

С одной стороны, имеют место равенства:

$$V^{q-1}\boldsymbol{\eta} = (V^2)^{\frac{q-1}{2}}\boldsymbol{\eta} = \left(p(-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}}\boldsymbol{\eta} = p^{\frac{q-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\boldsymbol{\eta}.$$

Так как, согласно критерию Эйлера, $p^{\frac{q-1}{2}} \equiv \left(\dfrac{p}{q}\right) \pmod q$, получаем

$$V^{q-1}\boldsymbol{\eta} \equiv \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\boldsymbol{\eta} \pmod{q\mathbb{Z}[\zeta]}. \tag{9}$$

Здесь под сравнением векторов $\mathbf{a} \equiv \mathbf{b} \pmod{q\mathbb{Z}[\zeta]}$ понимается покомпонентное сравнение их элементов.

С другой стороны, возведем сумму Гаусса τ_p в степень q:

$$\tau_p^q = \left(\sum_{k=1}^{p-1}\eta(k)\zeta^k\right)^q \equiv \sum_{k=1}^{p-1}\eta(k)^q\zeta^{qk} \pmod{q\mathbb{Z}[\zeta]}.$$

Поскольку $\eta(k) \in \{\pm 1\}$ и q нечетно, $\eta(k)^q = \eta(k)$. Учитывая, что $\eta(q)^2 = 1$, преобразуем сумму:

$$\sum_{k=1}^{p-1}\eta(k)\zeta^{qk} = \eta(q)\sum_{k=1}^{p-1}\eta(q)\eta(k)\zeta^{qk} = \eta(q)\sum_{k=1}^{p-1}\eta(qk)\zeta^{qk}.$$

Поскольку $(q,p) = 1$, при пробегании k всех ненулевых вычетов по модулю p индекс qk также пробегает все ненулевые вычеты. Следовательно, эта сумма в точности равна τ_p, откуда

$$\tau_p^q \equiv \left(\frac{q}{p}\right)\tau_p \pmod{q\mathbb{Z}[\zeta]}. \tag{10}$$

Так как p и q – различные простые числа, p обратимо по модулю q. Поскольку $\tau_p^2 = (-1)^{\frac{p-1}{2}} p$, элемент τ_p обратим по модулю идеала $q\mathbb{Z}[\zeta]$. Разделив обе части сравнения (10) на τ_p, получаем

$$\tau_p^{q-1} \equiv \left(\frac{q}{p}\right) \pmod{q\mathbb{Z}[\zeta]}.$$

Поскольку, согласно равенствам (8), вектор $\boldsymbol{\eta}$ является собственным для матрицы V с собственным значением τ_p, справедливо равенство $V^{q-1}\boldsymbol{\eta} = \tau_p^{q-1}\boldsymbol{\eta}$. Отсюда

$$V^{q-1}\boldsymbol{\eta} \equiv \left(\frac{q}{p}\right)\boldsymbol{\eta} \pmod{q\mathbb{Z}[\zeta]}. \tag{11}$$

Приравнивая результаты (9) и (11), получаем векторное сравнение:

$$\left(\frac{q}{p}\right)\boldsymbol{\eta} \equiv \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\boldsymbol{\eta} \pmod{q\mathbb{Z}[\zeta]}.$$

Рассматривая любую ненулевую компоненту вектора $\boldsymbol{\eta}$ (например, первую, где $\eta(1) = 1$), приходим к скалярному сравнению:

$$\left(\frac{q}{p}\right) \equiv \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \pmod{q\mathbb{Z}[\zeta]},$$

и, следовательно,

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Далее рассмотрим связи между определителем Вандермонда $|V|$ и квадратичной суммой Гаусса. Согласно равенству (5), имеем:

$$|V|^2 = (-1)^{\frac{p-1}{2}} p^p. \tag{12}$$

Следовательно, из равенства (7) вытекает, что

$$|V| p^{-\frac{p-1}{2}} = \pm\tau_p. \tag{13}$$

Тогда равенство (12) и сравнение

$$|V|^p \equiv \left(\frac{p}{q}\right)|V| \pmod{q\mathbb{Z}[\zeta_n]},$$

которое следует из леммы 23 3), с одной стороны, и равенство (7) и сравнение

$$\tau_p^q \equiv \left(\frac{q}{p}\right)\tau_p \pmod{q\mathbb{Z}[\zeta]}, \tag{14}$$

с другой, несложно выводятся друг из друга.

Проблема определения знака в формуле (13) тесно связана с одной из знаменитых классических задач теории чисел – вычислением точного значения квадратичной суммы Гаусса. Классические решения этой задачи, как правило, весьма нетривиальны. К.Ф. Гаусс решал ее в течение четырех лет. В 2003 году Каору Мотосе в своей работе [27] предложил исключительно изящный чисто алгебраический подход. Мотосе показал, что как сам квадратичный закон взаимности, так и точное значение квадратичной суммы Гаусса могут быть элегантно выведены через исследование определителя матрицы Вандермонда, построенной на корнях из единицы.

Пусть $\boldsymbol{e}_0 = \Big(1, \ \ 0, \ \ \ldots, \ \ 0\Big)^T$ и χ_* – образующий характер циклической группы характеров поля $\mathbb{F}_p^*$. Для каждого $0 \le k \le \dfrac{p-3}{2}$ вектор-столбец $\Big(0, \ \ \chi_*^k(1), \ \ \ldots, \ \ \chi_*^k(p-1)\Big)^T$ обозначим через $\boldsymbol{\chi}_k$.

Используя лемму 35, выпишем матрицу линейного оператора $\boldsymbol{A}$, действующего в векторном пространстве векторов-столбцов $\mathbb{F}_p^p$ согласно правилу $\boldsymbol{x} \mapsto V\boldsymbol{x}$, относительно базиса

$$\boldsymbol{e}_0, \ \boldsymbol{\chi}_0, \ \boldsymbol{\chi}_{\frac{p-1}{2}}, \ \boldsymbol{\chi}_1, \ \overline{\boldsymbol{\chi}}_1, \ \ldots, \ \boldsymbol{\chi}_{\frac{p-3}{2}}, \ \overline{\boldsymbol{\chi}}_{\frac{p-3}{2}}. \tag{15}$$

Имеют место равенства

$$V\boldsymbol{e}_0 = \Big(1, \ \ 1, \ \ 1, \ \ \ldots, \ \ 1\Big)^T = \boldsymbol{e}_0 + \boldsymbol{\chi}_0.$$

Так как $(V\boldsymbol{\chi}_0)_0 = \sum\limits_{k=1}^{p-1} 1 = p-1$ и $(V\boldsymbol{\chi}_0)_j = \sum\limits_{k=1}^{p-1} \zeta^{jk} = -1$ при $j > 0$, получаем

$$V\boldsymbol{\chi}_0 = \Big(p-1, \ \ -1, \ \ -1, \ \ \ldots, \ \ -1\Big)^T = (p-1)\boldsymbol{e}_0 - \boldsymbol{\chi}_0.$$

Согласно лемме 35, для квадратичного характера имеем

$$V\boldsymbol{\chi}_{\frac{p-1}{2}} = \tau_p \overline{\boldsymbol{\chi}}_{\frac{p-1}{2}} = \tau_p \boldsymbol{\chi}_{\frac{p-1}{2}}.$$

Теперь рассмотрим пары $(\boldsymbol{\chi}_k, \overline{\boldsymbol{\chi}}_k)$ для всех $k = 1, 2, \ldots, \dfrac{p-3}{2}$. По лемме 35 справедливы соотношения:

$$V\boldsymbol{\chi}_k = \tau_{\chi_*^k}\overline{\boldsymbol{\chi}}_k = 0 \cdot \boldsymbol{\chi}_k + \tau_{\chi_*^k}\overline{\boldsymbol{\chi}}_k,$$
$$V\overline{\boldsymbol{\chi}}_k = \tau_{\overline{\chi_*}^k}\boldsymbol{\chi}_k = \tau_{\overline{\chi_*}^k}\boldsymbol{\chi}_k + 0 \cdot \overline{\boldsymbol{\chi}}_k.$$

Таким образом, матрица линейного оператора $\boldsymbol{A}$ относительно базиса (15) принимает блочно-диагональный вид:

$$V' = \operatorname{diag}\left(\begin{pmatrix} 1 & p-1 \\ 1 & -1 \end{pmatrix}, \ (\tau_p), \ \begin{pmatrix} 0 & \tau_{\overline{\chi_*}} \\ \tau_{\chi_*} & 0 \end{pmatrix}, \ \ldots, \ \begin{pmatrix} 0 & \tau_{\overline{\chi_*}^{\frac{p-3}{2}}} \\ \tau_{\chi_*^{\frac{p-3}{2}}} & 0 \end{pmatrix}\right).$$

Теорема 36. *Имеют место равенства*:

1) $|V| = \tau_p \cdot p^{\frac{p-1}{2}} \cdot \left(\frac{2}{p}\right)$;

2) $|V| = i^{\frac{p(p-1)}{2}} p^{\frac{p}{2}}$.

Доказательство. 1) Поскольку χ_* – образующий характер, то $\chi_* \colon \mathbb{F}_p^* \to \mathbb{C}^*$ является мономорфизмом групп, в частности, $\chi_*(-1) = -1$. Тогда, согласно лемме 35, определитель каждого внедиагонального блока 2×2 равен:

$$\begin{vmatrix} 0 & \tau_{\overline{\chi_*}^k} \\ \tau_{\chi_*^k} & 0 \end{vmatrix} = -\tau_{\chi_*^k}\tau_{\overline{\chi_*}^k} = -p\chi_*^k(-1) = -p(-1)^k.$$

Определитель матрицы V' (и, следовательно, V) равен произведению определителей ее диагональных блоков:

$$\begin{aligned} |V| = |V'| &= \begin{vmatrix} 1 & p-1 \\ 1 & -1 \end{vmatrix} \cdot \tau_p \cdot \prod_{k=1}^{\frac{p-3}{2}} \left(-\tau_{\chi_*^k}\tau_{\overline{\chi}_*^k}\right) = (-p) \cdot \tau_p \cdot \prod_{k=1}^{\frac{p-3}{2}} \left(-p(-1)^k\right) \\ &= \tau_p \cdot (-1) \cdot p \cdot (-p)^{\frac{p-3}{2}} \cdot (-1)^{1+2+\cdots+\frac{p-3}{2}} = \tau_p \cdot p^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{(p-3)(p-1)}{8}}. \end{aligned}$$

Замечая, что $\frac{p-1}{2} + \frac{(p-3)(p-1)}{8} = \frac{4(p-1)+(p-3)(p-1)}{8} = \frac{p^2-1}{8}$, окончательно получаем:

$$|V| = \tau_p \cdot p^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} = \tau_p \cdot p^{\frac{p-1}{2}} \cdot \left(\frac{2}{p}\right).$$

2) Согласно равенству (13), имеем:

$$|V| = \pm i^{\frac{p(p-1)}{2}} p^{\frac{p}{2}}. \tag{16}$$

Выясним точное значение знака в этой формуле. Из известной формулы для определителя Вандермонда следует равенство

$$|V| = \prod_{0 \le j < k \le p-1} (\zeta^k - \zeta^j).$$

Для каждых $0 \le j < k \le p-1$ имеем

$$\zeta^k - \zeta^j = e^{\frac{i\pi(k+j)}{p}} \left(e^{\frac{i\pi(k-j)}{p}} - e^{-\frac{i\pi(k-j)}{p}}\right) = 2i \cdot e^{\frac{i\pi(k+j)}{p}} \cdot \sin\left(\frac{\pi(k-j)}{p}\right).$$

Тогда

$$|V| = \left(\prod_{0 \le j < k \le p-1} 2i\right) \cdot \left(\prod_{0 \le j < k \le p-1} e^{\frac{i\pi(k+j)}{p}}\right) \cdot \left(\prod_{0 \le j < k \le p-1} \sin\frac{\pi(k-j)}{p}\right).$$

Рассмотрим первые два множителя:

$$\prod_{0\le j<k\le p-1} 2i = (2i)^{\sum\limits_{k=1}^{p-1}\sum\limits_{j=0}^{k-1} 1} = (2i)^{\frac{p(p-1)}{2}},$$

$$\prod_{0\le j<k\le p-1} e^{\frac{i\pi(k+j)}{p}} = e^{\frac{i\pi}{p}\sum\limits_{k=1}^{p-1}\sum\limits_{j=0}^{k-1}(k+j)}.$$

Так как

$$\sum_{k=1}^{p-1}\sum_{j=0}^{k-1}(k+j) = \sum_{k=1}^{p-1}\left(k^2+\frac{k(k-1)}{2}\right) = \sum_{k=1}^{p-1}\frac{3k^2-k}{2} = \frac{p(p-1)^2}{2},$$

а число $\dfrac{(p-1)^2}{2}$ является четным целым, то $e^{i\pi\cdot\frac{(p-1)^2}{2}} = 1$. Следовательно, вторая экспоненциальная часть равна 1.

Положим $S = \prod\limits_{0\le j<k\le p-1} \sin\frac{\pi(k-j)}{p}$. Так как все аргументы синусов лежат в интервале $(0,\pi)$, они строго положительны, откуда $S>0$. Тогда

$$|V| = i^{\frac{p(p-1)}{2}} 2^{\frac{p(p-1)}{2}} S.$$

Сопоставляя это с (16), замечаем, что вещественный множитель $2^{\frac{p(p-1)}{2}}S$ строго положителен. Значит, знак в равенстве (16) однозначно определяется как плюс. Следовательно, имеет место равенство

$$|V| = i^{\frac{p(p-1)}{2}} p^{\frac{p}{2}}.$$ □

Следующее утверждение непосредственно вытекает из приравнивания двух выражений для $|V|$, полученных в предыдущей теореме.

Теорема 37 (К. Ф. Гаусс, 1818 г., [30])**.** *Имеем*

$$\tau_p = \left(\frac{2}{p}\right) i^{\frac{p(p-1)}{2}}\sqrt{p}.$$

Отметим, что доказательство теоремы 37, основанное на изучении собственных значений матрицы Вандермонда и близкое к предложенному в работе [27], приведено в известном учебнике по теории чисел [33, с. 397–401].

Для краткости будем использовать аббревиатуру КЗВ для классического квадратичного закона взаимности. В своих работах [27, 31, 32] К. Мотосе предложил в общей сложности четыре различных доказательства КЗВ. Два из них, основанные на аппарате теории коммутативных групповых алгебр, содержатся в статьях [31, 32]. В работе [27] автором представлены еще два доказательства КЗВ. При этом первое из них может быть получено из второго доказательства теоремы 26 путем выбора в качестве G циклической группы простого нечетного порядка q (где $q\neq p$). Отметим, что это рассуждение

было воспроизведено в недавней работе [25], где удалось достичь определенного упрощения исходных выкладок за счет вывода ключевого сравнения (14) с помощью леммы Золотарёва–Фробениуса. Второе доказательство из статьи [27], опирающееся на свойства матрицы Вандермонда, сформулированные в лемме 35, было подробно изложено выше.

Равенство (7) и сравнение (10) составляют основу доказательства КЗВ, представленного в [34, глава 6, §3]. Этот подход, использующий базовую арифметику круговых полей, был предложен О. Коши, Г. Эйзенштейном и К. Якоби и органично вытекает из идей шестого доказательства квадратичной взаимности К.Ф. Гаусса [30]. Оригинальное доказательство Гаусса детально разобрано в монографиях [35, 36].

Существенное упрощение доказательства КЗВ, опирающегося на идеи Гаусса из работы [30], достигается за счет использования аппарата теории конечных полей. Рассмотрим аналог суммы Гаусса над конечным полем:

$$\tau = \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \varepsilon^k,$$

где ε – элемент порядка q из мультипликативной группы алгебраического замыкания $\overline{\mathbb{F}}_p$. В статье [37] было получено исключительно краткое доказательство закона квадратичной взаимности на основе следующих тождеств:

$$\tau^2 = (-1)^{\frac{q-1}{2}} q \cdot 1_{\mathbb{F}_p}, \quad \tau^p = \left(\frac{p}{q}\right)\tau. \tag{17}$$

Как и в комплексном случае, можно показать, что $|V| q^{-\frac{q-1}{2}} = \pm\tau$, где V – матрица, совпадающая с матрицей A из равенства (4), если положить в ней $m = q$. Тогда несложно установить взаимную выводимость формул (17), с одной стороны, и формул

$$|V|^2 = (-1)^{\frac{q-1}{2}} q^q \cdot 1_{\mathbb{F}_p}, \quad |V|^p = \left(\frac{p}{q}\right)|V|, \tag{18}$$

с другой. Равенства (18) лежат в основе доказательств КЗВ, представленных в работах [28, 29]. В статье [29] равенство $|V|^p = \left(\frac{p}{q}\right)|V|$ доказывается с привлечением леммы Гаусса. В работе [28] это же равенство получено с помощью критерия Эйлера, данное доказательство также воспроизведено в [13, с. 67].

Таким образом, доказательства КЗВ, использующие свойства определителя Вандермонда, идейно глубоко родственны классическим доказательствам, основанным на аппарате квадратичных сумм Гаусса и восходящим к его шестому доказательству. При этом одно из наиболее коротких доказательств КЗВ в духе Гаусса, приведенное в разделе 3.1, достигается именно за счет рассмотрения определителя Вандермонда над конечными полями в комбинации с леммой Золотарёва–Фробениуса.

4. Символ Картье

4.1. Основные свойства символа Картье. Для конечной абелевой группы G порядка n отображение

$$\varphi_a : g \mapsto g^a,$$

где a – целое число, взаимно простое с n, является автоморфизмом группы G. Согласно определению символа Дьюка–Хопкинс символ $\left(\frac{a}{G}\right)_{\mathrm{DH}}$ является знаком этого автоморфизма. Естественным обобщением символа Дьюка–Хопкинс является переход от рассмотрения знаков "скалярных" автоморфизмов вида $g \mapsto g^a$ к рассмотрению знаков произвольных автоморфизмов конечных абелевых групп. Именно этот подход был развит П. Картье, еще в 1970 году в своей работе [15] он ввел символ $\left(\frac{u}{G}\right)$ (сам Картье в статье утверждает, что этот символ был предложен Фробениусом в [17]: "il suggere immediatement la definition suivante des symboles $\left(\frac{u}{G}\right)$"). Этот символ определяется как знак перестановки элементов конечной абелевой группы G нечетного порядка, индуцированной произвольным ее автоморфизмом u.

Таким образом, подход Картье предвосхитил частный случай интерпретации группового символа для абелевых групп более чем на три десятилетия (статья Дьюка и Хопкинс [19] была опубликована в 2005 году). Тот факт, что эта работа Картье, не нашла отражения в статье Дьюка и Хопкинс, может быть объяснен, как предполагают П.Л. Кларк и А. Бруниэйт [14], большей известностью трудов Картье в то время преимущественно во франкоязычной научной среде. Но с другой стороны, в классической монографии К. Айерлэнда и М. Роузена [34] (замечания к главе 5) символ, введенный в работе Картье, охарактеризован как «интересное обобщение» символа Лежандра. Дадим определение этому символу, который в дальнейшем будем называть символом Картье.

Определение 38 (символ Картье)**.** Пусть G – конечная абелева группа нечетного порядка n. Пусть $\varphi \in \mathrm{Aut}(G)$ – автоморфизм группы G. Действие φ на элементах группы G индуцирует перестановку Φ на множестве элементов G. Символ Картье $\left(\frac{\varphi}{G}\right)_{\mathrm{C}}$ для автоморфизма $\varphi \in \mathrm{Aut}(G)$ определяется как знак перестановки Φ:

$$\left(\frac{\varphi}{G}\right)_{\mathrm{C}} := \mathrm{sgn}(\Phi).$$

Предложение 39. *Пусть G – конечная абелева группа нечетного порядка n, и a – целое число, взаимно простое с n. Тогда*

$$\left(\frac{\varphi_a}{G}\right)_{\mathrm{C}} = \left(\frac{a}{G}\right)_{\mathrm{DH}},$$

где $\varphi_a \in \mathrm{Aut}(G)$ – автоморфизм, заданный правилом $\varphi_a(g) = g^a$.

Предложение 40. *Пусть G – конечная абелева группа нечетного порядка n, и пусть $\varphi, \psi \in \mathrm{Aut}(G)$ – произвольные автоморфизмы G, а φ_{-1} и φ_2 – автоморфизмы G, заданные правилами $g \mapsto g^{-1}$ и $g \mapsto g^2$ соответственно. Тогда*

1) $\left(\frac{\varphi\psi}{G}\right)_{\mathrm{C}} = \left(\frac{\varphi}{G}\right)_{\mathrm{C}}\left(\frac{\psi}{G}\right)_{\mathrm{C}}$;

2) $\left(\frac{\varphi_{-1}}{G}\right)_{\mathrm{C}} = (-1)^{\frac{n-1}{2}}$;

3) $\left(\frac{\varphi_2}{G}\right)_{\mathrm{C}} = (-1)^{\frac{n^2-1}{8}}$.

Одним из важнейших свойств, доказанных Картье, является результат, который он называет обобщенной леммой Гаусса–Шеринга. Эта лемма дает комбинаторный способ вычисления символа Картье через так называемые "полусистемы" элементов группы.

Теорема 41 (обобщенная лемма Гаусса–Шеринга; Картье [15])**.** *Пусть G – конечная абелева группа нечетного порядка, $\varphi \in \mathrm{Aut}(G)$ – автоморфизм группы G. Пусть S – полусистема в $G^* = G \setminus \{0\}$, т. е. такое подмножество $S \subset G^*$, что для каждого $x \in G^*$ ровно один из элементов x или $-x$ принадлежит S (эквивалентно, $S \cap S^- = \emptyset$ и $S \cup S^- = G^*$, где $S^- = \{-s \mid s \in S\}$). Тогда символ Картье выражается как:*

$$\left(\frac{\varphi}{G}\right)_{\mathrm{C}} = (-1)^{|\varphi(S)\cap S^-|}.$$

Доказательство. Поскольку $\varphi(0) = 0$, знак перестановки φ, действующей на G, совпадает со знаком ее ограничения φ^* на $G^* = G \setminus \{0\}$. Пусть $|G| = n_G$. Так как n нечетно, положим $n = 2k + 1$. Тогда $|G^*| = 2k$ и полусистема S содержит $k = (n_G - 1)/2$ элементов.

Пусть $S = \{x_1, \ldots, x_k\}$. Зафиксируем некоторый линейный порядок $<$ на элементах множества G^*, при котором $x_1 < \cdots < x_k < -x_k < \cdots < -x_1$. Ключевыми свойствами такого порядка являются:

a) если $x < y$, то $-y < -x$;

b) $S = \{x \in G^* \mid x < -x\}$.

Символ Картье $\left(\frac{\varphi}{G}\right)_{\mathrm{C}}$, будучи знаком перестановки φ^*, равен $(-1)^{|I|}$, где I – множество инверсий, т. е. пар $(x, y) \in G^* \times G^*$ таких, что $x < y$ и $\varphi(x) > \varphi(y)$. Рассмотрим отображение $\theta : I \to I$, заданное правилом $\theta(x, y) = (-y, -x)$. Ясно, что θ является инволюцией на множестве I, т. е. $\theta \circ \theta = \mathrm{id}_I$. Следовательно, число элементов $|I|$ имеет ту же четность, что и число m неподвижных точек инволюции θ в I. Положим

$$A = \{(x, y) \in G^* \times G^* \mid x < y, \varphi(x) > \varphi(y)\}, \quad B = \{x \in S \mid \varphi(x) > \varphi(-x)\}.$$

Тогда $|A| \equiv |B| \pmod 2$. Так как в силу определения линейного порядка на G^*, очевидно, $B = \{x \in S \mid \varphi(x) \in S^-\} = S \cap \varphi^{-1}(S^-)$, то $|B| = |\varphi(S \cap \varphi^{-1}(S^-))| = |\varphi(S) \cap S^-|$. Таким об-

разом,

$$\left(\frac{\varphi}{G}\right)_{\mathrm{C}} = (-1)^{|I|} = (-1)^m = (-1)^{|\varphi(S)\cap S^-|}.$$

□

Для произвольного целого числа x и целого $n \neq 0$ остаток от деления x на n будем обозначать через $\mathrm{res}_n(x)$.

Следствие 42 (лемма Гаусса–Шеринга, [38])**.** *Пусть $n > 1$ – нечетное натуральное число, а m – целое число, взаимно простое с n. Тогда*

$$\left(\frac{m}{n}\right) = (-1)^{|I|},$$

где

$$I = \left\{ i \in \mathbb{Z} \;\middle|\; 1 \leq i \leq \frac{n-1}{2},\ \mathrm{res}_n(m \cdot i) > \frac{n}{2} \right\}.$$

Как показывают рассуждения из доказательства теоремы 41, между леммами Гаусса–Шеринга и Золотарёва–Фробениуса существует тесная связь. Действительно, пусть $m, n > 1$ – взаимно простые нечетные натуральные числа. Положим

$$A = \{(i,j) \mid 1 \leq i < j \leq n,\ \mathrm{res}_n(mi) > \mathrm{res}_n(mj)\},$$

$$B = \left\{ i \in \mathbb{Z} \;\middle|\; 1 \leq i \leq \frac{n-1}{2},\ \mathrm{res}_n(m \cdot i) > \frac{n}{2} \right\}.$$

Тогда, согласно доказательству теоремы 41, имеет место сравнение

$$|A| \equiv |B| \pmod 2. \tag{19}$$

Так как, согласно леммам Золотарёва–Фробениуса и Гаусса–Шеринга соответственно, справедливы равенства

$$\left(\frac{m}{n}\right) = (-1)^{|A|}, \qquad \left(\frac{m}{n}\right) = (-1)^{|B|},$$

то из сравнения (19) вытекает несложная взаимная выводимость этих лемм.

В работе [15] было доказано следующее фундаментальное свойство рассматриваемого символа.

Теорема 43. *Пусть G – конечная абелева группа нечетного порядка, G' – подгруппа в G, инвариантная относительно автоморфизма $\varphi \in \mathrm{Aut}(G)$. Пусть также $G'' = G/G'$ – фактор-группа. Обозначим через φ' автоморфизм подгруппы G', индуцированный ограничением φ на G' (т. е., $\varphi' = \varphi|_{G'}$), и через φ'' – автоморфизм факторгруппы G'', индуцированный φ (т. е., $\varphi''(gG') = \varphi(g)G'$). Тогда справедливо равенство:*

$$\left(\frac{\varphi}{G}\right)_{\mathrm{C}} = \left(\frac{\varphi'}{G'}\right)_{\mathrm{C}} \cdot \left(\frac{\varphi''}{G''}\right)_{\mathrm{C}}.$$

Доказательство. Обозначим через $\pi : G \to G'' = G/G'$ канонический гомоморфизм. Выберем полусистему S' в $(G')^* = G' \setminus \{0_{G'}\}$. Выберем полусистему S'' в $(G'')^* = G'' \setminus \{0_{G''}\}$. Построим полусистему S для группы G. Положим $T = \pi^{-1}(S'')$. Поскольку $S'' \subset (G'')^*$, то $0_{G''} \notin S''$, и, следовательно, $G' \cap T = \emptyset$.

Покажем, что $S = S' \cup T$ является полусистемой в G^*. Для этого нужно доказать, что для любого элемента $g \in G^*$ ровно один из элементов g или $-g$ принадлежит S. Рассмотрим два непересекающихся случая.

Случай, когда $g \in G' \setminus \{0\}$. Поскольку S' является полусистемой в $(G')^*$, то ровно один из элементов g или $-g$ принадлежит S'. С другой стороны, так как $\pi(g) = \pi(-g) = 0_{G''}$, а $0_{G''} \notin S''$, то ни g, ни $-g$ не принадлежат $T = \pi^{-1}(S'')$. Следовательно, ровно один из g или $-g$ принадлежит $S' \cup T = S$.

И второй случай, когда $g \in G \setminus G'$. В этом случае $\pi(g) \neq 0_{G''}$. Так как S'' – полусистема в $(G'')^*$, то ровно один из элементов $\pi(g)$ или $\pi(-g) = -\pi(g)$ принадлежит S''. Если $\pi(g) \in S''$, то $g \in T$. При этом $\pi(-g) \notin S''$, значит $-g \notin T$. Если же $\pi(-g) \in S''$, то $-g \in T$, а $g \notin T$.

Поскольку $g \notin G'$, то ни g, ни $-g$ не могут принадлежать $S' \subset G'$. Таким образом, и в этом случае ровно один из элементов g или $-g$ принадлежит S.

Из этих двух случаев следует, что S действительно является полусистемой в G^*. Согласно обобщенной лемме Гаусса–Шеринга (теорема 41):

$$\left(\frac{\varphi}{G}\right)_{\mathrm{C}} = (-1)^{|\varphi(S)\cap S^-|}$$

Поскольку $S = S' \cup T$ является дизъюнктным объединением, и $\varphi(G') = G'$, то $\varphi(S) = \varphi(S') \cup \varphi(T) = \varphi'(S') \cup \varphi(T)$. При этом $\varphi'(S') \subset G'$, а $\varphi(T) \subset T$ (поскольку φ индуцирует автоморфизм на G'', $\varphi(\pi^{-1}(S'')) = \pi^{-1}(\varphi''(S''))$). Тогда пересечение $\varphi(S) \cap S^-$ можно разбить на две непересекающиеся части:

$$\varphi(S) \cap S^- = (\varphi'(S') \cap (S')^-) \cup (\varphi(T) \cap T^-)$$

(здесь мы учли, что $S^- = (S')^- \cup T^-$ и $(S')^- \subset G'$, $T^- \subset G \setminus G'$). Следовательно, получаем равенство

$$|\varphi(S) \cap S^-| = |\varphi'(S') \cap (S')^-| + |\varphi(T) \cap T^-|.$$

Рассмотрим член $|\varphi(T) \cap T^-|$. Множество $\varphi(T) \cap T^-$ является объединением тех смежных классов группы G по подгруппе G', которые соответствуют элементам множества $\varphi''(S'') \cap (S'')^-$ в фактор-группе G''. Каждый такой смежный класс содержит ровно $|G'|$ элементов.

Поскольку группа G имеет нечетный порядок, ее подгруппа G' также имеет нечетный порядок, т. е. $|G'|$ – нечетное число. Следовательно, $|\varphi(T) \cap T^-| = |G'| \cdot |\varphi''(S'') \cap (S'')^-|$.

Так как $|G'|$ нечетно, получаем сравнение по модулю 2:

$$|\varphi(T) \cap T^-| \equiv |\varphi''(S'') \cap (S'')^-| \pmod 2.$$

Подставляя полученные результаты, имеем:

$$\left(\frac{\varphi}{G}\right)_{\mathrm{C}} = (-1)^{|\varphi(S)\cap S^-|} = (-1)^{|\varphi'(S')\cap(S')^-|+|\varphi(T)\cap T^-|} = (-1)^{|\varphi'(S')\cap(S')^-|} \cdot (-1)^{|\varphi(T)\cap T^-|} =$$
$$= \left(\frac{\varphi'}{G'}\right)_{\mathrm{C}} \cdot (-1)^{|\varphi''(S'')\cap(S'')^-|} = \left(\frac{\varphi'}{G'}\right)_{\mathrm{C}} \cdot \left(\frac{\varphi''}{G''}\right)_{\mathrm{C}}.$$

Это завершает доказательство теоремы. □

Следствие 44. *Пусть G_1 и G_2 – конечные абелевы группы нечетных порядков. Пусть $\varphi_1 \in \mathrm{Aut}(G_1)$ и $\varphi_2 \in \mathrm{Aut}(G_2)$ – автоморфизмы этих групп. Рассмотрим автоморфизм $\varphi = \varphi_1 \times \varphi_2$ на группе $G = G_1 \times G_2$, определенный правилом $\varphi((g_1, g_2)) = (\varphi_1(g_1), \varphi_2(g_2))$ для всех $(g_1, g_2) \in G$. Тогда*

$$\left(\frac{\varphi}{G_1 \times G_2}\right)_{\mathrm{C}} = \left(\frac{\varphi_1}{G_1}\right)_{\mathrm{C}} \cdot \left(\frac{\varphi_2}{G_2}\right)_{\mathrm{C}}.$$

Заметим, что утверждение следствия 44 также непосредственно вытекает из леммы 1 b).

Теорема 45. *Пусть $0 \to G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} \dots G_{k-1} \xrightarrow{f_{k-1}} G_k \to 0$ $(k \geq 3)$ – точная последовательность конечных абелевых групп, $\varphi_1 \in \mathrm{Aut}(G_1), \dots, \varphi_k \in \mathrm{Aut}(G_k)$ и равенство $\varphi_{i+1} f_i = f_i \varphi_i$ выполнено для каждого $1 \leq i \leq k-1$. Тогда имеет место равенство*

$$\left(\frac{\varphi_1}{G_1}\right)_{\mathrm{C}} \cdot \left(\frac{\varphi_2}{G_2}\right)_{\mathrm{C}} \cdot \ldots \cdot \left(\frac{\varphi_k}{G_k}\right)_{\mathrm{C}} = 1. \tag{20}$$

Доказательство. Докажем утверждение теоремы с помощью математической индукции по k. Для $k = 3$ равенство (20) следует из теоремы 43. Предположим, что равенство (20) верно для некоторого $k \geq 3$. Рассмотрим точную последовательность конечных абелевых групп $0 \to G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} \dots G_k \xrightarrow{f_k} G_{k+1} \to 0$ и семейство автоморфизмов $\varphi_1 \in \mathrm{Aut}(G_1), \dots, \varphi_{k+1} \in \mathrm{Aut}(G_{k+1})$, для которого равенство $\varphi_{i+1} f_i = f_i \varphi_i$ выполнено для каждого $1 \leq i \leq k$. Имеют место точные последовательности $0 \to G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} \dots G_{k-1} \xrightarrow{f_{k-1}} f_{k-1}(G_{k-1}) \to 0$ и $0 \to f_{k-1}(G_{k-1}) \xrightarrow{\iota} G_k \xrightarrow{f_k} G_{k+1} \to 0$, где $\iota : f_{k-1}(G_{k-1}) \to G_k$ – естественное вложение. Заметим, что $\varphi_k(f_{k-1}(G_{k-1})) \subseteq f_{k-1}(G_{k-1})$. Тогда по предположению индукции имеют место равенства

$$\left(\frac{\varphi_1}{G_1}\right)_{\mathrm{C}} \left(\frac{\varphi_2}{G_2}\right)_{\mathrm{C}} \dots \left(\frac{\varphi'_k}{f_{k-1}(G_{k-1})}\right)_{\mathrm{C}} = 1,$$

$$\left(\frac{\varphi'_k}{f_{k-1}(G_{k-1})}\right)_{\mathrm{C}}\left(\frac{\varphi_k}{G_k}\right)_{\mathrm{C}}\left(\frac{\varphi_{k+1}}{G_{k+1}}\right)_{\mathrm{C}}=1,$$

где $\varphi'_k \in \mathrm{Aut}(f_{k-1}(G_{k-1}))$ – ограничение автоморфизма φ_k на подгруппу $f_{k-1}(G_{k-1})$. Таким образом,

$$1=\left(\frac{\varphi_1}{G_1}\right)_{\mathrm{C}}\left(\frac{\varphi_2}{G_2}\right)_{\mathrm{C}}\dots\left(\frac{\varphi'_k}{f_{k-1}(G_{k-1})}\right)_{\mathrm{C}}\left(\frac{\varphi'_k}{f_{k-1}(G_{k-1})}\right)_{\mathrm{C}}\left(\frac{\varphi_k}{G_k}\right)_{\mathrm{C}}\left(\frac{\varphi_{k+1}}{G_{k+1}}\right)_{\mathrm{C}}=$$
$$=\left(\frac{\varphi_1}{G_1}\right)_{\mathrm{C}}\left(\frac{\varphi_2}{G_2}\right)_{\mathrm{C}}\dots\left(\frac{\varphi_k}{G_k}\right)_{\mathrm{C}}\left(\frac{\varphi_{k+1}}{G_{k+1}}\right)_{\mathrm{C}}. \qquad \square$$

Далее рассмотрим свойства символа Картье $\left(\frac{\varphi}{G}\right)_{\mathrm{C}}$ в случае, когда G – векторное пространство над конечным полем, а φ – линейный оператор, действующий на G. Отметим, что во избежание путаницы с мощностью множеств или порядком элементов группы, определитель абстрактного линейного оператора $\mathcal{A}$ (или матрицы A) в этом разделе мы будем обозначать стандартным символом $\det\mathcal{A}$, что равносильно использовавшемуся ранее обозначению $|A|$.

Лемма 46. *Пусть $q=p^k$, где p – нечетное простое число и $k\geq 1$. Тогда отображение $\varphi\colon \mathrm{GL}_n(\mathbb{F}_q)\to\{\pm1\}$, действующее согласно правилу*

$$\varphi\colon A\mapsto\left(\frac{\det A}{\mathbb{F}_q}\right),$$

является единственным нетривиальным гомоморфизмом из группы $\mathrm{GL}_n(\mathbb{F}_q)$ в группу $\{\pm1\}$.

Доказательство. Покажем сначала, что φ – нетривиальный гомоморфизм. Пусть $d\in\mathbb{F}_q^*\backslash\mathbb{F}_q^{*2}$. Тогда для диагональной матрицы $A_0=\mathrm{diag}(d,1,\dots,1)\in\mathrm{GL}_n(\mathbb{F}_q)$ имеем:

$$\varphi(A_0)=\left(\frac{\det A_0}{\mathbb{F}_q}\right)=\left(\frac{d}{\mathbb{F}_q}\right)=-1.$$

Следовательно, ядро гомоморфизма φ не совпадает со всей группой, и φ нетривиален.

Предположим теперь, что $\psi_1\colon \mathrm{GL}_n(\mathbb{F}_q)\to\{\pm1\}$ и $\psi_2\colon \mathrm{GL}_n(\mathbb{F}_q)\to\{\pm1\}$ – два произвольных нетривиальных гомоморфизма. Из свойств коммутанта вытекает, что

$$[\mathrm{GL}_n(\mathbb{F}_q),\mathrm{GL}_n(\mathbb{F}_q)]\subseteq\ker(\psi_1)\cap\ker(\psi_2).$$

Согласно [39, с. 38]:

$$\mathrm{SL}_n(\mathbb{F}_q)=[\mathrm{GL}_n(\mathbb{F}_q),\mathrm{GL}_n(\mathbb{F}_q)]\subseteq\ker(\psi_1)\cap\ker(\psi_2).$$

Поскольку для гомоморфизма взятия определителя $\det\colon \mathrm{GL}_n(\mathbb{F}_q)\to\mathbb{F}_q^*$ имеет место равенство $\ker(\det)=\mathrm{SL}_n(\mathbb{F}_q)$, по теореме о гомоморфизме существуют такие гомоморфиз-

мы ψ_1' и ψ_2', действующие из $\mathbb{F}_q^*$ в $\{\pm 1\}$, что выполняются равенства:

$$\psi_1 = \psi_1' \circ \det, \qquad \psi_2 = \psi_2' \circ \det .$$

Так как мультипликативная группа поля $\mathbb{F}_q^*$ является циклической группой четного порядка, для нее существует единственный нетривиальный гомоморфизм в $\{\pm 1\}$. Таким образом, $\psi_1' = \psi_2'$, откуда окончательно получаем $\psi_1 = \psi_2$. □

Теорема 47. *Пусть $\mathbb{F}_q$ – конечное поле из q элементов, где $q = p^s$ и p – нечетное простое число. Если V – конечномерное векторное пространство над полем $\mathbb{F}_q$, то для каждого обратимого линейного оператора $\mathcal{A} \in \mathrm{GL}(V)$ имеет место равенство*

$$\left(\frac{\mathcal{A}}{V}\right)_{\mathrm{C}} = \left(\frac{\det \mathcal{A}}{\mathbb{F}_q}\right).$$

Доказательство. Покажем, что гомоморфизм $\psi\colon \mathrm{GL}(V) \to \{\pm 1\}$, заданный согласно правилу $\psi(\mathcal{A}) = \left(\frac{\mathcal{A}}{V}\right)_{\mathrm{C}}$ является нетривиальным. Выберем в V некоторый базис $\{e_1, \ldots, e_n\}$. Рассмотрим линейный оператор $\mathcal{A}\colon V \to V$, действующий согласно правилу

$$x_1 e_1 + \ldots + x_n e_n \mapsto a x_1 e_1 + x_2 e_2 + \ldots + x_n e_n,$$

где $a \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$. Оператор $\mathcal{A}$ можно рассматривать как прямое произведение оператора умножения на a на подпространстве $\langle e_1 \rangle$ и тождественного оператора на подпространстве $\langle e_2, \ldots, e_n \rangle$. Согласно лемме 1 b) и тому факту, что знак отображения $x \mapsto ax$ на $\mathbb{F}_q$ равен $\left(\frac{a}{\mathbb{F}_q}\right)$, получаем

$$\left(\frac{\mathcal{A}}{V}\right)_{\mathrm{C}} = \left(\frac{a}{\mathbb{F}_q}\right)^{|\mathbb{F}_q^{n-1}|} = (-1)^{q^{n-1}} = -1,$$

поскольку q нечетно.

Таким образом, гомоморфизм ψ является нетривиальным. Следовательно, согласно лемме 46, он совпадает с единственным нетривиальным гомоморфизмом из $\mathrm{GL}(V)$ в $\{\pm 1\}$, и для всякого обратимого линейного оператора $\mathcal{A} \in \mathrm{GL}(V)$ имеет место равенство

$$\left(\frac{\mathcal{A}}{V}\right)_{\mathrm{C}} = \left(\frac{\det \mathcal{A}}{\mathbb{F}_q}\right). \qquad \square$$

Непосредственным следствием предыдущей теоремы является следующее классическое утверждение.

Теорема 48 (Фробениуса–Золотарёва)**.** *Пусть p – нечетное простое число, $k \geq 1$, а $G = \mathbb{F}_p^k$ – k-мерное векторное пространство над полем $\mathbb{F}_p$. Пусть $\varphi \in \mathrm{Aut}(G)$ – автоморфизм группы G, который как линейное преобразование этого векторного простран-*

ства задается обратимой матрицей $A \in \mathrm{GL}_k(\mathbb{F}_p)$. *Тогда*

$$\left(\frac{\varphi}{G}\right)_{\mathrm{C}} = \left(\frac{\det A}{p}\right),$$

где справа стоит классический символ Лежандра.

Обобщение теоремы Фробениуса–Золотарёва на случай абелевой группы $\mathbb{Z}_n^k$, где n нечетно, было получено И. Шуром в работе [40]. Более широкие результаты были получены Д.Г. Лемером [41]. Сделаем следующую оговорку: излагая результат Лемера, мы будем обозначать этот знак как $\left(\frac{\varphi}{G}\right)_{\mathrm{C}}$, понимая это как естественное распространение основной идеи символа Картье на группы любого порядка. Лемер передоказывает ранее полученные результаты для нечетных n и устанавливает явные формулы для символа Картье в ряде случаев для четных n.

Теорема 49 (Лемер [41])**.** *Пусть* n *– натуральное число, и* $k \geq 2$. *Рассмотрим* $G = \mathbb{Z}_n^k$ *как свободный модуль ранга* k *над кольцом* $\mathbb{Z}_n$. *Для любого автоморфизма* $\varphi \in \mathrm{Aut}(G)$, *который как автоморфизм модуля над* $\mathbb{Z}_n$ *представим обратимой матрицей* $A \in \mathrm{GL}_k(\mathbb{Z}_n)$, *справедливы утверждения*:

1) *Если* n *– нечетно, то*

$$\left(\frac{\varphi}{G}\right)_{\mathrm{C}} = \left(\frac{\det A}{n}\right);$$

(*это утверждение согласуется с теоремой Шура*).

2) *Если* n *– четно, тогда*:

a) *Если* $k \geq 3$ *или* $k \geq 2$ *и* $n \equiv 0 \pmod 4$, *тогда*

$$\left(\frac{\varphi}{G}\right)_{\mathrm{C}} = 1;$$

b) *Если* $k = 2$ *и* $n \equiv 2 \pmod 4$, *то пусть* $A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z})$ *– единственная матрица с элементами из* $\{0, 1\}$, *такая, что ее элементы сравнимы по модулю 2 с соответствующими элементами матрицы* A. *Тогда*

$$\left(\frac{\varphi}{G}\right)_{\mathrm{C}} = (-1)^{a'+b'+c'+d'}(a'd' - b'c').$$

Теорема Лемера дает конкретные значения для символа Картье в ряде случаев, когда порядок группы $\mathbb{Z}_n^k$ является четным. Однако сама структура этих результатов, с разделением на подслучаи в зависимости от k и сравнимости n по модулю 4, уже намекает на значительную сложность общей картины для групп четного порядка по сравнению с более единообразными результатами для нечетных порядков. Эту возрастающую сложность отмечали Кларк и Бруниэйт в работе [14], что подчеркивает нетривиальность разработки общей и единой формулы символа Картье для групп четного порядка.

4.2. Формула для символа Картье. Пусть R – абстрактное числовое кольцо и P – простой идеал кольца R. R-модуль M называется P-примарным, если для каждого элемента $m \in M$ существует натуральное число n, для которого выполнено равенство $P^n m = 0$.

Рассмотрим произвольный ненулевой конечно порожденный P-примарный модуль M. Хорошо известно, что для некоторых натуральных чисел $n_1 \leq n_2 \leq \ldots \leq n_k$ имеет место изоморфизм $M \cong R/P^{n_1} \oplus R/P^{n_2} \oplus \cdots \oplus R/P^{n_k}$. Ясно, что M – конечный модуль. Для некоторого элемента $p \in P$ имеет место равенство $(pR + P^{n_k})/P^{n_k} = P/P^{n_k}$ и $P^i/P^{n_k} = (p^i R + P^{n_k})/P^{n_k}$ $(0 \leq i \leq n_k)$ – все подмодули модуля R/P^{n_k}. Для любых $n_i \leq n_j$ имеют место хорошо известные изоморфизмы

$$R/P^{n_i} \cong \mathrm{Hom}_R(R/P^{n_j}, R/P^{n_i}), R/P^{n_i} \cong \mathrm{Hom}_R(R/P^{n_i}, R/P^{n_j}),$$

действующие соответственно согласно правилам

$$r + P^{n_i} \mapsto (x + P^{n_j} \mapsto rx + P^{n_i}), r + P^{n_i} \mapsto (x + P^{n_i} \mapsto rxp^{n_j - n_i} + P^{n_j}). \tag{21}$$

Рассмотренные выше изоморфизмы индуцируют изоморфизм α_1 действующий из кольца формальных матриц

$$(R/P^{\min(n_i,n_j)})_{i,j} = \begin{pmatrix} R/P^{n_1} & R/P^{n_1} & \ldots & R/P^{n_1} \\ R/P^{n_1} & R/P^{n_2} & \ldots & R/P^{n_2} \\ \vdots & \vdots & \ddots & \vdots \\ R/P^{n_1} & R/P^{n_2} & \ldots & R/P^{n_k} \end{pmatrix},$$

в котором матричные единицы умножаются согласно правилам:

$$E_{ij}E_{js} = s_{ijs}E_{is}, \text{ где } s_{ijs} = \begin{cases} p^{n_j}/p^{\max(n_i,n_s)}, & i < j > s; \\ p^{\min(n_i,n_s)}/p^{n_j}, & i > j < s; \\ 1_R, & \text{иначе} \end{cases}$$

в кольцо формальных матриц

$$(\mathrm{Hom}(R/P^{n_j}, R/P^{n_i}))_{i,j} = \begin{pmatrix} \mathrm{Hom}(R/P^{n_1}, R/P^{n_1}) & \mathrm{Hom}(R/P^{n_2}, R/P^{n_1}) & \ldots & \mathrm{Hom}(R/P^{n_k}, R/P^{n_1}) \\ \mathrm{Hom}(R/P^{n_1}, R/P^{n_2}) & \mathrm{Hom}(R/P^{n_2}, R/P^{n_2}) & \ldots & \mathrm{Hom}(R/P^{n_k}, R/P^{n_2}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Hom}(R/P^{n_1}, R/P^{n_k}) & \mathrm{Hom}(R/P^{n_2}, R/P^{n_k}) & \ldots & \mathrm{Hom}(R/P^{n_k}, R/P^{n_k}) \end{pmatrix}.$$

При этом на компонентах матриц изоморфизм α_1 действует согласно правилам (21).

Пусть $\Psi : M \to \bigoplus_{i=1}^{k} R/P^{n_i}$ – некоторый изоморфизм. Изоморфизм Ψ индуцирует изоморфизм колец $\Psi' : \mathrm{End}_R(M) \to \mathrm{End}_R\left(\bigoplus_{i=1}^{k} R/P^{n_i}\right)$, действующий согласно

правилу $f \mapsto \Psi f \Psi^{-1}$. Таким образом, имеем изоморфизм

$$\alpha_1 \circ \alpha_2 \circ \Psi' : \mathrm{End}_R(M) \to (R/P^{\min(n_i,n_j)})_{i,j},$$

где $\alpha_2 : \mathrm{End}_R(\oplus_{i=1}^k R/P^{n_i}) \to (\mathrm{Hom}(R/P^{n_j}, R/P^{n_i}))_{i,j}$ – канонический изоморфизм. Для любого $f \in \mathrm{End}_R(M)$ матрицу $\alpha_1 \circ \alpha_2 \circ \Psi'(f)$ будем называть матрицей эндоморфизма f.

Пусть f – эндоморфизм из $\mathrm{End}_R(M)$ и $(a_{ij} + P^{\min(n_i,n_j)})_{i,j}$ – его матрица. Для произвольного $m \in M$ будем рассматривать $\Psi(m) \in \bigoplus\limits_{i=1}^{k} R/P^{n_i}$ как вектор-столбец длины k. Тогда для всякого $m \in M$, у которого $\Psi(m) = \begin{pmatrix} r_1 + P^{n_1} \\ r_2 + P^{n_2} \\ \vdots \\ r_k + P^{n_k} \end{pmatrix}$, вектор-столбец $\Psi(f(m))$ равен

$$\begin{pmatrix} a_{11}r_1 + a_{12}r_2 + \ldots + a_{1k}r_k + P^{n_1} \\ a_{21}p^{n_2-n_1}r_1 + a_{22}r_2 + \ldots + a_{2k}r_k + P^{n_2} \\ \vdots \\ a_{k1}p^{n_k-n_1}r_1 + a_{k2}p^{n_k-n_2}r_2 + \ldots + a_{kk}r_k + P^{n_k} \end{pmatrix}.$$

Теорема 50. *Пусть R – абстрактное числовое кольцо, P – нечетный простой идеал кольца R, M – конечно порожденный P-примарный R-модуль и*

$$M \cong \bigoplus_{i=1}^{t} M_i, \quad \textit{где } M_i = (R/P^{n_i})^{k_i} = \underbrace{R/P^{n_i} \oplus \cdots \oplus R/P^{n_i}}_{k_i \textit{ раз}},$$

и $1 \le n_1 < n_2 < \cdots < n_t$, а $k_i \ge 1$. Если φ – автоморфизм модуля M, матрица которого имеет вид:

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1t} \\ A_{21} & A_{22} & \cdots & A_{2t} \\ \vdots & \vdots & \ddots & \vdots \\ A_{t1} & A_{t2} & \cdots & A_{tt} \end{pmatrix}, \quad \textit{где } A_{ij} \in \mathrm{Mat}_{k_i \times k_j}\left(R/P^{\min(n_i,n_j)}\right),$$

то символ Картье для φ вычисляется по формуле:

$$\left(\frac{\varphi}{M}\right)_{\mathrm{C}} = \prod_{i=1}^{t} \left(\frac{\det A_{ii}}{P^{n_i}}\right).$$

Доказательство. Доказательство проведем методом математической индукции по максимальному показателю $N = n_t$.

Если $N = n_t = 1$, то

$$M \cong (R/P)^{k_1}.$$

В этом случае M имеет естественную структуру векторного пространства над полем R/P и φ – невырожденное линейное преобразование M, матрица которого равна A_{11}. Поэтому согласно теореме 47 имеет место равенство:

$$\left(\frac{\varphi}{M}\right)_{\mathrm{C}} = \left(\frac{\det A_{11}}{P}\right).$$

Пусть $M \cong \bigoplus\limits_{i=1}^{t}(R/P^{n_i})^{k_i}$ и $N = n_t > 1$. Предположим, что теорема 50 верна для всех конечно порожденных P-примарных R-модулей M', для которых существует такое натуральное число N', строго меньшее N, что $P^{N'}M' = 0$.

Рассмотрим подмодуль PM. Ясно, что

$$PM \cong \bigoplus_{i\in I'} \left(P/P^{n_i-1}\right)^{k_i} \cong \bigoplus_{i\in I'} \left(R/P^{n_i-1}\right)^{k_i}, \quad \text{где } I' = \{i \mid n_i > 1\}.$$

Так как PM – вполне инвариантный подмодуль модуля M, то φ индуцирует изоморфизм $\varphi' = \varphi_{|PM}$ и изоморфизм $\overline{\varphi} : M/PM \to M/PM$, действующий согласно правилу $m + PM \mapsto \varphi(m) + PM$. Из мультипликативности символа Картье следует равенство

$$\left(\frac{\varphi}{M}\right)_{\mathrm{C}} = \left(\frac{\varphi'}{PM}\right)_{\mathrm{C}} \left(\frac{\overline{\varphi}}{M/PM}\right)_{\mathrm{C}}.$$

Положим $F = \bigoplus\limits_{i=1}^{t}(R/P^{n_i})^{k_i}$. Согласно предположению существует изоморфизм $\Psi : M \to F$. Этот изоморфизм индуцирует изоморфизмы $\Psi_1 : M/PM \to F/PF$ и $\Psi_2 : PM \to PF$. Матрицу эндоморфизма φ, которая определяется с помощью изоморфизма Ψ и некоторого порождающего циклического R-модуля R/P^{n_k}, обозначим $A = (A_{ij})_{1\le i,j\le t}$, где $A_{ij} \in \mathrm{Mat}_{k_i\times k_j}\left(R/P^{\min(n_i,n_j)}\right)$.

Пусть $n = \sum\limits_{i=1}^{t} k_i$. Для каждого $1 \le j \le n$ через e_j обозначим элемент из $\bigoplus\limits_{i=1}^{t}(R/P^{n_i})^{k_i}$, у которого все компоненты за исключением j-й равны 0, а j-я компонента равна единице в фактор-кольце, которое соответствует индексу j. Модули M/PM и F/PF имеют естественные структуры векторного пространства над полем R/M при этом, очевидно, $(e_i + PF)_{i=1}^{n}$ – базис векторного пространства F/PF. Несложно заметить, что матрица эндоморфизма $\Psi_1\overline{\varphi}\Psi_1^{-1}$ имеет вид

$$\overline{A} = \begin{pmatrix} A_{11} \pmod P & A_{12} \pmod P & \cdots & A_{1t} \pmod P \\ 0 & A_{22} \pmod P & \cdots & A_{2t} \pmod P \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_{tt} \pmod P \end{pmatrix}.$$

Тогда согласно теореме 47

$$\left(\frac{\overline{\varphi}}{M/PM}\right)_{\mathrm{C}} = \left(\frac{\det \overline{A}}{R/P}\right) = \left(\frac{\prod_{i=1}^{t} \det(A_{ii} \pmod P)}{R/P}\right) = \prod_{i=1}^{t}\left(\frac{\det(A_{ii} \pmod P)}{P}\right).$$

Матрица эндоморфизма $\Psi_2\varphi'\Psi_2^{-1}$ равна $(A_{ij} \pmod{P^{\min(n_i,n_j)-1}})_{i,j\in I'}$. Тогда по предположению индукции имеем

$$\left(\frac{\varphi'}{PM}\right)_{\mathrm{C}} = \prod_{i\in I'}\left(\frac{\det(A_{ii} \pmod{P^{n_i-1}})}{P^{n_i-1}}\right) = \prod_{i\in I'}\left(\frac{\det A_{ii} \pmod P)}{P}\right)^{n_i-1}.$$

Пусть $I'' = \{i \mid n_i = 1\}$. Тогда

$$\prod_{i=1}^{t}\left(\frac{\det(A_{ii} \pmod P)}{P}\right) = \left(\prod_{i\in I''}\left(\frac{\det A_{ii} \pmod P)}{P}\right)\right)\left(\prod_{i\in I'}\left(\frac{\det A_{ii} \pmod P)}{P}\right)\right).$$

При этом, если $I'' = \emptyset$, то будем считать, что $\left(\prod_{i\in I''}\left(\frac{\det A_{ii} \pmod P)}{P}\right)\right) = 1$.

Таким образом, имеют место равенства

$$\left(\frac{\varphi}{M}\right)_{\mathrm{C}} = \left(\frac{\varphi'}{PM}\right)_{\mathrm{C}}\left(\frac{\overline{\varphi}}{M/PM}\right)_{\mathrm{C}} = \left(\prod_{i\in I'}\left(\frac{\det A_{ii} \pmod P}{P}\right)^{n_i-1}\right)\left(\prod_{i=1}^{t}\left(\frac{\det A_{ii} \pmod P}{P}\right)\right) =$$
$$\left(\prod_{i\in I'}\left(\frac{\det A_{ii} \pmod P}{P}\right)^{n_i-1}\right)\left(\prod_{i\in I''}\left(\frac{\det A_{ii} \pmod P}{P}\right)\right)\left(\prod_{i\in I'}\left(\frac{\det A_{ii} \pmod P}{P}\right)\right) =$$
$$\left(\prod_{i\in I'}\left(\frac{\det A_{ii} \pmod P}{P}\right)^{n_i}\right)\left(\prod_{i\in I''}\left(\frac{\det A_{ii} \pmod P}{P}\right)\right) = \prod_{i=1}^{t}\left(\frac{\det A_{ii} \pmod P}{P}\right)^{n_i} =$$
$$\prod_{i=1}^{t}\left(\frac{\det A_{ii}}{P^{n_i}}\right).$$

Это завершает индукционный шаг. □

Следующие утверждения несложно следуют из предыдущей теоремы с помощью свойства мультипликативности символа Картье и китайской теоремы об остатках для колец.

Теорема 51. *Пусть M – конечно порожденный периодический модуль над абстрактным числовым кольцом R и*

$$M \cong \bigoplus_{i=1}^{r}\bigoplus_{j=1}^{t_i}\left(R/P_i^{n_{ij}}\right)^{k_{ij}},$$

где $P_1, \ldots, P_r$ – различные нечетные простые идеалы R и $1 \leq n_{i1} < \cdots < n_{it_i}$ для каждого $1 \leq i \leq r$. Если $\varphi \in \mathrm{Aut}(M)$, φ_i – автоморфизм P_i-примарной компоненты M, который

является ограничением φ на нее, и $A^{(i)} = (A^{(i)}_{lm})$ – матрица φ_i, где $A^{(i)}_{jj} \in M_{k_{ij}}(R/P_i^{n_{ij}})$, то

$$\left(\frac{\varphi}{M}\right)_{\mathrm{C}} = \prod_{i=1}^{r}\left(\prod_{j=1}^{t_i}\left(\frac{\det(A^{(i)}_{jj})}{P_i^{n_{ij}}}\right)\right).$$

Теорема 52 (И. Шур, 1921, [40]). *Пусть n – нечетное натуральное число, и $k \geq 1$. Рассмотрим $G = \mathbb{Z}_n^k$ как свободный модуль ранга k над кольцом $\mathbb{Z}_n$. Для любого автоморфизма $\varphi \in \mathrm{Aut}(G)$, который как автоморфизм модуля над $\mathbb{Z}_n$ представим обратимой матрицей $A \in \mathrm{GL}_k(\mathbb{Z}_n)$, справедливо равенство*:

$$\left(\frac{\varphi}{G}\right)_{\mathrm{C}} = \left(\frac{\det A}{n}\right),$$

где $\left(\dfrac{\det A}{n}\right)$ – символ Якоби.

5. Законы взаимности для многочленов

5.1. Квадратичный закон взаимности для многочленов. До конца этого параграфа будем считать, что $q = p^k$, где p – нечетное простое число. Ненулевой многочлен $f \in \mathbb{F}_q[t]$ будем называть нормированным, если его старший коэффициент равен единице. Для произвольного ненулевого многочлена $f \in \mathbb{F}_q[t]$ количество элементов в фактор-алгебре $\mathbb{F}_q[t]/(f)$ будем обозначать $|f|$. Ясно, что $|f| = q^{\deg(f)}$.

Теорема 53 (закон взаимности Дедекинда–Артина (Дедекинд, 1857 [42]; Кюне, 1902 [43]; Артин, 1924 [44])). *Пусть $f, g \in \mathbb{F}_q[t]$ – ненулевые взаимно простые нормированные многочлены, степени которых ≥ 1. Тогда справедливо равенство*:

$$\left(\frac{f}{g}\right)\left(\frac{g}{f}\right) = (-1)^{\frac{|f|-1}{2}\cdot\frac{|g|-1}{2}} = (-1)^{\frac{q-1}{2}\deg f \deg g}.$$

Доказательство. Пусть

$$f = t^n + a_{n-1}t^{n-1} + \cdots + a_0, \qquad g = t^m + b_{m-1}t^{m-1} + \cdots + b_0.$$

Всякий смежный класс $[h]_{fg}$ из $\mathbb{F}_q[t]/(fg)$ можно однозначно представить в одном из трех видов:

$$[h]_{fg} = [u_1 + fv_1]_{fg} = [gu_2 + v_2]_{fg} = [u_3 + t^n v_3]_{fg},$$

где $\deg u_1, \deg u_2, \deg u_3 < n$, а $\deg v_1, \deg v_2, \deg v_3 < m$.

Пусть $\mathcal{A}$ и $\mathcal{B}$ – линейные операторы, действующие в векторном пространстве $\mathbb{F}_q[t]/(fg)$ соответственно по правилам:

$$\mathcal{A}\colon [u + t^n v]_{fg} \mapsto [u + fv]_{fg}, \qquad \mathcal{B}\colon [u + t^n v]_{fg} \mapsto [gu + v]_{fg},$$

где $\deg u < n$, $\deg v < m$.

Согласно теореме 7 имеют место равенства:

$$\left(\frac{f}{g}\right)\left(\frac{g}{f}\right) = Z(f,g) = \operatorname{sgn}(\mathcal{A})\operatorname{sgn}(\mathcal{B}).$$

Выпишем матрицы линейных операторов $\mathcal{A}$ и $\mathcal{B}$ относительно базиса $[1]_{fg}, [t]_{fg}, \ldots, [t^{m+n-1}]_{fg}$ векторного пространства $\mathbb{F}_q[t]/(fg)$.

Так как $\mathcal{A}([t^i]_{fg}) = [t^i]_{fg}$ для $0 \leq i < n$ и $\mathcal{A}([t^{n+i}]_{fg}) = [ft^i]_{fg}$ для $0 \leq i < m$, то матрица A оператора $\mathcal{A}$ имеет верхнетреугольный блочный вид:

$$A = \begin{pmatrix} 1 & 0 & \ldots & 0 & a_0 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & a_1 & a_0 & \ldots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 & a_{n-1} & a_{n-2} & \ldots & * \\ 0 & 0 & \ldots & 0 & 1 & a_{n-1} & \ldots & * \\ 0 & 0 & \ldots & 0 & 0 & 1 & \ldots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 1 \end{pmatrix}.$$

Ясно, что $|A| = 1$.

Теперь обратимся к оператору $\mathcal{B}$. Так как $\mathcal{B}([t^i]_{fg}) = [gt^i]_{fg}$ для $0 \leq i < n$ и $\mathcal{B}([t^{n+i}]_{fg}) = [t^i]_{fg}$ для $0 \leq i < m$, то его матрица B имеет вид:

$$B = \begin{pmatrix} b_0 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ b_1 & b_0 & \ldots & * & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{m-1} & b_{m-2} & \ldots & * & 0 & 0 & \ldots & 1 \\ 1 & b_{m-1} & \ldots & * & 0 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & * & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 & 0 & 0 & \ldots & 0 \end{pmatrix}.$$

В матрице B поменяем местами две подматрицы, состоящие соответственно из первых n столбцов и последних m столбцов. В результате получим матрицу

$$B' = \begin{pmatrix} 1 & 0 & \dots & 0 & b_0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & b_1 & b_0 & \dots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & b_{m-1} & b_{m-2} & \dots & * \\ 0 & 0 & \dots & 0 & 1 & b_{m-1} & \dots & * \\ 0 & 0 & \dots & 0 & 0 & 1 & \dots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Так как $|B'| = 1$, то $|B| = (-1)^{nm}|B'| = (-1)^{nm}$.

Тогда, согласно теореме 47 и лемме Эйлера, имеют место равенства:

$$Z(f,g) = \operatorname{sgn}(\mathcal{A})\operatorname{sgn}(\mathcal{B}) = \left(\frac{\det A}{\mathbb{F}_q}\right)\left(\frac{\det B}{\mathbb{F}_q}\right) = \left(\frac{(-1)^{nm}}{\mathbb{F}_q}\right) = \left(\frac{-1}{\mathbb{F}_q}\right)^{nm} = (-1)^{\frac{q-1}{2}nm}.$$

Несложно заметить, что

$$nm\,\frac{q-1}{2} \equiv \frac{|f|-1}{2}\cdot\frac{|g|-1}{2} \pmod 2.$$

Таким образом, окончательно получаем:

$$\left(\frac{f}{g}\right)\left(\frac{g}{f}\right) = (-1)^{\frac{|f|-1}{2}\cdot\frac{|g|-1}{2}}.$$ □

Следствие 54. *Пусть $f, g \in \mathbb{F}_q[t]$ – ненулевые нормированные многочлены и $(f,g) = 1$. Тогда $\left(\frac{f}{g}\right) = \left(\frac{g}{f}\right)$, если выполняется одно из условий*:

1) $q \equiv 1 \pmod 4$;

2) *f или g имеют четную степень.*

Лемма 55. *Пусть $c \in \mathbb{F}_q^*$ и $g \in \mathbb{F}_q[t]$ – нормированный ненулевой многочлен. Тогда*

$$\left(\frac{c}{g}\right) = \left(\frac{c}{\mathbb{F}_q}\right)^{\deg(g)}.$$

В частности, если g имеет четную степень, то

$$\left(\frac{c}{g}\right) = 1.$$

Доказательство. Пусть $g = \pi_1^{\alpha_1}\cdot\ldots\cdot\pi_s^{\alpha_s}$ – разложение g на неприводимые нормированные

множители в $\mathbb{F}_q[t]$. Тогда

$$\left(\frac{c}{g}\right)_{\mathbb{F}_q[t]} = \prod_{i=1}^{s}\left(\frac{c}{\pi_i}\right)^{\alpha_i} = \prod_{i=1}^{s}\left(\frac{c}{\mathbb{F}_q[t]/(\pi_i)}\right)^{\alpha_i}.$$

Для каждого $1 \leq i \leq s$ имеют место равенства

$$\left(\frac{c}{\mathbb{F}_q[t]/(\pi_i)}\right) = c^{\frac{q^{\deg(\pi_i)}-1}{2}} = \left(c^{\frac{q-1}{2}}\right)^{1+q+\cdots+q^{\deg\pi_i-1}} = \left(\frac{c}{\mathbb{F}_q}\right)^{1+q+\cdots+q^{\deg\pi_i-1}} = \left(\frac{c}{\mathbb{F}_q}\right)^{\deg(\pi_i)}.$$

Таким образом,

$$\left(\frac{c}{g}\right) = \prod_{i=1}^{s}\left(\left(\frac{c}{\mathbb{F}_q}\right)^{\deg\pi_i}\right)^{\alpha_i} = \left(\frac{c}{\mathbb{F}_q}\right)^{\sum\limits_{i=1}^{s}\alpha_i\deg\pi_i} = \left(\frac{c}{\mathbb{F}_q}\right)^{\deg(g)}. \qquad \square$$

5.2. Квадратичный закон взаимности для линейных операторов. Пусть q – степень нечетного простого числа, а $\mathbb{F}_q$ – конечное поле из q элементов. Рассмотрим векторное пространство V конечной размерности N над полем $\mathbb{F}_q$ и произвольный линейный оператор $A : V \to V$. Векторное пространство V обладает естественной структурой модуля над кольцом многочленов $\mathbb{F}_q[x]$, где умножение задается правилом:

$$f(x)\cdot v := f(A)(v) \quad \text{для любых } f(x) \in \mathbb{F}_q[x] \text{ и } v \in V.$$

Полученный модуль мы будем обозначать ${}_AV$.

Известно, что аннулятором этого модуля является идеал, порожденный минимальным многочленом оператора A, который мы обозначим $n(x)$. Рассмотрим нормированный многочлен $m(x) \in \mathbb{F}_q[x]$, взаимно простой с $n(x)$. Поскольку $(m(x), n(x)) = 1$, оператор $m(A)$ обратим на V и, следовательно, умножение на $m(x)$ задает автоморфизм конечного модуля ${}_AV$. Этот автоморфизм индуцирует перестановку на конечном множестве векторов пространства V. Знак этой перестановки есть символ Картье, который мы обозначаем $\left(\frac{m(x)}{{}_AV}\right)$.

Теорема 56. *Пусть V – векторное пространство размерности N над конечным полем $\mathbb{F}_q$ нечетной характеристики, $A \in \mathrm{End}_{\mathbb{F}_q}V$ и $m(x) \in \mathbb{F}_q[x]$ – нормированный многочлен, взаимно простой с минимальным многочленом $n(x)$ линейного оператора A. Тогда*:

$$\left(\frac{m(x)}{{}_AV}\right) = \left(\frac{\det(A - xE)}{m(x)}\right).$$

Доказательство. Пусть $n(x) = p_1(x)^{e_1}p_2(x)^{e_2}\dots p_k(x)^{e_k}$ – разложение многочлена $n(x)$ на попарно различные неприводимые над $\mathbb{F}_q$ нормированные множители. Характеристический многочлен оператора A имеет вид $(-1)^N p_1(x)^{c_1}\dots p_k(x)^{c_k}$, где $c_i \geq e_i$ для каждого

$1 \le i \le k$. Тогда хорошо известно, что имеет место изоморфизм

$$ {}_AV \cong \bigoplus_{j=1}^{k} \bigoplus_{i=1}^{t_j} \left(\mathbb{F}_q[x]/(p_j(x))^{s_{ji}}\right)^{k_{ji}}, $$

где $c_j = \sum\limits_{i=1}^{t_j} k_{ji}s_{ji}$. Следовательно, согласно теореме 43 имеем

$$ \left(\frac{m(x)}{{}_AV}\right) = \left(\frac{m(x)}{\bigoplus\limits_{j=1}^{k}\bigoplus\limits_{i=1}^{t_j}\left(\mathbb{F}_q[x]/(p_j(x))^{s_{ji}}\right)^{k_{ji}}}\right) = \prod_{j=1}^{k}\prod_{i=1}^{t_j}\left(\frac{m(x)}{p_j(x)}\right)^{k_{ji}s_{ji}} = \prod_{j=1}^{k}\left(\frac{m(x)}{p_j(x)}\right)^{\sum_{i=1}^{t_j}k_{ji}s_{ji}} = $$

$$ \prod_{j=1}^{k}\left(\frac{m(x)}{p_j(x)}\right)^{c_j} = \left(\frac{m(x)}{p_A(x)}\right). $$

Поскольку многочлены $m(x)$ и $p_A(x)$ взаимно просты, и оба по условию являются нормированными, то согласно теореме 53 имеет место равенство:

$$ \left(\frac{m(x)}{p_A(x)}\right)) = (-1)^{\frac{q-1}{2}\deg(m(x))N}\left(\frac{p_A(x)}{m(x)}\right). $$

Согласно лемме 55 имеем

$$ \left(\frac{(-1)^N}{m(x)}\right) = (-1)^{\frac{q-1}{2}N\deg(m(x))}. $$

Таким образом, имеют место равенства

$$ \left(\frac{m(x)}{{}_AV}\right) = \left(\frac{(-1)^N}{m(x)}\right)\left(\frac{p_A(x)}{m(x)}\right) = \left(\frac{(-1)^N p_A(x)}{m(x)}\right) = \left(\frac{\det(A-xE)}{m(x)}\right). \qquad \square $$

Следующее утверждение можно рассматривать как аналог предложения 15.

Следствие 57. *Пусть V – векторное пространство размерности N над конечным полем $\mathbb{F}_q$ нечетной характеристики, $A, B \in \mathrm{End}_{\mathbb{F}_q} V$ – нильпотентные линейные операторы, а $m(x) \in \mathbb{F}_q[x]$ – нормированный многочлен с ненулевым свободным членом. Тогда*:

$$ \left(\frac{m(x)}{{}_AV}\right) = \left(\frac{m(x)}{{}_BV}\right). $$

5.3. Степенной закон взаимности для многочленов. До конца настоящего параграфа будем предполагать, что $q = p^k$, где p – нечетное простое число, а $n > 1$ – натуральное число, для которого выполнено условие $n \mid (q-1)$.

Лемма 58. *Пусть $\pi \in \mathbb{F}_q[t]$ – неприводимый нормированный многочлен, $f \in \mathbb{F}_q[t]$ – ненулевой нормированный многочлен, причем $(f, \pi) = 1$. Тогда элемент $[f]_\pi^{\frac{|\pi|-1}{n}} \in \mathbb{F}_q[x]/(\pi)$ при-*

надлежит подполю $\mathbb{F}_q$ *и является корнем многочлена* $x^n - 1$.

Доказательство. Поскольку многочлены f и π взаимно просты, по малой теореме Ферма для конечного поля $\mathbb{F}_q[t]/(\pi)$ имеет место равенство $[f]_\pi^{|\pi|-1} = 1$. Следовательно, элемент $[f]_\pi^{\frac{|\pi|-1}{n}}$ является корнем многочлена $x^n - 1$. Утверждение леммы теперь непосредственно вытекает из того факта, что согласно условию $n \mid (q-1)$, все корни уравнения $x^n - 1 = 0$ лежат в основном поле $\mathbb{F}_q$. □

Пусть $\pi \in \mathbb{F}_q[t]$ – неприводимый нормированный многочлен, $f \in \mathbb{F}_q[t]$ – ненулевой нормированный многочлен и $(f, \pi) = 1$. Согласно лемме 58, существует однозначно определенный корень n-й степени из единицы $c \in \mathbb{F}_q$, для которого в кольце $\mathbb{F}_q[t]$ имеет место сравнение:

$$c \equiv f^{\frac{|\pi|-1}{n}} \pmod{\pi}.$$

Этот элемент c обозначается $\left(\frac{f}{\pi}\right)_n$ и называется обобщенным символом Лежандра многочлена f по модулю π.

Следующее утверждение проверяется непосредственно.

Лемма 59. *Пусть* $\pi \in \mathbb{F}_q[t]$ *– неприводимый нормированный многочлен,* $f, g \in \mathbb{F}_q[t]$ *– ненулевые нормированные многочлены и* $(fg, \pi) = 1$. *Тогда*:

$$\left(\frac{fg}{\pi}\right)_n = \left(\frac{f}{\pi}\right)_n \cdot \left(\frac{g}{\pi}\right)_n.$$

Пусть $g \in \mathbb{F}_q[t]$ – нормированный многочлен, $g = \pi_1^{a_1} \cdots \pi_s^{a_s}$ – его разложение на попарно различные неприводимые нормированные множители $\pi_1, \ldots, \pi_s$ и $f \in \mathbb{F}_q[t]$ – нормированный многочлен, взаимно простой с g. Обобщенный символ Якоби для многочлена f по модулю g определяется согласно правилу:

$$\left(\frac{f}{g}\right)_n := \prod_{i=1}^{s} \left(\frac{f}{\pi_i}\right)_n^{a_i}.$$

Пусть $f, g \in \mathbb{F}_q[t]$ – нормированные многочлены,

$$f = (t - \alpha_1) \ldots (t - \alpha_d), \qquad g = (t - \beta_1) \ldots (t - \beta_m),$$

где $\alpha_i, \beta_j \in \overline{\mathbb{F}}_q$. Тогда для результанта $\mathrm{res}(f, g)$ многочленов f и g имеет место равенство

$$\mathrm{res}(f, g) = \prod_{j=1}^{m} f(\beta_j) = \prod_{i=1}^{d} \prod_{j=1}^{m} (\beta_j - \alpha_i) \in \mathbb{F}_q.$$

Следующие два утверждения проверяются непосредственно.

Лемма 60 (бимультипликативность результанта)**.** *Пусть P – поле и $f_1, f_2, g_1, g_2 \in P[t]$ – нормированные многочлены. Тогда*

$$\operatorname{res}(f_1 f_2, g) = \operatorname{res}(f_1, g) \cdot \operatorname{res}(f_2, g),$$
$$\operatorname{res}(f, g_1 g_2) = \operatorname{res}(f, g_1) \cdot \operatorname{res}(f, g_2).$$

Лемма 61 (закон взаимности для многочленов в слабой форме)**.** *Пусть P – поле и $f, g \in P[t]$ – нормированные многочлены. Тогда справедливо равенство*

$$\operatorname{res}(f, g) = (-1)^{\deg(f)\cdot\deg(g)} \operatorname{res}(g, f). \tag{22}$$

Теорема 62. *Для нормированных взаимно простых многочленов $f, g \in \mathbb{F}_q[t]$ имеет место равенство*

$$\left(\frac{f}{g}\right)_n = (\operatorname{res}(f, g))^{\frac{q-1}{n}}.$$

В частности, если g – неприводимый многочлен то уравнение $x^n = [f]_g$ имеет решение в поле $\mathbb{F}_q[x]/(g)$ в точности тогда, когда уравнение $x^n = \operatorname{res}(f, g)$ имеет решение в поле $\mathbb{F}_q$.

Доказательство. Предположим сначала, что g – неприводимый нормированный многочлен. Пусть $\alpha \in \overline{\mathbb{F}}_q$ – корень многочлена g. Тогда автоморфизм Фробениуса поля $\mathbb{F}_q(\alpha)$, действующий согласно правилу $x \mapsto x^q$, является образующим циклической группы Галуа расширения $\mathbb{F}_q(\alpha)/\mathbb{F}_q$. Поскольку всякий автоморфизм из группы Галуа однозначно определяется своим действием на элемент α и $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \deg(g)$, то

$$\alpha, \alpha^q, \ldots, \alpha^{q^{\deg(g)-1}}$$

– все попарно различные корни многочлена g. Тогда

$$\operatorname{res}(f, g) = \prod_{j=0}^{\deg(g-1} f(\alpha^{q^j}) = \prod_{j=0}^{\deg(g)-1} f(\alpha)^{q^j} = f(\alpha)^{\sum\limits_{j=0}^{\deg(g)-1} q^j} = f(\alpha)^{\frac{q^{\deg(g)}-1}{q-1}}.$$

Следовательно, учитывая, что $|g| = q^{\deg(g)}$, имеем

$$(\operatorname{res}(f, g))^{\frac{q-1}{n}} = f(\alpha)^{\frac{|g|-1}{n}}.$$

При гомоморфизме $\varphi\colon \mathbb{F}_q[t] \to \mathbb{F}_q(\alpha)$, действующем на произвольный многочлен $h(t) \in \mathbb{F}_q[t]$ по правилу $h(t) \mapsto h(\alpha)$, многочлен $f(t)^{\frac{|g|-1}{n}}$ переходит в элемент $f(\alpha)^{\frac{|g|-1}{n}}$, который является корнем уравнения $x^n - 1 = 0$. Тогда $f(\alpha)^{\frac{|g|-1}{n}} \in \mathbb{F}_q$ и в кольце $\mathbb{F}_q[x]$ имеет место сравнение:

$$f(\alpha)^{\frac{|g|-1}{n}} \equiv f(t)^{\frac{|g|-1}{n}} \pmod{g}.$$

Следовательно, по определению обобщенного символа Лежандра имеем $f(\alpha)^{\frac{|g|-1}{n}} = \left(\frac{f}{g}\right)_n$. Таким образом,

$$\left(\frac{f}{g}\right)_n = (\mathrm{res}(f,g))^{\frac{q-1}{n}}.$$

Пусть теперь g – произвольный нормированный многочлен, взаимно простой с f. Разложим g на нормированные неприводимые множители:

$$g = \pi_1^{a_1} \cdots \pi_s^{a_s}.$$

Тогда, согласно изложенному выше и лемме 60, имеют место равенства

$$\left(\frac{f}{g}\right)_n = \prod_{i=1}^{s} \left(\frac{f}{\pi_i}\right)_n^{a_i} = \prod_{i=1}^{s} \left[(\mathrm{res}(f,\pi_i))^{\frac{q-1}{n}}\right]^{a_i} = \prod_{i=1}^{s} (\mathrm{res}(f,\pi_i))^{a_i \frac{q-1}{n}} =$$
$$= \left(\prod_{i=1}^{s} (\mathrm{res}(f,\pi_i))^{a_i}\right)^{\frac{q-1}{n}} = (\mathrm{res}(f,g))^{\frac{q-1}{n}}.$$

□

Теорема 63 (степенной закон взаимности для многочленов; Артин, 1924 [44])**.** *Для нормированных взаимно простых многочленов $f, g \in \mathbb{F}_q[t]$ имеет место равенство*

$$\left(\frac{f}{g}\right)_n = (-1)^{\deg(f)\deg(g)\frac{q-1}{n}} \left(\frac{g}{f}\right)_n.$$

Доказательство. Согласно теоремам 62 и 61 имеют место равенства:

$$\left(\frac{f}{g}\right)_n = (\mathrm{res}(f,g))^{\frac{q-1}{n}} = \left((-1)^{\deg(f)\deg(g)}\,\mathrm{res}(g,f)\right)^{\frac{q-1}{n}}$$
$$= \left((-1)^{\deg(g)\deg(f)}\right)^{\frac{q-1}{n}} \cdot (\mathrm{res}(g,f))^{\frac{q-1}{n}} = (-1)^{\deg(f)\deg(g)\frac{q-1}{n}} \left(\frac{g}{f}\right)_n.$$

□

Отметим, что широкие обобщения теоремы 63 были предложены в недавних работах [45, 46].

5.4. Результант и квадратичный закон взаимности. В данном параграфе будут рассмотрены подходы к доказательству квадратичного закона взаимности, основанные на равенстве (22).

Следующее утверждение, которое является следствием леммы Гаусса–Шеринга, хорошо известно (см., например, [47, с. 142–143]).

Лемма 64. *Для любых положительных нечетных взаимно простые чисел m, n имеет*

место равенство

$$\left(\frac{m}{n}\right) = (-1)^{\sum_{i=1}^{\frac{n-1}{2}}\left[\frac{mi}{n}\right]}.$$

С помощью этой леммы, используя геометрические соображения, Эйзенштейн в работе [48] привел короткое доказательство квадратичного закона взаимности, которое изложено во многих учебниках по теории чисел. В работе [49] Кронекер нашел другое короткое менее известное доказательство на основе леммы 64, которое непосредственно следует из следующего утверждения.

Лемма 65. *Пусть m, n – положительные нечетные взаимно простые числа > 1. Тогда*

$$\left(\frac{m}{n}\right) = \operatorname{sgn}\left(\prod_{j=1}^{\frac{m-1}{2}}\prod_{i=1}^{\frac{n-1}{2}}\left(\frac{j}{m} - \frac{i}{n}\right)\right).$$

Доказательство. Далее для произвольного ненулевого вещественного числа a положим

$$\operatorname{sgn}(a) := \begin{cases} 1, & \text{если } a > 0; \\ -1, & \text{если } a < 0. \end{cases}$$

Так как для любых нечетных положительных чисел $n, m \geq 3$ выполнено неравенство $\left[\frac{n-1}{n} \cdot \frac{m}{2}\right] \leq \frac{m-1}{2}$, то при каждом фиксированном i количество натуральных $j \in \left\{1, \ldots, \frac{m-1}{2}\right\}$, таких что $j - \frac{im}{n} < 0$, в точности равно $\left[\frac{mi}{n}\right]$. Следовательно, согласно лемме 64 имеем

$$\operatorname{sgn}\left(\prod_{i=1}^{\frac{n-1}{2}}\prod_{j=1}^{\frac{m-1}{2}}\left(\frac{j}{m} - \frac{i}{n}\right)\right) = \operatorname{sgn}\left(\prod_{i=1}^{\frac{n-1}{2}}\prod_{j=1}^{\frac{m-1}{2}}\left(j - \frac{im}{n}\right)\right) = \prod_{i=1}^{\frac{n-1}{2}}(-1)^{\left[\frac{mi}{n}\right]} = \left(\frac{m}{n}\right). \qquad \square$$

Пусть f – произвольная строго возрастающая вещественная функция и для каждого нечетного $k \in \mathbb{N}$ положим $F_k(x) = \prod_{i=1}^{\left[\frac{k}{2}\right]}\left(x - f\left(\frac{i}{k}\right)\right)$. Из предыдущей леммы следует, что для любых нечетных положительных чисел $n, m \geq 3$ имеет место равенство

$$\operatorname{sgn}(\operatorname{res}(F_m(x), F_n(x))) = \left(\frac{m}{n}\right),$$

которое в силу равенства (22) с помощью выбранного семейства многочленов $(F_k(x))_{k\in\mathbb{N}}$ будет давать доказательство квадратичного закона взаимности. Интересно отметить, что существуют семейства многочленов $(F_k(x))_{k\in\mathbb{N}}$, тесно связанных с многочленами Чебышева первого и второго рода и для которых для любых нечетных положительных чисел

$n, m \geq 3$ выполняется равенство

$$\operatorname{res}(F_m(x), F_n(x)) = \left(\frac{m}{n}\right),$$

не содержащее функцию знака. Напомним, что многочлены Чебышева первого и второго рода определяются соответственно с помощью следующих равенств:

$$\cos \alpha n = T_n(\cos \alpha), \qquad \frac{\sin \alpha n}{\sin \alpha} = U_n(\cos \alpha).$$

При этом явные выражения для соответственно многочленов Чебышева первого и второго рода имеют вид

$$T_n(x) = \frac{1}{2} \sum_{i=0}^{[n/2]} (-1)^i \frac{n}{(n-i)} \binom{n-i}{i} (2x)^{n-2i},$$

$$U_n(x) = \sum_{i=0}^{[\frac{n-1}{2}]} (-1)^i \binom{n-i-1}{i} (2x)^{n-2i-1}.$$

Если n – нечетное натуральное число, то существуют многочлены $H_n(x)$ и $F_n(x)$, для которых соответственно имеют место равенства

$$T_n(x) = (-1)^{\frac{n-1}{2}} \cdot x \cdot H_n(-4x^2), \qquad U_n(x) = F_n(4x^2 - 4).$$

Для нечетных взаимно простых m, n равенство $\operatorname{res}(F_m(x), F_n(x)) = \left(\frac{m}{n}\right)$ следует из несложной вариации доказательства Эйзенштейна [51, с. 20–21] закона взаимности, приведенного в работе [50, с. 322], а элегантное доказательство равенства $\operatorname{res}(H_m(x), H_n(x)) = \left(\frac{m}{n}\right)$ найдено М. Бейкером [52].

Список литературы

[1] И.Г. Башмакова, Е.И. Славутин, *История диофантова анализа от Диофанта до Ферма*, Наука, М., 1984.

[2] Г.П. Матвиевская, Е.П. Ожигова, *Неопубликованные материалы Л. Эйлера по теории чисел*, Наука, СПб., 1997.

[3] L. Euler, *Theoremata circa divisores numerorum in hac forma* $pa^2 \pm qb^2$ *contentorum*, Comm. Acad. Sci. Petersburg **14**, 151–181 (1744/1746).

[4] L. Euler, Observationes circa divisionem quadratorum per numeros primos, in: Opera Omnia, Series I, V. **3**, 477–512 (1783).

[5] A. Legendre, *Reserches dánalyse indéterminée*, Histoiré de l'Académie Royale des Sciences de Paris, 465–559 (1785).

[6] A. Legendre, Essai sur la théorie des nombres, Paris, 1798.

[7] C.F. Gauss, *Theorematis arithmetici demonstratio nova*, Comment. Soc. regiae sci. Göttingen XVI, 1808.

[8] К.Ф. Гаусс, *Труды по теории чисел*, ред. И.М. Виноградов, коммент. Б.Н. Делоне, Изд-во АН СССР, М., 1959.

[9] F. Lemmermeyer, *Proofs of the quadratic reciprocity law*. URL: https://uni-heidelberg.de (архивировано: https://web.archive.org/web/20250106010310/https://www.mathi.uni-heidelberg.de/~flemmermeyer/qrg_proofs.html).

[10] E. Artin, *Beweis des allgemeinen Reziprozitätsgesetzes*, Abh. Math. Semin. Univ. Hambg. **5** (1), 353–363 (1927).
DOI: https://doi.org/10.1007/BF02952531

[11] Н.Г. Чеботарёв, *Собрание сочинений*: *в* 3 *т.*, Изд-во АН СССР, М.–Л., 1949–1950.

[12] G. Zolotareff, *Nouvelle démonstration de la réciprocité de Legendre*, Nouv. Ann. Math. (ser. 2) **11**, 109–111 (1872).

[13] F. Keune, *Number fields*, Radboud University Press, 2023.

[14] A. Brunyate, P.L. Clark, *Extending the Zolotarev–Frobenius approach to quadratic reciprocity*, Ramanujan J. **37** (1), 25–50 (2015).
DOI: https://doi.org/10.1007/s11139-014-9635-y

[15] P. Cartier, *Sur une généralisation des symboles de Legendre–Jacobi*, L'Enseignement Mathématique. 2e sér **16** (1), 31–48 (1970).

[16] B.R. McDonald, *Finite rings with identity*, Marcel Dekker, Inc., New York, 1974.

[17] G. Frobenius, *Über das quadratische Reciprozitätsgesetz.* I, S.–B. Preuss. Akad. Wiss., Berlin, 335–349, 1914.

[18] M. Lerch, *Sur un théorème de Zolotarev*, Bull. Intern. de l'Acad. Fr. Joseph **3**, 34–37 (1896).

[19] W. Duke, K. Hopkins, *Quadratic reciprocity in a finite group*, Amer. Math. Monthly **112** (3), 251–256 (2005).
DOI: https://doi.org/10.1080/00029890.2005.11920190

[20] M. Hablicsek, G. Mantilla-Soler, *Power map permutations and symmetric differences in finite groups*, J. Algebra Appl. **10** (5), 947–959 (2011).
DOI: https://doi.org/10.1142/S0219498811005051

[21] J. Neukirch, *Algebraic number theory*, in: Grundlehren der mathematischen Wissenschaften **322**, Springer-Verlag, Berlin, 1999.
DOI: https://doi.org/10.1007/978-3-662-03983-0

[22] Г.Дж. Януш, *Алгебраические числовые поля*, Научная книга (ИДМИ), Новосибирск, 2001.

[23] О. Зарисский, П. Самюэль, *Коммутативная алгебра, Т.* 1, Изд-во иностранной литературы, М., 1963.

[24] А.Н. Абызов, *Квадратичный закон взаимности по Золотареву и его обобщение*, Матем. и теор. комп. науки **3** (1), 4–11 (2025).
DOI: https://doi.org/10.26907/2949-3919.2025.1.4-11

[25] H. Chua, *Quadratic reciprocity via Vandermonde matrix*, Amer. Math. Monthly **133** (4), 376–379 (2026).
DOI: https://doi.org/10.1080/00029890.2025.2600902

[26] J. Delsarte, *Une démonstration de la loi de réciprocité quadratique*, Œuvres de Jean Delsarte Vol. **2**, 827–850 (1950).

[27] K. Motose, *On Gauss sums and Vandermonde matrices*, Bull. Fac. Sci. Technol. Hirosaki Univ. **6** (1), 19–23 (2003).

[28] F. Keune, *Quadratic reciprocity and finite fields*, Nieuw. Arch. Wisk. **9**, 263–266 (1991).

[29] M. Dicker, *A proof of the quadratic reciprocity law*, arXiv:1210.7744 (2012).
URL: http://arxiv.org/abs/1210.7744.

[30] C.F. Gauss, *Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et amplicationes novae*, 1818, Werke, vol. II, in: Georg Olms Verlag, Hildescheim, 47–64, 1973.

[31] K. Motose, *On commutative group algebras*, Sci. Rep. Hirosaki Univ. **40** (2), 127–131 (1993).

[32] K. Motose, *On commutative group algebras.* III, Bull. Fac. Sci. Technol. Hirosaki Univ. **1** (2), 93–97 (1999).

[33] З.И. Боревич, И.Р. Шафаревич, *Теория чисел*, Наука, М., 1972.

[34] К. Айерлэнд, М. Роузен, *Классическое введение в современную теорию чисел*, Мир, М., 1987.

[35] O. Baumgart, *The quadratic reciprocity law. A collection of classical proofs*, Edited, translated from the German, and with contributions by Franz Lemmermeyer. Birkhäuser/Springer, Cham, 2015.
DOI: https://doi.org/10.1007/978-3-319-16283-6

[36] F. Lemmermeyer, *Quadratic number fields*, Springer, Cham, 2021.
DOI: https://doi.org/10.1007/978-3-030-78652-6

[37] A. Hausner, *On the quadratic reciprocity theorem*, Arch. Math. **12**, 182–183 (1961).
DOI: https://doi.org/10.1007/BF01650546

[38] E. Schering, *Zur Theorie der Quadratischen Reste*, Acta Math. **1**, 153–170 (1882).
DOI: https://doi.org/10.1007/BF02592132

[39] J.A. Dieudonné, *La géométrie des groupes classiques*, Springer-Verlag, Berlin–New York, 1971.
DOI: https://doi.org/10.1007/978-3-662-59144-4

[40] I. Schur, *Über die Gaußschen Summen*, K. Gesell. Wiss. Göttingen, Nachrichten, Math.-Phys. Kl., 147–153, 1921.

[41] D.H. Lehmer, *The characters of linear permutations*, Linear and Multilinear Algebra **4** (1), 1–16 (1976).
DOI: https://doi.org/10.1080/03081087608817124

[42] R. Dedekind, *Abriss einer Theorie der höhern Congruenzen in Bezug auf einen reellen Primzahl-Modulus*, J. Reine Angew. Math. **54**, 1–26 (1857).

[43] H. Kühne, *Eine Wechselbeziehung zwischen Functionen mehrerer Unbestimmten, die zu Reciprocitätsgesetzen führt*, J. Reine Angew. Math. **124**, 121–133 (1902).

[44] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen*, Math. Zeit. **19**, 153–246 (1924).

[45] P.L. Clark, P. Pollack, *Reciprocity by resultant in $k[t]$*, Enseign. Math. **65** (1–2), 101–116 (2019).

[46] D.Q.N. Nguyen, *Higher reciprocity law and an analogue of the Grunwald–Wang theorem for the ring of polynomials over an ultra-finite field*, Ann. Pure Appl. Logic **175** (1), paper No. 103438 (2024).
DOI: https://doi.org/10.1016/j.apal.2024.103438

[47] Ю.В. Нестеренко, *Теория чисел: учебник для вузов*, МЦНМО, М., 2025.

[48] G. Eisenstein, *Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste*, J. Reine Angew. Math. **28**, 186–191 (1844).

[49] L. Kronecker, *Ueber das Reciprocitätsgesetz*, Monatsber. Berlin, 331–341 (1876).

[50] А.Н. Абызов, *Метод Фаньяно решения алгебраических уравнений: исторический обзор и его развитие*, Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки **163** (3–4), 304–348 (2021).
DOI: https://doi.org/10.26907/2541-7746.2021.3-4.304-348

[51] Ж.-П. Серр, *Курс арифметики*, Мир, М., 1972.

[52] M. Baker, *Quadratic reciprocity via Lucas polynomials*, Matt Baker's Math Blog, 2020.
URL: http://mattbaker.blog

Адель Наилевич Абызов
Казанский (Приволжский) федеральный университет,
ул. Кремлевская, д. 18, г. Казань, 420008, Россия,
e-mail: Adel.Abyzov@kpfu.ru

Павел Николаевич Буутай
Национальный исследовательский университет «Высшая школа экономики»,
ул. Мясницкая, д. 20, г. Москва, 101000, Россия,

Северо-Восточный федеральный университет имени М.К. Аммосова,
ул. Белинского, д. 58, г. Якутск, 677000, Республика Саха (Якутия), Россия
e-mail: buutay.p@hse.ru

Volume 4, Issue 2
pp. 4–75 (2026)

UDC 512.55
MSC 18G05

The quadratic reciprocity law and its generalizations

A.N. Abyzov, P.N. Buutai

Abstract. This paper is expository and methodological in nature and is devoted to the development of E.I. Zolotarev's ideas embedded in his approach to the proof of the quadratic reciprocity law (1872). We consider extensions of Zolotarev's approach to abstract number rings presented in the work of A. Brunyate and P.L. Clark (2015), and to finite groups studied in the paper by W. Duke and K. Hopkins (2005). We also discuss the connections between these studies and certain classical results, as well as various approaches to proving the quadratic reciprocity law.

Keywords: quadratic reciprocity law, group symbol, character table, Vandermonde determinant, resultant.

DOI: 10.26907/2949-3919.2026.2.4-75

References

[1] I.G. Bashmakova, E.I. Slavutin, *The history of Diophantine analysis from Diophantus to Fermat*, Nauka, M., 1984 [in Russian].

[2] G.P. Matvievskaya, E.P. Ojigova, *Unpublished materials by L. Euler on number theory*, Nauka, Spb., 1997 [in Russian].

[3] L. Euler, *Theoremata circa divisores numerorum in hac forma* $pa^2 \pm qb^2$ *contentorum*, Comm. Acad. Sci. Petersburg **14**, 151–181 (1744/1746).

[4] L. Euler, Observationes circa divisionem quadratorum per numeros primos, in: Opera Omnia, Series I, V. **3**, 477–512 (1783).

[5] A. Legendre, *Reserches dánalyse indéterminée*, Histoiré de l'Académie Royale des Sciences de Paris, 465–559 (1785).

[6] A. Legendre, Essai sur la théorie des nombres, Paris, 1798.

[7] C.F. Gauss, *Theorematis arithmetici demonstratio nova*, Comment. Soc. regiae sci. Göttingen XVI, 1808.

Acknowledgements. The work of A.N. Abyzov is supported by the Russian Science Foundation (grant no. 25-11-00348) and performed under the development program of Volga Region Mathematical Center (agreement no. 075-02-2026-1328/1).

Received: 09 June 2026. Accepted: 30 June 2026. Published: 07 July 2026.

[8] C.F. Gauss, *Works on number theory*, ed. I.M. Vinogradov, comments by B.N. Delone. Izd-vo AN USSR, M., 1959 [is Russian].

[9] F. Lemmermeyer, *Proofs of the quadratic reciprocity law*. URL: https://uni-heidelberg.de (archived: https://web.archive.org/web/20250106010310/https://www.mathi.uni-heidelberg.de/~flemmermeyer/qrg_proofs.html).

[10] E. Artin, *Beweis des allgemeinen Reziprozitätsgesetzes*, Abh. Math. Semin. Univ. Hambg. **5** (1), 353–363 (1927).
DOI: https://doi.org/10.1007/BF02952531

[11] N.G. Chebotarev, *Collected works*: *in* 3 *volumes*, Izd-vo AN USSR, M.–L., 1949–1950 [in Russian].

[12] G. Zolotareff, *Nouvelle démonstration de la réciprocité de Legendre*, Nouv. Ann. Math. (ser. 2) **11**, 109–111 (1872).

[13] F. Keune, *Number fields*, Radboud University Press, 2023.

[14] A. Brunyate, P.L. Clark, *Extending the Zolotarev–Frobenius approach to quadratic reciprocity*, Ramanujan J. **37** (1), 25–50 (2015).
DOI: https://doi.org/10.1007/s11139-014-9635-y

[15] P. Cartier, *Sur une généralisation des symboles de Legendre–Jacobi*, L'Enseignement Mathématique. 2e sér **16** (1), 31–48 (1970).

[16] B.R. McDonald, *Finite rings with identity*, Marcel Dekker, Inc., New York, 1974.

[17] G. Frobenius, *Über das quadratische Reciprozitätsgesetz.* I, S.–B. Preuss. Akad. Wiss., Berlin, 335–349, 1914.

[18] M. Lerch, *Sur un théorème de Zolotarev*, Bull. Intern. de l'Acad. Fr. Joseph **3**, 34–37 (1896).

[19] W. Duke, K. Hopkins, *Quadratic reciprocity in a finite group*, Amer. Math. Monthly **112** (3), 251–256 (2005).
DOI: https://doi.org/10.1080/00029890.2005.11920190

[20] M. Hablicsek, G. Mantilla-Soler, *Power map permutations and symmetric differences in finite groups*, J. Algebra Appl. **10** (5), 947–959 (2011).
DOI: https://doi.org/10.1142/S0219498811005051

[21] J. Neukirch, *Algebraic number theory*, in: Grundlehren der mathematischen Wissenschaften **322**, Springer-Verlag, Berlin, 1999.
DOI: https://doi.org/10.1007/978-3-662-03983-0

[22] G.J. Janusz, *Algebraic number fields*, Graduate Studies in Mathematics **7**, AMS, Providence, RI, 1996.

[23] O. Zariski, P. Samuel, *Commutative algebra. Vol.* 1, Graduate Texts in Mathematics **28**, Springer-Verlag, New York-Heidelberg-Berlin, 1975.
URL: https://link.springer.com/book/9780387900896

[24] A.N. Abyzov, *The Quadratic Reciprocity Law by Zolotarev and its generalizations*, Math. Theor. Comp. Sci. **3** (1), 4–11 (2025) [in Russian].
DOI: https://doi.org/10.26907/2949-3919.2025.1.4-11

[25] H. Chua, *Quadratic reciprocity via Vandermonde matrix*, Amer. Math. Monthly **133** (4), 376–379 (2026).
DOI: https://doi.org/10.1080/00029890.2025.2600902

[26] J. Delsarte, *Une démonstration de la loi de réciprocité quadratique*, Œuvres de Jean Delsarte Vol. **2**, 827–850 (1950).

[27] K. Motose, *On Gauss sums and Vandermonde matrices*, Bull. Fac. Sci. Technol. Hirosaki Univ. **6** (1), 19–23 (2003).

[28] F. Keune, *Quadratic reciprocity and finite fields*, Nieuw. Arch. Wisk. **9**, 263–266 (1991).

[29] M. Dicker, *A proof of the quadratic reciprocity law*, arXiv:1210.7744 (2012).
URL: http://arxiv.org/abs/1210.7744.

[30] C.F. Gauss, *Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et amplicationes novae*, 1818, Werke, vol. II, in: Georg Olms Verlag, Hildescheim, 47–64, 1973.

[31] K. Motose, *On commutative group algebras*, Sci. Rep. Hirosaki Univ. **40** (2), 127–131 (1993).

[32] K. Motose, *On commutative group algebras.* III, Bull. Fac. Sci. Technol. Hirosaki Univ. **1** (2), 93–97 (1999).

[33] Z.I. Borevich, I.R. Shafarevich, *Number theory*, Academic Pres, New York and London, 1966.

[34] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics **84**, Springer-Verlag, New York, 1990.
DOI: https://doi.org/10.1007/978-1-4757-2103-4

[35] O. Baumgart, *The quadratic reciprocity law. A collection of classical proofs*, Edited, translated from the German, and with contributions by Franz Lemmermeyer. Birkhäuser/Springer, Cham, 2015.
DOI: https://doi.org/10.1007/978-3-319-16283-6

[36] F. Lemmermeyer, *Quadratic number fields*, Springer, Cham, 2021.
DOI: https://doi.org/10.1007/978-3-030-78652-6

[37] A. Hausner, *On the quadratic reciprocity theorem*, Arch. Math. **12**, 182–183 (1961).
DOI: https://doi.org/10.1007/BF01650546

[38] E. Schering, *Zur Theorie der Quadratischen Reste*, Acta Math. **1**, 153–170 (1882).
DOI: https://doi.org/10.1007/BF02592132

[39] J.A. Dieudonné, *La géométrie des groupes classiques*, Springer-Verlag, Berlin–New York, 1971.
DOI: https://doi.org/10.1007/978-3-662-59144-4

[40] I. Schur, *Über die Gaußschen Summen*, K. Gesell. Wiss. Göttingen, Nachrichten, Math.-Phys. Kl., 147–153, 1921.

[41] D.H. Lehmer, *The characters of linear permutations*, Linear and Multilinear Algebra **4** (1), 1–16 (1976).
DOI: https://doi.org/10.1080/03081087608817124

[42] R. Dedekind, *Abriss einer Theorie der höhern Congruenzen in Bezug auf einen reellen Primzahl-Modulus*, J. Reine Angew. Math. **54**, 1–26 (1857).

[43] H. Kühne, *Eine Wechselbeziehung zwischen Functionen mehrerer Unbestimmten, die zu Reciprocitätsgesetzen führt*, J. Reine Angew. Math. **124**, 121–133 (1902).

[44] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen*, Math. Zeit. **19**, 153–246 (1924).

[45] P.L. Clark, P. Pollack, *Reciprocity by resultant in $k[t]$*, Enseign. Math. **65** (1–2), 101–116 (2019).

[46] D.Q.N. Nguyen, *Higher reciprocity law and an analogue of the Grunwald–Wang theorem for the ring of polynomials over an ultra-finite field*, Ann. Pure Appl. Logic **175** (1), paper No. 103438 (2024).
DOI: https://doi.org/10.1016/j.apal.2024.103438

[47] Yu.V. Nesterenko, *Number theory*, MCCME, M., 2025 [in Russian].

[48] G. Eisenstein, *Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste*, J. Reine Angew. Math. **28**, 186–191 (1844).

[49] L. Kronecker, *Ueber das Reciprocitätsgesetz*, Monatsber. Berlin, 331–341 (1876).

[50] A.N. Abyzov, *Fagnano's method for solving algebraic equations: Its historical overview and development*, Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki **163** (3–4), 304–348 (2021) [in Russian].
DOI: https://doi.org/10.26907/2541-7746.2021.3-4.304-348

[51] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics **7**, Springer-Verlag, New York–Heidelberg, 1973.
DOI: https://doi.org/10.1007/978-1-4684-9884-4

[52] M. Baker, *Quadratic reciprocity via Lucas polynomials*, Matt Baker's Math Blog, 2020.
URL: http://mattbaker.blog

Adel Nailevich Abyzov
Kazan Federal University,
18 Kremlyovskaya str., Kazan 420008, Russia,
e-mail: Adel.Abyzov@kpfu.ru

Pavel Nikolaevich Buutai
HSE University,
20 Myasnitskaya str., Moscow 101000, Russia,
North-Eastern Federal University,
58 Belinskogo str., Yakutsk 677000, Russia,
e-mail: buutay.p@hse.ru

Том 4, Выпуск 2
Стр. 76–85 (2026)

УДК 517.18
MSC 30D05

Применение полиэлементных уравнений для функций, аналитических в плоскости с разрезом, к интерполяционным задачам для целых функций класса A

Ф.Н. Гарифьянов, Э.И. Гиззатуллина

Аннотация. Исследуются линейные полиэлементные уравнения для функций, аналитических в плоскости с симметричным разрезом по мнимой оси и исчезающих на бесконечности. Решение ищется в классе функций, представимых интегралом типа Коши по данным разрезам с четной или нечетной плотностью. Проводится регуляризация этих уравнений и исследование вопроса об ее равносильности. При этом существенно используется теория эллиптических функций. Полученные результаты применимы к исследованию интерполяционных задач для целых функций экспоненциального типа из класса A.

Ключевые слова: полиэлементные уравнения, метод регуляризации, эллиптические функции, целые функции класса A.

DOI: 10.26907/2949-3919.2026.2.76-85

Введение

Цель данной работы – исследование полиэлементного уравнения для функций, аналитических в плоскости с разрезами по мнимой оси, и его приложения к интерполяционным задачам для целых функций класса A ([1], гл. V).

Пусть $\Gamma_1 = (2i, 3i)$, $\Gamma_2 = -\Gamma_1$, $\Gamma = \Gamma_1 \cup \Gamma_2$, а D – квадрат с вершинами $\pm 1 \pm i$ (знаки не согласованы). Рассмотрим полиэлементное функциональное уравнение

$$(Vf)(z) \equiv (V_1, f)(z) + i^k (V_1, f)(iz) = g(z), \quad z \in D, \;\; k = \overline{1,4}, \tag{1}$$

где

$$\begin{aligned}(V_1, f)(z) \equiv & f(z+1+3i) + f(z-1-3i) + f(z-1+3i) + f(z+1-3i) \\ & + f(z+1+i) + f(z-1-i) + f(z-1+i) + f(z+1-i),\end{aligned} \tag{2}$$

при следующих предположениях.

1) Решение ищется в классе функций B, представимых интегралом типа Коши

$$f(z) = \frac{1}{2i\pi} \int_{\Gamma} (\tau - z)^{-1} \phi(\tau) d(\tau) \tag{3}$$

Поступила: 26.02.2026. Принята: 05.05.2026. Опубликована: 07.07.2026.

с плотностью $\phi(\tau) \in H(\overline{\Gamma})$. Эта плотность нечетна, если $k = 2, 4$ и четна, если $k = 1, 3$. Другими словами, это класс четных или нечетных функций соответственно, голоморфных в плоскости с разрезом по Γ и исчезающих на бесконечности. Граничные значения решений $f^{\pm}(t)$ на Γ также удовлетворяют условию Гёльдера, а в точках $\pm 2i, \pm 3i$ у них возможны, самое большее, логарифмические особенности.

2) Свободный член $g(z)$ голоморфен в D, $g(iz) = i^k g(z)$ и его граничное значение $g^+(t) \in H(\partial D)$.

Поясним постановку задачи. Множество точек, в которых голоморфна функция $(Vf)(z)$, несвязно. Оно распадается на две связные компоненты, одной из которых является квадрат D, на котором и задано соотношение (1), а другая содержит бесконечно удаленную точку. Именно это обеспечивает нетривиальность уравнения (1). Более подробно по данному поводу см. введение в [2] или замечание 2 в [3].

Подчеркнем, что свободный член не обязан быть аналитически продолжимым из D через какой-либо отрезок границы ∂D, а решение и свободный член принадлежат, вообще говоря, разным классам аналитических функций. Даже в случае однородного уравнения

$$(Vf)(z) = 0, \quad z \in D$$

нельзя сделать вывод, что оно выполняется в некоторой окрестности бесконечно удаленной точки.

Решение $f(z) \in B$ является нижней функцией, ассоциированной по Борелю ([4], §1, п. 1.1) с верхней целой функций экспоненциального типа (ц.ф.э.т.) $F(z) \in A$. Ее индикаторной диаграммой будет, вообще говоря, интервал мнимой оси $(-3i; 3i)$. Именно эта связь уравнения (1) с ц.ф.э.т. используется в дальнейшем для получения приложений.

История возникновения таких задач и некоторые подобные результаты см. в обзорной статье ([5], разд. 5). Наиболее близка к данной статья [6], где рассматривалось уравнение (1) при $k = 2$, $\Gamma = (-2i; -i) \cup (i; 2i)$ и

$$(V_1, f)(z) = f(z+1+2i) + f(z-1-2i) + f(z-1+2i) + f(z+1-2i) + f(z-1) + f(z+1). \quad (4)$$

Заметим, что оператор (4) содержит шесть слагаемых, в то время, как оператор (2), используемый в данной статье содержит восемь слагаемых. Объясняется это тем, что в статье [6] оба преобразования $\sigma(z) = z \pm 1$ переводят точки $\pm i$ в вершины D, а здесь надо рассмотреть четыре преобразования $\sigma(z) = z \pm 1 \pm i$, переводящие точки $\pm 2i$ в какие-то из вершин D.

Данная статья, кроме введения, содержит еще три раздела. В разделе 1 проведена регуляризация уравнения (1) и показано, что в зависимости от выбора k оно имеет различную картину разрешимости. При этом существенно используется принцип сжимающихся отображений в банаховом пространстве. Получены условия равносильности регуляризации. Далее в разделе 2 для определенности ограничимся рассмотрением уравнения (1)

при $k = 3$. Получены приложения к проблеме моментов для ц.ф.э.т. класса A. В разделе 3 обсуждается вопрос об обобщении полученных результатов на случай некоторых других разрезов по мнимой оси.

1. Регуляризация функционального уравнения

С учетом (3) имеем

$$(1) \Leftrightarrow (E\phi)(z) \equiv \frac{1}{2\pi i}\int_{\underline{\Gamma}} G(z,\tau)\phi(\tau)d\tau = g(z), \quad z \in D, \tag{5}$$

где

$$\begin{aligned} G(z,\tau) &= G_1(z,\tau) + i^k G_1(iz,\tau), \\ G_1(z,\tau) =& (w+1+3i)^{-1} + (w-1-3i)^{-1} + (w+1-3i)^{-1} + (w-1+3i)^{-1} \\ &+ (w+1+i)^{-1} + (w-1-i)^{-1} + (w+1-i)^{-1} + (w-1+i)^{-1} \end{aligned}$$

и $w = \tau - z$.

Пусть $t \in \Gamma_2$, т. е. $t + 3i \pm 1 \in \partial D$. Если в равенстве (5) $z \to t + 3i \pm 1$, то по формуле Ю.В. Сохоцкого ([7], гл. 1, §4, п. 4.2) имеем

$$(E^+\phi)(t + 3i \pm 1) = \pm 2^{-1}\phi(t) + (E\phi)(t + 3i \pm 1). \tag{6}$$

Знаки в формуле (6) согласованы. Особый интеграл в правой части (6) получен формальной заменой $z \in D$ в соотношении (5) на точки $t + 3i \pm 1 \in \partial D$ и понимается в смысле главного значения по Коши. Тогда

$$(E^+\phi)(t + 3i + 1) - (E^+\phi)(t + 3i - 1) = (T\phi)(t),$$

где интегральный оператор

$$(T\phi)(t) \equiv \phi(t) + \frac{1}{2i\pi}\int_{\Gamma} K(t,\tau)\phi(\tau)d(\tau) = g^+(t + 3i + 1) - g^+(t + 3i - 1)$$

с ядром

$$\begin{aligned} K(t,\tau) =& (u-2-6i)^{-1} + (u-2)^{-1} + (u-2-2i)^{-1} + (u-2-4i)^{-1} \\ &- (u+2)^{-1} - (u+2-6i)^{-1} - (u+2-2i)^{-1} - (u+2-4i)^{-1} \\ &+ j^k[(v-4i+2)^{-1} + (v-4i+4)^{-1} - (v+4i+2)^{-1} - (v+4i+4)^{-1}], \end{aligned}$$

причем $u = \tau - t$, $v = \tau - it$. Это ядро ограничено и

$$|K(t,\tau)| < \gamma_k, \quad k = \overline{1,4}, \tag{7}$$

причем $\gamma_k = \{3.54,\ k=1;\ 2.34,\ k=2;\ 1.16,\ k=3;\ 2.83,\ k=4\}$. Итак, проведена регуляризация полиэлементного функционального уравнения (1). Запишем полученное уравнение Фредгольма второго рода в виде

$$(T\phi)(t) = g^+(t + 3i(-1)^j + 1) - g^+(t + 3i(-1)^j - 1), \tag{8}$$

где $t \in \Gamma_j$, $j = 1, 2$. Подчеркнем три обстоятельства. Во-первых, оценка (7) справедлива и при $t \in \Gamma_1$. Это следует из симметрии разреза Γ и вида полиэлементного уравнения (1). Поэтому нет необходимости выписывать явное выражение ядра $K(t, \tau)$ при $t \in \Gamma_1$, хотя это легко сделать. Во-вторых, правая часть уравнения (8) четна (нечетна), если четен (нечетен) свободный член $g(z)$. В-третьих, $(T\phi)(t) = (T\phi)(-t)$. В этом легко убедиться, если заменить переменные τ и t на $-\tau$ и $-t$ соответственно, и воспользоваться равенством $K(t, \tau) = K(-t, -\tau)$.

Будем считать оператор T определенным на банаховом пространстве $C(\overline{\Gamma})$ с естественным образом определенной нормой $\|\phi\| = \max|\phi(t)|$, $t \in \overline{\Gamma}$. В силу оценки (7) и принципа сжимающихся отображений справедлива

Лемма 1. *Однородное уравнение*

$$T\phi = 0$$

при $k = 2, 3, 4$ *имеет лишь тривиальное решение, а неоднородное уравнение* (8) *разрешимо и имеет единственное решение.*

Рассмотрим обратный переход от интегрального уравнения (8) к полиэлементному уравнению (1), т. е. выясним вопрос о равносильности регуляризации.

Теорема 2. *При* $k = 2, 3$ *проведенная регуляризация является равносильной, т. е.* (8) $\Rightarrow$ (1).

Доказательство. Пусть вначале для определенности $k = 2$. Функция $(V_1 f)(z)$ четна, поскольку четно решение $f(z)$. Это, в свою очередь, следует из нечетности плотности интеграла типа Коши (3). Действительно, (8) $\Rightarrow (T\phi_1)(t) = 0$, где $\phi_1(t) = \phi(t) + \phi(-t)$, и остается применить лемму 1. Тогда $(Vf)(iz) = -(Vf)(z)$ и

$$(E\phi)(z) = g(z) + \Omega(z), \quad z \in D. \tag{9}$$

Функция $\Omega(z)$ голоморфна в D, $\Omega(iz) = -\Omega(z)$ и $\Omega^+(t-1) = \Omega^+(t+1)$, где $t \in (-i; i)$. Другими словами, функция $\Omega(z)$ голоморфна в горизонтальной полосе $|\operatorname{Im} z| < 1$ и имеет там действительный период 2. Пусть $\operatorname{Im} z = -1$. Тогда

$$\Omega^+(t + 2i) = -\Omega^+(-it + 2) = -\Omega^+(-it) = \Omega^+(t).$$

Итак, функция $\Omega(z)$ имеет примитивные периоды 2 и $2i$, а на ∂D у нее возможны самое большее логарифмические особенности. Значит, эллиптическая функция $\Omega(z)$ нулевого порядка ([8], ч. 2, гл. 1, §5), т. е. константа. Но из условия $c = -c$ имеем $\Omega(z) \equiv 0$.

Совершенно аналогично рассмотрим случай $k = 3$. В соответствии с (9) имеем $\Omega(z) \equiv 0$, поскольку $(Vf)(iz) = i(Vf)(z)$ и $c = ic$. □

Теорема 3. *При $k = 4$ полиэлементоное уравнение* (1) *разрешимо, если только*

$$(E\phi)(0) = g(0). \tag{10}$$

Доказательство. Для единственности решения $\phi(t)$ интегрального уравнения (8) имеем $\Omega(z) \equiv \text{const}$ в соотношении (9).

Условие (10) является не только условием разрешимости полиэлементного уравнения (1), но и обеспечивает равносильность регуляризации. □

Замечание 4. По каждой функции $g(z)$ можно найти такую постоянную c_g, что для функции $g(z) + c_g$ условие (10) выполнено, т. е. уравнение (1) разрешимо.

Осталось рассмотреть случай $k = 1$. Здесь нельзя гарантировать даже разрешимость интегрального уравнения (8).

Теорема 5. *При $k = 1$ полиэлементное уравнение* (1) *имеет не более чем конечное число условий разрешимости. Все они являются условиями разрешимости интегрального уравнения* (8).

2. Приложение к проблеме моментов для ц.ф.э.т. класса A

Далее для определенности считаем, что $k = 3$ в соотношении (1). Перепишем его в терминах ц.ф.э.т., пользуясь нечетностью нижней функции и формулой преобразования Бореля

$$f(z) = \int_0^\infty F(x) \exp(-zx) dx, \quad \operatorname{Re} z > 0.$$

Пусть, кроме того,

$$g(z) = -16 \sum_{j=0}^{\infty} \frac{\beta_j z^{4j+1}}{(4j+1)!}, \tag{11}$$

причем радиус сходимости этого степенного ряда $R > \sqrt{2}$. Тогда уравнение (1) запишем в виде

$$-8 \int_0^\infty F(x) \exp^{-x} \cos x \cos 2x \, [\sin(xz) + \operatorname{sh}(xz)] dx = g(z), \quad |z| < 1. \tag{12}$$

Ядро интеграла в левой части уравнения (7) состоит из двух слагаемых. Если хотя бы одно из этих слагаемых отсутствует, то такое уравнение решалось бы в явном виде с помощью синус-преобразования Фурье. При этом областью сходимости соответствующего несобственного интеграла была бы полоса шириной 2, вертикальная или горизонтальная, симметричная относительно оси ординат или абсцисс. Здесь же областью сходимости

является квадрат D, образованный пересечением горизонтальной и вертикальной полос. Поэтому и возникает необходимость прибегнуть к методу интегральных уравнений.

Приравняем коэффициенты Маклорена левой и правой частей равенства (12). С учетом (11) имеем

$$L[F,j] \equiv \int_0^\infty F(x)e^{-x}x^{4j+1}\cos x\cos 2x dx = \beta_j. \tag{13}$$

Теорема 6. *Лакунарная степенная проблема моментов Стилтьеса* (13) *для четной ц.ф.э.т. $F(z)$, ассоциированной по Борелю с нижней функцией $f(z) \in B$ с весом*

$$P(x) = e^{-x}\cos x\cos 2x$$

при сделанных предположениях разрешима и имеет единственное решение.

Положим $g_j(z) = -16[4j+1]^{-1}z^{4j+1}$. Возьмем систему интегралов типа Коши (3) $f_j(z) : (Vf_j)(z) = g_j(z)$, где $z \in D$, $j = \overline{0,\infty}$ и систему ц.ф.э.т. $\{F_j(z)\}$ из класса A, ассоциированных с ними по Борелю. Ясно, что $L[F_m; j] = \sigma_{m,j}$. По поводу приложений подобных биортогональных систем более подробно см. работу [9]. Там рассматривалось уравнение при $k = 3$, $\Gamma = (-i; i)$, $(V_1 f)(z) = f(z+1+i) + f(z-1+i) + f(z+1-i) + f(z-1-i)$.

Ц.ф.э.т. $F_j(z)$ ограничена по модулю на вещественной оси и вполне регулярного роста ([10], гл. 1, §4, п. 3) с индикатором $h_F(\theta) = 3\,|\sin\theta|$.

3. Обобщение на случай других разрезов по мнимой оси

Пусть теперь $\Gamma_1 = (ni, (n+1)i)$, $\Gamma_2 = -\Gamma_1$, $\Gamma = \Gamma_1 \cup \Gamma_2, n = 3, 4, \ldots$. Исследуем уравнение (1), но вместо оператора (2) возьмем

$$\begin{aligned}(V_1, f)(z) \equiv & f(z+(n+1)i+1) + f(z-(n+1)i-1) + f(z+(n+1)i-1)\\ & + f(z-(n+1)i+1) + f(z+(n-1)i+1) + f(z-(n-1)i-1)\\ & + f(z+(n-1)i-1) + f(z-(n-1)i+1).\end{aligned}$$

Преобразование $\sigma(z) = z \pm (n-1)i \pm 1$ (знаки не согласованы) переводит одну из точек $\pm ni$ в какую-то из вершин D. Решение ищется в классе функций B, представимых интегралом типа Коши (3) с четной или нечетной плотностью, аналогично тому, как это сделано в разделе 1. Еще раз отметим, что у граничных значений решение $f^{\pm}(t)$, $t \in \underline{\Gamma}$ в точках $\pm ni$, $\pm(n+1)i$ возникают, самое большее, логарифмические особенности. Рассуждая аналогично тому, как это сделано в разделе 1, придем к интегральному уравнению Фредгольма

$$\phi(t) + \frac{1}{2\pi i}\int_{\underline{\Gamma}} K(t,\tau)\phi(\tau)d\tau = g^+(t+(-1)^j(n+1)i+1) - g^+(t+(-1)^j(n+1)i-1),$$
$$t \in \Gamma_j, \quad j = 1, 2.$$

При $t \in \Gamma_2$ имеем

$$\begin{aligned}K(t,\tau) =&(u-2(n+1)i-2)^{-1}+(u-2)^{-1}+(u-2ni-2)^{-1}+(u-2i-2)^{-1}\\&-(u+2)^{-1}-(u-2(n+1)i+2)^{-1}-(u-2i+2)^{-1}\\&-(u-2ni+2)^{-1}+i^k[(v-(n+2)i+n)^{-1}+(v-(n+2)i+n+2)^{-1}\\&+(v+(n-2)i+n+2)^{-1}+(v+(n-2)i+n)^{-1}-(v+(n+2)i+n+2)^{-1}\\&-(v+(n+2)i+n)^{-1}-(v+(2-n)i+n)^{-1}-(v+(2-n)i+n+2)^{-1}].\end{aligned}$$

При $n=3$ для модуля ядра справедлива оценка (7), но теперь

$$\gamma_k = \{3.44,\ k=1;\ 2.65,\ k=2;\ 0.53,\ k=3;\ 2.35,\ k=4\}.$$

Итак, при $k=1$ опять неприменим принцип сжимающихся отображений, и не удается найти число условий разрешимости уравнения (1), т. е. ситуация в некотором смысле аналогична указанной в замечании 2 из работы [9]. Остается сделать вывод о справедливости теорем 2, 3, 5 и для данной задачи.

Замечание 7. В статье [6] рассматривается разрез Γ при $n=1$. Там ядро $K(t,\tau)$ содержит десять слагаемых. В разделе 1 данной статьи рассматривается разрез Γ при $n=2$, и ядро $K(t,\tau)$ содержит двенадцать слагаемых. А вот при $n \geq 3$ ядро $K(t,\tau)$ содержит уже шестнадцать слагаемых.

Положим в уравнении (1) $k=1$ и вместо ряда (11) возьмем ряд

$$g(z) = 16\sum_{j=0}^{\infty}\frac{\beta_j z^{4j}}{(4j)!}.$$

Обратим внимание на то, что в силу теоремы 3 и замечания 4 первый коэффициент ряда β_0 подобран так, что разрешимо уравнение (1), а радиус сходимости этого степенного ряда $R > \sqrt{2}$.

Теорема 8. *Лакунарная степенная проблема моментов Стилтьеса*

$$\int_0^{\infty} F(x)e^{-x}x^{4k}\cos 3x\cos x dx = \beta_k, \quad k=\overline{1,\infty}$$

для нечетной ц.ф.э.т. $F(z)$, ассоциированной по Борелю с нижней функцией $f(z) \in \beta$, разрешима и имеет единственное решение.

Список литературы

[1] Б.Я. Левин, *Распределение корней целых функций*, ГИТТЛ, М., 1956.

[2] Ф.Н. Гарифьянов, Е.В. Стрежнева, *Интерполяционные задачи для целых функций, индуцированные правильным шестиугольником*, Сиб. матем. журн. **59** (1), 78–85 (2018).
DOI: https://doi.org/10.17377/smzh.2018.59.107

[3] E.P. Aksenteva, F.N. Garifyanov, *Sum-difference equation for analytic functions generated by pentagon and its application*, Lobachevskii J. Math. **37** (2), 101–104 (2016).
DOI: https://doi.org/10.1134/S1995080216020037

[4] Л. Бибербах, *Аналитическое продолжение*, Наука, М., 1967.

[5] Ф.Н. Гарифьянов, *Полиэлементные функциональные уравнения, связанные с ядром Карлемана, и их приложения*, Изв. вузов. Матем. (11), 21–37 (2022).
DOI: https://doi.org/10.26907/0021-3446-2022-11-21-37

[6] Ф.Н. Гарифьянов, *О полиэлементных уравнениях, приводящих к проблеме моментов для целых функций класса A*, Изв. вузов. Матем. (4), 3–7 (2017).
URL: https://www.mathnet.ru/rus/ivm9222

[7] Ф.Д. Гахов, *Краевые задачи*, Наука, М., 1977.

[8] А. Гурвиц, Р. Курант, *Теория функций*, Наука, М., 1968.

[9] Ф.Н. Гарифьянов, Е.В. Стрежнева, *О системе целых функций класса A, биортогональной с весом лакунарной системе степеней на луче*, Сиб. матем. журн. **58** (1), 83–87 (2017).
DOI: https://doi.org/10.17377/smzh.2017.58.108

[10] А.Ф. Леонтьев, *Ряды экспонент*, Наука, М., 1976.

Фархат Нургаязович Гарифьянов
Казанский государственный энергетический университет,
ул. Красносельская, д. 51, г. Казань, 420066, Россия,
e-mail: f.garifyanov@mail.ru

Эльвира Ильхамовна Гиззатуллина
Казанский государственный энергетический университет,
УПО «КОЛЛЕДЖ КИУ»,
ул. Красносельская, д. 51, г. Казань, 420066, Россия,
e-mail: hasanovae19966@mail.ru

Volume 4, Issue 2
pp. 76–85 (2026)

UDC 517.18
MSC 30D05

Application of polyelement equations for functions analytic in a cut plane to interpolation problems for entire functions of class A

F.N. Garif'yanov, E.I. Gizzatullina

Abstract. Linear polyelement equations are investigated for functions analytic in a plane with a symmetric cut along the imaginary axis and vanishing at infinity. The solution is sought in the class of functions representable by a Cauchy-type integral over given cuts with an even or odd density. The regularization of these equations and the question of its equivalence are studied. In this process, the theory of elliptic functions is substantially used. The obtained results are applicable to the study of interpolation problems for entire functions of exponential type from class A.

Keywords: polyelement equations, regularization method, elliptic functions, entire functions of class A.

DOI: 10.26907/2949-3919.2026.2.76-85

References

[1] B.Ja. Levin, *Distribution of zeros of entire functions*, AMS, Providence, RI, 1980.

[2] F.N. Garif'yanov, E.V. Strezhneva, *Interpolation problems for entire functions induced by regular hexagons*, Siberian Math. J. **59** (1), 59–64 (2018).
DOI: https://doi.org/10.1134/S003744661801007X

[3] E.P. Aksenteva, F.N. Garifyanov, *Sum-difference equation for analytic functions generated by pentagon and its application*, Lobachevskii J. Math. **37** (2), 101–104 (2016).
DOI: https://doi.org/10.1134/S1995080216020037

[4] L. Bieberbach, *Analytische fortsetzung*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1955 [in German].

[5] F.N. Garif'yanov, *Polyelement functional equations related to the Carleman kernel and their applications*, Russian Math. (Iz. VUZ) **66** (11), 18–32 (2022).
DOI: https://doi.org/10.3103/S1066369X22110020

[6] F.N. Garif'yanov, *Poly-element equations reducible to moment problem for entire functions of class A*, Russian Math. (Iz. VUZ) **61** (4), 1–4 (2017).
DOI: https://doi.org/10.3103/S1066369X17040016

Received: 26 February 2026. Accepted: 05 May 2026. Published: 07 July 2026.

[7] F.D. Gakhov, *Boundary value problems*, Pergamon Press, Oxford; Addison-Wesley Publishing Co., Inc., Reading, Mass.-London, 1966.

[8] A. Hurwitz, *Vorlesungen über allgemeine Funktionentheorie und elliptische Funktionen*, R. Courant, *Herausgegeben und ergânzt durch einen Abschnitt über geometrische Funktionentheorie*, Springer-Verlag, Berlin, 1964 [in German].

[9] F.N. Garif'yanov, E.V. Strezhneva, *On a system of entire functions of class A which is biorthogonal to a lacunar power system on the ray*, Siberian Math. J. **58** (1), 63–66 (2017). DOI: https://doi.org/10.1134/S0037446617010086

[10] A.F. Leontiev, *Exponential series*, Nauka, Moscow, 1976 [in Russian].

Farhat Nurgayazovich Garif'yanov
Kazan State Power Engineering University,
51 Krasnoselskaya str., Kazan 420066, Russia,
e-mail: f.garifyanov@mail.ru

Elvira Ilhamovna Gizzatullina
Kazan State Power Engineering University,
UPO «KIU College»,
51 Krasnoselskaya str., Kazan 420066, Russia,
e-mail: hasanovae19966@mail.ru

Том 4, Выпуск 2
Стр. 86–103 (2026)

УДК 517.986
MSC 16S10, 20M30, 46L05, 46M40, 47L40

Полугрупповые C^*-алгебры, порожденные изометрическими представлениями свободных произведений полугрупп рациональных чисел

Р.Н. Гумеров, Е.В. Липачева

Аннотация. Рассматриваются приведенные полугрупповые C^*-алгебры, порожденные левыми регулярными изометрическими представлениями свободных произведений счетных семейств полугрупп рациональных чисел. Показывается, что эти алгебры являются ядерными и аменабельными. Получена их характеризация в качестве универсальных C^*-алгебр, задаваемых множествами порождающих элементов, удовлетворяющих полиномиальным соотношениям.

Ключевые слова: аменабельная C^*-алгебра, индуктивная последовательность, левоаменабельная полугруппа, полугрупповая C^*-алгебра, свободное произведение полугрупп, универсальная C^*-алгебра, ядерная C^*-алгебра.

DOI: 10.26907/2949-3919.2026.2.86-103

1. Введение

Статья посвящена приведенным полугрупповым C^*-алгебрам, порожденным левыми регулярными изометрическими представлениями свободных произведений счетных семейств полугрупп рациональных чисел. Основным результатом работы является описание этих алгебр в качестве универсальных C^*-алгебр, задаваемых счетными множествами порождающих элементов, которые удовлетворяют счетным наборам полиномиальных соотношений.

Приведенные полугрупповые C^*-алгебры играют важную роль как в теории C^*-алгебр, так и в ее приложениях к теории операторов в гильбертовых пространствах, а также в математической и теоретической физике. За историей исследований этого класса C^*-алгебр и обширной литературой по обсуждаемому предмету мы отсылаем читателя к работе С. Ли [1].

В этой статье мы продолжаем наше исследование приведенных полугрупповых C^*-алгебр с точки зрения теории универсальных C^*-алгебр, определяемых множествами

Благодарности. Исследование выполнено за счет гранта Российского научного фонда и Академии наук Республики Татарстан по проекту №24-21-20112, https://www.rscf.ru/project/24-21-20112/.

Поступила: 29.03.2026. Принята: 19.05.2026. Опубликована: 07.07.2026.

порождающих элементов, удовлетворяющих наборам соотношений (см. [2, 3]). Систематическое изучение универсальных C^*-алгебр было проведено Б. Блакадаром в статье [4] с целью их приложений в теории шейпов C^*-алгебр. Отметим, что характеризация операторных алгебр в качестве универсальных C^*-алгебр позволяет строить морфизмы между C^*-алгебрами, а также аппроксимировать сложно устроенные C^*-алгебры индуктивными системами, состоящими из более простых C^*-алгебр и их $*$-гомоморфизмов. Интересные приложения теории универсальных C^*-алгебр содержатся в монографии Т. Лоринга [5].

В статьях [2] и [3] в качестве универсальных C^*-алгебр были охарактеризованы приведенные полугрупповые C^*-алгебры, порожденные левыми регулярными представлениями соответственно полугрупп рациональных чисел и свободных произведений конечных семейств этих полугрупп. При этом важную роль сыграли построенные аппроксимации этих полугрупповых C^*-алгебр индуктивными последовательностями алгебр Теплица и Теплица–Кунца соответственно (см., например, [6, 7]). В свою очередь, в данной статье описание приведенных полугрупповых C^*-алгебр для свободных произведений бесконечных семейств полугрупп рациональных чисел в качестве универсальных C^*-алгебр опирается на представление этих алгебр в виде индуктивных пределов последовательностей, состоящих из копий алгебры Кунца, порожденной счетным набором изометрий со взаимно ортогональными образами [8].

Содержание статьи следующее. Она состоит из пяти разделов. Первый раздел служит введением в предмет статьи. Второй раздел содержит предварительные сведения и используемые в тексте обозначения. В третьем разделе по произвольному счетному набору $\overline{N}$ бесконечных последовательностей натуральных чисел строится полугруппа $\mathcal{Q}_{\overline{N}}$, являющаяся свободным произведением для счетного семейства полугрупп рациональных чисел, определяемых последовательностями набора $\overline{N}$. В частности, показывается, что полугруппы $\mathcal{Q}_{\overline{N}}$ не является ни левоаменабельными, ни правоаменабельными. Последние два раздела статьи посвящены полугрупповым C^*-алгебрам для полугрупп $\mathcal{Q}_{\overline{N}}$. В четвертом разделе показывается, что приведенные полугрупповые C^*-алгебры $C^*_\lambda(\mathcal{Q}_{\overline{N}})$, порожденные левыми изометрическими представлениями полугрупп $\mathcal{Q}_{\overline{N}}$, являются ядерными и аменабельными. Также в этом разделе устанавливается, что левые регулярные представления полных полугрупповых C^*-алгебр $C^*(\mathcal{Q}_{\overline{N}})$ для полугрупп $\mathcal{Q}_{\overline{N}}$ являются изоморфизмами между C^*-алгебрами $C^*(\mathcal{Q}_{\overline{N}})$ и $C^*_\lambda(\mathcal{Q}_{\overline{N}})$. Пятый раздел посвящен описанию полугрупповых C^*-алгебр $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ как универсальных C^*-алгебр, задаваемых счетными наборами порождающих элементов и соотношений для них.

2. Обозначения и предварительные сведения

Пусть S – дискретная полугруппа с левым сокращением и $l^2(S)$ – гильбертово пространство всех квадратично суммируемых комплекснозначных функций на S. В пространстве $l^2(S)$ рассмотрим стандартный ортонормированный базис $\{e_s \mid s \in S\}$, состоящий из функций $e_s : S \longrightarrow \mathbb{C}$, таких, что $e_s(t) = \delta_{st}$, где $t \in S$ и δ_{st} – символ Кронекера.

Пусть $\mathfrak{B}(l^2(S))$ – C^*-алгебра всех ограниченных линейных операторов на гильбертовом пространстве $l^2(S)$. Для каждого элемента $s \in S$ в пространстве $\mathfrak{B}(l^2(S))$ имеется изометрический оператор $T_s : l^2(S) \longrightarrow l^2(S)$, задаваемый формулой

$$T_s(e_t) = e_{st}, \quad t \in S. \tag{1}$$

В алгебре $\mathfrak{B}(l^2(S))$ рассмотрим C^*-подалгебру, порожденную множеством изометрий $\{T_s \mid s \in S\}$. Она называется *левой приведенной полугрупповой C^*-алгеброй полугруппы S* и обозначается символом $C^*_\lambda(S)$.

В этой статье мы будем иметь дело с левыми приведенными полугрупповыми C^*-алгебрами для свободных произведений бесконечных семейств полугрупп. Поэтому далее напомним построение свободного произведения полугрупп.

Пусть $\{S_\mu \mid \mu \in \Lambda\}$ – семейство непересекающихся полугрупп. Рассмотрим объединение этого семейства $\bigsqcup\limits_{\mu\in\Lambda} S_\mu$ в качестве алфавита для множества $\prod^*\{S_\mu \mid \mu \in \Lambda\}$, состоящего из всех непустых слов $s_1 s_2 \dots s_l$, $l \in \mathbb{N}$, таких, что любые две соседние буквы s_i и s_j принадлежат различным полугруппам семейства $\{S_\mu \mid \mu \in \Lambda\}$. На множестве $\prod^*\{S_\mu \mid \mu \in \Lambda\}$ зададим операцию умножения, обозначаемую символом $*$, следующим образом:

$$s_1 s_2 \dots s_l * t_1 t_2 \dots t_m = \begin{cases} s_1 \dots s_l t_1 t_2 \dots t_m, & \text{если } s_l \in S_\mu, t_1 \in S_\nu, \mu \neq \nu; \\ s_1 \dots s_{l-1}(s_l \cdot t_1) t_2 \dots t_m, & \text{если } s_l, t_1 \in S_\mu \text{ для некоторого } \mu, \end{cases}$$

где $s_1 s_2 \dots s_l, t_1 t_2 \dots t_m \in \prod^*\{S_\mu \mid \mu \in \Lambda\}$, $l, m \in \mathbb{N}$, $\mu, \nu \in \Lambda$. Множество $\prod^*\{S_\mu \mid \mu \in \Lambda\}$, наделенное операцией умножения $*$, является неабелевой полугруппой, которая называется *свободным произведением семейства полугрупп* $\{S_\mu \mid \mu \in \Lambda\}$.

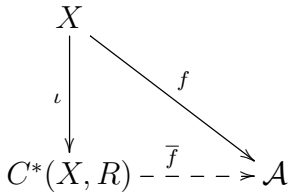
Теперь напомним определение универсальной C^*-алгебры, задаваемой множеством порождающих элементов, которые удовлетворяют полиномиальным соотношениям (см. детали, например, в [4, раздел 1] и [5, глава 3]). Аксиоматический подход к этому понятию, использующий язык теории категорий и функторов, был предложен в работе [9] и развит в статьях [10–12].

Пусть $X = \{x_i \mid i \in I\}$ – некоторое множество и $\mathcal{F}(X)$ – комплексная инволютивная алгебра некоммутативных многочленов от переменных из множества $X \sqcup X^*$, где $X^* = \{x_i^* \mid i \in I\}$. Пусть R – некоторое подмножество в $\mathcal{F}(X)$. Назовем X и R множествами *порождающих элементов* и *соотношений* соответственно. Пара (X, R) называется *$*$-полиномиальной парой* [10].

Пусть $\mathcal{A}$ – произвольная C^*-алгебра. Функция $f : X \longrightarrow \mathcal{A}$ называется *представлением* пары (X, R), если для каждого полинома $p(x_{i_1}, \dots, x_{i_s}, x_{j_1}^*, \dots, x_{j_t}^*)$ из R в C^*-алгебре $\mathcal{A}$ справедливо равенство $p(f(x_{i_1}), \dots, f(x_{i_s}), f(x_{j_1})^*, \dots, f(x_{j_t})^*) = 0$, где $s, t \in \mathbb{N}$.

Универсальной C^*-алгеброй, определяемой множеством порождающих элементов X и множеством соотношений R, называется пара $(C^*(X, R), \iota)$, состоящая из C^*-алгебры $C^*(X, R)$ и представления $\iota : X \longrightarrow C^*(X, R)$, удовлетворяющая следующему *свойству*

универсальности: для любой C^*-алгебры $\mathcal{A}$ и любого представления $f : X \longrightarrow \mathcal{A}$ существует единственный $*$-гомоморфизм $\overline{f} : C^*(X, R) \longrightarrow \mathcal{A}$, такой, что диаграмма



коммутативна, т. е., $f = \overline{f} \circ \iota$. При этом C^*-алгебра $C^*(X, R)$ сама часто называется универсальной C^*-алгеброй, порожденной парой (X, R).

Заметим, что универсальная C^*-алгебра, задаваемая множествами порождающих элементов и соотношений, не всегда существует. Б. Блакадар ввел понятие *допустимой пары* (X, R) [4, определение 1.2] и доказал, что для такой пары универсальная C^*-алгебра $C^*(X, R)$ всегда существует. Отметим, что для каждой C^*-алгебры $\mathcal{A}$ существует $*$-полиномиальная пара (X, R), такая, что $\mathcal{A} = C^*(X, R)$ [10, теорема 2].

Если универсальная C^*-алгебра $C^*(X, R)$ является унитальной с единицей 1 и $\iota(x) = 1$ для некоторого $x \in X$, то элемент x также обозначается 1. При этом мы всегда предполагаем, что все естественные соотношения для 1 содержатся в R. При этом, для краткости, эти соотношения не пишутся.

Известен целый ряд различных интересных примеров универсальных C^*-алгебр (см., например, [13, II.8.3.2] и [14, приложение, A1]). В нашем изложении будет использоваться хорошо известная в математической физике алгебра Кунца $\mathcal{O}_\infty$, которая может быть определена как универсальная C^*-алгебра следующим образом:

$$\mathcal{O}_\infty = C^* \left(\{u_1, u_2, \ldots\}, \{u_i^* u_j = \delta_{ij} 1 \mid i, j \in \mathbb{N}\} \right). \tag{2}$$

Другими словами, алгебра $\mathcal{O}_\infty$ – это универсальная C^*-алгебра, порожденная счетным числом изометрий с попарно ортогональными образами (см. [13, II.8.3.3]). Эта алгебра была введена и изучена И. Кунцем [15]. Он, в частности, доказал, что алгебра $\mathcal{O}_\infty$ проста. Известно также, что эта алгебра аменабельна и ядерна (см., например, [13, IV.3.5.3]).

В работах [2, 3] приведены примеры универсальных C^*-алгебр, для которых выбор множеств порождающих элементов и соотношений обусловлен представлением этих алгебр в виде пределов индуктивных последовательностей алгебр Теплица и Теплица–Кунца.

В данной статье индуктивные последовательности также будут играть ключевую роль в описании приведенной полугрупповой C^*-алгебры для свободного произведения бесконечного семейства полугрупп. Напомним некоторые факты, связанные с индуктивными последовательностями.

Пусть $\{\mathcal{A}_k \mid k \in \mathbb{N}\}$ и $\{\varphi_k : \mathcal{A}_k \longrightarrow \mathcal{A}_{k+1} \mid k \in \mathbb{N}\}$ – счетные семейства C^*-алгебр и их $*$-гомоморфизмов, соответственно. Тогда говорят, что задана индуктивная последовательность C^*-алгебр $\{\mathcal{A}_k, \varphi_k \mid k \in \mathbb{N}\}$. Часто такую индуктивную последовательность

записывают в виде диаграммы

$$\mathcal{A}_1 \xrightarrow{\varphi_1} \mathcal{A}_2 \xrightarrow{\varphi_2} \mathcal{A}_3 \xrightarrow{\varphi_3} \dots. \tag{3}$$

Известно, что для любой индуктивной последовательности C^*-алгебр (3) существует индуктивный предел, который единствен с точностью до изоморфизма. Индуктивный предел представляет собой пару $(\mathcal{A}, \{\varphi_{k,\infty} \mid k \in \mathbb{N}\})$, состоящую из C^*-алгебры $\mathcal{A}$ и семейства $*$-гомоморфизмов $\{\varphi_{k,\infty} : \mathcal{A}_k \longrightarrow \mathcal{A} \mid k \in \mathbb{N}\}$, которые обладают важным свойством универсальности. При этом, с точностью до изоморфизма, имеет место равенство

$$\mathcal{A} = \overline{\bigcup_{k=1}^{+\infty} \varphi_{k,\infty}(\mathcal{A}_k)},$$

где замыкание берется в топологии нормы. Кроме того, часто C^*-алгебру $\mathcal{A}$ саму называют индуктивным пределом. Детальное изложение этих понятий и фактов о них содержится, например, в [16, глава 6].

3. Свободные произведения счетных семейств полугрупп рациональных чисел

В этом параграфе для произвольного счетного набора последовательностей натуральных чисел мы построим семейство полугрупп рациональных чисел и свободное произведение для полугрупп этого семейства. В дальнейшем будут изучены некоторые свойства полученного свободного произведения.

Рассмотрим произвольный счетный набор $\overline{N}$ бесконечных последовательностей натуральных чисел

$$\overline{N} := \Big(N_1 = \{n_{11}, n_{21}, n_{31}, \dots\}, N_2 = \{n_{12}, n_{22}, n_{32}, \dots\}, \dots\Big), \tag{4}$$

где $n_{ij} \in \mathbb{N}$ для всех $i, j \in \mathbb{N}$.

Для каждого $i \in \mathbb{N}$ определим аддитивную полугруппу рациональных чисел $\mathbb{Q}^+_{N_i}$ следующим образом:

$$\mathbb{Q}^+_{N_i} = \left\{ \frac{m}{n_{1i} \dots n_{ki}} \;\middle|\; m \in \mathbb{N}, k \in \mathbb{N} \right\},$$

где $i \in \mathbb{N}$.

Далее, для каждого $i \in \mathbb{N}$ рассмотрим полугруппу $\mathbb{Q}^+_{N_i} \times \{i\}$ с бинарной операцией, заданной формулой

$$(u, i) + (v, i) = (u + v, i), \quad u, v \in \mathbb{Q}^+_{N_i}.$$

Построим свободное произведение счетного семейства полугрупп $\{\mathbb{Q}^+_{N_i} \times \{i\} \mid i \in \mathbb{N}\}$

и, присоединив нейтральный элемент e, получим полугруппу

$$\mathcal{Q}_{\overline{N}} := \left(\prod\nolimits^{*} \{\mathbb{Q}^{+}_{N_i} \times \{i\} \mid i \in \mathbb{N}\} \right) \bigsqcup \{e\}.$$

Легко видеть, что полугруппа $\mathcal{Q}_{\overline{N}}$ неабелева, обладает левым и правым сокращением и вкладывается в группу, которая является свободным произведением аддитивных групп рациональных чисел $\{\mathbb{Q}_{N_i} \mid i \in \mathbb{N}\}$.

Нашей целью будет показать, что полугруппа $\mathcal{Q}_{\overline{N}}$ не является ни левоаменабельной, ни правоаменабельной.

Напомним, что дискретная полугруппа S называется (*лево*)*правоаменабельной*, если на S существует конечно-аддитивная (лево)правоинвариантная вероятностная мера, определенная на сигма-алгебре всех подмножеств в S. Например, любая абелева полугруппа является левоаменабельной и правоаменабельной.

В работе [17] изучались аменабельные полугруппы, вложимые в группы. В частности, в ней показано, что если полугруппа с сокращением является (лево) правоаменабельной, то она удовлетворяет (левому) правому условию Ope. А именно, для произвольных элементов $s, t \in S$ выполняется соотношение $sS \cap tS \neq \emptyset$ ($Ss \cap St \neq \emptyset$). Здесь $sS := \{sr \mid r \in S\}$ и $Ss := \{rs \mid r \in S\}$. Например, любая абелева полугруппа с сокращением удовлетворяет и левому, и правому условию Ope.

Теорема 1. *Пусть $\overline{N}$ – произвольный счетный набор бесконечных последовательностей натуральных чисел. Тогда для полугруппы $\mathcal{Q}_{\overline{N}}$ выполняются следующие свойства*:

1) *$\mathcal{Q}_{\overline{N}}$ не удовлетворяет ни левому, ни правому условию Ope*;

2) *$\mathcal{Q}_{\overline{N}}$ не является ни левоаменабельной, ни правоаменабельной.*

Доказательство. 1) Пусть $a = (p, i)$ и $b = (q, j)$, где $p \in \mathbb{Q}^{+}_{N_i}$, $q \in \mathbb{Q}^{+}_{N_j}$, $i, j \in \mathbb{N}$ и $i \neq j$. Очевидно, что справедливо равенство $a * \mathcal{Q}_{\overline{N}} \cap b * \mathcal{Q}_{\overline{N}} = \emptyset$. Таким образом, полугруппа $\mathcal{Q}_{\overline{N}}$ не удовлетворяет левому условию Ope. Аналогично показывается, что полугруппа $\mathcal{Q}_{\overline{N}}$ не удовлетворяет правому условию Ope.

2) Следует из 1) и [17, предложение 2]. □

4. Полугрупповые C^*-алгебры для свободных произведений счетных семейств полугрупп рациональных чисел

В этом параграфе мы рассмотрим левую приведенную полугрупповую C^*-алгебру $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ для полугруппы $\mathcal{Q}_{\overline{N}}$, построенной в предыдущем параграфе по счетному набору бесконечных последовательностей натуральных чисел (4). Мы покажем, что эта полугрупповая C^*-алгебра $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ и полная полугрупповая C^*-алгебра $C^*(\mathcal{Q}_{\overline{N}})$ канонически изоморфны.

В работе [8] была изучена структура C^*-алгебры $C^*_\lambda(\mathcal{Q}_{\overline{N}})$. Было показано, что $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ есть C^*-подалгебра в алгебре $\mathfrak{B}(l^2(\mathcal{Q}_{\overline{N}}))$ всех ограниченных операторов на гильбертовом пространстве $l^2(\mathcal{Q}_{\overline{N}})$, порожденная следующим семейством изометрий:

$$T_{1,i} := T_{(1,i)}, \quad T_{k+1,i} := T_{\left(\frac{1}{n_{1i}\cdots n_{ki}},i\right)}, \quad k,i \in \mathbb{N}. \tag{5}$$

Более того, пара $(C^*_\lambda(\mathcal{Q}_{\overline{N}}), \{\varphi_{k,\infty} \mid k \in \mathbb{N}\})$ является индуктивным пределом индуктивной последовательности алгебр Кунца

$$\mathcal{O}_\infty \xrightarrow{\varphi_1} \mathcal{O}_\infty \xrightarrow{\varphi_2} \mathcal{O}_\infty \xrightarrow{\varphi_3} \ldots. \tag{6}$$

Здесь связующие инъективные $*$-гомоморфизмы φ_k и инъективные $*$-гомоморфизмы $\varphi_{k,\infty}$ задаются значениями на порождающих элементах алгебры Кунца:

$$\varphi_k : \mathcal{O}_\infty \longrightarrow \mathcal{O}_\infty : u_i \longmapsto u_i^{n_{ki}},$$

$$\varphi_{k,\infty} : \mathcal{O}_\infty \longrightarrow C^*_\lambda(\mathcal{Q}_{\overline{N}}) : u_i \longmapsto T_{k,i},$$

где $k,i \in \mathbb{N}$. Таким образом, мы имеем равенство

$$C^*_\lambda(\mathcal{Q}_{\overline{N}}) \;=\; \overline{\bigcup_{k=1}^{+\infty} \varphi_{k,\infty}(\mathcal{O}_\infty)},$$

где замыкание берется в топологии нормы. Подробности содержатся в работе [8].

Напомним, что C^*-алгебра A называется *ядерной*, если для любой C^*-алгебры B существует только одна C^*-норма на алгебраическом тензорном произведении $A \otimes B$.

Теорема 2. *Пусть $\overline{N}$ – произвольный счетный набор бесконечных последовательностей натуральных чисел. Тогда левая приведенная полугрупповая C^*-алгебра $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ ядерна.*

Доказательство. Как уже упоминалось в предварительных сведениях, алгебра Кунца $\mathcal{O}_\infty$ ядерна. Так как левая приведенная полугрупповая C^*-алгебра $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ является пределом индуктивной последовательности, состоящей из копий алгебры Кунца $\mathcal{O}_\infty$ и инъективных $*$-гомоморфизмов, то она также ядерна [16, теорема 6.3.10]. □

Понятие ядерной C^*-алгебры тесно связано с важнейшим понятием аменабельной банаховой алгебры, введенным Б. Джонсоном [18]. Напомним, что банахова алгебра A называется аменабельной, если все ее одномерные группы когомологий с коэффициентами в дуальных банаховых A-бимодулях тривиальны, или, другими словами, каждое непрерывное дифференцирование алгебры A со значениями в любом дуальном банаховом A-бимодуле является внутренним (подробности см., например, в [19, гл. 7]). Знаменитая теорема Конна–Хаагерупа утверждает, что C^*-алгебра является ядерной тогда и только тогда, когда она аменабельна [20, 21]. В качестве следствия этого факта и теоремы 2 мы немедленно получаем следующий результат.

Теорема 3. *Пусть $\overline{N}$ – произвольный счетный набор бесконечных последовательностей натуральных чисел. Тогда левая приведенная полугрупповая C^*-алгебра $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ аменабельна.*

Кроме левой приведенной полугрупповой C^*-алгебры $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ мы будем рассматривать также полную полугрупповую C^*-алгебру $C^*(\mathcal{Q}_{\overline{N}})$. Поэтому дадим далее определение полной полугрупповой C^*-алгебры для произвольной дискретной полугруппы с левым сокращением.

Пусть S – полугруппа с левым сокращением. Наименьшую полугруппу частичных изометрий на гильбертовом пространстве $l^2(S)$, содержащую все изометрии T_s (см. (1)) и их сопряженные операторы T_s^*, $s \in S$, обозначим через $I_l(S)$. Полугруппа $I_l(S)$ является инверсной полугруппой, т. е. для каждого элемента $a \in I_l(S)$ существует единственный элемент $b \in I_l(S)$ такой, что $aba = a$ и $bab = b$. При этом используется обозначение $b = a^{-1}$. Отметим, что S можно рассматривать как подполугруппу в $I_l(S)$, так как существует естественное вложение $S \longrightarrow I_l(S) : s \longmapsto T_s$. Инверсная полугруппа $I_l(S)$ называется *левой инверсной оболочкой* полугруппы S.

Полная полугрупповая C^*-алгебра полугруппы S определяется как универсальная C^*-алгебра следующего вида [1, определение 5.6.38]:

$$C^*(S) := C^*\left(\{v_a\}_{a\in I_l(S)}, \{v_a v_b = v_{ab}, v_a^* = v_{a^{-1}}, v_0 = 0, \text{ если } 0 \in I_l(S), a, b \in I_l(S)\}\right).$$

Другими словами, $C^*(S)$ является C^*-алгеброй, универсальной относительно $*$-представлений инверсной полугруппы $I_l(S)$ частичными изометриями.

Заметим, что существует канонический сюръективный $*$-гомоморфизм

$$C^*(S) \longrightarrow C^*_\lambda(S) : v_a \longmapsto T_a, \quad a \in S,$$

который называется *левым регулярным представлением полной полугрупповой C^*-алгебры полугруппы S*. Подробности содержатся в работе [1, § 5.6.6].

Следующее утверждение вытекает из теоремы 4.4 и следствия 3.8 в [22] (см. также [23]).

Теорема 4. *Пусть $\overline{N}$ – произвольный счетный набор бесконечных последовательностей натуральных чисел. Тогда левое регулярное представление полной полугрупповой C^*-алгебры полугруппы $\mathcal{Q}_{\overline{N}}$*

$$C^*(\mathcal{Q}_{\overline{N}}) \longrightarrow C^*_\lambda(\mathcal{Q}_{\overline{N}}) : v_a \longmapsto T_a, \quad a \in \mathcal{Q}_{\overline{N}},$$

является изоморфизмом C^*-алгебр.

В следующем параграфе мы получим простое и естественное описание C^*-алгебр $C^*(\mathcal{Q}_{\overline{N}})$ и $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ в терминах порождающих элементов и соотношений для них.

5. Характеризация полугрупповых алгебр $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ как универсальных C^*-алгебр

В этом разделе мы продолжим изучение левых приведенных полугрупповых C^*-алгебр $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ и покажем, что они могут быть охарактеризованы как универсальные C^*-алгебры, определяемые счетными множествами порождающих элементов и соотношений. А именно, мы докажем, что C^*-алгебра $C^*_\lambda(\mathcal{Q}_{\overline{N}})$, построенная по счетному набору (4) бесконечных последовательностей натуральных чисел $\overline{N}$, изоморфна универсальной C^*-алгебре $C^*(X,R)$, где

$$X = \{1, x_{ki} \mid k,i \in \mathbb{N}\}, \tag{7}$$

$$R = \left\{x^*_{ki}x_{kj} = \delta_{ij}1,\ x_{ki} = x^{n_{ki}}_{k+1,i} \;\middle|\; k,i,j \in \mathbb{N}\right\}. \tag{8}$$

Отметим, что согласно определению 1.1 из [4], пара (X,R) является допустимой, и, следовательно, универсальная C^*-алгебра $C^*(X,R)$, порожденная (7) и (8), существует [4].

Для построения требуемого изоморфизма C^*-алгебр мы докажем две леммы, в которых построим два $*$-гомоморфизма между C^*-алгебрами $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ и $C^*(X,R)$. Затем покажем, что эти $*$-гомоморфизмы являются взаимно обратными, т. е. определяют изоморфизм рассматриваемых C^*-алгебр.

Лемма 5. *Существует единственный унитальный $*$-гомоморфизм C^*-алгебр*

$$\varphi : C^*(X,R) \longrightarrow C^*_\lambda(\mathcal{Q}_{\overline{N}}),$$

такой, что для любых $k,i \in \mathbb{N}$ выполняется условие:

$$\varphi(\iota(x_{ki})) = T_{k,i}. \tag{9}$$

Доказательство. Зададим функцию $g : X \longrightarrow C^*_\lambda(\mathcal{Q}_{\overline{N}})$ формулой

$$g(x) = \begin{cases} 1, & \text{если } x = 1; \\ T_{k,i}, & \text{если } x = x_{ki},\ k,i \in \mathbb{N}. \end{cases}$$

Проверим, что для элементов $g(x_{ki})$ в C^*-алгебре $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ выполняются соотношения:

$$1)\ g(x_{ki})^*g(x_{ki}) = 1; \qquad 2)\ g(x_{ki})^*g(x_{kj}) = 0; \qquad 3)\ g(x_{ki}) = g(x_{k+1,i})^{n_{ki}}$$

для любых $k,i,j \in \mathbb{N}$, $i \neq j$. Равенство 1) очевидно. Для доказательства 2) достаточно проверить, что равенство

$$T^*_{k,i}T_{k,j}e_s = 0 \tag{10}$$

справедливо для любого базисного вектора e_s. Зафиксируем $s \in \mathcal{Q}_{\overline{N}}$. Для произвольного

элемента $t \in \mathcal{Q}_{\overline{N}}$ вычислим скалярное произведение векторов из пространства $l^2(\mathcal{Q}_{\overline{N}})$:

$$\langle e_t, T^*_{k,i}T_{k,j}e_s\rangle = \langle T_{k,i}e_t, T_{k,j}e_s\rangle = \langle e_{(p,i)*t}, e_{(q,j)*s}\rangle,$$

где $p = q = 1$, если $k = 1$ и $p = \dfrac{1}{n_{1i}\dots n_{(k-1)i}}$, $q = \dfrac{1}{n_{1j}\dots n_{(k-1)j}}$, если $k \geqslant 2$ (см. (5)). Так как $i \neq j$, то, очевидно, мы имеем соотношение

$$(p,i) * t \neq (q,j) * s.$$

Следовательно, справедливо равенство

$$\langle e_{(p,i)*t}, e_{(q,j)*s}\rangle = 0.$$

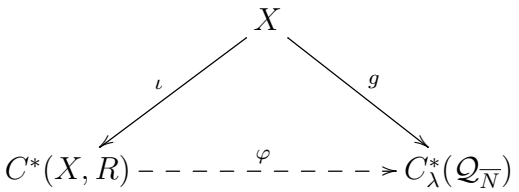
Таким образом, имеем равенство

$$\langle e_t, T^*_{k,i}T_{k,j}e_s\rangle = 0$$

для любого $t \in Q$, что доказывает (10), а значит, и равенство 2). Наконец, используя (1) и (5), мы получаем 3):

$$g(x_{k+1,i})^{n_{ki}} = T^{n_{ki}}_{k+1,i} = T_{\left(\frac{n_{ki}}{n_{1i}\dots n_{ki}},i\right)} = T_{k,i} = g(x_{ki}).$$

По свойству универсальности C^*-алгебры $C^*(X,R)$ существует единственный унитальный $*$-гомоморфизм C^*-алгебр $\varphi : C^*(X,R) \longrightarrow C^*_\lambda(\mathcal{Q}_{\overline{N}})$, такой, что диаграмма



коммутативна, т. е. выполняется условие (9). □

Лемма 6. *Существует единственный унитальный $*$-гомоморфизм C^*-алгебр*

$$\psi : C^*_\lambda(\mathcal{Q}_{\overline{N}}) \longrightarrow C^*(X,R),$$

такой, что для любых $k, i \in \mathbb{N}$ выполняется условие:

$$\psi(T_{k,i}) = \iota(x_{ki}) \tag{11}$$

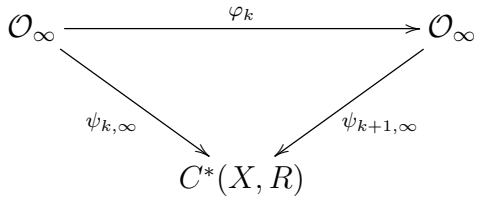
Более того, $*$-гомоморфизм ψ инъективен.

Доказательство. Во-первых, отметим, что для любого $k \in \mathbb{N}$ существует единственный $*$-гомоморфизм

$$\psi_{k,\infty} : \mathcal{O}_\infty \longrightarrow C^*(X, R),$$

такой, что $\psi_{k,\infty}(u_i) = \iota(x_{ki})$ для любого $i \in \mathbb{N}$. Действительно, элементы $\iota(x_{k1}), \iota(x_{k2}), \ldots$ в C^*-алгебре $C^*(X, R)$ удовлетворяют соотношениям, определяющим универсальную C^*-алгебру $\mathcal{O}_\infty$ (см. (8) и (2)). Поэтому, по свойству универсальности C^*-алгебры $\mathcal{O}_\infty$, существует требуемый $*$-гомоморфизм $\psi_{k,\infty}$.

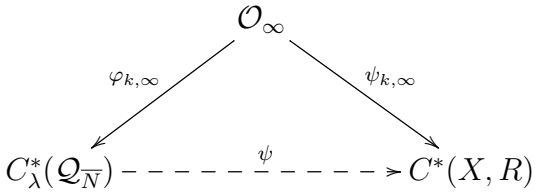
Во-вторых, покажем, что для каждого $k \in \mathbb{N}$ следующая диаграмма коммутативна:



Для этого достаточно проверить совпадение значений $*$-гомоморфизмов на порождающих элементах $u_1, u_2, \ldots$ алгебры Кунца $\mathcal{O}_\infty$. Действительно, для любого $i \in \mathbb{N}$ имеем следующие равенства:

$$\psi_{k+1,\infty}(\varphi_k(u_i)) = \psi_{k+1,\infty}(u_i^{n_{ki}}) = \iota(x_{k+1,i})^{n_{ki}} = \iota(x_{ki}) = \psi_{k,\infty}(u_i).$$

В-третьих, по свойству универсальности индуктивного предела индуктивной последовательности алгебр Кунца (6), существует единственный унитальный $*$-гомоморфизм $\psi : C^*_\lambda(\mathcal{Q}_{\overline{N}}) \longrightarrow C^*(X, R)$, делающий диаграмму



коммутативной для любого $k \in \mathbb{N}$, т. е. справедливо равенство

$$\psi \circ \varphi_{k,\infty} = \psi_{k,\infty}. \tag{12}$$

Из равенства (12) вытекает, что $*$-гомоморфизм ψ удовлетворяет требуемому условию (11):

$$\psi(T_{k,i}) = \psi(\varphi_{k,\infty}(u_i)) = \psi_{k,\infty}(u_i) = \iota(x_{ki})$$

для любых $k, i \in \mathbb{N}$.

Наконец, отметим, что C^*-алгебра $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ является простой, так как она служит индуктивным пределом последовательности простых C^*-алгебр [8, теорема 1]. Следовательно, $*$-гомоморфизм ψ инъективен. □

Далее мы получим описание левой приведенной полугрупповой C^*-алгебры $C^*_\lambda(\mathcal{Q}_{\overline{N}})$ как универсальной C^*-алгебры, порожденной множествами порождающих (7) и соотношений (8).

Теорема 7. *Пусть $\overline{N}$ – произвольный счетный набор бесконечных последовательностей натуральных чисел:*

$$\overline{N} = \Big(\{n_{11}, n_{21}, n_{31}, \dots\}, \{n_{12}, n_{22}, n_{32}, \dots\}, \dots\Big).$$

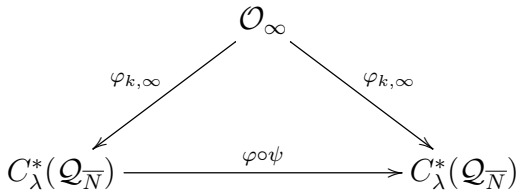
Пусть $X = \{1, x_{ki} \mid k, i \in \mathbb{N}\}$ – множество элементов, удовлетворяющих набору соотношений

$$R = \left\{x^*_{ki}x_{kj} = \delta_{ij}1, x_{ki} = x^{n_{ki}}_{k+1,i} \;\middle|\; k, i, j \in \mathbb{N}\right\}.$$

Тогда универсальная C^*-алгебра $C^*(X, R)$ изоморфна левой приведенной полугрупповой C^*-алгебре $C^*_\lambda(\mathcal{Q}_{\overline{N}})$.

Доказательство. Рассмотрим $*$-гомоморфизмы φ и ψ, построенные в леммах 5 и 6. Покажем, что φ и ψ – взаимно обратные изоморфизмы между C^*-алгебрами $C^*(X, R)$ и $C^*_\lambda(\mathcal{Q}_{\overline{N}})$, т. е. что выполняются равенства: $\varphi \circ \psi = \mathrm{Id}_{C^*_\lambda(\mathcal{Q}_{\overline{N}})}$ и $\psi \circ \varphi = \mathrm{Id}_{C^*(X,R)}$.

С этой целью покажем, что диаграмма



(13)

коммутативна для каждого $k \in \mathbb{N}$, т. е. справедливо равенство

$$\varphi \circ \psi \circ \varphi_{k,\infty} = \varphi_{k,\infty}. \tag{14}$$

Проверку этого равенства достаточно провести на порождающих элементах $u_1, u_2 \dots$ алгебры Кунца. В силу (9) и (11), получаем следующие равенства:

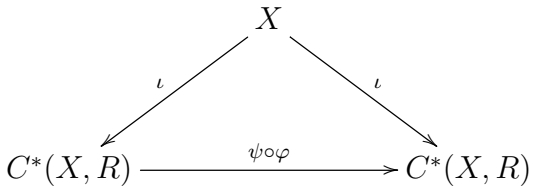
$$\varphi \circ \psi(\varphi_{k,\infty}(u_i)) = \varphi \circ \psi(T_{k,i}) = \varphi(\iota(x_{ki})) = T_{k,i} = \varphi_{k,\infty}(u_i),$$

где $i \in \mathbb{N}$. Это доказывает равенство (14).

По свойству универсальности C^*-алгебры $C^*_\lambda(\mathcal{Q}_{\overline{N}})$, рассматриваемой как индуктивный предел индуктивной последовательности алгебр Кунца (6), существует единственный $*$-гомоморфизм, делающий диаграмму (13) коммутативной для каждого $k \in \mathbb{N}$. Таким образом, мы получаем первое из требуемых равенств:

$$\varphi \circ \psi = \mathrm{Id}_{C^*_\lambda(\mathcal{Q}_{\overline{N}})}.$$

Далее, рассмотрим диаграмму



(15)

Используя (9) и (11), мы получаем равенства

$$\psi \circ \varphi(\iota(x_{ki})) = \psi(T_{k,i}) = \iota(x_{ki})$$

для любых $k, i \in \mathbb{N}$. Кроме того, по леммам 5 и 6, мы также имеем равенство $\psi \circ \varphi \circ \iota(1) = \iota(1)$. Таким образом, диаграмма (15) коммутативна.

Теперь второе из требуемых равенств следует из свойства универсальности C^*-алгебры $C^*(X, R)$:

$$\psi \circ \varphi = \mathrm{Id}_{C^*(X,R)}. \qquad \square$$

Заметим, что существует другой способ доказательства теоремы 7. А именно, можно использовать хорошо известную конструкцию универсальной C^*-алгебры $C^*(X, R)$ [4, определение 1.2] и инъективность $*$-гомоморфизма ψ из леммы 6. Для того чтобы показать, что ψ является изоморфизмом C^*-алгебр, достаточно доказать, что образ этого $*$-гомоморфизма всюду плотен в $C^*(X, R)$ [19, следствие 4.7.84].

Из теорем 7 и 4 получаем

Следствие 8. *В предположениях теоремы* 7*, полная полугрупповая C^*-алгебра $C^*(\mathcal{Q}_{\overline{N}})$ с точностью до изоморфизма является универсальной C^*-алгеброй $C^*(X, R)$.*

Список литературы

[1] X. Li, *Semigroup C^*-algebras*, in: K-theory for group C^*-algebras and semigroup C^*-algebras, Oberwolfach Seminars **47**, Birkhäuser, Cham, 167–272 (2017).
DOI: https://doi.org/10.1007/978-3-319-59915-1_5

[2] R. Gumerov, A. Kuklin, E. Lipacheva, *A universal property of semigroup C^*-algebras generated by cones in groups of rationals*, Ann. Funct. Anal. **15** (3), paper no. 72 (2024).
DOI: https://doi.org/10.1007/s43034-024-00374-5

[3] R.N. Gumerov, A.S. Kuklin, E.V. Lipacheva *A universal property of semigroup C^*-algebras for the free products of semigroups of rationals*, Уфимск. матем. журн. **18** (1), 120–133 (2026).
DOI: https://doi.org/article/10.13108/2026-18-1-113

[4] B. Blackadar, *Shape theory for C^*-algebras*, Math. Scand. **56** (2), 249–275 (1985).
DOI: https://doi.org/10.7146/math.scand.a-12100

[5] T.A. Loring, *Lifting solutions to perturbing problems in C^*-algebras*, Fields Institute Monographs **8**, AMS, Providence, RI, 1997.
DOI: https://doi.org/10.1090/fim/008

[6] Р.Н. Гумеров, *Предельные автоморфизмы C^*-алгебр, порожденных изометрическими представлениями полугрупп рациональных чисел*, Сиб. матем. журн. **59** (1), 95–109 (2018).
URL: https://doi.org/10.17377/smzh.2018.59.109

[7] R.N. Gumerov, E.V. Lipacheva, *Automorphisms of the limits for the direct sequences of the Toeplitz–Cuntz algebras*, J. Math. Anal. Appl. **533** (2), paper no. 127991 (2024).
DOI: https://doi.org/10.1016/j.jmaa.2023.127991

[8] R.N. Gumerov, E.V. Lipacheva, *An approximation of semigroup C^*-algebras*, Lobachevskii J. Math. **47** (2), 526–532 (2026).
DOI: https://doi.org/10.1134/S1995080225615164

[9] T.A. Loring, *C^*-algebra relations*, Math. Scand. **107** (1), 43–72 (2010).
DOI: https://doi.org/10.7146/math.scand.a-15142

[10] I.S. Berdnikov, R.N. Gumerov, E.V. Lipacheva, K.A. Shishkin, *On C^*-algebra and $*$-polynomial relations*, Lobachevskii J. Math. **44** (6), 1990–1997 (2023).
DOI: https://doi.org/10.1134/S1995080223060112

[11] R.N. Gumerov, E.V. Lipacheva, K.A. Shishkin, *Categorical criterion for existence of universal C^*-algebras*, Уфимск. матем. журн. **16** (3), 118–129 (2024).
DOI: https://doi.org/10.13108/2024-16-3-113

[12] К.А. Шишкин, *Функторы между *-соотношениями*, Изв. вузов. Матем. (4), 84–100 (2026).
DOI: https://doi.org/10.26907/0021-3446-2026-4-84-100

[13] B. Blackadar, *Operator algebras. Theory of C^*-algebras and von Neumann algebras*, Encyclopaedia of Mathematical Sciences **122**, Springer-Verlag, Berlin, 2006.
DOI: https://doi.org/10.1007/3-540-28517-2

[14] M. Weber, *On C^*-algebras generated by isometries with twisted commutation relations*, J. Funct. Anal. **264** (8), 1975–2004 (2013).
DOI: https://doi.org/10.1016/j.jfa.2013.02.001

[15] J. Cuntz, *Simple C^*-algebras generated by isometries*, Comm. Math. Phys. **57** (3), 173–185 (1977).
DOI: https://doi.org/10.1007/BF01625776

[16] Дж. Мерфи, *C^*-алгебры и теория операторов*, Факториал, М., 1997.

[17] Р.И. Григорчук, А.М. Степин, *Об аменабельности полугрупп с сокращением*, Вестн. Моск. ун-та. Сер. 1. Матем., мех. (3), 12–16 (1998).
URL: https://www.mathnet.ru/vmumm1777

[18] B.E. Johnson, *Cohomology in Banach algebras*, Mem. Amer. Math. Soc. **127**, AMS, Providence, RI, 1972.
DOI: https://doi.org/10.1090/memo/0127

[19] А.Я. Хелемский, *Банаховы и полинормированные алгебры: общая теория, представления, гомологии*, Наука. Гл. ред. физ.-мат. лит., М., 1989.

[20] A. Connes, *On the cohomology of operator algebras*, J. Funct. Anal. **28** (2), 248–253 (1978).
DOI: https://doi.org/10.1016/0022-1236(78)90088-5

[21] U. Haagerup, *All nuclear C^*-algebras are amenable*, Invent. Math. **74** (2), 305–319 (1983).
DOI: https://doi.org/10.1007/BF01394319

[22] M. Laca, I. Raeburn, *Semigroup crossed products and the Toeplitz algebras of nonabelian groups*, J. Funct. Anal. **139** (2), 415–440 (1996).
DOI: https://doi.org/10.1006/jfan.1996.0091

[23] A. Nica, *C^*-algebras generated by isometries and Wiener–Hopf operators*, J. Operator Theory **27** (1), 17–52 (1992).
URL: https://www.theta.ro/jot/archive/1992-027-001/1992-027-001-002.html

Ренат Нельсонович Гумеров
Казанский (Приволжский) федеральный университет,
Институт математики и механики им. Н.И. Лобачевского,
ул. Кремлевская, д. 18, г. Казань, 420008, Россия,
e-mail: Renat.Gumerov@kpfu.ru

Екатерина Владимировна Липачева
Казанский государственный энергетический университет,
ул. Красносельская, д. 51, г. Казань, 420066, Россия,
e-mail: elipacheva@gmail.com

Volume 4, Issue 2
pp. 86–103 (2026)

UDC 517.986
MSC 16S10, 20M30, 46L05, 46M40, 47L40

Semigroup C^*-algebras generated by isometric representations for free products of rational number semigroups

R.N. Gumerov, E.V. Lipacheva

Abstract. We study the reduced semigroup C^*-algebras generated by the left regular representations of free products for countable families of rational number semigroups. It is shown that these algebras are nuclear and amenable. We give their characterization as universal C^*-algebras determined by generators subject to polynomial relations.

Keywords: amenable C^*-algebra, free product of semigroups, inductive sequence, left amenable semigroup, nuclear C^*-algebra, semigroup C^*-algebra, universal C^*-algebra.

DOI: 10.26907/2949-3919.2026.2.86-103

References

[1] X. Li, *Semigroup C^*-algebras*, in: K-theory for group C^*-algebras and semigroup C^*-algebras, Oberwolfach Seminars **47**, Birkhäuser, Cham, 167–272 (2017).
DOI: https://doi.org/10.1007/978-3-319-59915-1_5

[2] R. Gumerov, A. Kuklin, E. Lipacheva, *A universal property of semigroup C^*-algebras generated by cones in groups of rationals*, Ann. Funct. Anal. **15** (3), paper no. 72 (2024).
DOI: https://doi.org/10.1007/s43034-024-00374-5

[3] R.N. Gumerov, A.S. Kuklin, E.V. Lipacheva *A universal property of semigroup C^*-algebras for the free products of semigroups of rationals*, Ufa Math. J. **18** (1), 120–133 (2026).
DOI: https://doi.org/article/10.13108/2026-18-1-113

[4] B. Blackadar, *Shape theory for C^*-algebras*, Math. Scand. **56** (2), 249–275 (1985).
DOI: https://doi.org/10.7146/math.scand.a-12100

[5] T.A. Loring, *Lifting solutions to perturbing problems in C^*-algebras*, Fields Institute Monographs **8**, AMS, Providence, RI, 1997.
DOI: https://doi.org/10.1090/fim/008

Acknowledgements. The work is supported by the grant of the Russian Science Foundation and the State institution "Tatarstan Academy of Sciences", project no. 24-21-20112, https://rscf.ru/en/project/24-21-20112/.

Received: 29 March 2026. Accepted: 19 May 2026. Published: 07 July 2026.

[6] R.N. Gumerov, *Limit automorphisms of the C^*-algebras generated by isometric representations for semigroups of rationals*, Siberian Math. J. **59** (1), 73–84 (2018).
DOI: https://doi.org/10.1134/S0037446618010093

[7] R.N. Gumerov, E.V. Lipacheva, *Automorphisms of the limits for the direct sequences of the Toeplitz–Cuntz algebras*, J. Math. Anal. Appl. **533** (2), paper no. 127991 (2024).
DOI: https://doi.org/10.1016/j.jmaa.2023.127991

[8] R.N. Gumerov, E.V. Lipacheva, *An approximation of semigroup C^*-algebras*, Lobachevskii J. Math. **47** (2), 526–532 (2026).
DOI: https://doi.org/10.1134/S1995080225615164

[9] T.A. Loring, *C^*-algebra relations*, Math. Scand. **107** (1), 43–72 (2010).
DOI: https://doi.org/10.7146/math.scand.a-15142

[10] I.S. Berdnikov, R.N. Gumerov, E.V. Lipacheva, K.A. Shishkin, *On C^*-algebra and $*$-polynomial relations*, Lobachevskii J. Math. **44** (6), 1990–1997 (2023).
DOI: https://doi.org/10.1134/S1995080223060112

[11] R.N. Gumerov, E.V. Lipacheva, K.A. Shishkin, *Categorical criterion for existence of universal C^*-algebras*, Ufa Math. J. **16** (3), 118–129 (2024).
DOI: https://doi.org/10.13108/2024-16-3-113

[12] K.A. Shishkin, *Functors between *-relations*, Russian Math. (Iz. VUZ), to appear.

[13] B. Blackadar, *Operator algebras. Theory of C^*-algebras and von Neumann algebras*, Encyclopaedia of Mathematical Sciences **122**, Springer-Verlag, Berlin, 2006.
DOI: https://doi.org/10.1007/3-540-28517-2

[14] M. Weber, *On C^*-algebras generated by isometries with twisted commutation relations*, J. Funct. Anal. **264** (8), 1975–2004 (2013).
DOI: https://doi.org/10.1016/j.jfa.2013.02.001

[15] J. Cuntz, *Simple C^*-algebras generated by isometries*, Comm. Math. Phys. **57** (3), 173–185 (1977).
DOI: https://doi.org/10.1007/BF01625776

[16] G.J. Murphy, *C^*-algebras and operator theory*, Academic Press, Boston, MA, 1990.

[17] R.I. Grigorchuk, A.M. Stepin, *On amenability of semigroups with cancellation*, Mosc. Univ. Math. Bull. **53** (3), 7–11 (1998).

[18] B.E. Johnson, *Cohomology in Banach algebras*, Mem. Amer. Math. Soc. **127**, AMS, Providence, RI, 1972.
DOI: https://doi.org/10.1090/memo/0127

[19] A.Ya. Helemskii, *Banach and locally convex algebras*, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1993.
DOI: https://doi.org/10.1112/blms/27.6.613

[20] A. Connes, *On the cohomology of operator algebras*, J. Funct. Anal. **28** (2), 248–253 (1978). DOI: https://doi.org/10.1016/0022-1236(78)90088-5

[21] U. Haagerup, *All nuclear C^*-algebras are amenable*, Invent. Math. **74** (2), 305–319 (1983). DOI: https://doi.org/10.1007/BF01394319

[22] M. Laca, I. Raeburn, *Semigroup crossed products and the Toeplitz algebras of nonabelian groups*, J. Funct. Anal. **139** (2), 415–440 (1996). DOI: https://doi.org/10.1006/jfan.1996.0091

[23] A. Nica, *C^*-algebras generated by isometries and Wiener–Hopf operators*, J. Operator Theory **27** (1), 17–52 (1992). URL: https://www.theta.ro/jot/archive/1992-027-001/1992-027-001-002.html

Renat Nelsonovich Gumerov
Kazan Federal University,
N.I. Lobachevsky Institute of Mathematics and Mechanics,
35 Kremlyovskaya str., Kazan 420008, Russia,
e-mail: Renat.Gumerov@kpfu.ru

Ekaterina Vladimirovna Lipacheva
Kazan State Power Engineering University,
51 Krasnoselskaya str., Kazan 420066, Russia,
e-mail: elipacheva@gmail.com

Том 4, Выпуск 2
Стр. 104–117 (2026)

УДК 517.98, 530.145, 510.223, 517.518.3
MSC 03E55, 46L30, 81P47, 46G10

Квантовые каналы, сохраняющие сигма-аддитивность, и измеримые по Уламу кардиналы

С.В. Дженжер

Аннотация. Исследуется взаимосвязь между свойствами квантовых состояний в гильбертовом пространстве $\ell_2(\kappa)$ и теоретико-множественной природой кардинала κ. Основное внимание уделяется вопросу существования сингулярных σ-аддитивных состояний – функционалов, индуцированные меры которых являются σ-аддитивными, но при этом обращаются в нуль на конечных множествах. Хотя известно, что существование таких состояний эквивалентно измеримости κ по Уламу, их структурные и динамические свойства остаются во многом неизученными. Мы доказываем, что любое σ-аддитивное состояние на диагональной алгебре представимо в виде интеграла Петтиса по сингулярной σ-аддитивной мере, что расширяет классическую теорию представлений на ненормальный сектор. Кроме того, мы конструируем класс квантовых каналов, использующих σ-полные ультрафильтры, которые отображают нормальные состояния в сингулярные σ-аддитивные состояния, фактически «архивируя» информацию в сингулярную часть пространства состояний.

Ключевые слова: измеримые кардиналы, квантовая динамика, сингулярные квантовые состояния, интеграл Петтиса.

DOI: 10.26907/2949-3919.2026.2.104-117

Введение

Математические основания квантовой механики опираются на представление физических состояний в виде линейных функционалов на алгебре наблюдаемых. Для гильбертова пространства $\mathcal{H}$ пространство состояний $\Sigma(\mathcal{H})$ традиционно разлагается на нормальные состояния, которые являются $*$-слабо непрерывными и однозначно представляются операторами ядерного класса, и сингулярные состояния, которые обращаются в нуль на идеале компактных операторов [1].

Мощным инструментом анализа структуры состояний является интеграл Петтиса, позволяющий получать спектрально-подобные разложения состояний по множеству чистых векторных состояний. Как было установлено Г. Амосовым и В. Сакбаевым [2, 3], в стандартном сепарабельном случае состояние является нормальным тогда и только тогда, когда оно может быть представлено в виде интеграла Петтиса по дискретной

Поступила: 29.04.2026. Принята: 12.05.2026. Опубликована: 07.07.2026.

σ-аддитивной мере. Эта эквивалентность подкрепляет интуитивное представление о том, что σ-аддитивность является отличительным признаком нормальности.

Однако недавние исследования квантовой динамики в бесконечномерных системах показали, что в несепарабельном случае это может нарушаться. Изучение случайных сдвигов, операторных блужданий и предельной динамики на абелевых алгебрах показало, что сингулярные состояния естественным образом возникают как пределы физических процессов [4–7]. Это порождает два фундаментальных вопроса:

1) может ли состояние быть одновременно сингулярным и σ-аддитивным?
2) может ли нормальное состояние обладать представлением Петтиса по σ-аддитивной мере, которая обращается в нуль на конечных множествах?

В стандартной теории множеств ZFC, если на системе всех подмножеств некоторого множества существует вполне-аддитивная мера, которая обращается в нуль на одноточечных (или, что равносильно, на конечных) множествах, то само множество обязано быть измеримым кардиналом; см, например, [9]. Таким образом, существование ненормальных σ-аддитивных состояний неразрывно связано с существованием измеримых кардиналов.

Существование таких состояний было недавно подтверждено Д. Блехером и Н. Уивером [8], которые доказали, что сингулярные σ-аддитивные состояния существуют на $\mathcal{B}(\ell_2(\kappa))$ тогда и только тогда, когда κ является измеримым по Уламу кардиналом. Хотя их работа дает окончательную теоретико-множественную классификацию, операционная природа и внутренняя структура этих состояний все еще требуют изучения. В данной статье мы восполняем пробел между аксиоматическими результатами [8] и теорией представлений, развитой в [2, 3]. Наш вклад имеет двойное дно:

1) Мы демонстрируем, что соответствие между состояниями и интегралами Петтиса «выживает» при переходе к сингулярному сектору на измеримых кардиналах. В частности, мы доказываем, что любое σ-аддитивное состояние на диагональной алгебре $\mathcal{D}(\ell_2(\kappa)) \cong \ell_\infty(\kappa)$ является интегралом Петтиса по своей индуцированной σ-аддитивной мере, даже если эта мера обращается в нуль на конечных множествах.
2) Мы конструируем явный класс квантовых каналов, используя σ-полные ультрафильтры. Мы показываем, что эти каналы действуют как механизм «архивации информации», отображая нормальные состояния в сингулярные σ-аддитивные результаты. Это дает динамическую интерпретацию измеримых кардиналов как области, где квантовая информация может сохраняться σ-аддитивным образом, становясь при этом недоступной для конечномерных наблюдений.

Статья организована следующим образом: в разделе 1 приводятся необходимые сведения о больших кардиналах; в разделе 2 устанавливается представление Петтиса для сингулярных состояний; а в разделе 3 вводятся и анализируются свойства архивирующих квантовых каналов.

1. Измеримые кардиналы

Пусть $\{r_i : i \in I\}$ – семейство неотрицательных действительных чисел. Напомним, что

$$\sum_{i\in I} r_i = \sup\left\{\sum_{i\in E} r_i : E \subset I \text{ конечно}\right\}.$$

Если эта сумма конечна, то существует не более чем счетное подсемейство ненулевых r_i.

Для множества X обозначим через $\mathcal{P}(X)$ семейство всех его подмножеств.

Пусть $\kappa > \aleph_0$ – кардинал. Напомним, что мера $\mu\colon \mathcal{P}(\kappa) \to [\,0,1\,]$ представляет собой конечно-аддитивное отображение. В данной работе мы всегда рассматриваем вероятностные меры; т. е. $\mu(\kappa) = 1$. Следуя [8], мы называем меру $\mu\colon \mathcal{P}(\kappa) \to [\,0,1\,]$ ***<κ-аддитивной***, если для любого семейства $\{A_i : i \in I\}$ попарно непересекающихся подмножеств $A_i \subset \kappa$ при $|I| < \kappa$ выполняется

$$\mu\left(\bigsqcup_{i\in I} A_i\right) = \sum_{i\in I} \mu(A_i).$$

Заметим, что стандартное определение *κ-аддитивности* не согласуется с σ-аддитивностью в случае, когда берется именно счетное семейство. Поэтому мы используем обозначение $<\kappa$.

Ультрафильтр $\mathcal{U} \subsetneq \mathcal{P}(\kappa)$ на кардинале κ называется ***<κ-полным***, если для любого семейства $\{A_i : i \in I\}$ элементов $A_i \in \mathcal{U}$ при $|I| < \kappa$ их пересечение также лежит в ультрафильтре:

$$\bigcap_{i\in I} A_i \in \mathcal{U}.$$

Заметим, что если ультрафильтр является $< \kappa$-полным при $\kappa > \aleph_0$, то он является σ-полным, т. е. замкнут относительно счетных пересечений. Ультрафильтр называется ***неглавным***, если он не имеет наименьшего элемента; иными словами, если пересечение всех его элементов пусто.

Между двузначными мерами и ультрафильтрами существует тесная связь. Так, для данного ультрафильтра $\mathcal{U} \subsetneq \mathcal{P}(\kappa)$ можно определить двузначную меру $\mu_{\mathcal{U}}\colon \mathcal{P}(\kappa) \to \{0,1\}$ правилом

$$\mu_{\mathcal{U}}(A) := \begin{cases} 1, & \text{если } A \in \mathcal{U}; \\ 0, & \text{иначе.} \end{cases}$$

И наоборот, по двузначной вероятностной мере μ можно построить ультрафильтр, состоящий из множеств меры 1. Легко проверить, что:

- мера $\mu_{\mathcal{U}}$ является (σ-) $<\kappa$-аддитивной тогда и только тогда, когда $\mathcal{U}$ является (σ-) $<\kappa$-полным;
- мера $\mu_{\mathcal{U}}$ обращается в нуль на конечных множествах тогда и только тогда, когда $\mathcal{U}$ неглавный.

Следуя [8], мы говорим, что кардинал $\kappa > \aleph_0$ является:

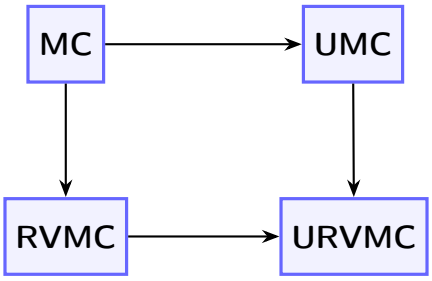


Рис. 1. Очевидные связи между свойствами измеримости кардиналов. MC – измеримый кардинал. UMC – измеримый по Уламу кардинал. RVMC – вещественно-значно измеримый кардинал. URVMC – вещественно-значно измеримый по Уламу кардинал

- ***измеримым***, если существует $<\kappa$-аддитивная двузначная мера $\mathcal{P}(\kappa) \to \{0,1\}$, обращающаяся в нуль на конечных множествах;
- ***вещественно-значно измеримым***, если существует $<\kappa$-аддитивная вероятностная мера $\mathcal{P}(\kappa) \to [\,0,1\,]$, обращающаяся в нуль на конечных множествах;
- ***измеримым по Уламу***, если существует σ-аддитивная двузначная мера $\mathcal{P}(\kappa) \to \{0,1\}$, обращающаяся в нуль на конечных множествах;
- ***вещественно-значно измеримым по Уламу***, если существует σ-аддитивная вероятностная мера $\mathcal{P}(\kappa) \to [\,0,1\,]$, обращающаяся в нуль на конечных множествах.

Заметим, что (уламовская) измеримость эквивалентна следующему: κ является (уламовски) измеримым, если существует неглавный (σ-) $<\kappa$-полный ультрафильтр. Некоторые тривиальные соотношения между этими определениями приведены на рис. 1. Известно также, что вещественно-значно измеримый кардинал κ является измеримым, если $\kappa > \mathfrak{c}$, и никакой измеримый кардинал не может быть меньше $\mathfrak{c}$. Более того, любой кардинал κ измерим по Уламу тогда и только тогда, когда он не меньше некоторого измеримого кардинала (который является недостижимым, и, следовательно, $\kappa > \mathfrak{c}$). Любой кардинал κ вещественно-значно измерим по Уламу тогда и только тогда, когда он не меньше некоторого вещественно-значно измеримого кардинала (который является слабо недостижимым); в этом случае, если $\mathfrak{c} \geqslant \kappa$, то континуум-гипотеза ложна. Подробности см., например, в [8, 9].

2. Представимость по Петтису сингулярных сигма-аддитивных состояний

Зафиксируем произвольный (не обязательно измеримый) кардинал $\kappa > \aleph_0$. Будем рассматривать гильбертово пространство $\mathcal{H} := \ell_2(\kappa)$ функций $f\colon \kappa \to \mathbb{C}$ со счетным носителем и нормой

$$\|f\| := \sqrt{\sum_{i<\kappa} |f(i)|^2}.$$

Обозначим через $\{e_i\}$ его ортонормированный базис.

Пусть $\mathcal{B}(\mathcal{H})$ – банахова алгебра линейных ограниченных операторов $\mathcal{H} \to \mathcal{H}$. Мы ограничим наше внимание банаховой подалгеброй $\mathcal{D}(\mathcal{H}) \subset \mathcal{B}(\mathcal{H})$ диагональных операторов. Очевидно, что $\mathcal{D}(\mathcal{H})$ изоморфна $\ell_\infty(\kappa)$. Элементы $\mathcal{D}(\mathcal{H})$ называются ***наблюдаемыми***. Заметим, что проекторы из $\mathcal{D}(\mathcal{H})$ – это в точности диагональные операторы с собственными значениями, равными 0 и 1. Для любого $I \subset \kappa$ обозначим через $\mathbf{P}_I$ проектор на подпространство, образованное базисными векторами $\{e_i\}_{i\in I}$. В частности, через $\mathbf{P}_\kappa$ мы обозначим тождественный оператор (который является проектором на все $\mathcal{H}$).

Обозначим через $\Sigma(\mathcal{H}) := S^{1+}(\mathcal{D}(\mathcal{H})^*)$ пространство ***квантовых состояний***, т. е. линейных функционалов $\mathcal{D}(\mathcal{H}) \to \mathbb{C}$, лежащих на пересечении положительного конуса и единичной сферы. Мы обозначаем ***действие*** квантового состояния $\rho \in \Sigma(\mathcal{H})$ на наблюдаемую $\mathbf{D} \in \mathcal{D}(\mathcal{H})$ как

$$\langle \rho, \mathbf{D} \rangle.$$

В квантовой механике обычно рассматривают подпространство $\Sigma_n(\mathcal{H}) \subset \Sigma(\mathcal{H})$ ***нормальных квантовых состояний***, которые являются $*$-слабо непрерывными квантовыми состояниями. Известно [8], что состояние $\rho \in \Sigma(\mathcal{H})$ является нормальным тогда и только тогда, когда оно ***вполне аддитивно***, что означает выполнение равенства

$$\left\langle \rho, \sum_\alpha \mathbf{P}_\alpha \right\rangle = \sum_\alpha \langle \rho, \mathbf{P}_\alpha \rangle$$

для любых попарно ортогональных проекторов $\mathbf{P}_\alpha$. Для сепарабельных гильбертовых пространств известно, что нормальность эквивалентна тому, что супремум действия по проекторам на конечномерные подпространства равен единице [5]. В нашем случае это тоже верно.

Предложение 1. *Состояние ρ является нормальным тогда и только тогда, когда*

$$\sup_{I \subset \kappa \text{ конечно}} \langle \rho, \mathbf{P}_I \rangle = 1,$$

где супремум берется по проекторам на конечномерные подпространства.

Доказательство. Пусть ρ нормально. Тогда оно вполне аддитивно. Отсюда,

$$1 = \langle \rho, \mathbf{P}_\kappa \rangle = \sum_{i<\kappa} \langle \rho, \mathbf{P}_i \rangle = \sup_{I \subset \kappa \text{ конечно}} \langle \rho, \mathbf{P}_I \rangle .$$

где первое равенство в силу нормировки состояний, второе равенство в силу вполне аддитивности, а последнее равенство по определению суммы.

Обратно, пусть

$$\sup_{I \subset \kappa \text{ конечно}} \langle \rho, \mathbf{P}_I \rangle = 1.$$

По определению супремума, для любого $I \subset \kappa$ выполнено

$$\langle \rho, \mathbf{P}_I \rangle \geqslant \sum_{i \in I} \langle \rho, \mathbf{P}_i \rangle .$$

Тогда

$$1 = \langle \rho, \mathbf{P}_\kappa \rangle = \langle \rho, \mathbf{P}_I \rangle + \langle \rho, \mathbf{P}_{\kappa \setminus I} \rangle \geqslant \sum_{i \in I} \langle \rho, \mathbf{P}_i \rangle + \sum_{i \in \kappa \setminus I} \langle \rho, \mathbf{P}_i \rangle = \sum_{i < \kappa} \langle \rho, \mathbf{P}_i \rangle = 1.$$

Таким образом, неравенства обращаются в равенство, и для любого $I \subset \kappa$ выполнено

$$\langle \rho, \mathbf{P}_I \rangle = \sum_{i \in I} \langle \rho, \mathbf{P}_i \rangle .$$

Тогда для произвольного семейства $\{I_\alpha\}$ с условием $I = \bigsqcup_\alpha I_\alpha$ имеем

$$\langle \rho, \mathbf{P}_I \rangle = \sum_{i \in I} \langle \rho, \mathbf{P}_i \rangle = \sum_\alpha \sum_{i \in I_\alpha} \langle \rho, \mathbf{P}_i \rangle = \sum_\alpha \langle \rho, \mathbf{P}_{I_\alpha} \rangle ,$$

где перегруппировка слагаемых возможна в силу абсолютной сходимости рядов. Равенство первого и последнего выражений и есть вполне аддитивность. □

Для $u \in S^1(\mathcal{H})$ нормальное квантовое состояние $\rho = \rho_u \in \Sigma_n(\mathcal{H})$ называется ***чистым векторным состоянием***, если для всех $\mathbf{D} \in \mathcal{D}(\mathcal{H})$ выполнено

$$\langle \rho, \mathbf{D} \rangle = (u, \mathbf{D}u).$$

Нас будут больше интересовать другие квантовые состояния. Так, мы говорим, что состояние ρ лежит в подпространстве $\Sigma_s(\mathcal{H}) \subset \Sigma(\mathcal{H})$ ***сингулярных квантовых состояний***, если оно обращается в нуль на всех проекторах ранга 1; или, что эквивалентно, на всех компактных операторах. Другими словами, если

$$\langle \rho, \mathbf{P}_I \rangle = 0$$

для любого конечного $I \subset \kappa$. Разложение Иосиды–Хьюитта [1] утверждает, что

$$\Sigma(\mathcal{H}) = \Sigma_n(\mathcal{H}) \oplus \Sigma_s(\mathcal{H}),$$

что означает, что любое квантовое состояние $\rho \in \Sigma(\mathcal{H})$ может быть представлено в виде выпуклой комбинации

$$\rho = p\rho_n + (1-p)\rho_s$$

для некоторых $p \in [\,0, 1\,]$, $\rho_n \in \Sigma_n(\mathcal{H})$ и $\rho_s \in \Sigma_s(\mathcal{H})$.

Отметим, что рассмотрение только диагональной алгебры наблюдаемых интересно само по себе, например, в виду [8, утверждение 2.3]. Кроме того, в силу [8, теорема 5.1]

любое чистое состояние на диагональной алгебре имеет единственное продолжение до состояния на всей алгебре $\mathcal{B}(\mathcal{H})$, которое обязательно окажется чистым. Таким образом, рассмотрение даже диагональных операторов имеет квантовую специфику.

Далее мы переходим к рассмотрению связи между мерами и квантовыми состояниями. Известно (см., например, [3]), что любое квантовое состояние может быть представлено в виде интеграла Петтиса по некоторой конечно-аддитивной неотрицательной конечной мере на единичной сфере чистых векторных состояний. Поскольку мы упростили алгебру наблюдаемых до диагональных операторов, мы можем рассмотреть частный случай таких мер, сосредоточенных на чистых векторных состояниях на базисных векторах e_i. Для состояния $\rho \in \Sigma(\mathcal{H})$ определим (конечно-аддитивную) *индуцированную меру* $\nu_\rho \colon \mathcal{P}(\kappa) \to [\,0,1\,]$ как

$$\nu_\rho(I) := \langle \rho, \mathbf{P}_I \rangle\,.$$

Лемма 2. *Любое состояние $\rho \in \Sigma(\mathcal{H})$ может быть представлено в виде интеграла Петтиса*

$$\rho = \int_{i<\kappa} \rho_{e_i}\, d\nu_\rho(i).$$

Доказательство. Нам необходимо показать, что для любой наблюдаемой $\mathbf{D} \in \mathcal{D}(\mathcal{H})$ выполнено

$$\langle \rho, \mathbf{D} \rangle = \int_{i<\kappa} (e_i, \mathbf{D}e_i)\, d\nu_\rho(i).$$

Во-первых, предположим, что $\mathbf{D} = \mathbf{P}_I$ для некоторого $I \subset \kappa$. Тогда

$$\langle \rho, \mathbf{D} \rangle = \nu_\rho(I) = \int_{i\in I} d\nu_\rho(i) = \int_{i<\kappa} (e_i, \mathbf{D}e_i)\, d\nu_\rho(i).$$

Таким образом, в силу линейности лемма верна для конечных линейных комбинаций вида

$$\mathbf{D} = \sum_{k=1}^{K} d_k \mathbf{P}_{I_k}.$$

Теперь рассмотрим произвольную наблюдаемую $\mathbf{D} \in \mathcal{D}(\mathcal{H})$. Существует последовательность операторов $\mathbf{D}_n$ с конечным спектром, аппроксимирующая $\mathbf{D}$ по норме. В силу непрерывности ρ,

$$\langle \rho, \mathbf{D} \rangle = \lim_{n\to\infty} \langle \rho, \mathbf{D}_n \rangle.$$

Согласно определению интеграла по конечно-аддитивным мерам (см., например, [10]),

$$\lim_{n\to\infty} \langle \rho, \mathbf{D}_n \rangle = \lim_{n\to\infty} \int_{i<\kappa} (e_i, \mathbf{D}_n e_i)\, d\nu_\rho(i) = \int_{i<\kappa} \lim_{n\to\infty} (e_i, \mathbf{D}_n e_i)\, d\nu_\rho(i) = \int_{i<\kappa} (e_i, \mathbf{D}e_i)\, d\nu_\rho(i),$$

что завершает доказательство. □

Таким образом, существует соответствие между квантовыми состояниями и мерами на подмножествах κ. Следующая теорема отвечает на один из наших вопросов во введении:

нормальное состояние не может быть представлено мерой, которая обращается в нуль на конечных множествах.

Теорема 3. *Если состояние $\rho \in \Sigma(\mathcal{H})$ может быть представлено как интеграл Петтиса*

$$\rho = \int_{i<\kappa} \rho_{e_i}\, dm(i),$$

и мера m обращается в нуль на конечных множествах, то ρ является сингулярным.

Следовательно, состояние $\rho \in \Sigma(\mathcal{H})$ сингулярно тогда и только тогда, когда индуцированная мера ν_ρ обращается в нуль на конечных множествах.

Доказательство. Первая часть следует из того, что для любого конечного подмножества $I \subset \kappa$

$$\langle \rho, \mathbf{P}_I \rangle = m(I) = 0.$$

Вторая часть следует из того, что для конечного $I \subset \kappa$ величина

$$\langle \rho, \mathbf{P}_I \rangle = \nu_\rho(I)$$

равна нулю либо в силу первой части, либо в силу сингулярности ρ. □

Как мы помним, нормальность состояния эквивалентна вполне аддитивности его индуцированной меры. Следуя этой же логике, мы говорим, что состояние $\rho \in \Sigma(\mathcal{H})$ является ***σ-аддитивным***, если индуцированная мера ν_ρ является σ-аддитивной. Из вышесказанного ясно, что все нормальные состояния σ-аддитивны. Кроме того, если бы гильбертово пространство $\ell_2(\kappa)$ было сепарабельным, то σ-аддитивность и вполне аддитивность были бы эквивалентны. Иными словами, на гильбертовом сепарабельном пространстве σ-аддитивные и нормальные состояния суть одно и то же.

Согласно [8, утверждение 2.3.(i)], σ-аддитивное сингулярное состояние ρ существует тогда и только тогда, когда κ является вещественно-значно измеримым по Уламу кардиналом. Таким образом, согласно результату Улама [9, теорема 10.1] (см. заключительный аргумент доказательства этой теоремы), если существует σ-аддитивное сингулярное состояние ρ, то возможны два следующих варианта:

- либо κ не меньше наименьшего измеримого кардинала, который является недостижимым, и, следовательно, $\kappa > \mathfrak{c}$;
- либо $\mathfrak{c} \geqslant \kappa$, и κ не меньше наименьшего вещественно-значно измеримого кардинала, который является слабо недостижимым. В этом случае континуум-гипотеза ложна.

Чтобы оставить континуум-гипотезу в покое, сосредоточимся теперь на мире, в котором существует измеримый по Уламу кардинал. Пусть κ – такой кардинал. Согласно [8, утверждение 2.3.(ii)], должно существовать сингулярное σ-аддитивное чистое состояние. Пусть $\mathcal{U} \subsetneq \mathcal{P}(\kappa)$ – неглавный σ-полный ультрафильтр. Определим состояние $\rho_{\mathcal{U}} \in \Sigma(\mathcal{H})$

соотношением

$$\langle \rho_{\mathcal{U}}, \mathbf{D} \rangle := \lim_{\mathcal{U}} (e_i, \mathbf{D} e_i).$$

Тогда

$$\nu_{\rho_{\mathcal{U}}}(I) = \langle \rho_{\mathcal{U}}, \mathbf{P}_I \rangle = \lim_{\mathcal{U}} (e_i, \mathbf{P}_I e_i) = \mu_{\mathcal{U}}(I),$$

и, следовательно, индуцированная мера является σ-аддитивной и обращается в нуль на конечных множествах. Таким образом, при наличии измеримого по Уламу кардинала κ мы немедленно получаем σ-аддитивное сингулярное чистое состояние $\rho_{\mathcal{U}}$. ***Чистота*** здесь означает, что $\rho_{\mathcal{U}}$ является экстремальной точкой множества $\Sigma(\mathcal{H})$.

3. Квантовые каналы

Напомним, что обычно квантовый канал – это линейное сохраняющее след вполне положительное отображение. В нашем случае, поскольку мы работаем не только со следовыми операторами, мы избавляемся от свойства сохранения следа, оставляя только сохранение нормировки (которое включено в определение квантовых состояний); см., например, как это сделано в [7]. Итак, ***квантовый канал*** – это линейное вполне положительное отображение $\Sigma(\mathcal{H}) \to \Sigma(\mathcal{H})$.

Теперь зафиксируем измеримый по Уламу кардинал κ с неглавным σ-полным ультрафильтром $\mathcal{U}$. Пусть на κ задана структура абелевой группы. Например, это можно сделать, взяв группу $\bigoplus_{i<\kappa} \mathbb{Z}_2$ финитных (т. е., имеющих конечный прообраз единицы) функций $\kappa \to \mathbb{Z}_2$, мощность которой совпадает с κ. Обозначим через $\mathbf{U}_j \in \mathcal{B}(\mathcal{H})$ оператор сдвига, определенный как

$$\mathbf{U}_j e_i = e_{i+j}.$$

Определим квантовый канал $\mathbf{\Phi}_{\mathcal{U}}$ соотношением

$$\langle \mathbf{\Phi}_{\mathcal{U}} \rho, \mathbf{D} \rangle := \lim_{\mathcal{U}} \left\langle \rho, \mathbf{U}_j^* \mathbf{D} \mathbf{U}_j \right\rangle.$$

Теорема 4. *Для любого $\rho \in \Sigma(\mathcal{H})$ состояние $\mathbf{\Phi}_{\mathcal{U}} \rho$ является сингулярным и сохраняет σ-аддитивность.*

Доказательство. Сначала пусть $\rho = \rho_{e_i}$ – чистое векторное состояние. Тогда для любой наблюдаемой $\mathbf{D} \in \mathcal{D}(\mathcal{H})$

$$\left\langle \rho, \mathbf{U}_j^* \mathbf{D} \mathbf{U}_j \right\rangle = (\mathbf{U}_j e_i, \mathbf{D} \mathbf{U}_j e_i) = (e_{i+j}, \mathbf{D} e_{i+j}).$$

Следовательно, $\mathbf{\Phi}_{\mathcal{U}} \rho = \rho_{\mathcal{U}-i}$. В частности, это сингулярное σ-аддитивное состояние.

Теперь пусть ρ – нормальное состояние. Тогда оно является выпуклой не более чем счетной комбинацией чистых векторных состояний, которые, в свою очередь, являются выпуклыми не более чем счетными комбинациями чистых векторных состояний, сосредоточенных на базисных векторах. Поскольку $\lim_{\mathcal{U}}$ коммутирует со счетными суммами,

мы получаем, что $\mathbf{\Phi}_{\mathcal{U}}\rho$ снова является сингулярным и σ-аддитивным.

Наконец, пусть само состояние ρ сингулярно. Чтобы показать сингулярность $\mathbf{\Phi}_{\mathcal{U}}\rho$, достаточно доказать, что для любого конечного подмножества $I \subset \kappa$ выполнено

$$\langle \mathbf{\Phi}_{\mathcal{U}}\rho, \mathbf{P}_I \rangle = 0.$$

Имеем

$$\left\langle \rho, \mathbf{U}_j^* \mathbf{P}_I \mathbf{U}_j \right\rangle = \langle \rho, \mathbf{P}_{I-j} \rangle = 0,$$

откуда $\langle \mathbf{\Phi}_{\mathcal{U}}\rho, \mathbf{P}_I \rangle = \lim_{\mathcal{U}} 0 = 0$.

Ниже мы докажем σ-аддитивность $\mathbf{\Phi}_{\mathcal{U}}\rho$ для σ-аддитивного ρ. Обозначим

$$\nu(I) := \langle \mathbf{\Phi}_{\mathcal{U}}\rho, \mathbf{P}_I \rangle = \lim_{\mathcal{U}} \nu_\rho(I - j).$$

Нам нужно показать σ-аддитивность ν. Очевидно, что ν является конечно-аддитивной мерой на $\mathcal{P}(\kappa)$. Следовательно, достаточно доказать непрерывность ν сверху. Пусть $I_1 \supset I_2 \supset \ldots$ таковы, что $\bigcap\limits_{n\in\mathbb{N}} I_n = \varnothing$. Нам нужно доказать, что $\lim\limits_{n\to\infty} \nu(I_n) = 0$. Предположим от противного, что $\lim\limits_{n\to\infty} \nu(I_n) = L > 0$. Тогда для некоторого N и достаточно больших $n > N$ имеем

$$\left\{ j : \nu_\rho(I_n - j) > L/2 \right\} \in \mathcal{U}.$$

Поскольку ультрафильтр $\mathcal{U}$ является σ-полным, имеем

$$\bigcap_{n>N} \left\{ j : \nu_\rho(I_n - j) > L/2 \right\} \in \mathcal{U}.$$

В частности, это означает, что пересечение содержит по крайней мере один элемент j_0, общий для всех $n > N$. Таким образом, для этого j_0 и всех $n > N$ выполнено $\nu_\rho(I_n - j_0) > L/2$. Но $\nu_\rho(I_n - j_0) \xrightarrow[n\to\infty]{} 0$ в силу σ-аддитивности ν_ρ. Это приводит к противоречию. □

Таким образом, на измеримых по Уламу кардиналах можно сконструировать квантовые каналы, дающие сингулярные σ-аддитивные результаты. Они разрушают нормальные состояния, но сохраняют сингулярность и σ-аддитивность. Это можно представить так, будто эти квантовые каналы архивируют всю информацию где-то «далеко» на σ-полных ультрафильтрах.

4. Заключение

Мы продемонстрировали, что классификация квантовых состояний на $\ell_2(\kappa)$ неразрывно связана с аксиоматическими основаниями теории множеств. В частности, существование сингулярных σ-аддитивных состояний не является свойством одной лишь алгебры наблюдаемых, а зависит от того, является ли размерность κ измеримым по Уламу кардиналом.

Данная работа расширяет фундаментальные результаты Д. Блехера и Н. Уивера [8], предлагая конкретный аналитический и динамический базис для таких состояний. Установив их представимость через интеграл Петтиса, мы показали, что структура квантовых состояний, связанная с мерой, «выживает» при переходе к сингулярному сектору в присутствии больших кардиналов. Конструкция квантового канала $\mathbf{\Phi}_{\mathcal{U}}$ дополнительно иллюстрирует эту связь, выступая в роли механизма трансформации, который «переносит» информацию из нормальных состояний в сингулярные σ-аддитивные результаты. Этот результат позволяет предположить, что в пространствах достаточно большой размерности квантовая информация может быть «архивирована» таким образом, что она остается согласованной с σ-аддитивностью, но становится недоступной для любых локальных или компактных проекций.

В работе [8] было показано, что чистое состояние, заданное на алгебре наблюдаемых $\mathcal{D}(\ell_2(\kappa)) \cong \ell_\infty(\kappa)$, может быть единственным образом продолжено до чистого состояния на всей алгебре наблюдаемых $\mathcal{B}(\ell_2(\kappa))$. Представляет интерес связать эти результаты с представимостью состояний по Петтису; сложность здесь заключается в том, что нельзя определить индуцированную меру на всем $\mathcal{P}(S^1(\ell_2(\kappa)))$, так как она не будет даже конечно-аддитивной. Таким образом, было бы интересно получить аналогичные результаты для полной алгебры наблюдаемых $\mathcal{B}(\ell_2(\kappa))$.

Список литературы

[1] K. Yosida, E. Hewitt, *Finitely additive measures*, Trans. Amer. Math. Soc. **72** (1), 46–66 (1952).
DOI: https://doi.org/10.1090/S0002-9947-1952-0045194-X

[2] Г.Г. Амосов, В.Ж. Сакбаев, *Об аналогах спектрального разложения квантового состояния*, Матем. заметки **93** (3), 323–332 (2013).
DOI: https://doi.org/10.4213/mzm9085

[3] G. Amosov, V. Sakbaev, *On dynamics of quantum states generated by averaging of random shifts*, Adv. Oper. Theory **10** (3), paper No. 51 (2025).
DOI: https://doi.org/10.1007/s43036-025-00440-2

[4] И.В. Волович, В.Ж. Сакбаев, *Об универсальной краевой задаче для уравнений математической физики*, Тр. МИАН **285**, 64–88 (2014).
DOI: https://doi.org/10.1134/S037196851402006X

[5] И.В. Волович, В.Ж. Сакбаев, *О квантовой динамике на C^*-алгебрах*, Тр. МИАН **301**, 33–47 (2018).
DOI: https://doi.org/10.1134/S0371968518020036

[6] Ю.Н. Орлов, В.Ж. Сакбаев, Диффузия квантовых состояний, порождаемая классическим случайным блужданием, СМФН **71** (2), 275–286 (2025).
DOI: https://doi.org/10.22363/2413-3639-2025-71-2-275-286

[7] E.A. Dzhenzher, S.V. Dzhenzher, V.Zh. Sakbaev, *Banach and counting measures, and dynamics of singular quantum states generated by averaging of operator random walks*, Lobachevskii J. Math. (2026), принята к печати.

[8] D.P. Blecher and N. Weaver, *Quantum measurable cardinals*, J. Funct. Anal. **273** (5), 1870–1890 (2017).
DOI: https://doi.org/10.1016/j.jfa.2017.05.006

[9] T.J. Jech, *Measurable cardinals*, in: Set theory. Springer Monographs in Mathematics. Springer, Berlin, Heidelberg, 125–138 (2003).
DOI: https://doi.org/10.1007/3-540-44761-X_10

[10] N. Dunford, J. Schwartz, *Linear operators. Part* 1. *General theory*, Interscience Publ., New York, 1958.
URL: https://books.google.ru/books?id=x94XzQEACAAJ

Дженжер Святослав Вадимович
Московский физико-технический институт,
Институтский пер., д. 9, г. Долгопрудный, 141701, Россия,
e-mail: sdjenjer@yandex.ru

Volume 4, Issue 2
pp. 104–117 (2026)

UDC 517.98, 530.145, 510.223, 517.518.3
MSC 03E55, 46L30, 81P47, 46G10

Quantum channels preserving sigma-additivity and Ulam measurable cardinals

S.V. Dzhenzher

Abstract. We study the interplay between the properties of quantum states on the Hilbert space $\ell_2(\kappa)$ and the set-theoretic nature of the cardinal κ. We focus on the existence of singular σ-additive states – functionals whose induced measures are σ-additive yet vanish on singletons. While the existence of such states is known to be equivalent to the Ulam measurability of κ, their structural and dynamical properties remain largely unexplored. We prove that any σ-additive state on the diagonal algebra is representable as a Pettis integral over a singular σ-additive measure, extending the classical representation theory to the non-normal sector. Furthermore, we construct a class of quantum channels using σ-complete ultrafilters that map normal states to singular σ-additive states, effectively «archiving» information into the singular part of the state space.

Keywords: measurable cardinals; quantum dynamics; singular quantum states; Pettis integrals.

DOI: 10.26907/2949-3919.2026.2.104-117

References

[1] K. Yosida, E. Hewitt, *Finitely additive measures*, Trans. Amer. Math. Soc. **72** (1), 46–66 (1952).
DOI: https://doi.org/10.1090/S0002-9947-1952-0045194-X

[2] G.G. Amosov, V.Zh. Sakbaev, *On analogs of spectral decomposition of a quantum state*, Math. Notes **93** (3), 351–359 (2013).
DOI: https://doi.org/10.1134/S0001434613030012

[3] G. Amosov, V. Sakbaev, *On dynamics of quantum states generated by averaging of random shifts*, Adv. Oper. Theory **10** (3), paper No. 51 (2025).
DOI: https://doi.org/10.1007/s43036-025-00440-2

[4] I.V. Volovich, V.Zh. Sakbaev, *Universal boundary value problem for equations of mathematical physics*, Proc. Steklov Inst. Math. **285** (1), 56–80 (2014).
DOI: https://doi.org/10.1134/S0081543814040063

Received: 29 April 2026. Accepted: 12 May 2026. Published: 07 July 2026.

[5] I.V. Volovich, V.Zh. Sakbaev, *On quantum dynamics on C^*-algebras*, Proc. Steklov Inst. Math. **301** (1), 25–38 (2018).
DOI: https://doi.org/10.1134/S008154381804003X

[6] I.V. Volovich, V.Zh. Sakbaev, Diffusion of quantum states generated by a classical random walk, CMFD **71** (2), 275–286 (2025) [in Russian].
DOI: https://doi.org/10.22363/2413-3639-2025-71-2-275-286

[7] E.A. Dzhenzher, S.V. Dzhenzher, V.Zh. Sakbaev, *Banach and counting measures, and dynamics of singular quantum states generated by averaging of operator random walks*, Lobachevskii J. Math. (2026), to appear.

[8] D.P. Blecher and N. Weaver, *Quantum measurable cardinals*, J. Funct. Anal. **273** (5), 1870–1890 (2017).
DOI: https://doi.org/10.1016/j.jfa.2017.05.006

[9] T.J. Jech, *Measurable cardinals*, in: Set theory. Springer Monographs in Mathematics. Springer, Berlin, Heidelberg, 125–138 (2003).
DOI: https://doi.org/10.1007/3-540-44761-X_10

[10] N. Dunford, J. Schwartz, *Linear operators. Part* 1. *General theory*, Interscience Publ., New York, 1958.
URL: https://books.google.ru/books?id=x94XzQEACAAJ

Dzhenzher Sviatoslav Vadimovich
Moscow Institute of Physics and Technology,
9 Institutskii per., Dolgoprudny 141701, Russia,
e-mail: sdjenjer@yandex.ru

Том 4, Выпуск 2
Стр. 118–133 (2026)

УДК 517.988
MSC 47H60

О неподвижных точках строго положительных стохастических операторов на одномерном симплексе

Ш.Д. Нодиров, Ю.Х. Эшкабилов

Аннотация. Исследуется класс строго положительных стохастических операторов степени n, действующих на одномерном симплексе. Основное внимание уделяется задаче о количестве неподвижных точек таких операторов. Показано, что эта задача сводится к исследованию количества корней соответствующего полинома степени n на интервале $(0, 1)$. Доказано существование неподвижной точки для произвольного n.

Для квадратичного случая ($n = 2$) установлена единственность неподвижной точки. Для кубического оператора ($n = 3$) получены условия существования одной, двух или трех неподвижных точек. Для оператора четвертой степени ($n = 4$) доказаны критерии количества неподвижных точек в зависимости от параметров оператора.

Ключевые слова: неподвижная точка, стохастический оператор, симплекс, биномиальный коэффициент, полином, точки экстремума.

DOI: 10.26907/2949-3919.2026.2.118-133

Введение

Изучение стохастических операторов занимает центральное место в теории нелинейных динамических систем и математической биологии [1]. Особый интерес представляют стохастические операторы, сохраняющие симплекс и обладающие свойством полной симметрии коэффициентов [2–8]. Одной из фундаментальных задач, связанных с такими операторами, является исследование их неподвижных точек, которые определяют стационарные состояния системы и играют ключевую роль в анализе ее долгосрочного поведения.

В нашей работе рассматривается класс строго положительных стохастических операторов степени n, действующих на одномерном симплексе. Основное внимание уделяется задаче о количестве неподвижных точек таких операторов. Показано, что эта задача сводится к исследованию количества корней соответствующего полинома степени n на интервале $(0, 1)$, что устанавливает связь между теорией операторов и алгебраическими методами.

Благодарности. Исследование выполнено при поддержке прикладного гранта Агентства инновационного развития при Министерстве высшего образования, науки и инноваций Республики Узбекистан (номер AL-9224093956).

Поступила: 02.12.2025. Принята: 03.03.2026. Опубликована: 07.07.2026.

Особенностью этих операторов является их естественная интерпретация в задачах популяционной генетики полиплоидных организмов, где генотип потомка формируется при объединении генетического материала n родительских особей [1].

Целью работы является получение точных оценок и критериев для количества неподвижных точек в зависимости от степени оператора и значений его параметров. В работе последовательно исследуются квадратичные ($n = 2$), кубические ($n = 3$) и квартические ($n = 4$) операторы. Для каждого случая выводятся явные условия на коэффициенты, гарантирующие существование и единственность неподвижной точки, а также анализируются возможности возникновения множественных неподвижных точек.

Полученные результаты имеют приложения в различных областях, включая теорию меры Гиббса для моделей с континуумом значений спина, где неподвижные точки соответствующих операторов связаны с фазовыми переходами [9–11].

1. Предварительные сведения

В m-мерном вещественном векторном пространстве $\mathbb{R}^m$ определим множество

$$S^{(m-1)} = \left\{ (x_1, x_2, ..., x_m) \in \mathbb{R}^m : \ \sum_{i=1}^{m} x_i = 1,\ x_i \geq 0,\ i = \overline{1,m} \right\},$$

где $S^{(m-1)}$ это $(m-1)$-мерный базисный симплекс в $\mathbb{R}^m$.

Определение 1 ([2])**.** Произвольный непрерывный оператор V_n, определенный на симплексе $S^{(m-1)}$, будем называть стохастическим, если

$$(V_n x)_l = x'_l = \sum_{i_1, i_2, ..., i_n = 1}^{m} p_{i_1 i_2 ... i_n, l} x_{i_1} x_{i_2} ... x_{i_n}, \quad l = \overline{1,m}, \tag{1}$$

где

$$p_{i_1 i_2 ... i_n, l} \geq 0, \quad i_j = \overline{1,m}, \ \ j = \overline{1,n}, \ \ l = \overline{1,m};$$

$$p_{i_1 i_2 ... i_n, l} = p_{i_{\pi(1)} i_{\pi(2)} ... i_{\pi(n)}, l}, \quad l = \overline{1,m},$$

для любой перестановки π и

$$\sum_{l=1}^{m} p_{i_1 i_2 ... i_n, l} = 1, \quad i_j = \overline{1,m}, \ \ j = \overline{1,n}.$$

Мы будем изучать количество неподвижных точек стохастического оператора (1) на одномерном симплексе, в случае, когда все коэффициенты оператора $V_n : S^1 \to S^1$ строго положительные, т. е.

$$V_n(\mathbf{x}) = \left(\sum_{k=0}^{n} \binom{n}{k} p_{k(1,2),1} x_1^{n-k} x_2^k,\ \sum_{k=0}^{n} \binom{n}{k} p_{k(1,2),2} x_1^{n-k} x_2^k \right), \quad \mathbf{x} = (x_1, x_2) \in S^1, \qquad (2)$$

где $\binom{n}{k} = \dfrac{n!}{(n-k)!k!}$ – биномиальный коэффициент, $p_{k(1,2),i} > 0$, $\sum\limits_{i=1}^{2} p_{k(1,2),i} = 1$, $k(1,2) = \underbrace{111...1}_{n-k}\underbrace{222...2}_{k}$, $k = \overline{0,n}$.

Поскольку все его координатные функции представлены в виде многочленов со строго положительными коэффициентами, он отображает симплекс S^1 в множество векторов со строго положительными компонентами. Поэтому для определенности будем называть оператор (2) строго положительным стохастическим оператором. Отметим, что операторы такого вида возникают в задаче о нахождении неподвижных точек интегрального оператора Гаммерштейна с вырожденным ядром [11]. Количество таких точек, в свою очередь, соответствует количеству мер Гиббса для моделей с континуумом значений спина.

Множество неподвижных точек оператора (2) в одномерном симплексе обозначим через $\mathrm{Fix}(V_n)$, т. е.

$$\mathrm{Fix}(V_n) = \left\{ \mathbf{x} \in S^1 : V_n(\mathbf{x}) = \mathbf{x} \right\}.$$

Ясно, что $|\mathrm{Fix}(V_n)|$ означает количество неподвижных точек оператора V_n в S^1. Здесь $|A|$ – мощность множества A.

В данной работе исследуется класс строго положительных стохастических операторов V_n, действующих на одномерном симплексе. Данные операторы имеют важные приложения в популяционной генетике, где они описывают эволюцию частот аллелей в последовательных поколениях [1, 13, 14].

Биологическая интерпретация математической модели оператора V_n в S^1 может быть сформулирована так:

- $\mathbf{x} = (x_1, x_2)$ – вектор частот аллелей A_1 и A_2 в текущем поколении;
- n – количество родительских особей, участвующих в формировании генотипа потомка;
- k – число родителей, несущих аллель A_1;
- $p_{k(1,2),1}$ – вероятность наследования аллеля A_1 при условии, что ровно k из n родителей являются его носителями;
- $\binom{n}{k}$ – биномиальный коэффициент, учитывающий число способов выбора k родителей-носителей аллеля A_1 из n возможных.

Данная модель особенно хорошо описывает наследование признаков у полиплоидных организмов [13]. В случае тетраплоидных видов ($n = 4$) каждая хромосома представляется четырьмя гомологичными копиями, и генотип потомка формируется при объединении генетического материала четырех родительских хромосом [15]. Для диплоидных организмов ($n = 2$) модель сводится к классической схеме наследования по Менделю [3, 13].

Основной задачей работы является исследование множества неподвижных точек $\mathrm{Fix}(V_n)$. С биологической точки зрения, неподвижные точки соответствуют стабильным генетическим состояниям популяции, а их количество $|\mathrm{Fix}(V_n)|$ определяет возможное число устойчивых генетических конфигураций.

План настоящего исследования — провести детальный анализ неподвижных точек оператора V_n для малых степеней n. Работа структурирована следующим образом: в разделах последовательно исследуются случаи $n = 2$, $n = 3$ и $n = 4$. В каждом из этих разделов выводятся точные необходимые и достаточные условия на параметры оператора, определяющие количество его неподвижных точек.

Введем обозначение

$$\mu_k = \sum_{s=0}^{n-k} (-1)^s \binom{n-k}{s} p_{(k+s)(1,2),1}, \quad k = \overline{0,n},$$

и определим полином степени n следующим образом:

$$P_n(x) = \sum_{k=0}^{n-2} \binom{n}{n-k} \mu_k x^{n-k} + n(\mu_{n-1} - 1)x + \mu_n.$$

Лемма 2. *Количество неподвижных точек стохастического оператора* (2) *в* S^1 *совпадает с количеством корней полинома* $P_n(x)$ *в* $(0,1)$.

Доказательство. Ясно, что задача нахождения неподвижных точек оператора (2) в S^1 требует найти корни полинома

$$\sum_{k=0}^{n} \frac{n!}{(n-k)!\,k!}\, p_{k(1,2),1}\, x^{n-k}(1-x)^k - x = Q_n(x) - x$$

в отрезке $(0,1)$. Поскольку

$$(1-x)^k = \sum_{j=0}^{k} \binom{k}{j} (-1)^j x^j,$$

то подставляя это выражение в исходную сумму, получаем

$$Q_n(x) = \sum_{k=0}^{n} \binom{n}{k} p_{k(1,2),1} x^{n-k} \sum_{j=0}^{k} \binom{k}{j} (-1)^j x^j.$$

Перемножая x^{n-k} и x^j, имеем x^{n-k+j}, откуда

$$Q_n(x) = \sum_{k=0}^{n} \sum_{j=0}^{k} \binom{n}{k} \binom{k}{j} (-1)^j p_{k(1,2),1} x^{n-k+j}.$$

Пусть

$$m = n - k + j \quad \Longleftrightarrow \quad j = m - n + k.$$

Тогда коэффициент при x^m равен

$$\sum_{k=n-m}^{n} \binom{n}{k} \binom{k}{m-n+k} (-1)^{m-n+k} p_{k(1,2),1}.$$

Применяя равенство

$$\binom{n}{k} \binom{k}{m-n+k} = \binom{n}{m} \binom{m}{n-k},$$

получаем более симметричную форму:

$$\binom{n}{m} \sum_{s=0}^{m} (-1)^s \binom{m}{s} p_{(n-m+s)(1,2),1}.$$

Заменяя $m = n - k$, получаем

$$Q_n(x) - x = \sum_{k=0}^{n} \binom{n}{n-k} \left(\sum_{s=0}^{n-k} (-1)^s \binom{n-k}{s} p_{(k+s)(1,2),1} \right) x^{n-k} - x = P_n(x).$$

Отметим, что если $\mathbf{x}_0 = (x_0, 1 - x_0)$ является неподвижной точкой оператора (2), то $x_0 \in (0, 1)$ является корнем полинома $P_n(x)$ и наоборот. □

Лемма 3. *Полином $P_n(x)$ имеет по крайней мере один корень в интервале $(0, 1)$.*

Доказательство. По определению многочлена $P_n(x)$ имеем $P_n(0) = p_{n(1,2),1} > 0$ и $P_n(1) = p_{0(1,2),1} - 1 = -p_{0(1,2),2} < 0$. Следовательно, найдется точка x_0 из интервала $(0, 1)$, в которой функция $y = P_n(x)$ равна нулю. □

Из лемм 2 и 3 получаем следующее

Следствие 4. *Оператор (2) имеет неподвижную точку в S^1.*

2. Строго положительный квадратичный стохастический оператор, случай $n = 2$

В случае $n = 2$ оператор (2) задается квадратичной формой, поэтому его называют квадратичным стохастическим оператором. Отметим, что рассматриваемый класс операторов является хорошо изученным, что подтверждается исследованиями [3]. В основном изучение сосредоточено на таких свойствах, как неподвижные точки, динамика системы, поведение траекторий и инвариантные множества. Для более глубокого анализа квадратичные стохастические операторы принято разделять на несколько классов, например, таких как: Вольтерровский, квази-Вольтерровский, сепарабельный и т. д. Следует отметить, что такие операторы также встречаются при исследовании меры Гиббса на дереве Кэли для моделей с континуумом множеством значений спина [9].

Теорема 5. *Строго положительный квадратичный стохастический оператор V_2 имеет единственную неподвижную точку в S^1.*

Доказательство. Следствие 4 гарантирует существование неподвижных точек оператора V_2 в S^1. Мы докажем единственность неподвижных точек оператора V_2 в S^1.

Отметим, что задача нахождения неподвижных точек оператора V_2 в S^1 требует найти корни полинома

$$P_2(x) = (p_{11,1} - 2p_{12,1} + p_{22,1})x^2 + (2p_{12,1} - 2p_{22,1} - 1)x + p_{22,1}$$

в $(0,1)$. Мы проанализируем поведение графика функции $y = P_2(x)$. Рассмотрим несколько случаев.

1) Пусть $p_{11,1} - 2p_{12,1} + p_{22,1} > 0$. Тогда из соотношений

$$p_2(0) = p_{22,1} > 0, \quad p_2(1) = -p_{11,2} < 0 \quad \text{и} \quad \lim_{x\to\infty} P_2(x) = +\infty$$

имеем, что график функции $y = P_2(x)$ пересекает ось Ox в единственной точке $x_0 \in (0,1)$.

2) Пусть $p_{11,1} - 2p_{12,1} + p_{22,1} < 0$. Тогда из соотношений

$$P_2(0) = p_{22,1} > 0, \quad P_2(1) = -p_{11,2} < 0 \quad \text{и} \quad \lim_{x\to\infty} P_2(x) = -\infty$$

имеем, что парабола пересекает ось абсцисс в единственной точке $x_0 \in (0,1)$.

3) Пусть $p_{11,1} - 2p_{12,1} + p_{22,1} = 0$. Тогда корень полинома имеет следующий вид:

$$x = -\frac{p_{22,1}}{2p_{12,1} - 2p_{22,1} - 1} = \frac{p_{22,1}}{p_{11,2} + p_{22,1}} \in (0,1).$$

Во всех случаях полином $P_2(x)$ имеет единственный корень в $(0,1)$. Это указывает на существование единственной неподвижной точки оператора V_2 в S^1.

Теорема 5 доказана. □

После упрощений дискриминант полинома $P_2(x)$ принимает вид:

$$D = (2p_{12,1} - 1)^2 + 4p_{22,1}p_{11,2}.$$

Отметим, что точка $\mathbf{x_0} = (x_0, 1-x_0) \in S^1$ является неподвижной точкой оператора V_2. Здесь x_0 – корень полинома $P_2(x)$ в $(0,1)$. Таким образом, верна следующая

Теорема 6. *Для множества неподвижных точек строго положительного квадратичного стохастического оператора V_2 выполняются следующие утверждения*:

(*a*) *если* $p_{11,1} - 2p_{12,1} - p_{22,1} > 0$, *то*

$$\mathrm{Fix}(V_2) = \left\{ \left(\frac{2p_{12,1} - 2p_{22,1} - 1 - \sqrt{D}}{2(p_{11,1} - 2p_{12,1} - p_{22,1})}, \ \frac{2p_{11,1} - 6p_{12,1} + 1 + \sqrt{D}}{2(p_{11,1} - 2p_{12,1} - p_{22,1})} \right) \right\};$$

(*b*) *если* $p_{11,1} - 2p_{12,1} - p_{22,1} < 0$, *то*

$$\mathrm{Fix}(V_2) = \left\{ \left(\frac{2p_{12,1} - 2p_{22,1} - 1 + \sqrt{D}}{2(p_{11,1} - 2p_{12,1} - p_{22,1})}, \ \frac{2p_{11,1} - 6p_{12,1} + 1 - \sqrt{D}}{2(p_{11,1} - 2p_{12,1} - p_{22,1})} \right) \right\};$$

(*c*) *если* $p_{11,1} - 2p_{12,1} - p_{22,1} = 0$, *то*

$$\mathrm{Fix}(V_2) = \left\{ \left(\frac{p_{22,1}}{p_{11,2} + p_{22,1}}, \ \frac{p_{11,2}}{p_{11,2} + p_{22,1}} \right) \right\}.$$

3. Строго положительный кубический стохастический оператор, случай $n = 3$

В случае $n = 3$ рассматриваемый оператор (2) представляет собой строго положительный кубический стохастический оператор V_3. В последнее время данный класс операторов привлекает пристальное внимание исследователей, что подтверждается растущим числом публикаций по данной тематике (см. [4–8,16,17]). В работах [4,5] исследуются условия на матрицу, при которых соответствующий оператор сохраняет симплекс, и изучается его динамика. Подобные операторы также возникают при отыскании неподвижных точек интегрального оператора Гаммерштейна с вырожденным ядром, появляющегося в исследовании меры Гиббса [10].

Определим полином третьей степени P_3, соответствующий строго положительному стохастическому оператору V_3:

$$P_3(x) = a_0x^3 + a_1x^2 + a_2x + a_3,$$

где

$$a_0 = p_{111,1} - p_{222,1} + 3(p_{122,1} - p_{112,1}), \quad a_1 = 3p_{222,1} + 3p_{112,1} - 6p_{122,1},$$

$$a_2 = 3p_{122,1} - 3p_{222,1} - 1, \quad a_3 = p_{222,1}.$$

Теорема 7. *Если* $a_0 \geq 0$, *то строго положительный кубический стохастический оператор* V_3 *имеет единственную неподвижную точку в* S^1.

Доказательство. Согласно лемме 2, достаточно показать, что в случае $a_0 \geq 0$ многочлен $P_3(x)$ имеет единственный корень на интервале $(0, 1)$.

Пусть $a_0 > 0$. Тогда для полинома $P_3(x)$ справедливы следующие соотношения:

$$P_3(-\infty) < 0, \quad P_3(0) = p_{222,1}, \quad P_3(1) = -p_{111,2}, \quad P_3(+\infty) > 0.$$

Отсюда следует, что полином $P_3(x)$ имеет три вещественных корня x_1, x_2 и x_3 такие, что

$$x_1 \in (-\infty, 0), \quad x_2 \in (0, 1), \quad x_3 \in (1, +\infty).$$

В случае $a_0 = 0$ исходный полином $P_3(x)$ понижает свою степень до второй, что позволяет исследовать его корни методами, применимыми к квадратному полиному $P_2(x)$. Известно, что полином $P_2(x)$ имеет единственный корень на интервале $(0, 1)$, откуда следует, что при $a_0 = 0$ исходный полином $P_3(x)$ также обладает единственным корнем на интервале $(0, 1)$. Для ясности проверим дискриминант:

$$D_1 = a_2^2 - 4a_1a_3.$$

Далее из $a_0 = 0$ следует, что $p_{111,1} - p_{222,1} = 3(p_{112,1} - p_{122,1})$. Тогда

$$\begin{aligned}
D_1 &= (3p_{122,1} - 3p_{222,1} - 1)^2 - 4p_{222,1}(3p_{222,1} + 3p_{112,1} - 6p_{122,1}) = (3p_{122,1} - 3p_{222,1} - 1)^2 - \\
&\quad - 4p_{222,1}\left(3(p_{222,1} - p_{122,1}) + 3(p_{112,1} - p_{122,1})\right) \\
&= (3p_{122,1} - 3p_{222,1} - 1)^2 - 4p_{222,1}(3p_{222,1} - 3p_{122,1} + p_{111,1} - p_{222,1}) \\
&= (3p_{122,1} - 3p_{222,1} - 1)^2 - 4p_{222,1}(2p_{222,1} - 3p_{122,1} + p_{111,1}) \\
&= 9p_{122,1}^2 + 9p_{222,1}^2 + 1 - 18p_{122,1}p_{222,1} - 6p_{122,1} + 6p_{222,1} - 8p_{222,1}^2 + 12p_{122,1}p_{222,1} - 4p_{111,1}p_{222,1} \\
&= 9p_{122,1}^2 - 6p_{122,1}p_{222,1} + p_{222,1}^2 + 1 - 6p_{122,1} + 6p_{222,1} - 4p_{111,1}p_{222,1} \\
&= (3p_{122,1} - p_{222,1})^2 + 1 - 2(3p_{122,1} - p_{222,1}) + 4p_{222,1} - 4p_{111,1}p_{222,1} \\
&= (3p_{122,1} - p_{222,1} - 1)^2 + 4p_{222,1} - 4p_{111,1}p_{222,1} \\
&= (3p_{122,1} - p_{222,1} - 1)^2 + 4p_{222,1}(1 - p_{222,1}) = (3p_{122,1} - p_{222,1} - 1)^2 + 4p_{222,1}p_{111,2}.
\end{aligned}$$

Таким образом, $D_1 > 0$.

Как обычно, из условий $P_3(0) = p_{222,1} > 0$ и $P_3(1) = -p_{111,2} < 0$ следует, что при $a_0 = 0$ полином $P_3(x)$ имеет ровно один корень на интервале $(0, 1)$ независимо от знака a_1. □

Для анализа положительных корней полинома $P_3(x)$ целесообразно использовать правило знаков Декарта (см. [12, с. 38–40]). Составим таблицу всех возможных комбинаций знаков коэффициентов $P_3(x)$:

Таблица 1

$P_3(x)$	a_0	a_1	a_2	a_3	Число перемен знака коэффициентов
1.	$-$	$-$	$-$	$+$	1
2.	$-$	$+$	$+$	$+$	1
3.	$-$	$-$	$+$	$+$	1
4.	$-$	$+$	$-$	$+$	3

Согласно правилу Декарта в первых трех случаях уравнение $P_3(x) = 0$ имеет единственное положительное решение на $(0, 1)$.

Следствие 8. *Если выполняются соотношения*

$$a_0 < 0, \quad a_1 > 0, \quad a_2 < 0, \tag{3}$$

то строго положительный кубический стохастический оператор V_3 может иметь до трех неподвижных точек в S^1, т. е. $1 \le |\mathrm{Fix}(V_3)| \le 3$.

Определим число

$$\triangle := a_1^2 - 3a_0a_2.$$

В случае $\triangle > 0$ введем следующие обозначения:

$$\alpha = \frac{-a_1 + \sqrt{\triangle}}{3a_0}, \quad \beta = \frac{-a_1 - \sqrt{\triangle}}{3a_0}.$$

Очевидно, что числа α и β являются точками экстремума функции $y = P_3(x)$. При выполнении условий (3) выполняются неравенства $0 < \alpha < \beta$, причем функция $y = P_3(x)$ монотонно убывает на интервалах $(-\infty, \alpha]$ и $(\beta, +\infty)$ и монотонно возрастает на интервале $(\alpha, \beta]$.

Кроме того, на отрезке $[0, 1]$ справедливы следующие соотношения:

- $\min_{x\in[0,\beta]} P_3(x) = P_3(\alpha)$,
- $\max_{x\in[\alpha,1]} P_3(x) = P_3(\beta)$,
- $P_3(0) = p_{222,1} > 0$,
- $P_3(1) = -p_{111,2} < 0$.

Таким образом, анализ поведения функции $P_3(x)$ показывает, что верна следующая

Теорема 9. *Пусть выполнены условия* (3), $\triangle > 0$ *и* $\beta < 1$. *Тогда количество неподвижных точек* $|\mathrm{Fix}(V_3)|$ *строго положительного кубического стохастического оператора V_3 в S^1 равно:*

$$|\mathrm{Fix}(V_3)| = \begin{cases} 1, & \text{если } P_3(\alpha)P_3(\beta) > 0; \\ 2, & \text{если } P_3(\alpha)P_3(\beta) = 0; \\ 3, & \text{если } P_3(\alpha)P_3(\beta) < 0. \end{cases}$$

4. Строго положительный квартический стохастический оператор, случай $n = 4$

Поскольку в литературе полином четвертой степени часто называют квартикой, возникающий при $n = 4$ оператор, состоящий из таких полиномов от двух переменных, естественно назвать квартическим оператором.

Определим полином четвертой степени

$$P_4(x) = b_0x^4 + b_1x^3 + b_2x^2 + b_3x + b_4,$$

где

$$b_0 = p_{1111,1} - 4p_{1112,1} + 6p_{1122,1} - 4p_{1222,1} + p_{2222,1}, \quad b_1 = 4p_{1112,1} - 12p_{1122,1} + 12p_{1222,1} - 4p_{2222,1},$$

$$b_2 = 6p_{1122,1} - 12p_{1222,1} + 6p_{2222,1}, \quad b_3 = 4p_{1222,1} - 4p_{2222,1} - 1, \quad b_4 = p_{2222,1}.$$

Заметим, что при $b_0 = 0$ полином $P_4(x)$ понижает степень до третьей, и все результаты, изложенные в предыдущем разделе, полностью применимы к данному случаю.

Введем следующие обозначения, предполагая $b_0 \neq 0$:

$$p = \frac{8b_0b_2 - 3b_1^2}{16b_0^2}, \quad q = \frac{b_1^3 - 4b_0b_1b_2 + 8b_0^2b_3}{32b_0^3},$$

$$Q = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2.$$

Теорема 10. *Если $Q \geq 0$, то строго положительный квартический стохастический оператор V_4 имеет единственную неподвижную точку в S^1.*

Доказательство. Согласно лемме 2 достаточно исследовать количество корней полинома $P_4(x)$ на интервале $(0, 1)$. Для исследования количества корней полинома $P_4(x)$ на интервале $(0, 1)$ проанализируем его поведение. Сначала найдем стационарные точки, приравняв производную к нулю:

$$P_4'(x) = 0. \tag{4}$$

Количество вещественных решений уравнения (4) зависит от параметра Q.

(a) Рассмотрим случай $Q > 0$.

В этом случае уравнение (4) имеет единственную вещественную стационарную точку $x_0 \in \mathbb{R}$, которая является точкой экстремума. Проанализируем значения функции на концах интервала: $P_4(0) = p_{2222,1} > 0$, $P_4(1) = -p_{1111,2} < 0$. Так как функция $y = P_4(x)$ непрерывна, ее значения на концах интервала имеют противоположные знаки и график функции пересекает $(0, 1)$ ровно один раз.

(b) В случае $Q = 0$ уравнение (4) имеет либо один и двукратный, либо трехкратный корень. В обоих случаях функция $y = P_4(x)$ имеет единственную стационарную точку $x_0 \in \mathbb{R}$, которая является точкой экстремума. Аналогично предыдущему случаю полином $P_4(x)$ имеет ровно один корень на интервале $(0, 1)$. Теорема 10 доказана. □

В случае $Q < 0$ определим

$$\theta_l = 2\sqrt{-\frac{p}{3}}\cos\left(\frac{\alpha + 2\pi(l-2)}{3}\right), \quad l = \overline{1,2,3},$$

$$\cos\alpha = -\frac{q}{2}\left(-\frac{3}{p}\right)^{\frac{3}{2}}, \quad \alpha \in [0, \pi].$$

Обозначим

$$\gamma_1 = \theta_3 - \frac{\mu_1}{4\mu_0}, \quad \gamma_2 = \theta_1 - \frac{\mu_1}{4\mu_0}, \quad \gamma_3 = \theta_2 - \frac{\mu_1}{4\mu_0}.$$

В случае $Q < 0$ уравнение (4) имеет три различные вещественные корни $\gamma_1, \gamma_2, \gamma_3$, которые являются стационарными точками функции $P_4(x)$. Как следует из анализа угла θ_l, эти корни удовлетворяют строгому неравенству

$$\gamma_1 < \gamma_2 < \gamma_3.$$

Пусть $b_0 > 0$ (соответственно, $b_0 < 0$). Тогда график функции $y = P_4(x)$ является монотонно возрастающим на множестве $[\gamma_1, \gamma_2] \cup [\gamma_3, +\infty)$ и монотонно убывающим на множестве $(-\infty, \gamma_1] \cup [\gamma_2, \gamma_3]$ (соответственно, монотонно возрастающим на $(-\infty, \gamma_1] \cup [\gamma_2, \gamma_3]$ и монотонно убывающим на $[\gamma_1, \gamma_2] \cup [\gamma_3, +\infty)$).

Кроме того, выполняются следующие соотношения для значений функции в точках 0 и 1:

$$P_4(0) = p_{2222,1} > 0 \quad \text{и} \quad P_4(1) = -p_{1111,2} < 0.$$

Используя проведенный анализ, исследуем все возможные случаи поведения графика функции $y = P_4(x)$ и сформулируем следующий результат:

Теорема 11. *Пусть выполнены условия $Q < 0$, $\gamma_1 > 0$ и $\gamma_3 < 1$. Тогда количество неподвижных точек $|\mathrm{Fix}(V_4)|$ строго положительного квартического стохастического оператора V_4 в S^1 равно:*

$$|\mathrm{Fix}(V_4)| = \begin{cases} 1, & \textit{если} \quad b_0 \prod\limits_{i=1}^{3} P_4(\gamma_i) < 0; \\ 2, & \textit{если} \quad \prod\limits_{i=1}^{3} P_4(\gamma_i) = 0; \\ 3, & \textit{если} \quad b_0 \prod\limits_{i=1}^{3} P_4(\gamma_i) > 0. \end{cases}$$

Список литературы

[1] Ю.И. Любич, *Математические структуры в популяционной генетике*, Наук. Думка, Киев, 1983.

[2] Ф.А. Шахиди, *О бистохастических операторах, определенных в конечномерном симплексе*, Сиб. матем. журн. **50** (2), 463–468 (2009).
URL: https://www.mathnet.ru/rus/smj1973

[3] R. Ganikhodzhaev, F. Mukhamedov, U. Rozikov, *Quadratic stochastic operators and processes: results and open problems*, Infin. Dimens. Anal. Quantum Probab. Relat. Top. **14** (2), 279–335 (2011).
DOI: https://doi.org/10.1142/S0219025711004365

[4] J.N. Jumayev, *Criterion for the preservation of the one-dimensional simplex by a cubic operator*, Uzbek Math. J. **68** (4), 85–95 (2024).
DOI: https://doi.org/10.29229/uzmj.2024-4-9

[5] Ж.Н. Жумаев, *Достаточное условие кубического оператора для сохранения симплекса*, Журн. СФУ. Сер. Матем. и физ. **18** (5), 663–673 (2025).
URL: https://www.mathnet.ru/rus/jsfu1278

[6] U.U. Jamilov, A.Yu. Khamraev, M. Ladra, *On a Volterra cubic stochastic operator*, Bull. Math. Biol. **80** (2), 319–334 (2018).
DOI: https://doi.org/10.1007/s11538-017-0376-0

[7] A.Yu. Khamraev, J.N. Jumayev, *Dynamics of a cubic stochastic operator with one discontinuity point*, Uzbek Math. J. **69** (1), 79–86 (2025).
DOI: https://doi.org/10.29229/uzmj.2025-1-8

[8] A.Yu. Khamraev, N.P. Makhmatkobilov, *On the dynamics of a quasi-strictly non-Volterra cubic stochastic operator*, JCAM **15** (1), 1–9 (2025).
DOI: https://doi.org/10.62476/jcam.151.1

[9] Yu.Kh. Eshkabilov, Sh.D. Nodirov, F.H. Haydarov, *Positive fixed points of quadratic operators and Gibbs measures*, Positivity **20** (4), 929–943 (2016).
DOI: https://doi.org/10.1007/s11117-015-0394-9

[10] Ю.Х. Эшкабилов, Ш.Д. Нодиров, *Положительные неподвижные точки кубических операторов на $\mathbb{R}^2$ и меры Гиббса*, Журн. СФУ. Сер. Матем. и физ. **12** (6), 663–673 (2019).
DOI: https://doi.org/10.17516/1997-1397-2019-12-6-663-673

[11] Ю.Х. Эшкабилов, Ш.Д. Нодиров, *Положительные неподвижные точки интегральных операторов типа Гаммерштейна с вырожденным ядром*, Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки **166** (3), 437–449 (2024).
DOI: https://doi.org/10.26907/2541-7746.2024.3.437-449

[12] В.В. Прасолов, *Многочлены*, МЦНМО, М., 2003.
URL: https://math.ru/lib/391

[13] R. Bürger, *The mathematical theory of selection, recombination, and mutation*, John Wiley & Sons, Ltd., Chichester, 2000.

[14] W.J. Ewens, *Mathematical population genetics.* I. *Theoretical introduction*, Springer-Verlag, New York, 2004.
DOI: https://doi.org/10.1007/978-0-387-21822-9

[15] S.P. Otto, J. Whitton, *Polyploid incidence and evolution*, Annu. Rev. Genet. **34**, 401–437 (2000).
DOI: https://doi.org/10.1146/annurev.genet.34.1.401

[16] B.S. Baratov, U.U. Jamilov, *On separable cubic stochastic operators*, Qual. Theory Dyn. Syst. **23** (2), paper no. 93 (2024).
DOI: https://doi.org/10.1007/s12346-023-00950-5

[17] B.S. Baratov, *The dynamics of a separable cubic operator*, Uzbek Math. J. **68** (2), 27–41 (2024).
DOI: https://doi.org/10.29229/uzmj.2024-2-4

Шохрух Дилмуродович Нодиров
Каршинский государственный университет,
ул. Кучабаг, д. 17, г. Карши, 180119, Узбекистан,
Казанский (Приволжский) федеральный университет,
Научно-образовательный математический центр ПФО,
ул. Кремлевская, д. 35, г. Казань, 420008, Россия,
e-mail: shoh0809@mail.ru

Юсуп Халбаевич Эшкабилов
Каршинский государственный университет,
ул. Кучабаг, д. 17, г. Карши, 180119, Узбекистан,
e-mail: yusup62@mail.ru

Volume 4, Issue 2
pp. 118–133 (2026)

UDC 517.988
MSC 47H60

On fixed points of strictly positive stochastic operators on a one-dimensional simplex

Sh.D. Nodirov, Yu.Kh. Eshkabilov

Abstract. A class of strictly positive stochastic operators of degree n acting on a one-dimensional simplex is investigated. The main focus is on the problem of the number of fixed points of such operators. It is shown that this problem reduces to studying the number of roots of the corresponding degree n polynomial on the interval $(0, 1)$. The existence of at least one fixed point is proved for arbitrary n.

For the quadratic case ($n = 2$), the uniqueness of the fixed point is established. For a cubic operator ($n = 3$), conditions for the existence of one, two, or three fixed points are obtained. For a quartic operator ($n = 4$), criteria determining the number of fixed points are proved in terms of the operator's parameters.

Keywords: fixed point, simplex, stochastic operator, binomial coefficient, polynomial, extreme points.

DOI: 10.26907/2949-3919.2026.2.118-133

References

[1] Y.I. Lyubich, *Mathematical structures in population genetics*, Springer-Verlag, Berlin, 1992.

[2] F.A. Shahidi, *Doubly stochastic operators on a finite-dimensional simplex*, Siberian Math. J. **50** (2), 368–372 (2009).
DOI: https://doi.org/10.1007/s11202-009-0042-3

[3] R. Ganikhodzhaev, F. Mukhamedov, U. Rozikov, *Quadratic stochastic operators and processes: results and open problems*, Infin. Dimens. Anal. Quantum Probab. Relat. Top. **14** (2), 279–335 (2011).
DOI: https://doi.org/10.1142/S0219025711004365

[4] J.N. Jumayev, *Criterion for the preservation of the one-dimensional simplex by a cubic operator*, Uzbek Math. J. **68** (4), 85–95 (2024).
DOI: https://doi.org/10.29229/uzmj.2024-4-9

Acknowledgements. This research was supported by an applied grant from the Agency for Innovative Development under the Ministry of Higher Education, Science and Innovations of the Republic of Uzbekistan (Grant No. AL-9224093956).

Received: 02 December 2025. Accepted: 03 March 2026. Published: 07 July 2026.

[5] J.N. Jumayev, *A sufficient condition for a cubic operator to preserve a simplex*, J. Sib. Fed. Univ. Math. Phys. **18** (5), 663–673 (2025).
URL: https://www.mathnet.ru/rus/jsfu1278

[6] U.U. Jamilov, A.Yu. Khamraev, M. Ladra, *On a Volterra cubic stochastic operator*, Bull. Math. Biol. **80** (2), 319–334 (2018).
DOI: https://doi.org/10.1007/s11538-017-0376-0

[7] A.Yu. Khamraev, J.N. Jumayev, *Dynamics of a cubic stochastic operator with one discontinuity point*, Uzbek Math. J. **69** (1), 79–86 (2025).
DOI: https://doi.org/10.29229/uzmj.2025-1-8

[8] A.Yu. Khamraev, N.P. Makhmatkobilov, *On the dynamics of a quasi-strictly non-Volterra cubic stochastic operator*, JCAM **15** (1), 1–9 (2025).
DOI: https://doi.org/10.62476/jcam.151.1

[9] Yu.Kh. Eshkabilov, Sh.D. Nodirov, F.H. Haydarov, *Positive fixed points of quadratic operators and Gibbs measures*, Positivity **20** (4), 929–943 (2016).
DOI: https://doi.org/10.1007/s11117-015-0394-9

[10] Yu.Kh. Eshkabilov, Sh.D. Nodirov, *Positive fixed points of cubic operators on* $\mathbb{R}^2$ *and Gibbs measures*, J. Sib. Fed. Univ. Math. Phys. **12** (6), 663–673 (2019).
DOI: https://doi.org/10.17516/1997-1397-2019-12-6-663-673

[11] Yu.Kh. Eshkabilov, Sh.D. Nodirov, *Positive fixed points of Hammerstein integral operators with degenerate kernel*, Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki **166** (3), 437–449 (2024). [in Russian].
DOI: https://doi.org/10.26907/2541-7746.2024.3.437-449

[12] V.V. Prasolov, *Polynomials*, Springer-Verlag, Berlin, 2004.
DOI: https://doi.org/10.1007/978-3-642-03980-5

[13] R. Bürger, *The mathematical theory of selection, recombination, and mutation*, John Wiley & Sons, Ltd., Chichester, 2000.

[14] W.J. Ewens, *Mathematical population genetics.* I. *Theoretical introduction*, Springer-Verlag, New York, 2004.
DOI: https://doi.org/10.1007/978-0-387-21822-9

[15] S.P. Otto, J. Whitton, *Polyploid incidence and evolution*, Annu. Rev. Genet. **34**, 401–437 (2000).
DOI: https://doi.org/10.1146/annurev.genet.34.1.401

[16] B.S. Baratov, U.U. Jamilov, *On separable cubic stochastic operators*, Qual. Theory Dyn. Syst. **23** (2), paper no. 93 (2024).
DOI: https://doi.org/10.1007/s12346-023-00950-5

[17] B.S. Baratov, *The dynamics of a separable cubic operator*, Uzbek Math. J. **68** (2), 27–41 (2024).
DOI: https://doi.org/10.29229/uzmj.2024-2-4

Shohruh Dilmurodovich Nodirov
Karshi State University,
17 Kuchabag str., Karshi 180119, Uzbekistan,
Kazan Federal University,
Volga Region Mathematical Center,
18 Kremlyovskaya str., Kazan 420008, Russia,
e-mail: shoh0809@mail.ru

Yusup Khalbayevich Eshkabilov
Karshi State University,
17 Kuchabag str., Karshi 180119, Uzbekistan,
e-mail: yusup62@mail.ru

Том 4, Выпуск 2
Стр. 134–146 (2026)

УДК 510.54, 510.57
MSC 03D45, 03D30

Об одном классе взаимных расположений двух M-кривых степени 4

Н.Д. Пучкова

Аннотация. Рассматривается задача вещественной изотопической классификации взаимных расположений в вещественной проективной плоскости двух M-кривых степени 4. На изучаемые расположения наложены условие максимальности (овал одной из этих кривых имеет 16 попарно различных общих точек с овалом другой из них) и условие комбинаторного характера, выделяющее специальный тип таких расположений. Получена полная изотопическая классификация указанных расположений. Доказательства алгебраической нереализуемости топологических моделей расположений изучаемого класса кривыми степени 8 проводятся методом Оревкова, основанным на применении теории кос и зацеплений.

Ключевые слова: плоские вещественные алгебраические кривые, распадающиеся кривые, квазиположительные косы, метод Оревкова, неравенство Мурасуги.

DOI: 10.26907/2949-3919.2026.2.134-146

Введение

В 1900 году на Международном конгрессе математиков в Париже Давид Гильберт представил список проблем, которые, по его мнению, в первую очередь ждут решения в XX веке. В первой части 16-й проблемы Д. Гильберт поставил задачу вещественной изотопической классификации неособых плоских вещественных алгебраических кривых. На данный момент завершена классификация неособых кривых до седьмой степени включительно.

Каковы возможные расположения вещественной распадающейся кривой данной степени на вещественной проективной плоскости? Этот вопрос интенсивно изучался в последние десятилетия. Топологическая классификация распадающихся кривых степени 6 при некоторых условиях максимальности и общего положения была найдена Г.М. Полотовским в 1977 г. [1], аналогичная задача о кривых степени 7 почти завершена, ей занималась большая группа авторов (А.Б. Корчагин, С.Ю. Оревков, Г.М. Полотовский, Е.И. Шустин и др., библиографические ссылки см. в [2]).

Благодарности. Исследование осуществлено в рамках Программы фундаментальных исследований НИУ ВШЭ.

Поступила: 30.09.2024. Принята: 14.10.2025. Опубликована: 07.07.2026.

Данная статья посвящена изучению взаимных расположений в вещественной проективной плоскости $\mathbb{R}P^2$ двух M-кривых степени 4, находящихся в общем положении, и является продолжением исследований [3, 4]. Далее в работе вводится определенный тип таких расположений, рассмотрением которого ограничиваемся ввиду большого числа всех подлежащих исследованию возможностей. Для расположений этого типа удалось получить полную классификацию, которая приведена в конце статьи.

Автор благодарит Г.М. Полотовского за предложенную задачу и помощь в работе и С.Ю. Оревкова за ценные замечания.

1. Постановка задачи

Через C_k будем обозначать вещественную проективную алгебраическую кривую степени k, т. е. однородный многочлен степени k с вещественными коэффициентами от трех переменных, рассматриваемый с точностью до ненулевого постоянного множителя, а через $\mathbb{R}C_k$ – множество вещественных точек кривой C_k, т. е. множество точек вещественной проективной плоскости, в которых многочлен C_k обращается в нуль.

Пусть многочлен C_8 распадается в произведение двух многочленов степени 4: $C_8 = C_4 \cdot \widetilde{C_4}$, т. е. $\mathbb{R}C_8 = \mathbb{R}C_4 \cup \mathbb{R}\widetilde{C_4}$. Данная работа посвящена топологической классификации троек

$$\left(\mathbb{R}P^2, \mathbb{R}C_8, \mathbb{R}C_4\right)$$

при следующих условиях:

1) кривые C_4 и $\widetilde{C_4}$ являются M-кривыми, т. е. каждая из них состоит в $\mathbb{R}P^2$ из четырех попарно не пересекающихся овалов (двусторонне вложенных в проективную плоскость топологических окружностей), лежащих вне друг друга;
2) общие вещественные точки кривых C_4 и $\widetilde{C_4}$ попарно различны и их число максимально, т. е. $\#(\mathbb{R}C_4 \cap \mathbb{R}\widetilde{C_4}) = 16$;
3) все эти 16 точек лежат на одном овале кривой C_4 и на одном овале кривой $\widetilde{C_4}$.

Назовем *топологической моделью* распадающейся кривой рассматриваемого вида (для краткости ниже – просто "модель") набор восьми топологических окружностей, которые вложены в $\mathbb{R}P^2$ двусторонне и которые ведут себя с точки зрения числа и расположения общих точек так, как две кривые степени 4 при условиях 1)–3) выше. Наша задача – выяснить, какие модели могут быть реализованы как объединение двух M-кривых степени 4, а какие – нет.

Определение 1. Пусть овал O целиком лежит в аффинной плоскости[1]. Рассмотрим незамкнутую дугу без самопересечений, тоже целиком лежащую в аффинной плоскости и пересекающую овал O в восьми попарно различных точках. Эту дугу будем называть *образующей дугой*. При достаточно малом ε граница ε-окрестности этой дуги представляет

[1] Для овала M-кривой степени 4 этого всегда можно добиться, выбрав в качестве бесконечно удаленной прямой аффинной плоскости слегка сдвинутую двойную касательную к этой кривой.

собой другой овал, который пересекает исходный овал O в 16 попарно различных точках. Этот второй овал будем называть *змеей*, а такое взаимное расположение двух овалов будем называть пересечением ветвей типа *"змея, обвивающаяся вокруг овала"*.

Определение 2. Пусть в вещественной проективной плоскости $\mathbb{R}P^2$ имеем пересечение двух овалов типа "змея, обвивающаяся вокруг овала" такое, что один (а, значит, и второй) конец образующей дуги лежит в диске, ограниченном овалом O. Отвечающую такой дуге змею назовем *"змеей с концом внутри овала"*.

В данной работе будем исследовать некоторое подмножество расположений двух кривых степени 4, содержащих "змею с концом внутри овала", придерживаясь следующей схемы:

1) перечисление моделей, удовлетворяющих наложенным условиям;
2) доказательства нереализуемости некоторых моделей из списка п. 1) алгебраическими кривыми степени 8;
3) реализация остальных моделей алгебраическими кривыми степени 8.

Мы будем доказывать запреты с помощью теоремы Безу и с помощью метода Оревкова, основанного на теории кос и зацеплений.

2. Перечисление моделей

2.1. Кодировка расположений пересекающихся овалов и список кодов. Пусть имеется модель кривой степени 8, распадающейся в произведение двух M-кривых степени 4, со змеей с концом внутри овала. В дальнейшем кривую, один из овалов которой есть змея, будем называть *кривой номер* 1, а кривую, вокруг овала которой обвивается змея, будем называть *кривой номер* 2. Овалы, на которых нет точек пересечения (в нашем случае таких овалов шесть: три овала кривой номер 1 и три овала кривой номер 2), называются *свободными*. Напомним, что в силу условия 1) овалы, принадлежащие кривой с одним номером, лежат вне друг друга.

Занумеруем на овале кривой номер 2 подряд восемь точек – точек пересечения овала с образующей дугой. Тогда расположение образующей дуги относительно пересекаемого ею овала можно кодировать подстановкой порядка 8, запись которой в виде цикла получается выписыванием номеров точек на овале, проходимых при движении по образующей дуге от одного ее конца до второго.

Чтобы получить однозначную кодировку расположения образующей дуги, ориентируем образующую дугу и овал кривой номер 2. В кодировке следом за подстановкой в квадратных скобках будем записывать четыре знака: первый отвечает сегменту образующей дуги, соединяющему первый и второй элементы подстановки, второй знак – третий и четвертый элементы, третий – пятый и шестой, четвертый – седьмой и восьмой. Если ориентация образующей дуги на рассматриваемом сегменте совпадает с ориентацией

овала, то будем ставить знак “+”, иначе – знак “−”. Например, коду $(12345876)[++-+]$ отвечает расположение на рис. 1.

Если двум разным кодам соответствуют гомеоморфные расположения кривых, то оставим тот, в котором подстановка и набор знаков, записываемых за ней, меньше в смысле лексикографического порядка. Знак “+” будем считать меньше в смысле лексикографического порядка, чем знак “−”.

С помощью устранения точек пересечения (эти устранения независимы в силу теоремы Брюзотти – см., например, [5]) докажем, что расположения, отвечающие некоторым подстановкам, не могут быть реализованы кривой степени 8. Например, кривая на рис. 2, получаемая устранением точек пересечения на рис. 1, имеет два гнезда[2] веса 2 с разными внешними овалами, окруженные еще одним овалом; известно, что такое расположение овалов не может быть реализовано кривой степени 8 (в силу противоречия теореме Безу при пересечении с прямой), поэтому нереализуемо и расположение рис. 1.

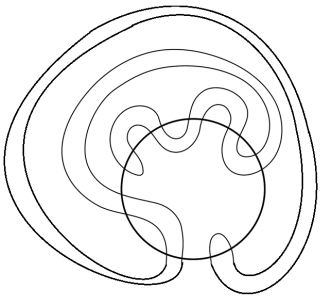


Рис. 1

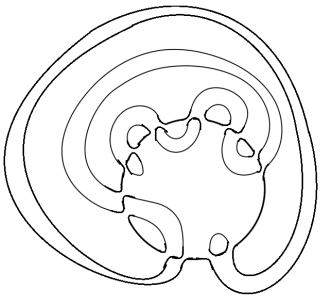


Рис. 2

Применением описанного приема доказывается следующая

Теорема 3. *Полный список кодов, отвечающих попарно различным образующим дугам для не противоречащих теореме Безу моделей расположений двух кривых степени* 4 *типа “змея с концом внутри овала”, состоит из следующих кодов*:

1. $(12345678)[++++]$,	2. $(12345678)[+++-]$,	3. $(12345678)[++-+]$,
4. $(12345687)[+++-]$,	5. $(12345876)[+++-]$,	6. $(12345876)[++--]$,
7. $(12346785)[+++-]$,	8. $(12347658)[++-+]$,	9. $(12347658)[++--]$,
10. $(12348756)[++-+]$,	11. $(12348765)[++--]$,	12. $(12365478)[++-+]$,
13. $(12365478)[+--+]$,	14. $(12365487)[++--]$,	15. $(12367854)[+++-]$,
16. $(12367854)[+-+-]$,	17. $(12456783)[+++-]$,	18. $(12458763)[++--]$,
19. $(12763458)[+-++]$,	20. $(12763458)[+-+-]$,	21. $(12765438)[+--+]$,
22. $(12765438)[+---]$,	23. $(12876534)[+--+]$.	

2.2. О расположениях свободных овалов. Для каждого из расположений, коды которых перечислены в теореме 3, дополнение плоскости $\mathbb{R}P^2$ к объединению пересекающихся овалам состоит из восемнадцати компонент связности. В этих компонентах

[2]Гнездом веса s называется набор из s овалов, последовательно окружающих друг друга.

связности должны располагаться шесть овалов – по три для каждой из пересекающихся кривых. Количество допустимых попарно различных распределений овалов между этими областями зависит от топологии объединения пересекающихся овалов. *Имеются семь расположений, для которых условия распределений этих шести овалов между компонентами связности дополнения к пересекающимся овалам одинаковы – это расположения под номерами* $2, 3, 5, 6, 9, 13$ *и* 16 *из теоремы* 3. *Именно эти семь расположений изучаются в дальнейшем.*

Покажем, как запрещаются по теореме Безу модели, рассмотрев конкретный пример – змею, отвечающую коду $(12345678)[+++-]$, см. рис. 3.

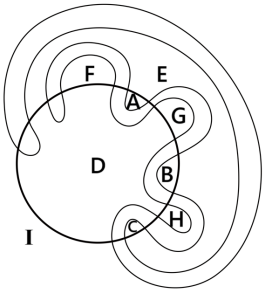


Рис. 3

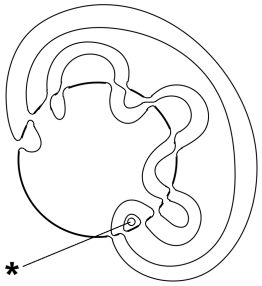


Рис. 4

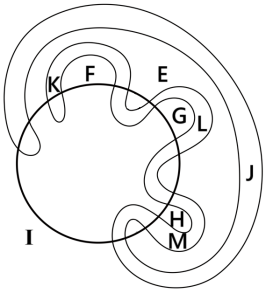


Рис. 5

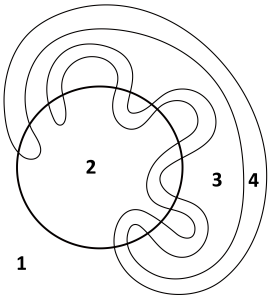


Рис. 6

Найдем сначала все возможные области для расположения овалов кривой номер 1. Напомним, что эти овалы должны располагаться вне друг друга и вне змеи.

Дополнение к пересекающимся овалам вне змеи состоит из девяти областей. Обозначим эти области буквами латинского алфавита, см. рис. 3. В области C свободный овал лежать не может: устраняя точки пересечения так, как показано на рис. 4 ($*$ – добавленный свободный овал), получим расположение с гнездом веса 4 и еще одним овалом, чего не может быть у кривой степени 8. Совершенно аналогично доказывается невозможность расположения свободного овала кривой номер 1 в областях A, B, F–H.

Аналогично для кривой с номером 2 снова имеем девять областей для свободных овалов, которые обозначены на рис. 5 буквами латинского алфавита. Также с помощью теоремы Брюзотти убеждаемся, что свободные овалы не могут лежать в областях F–H и K–M.

Подведем итог: допустимо распределение свободных овалов только между четырьмя областями, пронумерованными на рис. 6, причем в области 2 могут располагаться только овалы кривой номер 1, в области 4 – только овалы кривой номер 2, а в областях 1 и 3 – как овалы кривой номер 1, так и овалы кривой номер 2 (но вне друг друга). Можно перечислить все возможные распределения шести свободных овалов между этими областями, удовлетворяющие следствиям из теоремы Безу (что и делалось в предыдущих работах – см. таблицы 1 в [3, 4]), но в этом нет необходимости: во-первых, имеются еще другие ограничения, вытекающие из теоремы Безу, а во-вторых, все не противоречащие теореме Безу распределения свободных овалов будут перебираться ниже с помощью компьютера.

3. Запреты с помощью теории кос и зацеплений

Будем доказывать нереализуемость изучаемых моделей алгебраическими кривыми степени 8 с помощью метода, который предложил С.Ю. Оревков в 1999 году в [6]. Подробнее о методе и его применениях см., например, [2–4, 7]. Ограничимся описанием примера его применения к той же змее, отвечающей подстановке $(12345678)[+++-]$.

Изобразим исследуемое расположение так, как показано на рис. 7. Здесь "змея" – овал, нарисованный тонкой линией, а нумерация областей такая же, как на рис. 6.

Выберем в проективной плоскости точку P, не лежащую на кривой, так, чтобы каждая прямая пучка прямых с центром в этой точке пересекала объединение кривых номер 1 и 2 не менее, чем в $8 - 2 = 6$ точках, и нашлась бы прямая l_M ("максимальная"), пересекающая эту кривую в восьми точках, см. рис. 7. Такой пучок будем называть *максимальным*.

Преобразим рис. 7 так, чтобы прямая l_M стала бесконечно удаленной. Получим рис. 8.

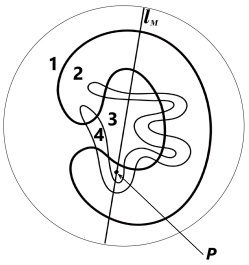


Рис. 7

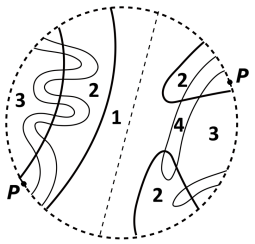


Рис. 8

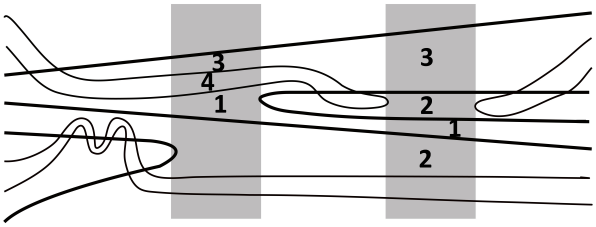


Рис. 9

Изобразим рис. 8 в виде "развертки" (у С.Ю. Оревкова – термин "послойное расположение"), изображенной на рис. 9 (теперь точка P – "бесконечно удаленная на вертикальной оси OY").

В силу теоремы Безу шесть свободных овалов модели могут располагаться только в закрашенных на рис. 9 вертикальных полосах, причем при движении прямой пучка (вертикальной прямой на рис. 9) эти овалы пересекаются поочередно. Числа в этих полосах соответствуют номерам областей на рис. 7. В левой полосе могут быть только овалы кривой номер 2, в правой – только овалы кривой номер 1.

Следуя С.Ю. Оревкову, развертки будем кодировать с помощью так называемого X-кода, который получается последовательным выписыванием символов $\subset_k$, $\supset_k$, x_k, $k \in \{1, 2, \ldots, 7\}$, при движении вертикальной прямой слева направо; эти символы кодируют расположения кривой в окрестности критических прямых пучка (тех прямых, которые касаются кривой или проходят через двойную точку кривой) в соответствии с рис. 10. Символ o_k заменяет пару символов $\subset_k \supset_k$ и отвечает расположению свободного овала в полосе над $(k-1)$-й линией ("в k-м слое"), считая снизу.

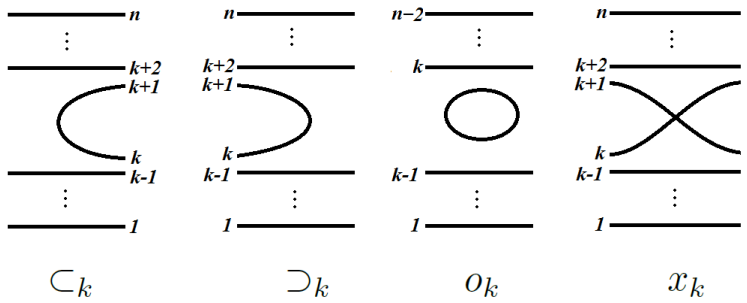


Рис. 10

В частности, развертка рис. 9 описывается X-кодом

$$x_6x_7x_3x_2x_2x_3x_3x_2x_2x_3x_1x_2 \supset_3 \ldots \subset_4 x_5x_6 \supset_5 \ldots \subset_5 x_6x_5, \tag{1}$$

где вместо многоточий должны располагаться символы, показывающие расположение свободных овалов в закрашенных полосах и порядок их прохождения при движении вертикальной прямой слева направо.

В методе Оревкова каждой развертке ставится в соответствие зацепление и коса из восьми нитей, замыканием которой является это зацепление. Известно, что если все косы из n нитей, отвечающие всем возможным разверткам при данном выборе центра пучка, не являются квазиположительными[3], то эта модель не может быть реализована как множество вещественных точек кривой степени n. В качестве проверки на квазиположительность, следуя С.Ю. Оревкову, будет использоваться следующая

Теорема 4 (неравенство Мурасуги). *Если $b = \prod \sigma_i^{k_i}$ – квазиположительная коса из m нитей, то для ее замыкания выполняется неравенство*

$$\eta = |\sigma(b)| + m - e(b) - n(b) \leqslant 0,$$

где $\sigma(b)$ и $n(b)$ – сигнатура и дефект замыкания косы b; $e(b) = \sum k_i$ – алгебраическая степень косы b.

В данной работе удается так выбирать центр пучка прямых, что для каждой модели расположения пересекающихся овалов развертка строится однозначно с точностью до эквивалентностей фрагментов, указанных в [6, с. 795]. Однако проверка выполнения неравенства Мурасуги даже для одной модели расположения пересекающихся овалов требует выполнения вычислений, которые нельзя провести вручную из-за большого числа вариантов расположений свободных овалов и необходимости вычисления для каждого из этих вариантов собственных чисел достаточно больших матриц.

[3]Коса в группе кос из n нитей с образующими $\sigma_1, \ldots, \sigma_{n-1}$ называется квазиположительной, если ее можно записать в виде $\prod_{j=1}^{k} \omega_j \sigma_{i_j} \omega_j^{-1}$, где ω_j, $j \in \{1, 2, \ldots, k\}$, – некоторые слова в алфавите $\{\sigma_1, \ldots, \sigma_{n-1}, \sigma_1^{-1}, \ldots, \sigma_{n-1}^{-1}\}$.

Для вычислений мы пользовались программой, написанной для задач такого типа И.М. Борисовым. Эта программа для заданных на входе X-кода вида (1), номеров горизонтальных полос в закрашенных вертикальных зонах, в которых могут располагаться свободные овалы, и количеств свободных овалов в каждой закрашенной зоне, перебирает все возможные распределения свободных овалов в этих зонах во всевозможных порядках. Затем, подставляя поочередно в код вида (1) вместо многоточий слова вида $o_{i_1}o_{i_2}\dots o_{i_k}$, где k – количество овалов в данной закрашенной зоне, полученные в результате описанного выше перебора, для каждого полученного X-кода (уже без многоточий) вычисляет левую часть неравенства Мурасуги. На выходе программа дает список X-кодов, для которых неравенство Мурасуги выполняется, приведенный в таблице 1.

Центр P пучка всегда выбирался вне свободных овалов. Положение точки P указано после подстановки во втором столбце таблицы 1, где буквой A обозначен выбор центра пучка внутри змеи и вне несвободного овала кривой номер 2, а буквой B – вне змеи и внутри несвободного овала кривой номер 2. При этом запись As обозначает, что точка P выбиралась внутри двуугольной компоненты связности дополнения к пересекающимся овалам, на границе которой лежит точка с номером s, а запись Ast – что точка P лежит в четырехугольной компоненте связности этого дополнения, на границах которой лежат точки с номерами s и t. Запись вида Bpq означает, что центр P выбирался внутри несвободного обвала кривой 2 в области, в границу которой входит часть дуги (p, q) этого овала, не содержащая других занумерованных точек.

Таблица 1

Подстановка	X-код
$(12345678)[+++-]B67$	$x_6x_7x_3x_2x_2x_3x_3x_2x_2x_3x_1x_2 \supset_3 o_4o_6o_6 \subset_4 x_5x_6 \supset_5 o_5o_5o_5 \subset_5 x_6x_5$
$(12345678)[++-+]B45$	$x_5x_6 \supset_5 o_5o_5o_5 \subset_5 x_2x_1x_6x_5x_5x_6x_6x_5x_5x_6 \supset_7 o_2o_2o_4 \subset_4 x_3x_2x_2x_3$
$(12345876)[+++-]B78$	$x_5x_4 \supset_5 o_5o_5o_5 \subset_5 x_6x_7x_5x_6 \supset_5 o_2o_2o_4 \subset_2 x_3x_4x_4x_3x_3x_4x_4x_3x_6x_7$
$(12345876)[++--]A12$	$x_4x_3x_3x_4 \supset_3 o_3o_3o_3 \subset_7 x_5x_6x_6x_5x_5x_6x_6x_5 \supset_4 o_4o_4o_6 \subset_4 x_5x_6x_1x_1$
$(12347658)[++--]B45$	$x_4x_3x_3x_4x_2x_1x_3x_2x_6x_7 \supset_3 o_4o_6o_6 \subset_4 x_5x_6 \supset_5 o_5o_5o_5 \subset_5 x_4x_5x_5x_4$
$(12365478)[+--+]B23$	$x_3x_2x_4x_3x_3x_2 \supset_3 o_3o_3o_3 \subset_3 x_2x_3x_3x_2x_6x_7 \supset_1 o_4o_4o_6 \subset_4 x_5x_4x_6x_5$
$(12367854)[+-+-]A12$	$x_7x_6x_3x_4x_2x_3x_3x_4 \supset_3 o_3o_3o_3 \subset_5 x_6x_7 \supset_6 o_6o_6o_6 \subset_6 x_5x_6x_4x_5x_1x_1$

4. Построения кривых

Как и в работах [3, 4], построения производились путем возмущения квадрата коники в расположениях коники и M-кривой степени 4, пересекающихся в восьми точках на одном овале кривой степени 4. Полная классификация таких расположений получена в [1], она состоит из пятнадцати типов, фрагмент классификации приведен на рис. 11. На рис. 12 в качестве примера показано построение расположений D, E, F рис. 13 из исходного расположения номер 6 на рис. 11.

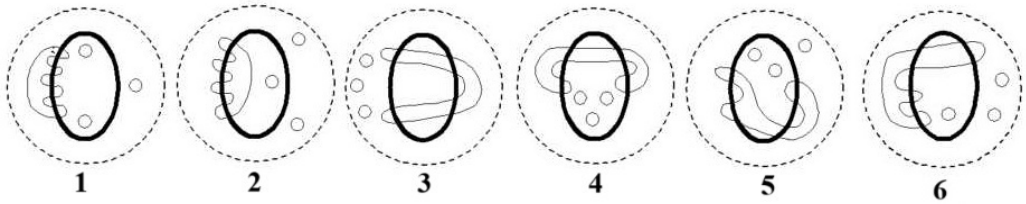


Рис. 11

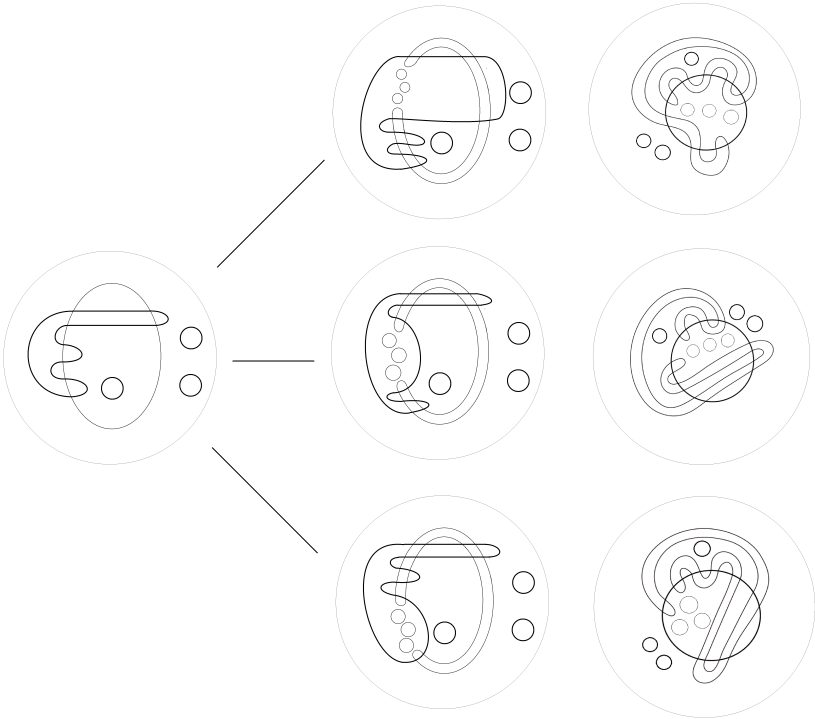


Рис. 12

5. Основной результат

Из изложенных выше запретов и построений непосредственно вытекает следующая

Теорема 5. *Для двух M-кривых степени* 4 *алгебраически реализуемы те и только те семь расположений типа "змея с концом внутри овала", принадлежащих выделенному подклассу, которые указаны на рис.* 13.

Расположения A и G рис. 13 реализуются путем возмущения квадрата коники из расположения номер 1 на рис. 11, расположения B и C – из расположений номер 4 и 5 соответственно.

Заметим, что в данном случае, как и в случае, рассмотренном в статье [4], реализуются те и только те расположения, которые можно получить из расположений коники и кривой степени 4 с помощью возмущения квадрата коники.

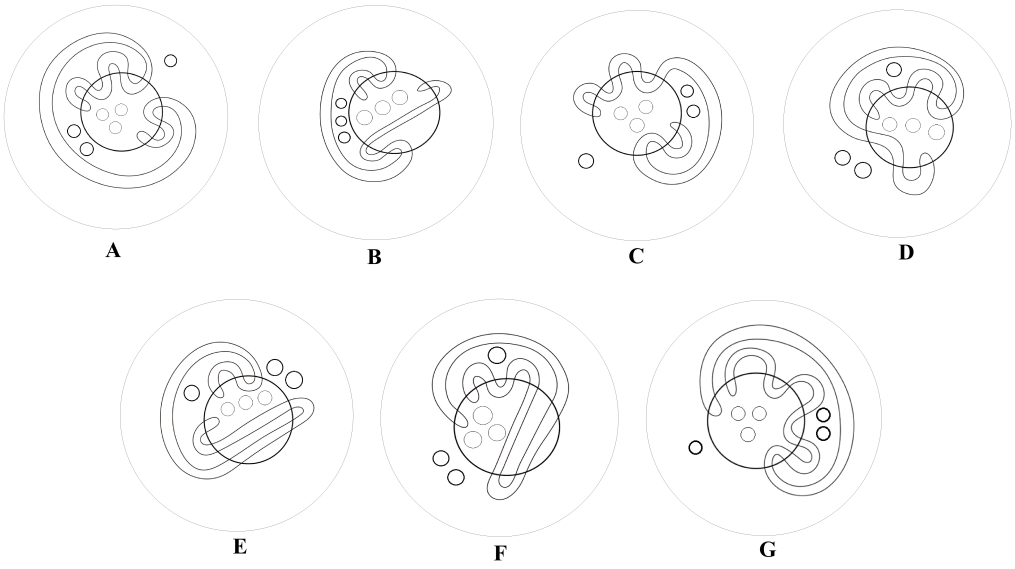


Рис. 13

Список литературы

[1] Г.М. Полотовский, *Полная классификация M-распадающихся кривых* 6*-го порядка в вещественной проективной плоскости*, Деп. в ВИНИТИ. № 1349–78, М., 1978.

[2] И.М. Борисов, Г.М. Полотовский, *О топологии плоских вещественных распадающихся кривых степени* 8, Итоги науки и техн. Сер. Соврем. мат. и ее прил. Темат. обз. **176**, 3–18 (2020).
DOI: https://doi.org/10.36535/0233-6723-2020-176-3-18

[3] Н.Д. Пучкова, *О взаимных расположениях двух M-кривых степени* 4, Итоги науки и техн. Соврем. мат. и ее прил. Темат. обз. **222**, 69–82 (2023).
DOI: https://doi.org/10.36535/0233-6723-2023-222-69-82

[4] Н.Д. Пучкова, *О расположениях двух M-кривых степени* 4*, овал одной из которых обвивается вокруг овала другой*, Чебышевский сб. **24** (3), 56–70 (2023).
DOI: https://doi.org/10.22405/2226-8383-2023-24-3-56-70

[5] Д.А. Гудков, *Топология вещественных проективных алгебраических многообразий*, УМН **29** (4), 3–79 (1974).
URL: https://www.mathnet.ru/rus/rm7210

[6] S.Yu. Orevkov, *Link theory and oval arrangements of real algebraic curves*, Topology **38** (4), 779–810 (1999).
DOI: https://doi.org/10.1016/S0040-9383(98)00021-4

[7] В.А. Горская, Г.М. Полотовский, *О расположениях кубики и пары коник в вещественной проективной плоскости*, Журнал СВМО **22** (1), 24–37 (2020).
DOI: https://doi.org/10.15507/2079-6900.22.202001.24-37

Наталья Дмитриевна Пучкова
Национальный исследовательский университет «Высшая школа экономики» в г. Нижний Новгород,
ул. Большая Печерская д. 25/12, г. Нижний Новгород, 603155, Россия,
e-mail: nataha1910@mail.ru

Volume 4, Issue 2
pp. 134–146 (2026)

UDC 510.54, 510.57
MSC 03D45, 03D30

On a class of dispositions of two M-curves of degree 4

N.D. Puchkova

Abstract. We consider the isotopic classification problem of arrangements in the real projective plane of two M-curves of degree 4. We study the arrangements that satisfy the maximality condition (an oval of the first curve has 16 pairwise different common points with an oval of the second one) and some combinatorial condition distinguishing a special type. We have obtained a complete classification of algebraic curves of the class under consideration. The proofs of algebraic non-realizability for the arrangements of the studied class of curves of degree 8 use Orevkov's method based on braids and links theory.

Keywords: plane real algebraic curves, decomposable curves, quasi-positive braids, Orevkov's method, Murasugi inequality.

DOI: 10.26907/2949-3919.2026.2.134-146

References

[1] G.M. Polotovskiy, *Complete classification of M-decomposional curves of degree* 6 *in the real projective plane*, Dep. in VINITI, no. 1349-78, 1978.

[2] I.M. Borisov, G.M. Polotovskiy, *On the topology of plane real decomposable curves of degree* 8, J. Math. Sci. **275** (5), 525–540 (2023).
DOI: https://doi.org/10.1007/s10958-023-06694-6

[3] N.D. Puchkova, On mutual arrangements of two M-curves of degree 4, Itogi Nauki i Tekhniki. Sovrem. Mat. Pril. Temat. Obz. **222**, 69–82 (2023) [in Russian].
DOI: https://doi.org/10.36535/0233-6723-2023-222-69-82

[4] N.D. Puchkova, *On arrangements of two M-curves of degree* 4 *with an oval of the first curve coiling around an oval of the second one*, Chebyshevskii Sb. **24** (3), 56–70 (2023).
DOI: https://doi.org/10.22405/2226-8383-2023-24-3-56-70

[5] D.A.Gudkov, *The topology of real projective algebraic varieties*, Russian Math. Surveys **29** (4), 1–79 (1974).
DOI: https://doi.org/10.1070/RM1974v029n04ABEH001288

Acknowledgements. This article is an output of a research project implemented as part of the Basic Research Program at the National Research University Higher School of Economics (HSE University).

Received: 30 September 2024. Accepted: 14 October 2025. Published: 07 July 2026.

[6] S.Yu. Orevkov, *Link theory and oval arrangements of real algebraic curves*, Topology **38** (4), 779–810 (1999).
DOI: https://doi.org/10.1016/S0040-9383(98)00021-4

[7] V.A. Gorskaya, G.M. Polotovskiy, *On the disposition of cubic and pair of conics in a real projective plane*, Zhurnal SVMO **22** (1), 24–37 (2020) [in Russian].
DOI: https://doi.org/10.15507/2079-6900.22.202001.24-37

Natalya Dmitrievna Puchkova
National Research University «Higher School of Economics» (Nizhny Novgorod),
25/12 B. Pecherskaya str., Nizhny Novgorod 603155, Russia,
e-mail: nataha1910@mail.ru

Календарь конференций (август 2026 г. – октябрь 2026 г.)

Август 2026 г.

- **Аналитические методы небесной механики**
  Международный математический институт им. Л. Эйлера, Песочная набережная, 10, г. Санкт-Петербург, Россия, 17–21 августа 2026 г.
  Сайт: **https://amcm.conf-pdmi.ru/2026**
  Срок регистрации – **до 22 июля 2026 г.**

- **VI Конференция математических центров России**
  Казанский (Приволжский) федеральный университет, г. Казань, Россия, 17–22 августа 2026 г.
  Сайт: **https://mathcenter.kpfu.ru/mc-conf**
  Регистрация завершена.

- **Международная научная конференция "Современные методы и проблемы теории операторов и гармонического анализа и их приложения – XVI (OTHA-2026)"**
  г. Ростов-на-Дону, Россия, 23–28 августа 2026 г.
  Сайт: **https://otha.sfedu.ru/conf2026**
  Срок регистрации – **до 31 июля 2026 г.**

- **Международная конференция "Novikov-125", посвящённая 125-летию со дня рождения П.С. Новикова**
  МИАН, ул. Губкина, д. 8, г. Москва, Россия, 24–28 августа 2026 г.
  Сайт: **https://www.mathnet.ru/rus/conf2717**

- **Russia-Vietnam Conference on Algebraic Geometry, Algebraic Groups, Commutative Algebra, and Applications**
  Leonhard Euler International Mathematical Institute, Saint Petersburg, Россия, 24–28 августа 2026 г.
  Сайт: **https://indico.eimi.ru/event/2065**
  Срок регистрации – **до 31 июля 2026 г.**

- **Вторая всероссийская конференция "Теоретическая и прикладная математика, включая аттестацию кадров высшей квалификации"**
  Республика Бурятия, с. Гремячинск, Россия, 24–29 августа 2026 г.
  Сайт: **https://conf.ict.nsc.ru/tam2026/ru/general_info**

- **Молодёжный коллоквиум по математической логике и её приложениям**
  МИАН, ул. Губкина, д. 8, г. Москва, Россия, 31 августа–4 сентября 2026 г.
  Сайт: **https://www.mathnet.ru/rus/conf2744**
  Срок регистрации – **до 01 августа 2026 г.**

Сентябрь 2026 г.

- **Первая конференция и мастер-класс по математике и искусственному интеллекту**
  Назарбаев Университет, г. Астана, Казахстан, 9–11 сентября 2026 г.
  Сайт: **https://issai.nu.edu.kz/math-ai-conference**
  Срок регистрации – **до 15 августа 2026 г.**

- **Вавиловские чтения 2026**
  Международный математический институт им. Л. Эйлера, Песочная набережная, 10, г. Санкт-Петербург, Россия, 17–19 сентября 2026 г.
  Сайт: **https://vavilov-memorial.conf-pdmi.ru/2026**

- **8-я Международная конференция по анализу и прикладной математике (ICAAM 2026)**
  Отель "Мирамор", Анталья, Кемер, Кириш, Турция, 26 сентября–3 октября 2026 г.
  Сайт: **https://icaam-online.org/index.html**

- **Конференция "Квантовая оптика и смежные вопросы 2026"**
  Онлайн, Россия, 26 сентября–4 октября 2026 г.
  Сайт: **https://sites.google.com/view/qoart/2026**

- **V Конференция с международным участием "Вычислительные технологии и прикладная математика"**
  г. Петропавловск-Камчатский, Россия, 28 сентября–2 октября 2026 г.
  Сайт: **https://kamchatgtu.ru/42150-2**
  Регистрация завершена.

- **Нелинейные волны: гиперболические и дисперсионные модели гидродинамики**
  Международный математический центр Сириус, Россия, 28 сентября–2 октября 2026 г.
  Сайт: **https://siriusmathcenter.ru/076w**
  Срок регистрации – **до 28 августа 2026 г.**

- **Уфимская осенняя математическая школа**
  Уфимский университет науки и технологий, г. Уфа, Россия, 29 сентября–2 октября 2026 г.
  Сайт: **https://conf-bashedu-fmit.ru**
  Срок регистрации – **до 10 сентября 2026 г.**

Октябрь 2026 г.

- **Международная конференция "Интегрируемые системы и квантовая теория", посвященная 80-летию А.К. Погребкова**
  Москва, МИАН, Санкт-Петербург, СПбГУ, Россия, 1–8 октября 2026 г.
  Сайт: **https://www.mathnet.ru/rus/conf2728**

- **Международная конференция "Новые горизонты математической физики", посвященная 80-летию И.В. Воловича**
  Математический институт им. В.А. Стеклова РАН, г. Москва, Россия, 5–9 октября 2026 г.
  Сайт: **https://www.mathnet.ru/rus/conf2723**
  Срок регистрации – **до 05 сентября 2026 г.**

- **Международная конференция "Перспективные направления в квантовой теории поля и суперструнах", посвященная 80-летию И.Я. Арефьевой**
  Математический институт им. В.А. Стеклова РАН, г. Москва, Россия, 12–17 октября 2026 г.
  Сайт: **https://www.mathnet.ru/rus/conf2727**
  Срок регистрации – **до 07 сентября 2026 г.**

- **Конференция, посвященная 75-летию со дня рождения А.А. Суслина**
  Санкт-Петербургское отделение Математического института им. В.А. Стеклова РАН, г. Санкт-Петербург, Россия, 19–20 октября 2026 г.
  Сайт: **https://indico.eimi.ru/e/Suslin_75th_2026**

- **Международная конференция по комплексному анализу памяти А.А. Гончара и А.Г. Витушкина**
  МИАН, конференц-зал 9 этаж, г. Москва, Россия, 19–21 октября 2026 г.
  Сайт: **https://www.mathnet.ru/rus/conf2773**

- **Международная конференция "Алгебраическая топология и действия групп"**
  МИАН, конференц-зал на 9 этаже, г. Москва, Россия, 19–23 октября 2026 г.
  Сайт: **https://www.mathnet.ru/rus/conf2770**