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:

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

□

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

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

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

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

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

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 $\left(\frac{m}{\mathbb{Z}_{2^k}}\right)_{\mathrm{DH}} = \mathrm{sgn}(\pi_m)$ и $\left(\frac{m}{\mathbb{Z}_t}\right)_{\mathrm{DH}} = \mathrm{sgn}(\sigma_m)$. Согласно лемме 1 b), знак перестановки φ_m, действующей на прямом произведении $\mathbb{Z}_{2^k} \times \mathbb{Z}_t$, равен:

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

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

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

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:

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

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 $\left(\frac{a}{b_1}\right) = \left(\frac{a}{\mathbb{Z}_{b_1}}\right)_{\mathrm{DH}}$, получим:

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

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 $\boldsymbol{\chi}$:

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

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

$$V\boldsymbol{e}_0 = \begin{pmatrix}1, & 1, & 1, & \ldots, & 1\end{pmatrix}^T = \boldsymbol{e}_0 + \boldsymbol{\chi}_0.$$

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

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

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 $S = \{x_1, \dots, x_k\}$. Зафиксируем некоторый линейный порядок $<$ на элементах множества G^*, при котором $x_1 < \dots < x_k < -x_k < \dots < -x_1$. 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*

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

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 $\left(\frac{\det A}{n}\right)$ *– 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

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

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 $\operatorname{res}(f, g)$ многочленов f и g имеет место равенство

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

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,

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

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

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

□

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:

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

□

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