Том 3, Выпуск 1
Стр. 4–11 (2025)

УДК 512.55
MSC 18G05

Квадратичный закон взаимности по Золотареву и его обобщение

А.Н. Абызов

Аннотация. В работе Дьюка и Хопкинса (2005), следуя подходу Е.И. Золотарева, получен аналог квадратичного закона взаимности для групп с использованием символа Кронекера. В нашей заметке предложено короткое доказательство этого утверждения с использованием символа Якоби. Работа в основном носит методический характер. В связи с этим в ней также приведено доказательство результата установленного в работе Фробениуса (1914), связанного с комбинаторной интерпретацией символа Якоби.

Ключевые слова: символ Якоби, квадратичный закон взаимности, характеры, конечные поля.

DOI: 10.26907/2949-3919.2025.1.4-11

В 1872 году в [4] Е.И. Золотаревым было найдено новое доказательство квадратичного закона взаимности на основе обнаруженной им новой интерпретации символа Лежандра, согласно которой для произвольного простого числа p и целого числа a, взаимно простого с p, значение символа Лежандра $\left(\frac{a}{p}\right)$ совпадает со знаком перестановки, действующей на $\mathbb{Z}/(p)$ согласно правилу $x \mapsto ax$. В работах [2,3] была получена аналогичная интерпретация символа Якоби. Короткое доказательство квадратичного закона взаимности для символа Якоби на основе его комбинаторной интерпретации найдено в работе [5]. Изложение такого подхода к доказательству квадратичного закона взаимности для символа Якоби на русском языке приведено в статье [6]. В недавней работе [7] на основе подхода Золотарева был получен аналог квадратичного закона взаимности для дедекиндовых колец, у которых факторы по максимальным идеалам конечны.

Пусть G – конечная группа порядка n. Далее будем придерживаться следующих обозначений. Через $C_1, \dots, C_k$ обозначим все классы сопряженности группы G, количество элементов в этих классах обозначим, соответственно, через $d_1, \dots, d_k$. Если $a \in \mathbb{Z}$ и $(a, n) = 1$, то биективное отображение группы G в себя, действующее по правилу $g \mapsto g^a$, индуцирует перестановку классов сопряженности группы G, которую обозначим π_a. Следуя [1], определим значение квадратичного символа для G в произвольном целом числе a

Поступила: 11.02.2025. Принята: 31.03.2025. Опубликована: 24.04.2025.

согласно правилу

$$\left(\frac{a}{G}\right) = \begin{cases} 0, & \text{если } (a,n) \neq 1, \\ 1, & \text{если перестановка } \pi_a \text{ четна}, \\ -1, & \text{если перестановка } \pi_a \text{ нечетна}. \end{cases}$$

Количество классов сопряженности группы G, для которых выполнено равенство $C_i^{-1} = C_i$, обозначим через r_1. Тогда для некоторых натуральных чисел r_2 и t имеют место равенства $k = r_1 + 2r_2$, $d_1 \cdots d_k = d_1 \cdots d_{r_1} t^2$. Через d_G будем обозначать число $(-1)^{r_2}(d_1 \cdots d_{r_1})^{-1} n^{r_1}$. Если n нечетно, то несложно показать, что $r_1 = 1$ и, следовательно, $d_G = (-1)^{\frac{n-1}{2}} n$. В [1] для произвольного целого числа a и конечной группы G доказано равенство

$$\left(\frac{a}{G}\right) = \left(\frac{d_G}{a}\right), \tag{1}$$

где $\left(\frac{\cdot}{a}\right)$ – символ Кронекера. В [1] равенство (1) доказывается с использованием теории характеров и элементов теории алгебраических чисел. В нашей заметке мы приведем короткое доказательство, того же характера, этого равенства в случае, когда в нем используется символ Якоби, но с использованием теории конечных полей.

Теорема 1. *Пусть G – конечная группа порядка n, a – нечетное натуральное число большее единицы и $(n,a) = 1$. Тогда*

$$\left(\frac{a}{G}\right) = \left(\frac{d_G}{a}\right).$$

Доказательство. Будем придерживаться введенных выше обозначений. Ясно, что достаточно показать, что для произвольного нечетного простого числа p, взаимно простого с n, имеет место равенство $\left(\frac{p}{G}\right) = \left(\frac{d_G}{p}\right)$. Пусть $\overline{\mathbb{F}}_p$ – алгебраическое замыкание поля $\mathbb{F}_p$. Далее все характеры группы G будут рассматриваться относительно представлений G над полем $\overline{\mathbb{F}}_p$. Пусть $\chi_1, \ldots, \chi_k$ – все неприводимые характеры G. Положим

$$A = \begin{pmatrix} \chi_1(C_1) & \ldots & \chi_1(C_k) \\ \vdots & \ddots & \vdots \\ \chi_k(C_1) & \ldots & \chi_k(C_k) \end{pmatrix}.$$

Из соотношения ортогональности для характеров следует равенство

$$\begin{vmatrix} \chi_1(C_1) & \ldots & \chi_1(C_k) \\ \vdots & \ddots & \vdots \\ \chi_k(C_1) & \ldots & \chi_k(C_k) \end{vmatrix} \cdot \begin{vmatrix} d_1\chi_1(C_1^{-1}) & \ldots & d_1\chi_k(C_1^{-1}) \\ \vdots & \ddots & \vdots \\ d_k\chi_1(C_k^{-1}) & \ldots & d_k\chi_k(C_k^{-1}) \end{vmatrix} = \begin{vmatrix} n & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & n \end{vmatrix}.$$

Из определения символа $\left(\frac{-1}{G}\right)$ следует, что второй сомножитель в левой части предыду-

щего равенства равен $\left(\frac{-1}{G}\right) d_1 \cdots d_k \, |A|$. Тогда

$$\left(\frac{-1}{G}\right) d_1 \cdots d_k \, |A|^2 = n^k,$$

$$(|A| \, tn^{-r_2})^2 = \left(\frac{-1}{G}\right) (d_1 \cdots d_{r_1})^{-1} n^{r_1} = (-1)^{r_2} (d_1 \cdots d_{r_1})^{-1} n^{r_1} = d_G. \tag{2}$$

Следовательно, имеет место эквивалентность

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

Непосредственно проверяется, что для произвольного $g \in G$ и характера χ группы G имеет место равенство $\chi(g)^p = \chi(g^p)$. Тогда

$$|A|^p = \begin{vmatrix} \chi_1(C_1^p) & \cdots & \chi_1(C_k^p) \\ \vdots & \ddots & \vdots \\ \chi_k(C_1^p) & \cdots & \chi_k(C_k^p) \end{vmatrix} = \left(\frac{p}{G}\right) |A|. \tag{3}$$

Таким образом, имеют место эквивалентности

$$|A| \in \mathbb{F}_p \Leftrightarrow |A| = |A|^p \Leftrightarrow \left(\frac{p}{G}\right) = 1 \tag{4}$$

и, следовательно, $\left(\frac{p}{G}\right) = \left(\frac{d_G}{p}\right)$. □

Если в предыдущей теореме в качестве G взять группу $\mathbb{Z}_n$, то учитывая комбинаторную интерпретацию символа Якоби, рассмотренную в работах [2, 3], непосредственно получаем закон взаимности для символа Якоби.

Ради полноты изложения приведем доказательство, упомянутого выше результата из работ [2,3]. Пусть G – группа и X – G-множество, где X – конечное множество. Представление группы G перестановками множества X, соответствующее G-множеству X, будем обозначать через $\pi_X : G \to \mathrm{Sym}(X)$, где $\mathrm{Sym}(X)$ – 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 π'_X. Следующее утверждение проверяется непосредственно.

Лемма 2.

1) *Если конечное G-множество X является дизъюнктным объединением своих G-подмножеств $X_1, \ldots, X_k$, то $\pi'_X(g) = \pi'_{X_1}(g) \cdots \pi'_{X_k}(g)$ для каждого $g \in G$.*
2) *Если $X_1, \ldots, X_k$ – конечные G-множества, $| X_1 | = n_1, \ldots, | X_k | = n_k$ и $n = n_1 \cdots n_k$, то $\pi'_{X_1 \times \cdots \times X_k}(g) = \pi'_{X_1}(g)^{\frac{n}{n_1}} \cdots \pi'_{X_k}(g)^{\frac{n}{n_k}}$ для каждого $g \in G$. В частности, если все натуральные числа $n_1, \ldots, n_k$ нечетны, то $\pi'_{X_1 \times \cdots \times X_k}(g) = \pi'_{X_1}(g) \cdots \pi'_{X_k}(g)$ для каждого $g \in G$.*

Через ε_G будем обозначать представление Кэли группы G, т. е. гомоморфизм $G \to \mathrm{Sym}(G)$, действующий по правилу $g \mapsto (a \mapsto ga)$. Для произвольного целого нечетного числа $n > 1$ и целого числа m, взаимно простого с n, через $\left[\frac{m}{n}\right]$ обозначим знак перестановки множества $\mathbb{Z}/(n)$, действующей по правилу $a + (n) \mapsto ma + (n)$. Доказательство следующего утверждения основано на идеях из работы [7].

Теорема 3 ([2, 3])**.** *Для произвольного целого нечетного числа $n > 1$ и целого числа m, взаимно простого с n, имеет место равенство*

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

Доказательство. Предположим, что $n = p^a$, где p – простое нечетное число. Положим $G = U(\mathbb{Z}/(p^a))$. Для каждого натурального числа $k \leq a$ кольцо вычетов $\mathbb{Z}/(p^k)$ имеет естественную структуру $\mathbb{Z}/(p^a)$-модуля. Этот модуль индуцирует на $\mathbb{Z}/(p^k)$ структуру G-множества, которое, как не сложно заметить, является дизъюнктным объединением своих G-подмножеств $U(\mathbb{Z}/(p^k))$ и $p\mathbb{Z}/(p^k)$. Так как $\mathbb{Z}/(p^a)$-модули $p\mathbb{Z}/(p^k)$ и $\mathbb{Z}/(p^{k-1})$ изоморфны, то они изоморфны как G-множества и, следовательно, имеет место изоморфизм G-множеств $\mathbb{Z}/(p^k) \cong U(\mathbb{Z}/(p^k)) \sqcup \mathbb{Z}/(p^{k-1})$. Тогда с помощью индукции получаем изоморфизм G-множеств $\mathbb{Z}/(p^a) \cong U(\mathbb{Z}/(p)) \sqcup \cdots \sqcup U(\mathbb{Z}/(p^a)$. Для каждого натурального числа $k \leq a$ образ $\varepsilon_{U(\mathbb{Z}/(p^k))}(g)$ порождающего элемента g циклической группы $U(\mathbb{Z}/(p^k))$ является циклом четной длины $p^k - p^{k-1}$. Следовательно, гомоморфизм $\pi'_{U(\mathbb{Z}/(p^k))} : G \to \{\pm 1\}$ является неединичным. Заметим, что символ Лежандра $\left(\frac{\cdot}{p}\right)$, также индуцирует неединичный гомоморфизм из G в $\{\pm 1\}$, действующий согласно правилу $x + (p^a) \mapsto \left(\frac{x}{p}\right)$, который будем обозначать также через $\left(\frac{\cdot}{p}\right)$. Так как группа G является циклической четного порядка $p^a - p^{a-1}$, то в ней существует единственная подгруппа индекса два и, следовательно, существует единственный неединичный гомоморфизм, действующий из G в $\{\pm 1\}$. Таким образом, имеют место равенства

$$\left(\frac{\cdot}{p}\right) = \pi'_{U(\mathbb{Z}/(p^a))} = \ldots = \pi'_{U(\mathbb{Z}/(p))}.$$

Тогда согласно п. 1) леммы 2 для каждого целого числа m, взаимно простого с p, имеют место равенства

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

Рассмотрим общий случай. Пусть $n = p_1^{a_1} \cdots p_k^{a_k}$, где $p_1, \ldots, p_k$ – различные простые нечетные числа, и $G = U(\mathbb{Z}/(n))$. Согласно китайской теореме об остатках диагональный кольцевой гомоморфизм из $\mathbb{Z}$ в $\mathbb{Z}/(p^{a_1}) \times \cdots \times \mathbb{Z}/(p^{a_k})$, действующий по правилу

$a \to (a+(p^{a_1}), \dots, a+(p^{a_k}))$, индуцирует изоморфизм $\mathbb{Z}/(n)$-модулей

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(p^{a_1}) \times \ldots \times \mathbb{Z}/(p^{a_k}),$$

который также является изоморфизмом G-множеств. Тогда согласно п. 2) леммы 2 для каждого целого числа m, взаимно простого с n, имеют место равенства

$$\left[\frac{m}{n}\right] = \pi'_{\mathbb{Z}/(n)}(m+(n)) = \pi'_{\mathbb{Z}/(p^{a_1})}(m+(n)) \cdots \pi'_{\mathbb{Z}/(p^{a_k})}(m+(n)) = \left(\frac{m}{p^{a_1}}\right) \cdots \left(\frac{m}{p^{a_k}}\right) = \left(\frac{m}{n}\right).$$

□

Замечание 4. Теорему 3 также можно вывести из теоремы 1, используя стандартные свойства символа Якоби.

Заметим, что приведенный выше подход к доказательству квадратичного закона взаимности для групп дает короткое доказательство классического квадратичного закона взаимности, в котором используются только базовые факты из теории конечных полей. Пусть p, q – различные простые нечетные числа и $\varepsilon \in \overline{\mathbb{F}}_p$ – примитивный корень степени q из единицы. Положим

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

Так как

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & \varepsilon & \dots & \varepsilon^{q-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \varepsilon^{q-1} & \dots & (\varepsilon^{q-1})^{q-1} \end{vmatrix} \cdot \begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & \varepsilon^{-1} & \dots & \varepsilon^{-(q-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \varepsilon^{-(q-1)} & \dots & (\varepsilon^{q-1})^{-(q-1)} \end{vmatrix} = \begin{vmatrix} q & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & q \end{vmatrix},$$

то равенства (2) принимают вид

$$\left(|A|\, q^{-\frac{q-1}{2}}\right)^2 = (-1)^{\frac{q-1}{2}} q.$$

Тогда согласно (3) и (4) имеют место эквивалентности $|A| \in \mathbb{F}_p \Leftrightarrow \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) = 1$ и $|A| \in \mathbb{F}_p \Leftrightarrow |A| = |A|^p \Leftrightarrow \left(\frac{p}{q}\right) = 1$, т. е. имеет место равенство $\left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{q}{p}\right)$.

Список литературы

[1] 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

[2] G. Frobenius, *Über das quadratische Reciprocitätsgesetz*, in: Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin, 335–349 (1914).

[3] M. Lerch, Sur un théorème arithmétique de Zolotarev, Bulletin int. de l'Ac. Prague **3**, 34–37 (1896).

[4] G. Zolotareff, *Nouvelle démonstration de la loi de réciprocité de Legendre*, Nouv. Ann. Math. (2^e série) **11**, 354–362 (1872).

[5] G. Rousseau, *On the Jacobi symbol*, J. Number Theory **48** (1), 109–111 (1994).
DOI: https://doi.org/10.1006/jnth.1994.1057

[6] Е.А. Горин, *Перестановки и квадратичный закон взаимности по Золотареву–Фробениусу–Руссо*, Чебышевский сб. **14** (4), 80–94 (2013).
URL: https://www.mathnet.ru/rus/cheb305

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

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

Volume 3, Issue 1
pp. 4–11 (2025)

UDC 512.55
MSC 18G05

The Quadratic Reciprocity Law by Zolotarev and its generalizations

A.N. Abyzov

Abstract. In the paper of Duke and Hopkins (2005), following the approach of E.I. Zolotarev, an analogue of the quadratic reciprocity law for groups was obtained using the Kronecker symbol. We present a short proof of this statement using the Jacobi symbol. The work is mainly of a methodological nature. In this regard, we also provide a proof of the result established in the paper by Frobenius (1914), related to the combinatorial interpretation of the Jacobi symbol.

Keywords: Jacobi symbol, quadratic reciprocity law, characters, finite fields.

DOI: 10.26907/2949-3919.2025.1.4-11

References

[1] 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

[2] G. Frobenius, *Über das quadratische Reciprocitätsgesetz*, in: Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin, 335–349 (1914).

[3] M. Lerch, Sur un théorème arithmétique de Zolotarev, Bulletin int. de l'Ac. Prague **3**, 34–37 (1896).

[4] G. Zolotareff, *Nouvelle démonstration de la loi de réciprocité de Legendre*, Nouv. Ann. Math. (2^e série) **11**, 354–362 (1872).

[5] G. Rousseau, *On the Jacobi symbol*, J. Number Theory **48** (1), 109–111 (1994).
DOI: https://doi.org/10.1006/jnth.1994.1057

[6] E.A. Gorin, *Permutations and reciprocity law by Zolotarev–Frobenius–Russo*, Chebyshevskii sb. **14** (4), 80–94 (2013) [in Russian].
URL: https://www.mathnet.ru/rus/cheb305

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

Received: 11 February 2025. Accepted: 31 March 2025. Published: 24 April 2025.

Adel Nailevich Abyzov
Kazan Federal University,
18 Kremlyovskaya str., Kazan 420008, Russia,
e-mail: Adel.Abyzov@kpfu.ru