

МАТЕМАТИКА И ТЕОРЕТИЧЕСКИЕ КОМПЬЮТЕРНЫЕ НАУКИ

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

Том 3
Выпуск 1



Казань
2025

МАТЕМАТИКА И ТЕОРЕТИЧЕСКИЕ КОМПЬЮТЕРНЫЕ НАУКИ

Издается с 2023 года

Выходит 4 раза в год

ISSN 2949-3919

Том 3

Выпуск 1

Специальный выпуск трудов конференции
«Алгебра и математическая логика: теория и приложения»,
27 июня – 1 июля 2024 г., Казань, КФУ

Казань

2025

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

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

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

математики, теоретической информатики и компьютерных наук:

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

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

Главный редактор

Арсланов М.М. (Россия, г. Казань)

Заместители главного редактора

Бикчентаев А.М. (Россия, г. Казань)

Файзрахманов М.Х. (Россия, г. Казань)

Ответственный секретарь

Тапкин Д.Т. (Россия, г. Казань)

Редакционная коллегия

Аблаев Ф.М. (Россия, г. Казань)

Абызов А.Н. (Россия, г. Казань)

Авхадиев Ф.Г. (Россия, г. Казань)

Амосов Г.Г. (Россия, г. Москва)

Асташкин С.В. (Россия, г. Самара)

Баженов Н.А. (Россия, г. Новосибирск)

Герман О.Н. (Россия, г. Москва)

Данчев П.В. (Болгария, г. София)

Демиденко Г.В. (Россия, г. Новосибирск)

Ефремова Л.С. (Россия, г. Нижний Новгород)

Касымов Н.Х. (Узбекистан, г. Ташкент)

Каюмов И.Р. (Россия, г. Казань)

Морозов А.С. (Россия, г. Новосибирск)

Мусин И.Х. (Россия, г. Уфа)

Насыров С.Р. (Россия, г. Казань)

Попов А.А. (Россия, г. Казань)

Семенов А.Л. (Россия, г. Москва)

Туганбаев А.А. (Россия, г. Москва)

Турилова Е.А. (Россия, г. Казань)

Фоменко А.Т. (Россия, г. Москва)

Швидефски М.В. (Россия, г. Новосибирск)

СОДЕРЖАНИЕ

Абызов А.Н. Квадратичный закон взаимности по Золотареву и его обобщение	4
Веселова А.А., Щучкин Н.А. Преобразование слов с помощью тернарных (L, M)-квазигрупп	12
Звонилов В.И. Графы тригональных кривых и жесткие изотопии особых вещественных алгебраических кривых бистепени $(4, 3)$ на гиперboloиде	26
Монастырева А.С. Некоторые свойства сжатого графа делителей нуля	52
Шахова С.А. Классы Леви квазимногообразий 2-нильпотентных групп	64

МАТЕМАТИЧЕСКАЯ ЖИЗНЬ

V Конференция математических центров России	78
Теория функций, ее приложения и смежные вопросы	80
Календарь конференций (май 2025 г. – июль 2025 г.)	81

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

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

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

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 $\chi_1, \dots, \chi_k$ – все неприводимые характеры G . Положим

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

Из соотношения ортогональности для характеров следует равенство

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

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

$$\begin{aligned} \left(\frac{-1}{G}\right) d_1 \cdots d_k |A|^2 &= n^k, \\ (|A| t n^{-r_2})^2 &= \left(\frac{-1}{G}\right) (d_1 \cdots d_{r_1})^{-1} n^{r_1} = (-1)^{r_2} (d_1 \cdots d_{r_1})^{-1} n^{r_1} = d_G. \end{aligned} \quad (2)$$

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

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

Таким образом, имеют место эквивалентности

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

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 $\pi_X : G \rightarrow \text{Sym}(X)$, где $\text{Sym}(X)$ – 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 $X_1, \dots, X_k$, то $\pi'_X(g) = \pi'_{X_1}(g) \cdots \pi'_{X_k}(g)$ для каждого $g \in G$.
- 2) 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 $G \rightarrow \text{Sym}(G)$, 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 дизъюнктивным 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 $\mathbb{Z}/(p^a) \cong U(\mathbb{Z}/(p)) \sqcup \dots \sqcup U(\mathbb{Z}/(p^a))$. 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 $\pi'_{U(\mathbb{Z}/(p^k))} : G \rightarrow \{\pm 1\}$ 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

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

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

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

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

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

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

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

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

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

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 Reziprocitätsgesetz*, 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>

Adel Nailevich Abyzov

Kazan Federal University,

18 Kremlyovskaya str., Kazan 420008, Russia,

e-mail: Adel.Abyzov@kpfu.ru

Преобразование слов с помощью тернарных (L, M) -квазигрупп

А.А. Веселова, Н.А. Щучкин

Аннотация. Построен алгоритм преобразования слов с помощью набора конечных квазигрупп в количестве, равном числу символов алфавита. Приведены некоторые свойства тернарных (L, M) -квазигрупп, которые играют важную роль при анализе и проектировании криптографических схем на основе этих алгебр, такие как полиномиальная полнота, отсутствие нетривиальных конгруэнций.

Ключевые слова: квазигруппа, полиномиальная полнота, конгруэнция.

DOI: 10.26907/2949-3919.2025.1.12-25

Введение

В последнее время активно разрабатываются криптографические алгоритмы, основанные на неассоциативных и некоммутативных алгебраических структурах [1]. Одной из наиболее подходящих алгебраических структур для таких целей является конечная квазигруппа. Известно широкое применение квазигрупп в криптографии (см., например, [2]). В работе [3] отмечалось, что квазигруппы могут быть очень полезны для криптографических целей главным образом потому, что легко определить функции шифрования и расшифрования, используя операции квазигрупп, и существует огромное количество квазигрупповых операций над заданным конечным множеством. В этой работе авторами было указано преобразование слов с помощью квазигрупп. Обобщая это преобразование на тернарный случай, в работах [4] и [5] были указаны преобразования слов с помощью тернарных квазигрупп, причем во второй работе применялись тернарные квазигруппы порядка 4. Аналогичные преобразования с помощью тернарных (L, M) -квазигрупп будут приведены ниже.

Исследовательской проблемой является идентификация подходящих квазигрупп для криптографических целей. В работе [6] отмечалось, что с алгебраической точки зрения полиномиально полные квазигруппы подходят для криптографии. Выбор полиномиально полных квазигрупп обосновывается результатом о NP-полноте проблемы проверки разрешимости уравнений над этим классом [7]. Наряду с полиномиально полными квазигруппами в криптографии можно использовать и такого же вида тернарные квазигруппы и

(L, M) -квазигруппы. В работе [8] были исследованы алгебраические свойства тернарных квазигрупп, такие как полиномиальная полнота, отсутствие нетривиальных конгруэнций. Аналогичные исследования проведем ниже для тернарных (L, M) -квазигрупп. Эти свойства могут сыграть важную роль при анализе и проектировании криптографических схем на основе тернарных (L, M) -квазигрупп.

1. Предварительные сведения

Обобщением квазигрупп являются n -арные квазигруппы [9], при $n = 3$ их называют тернарными квазигруппами. Итак, множество Q с одной тернарной операцией f называют тернарной квазигруппой, если для любых элементов a, b, c из Q уравнения

$$f(x, b, c) = a, \quad f(a, y, c) = b, \quad f(a, b, z) = c, \quad (1)$$

разрешимы однозначно.

Наряду с квазигруппами изучаются различные группоиды, тесно связанные с квазигруппами (см., например, [10]). По аналогии с квазигруппами можно также изучать тернарные группоиды, тесно связанные с тернарными квазигруппами. Например, рассматривать различные тернарные группоиды, в которых разрешимы однозначно не все три уравнения из (1), а только два или одно.

Тернарный группоид $\langle Q, f \rangle$, в котором для любых элементов a, b, c из Q разрешимы однозначно первые два уравнения из (1), будем называть тернарной (L, M) -квазигруппой. На множестве Q имеются еще две тернарные операции u, v , заданные по правилам

$$u(a, b, c) = d \Leftrightarrow f(d, b, c) = a; \quad v(a, b, c) = d \Leftrightarrow f(a, d, c) = b.$$

Операции u, v и f связаны тождествами

$$u(f(x, y, z), y, z) = x = f(u(x, y, z), y, z), \quad (2)$$

$$v(x, f(x, y, z), z) = y = f(x, v(x, y, z), z). \quad (3)$$

Таким образом, на тернарную (L, M) -квазигруппу $\langle Q, f \rangle$ можно смотреть как на универсальную алгебру $\langle Q, f, u, v \rangle$ с набором тождеств (2), (3).

2. Конечные тернарные (L, M) -квазигруппы

Пусть множество Q конечно и $Q = \{1, 2, \dots, m\}$. Тогда каждой тернарной (L, M) -квазигруппе $\langle Q, f \rangle$ соответствует трехмерная матрица m -го порядка

$$B = (b_{ijk} \mid i, j, k = 1, 2, \dots, m)$$

([11, с. 5]), где $b_{ijk} = f(i, j, k)$, причем, в силу однозначной разрешимости уравнений (1), в строках направления 1 и 2 стоят разные элементы из Q . Верно и обратное, любая трехмерная матрица m -го порядка $B = (b_{ijk} \mid i, j, k = 1, 2, \dots, m)$, у которой в строках направления 1 и 2 стоят разные элементы из Q , определяет тернарную (L, M) -квазигруппу $\langle Q, f \rangle$, где $f(i, j, k) = b_{ijk}$. Таким образом, между тернарными (L, M) -квазигруппами и трехмерными матрицами указанного вида имеется взаимно однозначное соответствие.

Построение трехмерной матрицы B для тернарной (L, M) -квазигруппы $\langle Q, f \rangle$ является аналогом построения таблицы умножения для обычной квазигруппы $\langle Q, \circ \rangle$, эту таблицу называют латинским квадратом. Наилучшую оценку для числа $L(m)$ латинских квадратов порядка m дает формула

$$L(m) = \left((1 + \alpha_m) \frac{m}{e^2} \right)^{m^2},$$

где $\alpha_m \rightarrow 0$ при $m \rightarrow \infty$ (см., например, [12]).

Мы оцениваем число $L(m; 3)$ тернарных (L, M) -квазигрупп порядка m :

$$L(m; 3) = L(m)^m.$$

Для примера, число латинских квадратов порядка 3 равно $L(3) = 12$, а число тернарных (L, M) -квазигрупп порядка 3 равно $L(3; 3) = 12^3 = 1728$, число латинских квадратов порядка 4 равно $L(4) = 576$, а число тернарных (L, M) -квазигрупп порядка 4 равно $L(4; 3) = 576^4 = 110075314176$.

Эта оценка указывает на большое количество тернарных (L, M) -квазигрупп, построенных на конечном множестве. Поэтому имеются перспективы использования тернарных (L, M) -квазигрупп в криптографии.

Каждая трехмерная матрица B , построенная для тернарной (L, M) -квазигруппы $\langle Q, f \rangle$, где $Q = \{1, 2, \dots, m\}$, определяет набор из m латинских квадратов на множестве Q с умножением $i \circ_k j = f(i, j, k)$ ($k = 1, 2, \dots, m$). Таким образом, на трехмерную матрицу B можно смотреть как на упорядоченный набор латинских квадратов в количестве, равном числу элементов множества Q .

3. Преобразования слов

Для преобразования слов в заданном алфавите используют квазигруппы [3]. Мы обобщаем преобразования слов из этой статьи на тернарный случай, т. е. в работе [8] было указано преобразование слов с помощью тернарных квазигрупп, а здесь будем преобразовывать слова с помощью тернарных (L, M) -квазигрупп.

Пусть $\langle Q, f \rangle$ – конечная тернарная (L, M) -квазигруппа, где $Q = \{1, \dots, m\}$. Множество всех непустых слов в алфавите Q обозначим $Q^+ = \{x_1 \dots x_s \mid x_i \in Q, s \geq 1\}$. Для заданной пары элементов a, b из Q (в терминах работы [3] эти элементы назовем лидерами)

на множестве Q^+ определим отображение

$$F_{a,b}(x_1x_2 \dots x_s) = y_1y_2 \dots y_s,$$

где

$$\begin{cases} y_1 = f(x_1, a, b), \\ y_2 = f(x_2, y_1, a), \\ y_{i+1} = f(x_{i+1}, y_i, y_{i-1}), \quad i = 2, 3, \dots, s-1. \end{cases} \quad (4)$$

Теорема 1. *Отображение $F_{a,b}$, построенное по правилу (4), является биективным.*

Доказательство. Пусть $F_{a,b}(x_1x_2 \dots x_s) = F_{a,b}(x'_1x'_2 \dots x'_s)$. Тогда $f(x_1, a, b) = f(x'_1, a, b)$, откуда, в силу однозначной разрешимости первого уравнения из (1), имеем $x_1 = x'_1$. Далее, из первого равенства следует $f(x_2, y_1, a) = f(x'_2, y_1, a)$, откуда, по той же причине, имеем $x_2 = x'_2$. Наконец, из первого равенства следует $f(x_{i+1}, y_i, y_{i-1}) = f(x'_{i+1}, y_i, y_{i-1})$, откуда, по той же причине, имеем $x_{i+1} = x'_{i+1}$ для всех $i = 2, 3, \dots, s-1$. Инъективность отображения $F_{a,b}$ доказана. Пусть теперь $y_1y_2 \dots y_s \in Q^+$. В силу разрешимости первого уравнения из (1), найдутся $x_1, x_2, \dots, x_s \in Q$ такие, что $y_1 = f(x_1, a, b)$, $y_2 = f(x_2, y_1, a)$, $y_{i+1} = f(x_{i+1}, y_i, y_{i-1})$ для всех $i = 2, 3, \dots, s-1$. Тогда $F_{a,b}(x_1x_2 \dots x_s) = y_1y_2 \dots y_s$. $\square$

Для той же пары элементов a, b из Q на множестве Q^+ строим еще одно отображение

$$G_{a,b}(y_1y_2 \dots y_s) = x_1x_2 \dots x_s,$$

где

$$\begin{cases} x_1 = u(y_1, a, b), \\ x_2 = u(y_2, y_1, a), \\ x_{i+1} = u(y_{i+1}, y_i, y_{i-1}), \quad i = 2, 3, \dots, s-1. \end{cases} \quad (5)$$

Теорема 2. *Отображение $G_{a,b}$, построенное по правилу (5), является обратным для отображения $F_{a,b}$.*

Доказательство. Для выбранного слова $x_1x_2 \dots x_s$ из Q^+ имеем

$$G_{a,b}(F_{a,b}(x_1x_2 \dots x_s)) = G_{a,b}(y_1y_2 \dots y_s) = x'_1x'_2 \dots x'_s,$$

где

$$\begin{aligned} x'_1 &= u(y_1, a, b) = u(f(x_1, a, b), a, b), \\ x'_2 &= u(y_2, y_1, a) = u(f(x_2, y_1, a), y_1, a), \\ x'_{i+1} &= u(y_{i+1}, y_i, y_{i-1}) = u(f(x_{i+1}, y_i, y_{i-1}), y_i, y_{i-1}), \quad i = 2, 3, \dots, s-1. \end{aligned}$$

Согласно (2), получим $x'_1 = x_1$, $x'_2 = x_2$, $x'_{i+1} = x_{i+1}$ для $i = 2, 3, \dots, s-1$, т.е. имеем равенство $G_{a,b}(F_{a,b}(x_1x_2 \dots x_s)) = x_1x_2 \dots x_s$. Аналогично доказывается равенство

$$F_{a,b}(G_{a,b}(y_1y_2 \dots y_s)) = y_1y_2 \dots y_s$$

для любого слова $y_1y_2 \dots y_s$ из Q^+ . $\square$

Для преобразования слов с помощью тернарных (L, M) -квазигрупп можно использовать композиции отображений вида (4). Выбираем (L, M) -тернарные квазигруппы $\langle Q, f_1 \rangle$, $\langle Q, f_2 \rangle$, ..., $\langle Q, f_t \rangle$ и упорядоченные пары $(a_1, b_1), (a_2, b_2), \dots, (a_t, b_t)$ элементов из Q ($t > 1$). Строим по правилу (4) отображения $F_{a_1, b_1}^1, F_{a_2, b_2}^2, \dots, F_{a_t, b_t}^t$, а затем рассматриваем композицию

$$F_{a_1, b_1, a_2, b_2, \dots, a_t, b_t} = F_{a_1, b_1}^1 \circ F_{a_2, b_2}^2 \circ \dots \circ F_{a_t, b_t}^t.$$

Для этих же тернарных (L, M) -квазигрупп и пар элементов строим по правилу (5) отображения $G_{a_1, b_1}^1, G_{a_2, b_2}^2, \dots, G_{a_t, b_t}^t$, и также рассматриваем композицию

$$G_{a_t, b_t, \dots, a_2, b_2, a_1, b_1} = G_{a_t, b_t}^t \circ \dots \circ G_{a_2, b_2}^2 \circ G_{a_1, b_1}^1.$$

Очевидно, $G_{a_t, b_t, \dots, a_2, b_2, a_1, b_1}$ – обратное отображение для отображения $F_{a_1, b_1, a_2, b_2, \dots, a_t, b_t}$.

В криптографии необходимо, чтобы зашифрованное слово можно было расшифровать однозначно. В нашем случае имеем следующий факт.

Теорема 3. Пусть $\langle Q, f_1 \rangle, \langle Q, f_2 \rangle, \dots, \langle Q, f_t \rangle$ – тернарные (L, M) -квазигруппы, где $Q = \{1, \dots, t\}$. Для любого слова $y_1y_2 \dots y_s$ из Q^+ и для любых упорядоченных пар $(a_1, b_1), (a_2, b_2), \dots, (a_t, b_t)$ элементов из Q существует единственное слово $x_1x_2 \dots x_s$ из Q^+ такое, что верно равенство

$$F_{a_1, b_1, a_2, b_2, \dots, a_t, b_t}(x_1x_2 \dots x_s) = y_1y_2 \dots y_s.$$

Доказательство. Существование и единственность слова $x_1x_2 \dots x_s$ из Q^+ доказывается применением к слову $y_1y_2 \dots y_s$ из Q^+ преобразования $G_{a_t, b_t, \dots, a_2, b_2, a_1, b_1}$. $\square$

Отображение $F_{a,b}$ в правиле (4) мы строили, помещая символы прообраза в первую позицию тернарной операции f , но можно строить $F_{a,b}$ еще другим способом: помещать символы прообраза во вторую позицию операции f , но тогда отображение $G_{a,b}$ в правиле (5) надо строить, используя тернарную операцию v . В этом случае можно строить выше указанную композицию $F_{a_1, b_1, a_2, b_2, \dots, a_t, b_t}$. Кроме того, можно также комбинировать оба рассмотренных случая при построении указанной композиции.

4. Конгруэнции на тернарных (L, M) -квазигруппах

Пусть τ – конгруэнция на тернарной (L, M) -квазигруппе $\langle Q, f, u, v \rangle$ (как универсальной алгебре с набором тождеств (2), (3)), т.е. τ – отношение эквивалентности, стабильное относительно всех тернарных операций f, u, v . Класс конгруэнции τ обозначим $[a]_\tau$.

Теорема 4. *Отношение эквивалентности τ на конечной тернарной (L, M) -квазигруппе $\langle Q, f, u, v \rangle$ является конгруэнцией тогда и только тогда, когда τ стабильно относительно операции f .*

Доказательство. Пусть τ стабильно относительно операции f . Для элементов $a, b \in Q$ рассмотрим перестановки $\alpha_{a,b}(x) = f(x, a, b)$, $\beta_{a,b}(x) = f(a, x, b)$ на множестве Q . Согласно тождествам (2), (3) верно $\alpha_{a,b}^{-1}(y) = u(y, a, b)$, $\beta_{a,b}^{-1}(y) = v(a, y, b)$. Так как Q конечно, то найдутся натуральные числа r, s такие, что $\alpha_{a,b}^r = 1 = \beta_{a,b}^s$. Тогда $\alpha_{a,b}^{r-1} = \alpha_{a,b}^{-1}$, $\beta_{a,b}^{s-1} = \beta_{a,b}^{-1}$.

Пусть $a_1 \tau a_2$, $b_1 \tau b_2$, $c_1 \tau c_2$. Индукцией по n легко доказывается, что для любого натурального n верно $\alpha_{b_1, c_1}^n(a_1) \tau \alpha_{b_2, c_2}^n(a_2)$, $\beta_{a_1, c_1}^n(b_1) \tau \beta_{a_2, c_2}^n(b_2)$. Тогда

$$u(a_1, b_1, c_1) = \alpha_{b_1, c_1}^{-1}(a_1) = \alpha_{b_1, c_1}^{r-1}(a_1) \tau \alpha_{b_2, c_2}^{r-1}(a_2) = \alpha_{b_2, c_2}^{-1}(a_2) = u(a_2, b_2, c_2).$$

Аналогично доказывается стабильность отношения τ относительно операции v . $\square$

Любые два класса конгруэнции тернарной (L, M) -квазигруппы равноможны, поскольку конгруэнция тернарной (L, M) -квазигруппы является конгруэнцией на каждой квазигруппе, определяемой тернарной операцией, а классы конгруэнции квазигруппы равноможны (см., например, [13, теорема 3.4]). В частности, если тернарная (L, M) -квазигруппа конечна, то порядок каждого класса конгруэнции делит порядок тернарной (L, M) -квазигруппы.

Элемент e тернарной (L, M) -квазигруппы $\langle Q, f \rangle$ назовем левой (средней) единицей, если верно равенство $f(e, e, a) = a$ ($f(e, a, e) = a$) для любого элемента $a \in Q$. Тогда верны равенства $f(e, e, e) = e = u(e, e, e) = v(e, e, e)$, т. е. левая и средняя единицы являются идемпотентами для всех тернарных операций f, u, v .

Теорема 5. *Если в тернарной (L, M) -квазигруппе $\langle Q, f \rangle$ имеется левая (средняя) единица e , то для любой конгруэнции τ этой тернарной (L, M) -квазигруппы ее класс $[e]_\tau$ является тернарной (L, M) -подквазигруппой, а любой класс $[a]_\tau = f([e]_\tau, e, a) = f(e, [e]_\tau, a)$ ($[a]_\tau = f([e]_\tau, a, e)$).*

Доказательство. Пусть посылка теоремы верна и $a, b, c \in [e]_\tau$, тогда $a \tau e$, $b \tau e$, $c \tau e$, откуда

$$f(a, b, c) \tau f(e, e, e) = e, \quad u(a, b, c) \tau u(e, e, e) = e, \quad v(a, b, c) \tau v(e, e, e) = e,$$

т. е. $f(a, b, c), u(a, b, c), v(a, b, c) \in [e]_\tau$. Значит, $[e]_\tau$ – тернарная (L, M) -подквазигруппа. Далее, если e – левая единица, то

$$\begin{aligned} b \in [a]_\tau &\Leftrightarrow b \tau a \Leftrightarrow u(b, e, a) \tau u(a, e, a) = e \Leftrightarrow b = f(u(b, e, a), e, a) \in f([e]_\tau, e, a), \\ b \in [a]_\tau &\Leftrightarrow b \tau a \Leftrightarrow v(e, b, a) \tau v(e, a, a) = e \Leftrightarrow b = f(e, v(e, b, a), a) \in f(e, [e]_\tau, a). \end{aligned}$$

Если e – средняя единица, то

$$b \in [a]_\tau \Leftrightarrow b \tau a \Leftrightarrow u(b, a, e) \tau u(a, a, e) = e \Leftrightarrow b = f(u(b, a, e), a, e) \in f([e]_\tau, a, e). \quad \square$$

В конце этого параграфа рассмотрим достаточный признак простоты конечной тернарной (L, M) -квазигруппы (такой же признак для квазигрупп имеется в [14, предложение 3.13]). Напомним, что тернарная (L, M) -квазигруппа называется простой, если в ней только тривиальные конгруэнции.

Пусть $\langle Q, f \rangle$ – конечная (L, M) -квазигруппа и $Q = \{1, \dots, m\}$. Для фиксированных элементов $i, j \in Q$ имеем подстановку β_{ik} на Q , действующую по правилу $\beta_{ik}(j) = f(i, j, k)$.

Теорема 6. Пусть τ – конгруэнция на конечной тернарной (L, M) -квазигруппе $\langle Q, f \rangle$ и подстановка β_{ik} имеет цикл $\{a, \beta_{ik}(a), \beta_{ik}^2(a), \dots, \beta_{ik}^{p-1}(a)\}$, $\beta_{ik}^p(a) = a$. Наименьшее положительное целое число q такое, что $\beta_{ik}^q(a)\tau a$, делит p .

Доказательство. Для наибольшего общего делителя d чисел q и p имеются целые числа s и t такие, что $d = qs + pt$. Тогда

$$\beta_{ik}^d(a) = \beta_{ik}^{qs+pt}(a) = (\beta_{ik}^q)^s \circ (\beta_{ik}^p)^t(a) = (\beta_{ik}^q)^s(a)\tau a.$$

Тогда $q = d$, откуда q делит p . □

Теорема 7. Пусть $\langle Q, f \rangle$ – конечная тернарная (L, M) -квазигруппа. Если имеется подстановка β_{ik} с циклом $\{a, \beta_{ik}(a), \beta_{ik}^2(a), \dots, \beta_{ik}^{p-1}(a)\}$, $\beta_{ik}^p(a) = a$, где p – простое число и $p > \frac{|Q|}{2}$, то $\langle Q, f \rangle$ будет простой.

Доказательство. Предположим, что в $\langle Q, f \rangle$ имеется нетривиальная конгруэнция τ . Пусть, как и выше, q – наименьшее положительное целое число такое, что $\beta_{ik}^q(a)\tau a$. Тогда по теореме 6 q делит p . Но p – простое число, значит, $q = 1$ или $q = p$. Если $q = p$, то все элементы множества $\{a, \beta_{ik}(a), \beta_{ik}^2(a), \dots, \beta_{ik}^{p-1}(a)\}$ из разных классов, что противоречит условию $p > \frac{|Q|}{2}$. Если $q = 1$, то все элементы множества $\{a, \beta_{ik}(a), \beta_{ik}^2(a), \dots, \beta_{ik}^{p-1}(a)\}$ лежат в одном классе $[a]_\tau$, т.е. $p \leq |[a]_\tau|$. Но, по предположению, $|[a]_\tau| \leq \frac{|Q|}{2}$, что вновь противоречит условию $p > \frac{|Q|}{2}$. □

В конечной тернарной (L, M) -квазигруппе $\langle Q, f \rangle$ для фиксированных элементов $j, k \in Q$ имеем подстановку α_{jk} на Q , действующую по правилу $\alpha_{jk}(i) = f(i, j, k)$. Теоремы 6 и 7 также доказываются для подстановки α_{jk} .

5. Полиномиально полные тернарные квазигруппы

Пусть A – непустое множество и F – набор алгебраических операций, действующих на этом множестве. Тогда A называют F -алгеброй. Обозначим через $T(F)$ наименьший клон операций над A , содержащий F . Операции из $T(F)$ называются термальными операциями в сигнатуре F .

Операция $f(x_1, \dots, x_n)$, действующая на множестве A , называется полиномиальной, если существуют термальная $(n + m)$ -арная операция g и элементы $a_1, \dots, a_m \in A$ такие, что

$$f(x_1, \dots, x_n) = g(x_1, \dots, x_n, a_1, \dots, a_m)$$

для любых элементов $x_1, \dots, x_n \in A$.

Клон $\text{Pol}(F)$ всех полиномиальных операций является наименьшим клоном, содержащим F и все нульместные операции.

F -алгебра A называется полиномиально полной, если множество всех алгебраических операций, действующих на A , совпадает с $\text{Pol}(F)$.

Тернарная операция $m(x, y, z)$, действующая на множестве A , называется термом Мальцева, если верны тождества $m(x, x, y) = y = m(y, x, x)$.

Теорема 8. В тернарной (L, M) -квазигруппе $\langle Q, f \rangle$ тернарная операция

$$m(x, y, z) = f(u(x, v(x, y, z), z), v(x, z, z), z)$$

является термом Мальцева.

Доказательство. Согласно тождеству (3) имеем равенство $f(x, v(x, x, y), y) = x$ и элемент $u(x, v(x, x, y), y)$ является решением уравнения $f(t, v(x, x, y), y) = x$ с переменной t . Поэтому в силу однозначной разрешимости этого уравнения, получим $u(x, v(x, x, y), y) = x$. Теперь, вновь с использованием тождества (3), получим

$$m(x, x, y) = f(u(x, v(x, x, y), y), v(x, y, y), y) = f(x, v(x, y, y), y) = y.$$

Используя тождество (2), получим

$$m(y, x, x) = f(u(y, v(y, x, x), x), v(y, x, x), x) = y. \quad \square$$

Алгебра A называется аффинной (см. [14]), если A снабжена структурой аддитивной абелевой группы такой, что каждая термальская операция g имеет вид

$$g(x_1, \dots, x_n) = a_0 + \alpha_1 x_1 + \dots + \alpha_n x_n, \quad (6)$$

где $a_0 \in A$, $\alpha_1, \dots, \alpha_n$ являются групповыми эндоморфизмами. Известно, что если в аффинной алгебре A имеется терм Мальцева, который является полиномиальной операцией, то сложение в определении аффинной алгебры является полиномиальной операцией (см. [14, предложение 2.7]).

Теорема 9. Тернарная (L, M) -квазигруппа $\langle Q, f \rangle$ является аффинной тогда и только тогда, когда на $\langle Q, f \rangle$ существует структура абелевой группы $\langle Q, +, 0, - \rangle$ такая, что

$$f(x, y, z) = \alpha x + \beta y + \gamma z + c$$

для некоторых автоморфизмов α, β , эндоморфизма γ группы $\langle Q, +, 0, - \rangle$ и для некоторого элемента $c \in Q$.

Доказательство. Пусть тернарная (L, M) -квазигруппа $\langle Q, f \rangle$ является аффинной. Тогда (L, M) -квазигруппа $\langle Q, f \rangle$ снабжена структурой абелевой группы $\langle Q, +, 0, - \rangle$ и для

операции f найдутся эндоморфизмы α, β, γ этой группы и элемент $c \in Q$ такие, что $f(x, y, z) = \alpha x + \beta y + \gamma z + c$. Докажем, что α, β будут автоморфизмами. Докажем сюръективность α . Выбираем любой элемент $q \in Q$ и находим решение r уравнения $f(t, 0, 0) = q + c$. Тогда, с одной стороны, $f(r, 0, 0) = q + c$, а с другой — $f(r, 0, 0) = \alpha r + \beta 0 + \gamma 0 + c = \alpha r + c$. Значит, $\alpha r = q$, т.е. α — сюръективное отображение. Докажем инъективность α . Пусть $\alpha(x_1) = \alpha(x_2) = d$ для некоторых элементов x_1, x_2 из Q . Тогда x_1 и x_2 являются решениями уравнения $f(t, 0, 0) = d + c$, но это уравнение имеет единственное решение, значит, $x_1 = x_2$, т.е. α — инъективное отображение. Аналогично доказывается, что β будет автоморфизмом.

Пусть второе условие теоремы выполнено. Тогда, согласно определению тернарных операций u, v , получим

$$\begin{aligned} u(x, y, z) &= \alpha^{-1}x - \alpha^{-1}\beta y - \alpha^{-1}\gamma z - \alpha^{-1}c, \\ v(x, y, z) &= -\beta^{-1}\alpha x + \beta^{-1}y - \beta^{-1}\gamma z - \beta^{-1}c. \end{aligned}$$

Выбираем термальную операцию $g(x_1, \dots, x_n)$ тернарной (L, M) -квазигруппы $\langle Q, f \rangle$. Так как операция g получается с помощью повторной композиции тернарных квазигрупповых операций f, u, v и проекций, то найдутся эндоморфизмы $\alpha_1, \dots, \alpha_n$ группы $\langle Q, +, 0, - \rangle$ и элемент $a_0 \in Q$ такие, что верно (6). $\square$

Теорема 10. Пусть $\langle Q, f \rangle$ — конечная тернарная (L, M) -квазигруппа, где $Q = \{1, \dots, t\}$, и B — трехмерная матрица как таблица тернарной операции f . Если $\langle Q, f \rangle$ является аффинной, то каждая квазигруппа из набора t квазигрупп, определенных матрицей B , является аффинной.

Доказательство. Согласно теореме 9, на $\langle Q, f \rangle$ существует структура абелевой группы $\langle Q, +, 0, - \rangle$ такая, что $f(x, y, z) = \alpha x + \beta y + \gamma z + c$, где α, β — автоморфизмы, γ — эндоморфизм группы $\langle Q, +, 0, - \rangle$ и $c \in Q$. Выбираем, например, квазигруппу $\langle Q, \circ_k \rangle$, где $i \circ_k j = f(i, j, k)$. Тогда

$$i \circ_k j = f(i, j, k) = \alpha i + \beta j + \gamma k + c = \alpha i + \beta j + d,$$

где $d = \gamma k + c$ — элемент из Q , т.е. $\langle Q, \circ_k \rangle$ — T -квазигруппа, а значит, она будет аффинной [14]. $\square$

Теорема 11 ([15]). Пусть A — конечная F -алгебра, содержащая по меньшей мере два элемента. Тогда следующие условия эквивалентны:

- 1) A полиномиально полна;
- 2) существует терм Мальцева в $\text{Pol}(F)$ на A и алгебра A является простой и неаффинной.

Следствие 12. Пусть $\langle Q, f \rangle$ — конечная тернарная (L, M) -квазигруппа, содержащая по меньшей мере два элемента. Тогда $\langle Q, f \rangle$ полиномиально полна если и только если $\langle Q, f \rangle$ является простой и неаффинной.

Доказательство. В тернарной (L, M) -квазигруппе $\langle Q, f \rangle$ существует терм Мальцева (теорема 8). Осталось применить теорему 11. $\square$

Устанавливать неаффинность тернарной (L, M) -квазигруппы можно (согласно теореме 10) по неаффинности хотя бы одной квазигруппы из набора квазигрупп, определенных трехмерной матрицей как таблицей тернарной операции. Например, в работе [7] неаффинность квазигруппы порядка 4 устанавливали по их соответствующим латинским квадратам.

Теорема 13. Пусть $\langle Q, f \rangle$ – конечная тернарная (L, M) -квазигруппа порядка m , $A_1, A_2, \dots, A_m$ – набор латинских квадратов на множестве Q с умножениями $i \circ_k j = f(i, j, k)$ ($k = 1, 2, \dots, m$). Тогда если

- 1) найдется латинский квадрат A_i , $1 \leq i \leq m$, в котором есть строка или столбец, в разложении которой как перестановки на произведение независимых циклов имеется цикл длины p , где $p > \frac{m}{2}$ и p – простое число,
- 2) найдется латинский квадрат A_j , $1 \leq j \leq m$, который определяет неаффинную квазигруппу $\langle Q, \circ_j \rangle$,

то тернарная (L, M) -квазигруппа $\langle Q, f \rangle$ будет полиномиально полна.

Доказательство. Из п. 1) по теореме 7 $\langle Q, f \rangle$ будет простой. Кроме того, по теореме 10 $\langle Q, f \rangle$ будет неаффинной, поскольку квазигруппа $\langle Q, \circ_j \rangle$ неаффинная согласно п. 2). Осталось применить следствие 12. $\square$

В заключение приведем пример полиномиально полной тернарной (L, M) -квазигруппы четвертого порядка. Пусть $Q = \{1, 2, 3, 4\}$. Тернарная операция f задается трехмерной матрицей B четвертого порядка, которая определяется, в свою очередь, четырьмя латинскими квадратами с бинарными операциями $i \circ_k j = f(i, j, k)$, $k = 1, 2, 3, 4$ (таблица 1). Например, чтобы вычислить $f(3, 4, 2)$, надо выбрать второй квадрат ($k = 2$) и в этом квадрате выбрать элемент, стоящий на пересечении третьей строки и четвертого столбца, получим $f(3, 4, 2) = 2$. Первый латинский квадрат в таблице 1 определяет неаффинную квазигруппу (см. [14]) и в этом квадрате третья строка, как перестановка, является циклом длины 3. Согласно теореме 13, тернарная (L, M) -квазигруппа $\langle Q, f \rangle$ будет полиномиально полна.

Таблица 1. Трехмерная таблица из четырех латинских квадратов

$\circ_1$	1	2	3	4
1	4	1	2	3
2	3	2	1	4
3	2	4	3	1
4	1	3	4	2

$\circ_2$	1	2	3	4
1	3	2	4	1
2	2	4	1	3
3	1	3	2	4
4	4	1	3	2

$\circ_3$	1	2	3	4
1	1	3	4	2
2	2	4	3	1
3	4	1	2	3
4	3	2	1	4

$\circ_4$	1	2	3	4
1	1	3	4	2
2	4	1	2	3
3	3	2	1	4
4	2	4	3	1

Список литературы

- [1] В.Т. Марков, А.В. Михалёв, А.А. Нечаев, *Неассоциативные алгебраические структуры в криптографии и кодировании*, Фундамент. и прикл. матем. **21** (4), 99–124 (2016). URL: <https://www.mathnet.ru/rus/fpm1749>
- [2] М.М. Глухов, *О применениях квазигрупп в криптографии*, ПДМ (2), 28–32 (2008). URL: <https://www.mathnet.ru/rus/pdm29>
- [3] S. Markovski, D. Gligoroski, V. Bakeva, *Quasigroup string processing*. I, Makedon. Akad. Nauk. Umet. Oddel. Mat.-Tehn. Nauk. Prilozi **20** (1–2), 13–28 (2001).
- [4] A. Petrescu, *n-quasigroup cryptographic primitives: stream ciphers*, Stud. Univ. Babeş-Bolyai Inform. **55** (2), 27–34 (2010).
- [5] V. Dimitrova, H. Mihajloska, *An application of ternary quasigroup string transformations*, ICT Innovations 2010, Web Proceedings, 251–259 (2010).
- [6] В.А. Артамонов, *Квазигруппы и их приложения*, Чебышевский сб. **19** (2), 111–122 (2018). DOI: <https://doi.org/10.22405/2226-8383-2018-19-2-111-122>
- [7] V.A. Artamonov, S. Chakrabarti, S.K. Pal, *Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations*, Discrete Appl. Math. **200**, 5–17 (2016). DOI: <https://doi.org/10.1016/j.dam.2015.06.033>
- [8] Н.А. Щучкин, *Применение тернарных квазигрупп к преобразованию слов*, Дискрет. матем. **36** (2), 132–143 (2024). DOI: <https://doi.org/10.4213/dm1809>
- [9] В.Д. Белоусов, *n-Арные квазигруппы*, Штиинца, Кишинев, 1972.
- [10] В.А. Щербаков, А. Х. Табаров, Д.И. Пушкашу, *О конгруэнциях группоидов, тесно связанных с квазигруппами*, Фундамент. и прикл. матем. **14** (5), 237–251 (2008). URL: <https://www.mathnet.ru/rus/fpm1154>
- [11] Н.П. Соколов, *Введение в теорию многомерных матриц*, Наукова думка, Киев, 1972.
- [12] H.J. Ryser, *Permanents and systems of distinct representatives*, in: Combin. Math. Appl. (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967), Univ. North Carolina Pr., Chapel Hill, 55–70 (1969).
- [13] Г.Б. Белявская, *T-квазигруппы и центр квазигруппы*, Матем. исслед. **111**, 24–43 (1989).
- [14] V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal, *Latin squares of polynomially complete quasigroups and quasigroups generated by shifts*, Quasigroups and Related Systems **21** (2), 117–130 (2013).

- [15] J. Hagemann, C. Herrmann, *Arithmetically locally equational classes and representation of partial functions*, Colloq. Math. Soc. János Bolyai **29**, 345–360 (1982).

Александра Андреевна Веселова

Волгоградский государственный социально-педагогический университет,
Кафедра высшей математики и физики,
пр-т им. В.И. Ленина, д. 27, г. Волгоград, 400005, Россия,
e-mail: alexandra.912@mail.ru

Николай Алексеевич Щучкин

Волгоградский государственный социально-педагогический университет,
Кафедра высшей математики и физики,
пр-т им. В.И. Ленина, д. 27, г. Волгоград, 400005, Россия,
e-mail: nikolaj_shchuchkin@mail.ru

Word transformation using ternary (L, M) -quasigroups

A.A. Veselova, N.A. Shchuchkin

Abstract. We construct an algorithm for transforming words using a set of finite quasigroups in an amount equal to the number of characters of the alphabet. Some properties of ternary (L, M) -quasigroups are given, which play an important role in the analysis and design of cryptographic schemes based on these algebras, such as polynomial completeness, absence of nontrivial congruences.

Keywords: quasigroup, polynomial completeness, congruence.

DOI: 10.26907/2949-3919.2025.1.12-25

References

- [1] V.T. Markov, A.V. Mikhalev, A.A. Nechaev, *Nonassociative algebraic structures in cryptography and coding*, J. Math. Sci. **245** (2), 178–196 (2020).
DOI: <https://doi.org/10.1007/s10958-020-04685-5>
- [2] M.M. Glukhov, *On applications of quasigroups in cryptography*, Prikl. Diskret. Mat. (2), 28–32 (2008) [in Russian].
URL: <https://www.mathnet.ru/rus/pdm29>
- [3] S. Markovski, D. Gligoroski, V. Bakeva, *Quasigroup string processing. I*, Makedon. Akad. Nauk. Umet. Oddel. Mat.-Tehn. Nauk. Prilozi **20** (1–2), 13–28 (2001).
- [4] A. Petrescu, *n-quasigroup cryptographic primitives: stream ciphers*, Stud. Univ. Babeş-Bolyai Inform. **55** (2), 27–34 (2010).
- [5] V. Dimitrova, H. Mihajloska, *An application of ternary quasigroup string transformations*, ICT Innovations 2010, Web Proceedings, 251–259 (2010).
- [6] V.A. Artamonov, *Quasigroups and their applications*, Chebyshevskii Sb. **19** (2), 111–122 (2018) [in Russian].
DOI: <https://doi.org/10.22405/2226-8383-2018-19-2-111-122>
- [7] V.A. Artamonov, S. Chakrabarti, S.K. Pal, *Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations*, Discrete Appl. Math. **200**, 5–17 (2016).
DOI: <https://doi.org/10.1016/j.dam.2015.06.033>

- [8] N.A. Shchuchkin, *Application of ternary quasigroups to string transformation*, Diskr. Mat. **36** (2), 132–143 (2024) [in Russian].
DOI: <https://doi.org/10.4213/dm1809>
- [9] V.D. Belousov, *n-quasigroups*, Štiinca, Kishinev, 1972 [in Russian].
- [10] V.A. Shcherbacov, A.Kh. Tabarov, D.I. Puşcaşu, *On congruences of groupoids closely connected with quasigroups*, J. Math. Sci. **163** (6), 785–795 (2009).
DOI: <https://doi.org/10.1007/s10958-009-9716-4>
- [11] N.P. Sokolov, *Introduction to the theory of multidimensional matrices*, Naukova dumka, Kiev, 1972.
- [12] H.J. Ryser, *Permanents and systems of distinct representatives*, in: Combin. Math. Appl. (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967), Univ. North Carolina Pr., Chapel Hill, 55–70 (1969).
- [13] G.B. Belyavskaya, *T-quasigroups and the center of the quasigroup*, Matem. Issled. **111**, 24–43 (1989) [in Russian].
- [14] V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal, *Latin squares of polynomially complete quasigroups and quasigroups generated by shifts*, Quasigroups and Related Systems **21** (2), 117–130 (2013).
- [15] J. Hagemann, C. Herrmann, *Arithmetically locally equational classes and representation of partial functions*, Colloq. Math. Soc. János Bolyai **29**, 345–360 (1982).

Alexandra Andreevna Veselova

Volgograd State Socio-Pedagogical University,
Department of Higher Mathematics and Physics,
27 V.I. Lenin av., Volgograd 400005, Russia,
e-mail: alexandra.912@mail.ru

Nikolai Alekseevich Shchuchkin

Volgograd State Socio-Pedagogical University,
Department of Higher Mathematics and Physics,
27 V.I. Lenin av., Volgograd 400005, Russia,
e-mail: nikolaj_shchuchkin@mail.ru

Графы тригональных кривых и жесткие изотопии особых вещественных алгебраических кривых бистепени $(4, 3)$ на гиперboloиде

В.И. Звонилов

Аннотация. Жесткой изотопией вещественных алгебраических кривых некоторого класса называется путь в пространстве кривых этого класса. В работе завершена жесткая изотопическая классификация неособых вещественных алгебраических кривых бистепени $(4, 3)$ на гиперboloиде, начатая автором в более ранних работах. Даны отсутствовавшие доказательства единственности компонент связности 16-ти классов вещественных алгебраических кривых бистепени $(4, 3)$, имеющих единственную невырожденную двойную точку или точку возврата. Основным техническим средством являются графы вещественных тригональных кривых на поверхностях Хирцебруха.

Ключевые слова: пространства вещественных алгебраических кривых, кривые на гиперboloиде, тригональные кривые, вложенные графы.

DOI: 10.26907/2949-3919.2025.1.26-51

Введение

В работе автора [1, теорема 2] утверждалось, что *неособая кривая бистепени $(4, 3)$ на гиперboloиде определяется с точностью до жесткой изотопии своей комплексной схемой*. Для доказательства этого использовался подход, предложенный в [2] для получения жесткой изотопической классификации плоских вещественных квинтик и основанный на теореме 1 работы [1], указывающей все компоненты связности пространства кривых бистепени $(4, 3)$, имеющих единственную невырожденную двойную точку или точку возврата. Доказательство этой теоремы было начато автором в [1]; в [3] был указан пробел в этом доказательстве, который устранен в настоящей работе отличным от предыдущего способом – с использованием графов вещественных тригональных кривых на поверхности Хирцебруха Σ_3 , полученных из особых кривых бистепени $(4, 3)$.

Структура статьи: раздел 1 содержит необходимые сведения по топологии вещественных алгебраических кривых, имеющиеся в работах [4, 5], и в частности, кривых на гиперboloиде (см. [6]). В разделе 2 напоминаются определения поверхностей Хирцебруха

Благодарности. Работа выполнена в рамках государственного задания FSWR-2023-0034.

Σ_k и их бирациональных преобразований, необходимых в дальнейшем для связи между кривыми на гиперboloиде и тригональными кривыми на Σ_3 . Разделы 3 и 5, следуя работам [7] и [8], напоминают понятия, связанные с вещественными тригональными кривыми. В разделе 4 понятие скелета, введенное в [8] для максимально изогнутых тригональных кривых, распространяется на более широкий класс кривых. В разделе 6 описываются классы кривых бистепени (4,3), имеющих единственную невырожденную двойную точку или точку возврата, и восполняется указанный пробел, состоявший в отсутствии доказательства связности каждого из классов особых кривых $\omega_{inn}^\pm$, $\alpha_{lp}^\pm\langle l\rangle$, $l = 0, 1, 2, 4, 5$, $\alpha_{lp}^\pm\langle 3\rangle_I$, $\alpha_{lp}^\pm\langle 3\rangle_{II}$ (в обозначениях работ [1, 3]) на гиперboloиде. Те же аргументы дают доказательство связности остальных классов особых кривых.

1. Определения и обозначения

Вещественным алгебраическим многообразием называется комплексное алгебраическое многообразие V с антиголоморфной инволюцией $c = c_V : V \rightarrow V$. Множество неподвижных точек $\mathbb{R}V = \text{Fix } c$ называется *вещественной частью* многообразия V . Регулярный морфизм $f : V \rightarrow W$ двух вещественных многообразий называется *вещественным* или *эквивариантным* если $f \circ c_V = c_W \circ f$.

Гиперboloид X понимается как вещественная неособая квадрика $X = \mathbb{P}^1 \times \mathbb{P}^1$ с антиголоморфной инволюцией c_X , сохраняющей произведение, и вещественной частью $\mathbb{R}X = \mathbb{R}P^1 \times \mathbb{R}P^1$.

Зафиксируем пару P_1, P_2 образующих гиперboloида X , изоморфных $\mathbb{P}^1$. Фундаментальные классы $[P_1], [P_2]$ образуют базис группы $H_2(X) \cong \mathbb{Z} \oplus \mathbb{Z}$. Пусть A – алгебраическая кривая на X . Тогда $[A] = m_2[P_1] + m_1[P_2]$ для некоторых неотрицательных целых m_1, m_2 . Пара (m_1, m_2) называется *бистепенью* кривой A . Если $[x_0 : x_1], [y_0 : y_1]$ – однородные координаты на прямых P_1, P_2 , то кривая A задается биоднородным многочленом

$$F(x_0, x_1; y_0, y_1) = \sum_{i,j=1}^{m_1, m_2} a_{i,j} x_1^i x_0^{m_1-i} y_1^j y_0^{m_2-j},$$

имеющим степени однородности m_1 по x_0, x_1 и m_2 по y_0, y_1 , причем A вещественна тогда и только тогда, когда все $a_{i,j}$ могут быть выбраны вещественными.

Для указания топологии вещественной кривой на гиперboloиде мы используем модификацию стандартной кодировки вещественных схем плоских проективных кривых (см., например, [5]). Пусть $A \subset X$ – неособая вещественная алгебраическая кривая. Вещественная часть $\mathbb{R}A$ может иметь компоненты двух типов: стягиваемые в $\mathbb{R}X$ и нестягиваемые; стягиваемые компоненты называются *овалами*. Число овалов обозначается через l , число нестягиваемых компонент – через h . Каждый овал ограничивает топологический диск в $\mathbb{R}X$, называемый *внутренностью* овала. Фундаментальные классы $[\mathbb{R}P_1], [\mathbb{R}P_2]$, наделенные некоторыми (фиксированными) ориентациями, образуют базис группы $H_1(\mathbb{R}X) \cong \mathbb{Z} \oplus \mathbb{Z}$. Все нестягиваемые компоненты $N_1, \dots, N_h$ реализуют один и тот же

ненулевой класс (c_1, c_2) в $H_1(\mathbb{R}X)$, где c_1, c_2 взаимно просты. Вещественная схема кривой $\mathbb{R}A \subset \mathbb{R}X$ кодируется следующим образом:

$$\langle (c_1, c_2), \text{scheme}_1, (c_1, c_2), \text{scheme}_2, \dots, (c_1, c_2), \text{scheme}_h \rangle,$$

где $\text{scheme}_1, \dots, \text{scheme}_h$ – схемы расположения овалов, лежащих в связных компонентах поверхности $\mathbb{R}X \setminus (N_1 \cup \dots \cup N_h)$ (ср. [5, 6]).

Согласно Ф. Клейну (см. [9] или [4]) вещественная кривая A принадлежит *типу* I или *типу* II в зависимости от того, разбивает $\mathbb{R}A$ множество комплексных точек кривой A или нет. Если A принадлежит типу I, естественные ориентации компонент U и V пространства $A \setminus \mathbb{R}A$ дают две противоположные ориентации кривой $\mathbb{R}A = \partial U = \partial V$; они называются *комплексными ориентациями*. Вещественная схема, наделенная типом и, в случае типа I, комплексными ориентациями, называется *комплексной схемой*. Если нужно указать тип кривой с вещественной схемой $\langle B \rangle$ используются обозначения $\langle B \rangle_I$ и $\langle B \rangle_{II}$.

Все вещественные кривые бистепени (m, n) образуют пространство $C_{m,n} \cong \mathbb{R}P^N$ с $N = mn + m + n$. Множество $\Delta \subset C_{m,n}$ особых кривых имеет размерность $N - 1$. Через $S \subset \Delta$ обозначается подмножество кривых, имеющих особую точку, отличную от невырожденной двойной точки или точки возврата, или имеющих несколько особых точек. Множество $\Delta \setminus S$ является топологическим многообразием (хотя и не гладким подмногообразием в $C_{m,n}$). *Жестким изотопическим классом* кривой $A \in C_{m,n} \setminus \Delta$ (или $A \in \Delta \setminus S$) называется компонента пространства $C_{m,n} \setminus \Delta$ (соотв. $\Delta \setminus S$), содержащая A . Компоненты пространства $C_{m,n} \setminus \Delta$ (соотв. $\Delta \setminus S$) называются *камерами* (*стенками*).

2. Поверхности Хирцебруха и преобразования Нагаты

Поверхность Хирцебруха $\Sigma_k, k \geq 0$, является пространством расслоения $q : \Sigma_k \rightarrow \mathbb{P}^1$ со слоем $\mathbb{P}^1$, т. е. рациональной линейчатой поверхностью, с исключительным сечением E_k , $E_k^2 = -k$. Слои расслоения q называются *вертикальными*, например, мы говорим о вертикальных касательных, вертикальных перегибах и т. д. Поверхность $\Sigma_0 = \mathbb{P}^1 \times \mathbb{P}^1$ является гиперboloидом, в котором в качестве исключительного сечения можно взять любую кривую бистепени $(0, 1)$. Далее Σ_k считается вещественной поверхностью, с исключительным вещественным сечением.

Определение 1. *Положительным (отрицательным) преобразованием Нагаты* (см. [10, § 2 (3)]) называется послойное бирациональное преобразование $\Sigma_k \rightarrow \Sigma_{k+1}$ (соответственно, $\Sigma_k \rightarrow \Sigma_{k-1}$), состоящее из раздутия точки $p \in E_k$ (соответственно, $p \notin E_k$) и последующего стягивания в точку собственного прообраза слоя $q^{-1}(p)$.

Положительное (отрицательное) преобразование Нагаты переводит E_k в E_{k+1} (соответственно, в E_{k-1}).

3. Вещественные тригональные кривые

Тригональной кривой называется приведенная кривая $C \subset \Sigma_k$, не содержащая ни исключительного сечения, ни слоя в качестве компоненты и такая, что сужение $q|_C$ есть отображение степени три. Тригональная кривая C называется *собственной*, если $C \cap E_k = \emptyset$.

Слой поверхности Σ_k с лежащей на ней тригональной кривой C называется *особым*, если он пересекает $C \cup E_k$ геометрически менее, чем в четырех точках.

Согласно [11, п. 3.1.1], для собственной тригональной кривой $C \subset \Sigma_k, k \geq 1$, на Σ_k существует аффинная карта (x, y) , в которой исключительное сечение E_k определяется уравнением $y = \infty$, а кривая C – *уравнением Вейерштрасса*

$$y^3 + b(x)y + w(x) = 0,$$

где b, w – многочлены, $\deg b \leq 2k, \deg w \leq 3k$. Можно расширить карту до $\Sigma_k \setminus E_k$, считая b, w однородными многочленами степеней $2k, 3k$.

Вещественная собственная тригональная кривая C называется *почти общей*, если все критические точки сужения $q|_C$, т.е. все корни дискриминанта $\Delta(x) = 4b^3 + 27w^2$, простые (так что C неособая), и *максимально изогнутой*, если все корни дискриминанта вещественные (и не обязательно простые).

Вещественная собственная тригональная кривая C (возможно особая) называется *гиперболической*, если ограничение $\mathbb{R}C \rightarrow \mathbb{R}P^1$ отображения q является трехлистным накрытием.

Для вещественной тригональной кривой C рациональная функция $j = j_C = \frac{4b^3}{\Delta} = 1 - \frac{27w^2}{\Delta}$ называется *j -инвариантом* этой кривой. Кривая с постоянным j -инвариантом называется *изотривиальной*. Почти общая кривая называется *общей*, если для каждого вещественного критического значения t ее j -инварианта кратность каждого корня уравнения $j(x) = t$ равна 3 при $t = 0$, равна 2 при $t \neq 0$ и все эти корни при $t \notin \{0, 1\}$ вещественны. Любую почти общую тригональную кривую можно малым изменением коэффициентов уравнения кривой превратить в общую.

Вещественная часть неособой негиперболической кривой C имеет единственную *длинную компоненту* L , характеризующуюся тем, что ограничение $L \rightarrow \mathbb{R}P^1$ отображения q имеет степень ± 1 . Для всех остальных компонент множества $\mathbb{R}C$, называемых *овалами*, эта степень равна 0. Пусть $Z \subset \mathbb{R}P^1$ – множество точек с более чем одним прообразом в $\mathbb{R}C$. Каждый овал переводится отображением q в целую компоненту множества Z , которая также называется *овалом*. Остальные компоненты множества Z , а также их прообразы в L называются *зигзагами*.

Под *деформацией* тригональной кривой $C \subset \Sigma_k$ понимается деформация пары $(q : \Sigma_k \rightarrow P^1, C)$ в смысле Кодайры–Спенсера. Деформация почти общей тригональной кривой называется *послойной*, если кривая остается почти общей на протяжении всей деформации.

Деформационная эквивалентность вещественных тригональных кривых задается

отношением эквивалентности, порожденным эквивариантными послойными деформациями и вещественными изоморфизмами.

3.1. ГРАФ ТРИГОНАЛЬНОЙ КРИВОЙ. Далее нам понадобятся графы на круге (*dessins*, как частные случаи трихотомических графов, в терминологии работ [7, раздел 5], [12]), изоморфные графам вещественных тригональных кривых (см. определение в следующем абзаце). Согласно [7] любой такой граф является графом некоторой тригональной кривой. Если не оговорено противное, всюду ниже термин *граф* подразумевает существование вещественной тригональной кривой с таким графом.

Пусть D – круг, полученный факторизацией комплексной проективной прямой $\mathbb{P}^1$ по комплексному сопряжению, и $\text{pr} : \mathbb{P}^1 \rightarrow D$ – проекция. Точки, отрезки и т. д., лежащие на граничной окружности ∂D называются *вещественными*. Для j -инварианта $j_C : \mathbb{P}^1 \rightarrow \mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$ неизотривиальной вещественной тригональной кривой $C \subset \Sigma_k$ прямую $\mathbb{R}P^1$, лежащую в образе этой функции, наделим ориентацией, задаваемой порядком в $\mathbb{R}$, и раскрасим следующим образом: пусть 0 , 1 , и ∞ – это, соответственно, $\bullet$ -, $\circ$ - и $\times$ -вершина; $(\infty, 0)$, $(0, 1)$ и $(1, \infty)$ – это, соответственно, сплошное, жирное и пунктирное ребро. Поднимем эти ориентацию и раскраску на граф $\Gamma_C = \text{pr}(j_C^{-1}(\mathbb{R}P^1))$, получив *граф вещественной тригональной кривой C* . Его $\bullet$ -, $\circ$ - и $\times$ -вершины, являющиеся точками ветвления (критическими точками j -инварианта) с критическими значениями $0, 1$ и ∞ , называются *существенными*, остальные вершины, являющиеся точками ветвления с вещественными критическими значениями, отличными от $0, 1, \infty$, называются *монохромными*. Монохромные вершины подразделяются на сплошные, жирные и пунктирные согласно тому, какие ребра к ним примыкают. *Монохромный цикл* в Γ_C – это цикл, все вершины которого монохромны; следовательно, все его ребра и вершины одного цвета. Определение графа Γ_C подразумевает, что он не имеет ориентированных монохромных циклов.

Склеим из двух копий круга D сферу S , превратив круги в полусферы. Пусть $p : S \rightarrow D$ – проекция, отождествляющая копии, и $\Gamma'_C = p^{-1}(\Gamma_C)$ – граф на сфере с раскраской, индуцированной проекцией. *Полной валентностью* вершины v графа Γ_C называется валентность любой вершины $v' \in p^{-1}(v)$ графа Γ'_C . Степень отображения j_C имеет вид $6k$, $k \in \mathbb{N}$, поэтому сумма валентностей всех $\bullet$ -, $\circ$ - или $\times$ -вершин графа Γ'_C равна $12k$. Число $3k$ называется *степенью* графа Γ_C , оно равно степени многочлена w в уравнении кривой C . Граф степени 3 называется *кубическим*.

На рисунках *вещественная часть* $\partial D \cap \Gamma$ графа Γ и ее подмножества обозначены серыми полосами.

Для графа $\Gamma \subset D$ замыкания компонент связности множества $D \setminus \Gamma$ называются *гранями* графа Γ . Грань с тремя существенными вершинами на ее границе называется *треугольной*.

Граф кривой называется *неразветвленным*, если все его $\times$ -вершины вещественны. Другими словами, неразветвленными являются графы, соответствующие максимально изогнутым кривым.

3.2. СЕГМЕНТЫ ГРАФА. Граф Γ называется *гиперболическим*, если все его вещественные ребра являются пунктирными. Он соответствует гиперболической кривой.

Объединение замыканий некоторых одинаково раскрашенных вещественных ребер графа Γ называется *сегментом*, если оно гомеоморфно отрезку. Пунктирный (жирный) сегмент называется *максимальным* если его концами являются две $\times$ -вершины (соответственно, две $\bullet$ -вершины). Напомним (см. раздел 3), что максимальный пунктирный сегмент негиперболического графа Γ , содержащий четное/нечетное количество $\circ$ -вершин, называется овалом/зигзагом; он является проекцией овала/зигзага соответствующей тригональной кривой.

Максимальный пунктирный/жирный сегмент с четным/нечетным количеством $\circ$ -вершин называется *волной/скачком*.

3.3. ЭЛЕМЕНТАРНЫЕ ПРЕОБРАЗОВАНИЯ ГРАФОВ. Два графа называются *эквивалентными*, если с точностью до гомеоморфизма f круга D их можно соединить конечной последовательностью изотопий и следующих *элементарных преобразований*:

- *монохромная модификация*, см. рис. 1 (a);
- *создание (удаление) моста*, см. рис. 1 (b), где *мост* – это пара монохромных вершин, соединенных вещественным монохромным ребром;
- $\circ$ -*in* и обратное к нему $\circ$ -*out*, см. рис. 1 (c) и (d);
- $\bullet$ -*in* и обратное к нему $\bullet$ -*out*, см. рис. 1 (e) и (f).

В первых двух случаях преобразование считается возможным, только если в результате получается граф без ориентированных монохромных циклов.

Эквивалентность двух графов называется *ограниченной*, если гомеоморфизм $f = \text{id}_D$ и указанные выше изотопии сохраняют овалы, зигзаги, волны и скачки как множества.

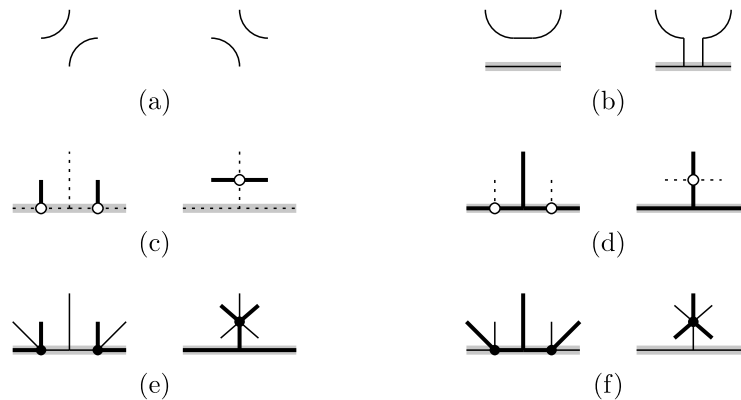


Рис. 1. Элементарные преобразования графов

Следующее утверждение доказывается так же, как и аналогичное утверждение [7, п. 5.3].

Теорема 2. *Две общие вещественные тригональные кривые деформационно эквивалентны (в классе почти общих вещественных тригональных кривых) тогда и только тогда, когда их графы эквивалентны.*

3.4. ЖЕСТКИЕ ИЗОТОПИИ И СЛАБАЯ ЭКВИВАЛЕНТНОСТЬ. Жесткая изотопия отличается от деформационной эквивалентности дополнительной парой взаимно обратных операций: выпрямлением/созданием зигзага, первая из которых состоит в слиянии двух вертикальных касательных, ограничивающих зигзаг, в одну касательную в точке перегиба с последующим превращением их в пару мнимых сопряженных слоев расслоения q . На уровне графов, эти операции показаны на рис. 2.

Определение 3. Два графа называются *слабо эквивалентными*, если они связаны последовательностью изотопий, элементарных преобразований (см. раздел 3.3) и операции *выпрямления/создания зигзага*, заключающейся в замене одного из фрагментов, показанных на рис. 2, другим.



Рис. 2. Выпрямление/создание зигзага

Следующее утверждение легко вывести из [7].

Предложение 4. *Две общие вещественные тригональные кривые жестко изотопны тогда и только тогда, когда их графы слабо эквивалентны.*

Как упоминалось в [13], следующую теорему можно вывести, например, из предложений 5.5.3 и 5.6.4 в [7] (см. также [14]).

Теорема 5. *Любая негиперболическая неособая вещественная тригональная кривая на поверхности Хирцебруха жестко изотопна максимально изогнутой.*

В рамках слабой эквивалентности графов нам понадобятся следующие два преобразования, уменьшающие число вещественных o -вершин графа:

- 1) удаление соседних скачка и зигзага, состоящее из выпрямления зигзага с последующими o - и $\bullet$ -in, а также обратное преобразование (см. рис. 3);
- 2) удаление пары соседних зигзагов, состоящее из $\bullet$ -out, и выпрямления двух зигзагов с последующими o - и $\bullet$ -in, а также обратное преобразование (см. рис. 4).

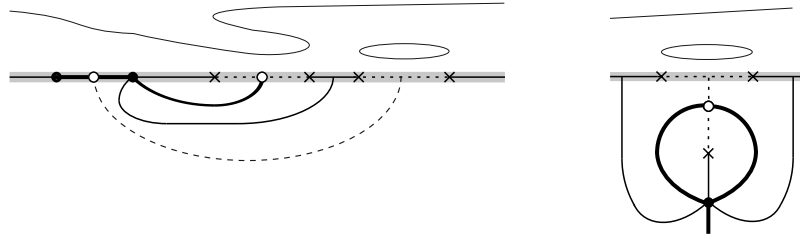


Рис. 3. Удаление/создание соседних скачка и зигзага

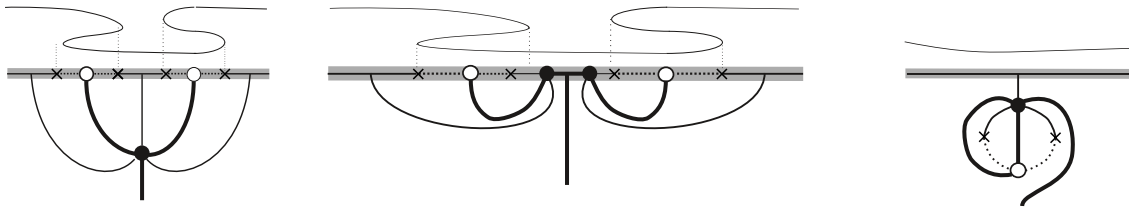


Рис. 4. Удаление/создание пары соседних зигзагов

3.5. ОСОВЫЕ ТРИГОНАЛЬНЫЕ КРИВЫЕ. Неизотривиальная тригональная кривая называется *нодально-каспидальной*, если все корни ее дискриминанта Δ имеют кратность не превосходящую трех.

Теорема 2 распространяется на вещественные нодально-каспидальные кривые и их графы (см. [11, теорема 4.26]).

Нетрудно проверить, что [8, теорема 3] распространяется на вещественные нодально-каспидальные кривые без мнимых особенностей:

Теорема 6. Любая вещественная нодально-каспидальная негиперболическая кривая без мнимых особенностей жестко изотопна максимально изогнутой.

Назовем *особыми* вершины графа, отвечающие особым точкам кривой. Вещественные особые $\times$ -вершины, к которым примыкают сплошные ребра, т.е. отвечающие изолированным особым точкам кривой (“вырожденным овалам”), назовем *изолированными* и включим их в число максимальных пунктирных сегментов.

Предложение 7. На вещественном отрезке без o -вершин изолированную особую точку можно поменять местами с овалом.

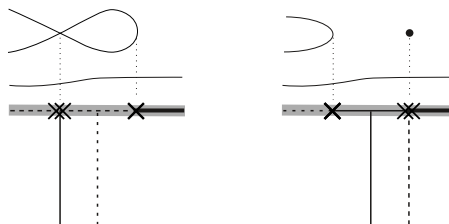


Рис. 5. Прохождение нодальной точки через касп

Доказательство. На таком отрезке все $\bullet$ -вершины встречаются парами, которые можно удалить с отрезка с помощью $\bullet$ -in. После этого преобразование на рис. 5 меняет местами изолированную особую точку и овал. $\square$

3.6. РАЗРЕЗЫ. Для $j = 1, 2$ пусть D_j – диск, $\Gamma_j \subset D_j$ – граф нодально-каспидальной кривой, $I_j \subset \partial D_j$ – отрезок и $\varphi : I_1 \rightarrow I_2$ – изоморфизм, то есть диффеоморфизм отрезков устанавливающий изоморфизм графов $\Gamma_1 \cap I_1 \rightarrow \Gamma_2 \cap I_2$. Рассмотрим фактор-множество $D_\varphi = (D_1 \sqcup D_2) / \{x \sim \varphi(x)\}$ и образ $\Gamma'_\varphi \subset D_\varphi$ графа $\Gamma_1 \cup \Gamma_2$. Обозначим через Γ_φ граф, полученный из Γ'_φ удалением образа отрезка I_1 , если φ меняет ориентацию, а если не меняет, то либо преобразованием образов концов отрезка I_1 в монокромные вершины, либо сохранением этих концов в качестве существенных вершин.

В дальнейшем мы всегда считаем, что I_j является частью ребра графа Γ_j (см. рис. 7), или I_j содержит одну $\circ$ -вершину, или заканчивается в особых вершинах и содержит одну монокромную вершину (см. рис. 6). С точностью до изотопии во втором и третьем случаях изоморфизм φ единственен; в первом случае для этого надо еще указать, сохраняет ли φ ориентацию или обращает ее. Если Γ_φ – граф тригональной кривой, его называют результатом *склейки* графов Γ_1, Γ_2 вдоль φ . Образ I_1 называется *разрезом* в Γ_φ . Разрез называется *естественным* (*искусственным*), если φ сохраняет (соответственно, обращает) ориентацию; он называется *сплошным*, *пунктирным* или *жирным* в зависимости от структуры отрезка $\Gamma \cap I_1$. (Названия пунктирный и жирный по-прежнему применяются к разрезам, содержащим $\circ$ -вершину.) *Контактом* называется естественный разрез, полученный склейкой двух графов вдоль изоморфных частей их зигзагов (см. левый рис. 6).



Рис. 6. Примеры естественного склеивания



Рис. 7. Примеры искусственного склеивания

4. Скелеты

Неразветвленные графы можно свести к более простым объектам, так называемым скелетам, которые получаются игнорированием всех ребер, кроме пунктирных.

Ниже понятие скелета, введенное в [8] для максимально изогнутых тригональных кривых, распространяется на случай графа кривой, полученной из максимально изогнутой преобразованиями на рис. 3 и рис. 4, добавлением внутренних неизолированных белых и крестовых вершин скелета (см. определение 9).

4.1. АБСТРАКТНЫЕ СКЕЛЕТЫ. Рассмотрим вложенный в круг D (конечный) граф $Sk \subset D$. Мы не исключаем возможности того, что некоторые вершины Sk принадлежат границе D ; такие вершины называются *вещественными*, остальные называются *мнимыми* или *внутренними*. Набор ребер, смежных с каждой вещественной (соответственно внутренней) вершиной v графа Sk получает от D пару противоположных линейных (соответственно циклических) порядков. *Непосредственные соседи* ребра e в вершине v – это непосредственные предшественник и преемник этого ребра относительно (любого) из этих порядков. *Первососедний путь* в Sk – это последовательность ориентированных ребер графа Sk , в которой за каждым ребром следует одно из его непосредственных соседних ребер.

Ниже рассматриваются графы с ребрами двух видов: ориентированными и неориентированными. Мы называем такие графы *частично ориентированными*. Ориентированные и неориентированные части (объединения соответствующих ребер и соседних вершин) частично ориентированного графа Sk обозначаются через Sk_{dir} и Sk_{ud} соответственно.

Определение 8. Пусть D – круг. *Абстрактный скелет* – это частично ориентированный вложенный граф $Sk \subset D$, не пересекающийся с ∂D за исключением некоторых вершин, и удовлетворяющий следующим условиям:

- 1) каждая вершина является *белой*, *черной* или *крестовой*; валентность любой мнимой белой вершины равна двум, любая мнимая черная вершина является изолированной, любая крестовая вершина является мнимой одновалентной и соединена входящим в нее ребром, исходящим из мнимой белой вершины; любое ребро, смежное с вещественной черной вершиной (называемой *источником*), является исходящим; оба ребра, смежных с мнимой белой вершиной, являются исходящими;
- 2) любая изолированная черная/белая вершина принадлежит Sk_{dir} / Sk_{ud} ;
- 3) любой непосредственный сосед входящего ребра – исходящее ребро;
- 4) Sk не имеет первососедних циклов;
- 5) множество вещественных вершин графа Sk непусто;
- 6) $b_1 + 3b = v + z + i$ для любой открытой грани R , т. е. компоненты дополнения в D объединения замыканий всех ребер графа Sk , где b_1 – количество лежащих на границе FrR грани R черных вершин, каждая из которых инцидентна одному

исходящему из нее ребру, лежащему на $\text{Fr}R$, b – количество изолированных (вещественных или мнимых) черных вершин в R , v – количество черных вершин на $\text{Fr}R$, каждая из которых инцидентна двум исходящим из нее ребрам, лежащим на $\text{Fr}R$, z – количество компонент связности множества $\text{Sk}_{\text{ud}} \cap \text{Fr}R$, i – количество мнимых белых вершин на $\text{Fr}R$, причем такая вершина считается дважды, если смежные с ней ребра на $\text{Fr}R$ являются внутренними, т. е. R примыкает к ним с двух сторон.

Если дополнительно

- 7) $\text{Sk}_{\text{dir}} \cap \text{Sk}_{\text{ud}} = \emptyset$;
- 8) в каждой вещественной вершине нет ориентированных исходящих ребер, являющихся непосредственными соседями;
- 9) каждая вещественная белая вершина Sk_{dir} имеет нечетную валентность и является *стоком*, что означает, что число соседних входящих в нее ребер на единицу больше числа исходящих;
- 10) каждая черная вершина вещественна и одновалентна (т. е. является источником);
- 11) вершины подграфов Sk_{dir} и Sk_{ud} чередуются вдоль ∂D ,
то Sk называется скелетом *типа I*.

4.2. ЭКВИВАЛЕНТНОСТЬ АБСТРАКТНЫХ СКЕЛЕТОВ. Два абстрактных скелета называются *эквивалентными*, если с точностью до гомеоморфизма $f : D \rightarrow D$ они могут быть связаны следующими *элементарными преобразованиями* (ср. раздел 3.3):

- *элементарная модификация*, см. рис. 8 (a);
- *создание (удаление) моста*, см. рис. 8 (b); вершина, показанная на рисунке, является белой, к ней могут примыкать и другие ребра скелета Sk ;
- *создание (удаление) неориентированного ребра*, см. рис. 8 (c); вершина, показанная на рисунке, является черной вещественной, примыкающие к ней ребра являются непосредственными соседями, кроме которых к ней могут примыкать и другие ориентированные исходящие ребра; ребро в правой части рисунка неориентированное;
- *$\bullet$ -in и обратное к нему $\bullet$ -out*, см. рис. 8 (d), (e); все вершины показанные на этих рисунках черные, на рисунке (d) могут присутствовать другие ориентированные исходящие ребра, примыкающие к вещественным вершинам;
- *удаление/создание соседних скачка и зигзага*, см. рис. 8 (f);
- *удаление/создание пары соседних зигзагов*, см. рис. 8 (g);
- *преобразование пары ориентированных ребер в неориентированное ребро и обратное преобразование*, см. рис. 8 (h).

Преобразование выполнимо только в том случае, если результатом опять является абстрактный скелет.

Эквивалентность двух абстрактных скелетов на одном круге с тем же набором вер-

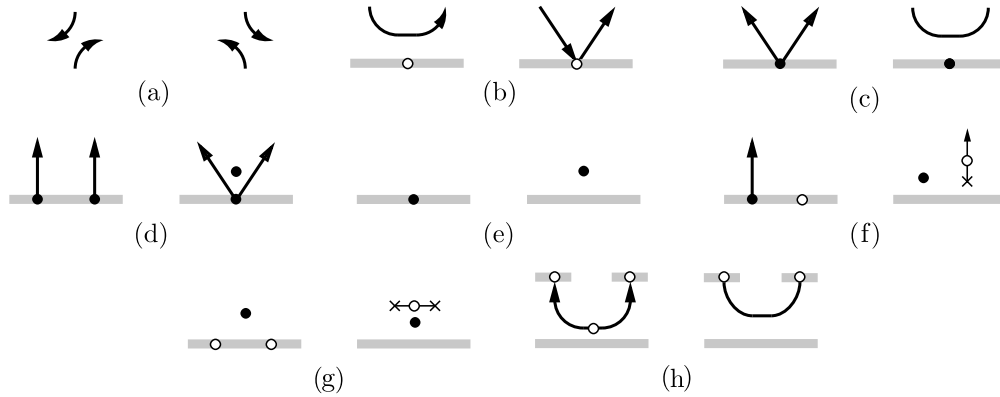


Рис. 8. Преобразования скелетов

шин называется *ограниченной*, если гомеоморфизм $f = \text{id}$ и указанные выше изотопии можно выбрать тождественными на вершинах.

4.3. ПУНКТИРНЫЕ СКЕЛЕТЫ. Интуитивно, пунктирный скелет (см. определение 9) получается из графа Γ некоторой общей тригональной кривой удалением всех ребер, кроме пунктирных, склейкой последних в вещественных $\circ$ -вершинах и добавлением мнимых $\bullet$ -, $\circ$ - и $\times$ -вершин. При этом неориентированные ребра скелета отвечают контактам графа Γ .

Определение 9. Пусть $\Gamma \subset D$ – неразветвленный граф или граф, полученный из неразветвленного удалением некоторых пар, состоящих из соседних скачка и зигзага, или пар соседних зигзагов (см. рис. 3, рис. 4). Пусть $\bar{D}$ – это круг, полученный из D стягиванием каждого максимального пунктирного/жирного сегмента в точку. (Пунктирный) скелет графа Γ представляет собой частично ориентированный граф $\text{Sk} = \text{Sk}_\Gamma \subset \bar{D}$, полученный из Γ следующим образом:

- каждый максимальный пунктирный/жирный сегмент стягивается в точку, которая объявляется белой/черной вершиной скелета Sk ;
- каждая внутренняя $\bullet$ -/ $\times$ -вершина графа Γ заменяется внутренней черной/крестовой вершиной скелета Sk ;
- каждая внутренняя $\circ$ -вершина графа Γ , не лежащая на контакте заменяется внутренней белой вершиной скелета Sk , а примыкающие к ней пунктирные ребра заменяются ориентированными ребрами скелета, направленными от этой белой вершины к крестовой или белой вещественной вершинам;
- каждый контакт заменяется неориентированным ребром скелета Sk , а каждое из не упомянутых выше внутренних пунктирных ребер графа Γ заменяется ориентированным ребром скелета Sk с ориентацией, полученной из ориентации пунктирного ребра;
- Sk_{dir} (Sk_{ud}) является объединением черных (соответственно белых) изолированных вершин и замыканий ориентированных (соответственно, неориентированных) ребер скелета Sk (так что Sk_{dir} и Sk_{ud} могут пересекаться в вещественных вершинах).

Следующие утверждения доказываются так же, как и утверждения [8, предложения 5–7, теорема 2].

Предложение 10. *Скелет Sk графа Γ из определения 9 представляет собой абстрактный скелет в смысле определения 8.*

Предложение 11. *Любой абстрактный скелет Sk является скелетом некоторого графа Γ в смысле определения 9; любые два таких графа можно соединить последовательностью изотопий и элементарных преобразований (см. раздел 3.3) сохраняющих скелет.*

Предложение 12. *Пусть скелеты Sk_1 и Sk_2 с одинаковым набором вершин получены из графов $\Gamma_1, \Gamma_2 \subset D$ в соответствии с определением 9. Тогда Γ_1 и Γ_2 связаны ограниченной эквивалентностью в том и только в том случае, когда соответствующие скелеты Sk_1 и Sk_2 ограниченно эквивалентны.*

Теорема 13. *Существует каноническая биекция между множеством классов жесткой изотопии почти общих вещественных тригональных кривых и множеством классов эквивалентности абстрактных скелетов.*

5. Конструктивное описание максимально изогнутых тригональных кривых

В этом разделе дается конструктивное описание вещественных частей неособых максимально изогнутых тригональных кривых.

5.1. Блоки. Рассмотрим класс неразветвленных графов, задаваемых конструктивно согласно следующему определению.

Определение 14. *Кубическим блоком типа I называется неразветвленный граф степени 3 типа I (см. рис. 9 I). Кубическим блоком типа II называется неразветвленный граф степени 3 типа II с внутренней $\bullet$ -вершиной (см. рис. 9 II). Несколько кубических блоков, искусственно склеенных вдоль отрезков сплошных ребер, образуют (общий) блок. Тип блока – это тип кривой, соответствующей блоку.*

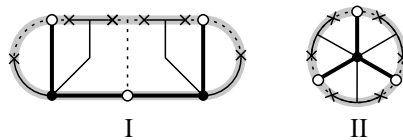


Рис. 9. Кубические блоки

Согласно [7, 5.6.7] и [8, 5.1], оба кубических блока единственны с точностью до изоморфизма.

Следующее предложение [8, предложение 8] дает описание блоков.

Предложение 15. Пусть $d \geq 1$ – целое число, и пусть $O, J \subset S^1 = \partial D$ – два непересекающихся d -элементных множества. Тогда существует единственный, с точностью до ограниченной эквивалентности, блок $\Gamma \subset D$ типа I и степени $3d$ с овалом вокруг каждой точки из O , скачком в вокруг каждой точки из J и зигзагом между любыми двумя точками $O \cup J$ (и без других пунктирных и жирных сегментов).

Блок степени $3d$ произвольного типа с c скачками, с овалами, b внутренними $\bullet$ -вершинами и z зигзагами соответствует абстрактному скелету в круге с c ориентированными непересекающимися хордами, b внутренними черными вершинами и z вещественными изолированными белыми вершинами, которые удовлетворяют следующим условиям:

- 1) $b + c = d$, $z + c = 3d$;
- 2) для каждой компоненты R_i замкнутого разреза круга по хордам, $z_i = c_i + 3b_i$, где c_i , b_i и z_i – число хорд, черных внутренних вершин и вещественных изолированных вершин этой компоненты.

Замечание 16. Из этого описания сразу следует, что естественную склейку двух блоков по жирным отрезкам можно заменить либо контактом двух других блоков, составленных из частей прежних блоков, либо искусственной склейкой вдоль отрезков сплошных ребер, т. е. новым блоком.

5.2. ВЕЩЕСТВЕННЫЕ ЧАСТИ МАКСИМАЛЬНО ИЗОГНУТЫХ КРИВЫХ. Полное описание вещественной части максимально изогнутой неособой тригональной кривой, т. е. описание топологии пары $(\mathbb{R}\Sigma_k, \mathbb{R}C)$, дано в [8, 5.3] и, с учетом замечания 16, выглядит следующим образом: граф максимально изогнутой кривой получается из дизъюнктного объединения блоков с помощью контактов, преобразующих круги блоков в один круг. При этом если все блоки имеют тип I и все склейки являются контактами, получается граф типа I, в противном случае – граф типа II.

5.3. БЛОКИ И СЛАБАЯ ЭКВИВАЛЕНТНОСТЬ ГРАФОВ. Согласно [8, предложение 10, лемма 1] для любого $d \geq 1$ существует единственный, с точностью до слабой эквивалентности, блок $\Gamma \subset D$ типа I степени $3d$.

Теорема 17. Блок типа II с не менее, чем двумя овалами слабо эквивалентен графу с контактом.

Доказательство. Пусть B – блок типа II и $d \geq 2$ – его степень. Если в B имеются два скачка, соединенных сплошным сегментом, то контакт получается после преобразований на рис. 8 (d), (c) скелета блока B . В противном случае каждый скачок имеет свой соседний зигзаг, и все скачки можно устранить с помощью преобразования на рис. 8 (f), получив, согласно предложению 15, граф с d (мнимыми) $\bullet$ -вершинами, с овалами и z зигзагами, $c \leq d$, $z \geq d$. Если после этого зигзаги будут чередоваться с овалами, то обратное преобразование возвращает к блоку типа I согласно тому же предложению. Поэтому B содержит

два соседних овала, между которыми (хотя бы на одном из вещественных отрезков) лежит $r \geq 2$ зигзагов. Применим к $[r/2]$ тройкам, состоящим из пары этих зигзагов и $\bullet$ -вершины, преобразование на рис. 8 (g). В зависимости от того, четно r или нет, преобразуем скелет полученного графа согласно рис. 10 или рис. 11. $\square$

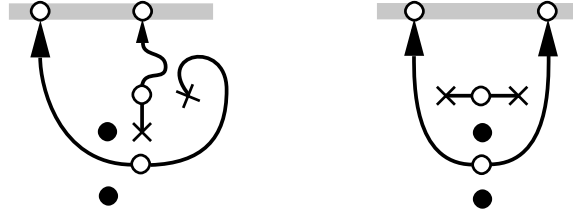


Рис. 10. Контакт с кубическим блоком типа II

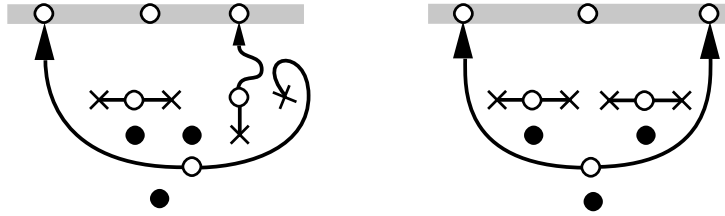


Рис. 11. Контакт с блоком степени 6

6. Особые кривые бистепени $(4,3)$ на гиперboloиде и собственные тригональные кривые

Хорошо известно (см., например, [11, 3.1.1]), что положительное и отрицательное преобразования Нагаты устанавливают соответствие между (тригональными) кривыми бистепени $(m, 3)$ на гиперboloиде и собственными тригональными кривыми: кривой $C \subset \Sigma_0$ отвечает ее образ $N(C) \subset \Sigma_m$ при положительном преобразовании Нагаты, раздувающим точки пересечения кривой C с кривой $E_0 \subset \Sigma_0 = \mathbb{P}^1 \times \mathbb{P}^1$.

Перечислим стенки в пространстве $C_{4,3}$ и найдем соответствие между жесткими изотопиями кривых в стенке и преобразованиями графов соответствующих собственных тригональных кривых.

6.1. СТЕНКИ В ПРОСТРАНСТВЕ $C_{4,3}$. На рис. 12, рис. 13, рис. 14 в обозначениях работы [1] указаны вещественные схемы кривых классов $\omega_{inn}^\pm$, $\omega_{out}^\pm$, $\tilde{\omega}$, $\gamma_{inn}^\pm$, $\gamma_{out}^\pm$, $\tilde{\gamma}$, $\alpha_{lp}^\pm\langle l \rangle$, $\alpha_{ov}^\pm\langle l \rangle$, $\tilde{\alpha}\langle l \rangle$ в пространстве $C_{4,3}$, отмеченные верхним индексом “+” (для кривых классов γ_{out}^+ , α_{lp}^+ , $\tilde{\alpha}$ показаны схемы с изолированной особой точкой). Схемы с верхним индексом “−” получаются отражением относительно вертикального слоя. Графы и скелеты на этих рисунках описываются ниже.

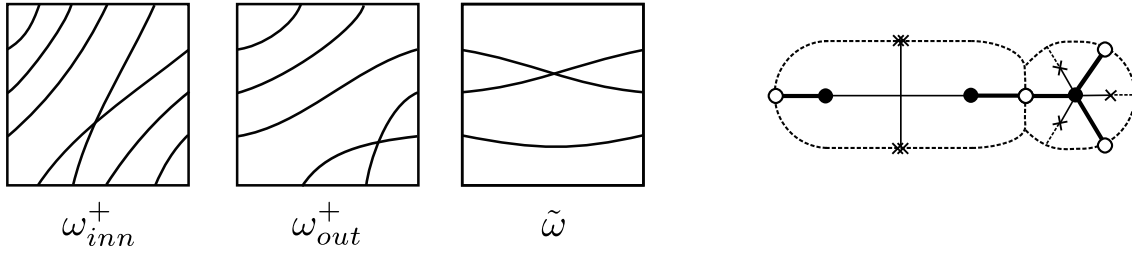


Рис. 12. Вещественные схемы кривых классов ω_{inn}^+ , ω_{out}^+ , $\tilde{\omega}$ и граф соответствующей тригональной кривой

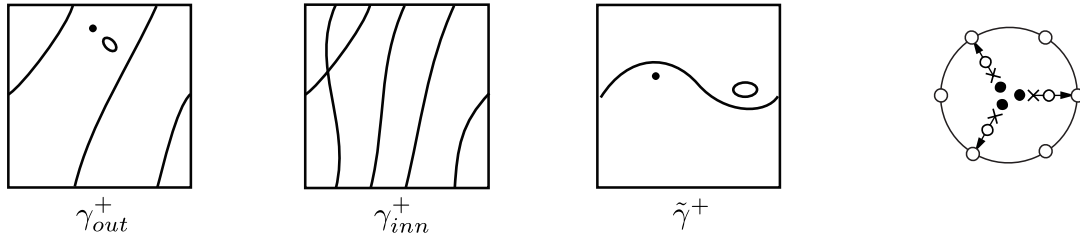


Рис. 13. Вещественные схемы кривых классов γ_{inn}^+ , γ_{out}^+ , $\tilde{\gamma}$ и скелет соответствующей тригональной кривой

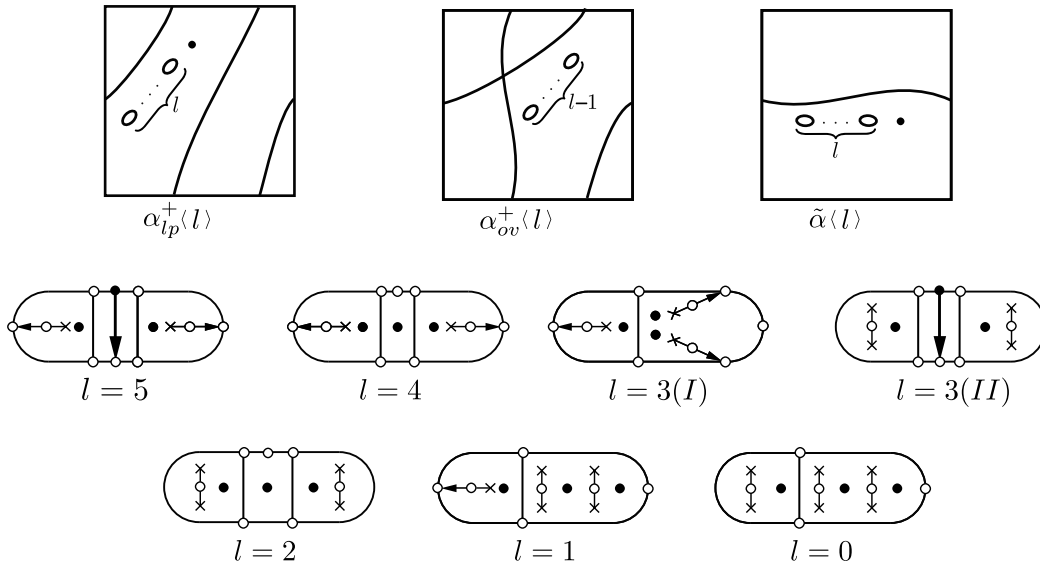


Рис. 14. Вещественные схемы кривых классов $\alpha_{lp}^+ \langle l \rangle$, $\alpha_{ov}^+ \langle l \rangle$, $\tilde{\alpha} \langle l \rangle$ и скелеты соответствующих тригональных кривых

В работе [1] доказано, что каждая из комплексных схем $\omega_{out}^\pm$, $\tilde{\omega}$, $\gamma_{inn}^\pm$, $\gamma_{out}^\pm$, $\tilde{\gamma}^\pm$, $\alpha_{ov}^\pm B$ ($B = \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle_I^\pm, \langle 3 \rangle_{II}, \langle 4 \rangle, \langle 5 \rangle^\pm$), $\tilde{\alpha} B$ ($B = \langle 0 \rangle, \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle_I, \langle 3 \rangle_{II}, \langle 4 \rangle, \langle 5 \rangle$) отвечает единственной стенке. То же самое осталось доказать для комплексных схем $\{\omega_{inn}^\pm, \alpha_{lp}^\pm B$ ($B = \langle 0 \rangle, \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle_I, \langle 3 \rangle_{II}, \langle 4 \rangle, \langle 5 \rangle$).

6.2. ОСОБЫЕ СЛОИ И ПРЕОБРАЗОВАНИЯ НАГАТЫ. Для получения с помощью преобразования Нагаты собственной тригональной кривой на Σ_3 из особой кривой $C \in \Delta \setminus S$ бистепени $(4, 3)$ на гиперboloиде в качестве исключительного сечения E_0 возьмем кривую бистепени $(0, 1)$, проходящую через особую точку кривой C , и рассмотрим на гиперboloиде карту (x, y) , где E_0 и особый слой F задаются уравнениями $y = \infty$ и $x = 0$. Тогда положительное преобразование Нагаты N с центром в точке $p = F \cap C \cap E_0$ задается равенством $(x, z) = (x, xy)$. Ниже кривая C и ее образ $N(C)$ задаются локальными уравнениями с указанием лишь необходимых начальных членов. Для кривых из классов $\omega_{inn}^\pm$, $\alpha_{lp}^\pm$ нам понадобятся преобразования Нагаты следующих особых слоев (слои $N(F)$ и $N^2(F)$ кривых $N(C)$ и $N^2(C)$ обозначены в соответствии с [11, 3.1.2]):

- 1) p – невырожденная двойная точка, в которой кривая C не касается ни F , ни E_0 .
 $C : x^2y^3 + y + 1 = 0$, $N(C) : z^3 + z + x = 0$, слой $N(F) : \tilde{A}_0$;
- 2) p – невырожденная двойная точка, в которой кривая C касается слоя F и не касается E_0 .
 $C : x^2y^3 + xy^2 + 1 = 0$, $N(C) : z^3 + z^2 + x = 0$, слой $N(F) : \tilde{A}_0^*$;
- 3) p – невырожденная двойная точка, в которой кривая C касается E_0 и не касается F .
 $C : x^3y^3 + xy^2 + y + 1 = 0$, $N^2(C) : z^3 + z^2 + xz + x^3 = 0$, слой $N^2(F) : \tilde{A}_1$;
- 4) p – невырожденная двойная точка, в которой кривая C касается как E_0 , так и F .
 $C : x^3y^3 + xy^2 + 1 = 0$, $N^2(C) : z^3 + z^2 + xz + x^3 = 0$, слой $N^2(F) : \tilde{A}_2$;
- 5) p – точка возврата, касательная в которой не совпадает ни с E_0 , ни с F .
 $C : x^2y^3 + 2xy^2 + y + x^2y^2 + 1 = 0$, $N(C) : z^3 + 2z^2 + z + xz^2 + x = 0$, слой $N(F) : \tilde{A}_0^*$;
- 6) p – точка возврата с вертикальной касательной.
 $C : x^2y^3 + 1 = 0$, $N(C) : z^3 + x = 0$, слой $N(F) : \tilde{A}_0^{**}$;
- 7) p – точка возврата с горизонтальной касательной.
 $C : x^3y^3 + y + 1 = 0$, $N^2(C) : z^3 + xz + x^3 = 0$, слой $N^2(F) : \tilde{A}_1^*$;
- 8) p – неособая точка кривой C с невертикальной и негоризонтальной касательной, а F пересекается с C в трех различных точках.
 $C : xy^3 + y^2 + 1 = 0$, $N(C) : z^3 + z^2 + x^2 = 0$, слой $N(F) : \tilde{A}_1$;
- 9) p – неособая точка кривой C с невертикальной и негоризонтальной касательной, а F касается кривой C (в точке, отличной от p).
 $C : xy^3 + y^2 + x = 0$, $N(C) : z^3 + z^2 + x^3 = 0$, слой $N(F) : \tilde{A}_2$;
- 10) p – неособая точка кривой C с вертикальной касательной и F пересекает кривую C в точке, отличной от p .
 $C : xy^3 + y + x = 0$, $N(C) : z^3 + xz + x^3 = 0$, слой $N(F) : \tilde{A}_1^*$;
- 11) p – точка перегиба кривой C с вертикальной касательной.
 $C : xy^3 + 1 = 0$, $N(C) : z^3 + x^2 = 0$, слой $N(F) : \tilde{A}_2^*$.

6.3. КРИВЫЕ $\omega_{inn}^\pm$. Кривая $C \in \omega_{inn}^\pm$ является гиперболической. Ее вещественную схему можно получить объединением вещественных схем $\langle(2, 3)\rangle$ и $\langle(1, 1)\rangle$ неособых ветвей

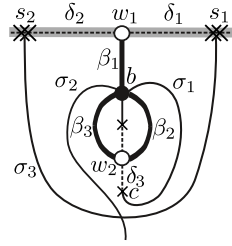


Рис. 15. Сплошной разрез

кривой, трансверсально пересекающихся в одной точке p (см. рис. 12). Поэтому кривая C имеет три особых слоя: два слоя вида 8) и слой F_p вида 1) из раздела 6.2. Следовательно, кривая $N_3(C) \subset \Sigma_3$, где N_3 – композиция трех положительных преобразований Нагаты, имеет две различные крестовые особые точки и неособую точку $a \in N_3(F_p)$, лежащую на образе ветви $(2, 3)$ (на той ее дуге, ограниченной особыми точками, которая имеет четную кратность пересечения с прямой $y = 0$).

Лемма 18. *Граф кривой $N_3(C)$ эквивалентен графу с естественным сплошным разрезом, соединяющим мнимую сплошную вершину с особыми вершинами.*

Доказательство. Так как степень 9 графа кривой $N_3(C)$ нечетна, он имеет нечетное число о-вершин. На вещественном отрезке графа, ограниченном особыми вершинами s_1, s_2 и имеющем нечетное число о-вершин, удалим все эти о-вершины, кроме одной, с помощью о-in и удалим появившиеся возможно мосты. Оставшаяся о-вершина w_1 соединена вещественными ребрами δ_1, δ_2 с s_1, s_2 и жирным ребром β_1 с некоторой $\bullet$ -вершиной b . Пусть β_2, β_3 – другие жирные ребра, исходящие из b (см. рис. 15), и w_2 – о-вершина, являющаяся концом ребра β_2 . Сделав при необходимости монохромные преобразования, получаем, что w_2 будет концом ребра β_3 и концом пути $b, \sigma_1, c, \delta_3, w_2$, где σ_1 – сплошное ребро, лежащее между β_1 и β_2 , c – $\times$ -вершина, δ_3 – пунктирное ребро. Соединим вершины b и s_1 сплошным ребром σ_2 , сделав, если нужно, монохромное преобразование. Грань полученного графа, содержащая на границе путь $s_1, \sigma_2, b, \beta_1, \delta_2, s_2, \sigma_3$, где σ_3 – сплошное ребро, не является треугольной, поэтому в ходе (сплошного) монохромного преобразования ребер σ_2, σ_3 можно остановиться в промежуточном положении, создав мнимую монохромную вершину и, тем самым, искомый разрез. $\square$

Замечание 19. Слой $N_3(F_p)$ отвечает точке графа кривой $N_3(C)$, лежащей на вещественном отрезке графа, ограниченном особыми вершинами s_1, s_2 и имеющем четное число о-вершин, иначе существует преобразование графа, переводящее s_1, s_2 в мнимую особую вершину, что невозможно, согласно сказанному в начале раздела 6.3.

Теорема 20. *Каждый из классов ω_{inn}^+ и ω_{inn}^- связан, т. е. состоит из одной стенки.*

Доказательство. После разреза, указанного в лемме 18, получаются кубический граф типа II и граф степени 6 с одним овалом, которые по теореме 5 слабо эквивалентны

соответствующим блокам (см. граф на рис. 12). Последние единственны с точностью до слабой эквивалентности согласно [8, предложение 8, лемма 1].

Если по собственной тригональной кривой кривая ω_{inn}^- построена, то кривую, симметричную кривой C относительно E_0 , можно получить из кривой, которая в аффинной карте $\Sigma_3 \setminus (E_3 \cup N_3(F_p))$ симметрична кривой $N_3(C)$ относительно оси x , и имеет, очевидно, тот же граф, что и кривая $N_3(C)$. $\square$

Замечание 21. Кривые из классов $\omega_{out}^\pm$, $\tilde{\omega}$ отличаются от кривой $C \in \omega_{inn}^\pm$ лишь выбором точки $a \in N_3(C)$ (на дуге образа ветви $(2, 1)$, ограниченной особыми точками, которая имеет нечетную кратность пересечения с прямой $y = 0$ – для классов $\omega_{out}^\pm$; на образе ветви $(1, 0)$ – для класса $\tilde{\omega}$). Поэтому те же аргументы доказывают связность и этих классов.

6.4. КРИВЫЕ $\alpha_{lp}^\pm \langle l \rangle$. Кривая $C \in \alpha_{lp}^\pm \langle l \rangle$ является негиперболической. Ее вещественная часть содержит (возможно особую) ветвь, реализующую класс $(1, \pm 2)$ в $H_1(\mathbb{R}X)$, и l овалов, если особая точка не лежит на овале (см. рис. 14). Поэтому кривая C имеет либо три особых слоя: два слоя видов 8)-11) и слой F_p одного из видов 1), 2), 5), 6) из раздела 6.2, либо два особых слоя: слой одного из видов 8)-11) и слой F_p одного из видов 3), 4), 7). Следовательно, собственная тригональная кривая $N_3(C) \subset \Sigma_3$ имеет особые слои, перечисленные в разделе 6.2. Для возвращения к кривой C с помощью отрицательных преобразований Нагаты надо раздуть особые точки кривой $N_3(C)$ и точку a , лежащую на образе ветви $(1, \pm 2)$ (на той ее дуге, ограниченной особыми точками, которая имеет четную кратность пересечения с прямой $y = 0$).

Замечание 22. При $l = 1$ кривая C принадлежит типу II. Кривая типа I с похожей вещественной схемой (см. рис. 13) принадлежит одной из стенок $\gamma_{out}^\pm$. Единственность последних, как и стенок $\tilde{\gamma}^\pm$, $\gamma_{inn}^\pm$, следует из единственности (см. [8, предложение 10, лемма 1]) блока степени 9, имеющего тип I, со скелетом на рис. 13, поскольку эти стенки отличаются лишь выбором точки $a \in N_3(C)$ (на дуге образа ветви $(1, \pm 2)$, ограниченной особыми точками, которая имеет четную/нечетную кратность пересечения с прямой $y = 0$ – для стенок $\gamma_{out}^\pm/\tilde{\gamma}^\pm$; на овале – для стенок $\gamma_{inn}^\pm$).

Лемма 23. *Существует нодально-каскадальная кривая с двумя невырожденными изолированными особыми точками, жестко изотопная кривой $N_3(C)$.*

Доказательство. Особые точки кривой $N_3(C)$ отвечают особым вершинам ее графа. Пусть особая вершина s не является изолированной. Если s соединена вещественным пунктирным ребром с (неособой) $\times$ -вершиной, то s можно превратить в изолированную вершину с помощью преобразования на рис. 5.

Пусть теперь особая вершина s соединена с двумя $\times$ -вершинами вещественными пунктирными отрезками, содержащими нечетное число o -вершин. С помощью o -in оставим по одной o -вершине на этих отрезках. Согласно теореме 6 граф кривой $N_3(C)$ является неразветвленным, поэтому результат Γ его возмущения, превращающего особые вершины в овалы, распадается на блоки после естественных разрезов по пунктирным ребрам

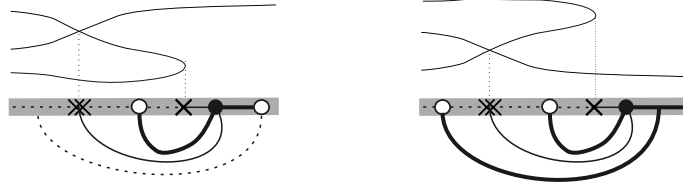


Рис. 16. Прохождение нодальной точки через точку $\tilde{A}_1^*$

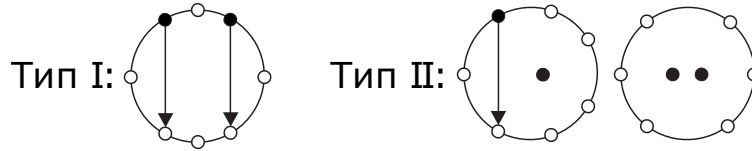


Рис. 17. Блоки степени 6 с точностью до слабой эквивалентности

(см. раздел 5.2). Следовательно, сплошной отрезок, полученный из s , лежит в одном из блоков между двумя зигзагами; поэтому блок имеет тип II и по теореме 17 имеет не более одного овала. Следовательно, рядом с одним из зигзагов лежит скачок. Возвращаясь к графу кривой $N_3(C)$ и применяя к фрагменту графа, содержащему $\bullet$ -вершину этого скачка, преобразования на рис. 16 и рис. 5, получаем изолированную особую вершину. Наконец, последний возможный случай, препятствующий применить преобразование на рис. 5 сразу, – это когда обе особые вершины s_1, s_2 лежат между двумя $\times$ -вершинами на одном пунктирном отрезке и разбивают его на три отрезка, содержащих нечетное число $\circ$ -вершин (поскольку для кривой C тоже, очевидно, справедливо замечание 19, между s_1, s_2 лежит нечетное число $\circ$ -вершин). С помощью $\circ$ -in оставим по одной $\circ$ -вершине на этих отрезках. Те же аргументы, что и в предыдущем случае, показывают, что рядом с одной из крайних $\times$ -вершин лежит скачок, поэтому применение преобразования на рис. 16 удаляет $\circ$ -вершину между s_1, s_2 , приводя к графу кривой, не лежащей в $\alpha_{lp}^\pm\langle l \rangle$ в силу замечания 19. $\square$

Используя доказанную лемму будем далее считать, что особые вершины графа $N_3(C)$ отвечают изолированным особым точкам. Обозначим через Γ результат возмущения этого графа, превращающего особые вершины в овалы.

Лемма 24. *Граф кривой $N_3(C)$ слабо эквивалентен графу с единственной вещественной $\circ$ -вершиной.*

Доказательство. Согласно замечанию 22 граф Γ не может быть блоком типа I, поэтому по теореме 17 граф является контактом трех кубических блоков или кубического блока и блока степени 6 (см. рис. 17). Преобразования на рис. 3, рис. 4 в крайних блоках в первом случае и в обоих блоках во втором с последующим стягиванием двух овалов в особые точки дают нужный граф. $\square$

Теорема 25. Стенка в классе кривых $\alpha_{lp}^{\pm}\langle l \rangle$ однозначно определяется комплексной схемой.

Доказательство. После преобразования, указанного в лемме 24, особые вершины можно менять местами с любыми овалами согласно предложению 7. Поэтому достаточно доказать теорему для графа Γ . Рассмотрим все значения l . Скелеты изучаемых ниже графов указаны на рис. 14.

- 1) При $l = 5$ в силу [8, лемма 1] граф Γ единственен с точностью до слабой эквивалентности как граф M -кривой.
- 2) При $l = 4$ в силу [7, 6.4.2] и [8, лемма 1] граф Γ единственен с точностью до слабой эквивалентности как граф $(M - 1)$ -кривой.
- 3) При $l = 3$, как уже говорилось в доказательстве леммы 24, граф Γ является контактом кубического блока K и графа B степени 6. При этом если Γ принадлежит типу I, K и B являются блоками типа I, единственными с точностью до слабой эквивалентности по [8, предложение 8, лемма 1]. Если Γ принадлежит типу II, B содержит контакт по теореме 17, иначе он был бы блоком типа I с двумя овалами и потому K тоже был бы блоком типа I. Поэтому Γ – контакт трех кубических блоков, один имеет тип I, а два – тип II. Объединение блока типа I и блока типа II дает граф $(M - 1)$ -кривой, в котором блоки можно переставить согласно [7, 6.4.2]. Следовательно, Γ эквивалентен графу с центральным кубическим блоком типа I и потому единственен.
- 4) При $l = 2$, как и при $l = 3$, граф Γ является контактом кубического блока K и графа B степени 6. Если K принадлежит типу I, следующие преобразования скелета графа Γ позволяют получить контакт с концами в соседних овалах, превратив K в кубический блок типа II: преобразования (f), (g) на рис. 8, примененные к K и B , преобразование (h) на рис. 8, примененное к контакту, преобразование (a) на рис. 8, примененное к ребрам e_1, e_2 на рис. 18, преобразование на рис. 10, примененное к ребрам e'_1, e_3 на рис. 18.

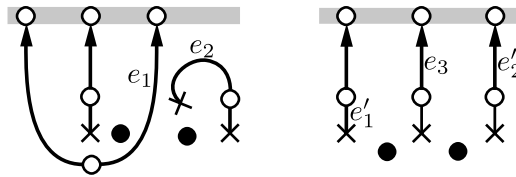


Рис. 18. Контакт с кубическим блоком типа I

- 5) При $l = 1$ граф Γ является контактом кубического блока K и блока B степени 6. Если K принадлежит типу I, такие же преобразования скелета графа Γ , как и при $l = 2$, переносят овал из K в B , помещая его рядом с любым из концов контакта. Обратные преобразования и преобразование на рис. 8 (g) дают скелет, указанный на рис. 14 ($l = 1$). Поэтому единственность Γ следует из его эквивалентности контакту кубического блока типа I и блока степени 6 без овалов.

- 6) При $l = 0$ граф Γ является контактом кубического блока K типа II и блока B степени 6 без овалов и потому единственен.

Если по собственной тригональной кривой кривая $C \in \alpha_{lp}^+(l)$ построена, то кривую из $\alpha_{lp}^-(l)$, симметричную C относительно E_0 , можно получить из кривой, которая в аффинной карте $\Sigma_3 \setminus (E_3 \cup N_3(F_p))$ симметрична кривой $N_3(C)$ относительно оси x , и имеет, очевидно, тот же граф, что и кривая $N_3(C)$. $\square$

Замечание 26. Кривые из классов $\tilde{\alpha}(l)$, $\alpha_{ov}^\pm(l)$, отличаются от кривой $C \in \alpha_{lp}^\pm(l)$ лишь выбором точки $a \in N_3(C)$ (на дуге образа ветви $(1, 0)$, ограниченной особыми точками, которая имеет нечетную кратность пересечения с прямой $y = 0$ – для классов $\tilde{\alpha}(l)$; на овале – для классов $\alpha_{ov}^\pm(l)$). Поэтому те же аргументы доказывают связность и этих классов.

7. Применение: кривые рода 4 на квадратичном конусе

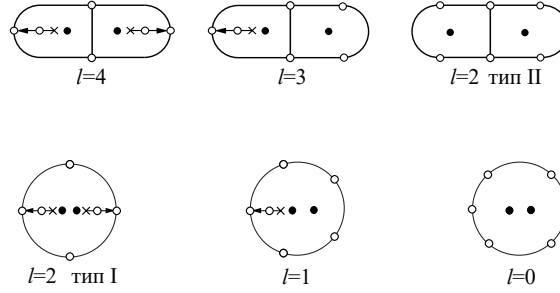


Рис. 19. Скелеты негиперболических кривых на Σ_2

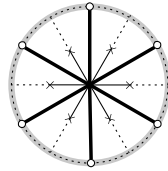


Рис. 20. Граф гиперболической кривой на Σ_2

Те же соображения, что и в доказательстве леммы 24, дают жесткую изотопическую классификацию неособых вещественных тригональных кривых рода 4 на квадратичном конусе (ср. [2, А3.6.1.]). После раздутия вершины конуса такая кривая дает собственную кривую на Σ_2 . Граф негиперболической кривой является либо блоком степени 6, либо контактом двух кубических блоков (см. рис. 19). Кривые, получаемые друг из друга отражением относительно оси OX , имеют один и тот же граф, но симметричные вещественные схемы. Класс жесткой изотопии определяется комплексной схемой; их число равно 11: при $l = 0$ схема гиперболической кривой (см. ее граф на рис. 20) и схема типа II, при $l = 2$ схема типа I и две симметричные друг другу схемы типа II, при $l = 1, 3, 4$ – по две симметричные друг другу схемы.

Автор выражает благодарность рецензенту за советы и замечания, позволившие устранить недочеты и неточности, имевшиеся в первоначальном варианте статьи.

Список литературы

- [1] В.И. Звонилов, *Жесткая изотопическая классификация вещественных алгебраических кривых бистепени (4,3) на гиперboloиде*, Вестник Сыктывкарского университета, Сер. 1 (3), 81–88 (1999).
- [2] A. Degtyarev, I. Itenberg, V. Kharlamov, *Real Enriques surfaces*, Lecture Notes in Math. **1746**, Springer-Verlag, Berlin, 2000.
DOI: <https://doi.org/10.1007/BFb0103960>
- [3] В.И. Звонилов, *Жесткая изотопическая классификация вещественных алгебраических кривых бистепени (4,3) на гиперboloиде. Приложение*, Вестник Сыктывкарского университета, Сер. 1 (5), 239–242 (2003).
- [4] В.А. Рохлин, *Комплексные топологические характеристики вещественных алгебраических кривых*, УМН **33** (5), 77–89 (1978).
URL: <https://www.mathnet.ru/rus/rm3519>
- [5] О.Я. Виро, *Успехи в топологии вещественных алгебраических многообразий за последние шесть лет*, УМН **41** (3), 45–67 (1986).
URL: <https://www.mathnet.ru/rus/rm2078>
- [6] В.И. Звонилов, *Комплексные топологические инварианты вещественных алгебраических кривых на гиперboloиде и эллипсоиде*, Алгебра и анализ, **3** (5), 88–108 (1991).
URL: <https://www.mathnet.ru/rus/aa280>
- [7] A. Degtyarev, I. Itenberg, V. Kharlamov, *On deformation types of real elliptic surfaces*, Amer. J. Math. **130** (6), 1561–1627 (2008).
DOI: <https://doi.org/10.1353/ajm.0.0029>
- [8] V.I. Zvonilov, *Maximally inflected real trigonal curves on Hirzebruch surfaces*, In: Topology, Geometry, and Dynamics: V.A. Rokhlin-Memorial, Contemp. Math. **772**, 331–345 (2021).
DOI: <http://dx.doi.org/10.1090/conm/772/15498>
- [9] F. Klein, *Gesammelte mathematische abhandlungen* II, Springer-Verlag Berlin, Heidelberg, 1922.
- [10] М. Нагата, *О рациональных поверхностях. I. Неприводимые кривые арифметического рода 0 и 1*, Математика **8** (1), 55–72 (1964).
URL: <https://www.mathnet.ru/rus/mat295>
- [11] A. Degtyarev, *Topology of algebraic curves. An approach via dessins d'enfants*, De Gruyter Studies in Mathematics **44**, Walter de Gruyter & Co., Berlin, 2012.
DOI: <https://doi.org/10.1515/9783110258424>

-
- [12] A.J. Puentes, *Rigid isotopy classification of generic rational curves of degree 5 in the real projective plane*, Geom. Dedicata **211**, 1–70 (2021).
DOI: <https://doi.org/10.1007/s10711-020-00540-8>
- [13] A. Degtyarev, I. Itenberg, V. Zvonilov, *Real trigonal curves and real elliptic surfaces of type I*, J. Reine Angew. Math. **686**, 221–246 (2014).
DOI: <https://doi.org/10.1515/crelle-2012-0020>
- [14] В.И. Звонилов, *Жесткие изотопии трехчленных кривых с максимальным числом овалов*, Вестник Сыктывкарского университета, Сер. 1 (6), 45–66 (2006).

Виктор Иванович Звонилов

Национальный исследовательский

Нижегородский государственный университет им. Н.И. Лобачевского,

проспект Гагарина, д. 23, г. Н. Новгород, 603950, Россия,

e-mail: zvonilov@itmm.unn.ru

Graphs of trigonal curves and rigid isotopies of singular real algebraic curves of bidegree $(4, 3)$ on a hyperboloid

V.I. Zvonilov

Abstract. A rigid isotopy of real algebraic curves of a certain class is a path in the space of curves of this class. Our study completes the rigid isotopic classification of nonsingular real algebraic curves of bidegree $(4, 3)$ on a hyperboloid, started by the author in his earlier works. Missing proofs of the uniqueness of the connected components for 16 classes of real algebraic curves of bidegree $(4, 3)$ having a single node or a cusp are given. The main technical tools are graphs of real trigonal curves on Hirzebruch surfaces.

Keywords: spaces of real algebraic curves, curves on a hyperboloid, trigonal curves, embedded graphs.

DOI: 10.26907/2949-3919.2025.1.26-51

References

- [1] V.I. Zvonilov, *Rigid isotopy classification of real algebraic curves of bidegree $(4, 3)$ on a hyperboloid*, Vestn. Syktyvkar. Univ. Ser. 1 Mat. Mekh. Inform. (3), 81–88 (1999) [in Russian].
- [2] A. Degtyarev, I. Itenberg, V. Kharlamov, *Real Enriques surfaces*, Lecture Notes in Math. **1746**, Springer-Verlag, Berlin, 2000.
DOI: <https://doi.org/10.1007/BFb0103960>
- [3] V.I. Zvonilov, *Appendix to: Rigid isotopy classification of real algebraic curves of bidegree $(4, 3)$ on a hyperboloid*, Vestn. Syktyvkar. Univ. Ser. 1 Mat. Mekh. Inform. (5), 239–242 (2003) [in Russian].
- [4] V.A. Rokhlin, *Complex topological characteristics of real algebraic curves*, Russian Math. Surveys **33** (5), 85–88 (1978).
DOI: <https://doi.org/10.1070/RM1978v033n05ABEH002514>
- [5] O.Ya. Viro, *Progress in the topology of real algebraic varieties over the last six years*, Russian Math. Surveys **41** (3), 55–82 (1986).
DOI: <https://doi.org/10.1070/RM1986v041n03ABEH003317>

Acknowledgements. The work was completed within the framework of a scientific project of the State assignment FSWR-2023-0034.

- [6] V.I. Zvonilov, *Complex topological invariants of real algebraic curves on a hyperboloid and on an ellipsoid*, St. Petersburg Math. J. **3** (5), 1023–1042 (1992).
- [7] A. Degtyarev, I. Itenberg, V. Kharlamov, *On deformation types of real elliptic surfaces*, Amer. J. Math. **130** (6), 1561–1627 (2008).
DOI: <https://doi.org/10.1353/ajm.0.0029>
- [8] V.I. Zvonilov, *Maximally inflected real trigonal curves on Hirzebruch surfaces*, In: Topology, Geometry, and Dynamics: V.A. Rokhlin-Memorial, Contemp. Math. **772**, 331–345 (2021).
DOI: <http://dx.doi.org/10.1090/conm/772/15498>
- [9] F. Klein, *Gesammelte mathematische abhandlungen II*, Springer-Verlag Berlin, Heidelberg, 1922.
- [10] M. Nagata, *On rational surfaces I. Irreducible curves of arithmetic genus 0 or 1*, Mem. Coll. Sci. Univ. Kyoto Ser. A. Math. **32** (3), 351–370 (1960).
DOI: <https://doi.org/10.1215/kjm/1250776405>
- [11] A. Degtyarev, *Topology of algebraic curves. An approach via dessins d'enfants*, De Gruyter Studies in Mathematics **44**, Walter de Gruyter & Co., Berlin, 2012.
DOI: <https://doi.org/10.1515/9783110258424>
- [12] A.J. Puentes, *Rigid isotopy classification of generic rational curves of degree 5 in the real projective plane*, Geom. Dedicata **211**, 1–70 (2021).
DOI: <https://doi.org/10.1007/s10711-020-00540-8>
- [13] A. Degtyarev, I. Itenberg, V. Zvonilov, *Real trigonal curves and real elliptic surfaces of type I*, J. Reine Angew. Math. **686**, 221–246 (2014).
DOI: <https://doi.org/10.1515/crelle-2012-0020>
- [14] V.I. Zvonilov, *Rigid isotopies of trinomial curves with the maximal number of ovals*, Vestn. Syktyvkar. Univ. Ser. 1 Mat. Mekh. Inform. (6), 45–66 (2006) [in Russian].

Victor Ivanovich Zvonilov

Lobachevsky State University of Nizhny Novgorod,
23 Gagarin av., Nizhny Novgorod 603950, Russia,
e-mail: zvonilov@itmm.unn.ru

Некоторые свойства сжатого графа делителей нуля

А.С. Монастырева

Аннотация. Показано, что если сжатый граф делителей нуля конечного ассоциативного кольца имеет единственную вершину, смежную со всеми остальными вершинами этого графа, то эта вершина имеет петлю. Кроме того, доказаны еще некоторые свойства сжатого графа делителей нуля конечного ассоциативного кольца.

Ключевые слова: сжатый граф делителей нуля, конечное кольцо, ассоциативное кольцо, делитель нуля.

DOI: 10.26907/2949-3919.2025.1.52-63

Введение

В нашей работе рассматриваются ассоциативные кольца (не обязательно коммутативные и не обязательно имеющие единицу).

Графом делителей нуля $\Gamma(R)$ кольца R называют граф, вершинами которого являются ненулевые делители нуля кольца (односторонние и двусторонние), причем различные две вершины x, y соединяются ребром тогда и только тогда, когда $xy = 0$ или $yx = 0$ [1].

Понятие графа делителей нуля для коммутативного кольца было введено Д. Андерсоном, П. Ливингстоном в работе [2]. Позже в [1] это понятие было обобщено для некоммутативного кольца. В частности, С. Редмонд доказал, что граф делителей нуля любого ассоциативного кольца является связным и его диаметр не превосходит трех.

С 1999 года вышел ряд статей, посвященных графам делителей нуля конечных колец. Одна из проблем, которая возникла, – это изображение и анализ графа делителей нуля для колец достаточно больших порядков. Возникла идея разбить множество вершин графа делителей нуля на классы, причем так, чтобы не нарушалось представление о строении графа делителей нуля в целом. В работах [3, 4] предложили довольно естественный способ решения этой проблемы для коммутативного случая. В статье [5] этот подход был обобщен на некоммутативный случай. Изложим суть этого метода.

Для этого нам понадобятся некоторые обозначения. Пусть R – произвольное кольцо. Для каждого элемента $x \in R$ положим $l(x) = \{a \in R : ax = 0\}$ и $r(x) = \{a \in R : xa = 0\}$.

Благодарности. Исследование выполнено за счет гранта Российского научного фонда № 24-21-00155, <https://rscf.ru/project/24-21-00155/>.

Пусть $D(R)$ – множество делителей нуля (односторонних и двусторонних) кольца R и $D(R)^* = D(R) \setminus \{0\}$.

Введем отношение эквивалентности на множестве $D(R)^*$ следующим образом:

$$\text{для любых } x, y \in D(R)^* \quad x \sim y \Leftrightarrow l(x) \cup r(x) = l(y) \cup r(y).$$

Обозначим через $[x]$ класс эквивалентности элемента $x \in D(R)^*$. Для любых $a \in [x], b \in [y]$, где $x, y \in D(R)^*$, очевидно, что $ab = 0$ или $ba = 0$ тогда и только тогда, когда $xy = 0$ или $yx = 0$. Обозначим через $\Gamma_{\sim}(R)$ граф, множеством вершин которого является множество $\{[x] : x \in D(R)^*\}$, причем две вершины $[x], [y]$ (не обязательно различные) будем соединять ребром (или петлей) тогда и только тогда, когда $xy = 0$ или $yx = 0$. Граф $\Gamma_{\sim}(R)$ будем называть *сжатым графом делителей нуля* кольца R .

Известно следующее

Предложение 1 ([5]). *Пусть R – произвольное кольцо и $x \in D(R)^*$. Если $x^2 = 0$, то $yz = 0$ или $zy = 0$ для любых $y, z \in [x]$; если же $x^2 \neq 0$, то $yz \neq 0$ и $zy \neq 0$ для любых $y, z \in [x]$.*

Из предложения 1 следует, что в графе $\Gamma_{\sim}(R)$ все вершины делятся на два типа. Если $x^2 = 0$, то $[x]$ – это вершина с петлей. Если $x^2 \neq 0$, то $[x]$ – это вершина без петли. Зная, сколько элементов содержится в каждом классе $[x]$, мы всегда от сжатого графа делителей нуля можем перейти к обычному графу делителей нуля. Более того, в сжатом графе нильпотентные элементы индекса нильпотентности два выделены петлей. Отметим, что не всякий связный граф может являться сжатым графом делителей нуля для какого-нибудь кольца. Например, если взять отрезок $[a] - [b]$, где обе вершины имеют петли, то он не является сжатым графом делителей нуля никакого кольца, поскольку вершины $[a]$ и $[b]$ на самом деле можно стянуть в одну вершину с петлей. И таких примеров много, причем не всегда причина в том, что граф не до конца сжат. В работе [5] описаны все связные графы делителей нуля (с петлями) на одной, двух и трех вершинах, которые являются сжатыми графами делителей нуля какого-либо конечного кольца. В статье [6] полностью описаны все связные графы с петлями на четырех вершинах, которые могут быть реализованы как сжатые графы делителей нуля какого-нибудь конечного кольца. Из 50 неизоморфных связных графов с петлями на четырех вершинах только 8, как оказалось, являются сжатыми графами делителей нуля какого-либо конечного кольца (см. [6]). Описаны полностью конечные кольца, сжатые графы делителей нуля которых содержат мост, вершины которого не являются висячими [7]. В работах [7, 8] получено описание конечных колец, сжатые графы делителей нуля которых являются полными (возможно, с петлями). Позже были описаны конечные кольца с ациклическими сжатыми графами делителей нуля [9].

В этой работе мы доказываем, что если в сжатом графе делителей нуля существует ровно одна вершина, смежная со всеми остальными вершинами этого графа, то такая вершина имеет петлю, т. е. смежна и сама с собой. Доказаны также некоторые другие свойства

сжатого графа делителей нуля, которые будут полезны при дальнейшем описании сжатых графов делителей нуля на пяти вершинах и более.

1. Предварительные сведения

Нам понадобятся некоторые обозначения и определения.

Обозначим $\text{Ann}(R) = \{a \in R : aR = Ra = (0)\}$. Через $J(R)$ обозначим *радикал Джекобсона* кольца R . Конечное кольцо R с единицей называется *локальным*, если факторкольцо $R/J(R)$ является полем [10]. Конечное поле порядка q будем обозначать через $GF(q)$, а полное кольцо матриц порядка n над кольцом R – через $M_n(R)$. Единичные матрицы в кольце $M_n(R)$, как обычно, обозначим e_{ij} , $i, j \in \{1, 2, \dots, n\}$. Для любого подмножества S кольца R будем полагать $S^* = S \setminus \{0\}$. Кольцо R называется *антикоммутативным*, если для всех $a, b \in R$ выполнено $ab = -ba$. Кольцо R называется *коммутативным по нулю*, если для всех $a, b \in R$ из $ab = 0$ следует, что $ba = 0$.

Пусть аддитивная группа кольца R разлагается в прямую сумму своих аддитивных подгрупп A_i , где $i = 1, \dots, n$ и $n \geq 2$, т.е. $R = A_1 \dot{+} \dots \dot{+} A_n$. Если все подгруппы A_i являются двусторонними идеалами кольца R , то кольцо R называют *разложимым* и пишут $R = A_1 \oplus \dots \oplus A_n$.

Элемент $e \in R$ называется *идемпотентом* кольца R , если $e = e^2$. Система ненулевых идемпотентов $e_1, \dots, e_k$ ($k \geq 2$) кольца R называется *ортогональной*, если $e_i e_j = e_j e_i = 0$ для любой пары различных чисел $i, j \in \{1, 2, \dots, k\}$. Далее, пусть R – произвольное кольцо (возможно, без единицы) и e – нетривиальный идемпотент кольца R , т.е. идемпотент, отличный от единицы (если она существует) и нуля. Обозначим

$$\begin{aligned} eRe &= \{ere : r \in R\}, & eR(1-e) &= \{er - ere : r \in R\}, \\ (1-e)Re &= \{re - ere : r \in R\}, & (1-e)R(1-e) &= \{r - re - er + ere : r \in R\}. \end{aligned}$$

Тогда для аддитивной группы кольца R имеет место следующее разложение, называемое *двусторонним пирсовским разложением* (см. [10, С. 32]):

$$R = eRe \dot{+} eR(1-e) \dot{+} (1-e)Re \dot{+} (1-e)R(1-e).$$

В кольце без единицы под записью $ex(1-e)$ мы будем понимать элемент $ex - exe$, аналогично $(1-e)xe = xe - exe$ и $(1-e)x(1-e) = x - ex - xe + exe$ для любого идемпотента $e \in R$ и для любого элемента $x \in R$.

Сжатый граф делителей нуля называется *полным*, если любые две различные вершины в этом графе соединены ребром, причем возможны петли. Заметим, что, если в полном графе две вершины с петлями, то их можно объединить в одну по определению сжатого графа делителей нуля. Таким образом, в полном сжатом графе делителей нуля петлю может иметь максимум одна вершина. Сжатый граф делителей нуля называется *звездой*, если все его вершины, может быть, кроме одной, являются висячими. Заметим,

что висячих вершин без петель может быть не более одной, поскольку две висячие вершины без петли могут быть объединены в одну по определению сжатого графа делителей нуля.

Вершину в графе мы будем называть *сильной*, если она смежна со всеми остальными вершинами графа. Заметим, что в сжатом графе делителей нуля $\Gamma_{\sim}(R)$ конечного ассоциативного кольца R не может быть двух сильных вершин с петлями, поскольку все элементы, входящие в такие вершины, должны быть объединены в одну сильную вершину с петлей по определению сжатого графа делителей нуля. Нильпотентное и локальное кольца всегда имеют в сжатом графе делителей нуля хотя бы одну сильную вершину с петлей.

2. Сильные вершины в сжатом графе делителей нуля

В работе [6] мы перебирали все связные графы на четырех вершинах (со всеми возможными расстановками петель) и выбирали те, которые являются сжатыми графами делителей нуля какого-нибудь конечного кольца. При доказательстве основного результата возникла гипотеза, что если в сжатом графе делителей нуля только одна сильная вершина, то эта вершина должна иметь петлю. Здесь мы покажем справедливость этой гипотезы.

Теорема 2. *Если в графе $\Gamma_{\sim}(R)$, где R – конечное ассоциативное кольцо, существует единственная сильная вершина, то эта вершина имеет петлю.*

Доказательство. Предположим, что в сжатом графе делителей нуля конечного ассоциативного кольца R существует единственная сильная вершина $[a]$, причем она не имеет петли. Ясно, что кольцо R не является нильпотентным или локальным. Если петель в графе $\Gamma_{\sim}(R)$ вообще нет, то R является прямой суммой полей [10]. Однако в этом случае либо в графе $\Gamma_{\sim}(R)$ вообще нет сильной вершины либо $R \cong GF(q_1) \oplus GF(q_2)$ и сильных вершин две, что противоречит условию. Таким образом, хотя бы одна вершина с петлей в графе $\Gamma_{\sim}(R)$ есть.

Докажем сначала, что кольцо R не содержит единицу. Предположим противное: в кольце R существует единица 1. Мы можем расписать $1 = e_1 + e_2 + \dots + e_n$, где $n \geq 2$ и $e_1, e_2, \dots, e_n$ – попарно ортогональные идемпотенты [10]. Если вершина $[a]$ не совпадает ни с одной вершиной $[e_i]$, $i = 1, 2, \dots, n$, то она смежна со всеми этими вершинами, т. е. $ae_i = 0$ или $e_i a = 0$ для всех i . Поэтому $a^2 = a \cdot 1 \cdot a = a(e_1 + e_2 + \dots + e_n)a = 0$, что противоречит тому, что вершина $[a]$ не имеет петли. Не нарушая общности, можем считать, что $[a] = [e_1]$. Если $n \geq 3$, то вершина $[e_1 + e_2]$ не смежна с $[a]$, не имеет петли, но и не совпадает с $[a]$, поскольку вершина $[a]$ смежна с $[e_2]$, а вершина $[e_1 + e_2]$ с этой вершиной не смежна. Получили противоречие, которое свидетельствует о том, что $n = 2$ и $1 = e_1 + e_2$. Тогда фактор-кольцо $R/J(R)$ изоморфно либо $M_2(GF(q))$, либо $GF(q_1) \oplus GF(q_2)$ [10]. В первом случае $R \cong M_2(S)$ для некоторого локального кольца S [10]. В этом случае $[a] = [e_{11}]$ и $1 = e_{11} + e_{22}$. Однако

$[e_{11}]$ не смежна с вершиной $[e_{11} + e_{12} + e_{21} + e_{22}]$ (заметим, что элемент $e_{11} + e_{12} + e_{21} + e_{22}$ является делителем нуля, так как $(e_{11} + e_{12} + e_{21} + e_{22})(e_{11} + e_{12} - e_{21} - e_{22}) = 0$). Противоречие. Итак, $R/J(R) \cong GF(q_1) \oplus GF(q_2)$, $R = e_1Re_1 + e_1Re_2 + e_2Re_1 + e_2Re_2$, причем $e_1Re_2 + e_2Re_1 \subseteq J(R)$ в силу коммутативности фактор-кольца $R/J(R)$. Кроме того, e_1Re_1 , e_2Re_2 являются локальными кольцами и $[a] = [e_1]$. Согласно [6, лемма 2.1] получаем, что e_1Re_1 является конечным полем. Элементы из множества $e_1Re_1^* + e_2Re_1^*$ (если они есть) образуют вершины, которые не смежны с $[a]$ и не смежны с $[e_2]$, чего быть не может. Значит, $e_1Re_2 = (0)$ или $e_2Re_1 = (0)$. Будем считать, что $e_2Re_1 = (0)$, т. е. $R = e_1Re_1 + e_1Re_2 + e_2Re_2$. Тогда $e_1Re_1^* + e_1Re_2 \subseteq [a] = [e_1]$, так как элементы этого множества не смежны с $[a]$, но являются делителями нуля. Далее, все делители нуля из множества $e_1Re_1^* + e_2Re_2^* + e_1Re_2$ тоже лежат в классе $[e_1] = [a]$, поскольку не смежны с этой сильной вершиной. Однако тогда они должны аннулировать (хотя бы с одной стороны) элементы из вершины $[e_2]$, чего быть не может. Противоречие показывает, что в множестве $e_1Re_1^* + e_2Re_2^* + e_1Re_2$ не существует делителей нуля. Другими словами, множество делителей нуля $D(R)$ состоит из элементов множеств $e_1Re_1 + e_1Re_2$ и $e_2Re_2 + e_1Re_2$. Тогда e_1Re_2 аннулирует все элементы из множества $D(R)$, т. е. существует еще одна сильная вершина и она с петлей; противоречие. Это позволяет нам заключить, что $e_1Re_2 = (0)$ и $R = e_1Re_2 \oplus e_2Re_2$, причем первое слагаемое является полем, а второе – локальным кольцом. Заметим, что вершина $[a] = [(1; 0)]$ смежна со всеми остальными. Рассмотрим элемент $b = (1; j)$, где $j \in J(e_2Re_2)^*$, $j^2 = 0$ (если такой существует). Тогда вершина $[b]$ не смежна с $[a]$, поэтому $[b] = [a]$. Однако вершина $[b]$ тогда является сильной и должна быть смежной с вершиной $[(0; 1)]$, которая не совпадает с $[a]$, поскольку в свою очередь не смежна с $[(0; j)]$. Итак, получили противоречие, которое говорит о том, что $J(e_2Re_2) = (0)$, т. е. кольцо R является прямой суммой двух конечных полей. Тогда сжатый граф делителей нуля кольца R не имеет петель. Противоречие. Значит, кольцо R не содержит единицу.

Итак, теперь будем полагать, что в кольце R нет единицы, но оно ненильпотентное. Тогда в R есть главный идемпотент e , образ которого в фактор-кольце $R/J(R)$ является единицей [10]. Сначала докажем, что $(1 - e)Re \neq (0)$ и $eR(1 - e) \neq (0)$. Предположим противное: пусть $(1 - e)Re = (0)$. Обозначим $B = (1 - e)R(1 - e)$. Если $B \neq (0)$, то мы можем взять ненулевой элемент $j \in \text{ann}(B)$. Тогда $jR = (0)$, т. е. вершина $[j]$ является сильной и имеет петлю; противоречие. Значит, $B = (0)$ и $R = eRe + eR(1 - e)$. Тогда $eR(1 - e) \subseteq l(R)$, т. е. существует сильная вершина с петлей. Противоречие доказывает, что $eR(1 - e) \neq (0)$ и $R = eRe$, т. е. R является кольцом с единицей. Выше мы доказали, что случай с единицей не возможен. Значит, $(1 - e)Re \neq (0)$. Аналогично доказывается, что $eR(1 - e) \neq (0)$. Покажем теперь, что $[a] \neq [e]$. Предположим противное: пусть $[a] = [e]$. Элементы множества $B_1 = eR(1 - e)^* + (1 - e)Re^*$ (а такие элементы есть, как доказано выше) не смежны с сильной вершиной $[e]$, поэтому $B_1 \subseteq [e] = [a]$. Возьмем ненулевой элемент $j \in \text{ann}(B)$ (если такой элемент существует). Тогда $jb = 0$ или $bj = 0$ для любого $b \in B_1 \subseteq [e] = [a]$. Следовательно, вершина $[j]$ смежна со всеми вершинами сжатого графа делителей нуля кольца R и является вершиной с петлей, чего быть не может. Противо-

речие доказывает, что $B = (0)$ и $R = eRe + eR(1 - e) + (1 - e)Re$. Согласно [6, лемма 2.1] eRe является прямой суммой полей. Мы можем идемпотент e расписать как сумму попарно ортогональных идемпотентов: $e = e_1 + \dots + e_n$ [10]. Если $n \geq 2$, то вершина $[a] = [e]$ не смежна с вершинами $[e_1]$ и $[e_2]$, а это две разные вершины без петель. Это противоречит нашему предположению, что вершина $[e]$ является сильной. Значит, $n = 1$ и eRe является конечным полем. Далее, делители нуля из множеств $eRe^* + eR(1 - e) + (1 - e)Re$ и $eR(1 - e)^* + (1 - e)Re^*$ не аннулируют e ни с одной стороны, т. е. эти элементы лежат в $[e]$. Остальные вершины состоят из элементов множеств $eR(1 - e)^*$ и $(1 - e)Re^*$, т. е. они все с петлями. Более того, каждый элемент из $eR(1 - e)^*$ аннулирует с какой-либо стороны каждый элемент из $eR(1 - e)^* + (1 - e)Re^* \subset [e]$. Поэтому все элементы из $eR(1 - e)^*$ и $(1 - e)Re^*$ аннулируют друг друга хотя бы с одной стороны. Следовательно в сжатом графе делителей нуля кольца R всего две вершины: одна с петлей, а вторая без петли. Понятно, что обе они являются сильными, что противоречит условию теоремы. Поэтому заключаем, что $[e] \neq [a]$. Докажем, что $a \in (1 - e)R(1 - e)$. Действительно, вершина $[a]$ смежна со всеми остальными вершинами и не равна вершине $[e]$. Следовательно, $a \notin eRe^* + eR(1 - e) + (1 - e)Re + (1 - e)R(1 - e)$ и $a \notin eR(1 - e)^* + (1 - e)Re^* + (1 - e)R(1 - e)$. Пусть, например, $a \in (1 - e)Re + (1 - e)R(1 - e)$, т. е. $a = (1 - e)re + (1 - e)s(1 - e)$ для некоторых элементов $r, s \in R$. Элемент a аннулирует хотя бы с одной стороны любой элемент вида $t = e + e\beta(1 - e) + (1 - e)\gamma e + (1 - e)\delta(1 - e)$, где $\beta, \gamma, \delta \in R$. Поэтому $at = 0$ или $ta = 0$. Отсюда получаем, что

$$er(1 - e)\gamma e + er(1 - e)\delta(1 - e) + (1 - e)s(1 - e)\gamma e + (1 - e)s(1 - e)\delta(1 - e) = 0$$

или

$$er(1 - e) + (1 - e)\delta(1 - e)s(1 - e) + (1 - e)\gamma er(1 - e) + e\beta(1 - e)s(1 - e) = 0.$$

Заметим, что в обоих равенствах все слагаемые из разных пирсовских компонент, т. е. из выполнения равенства суммы нулю следует, что все слагаемые этой суммы равны нулю. Заметим, что если $er(1 - e) = 0$, то $a \in (1 - e)R(1 - e)$, что и требовалось доказать. Пусть $er(1 - e) \neq 0$. Тогда $er(1 - e)\gamma e = 0$ и $er(1 - e) \cdot (1 - e)\delta(1 - e) = 0$ для любых $\gamma, \delta \in R$, т. е. $er(1 - e) \cdot (1 - e)Re = (0)$ и $er(1 - e) \cdot (1 - e)R(1 - e) = (0)$. Другими словами, элемент $er(1 - e)$ аннулирует все кольцо R слева, т. е. образует сильную вершину с петлей. Противоречие показывает, что $er(1 - e) = 0$ и $a \in (1 - e)R(1 - e)$. В этом случае элемент a является нильпотентным. Предположим, что $a^n = 0$, $a^{n-1} \neq 0$ и $n \geq 3$. Тогда $(a^{n-1})^2 = 0$, т. е. $[a^{n-1}]$ тоже является сильной вершиной, причем имеет петлю. Противоречие доказывает теорему. $\square$

Из теоремы следует, что если в сжатом графе делителей нуля некоторого конечного ассоциативного кольца есть сильная вершина без петли, то в этом графе обязательно содержится и причем единственная сильная вершина с петлей.

3. Дополнительные свойства сжатого графа делителей нуля

В этом разделе мы докажем некоторые свойства сжатого графа делителей нуля.

Определение сильной вершины можно ослабить, если говорить о некоторых выделенных вершинах в графе, для которых любая другая вершина графа смежна хотя бы с одной из выделенных вершин. Особую роль играют сильные вершины без петель. Если сильных вершин без петель в сжатом графе делителей нуля немного, то это накладывает ограничения на кольцо в случае, когда оно нильпотентное: дело в том, что идемпотенты как раз и образуют вершины без петель, а если такие вершины еще являются и сильными (или часть их), то многое можно сказать о радикале Джекобсона самого кольца. Такая ситуация часто возникала при описании графов делителей нуля порядка 4 в работе [6]. В первой теореме этого раздела как раз речь и пойдет о графе, в котором есть ровно две вершины без петель, причем они такие, что любая вершина с петлей смежна хотя бы с одной из этих двух вершин. Фактически теорема 3 продолжает [6, лемма 2.7].

Теорема 3. *Пусть в графе $\Gamma_{\sim}(R)$ ровно две вершины без петель и порядок графа больше двух, причем любая вершина с петлей смежна хотя бы с одной из вершин без петли. Тогда выполняется одно из условий:*

- 1) R – нильпотентное кольцо;
- 2) $R/J(R)$ – конечное поле;
- 3) в кольце R есть единица $1 = e_1 + e_2$, $R \cong GF(q_1) \oplus GF(q_2) \dot{+} e_1Re_2$, где e_i – единица поля $GF(q_i)$, $i = 1, 2$, и граф $\Gamma_{\sim}(R)$ является полным графом на трех вершинах, из которых только одна имеет петлю.

Доказательство. Если в кольце R нет единицы и оно не является нильпотентным, то согласно [6, лемма 2.9] в кольце R нет ортогональных идемпотентов, т. е. $R/J(R)$ является полем. Итак, мы можем считать, что кольцо R имеет единицу. Если единица не раскладывается в сумму попарно ортогональных идемпотентов, то $R/J(R)$ является полем [10]. Поскольку вершин без петель ровно две, то $1 = e_1 + e_2$, где e_1 и e_2 – ортогональные идемпотенты. В этом случае $R/J(R) \cong M_2(GF(q))$ или $R/J(R) \cong GF(q_1) \oplus GF(q_2)$. В первом случае $R \cong M_2(S)$ для некоторого локального кольца S [10]. Тогда в графе $\Gamma_{\sim}(R)$ есть минимум три вершины без петли: $[e_{11}]$, $[e_{22}]$ и $[e_{12} + e_{22}]$. Это все разные вершины, поскольку в треугольнике $[e_{21}] - [e_{22}] - [e_{11}] - [e_{21}]$ только вершина $[e_{11}]$ смежна с вершиной $[e_{12} + e_{22}]$. Противоречие. Значит, $R/J(R) \cong GF(q_1) \oplus GF(q_2)$, $R = e_1Re_1 \dot{+} e_1Re_2 \dot{+} e_2Re_1 \dot{+} e_2Re_2$, причем e_i – единица поля $GF(q_i)$, e_iRe_i – локальное кольцо, $i = 1, 2$. В силу коммутативности фактор-кольца $R/J(R)$ имеем $e_1Re_2 + e_2Re_1 \subseteq J(R)$. Поскольку $[e_1]$ и $[e_2]$ – две вершины без петель, причем любая вершина с петлей смежна хотя бы с одной из этих вершин, то по [6, лемма 2.7] e_1Re_1 и e_2Re_2 являются прямыми суммами конечных полей. Поскольку $1 = e_1 + e_2$, то e_1Re_1 и e_2Re_2 являются конечными полями. Элементы из множества $e_1Re_2^* + e_2Re_1^*$ не смежны ни с одной из вершин без петли $[e_1]$ и $[e_2]$. Значит, эти элементы содержатся в одной из этих вершин. Но поскольку $[e_1]$ и $[e_2]$ смежны, то снова получаем противоречие. Значит, $e_1Re_2 = (0)$ или $e_2Re_1 = (0)$. Будем считать,

что $e_2 Re_1 = (0)$, т.е. $R = (e_1 Re_1 \oplus e_2 Re_2) \dot{+} e_1 Re_2$. Тогда в графе $\Gamma_{\sim}(R)$ три вершины: $[e_1] = e_1 Re_1^* + e_1 Re_2$, $[e_2] = e_2 Re_2^* + e_1 Re_2$ и $[b] = e_1 Re_2^*$, причем только вершина $[b]$ имеет петлю и все три вершины образуют треугольник. Мы как раз и получили случай 3 из [8, теорема 1]. $\square$

В следующей теореме фактически доказывается, что если сжатый граф делителей нуля $\Gamma_{\sim}(R)$ имеет достаточно маленький порядок (не более шести) и все его вершины с петлями, то сам граф является звездой, а кольцо R является локальным или нильпотентным с $J(R)^3 = (0)$. Этот факт поможет сократить перебор графов при дальнейшем описании графов порядков 5 и более, которые могут быть реализованы как сжатые графы делителей нуля некоторого конечного кольца.

Теорема 4. Пусть в графе $\Gamma_{\sim}(R)$ все вершины имеют петли. Тогда кольцо R является локальным или нильпотентным, причем либо граф $\Gamma_{\sim}(R)$ является звездой и $J(R)^3 = (0)$, либо в графе $\Gamma_{\sim}(R)$ содержится более шести вершин.

Доказательство. Если кольцо R является ненильпотентным без единицы, то его главный идемпотент e образует вершину без петли (в таком кольце все элементы являются делителями нуля [10]); противоречие. Следовательно, кольцо R является нильпотентным или содержит единицу. Если в кольце R существует единица 1 и $1 = e_1 + e_2 + \dots + e_n$, где e_i – попарно ортогональные идемпотенты, то вершина $[e_1]$ не имеет петли. Следовательно, единицу нельзя представить в виде суммы попарно ортогональных идемпотентов. Значит, кольцо R является локальным [10].

Заметим, что если граф $\Gamma_{\sim}(R)$ является звездой, у которой все вершины имеют петли, то $J(R)^3 = (0)$ [9]. Поэтому можем считать, что граф $\Gamma_{\sim}(R)$ не является звездой. Не нарушая общности, также можем полагать, что кольцо R является нильпотентным, поскольку в локальном случае $\Gamma_{\sim}(R) = \Gamma_{\sim}(J(R))$ [10]. Поскольку в нильпотентном кольце R все элементы в квадрате равны нулю, кольцо R является антикоммутативным, а следовательно, и коммутативным по нулю. Далее, в $\Gamma_{\sim}(R)$ есть сильная вершина с петлей. Обозначим ее через $[a]$. Напомним, что не может быть двух сильных вершин с петлями, поэтому в нашем случае в графе $\Gamma_{\sim}(R)$ существует единственная сильная вершина с петлей. Кроме того, в графе $\Gamma_{\sim}(R)$ не может существовать треугольников $[a] - [b] - [c] - [a]$, в которых вершины $[b]$ и $[c]$ не смежны больше ни с какими другими вершинами графа $\Gamma_{\sim}(R)$, кроме вершин этого треугольника. Действительно, в этом случае вершины $[b]$ и $[c]$ нужно объединить в одну висячую вершину с петлей. Поскольку $\Gamma_{\sim}(R)$ не является звездой, то в графе $\Gamma_{\sim}(R)$ должен быть треугольник $[a] - [b_1] - [b_2] - [a]$. Вершины $[b_1]$ и $[b_2]$ различны и смежны друг с другом. Поэтому должна существовать четвертая вершина $[b_3]$, которая смежна, например, с $[b_2]$ и не смежна с $[b_1]$. Если других вершин нет, то вершины $[a]$ и $[b_2]$ можно стянуть; противоречие. Следовательно, существует вершина $[b_4]$, не смежная с $[b_2]$. Итак, в графе $\Gamma_{\sim}(R)$ как минимум пять вершин. Далее, вершина $[b_1 + b_3]$ не смежна с вершинами $[b_1]$ и $[b_3]$, поэтому она и не может совпасть с вершинами $[a]$, $[b_1]$, $[b_2]$ и $[b_3]$. Поскольку $[b_1 + b_3]$ смежна с $[b_2]$, а вершина $[b_4]$ с $[b_2]$ не смежна, то

$[b_1 + b_3] \neq [b_4]$. Таким образом, $[b_1 + b_3]$ является шестой вершиной графа $\Gamma_{\sim}(R)$. Теперь рассмотрим вершину $[b_2 + b_4]$, которая не смежна с $[b_2]$ и $[b_4]$. Поэтому вершина $[b_2 + b_4]$ не может совпадать ни с одной из вершин $[b_1]$, $[b_2]$, $[b_3]$, $[b_4]$ и $[a]$. Наконец, $(b_1 + b_3)b_2 = 0$, а вершины $[b_2]$ и $[b_2 + b_4]$ не смежны, то $[b_1 + b_3] \neq [b_2 + b_4]$. Мы нашли седьмую вершину графа $\Gamma_{\sim}(R)$ – это вершина $[b_2 + b_4]$. Это доказывает теорему. $\square$

Список литературы

- [1] S.P. Redmond, *The zero-divisor graph of a noncommutative ring*, Int. J. Commut. Rings **1** (4), 203–211 (2002).
- [2] D.F. Anderson, P.S. Livingston, *The zero-divisor graph of a commutative ring*, J. Algebra **217** (2), 434–447 (1999).
DOI: <https://doi.org/10.1006/jabr.1998.7840>
- [3] N. Bloomfield, C. Wickham, *Local rings with genus two zero divisor graph*, Comm. Algebra **38** (8), 2965–2980 (2010).
DOI: <https://doi.org/10.1080/00927870903100093>
- [4] N. Bloomfield, *The zero divisor graphs of commutative local rings of order p^4 and p^3* , Comm. Algebra **41** (2), 765–775 (2013).
DOI: <https://doi.org/10.1080/00927872.2011.635619>
- [5] Е.В. Журавлев, А.С. Монастырева, *Сжатые графы делителей нуля конечных ассоциативных колец*, Сиб. матем. журн. **61** (1), 96–106 (2020).
DOI: <https://doi.org/10.33048/smzh.2020.61.106>
- [6] A.S. Monastyreva, *The compressed zero-divisor graphs of order 4*, J. Algebra Appl. **21**(9), art. 2250179 (2022).
DOI: <https://doi.org/10.1142/S0219498822501791>
- [7] А.А. Афанасьев, А.С. Монастырева, *Сжатые и частично сжатые графы делителей нуля конечных ассоциативных колец*, Сиб. матем. журн. **64** (2), 281–291 (2023).
DOI: <https://doi.org/10.33048/smzh.2023.64.204>
- [8] A.S. Monastyreva, *Finite non-nilpotent rings with complete compressed zero-divisor graphs*, Lobachevskii J. Math **41** (9), 1666–1671 (2020).
DOI: <https://doi.org/10.1134/S1995080220090206>
- [9] А.С. Монастырева, *Конечные кольца с ациклическими сжатыми графами делителей нуля*, Сиб. электрон. матем. изв. **21** (1), 405–416 (2024).
DOI: <https://doi.org/10.33048/semi.2024.21.030>
- [10] В.П. Елизаров, *Конечные кольца. Основы теории*, Гелиос АРВ, М., 2006.

Анна Сергеевна Монастырева

Алтайский государственный университет,

пр. Ленина, д. 61, г. Барнаул, 656049, Россия

e-mail: akuzmina1@yandex.ru

Some properties of compressed zero-divisor graph

A.S. Monastyreva

Abstract. We prove that if the compressed zero-divisor graph of a finite associative ring contains only one strong vertex then this vertex has a loop. Moreover, more properties of the compressed zero-divisor graph of a finite associative ring are proved.

Keywords: compressed zero-divisor graph, finite ring, associative ring, zero-divisor.

DOI: 10.26907/2949-3919.2025.1.52-63

References

- [1] S.P. Redmond, *The zero-divisor graph of a noncommutative ring*, Int. J. Commut. Rings **1** (4), 203–211 (2002).
- [2] D.F. Anderson, P.S. Livingston, *The zero-divisor graph of a commutative ring*, J. Algebra **217** (2), 434–447 (1999).
DOI: <https://doi.org/10.1006/jabr.1998.7840>
- [3] N. Bloomfield, C. Wickham, *Local rings with genus two zero divisor graph*, Comm. Algebra **38** (8), 2965–2980 (2010).
DOI: <https://doi.org/10.1080/00927870903100093>
- [4] N. Bloomfield, *The zero divisor graphs of commutative local rings of order p^4 and p^3* , Comm. Algebra **41** (2), 765–775 (2013).
DOI: <https://doi.org/10.1080/00927872.2011.635619>
- [5] E.V. Zhuravlev, A.S. Monastyreva, *Compressed zero-divisor graphs of finite associative rings*, Siberian Math. J. **61**(1), 76–84 (2020).
DOI: <https://doi.org/10.1134/S0037446620010061>
- [6] A.S. Monastyreva, *The compressed zero-divisor graphs of order 4*, J. Algebra Appl. **21**(9), art. 2250179 (2022).
DOI: <https://doi.org/10.1142/S0219498822501791>

Acknowledgements. The research was funded by the Russian Science Foundation (project no. 24-21-00155, <https://rscf.ru/project/24-21-00155/>).

Received: 30 September 2024. Accepted: 03 April 2025. Published: 24 April 2025.

-
- [7] A.A. Afanas'ev, A.S. Monastyreva, *Compressed and partially compressed zero-divisor graphs of finite associative rings*, Siberian Math. J. **64** (2), 281–291 (2023).
DOI: <https://doi.org/10.1134/s0037446623020040>
- [8] A.S. Monastyreva, *Finite non-nilpotent rings with complete compressed zero-divisor graphs*, Lobachevskii J. Math **41** (9), 1666–1671 (2020).
DOI: <https://doi.org/10.1134/S1995080220090206>
- [9] A.S. Monastyreva, *Finite rings with acyclic compressed zero-divisor graphs*, Sib. Electron. Math. Rep **21** (1), 405–416 (2024) [in Russian].
DOI: <https://doi.org/10.33048/semi.2024.21.030>
- [10] V.P. Elizarov, *Finite rings*, Gelios ARV, Moscow, 2006 [in Russian].

Anna Sergeevna Monastyreva

Altai State University,

61 Lenina av., Barnaul 656049, Russia,

e-mail: akuzmina1@yandex.ru

Классы Леви квазимногообразий 2-нильпотентных групп

С.А. Шахова

Аннотация. Классом Леви $L(\mathcal{M})$, порожденным классом групп $\mathcal{M}$, называется класс всех групп, в которых нормальное замыкание каждой циклической подгруппы принадлежит $\mathcal{M}$. Пусть p – простое число, $p \neq 2$, s – натуральное число, $s \geq 2$, и $s > 2$ при $p = 3$; H_{p^s} – свободная ранга 2 группа в многообразии nilпотентных ступени ≤ 2 групп экспоненты p^s с коммутантом экспоненты p ; Z – бесконечная циклическая группа; $q\{H_{p^s}, Z\}$ – квазимногообразие, порожденное множеством групп $\{H_{p^s}, Z\}$. В работе найден базис квазитождеств класса Леви $L(q\{H_{p^s}, Z\})$ и установлено, что существует континуальное множество квазимногообразий $\mathcal{K}$ таких, что $L(\mathcal{K}) = L(q\{H_{p^s}, Z\})$.

Ключевые слова: квазимногообразие, класс Леви, nilпотентная группа.

DOI: 10.26907/2949-3919.2025.1.64-77

Введение

Для произвольного класса групп $\mathcal{M}$ обозначим через $L(\mathcal{M})$ класс всех групп G , в которых нормальное замыкание $\langle a \rangle^G$ каждого элемента a из G принадлежит классу групп $\mathcal{M}$. Класс $L(\mathcal{M})$ называется классом Леви, порожденным $\mathcal{M}$. Самое первое исследование классов Леви, а точнее, изучение свойств групп, покрываемых системой абелевых нормальных подгрупп вида $\langle a \rangle^G$, было предпринято в [1]. Из этой работы следует, что класс Леви всех абелевых групп является многообразием 2-энгелевых групп. Классы Леви nilпотентных групп изучались, например, в [2–6]. В [4], в частности, доказано, что если $\mathcal{M}$ – квазимногообразие групп, то $L(\mathcal{M})$ – также квазимногообразие групп. Для многообразий этот факт был установлен в [7]. К настоящему моменту достаточно подробно изучены классы Леви почти абелевых квазимногообразий nilпотентных групп.

Для каждого простого числа p и натурального числа s рассмотрим группы, имеющие в многообразии $\mathcal{N}_2$ nilпотентных ступени не выше двух группы следующие представления:

$$H_p = \langle x, y; [x, y]^p = 1 \rangle, \quad H_{p^s} = \langle x, y; x^{p^s} = y^{p^s} = [x, y]^p = 1 \rangle.$$

Заметим сразу, что при $s = 1$ будем писать H_{p^1} , подчеркивая отличие этой группы от группы H_p .

Пусть, как обычно, $F_2(\mathcal{N}_2)$ – свободная в многообразии $\mathcal{N}_2$ группа ранга 2; $q\mathcal{K}$ – квазимногообразие, порожденное классом групп $\mathcal{K}$. Будем писать qG , если $\mathcal{K} = \{G\}$. Согласно [8] квазимногообразия qH_{p^s} (исключая qH_{2^1}), qH_p , $qF_2(\mathcal{N}_2)$, где p пробегает множество простых чисел, а s пробегает множество натуральных чисел, составляют полный список почти абелевых квазимногообразий nilпотентных групп, т.е. неабелевых квазимногообразий nilпотентных групп, чьи собственные подквазимногообразия являются абелевыми.

В [9] доказано, что для любого простого p , $p \neq 2$, $L(qH_{p^1})$ совпадает с многообразием nilпотентных ступени не выше трех групп экспоненты p , а $L(qF_2(\mathcal{N}_2))$ – это квазимногообразие nilпотентных ступени не выше трех групп без кручения. В [10] и [11] для любого простого p , $p \neq 2$, и натурального s , $s \geq 2$, найдены системы квазитождеств от бесконечного числа переменных, задающие соответственно классы Леви $L(qH_p)$ и $L(qH_{p^s})$. В [12] установлено, что квазимногообразие $L(qH_{p^s})$ конечно аксиоматизируемо. В [13] доказано, что квазимногообразие $L(qH_p)$ имеет конечный аксиоматический ранг, т.е. может быть задано системой квазитождеств от конечного числа переменных.

Пусть $\mathcal{K}^{p^s}$ – квазимногообразие nilпотентных ступени не выше двух групп с коммутантом экспоненты p , в которых элементы порядка p^k при $k < s$ содержатся в центре группы, где p – простое число, $p \neq 2$, s – натуральное число, $s \geq 2$, и $s > 2$ при $p = 3$. Нетрудно заметить, что $qH_{p^s} \subseteq \mathcal{K}^{p^s}$, $qH_p \subseteq \mathcal{K}^{p^s}$. В [14] найдена бесконечная серия квазитождеств от двух переменных, задающая $L(\mathcal{K}^{p^s})$ в многообразии $\mathcal{N}_3$ nilпотентных ступени не выше трех групп. Это позволило доказать в [15], что в $\mathcal{K}^{p^s}$ существует континуальное множество квазимногообразий $\mathcal{K}$ таких, что $L(\mathcal{K}) = L(qH_{p^s})$.

Пусть p – простое число, $p \neq 2$, s – натуральное число, $s \geq 2$, и $s > 2$ при $p = 3$. В нашей работе найден базис квазитождеств квазимногообразия $L(q\{H_{p^s}, Z\})$, и доказано существование континуального множества квазимногообразий, каждое из которых порождает класс Леви, совпадающий с $L(q\{H_{p^s}, Z\})$, где Z – бесконечная циклическая группа.

1. Предварительные замечания

Используемые в работе сведения из теории групп можно найти в [16], а из теории квазимногообразий групп – в [17–19].

Всюду в работе p – простое число, $p \neq 2$, $s \geq 2$, $s \in \mathbf{N}$, где $\mathbf{N} = \{1, 2, \dots\}$ – множество натуральных чисел; $\mathbf{P}$ – множество простых чисел. Для целых чисел a, b и $c \in \mathbf{N}$ запись $a \equiv b(c)$ означает, что остаток от деления $a - b$ на c равен 0.

В работе также используются следующие обозначения: $[a, b] = a^{-1}b^{-1}ab$; $\langle a_1, a_2, \dots \rangle$ – группа, порожденная элементами $a_1, a_2, \dots$; Z_n – циклическая группа порядка n ; Z – бесконечная циклическая группа; $\langle a \rangle^G = \langle g^{-1}ag \mid g \in G \rangle$ – нормальное замыкание в группе G циклической подгруппы, порожденной элементом a ; $|g|$ – порядок элемента g ; G' – коммутант группы G ; $G \cong H$ – группы G и H изоморфны.

Пусть N – нормальная подгруппа группы G (обозначим $N \trianglelefteq G$), G/N – факторгруппа группы G по нормальной подгруппе N . Через $\bar{g}$ обозначим образ элемента $g \in G$

при естественном гомоморфизме $G \rightarrow G/N$.

Через $L_q(\mathcal{N})$ обозначим решетку подквазимногообразий, содержащихся в квазимногообразии $\mathcal{N}$. Пусть $\mathcal{K}_1, \mathcal{K}_2 \in L_q(\mathcal{N})$. Решеточные операции в $L_q(\mathcal{N})$ выглядят так: $\mathcal{K}_1 \wedge \mathcal{K}_2 = \mathcal{K}_1 \cap \mathcal{K}_2$, $\mathcal{K}_1 \vee \mathcal{K}_2$ – пересечение всех квазимногообразий, содержащих $\mathcal{K}_1, \mathcal{K}_2$.

Нам потребуется признак принадлежности конечно-определенной группы G квазимногообразию $q\mathcal{K}$, являющийся частным случаем [8, теорема 3]:

конечно определенная в квазимногообразии $\mathcal{N}$ группа G принадлежит квазимногообразию $q\mathcal{K}$ ($\mathcal{K} \subseteq \mathcal{N}$) тогда и только тогда, когда для любого элемента $g \in G$, $g \neq 1$, существует гомоморфизм φ_g группы G в некоторую группу из класса $\mathcal{K}$ такой, что $\varphi_g(g) \neq 1$.

Условимся при написании тождеств и квазитождеств кванторы всеобщности опускать.

Пусть p – простое число, $p \neq 2$, $s \in \mathbb{N}$, $s \geq 2$. Обозначим через $\mathcal{K}^p$ многообразие, заданное в $\mathcal{N}_2$ тождеством

$$[x, y]^p = 1, \quad (1)$$

и пусть $\mathcal{K}^{p^s}$ – квазимногообразие, заданное в $\mathcal{K}^p$ квазитождеством

$$x^{p^{s-1}} = 1 \rightarrow [x, y] = 1, \quad (2)$$

$\mathcal{K}_3^{p^s}$ – квазимногообразие, заданное в $\mathcal{K}^{p^s}$ квазитождеством

$$x^{p^{s+1}} = 1 \rightarrow x^{p^s} = 1, \quad (3)$$

$\mathcal{K}_{3,4}^{p^s}$ – квазимногообразие, заданное в $\mathcal{K}_3^{p^s}$ квазитождествами

$$x^q = 1 \rightarrow x = 1, \quad (4)$$

где q пробегает множество простых чисел, $q \neq p$.

Пусть $\mathcal{N}^{p^s}$ – квазимногообразие, заданное в $\mathcal{K}_{3,4}^{p^s}$ квазитождеством

$$x^p = [y, z] \rightarrow [y, z] = 1, \quad (5)$$

$\widehat{\mathcal{N}}^{p^s}$ – квазимногообразие, заданное в $\mathcal{N}^{p^s}$ тождеством

$$x^{p^s} = 1. \quad (6)$$

Очевидно, что квазитождества (3), (4) являются следствиями тождества (6).

Из квазитождеств (3), (4) следует, что если группа $G \in \mathcal{K}_{3,4}^{p^s}$, $g \in G$, $|g| < \infty$, то $|g| = p^t$ для некоторого t , $0 \leq t \leq s$, т. е. для любого $n \in \mathbb{N}$ в группе G истинно следующее квазитождество:

$$x^n = 1 \rightarrow x^{p^s} = 1. \quad (7)$$

Индукцией по n легко проверить, что в $\mathcal{N}_2$ для любого $n \in \mathbf{N}$ истинно тождество

$$(xy)^n = x^n y^n [y, x]^{\frac{n(n-1)}{2}},$$

из которого по (1) при $n = p$ следует истинность в $\mathcal{K}^p$ тождества

$$(xy)^p = x^p y^p. \quad (8)$$

Нам понадобится следующая

Лемма 1 ([15, лемма 1]). *Если $H = \langle a, a_1, \dots, a_n \rangle$, $H \in \widehat{\mathcal{N}}^{p^s}$, $\langle a_1, \dots, a_n \rangle$ – абелева группа, то $H \in qH_{p^s}$, где $p \in \mathbf{P}$, $p \neq 2$, $s \in \mathbf{N}$, $s \geq 2$.*

Лемма 2. *Если $H = \langle a, a_1, \dots, a_n \rangle$, $H \in \mathcal{N}^{p^s}$, $\langle a_1, \dots, a_n \rangle$ – абелева группа, то $H \in q\{H_{p^s}, Z\}$, где $p \in \mathbf{P}$, $p \neq 2$, $s \in \mathbf{N}$, $s \geq 2$.*

Доказательство. Если группа H – абелева, то утверждение леммы верно. Пусть H – неабелева группа, $H^{p^s} = \{h^{p^s} \mid h \in H\}$. Из (1), (8) вытекает, что $H^{p^s} \trianglelefteq H$. Проверим, что $\overline{H} = H/H^{p^s} \in \widehat{\mathcal{N}}^{p^s}$.

Поскольку (6) истинно в $\overline{H}$, то (3), (4) истинны в $\overline{H}$.

Предположим, что $\overline{x}^{p^{s-1}} = \overline{1}$ для $\overline{x} \in \overline{H}$. Тогда $x^{p^{s-1}} = h^{p^s}$ для некоторого $h \in H$, $(xh^{-p})^{p^{s-1}} = 1$. Согласно (1), (2) для любого $y \in H$ верны равенства $[xh^{-p}, y] = [x, y] = 1$, что доказывает истинность (2) в группе $\overline{H}$.

Если $\overline{x}^p = [\overline{y}, \overline{z}]$ для $\overline{x}, \overline{y}, \overline{z} \in \overline{H}$, то $x^p = [y, z]h^{p^s}$, $(xh^{-p^{s-1}})^p = [y, z]$. Так как (5) истинно в H , то $[y, z] = 1$, и (5) истинно в $\overline{H}$.

По лемме 1 $\overline{H} \in qH_{p^s}$. Из истинности формул (1), (7) в группе H получаем, что $H/H' \in q\{H_{p^s}, Z\}$. Поскольку любой элемент из H' можно записать в виде $[a, h]$ для некоторого элемента $h \in H$, то в силу квазитожества (5) верно $H' \cap H^{p^s} = \langle 1 \rangle$. По признаку принадлежности получаем, что $H \in q\{H_{p^s}, Z\}$. $\square$

Пусть $\mathcal{F}^p$ – многообразие, заданное в $\mathcal{N}_3$ тождеством

$$[x, y, x]^p = 1. \quad (9)$$

Так как тождество $[x, y, x] = [y, x, x]^{-1}$ истинно в $\mathcal{N}_3$, то тождество (9) эквивалентно в $\mathcal{N}_3$ тождеству $[x, y, y]^p = 1$.

Индукцией по n легко показать, что в многообразии $\mathcal{N}_3$ для любого $n \in \mathbf{N}$ истинно тождество

$$[x, y^n] = [x, y]^n [x, y, y]^{\frac{n(n-1)}{2}}, \quad (10)$$

из которого при $n = p$, $p \neq 2$, по (9) получаем, что в $\mathcal{F}^p$ истинно тождество

$$[x, y^p] = [x, y]^p. \quad (11)$$

Возведем обе части (10) в степень p . Из (9) следует, что в $\mathcal{F}^p$ для любого $n \in \mathbf{N}$ истинно тождество

$$[x, y^n]^p = [x, y]^{np}. \quad (12)$$

На самом деле, и в этом легко убедиться, тождество (12) истинно для любого $n \in \mathbf{Z}$.

Пусть $\mathcal{F}^{p^s}$ – квазимногообразие, заданное в $\mathcal{F}^p$ квазитождеством

$$[x, y]^{p^{s-1}} = 1 \rightarrow [x, y, x] = 1, \quad (13)$$

$\mathcal{F}_3^{p^s}$ – квазимногообразие, заданное в $\mathcal{F}^{p^s}$ квазитождеством (3),

$\mathcal{F}_{3,4}^{p^s}$ – квазимногообразие, заданное в $\mathcal{F}_3^{p^s}$ квазитождеством (4).

Нам потребуются следующие леммы из [14].

Лемма 3. В $L(\mathcal{K}^{p^s})$ истинно тождество $[x, y, z]^{3p} = 1$, где $p \in \mathbf{P}$, $p \neq 2$, $s \in \mathbf{N}$, $s \geq 2$.

Лемма 4. В многообразии $\mathcal{F}^p$ истинно тождество

$$[x, y, z]^{3p} = 1.$$

Лемма 5. В $\mathcal{F}^p$ при $p \neq 3$ для любого $k \in \mathbf{N}$ истинно тождество

$$\prod_{i=1}^k [x, x_i]^{3p} = \left[x, \prod_{i=1}^k x_i \right]^{3p},$$

а в $\mathcal{F}^3$ для любого $k \in \mathbf{N}$ истинно тождество

$$\prod_{i=1}^k [x, x_i]^3 = \left[x, \prod_{i=1}^k x_i \prod_{1 \leq i < j \leq k} [x_i, x_j] \right]^3.$$

В силу легко проверяемых коммутаторных тождеств

$$[xy, z] = [x, z][x, z, y][y, z], \quad [x, yz] = [x, z][x, y][x, y, z], \quad (14)$$

из леммы 4 вытекает, что если хотя бы одно из целых чисел k, l, m делится на p при $p \neq 3$, и делится на 9 при $p = 3$, то в квазимногообразии $\mathcal{F}^p$ истинны тождества

$$[x^k y^l, z^m] = [x^k, z^m][y^l, z^m], \quad [x^k, y^l z^m] = [x^k, y^l][x^k, z^m]. \quad (15)$$

Кроме того, из тождеств (14) следует, что в многообразии $\mathcal{N}_2$ истинны следующие тождества, выражающие используемое в дальнейших рассуждениях свойство линейности коммутаторов веса 2:

$$[xy, z] = [x, z][y, z], \quad [x, yz] = [x, y][x, z].$$

2. Основной результат

Пусть $\mathcal{M}^{p^s}$ – квазимногообразие, заданное в $\mathcal{F}_{3,4}^{p^s}$ квазитождеством

$$[x, z]^p = [x, y, x] \rightarrow [x, y, x] = 1, \quad (16)$$

а при $p = 3$ – ещё и квазитождеством

$$x^{3^{s-1}}[x, z]^3 = [x, y, x] \rightarrow [x, y, x] = 1. \quad (17)$$

Теорема 6. Пусть $p \in \mathbf{P}$, $p \neq 2$, $s \in \mathbf{N}$, $s \geq 2$, и $s > 2$ при $p = 3$, $\mathcal{K}$ – квазимногообразие групп, $q\{H_{p^s}, Z\} \subseteq \mathcal{K} \subseteq \mathcal{N}^{p^s}$. Тогда $L(\mathcal{K}) = \mathcal{M}^{p^s}$.

Доказательство. В [14, следствие 1] установлено, что $L(\mathcal{K}_3^{p^s}) = \mathcal{F}_3^{p^s}$. Из определения класса Леви сразу вытекает, что $L(\mathcal{K}_{3,4}^{p^s}) = \mathcal{F}_{3,4}^{p^s}$, и имеют место следующие включения:

$$L(\mathcal{K}) \subseteq L(\mathcal{N}^{p^s}) \subseteq L(\mathcal{K}_{3,4}^{p^s}).$$

Покажем, что $L(\mathcal{N}^{p^s}) \subseteq \mathcal{M}^{p^s}$. Достаточно проверить, что квазитождество (16), а при $p = 3$ ещё и квазитождество (17), истинны в классе $L(\mathcal{N}^{p^s})$. Пусть $G \in L(\mathcal{N}^{p^s})$, и для некоторых элементов x, y, z из группы G выполнено равенство $[x, z]^p = [x, y, x]$, которое можно записать в виде $(x^{-1}x^z)^p = [x^{-1}x^y, x]$. По определению класса Леви группа $\langle x \rangle^G \in \mathcal{N}^{p^s}$. В силу квазитождества (5) $[x^{-1}x^y, x] = 1$. Значит квазитождество (16) истинно в G . Пусть $p = 3$ и для некоторых элементов x, y, z из группы G выполнено равенство $x^{3^{s-1}}[x, z]^3 = [x, y, x]$, которое по (8) можно записать в виде

$$x^{3^{s-1}}(x^{-1}x^z)^3 = (x^{3^{s-2}}x^{-1}x^z)^3 = [x^{-1}x^y, x].$$

В силу квазитождества (5) $[x^{-1}x^y, x] = 1$. Значит квазитождество (17) истинно в G .

Итак, доказано, что $L(\mathcal{N}^{p^s}) \subseteq \mathcal{M}^{p^s}$. Значит $L(\mathcal{K}) \subseteq \mathcal{M}^{p^s}$.

Осталось установить, что $\mathcal{M}^{p^s} \subseteq L(\mathcal{K})$. Рассмотрим конечно-порожденную группу $G \in \mathcal{M}^{p^s}$. Докажем, что для любого элемента $a \in G$ выполнено $\langle a \rangle^G \in \mathcal{K}$. Обозначим $H = \langle a \rangle^G$. Можно считать, что $H = \langle a, a_1, \dots, a_n \rangle$, где $a_1 = [a, g_1], \dots, a_n = [a, g_n]$ для некоторых элементов $g_1, \dots, g_n$ группы G . Поскольку $\mathcal{M}^{p^s} \subseteq \mathcal{F}_{3,4}^{p^s}$, то из равенства $L(\mathcal{K}_{3,4}^{p^s}) = \mathcal{F}_{3,4}^{p^s}$ вытекает, что $H \in \mathcal{K}_{3,4}^{p^s} \subseteq \mathcal{N}_2$. Покажем, что H удовлетворяет условиям леммы 2. Достаточно проверить, что (5) истинно в H .

Произвольные элементы $x, y, z \in H$ можно представить в виде

$$x = a^l \prod_{i=1}^n a_i^{l_i} \prod_{i=1}^n [a, a_i]^{\alpha_i}, \quad y = a^m \prod_{i=1}^n a_i^{m_i} \prod_{i=1}^n [a, a_i]^{\beta_i}, \quad z = a^k \prod_{i=1}^n a_i^{k_i} \prod_{i=1}^n [a, a_i]^{\gamma_i}$$

для некоторых целых значений переменных $l, l_i, \alpha_i, m, m_i, \beta_i, k, k_i, \gamma_i$.

Используя линейность коммутатора веса 2 в многообразии $\mathcal{N}_2$ и линейность комму-

татора веса 3 в многообразии $\mathcal{N}_3$, можно записать

$$[y, z] = \left[a, \left(\prod_{i=1}^n g_i^{k_i} \right)^{-m} \left(\prod_{i=1}^n g_i^{m_i} \right)^k, a \right].$$

Предположим, что $x^p = [y, z]$, т. е. левая часть квазитождества (5) истинна. Коммутируя обе части равенства с произвольным элементом $g \in G$ и используя (11), получим равенство $[x^p, g] = [x, g]^p = 1$, верное для любого элемента $g \in G$. Так как квазитождество (13) истинно в группе G , то $[x, g, x] = 1$. Поскольку $[x, g, x] = [a, g, a]^{l^2} = 1$, то при $l \not\equiv 0(p)$, ввиду истинности тождества (9), получаем, что $[a, g, a] = 1$ для каждого элемента $g \in G$. Значит $[y, z] = 1$.

Предположим, что $l \equiv 0(p)$. Учитывая (1), применяя формулы (8) и (12), запишем верные равенства

$$x^p = \left(a^l \prod_{i=1}^n a_i^{l_i} \prod_{i=1}^n [a, a_i]^{\alpha_i} \right)^p = a^{lp} \prod_{i=1}^n a_i^{l_i p} = a^{lp} \prod_{i=1}^n [a, g_i]^{l_i p} = a^{lp} \prod_{i=1}^n [a, g_i^{l_i}]^p.$$

Пусть $p \neq 3$. Учитывая истинность тождества из леммы 5, а также истинность квазитождества (4), получаем, что верно равенство

$$x^p = a^{lp} [a, \prod_{i=1}^n g_i^{l_i}]^p.$$

При $p = 3$ применяем тождество из леммы 5 и получаем, что верно равенство

$$x^3 = a^{3l} \left[a, \prod_{i=1}^n g_i^{l_i} \prod_{1 \leq i < j \leq n} [g_i^{l_i}, g_j^{l_j}] \right]^3.$$

Если $l = 0$, то из истинности (16) в группе G получаем $[y, z] = 1$.

Рассмотрим теперь случай $l \equiv 0(p)$, $l \neq 0$. Тогда имеем: $lp = l'p^\delta$, где $\delta \geq 2$, $l' \not\equiv 0(p)$.

Пусть $p \neq 3$. Равенство $x^p = [y, z]$ представляется в виде

$$a^{l'p^\delta} \left[a, \prod_{i=1}^n g_i^{l_i} \right]^p = \left[a, \left(\prod_{i=1}^n g_i^{k_i} \right)^{-m} \left(\prod_{i=1}^n g_i^{m_i} \right)^k, a \right].$$

Коммутируя обе части этого равенства с произвольным элементом $g \in G$ и применяя тождества (15), (11), (12), лемму 4, квазитождество (4), получим равенство

$$[a^{l'p^\delta}, g] = [a^{l'}, g]^{p^\delta} = [a, g]^{l'p^\delta} = 1.$$

Согласно (4) верно равенство $[a, g]^{p^\delta} = 1$.

Если $\delta \leq s - 1$, то по (13) $[a, g, a] = 1$ для любого $g \in G$. Следовательно, $[y, z] = 1$.

Пусть $\delta \geq s$. По (3) верно равенство $[a, g]^{p^s} = 1$ для любого $g \in G$. Возведем обе части равенства $x^p = [y, z]$ в степень $p^{\delta-1}$ и, применяя (8), (9), получим равенства

$$\left(a^{l' p^\delta} \left[a, \prod_{i=1}^n g_i^{l_i} \right]^p \right)^{p^{\delta-1}} = a^{l' p^{2\delta-1}} \left[a, \prod_{i=1}^n g_i^{l_i} \right]^{p^\delta} = a^{l' p^{2\delta-1}} = 1.$$

Согласно (4) имеем $a^{p^{2\delta-1}} = 1$. Применяя (3), получаем, что истинно равенство $a^{p^s} = 1$. Следовательно, равенство $x^p = [y, z]$ можно записать в виде

$$\left[a, \prod_{i=1}^n g_i^{l_i} \right]^p = \left[a, \left(\prod_{i=1}^n g_i^{k_i} \right)^{-m} \left(\prod_{i=1}^n g_i^{m_i} \right)^k, a \right].$$

Из (16) вытекает, что $[y, z] = 1$.

Пусть $p = 3$. Равенство $x^3 = [y, z]$ имеет вид

$$a^{l' 3^\delta} \left[a, \prod_{i=1}^n g_i^{l_i} \prod_{1 \leq i < j \leq n} [g_i^{l_i}, g_j^{l_j}] \right]^3 = \left[a, \left(\prod_{i=1}^n g_i^{k_i} \right)^{-m} \left(\prod_{i=1}^n g_i^{m_i} \right)^k, a \right].$$

Возведя обе части этого равенства в степень 3 и используя (8), (9) получим равенство

$$a^{l' 3^{\delta+1}} \left[a, \prod_{i=1}^n g_i^{l_i} \prod_{1 \leq i < j \leq n} [g_i^{l_i}, g_j^{l_j}] \right]^{3^2} = 1.$$

Коммутируя обе части этого равенства с произвольным элементом $g \in G$ и применяя (15), (11), (12) и лемму 4, получим, что выполнены равенства

$$[a^{l' 3^{\delta+1}}, g] = [a^{l'}, g]^{3^{\delta+1}} = [a, g]^{l' 3^{\delta+1}} = 1.$$

Отсюда по (4) вытекает, что $[a, g]^{3^{\delta+1}} = 1$.

Если $\delta < s - 1$, то по (13) имеем $[a, g, a] = 1$ для любого $g \in G$. Значит $[y, z] = 1$.

Пусть $\delta \geq s - 1$. Из (3) следует, что $[a, g]^{3^s} = 1$ для любого $g \in G$. Возведем обе части равенства $x^3 = [y, z]$ в степень 3^δ и, применяя (8), (9), получим равенства

$$a^{l' 3^{2\delta}} \left[a, \prod_{i=1}^n g_i^{l_i} \prod_{1 \leq i < j \leq n} [g_i^{l_i}, g_j^{l_j}] \right]^{3^{\delta+1}} = a^{l' 3^{2\delta}} = 1.$$

Теперь по (3), (4) получаем, что истинно равенство $a^{3^s} = 1$.

Если $\delta \geq s$, то равенство $x^3 = [y, z]$ принимает вид

$$\left[a, \prod_{i=1}^n g_i^{l_i} \prod_{1 \leq i < j \leq n} [g_i^{l_i}, g_j^{l_j}] \right]^3 = \left[a, \left(\prod_{i=1}^n g_i^{k_i} \right)^{-m} \left(\prod_{i=1}^n g_i^{m_i} \right)^k, a \right].$$

В силу квазитождества (13) получаем $[y, z] = 1$.

Осталось рассмотреть случай, когда $\delta = s - 1$. В этом случае равенство $x^3 = [y, z]$ запишется в виде

$$a^{l'3^{s-1}} \left[a, \prod_{i=1}^n g_i^{l_i} \prod_{1 \leq i < j \leq n} [g_i^{l_i}, g_j^{l_j}] \right]^3 = \left[a, \left(\prod_{i=1}^n g_i^{k_i} \right)^{-m} \left(\prod_{i=1}^n g_i^{m_i} \right)^k, a \right].$$

Возведем обе части равенства $x^3 = [y, z]$ в подходящую степень u , $u \not\equiv 0(3)$, и получим

$$a^{3^{s-1}} \left[a, \left(\prod_{i=1}^n g_i^{l_i} \prod_{1 \leq i < j \leq n} [g_i^{l_i}, g_j^{l_j}] \right)^u \right]^3 = \left[a, \left(\left(\prod_{i=1}^n g_i^{k_i} \right)^{-m} \left(\prod_{i=1}^n g_i^{m_i} \right)^k \right)^u, a \right].$$

Так как квазитождество (17) истинно в группе G , то получаем, что $[y, z]^u = 1$. Следовательно, $[y, z] = 1$.

Итак, установлено, что квазитождество (5) истинно в группе H . Согласно лемме 2 $H \in q\{H_{p^s}, Z\}$. Поскольку $q\{H_{p^s}, Z\} \subseteq \mathcal{K}$, имеем $H \in \mathcal{K}$. $\square$

Лемма 7. Если G – конечно-порожденная группа, $G \in \mathcal{K} \vee qZ$, $\mathcal{K} \in L_q(\hat{\mathcal{N}}^{p^s})$, $Z_{p^s} \in \mathcal{K}$, то $G/G^{p^s} \in \mathcal{K}$, $G/G' \in q\{Z_{p^s}, Z\}$, где $G^{p^s} = \langle g^{p^s} | g \in G \rangle$.

Доказательство. Очевидно, что $G^{p^s} \trianglelefteq G$. Обозначим $\bar{G} = G/G^{p^s}$. Рассмотрим произвольный элемент $\bar{h} \in \bar{G}'$, $\bar{h} \neq \bar{1}$. Тогда $\bar{h} = gG^{p^s}$ для некоторого $g \in G'$, $g \neq 1$. По признаку принадлежности существует гомоморфизм $\varphi_g : G \rightarrow M \in \mathcal{K}$ такой, что $\varphi_g(g) \neq 1$.

Положим $\bar{\varphi}_g(\bar{x}) = \varphi_g(x)$ для любого $\bar{x} \in \bar{G}$. Проверим, что отображение $\bar{\varphi}_g$ является гомоморфизмом группы $\bar{G}$ в группу M .

Прежде всего проверим корректность отображения. Пусть $\bar{x} = \bar{y}$. Тогда по (8) $x = yz^{p^s}$ для некоторых элементов $x, y, z \in G$. Используя (6), получаем верные равенства

$$\bar{\varphi}_g(\bar{x}) = \varphi_g(x) = \varphi_g(yz^{p^s}) = \varphi_g(y)\varphi_g(z)^{p^s} = \varphi_g(y) = \bar{\varphi}_g(\bar{y}).$$

Нетрудно убедиться, что $\bar{\varphi}_g$ – гомоморфизм, причем

$$\bar{\varphi}_g(\bar{h}) = \bar{\varphi}_g(\bar{g}) = \varphi_g(g) \neq 1.$$

Поскольку $\bar{G}' = G'G^{p^s}/G^{p^s}$, то по [16, теорема 4.2.3]

$$\bar{G}/\bar{G}' \cong G/(G'G^{p^s}).$$

Таким образом, $\overline{G}/\overline{G}' \in qZ_{p^s}$. По признаку принадлежности $\overline{G} \in \mathcal{K}$.

Пусть $\overline{g} \in G/G'$, $|\overline{g}| = m$. Из (1) получаем, что $g^{mp} = 1$. Согласно (7) $g^{p^s} = 1$. Значит $G/G' \in q\{Z_{p^s}, Z\}$. $\square$

Лемма 8. *Замкнутый интервал $[qZ_{p^s}, \widehat{\mathcal{N}}^{p^s}]$ решетки $L_q(\widehat{\mathcal{N}}^{p^s})$ квазимногообразий, содержащихся в $\widehat{\mathcal{N}}^{p^s}$, изоморфно вложим в замкнутый интервал $[q(Z_{p^s}, Z), \mathcal{N}^{p^s}]$ решетки $L_q(\mathcal{N}^{p^s})$.*

Доказательство. Покажем, что отображение $\varphi : L_q(\widehat{\mathcal{N}}^{p^s}) \rightarrow L_q(\mathcal{N}^{p^s})$, при котором для любого $\mathcal{K} \in L_q(\widehat{\mathcal{N}}^{p^s})$ выполняется $\varphi(\mathcal{K}) = \mathcal{K} \vee qZ$, является изоморфным вложением интервала $[qZ_{p^s}, \widehat{\mathcal{N}}^{p^s}]$ решетки $L_q(\widehat{\mathcal{N}}^{p^s})$ в решетку $L_q(\mathcal{N}^{p^s})$.

Проверим, что верно равенство $\varphi(\mathcal{K}_1 \wedge \mathcal{K}_2) = \varphi(\mathcal{K}_1) \wedge \varphi(\mathcal{K}_2)$, т. е.

$$(\mathcal{K}_1 \wedge \mathcal{K}_2) \vee qZ = (\mathcal{K}_1 \vee qZ) \wedge (\mathcal{K}_2 \vee qZ),$$

для произвольных квазимногообразий $\mathcal{K}_1, \mathcal{K}_2$ из интервала $[qZ_{p^s}, \widehat{\mathcal{N}}^{p^s}]$.

Пусть $G \in (\mathcal{K}_1 \vee qZ) \wedge (\mathcal{K}_2 \vee qZ)$, G – конечно-порожденная группа. По лемме 7 $G/G^{p^s} \in \mathcal{K}_1 \wedge \mathcal{K}_2$, $G/G' \in q\{Z_{p^s}, Z\}$.

Легко видеть, что $G^{p^s} \cap G' = \langle 1 \rangle$. Действительно, если $g \in G^{p^s} \cap G'$, то $g = x^{p^s} = y$ для некоторых элементов $x \in G$, $y \in G'$. По (1) $y^p = 1$. Значит $x^{p^{s+1}} = 1$, и по (3) $g = x^{p^s} = 1$.

По признаку принадлежности получаем, что $G \in (\mathcal{K}_1 \wedge \mathcal{K}_2) \vee qZ$. Значит

$$(\mathcal{K}_1 \vee qZ) \wedge (\mathcal{K}_2 \vee qZ) \subseteq (\mathcal{K}_1 \wedge \mathcal{K}_2) \vee qZ.$$

Обратное включение очевидно. Следовательно, φ – гомоморфизм.

Предположим, что $\varphi(\mathcal{K}_1) = \varphi(\mathcal{K}_2)$, т. е. верно следующее равенство: $\mathcal{K}_1 \vee qZ = \mathcal{K}_2 \vee qZ$. Если G – конечно-порожденная группа, $G \in \mathcal{K}_1$, то $G \in \mathcal{K}_1 \vee qZ = \mathcal{K}_2 \vee qZ$. По лемме 7 $G \in \mathcal{K}_2$. Значит $\mathcal{K}_1 = \mathcal{K}_2$, и φ – изоморфное вложение интервала $[qZ_{p^s}, \widehat{\mathcal{N}}^{p^s}]$ решетки $L_q(\widehat{\mathcal{N}}^{p^s})$ в решетку $L_q(\mathcal{N}^{p^s})$. $\square$

В [15, теорема 2] доказано, что замкнутый интервал $[qH_{p^s}, \widehat{\mathcal{N}}^{p^s}]$ решетки $L_q(\widehat{\mathcal{N}}^{p^s})$ содержит континуум различных квазимногообразий. Из леммы 8 вытекает, что замкнутый интервал $[q\{H_{p^s}, Z\}, \mathcal{N}^{p^s}]$ решетки $L_q(\mathcal{N}^{p^s})$ также содержит континуум квазимногообразий. По теореме 6 получаем, что верна следующая

Теорема 9. *Пусть $p \in \mathbf{P}$, $p \neq 2$, $s \geq 2$, и $s > 2$ при $p = 3$. Существует континуум различных квазимногообразий, каждое из которых порождает класс Леви, совпадающий с $L(q\{H_{p^s}, Z\})$.*

Список литературы

- [1] F.W. Levi, *Groups in which the commutator operation satisfies certain algebraic conditions*, J. Indian Math. Soc. (N.S.) **6**, 87–97 (1942).

- [2] L.C. Kappe, *On Levi-formations*, Arch. Math. **23**, 561–572 (1972).
DOI: <https://doi.org/10.1007/BF01304934>
- [3] L.C. Kappe, R.F. Morse, *Groups with 3-abelian normal closures*, Arch. Math. **51** (2), 104–110 (1988).
DOI: <https://doi.org/10.1007/BF01206466>
- [4] А.И. Будкин, *Квазимногообразия Леви*, Сиб. матем. журн. **40** (2), 266–270 (1999).
URL: <https://www.mathnet.ru/rus/smj148>
- [5] А.И. Будкин, *О классах Леви, порожденных нильпотентными группами*, Алгебра и логика **39** (6), 635–647 (2000).
URL: <https://www.mathnet.ru/rus/al245>
- [6] А.И. Будкин, Л.В. Таранина, *О квазимногообразиях Леви, порожденных нильпотентными группами*, Сиб. матем. журн. **41** (2), 270–277 (2000).
URL: <https://www.mathnet.ru/rus/smj1524>
- [7] R.F. Morse, *Levi-properties generated by varieties*, In: The mathematical legacy of Wilhelm Magnus: groups, geometry and special functions, Contemp. Math. **169**, 467–474 (1994).
DOI: <http://dx.doi.org/10.1090/conm/169/01675>
- [8] А.И. Будкин, В.А. Горбунов, *К теории квазимногообразий алгебраических систем*, Алгебра и логика **14** (2), 123–142 (1975).
URL: <https://www.mathnet.ru/rus/al1462>
- [9] В.В. Лодейщикова, *О квазимногообразиях Леви, порожденных нильпотентными группами*, Изв. АлтГУ (1), 26–29 (2009).
- [10] В.В. Лодейщикова, *О классах Леви, порожденных нильпотентными группами*, Сиб. матем. журн. **51** (6), 1359–1366 (2010).
URL: <https://www.mathnet.ru/rus/smj2166>
- [11] В.В. Лодейщикова, *О квазимногообразиях Леви экспоненты p^s* , Алгебра и логика **50** (1), 26–41 (2011).
URL: <https://www.mathnet.ru/rus/al473>
- [12] С.А. Шахова, *Об аксиоматическом ранге классов Леви*, Алгебра и логика **57** (5), 587–600 (2018).
DOI: <https://doi.org/10.33048/alglog.2018.57.506>
- [13] S.A. Shakhova, *The axiomatic rank of the Levi class generated by the almost Abelian quasivariety of nilpotent groups*, Lobachevskii J. Math. **41** (9), 1680–1683 (2020).
DOI: <https://doi.org/10.1134/S1995080220090243>
- [14] С.А. Шахова, *Классы Леви квазимногообразий групп с коммутантом экспоненты p* , Алгебра и логика **60** (5), 510–524 (2021).
DOI: <https://doi.org/10.33048/alglog.2021.60.504>

- [15] В.В. Лодейщикова, С.А. Шахова, *Классы Леви квазимногообразий nilпотентных групп экспоненты p^s* , Алгебра и логика **61** (1), 77–92 (2022).
DOI: <https://doi.org/10.33048/alglog.2022.61.104>
- [16] М.И. Каргаполов, Ю.И. Мерзляков, *Основы теории групп*, Наука, М., 1977.
- [17] А.И. Мальцев, *Алгебраические системы*, Наука, М., 1970.
- [18] А.И. Будкин, *Квазимногообразия групп*, Изд-во Алт. гос. ун-та, Барнаул, 2002.
- [19] В.А. Горбунов, *Алгебраическая теория квазимногообразий*, Науч. книга, Новосибирск, 1999.

Светлана Александровна Шахова

Алтайский государственный университет,
пр. Ленина, д. 61, г. Барнаул, 656049, Россия
e-mail: ssa@math.asu.ru

Levi classes of quasivarieties of 2-nilpotent groups

S.A. Shakhova

Abstract. The Levi class $L(\mathcal{M})$ generated by the class of groups $\mathcal{M}$ is the class of all groups in which the normal closure of each cyclic subgroup belongs to $\mathcal{M}$. Let p be a prime number, $p \neq 2$, s be a natural number, $s \geq 2$, and $s > 2$ for $p = 3$; H_{p^s} be a free group of rank 2 in the variety of nilpotent groups of class ≤ 2 of exponent p^s with commutator subgroup of exponent p ; Z is an infinite cyclic group; $q\{H_{p^s}, Z\}$ is a quasivariety generated by the set of groups $\{H_{p^s}, Z\}$. We find a basis of quasi-identities of the Levi class $L(q\{H_{p^s}, Z\})$ and establish that there exists a continuous set of quasivarieties $\mathcal{K}$ such that $L(\mathcal{K}) = L(q\{H_{p^s}, Z\})$.

Keywords: quasivariety, Levi class, nilpotent group.

DOI: 10.26907/2949-3919.2025.1.64-77

References

- [1] F.W. Levi, *Groups in which the commutator operation satisfies certain algebraic conditions*, J. Indian Math. Soc. (N.S.) **6**, 87–97 (1942).
- [2] L.C. Kappe, *On Levi-formations*, Arch. Math. **23**, 561–572 (1972).
DOI: <https://doi.org/10.1007/BF01304934>
- [3] L.C. Kappe, R.F. Morse, *Groups with 3-abelian normal closures*, Arch. Math. **51** (2), 104–110 (1988).
DOI: <https://doi.org/10.1007/BF01206466>
- [4] A.I. Budkin, *Levi quasivarieties*, Siberian Math. J. **40** (2), 225–228 (1999).
DOI: <https://doi.org/10.1007/s11202-999-0003-x>
- [5] A.I. Budkin, *Levi classes generated by nilpotent groups*, Algebra Logic **39** (1), 363–369 (1999).
DOI: <https://doi.org/10.1023/A:1010224301576>
- [6] A.I. Budkin, L. V. Taranina, *On Levi quasivarieties generated by nilpotent groups*, Siberian Math. J. **41** (2), 218–223 (2000).
DOI: <https://doi.org/10.1007/BF02674590>

- [7] R.F. Morse, *Levi-properties generated by varieties*, In: The mathematical legacy of Wilhelm Magnus: groups, geometry and special functions, Contemp. Math. **169**, 467–474 (1994). DOI: <http://dx.doi.org/10.1090/conm/169/01675>
- [8] A.I. Budkin, V.A. Gorbunov, *On the theory of quasivarieties of algebraic systems*, Algebra i Logika **14** (2), 123–142 (1975) [in Russian].
- [9] V.V. Lodeyshchikova, *On Levi quasivarieties generated by nilpotent groups*, Izv. AltGU (1), 26–29 (2009).
- [10] V.V. Lodeyshchikova, *The Levi classes generated by nilpotent groups*, Siberian Math. J. **51** (6), 1075–1080 (2010). DOI: <https://doi.org/10.1007/s11202-010-0105-5>
- [11] V.V. Lodeyshchikova, *Levi quasivarieties of exponent p^s* , Algebra Logic **50** (1), 17–28 (2011). DOI: <https://doi.org/10.1007/s10469-011-9121-1>
- [12] S.A. Shakhova, *The axiomatic rank of Levi classes*, Algebra Logic **57** (5), 381–391 (2018). DOI: <https://doi.org/10.1007/s10469-018-9510-9>
- [13] S.A. Shakhova, *The axiomatic rank of the Levi class generated by the almost Abelian quasivariety of nilpotent groups*, Lobachevskii J. Math. **41** (9), 1680–1683 (2020). DOI: <https://doi.org/10.1134/S1995080220090243>
- [14] S.A. Shakhova, *Levi classes of quasivarieties of groups with commutator subgroup of order p* , Algebra Logic **60** (5), 336–347 (2021). DOI: <https://doi.org/10.1007/s10469-021-09659-3>
- [15] V.V. Lodeyshchikova, S.A. Shakhova, *Levi classes of quasivarieties of nilpotent groups of exponent p^s* , Algebra Logic **61** (1), 54–66 (2022). DOI: <https://doi.org/10.1007/s10469-022-09674-y>
- [16] M. I. Kargapolov, Ju.I. Merzljakov, *Fundamentals of the theory of groups*, Graduate Texts in Mathematics **62**, Springer-Verlag, New York–Berlin, 1979.
- [17] A.I. Mal'cev, *Algebraic Systems*, Springer-Verlag, New York–Heidelberg, 1973. DOI: <https://doi.org/10.1007/978-3-642-65374-2>
- [18] A.I. Budkin, *Quasivarieties of groups*, Izd-vo Altai State Univ., Barnaul, 2002 [in Russian].
- [19] V.A. Gorbunov, *Algebraic theory of quasivarieties*, Springer New York, New York, 1998.

Svetlana Aleksandrovna Shakhova

Altai State University,

61 Lenina av., Barnaul 656049, Russia,

e-mail: ssa@math.asu.ru

V Конференция математических центров России г. Красноярск, 11–16 августа 2025

V Конференция математических центров России – площадка для обмена последними достижениями в различных областях математики, обсуждения актуальных проблем и укрепления научных связей между ведущими математическими центрами страны.

Конференция призвана собрать широкий круг увлеченных математикой исследователей от студентов до ученых с мировым именем. К участию в конференции приглашаются представители российской и мировой математической общественности: аспиранты, студенты, сотрудники региональных математических центров и математических центров мирового уровня, научные и педагогические работники.

Формат работы конференции очный, будут представлены пленарные, секционные и постерные доклады по актуальным направлениям развития и современным достижениям математической науки.

В качестве финансовой поддержки молодых исследователей организаторы конференции предоставят бесплатное проживание ограниченному числу участников по рекомендации руководителей секций.

Секции конференции:

- алгебра и алгебраическая комбинаторика;
- алгебраическая геометрия;
- вещественный и функциональный анализ;
- геометрия и топология;
- дифференциальные уравнения, динамические системы и оптимальное управление;
- история математики и математическое образование;
- комплексный анализ;
- математическая логика и теоретическая информатика;
- прикладная математика и математическое моделирование;
- спектральная теория и математическая физика;
- теория вероятностей;
- теория чисел и дискретная математика;
- уравнения с частными производными;
- постерная секция (Молодежная секция. Для представления доклада на постерной секции подается заявка на участие в профильной секции, решение о включении доклада в программу принимают руководители соответствующей профильной секции).

Работа конференции будет проходить в Красноярске на базе Сибирского федерального университета.

Важные даты

- **До 24 мая** – регистрация заявок на участие в конференции.
- **До 9 июня** – определение списка секционных докладчиков. Рассылка оргкомитетом приглашений на конференцию.
- **До 12 июня** – прием заявок на бесплатное проживание от молодых участников.
- **До 19 июня** – определение списка молодых участников, которым будет предоставлено проживание на время конференции.
- **До 26 июня** – объявление предварительных программ работы секций.
- **До 4 августа** – представление сборника материалов конференции.

Сайт конференции: <https://kmc.sfu-kras.ru/conf2025/>.

XVII Международная Казанская школа-конференция ”Теория функций, ее приложения и смежные вопросы” г. Казань, 23–28 августа 2025

Казанский (Приволжский) федеральный университет совместно с Московским государственным университетом при поддержке Академии наук Республики Татарстан и Научно-образовательного математического центра ПФО организуют **с 23 по 28 августа 2025 г.** XVII Международную Казанскую школу-конференцию “Теория функций, ее приложения и смежные вопросы”. Ожидается вхождение в число организаторов мероприятия Математического института имени В.А. Стеклова РАН (официальное решение должно быть утверждено советом института в ближайшее время).

Будут работать следующие секции:

- теория функций действительного переменного;
- функциональный анализ и квантовая теория информации;
- теория функций комплексного переменного;
- краевые задачи для аналитических функций и эллиптических систем уравнений;
- дифференциальные и интегральные уравнения;
- приложения анализа в механике и физике.

Предполагается, что на конференции будут сделаны пленарные доклады, посвященные юбилейным датам замечательных математиков, долгие годы работавших в Казанском университете: 100-летию со дня рождения профессора Любови Ивановны Чибриковой и 80-летию со дня рождения профессора Данияра Хамидовича Муштари.

Работа конференции будет проходить в Казани на базе Института математики и механики им. Н.И.Лобачевского КФУ. Председатель оргкомитета – заведующий отделением математики Института математики и механики им. Н.И.Лобачевского КФУ профессор С.Р.Насыров, председатель программного комитета – академик РАН Б.С.Кашин.

Программа школы-конференции будет включать лекции ведущих российских ученых и доклады участников конференции. Тезисы докладов конференции будут опубликованы к ее открытию в очередном томе Трудов Математического центра имени Н.И. Лобачевского, материалы лучших докладов будут рекомендованы для публикации в авторитетные научные журналы.

Требования к оформлению тезисов докладов, информация об организационном взносе и другие полезные сведения будут сообщены в последующих информационных письмах и размещены на сайте конференции <https://kpfu.ru/math/conference/tf2025>.

Приглашаем вас принять участие в работе школе-конференции. Для этого необходимо зарегистрироваться на сайте <https://kpfu.ru/math/conference/tf2025> до **15 июня 2025 г.** По всем вопросам обращаться к ученому секретарю школы-конференции Даутовой Дине Наилевне по электронной почте theorfunc@gmail.com или по телефону +79274355448.

Календарь конференций (май 2025 г. – июль 2025 г.)

Май 2025 г.

- **Workshop OTHA Spring 2025 on operator theory and harmonic analysis and their applications**
Институт математики НАН Республики Армения, г. Ереван, Армения, 27 апреля–2 мая 2025 г.
Сайт: <https://otha.sfedu.ru/workshop-otha-spring-2025>
Участие в конференции с докладом – по приглашению организаторов.
- **XXXVIII Международная Воронежская весенняя математическая школа “Современные методы теории краевых задач. Понтрягинские чтения – XXXVI”, посвященная 120-летию со дня рождения академика Сергея Михайловича Никольского**
г. Воронеж, Россия, 30 апреля–4 мая 2025 г.
Сайт: <https://vvmsh.math-vsuv.ru>
Регистрация и прием тезисов завершены.
- **XXIV Международная конференция “Алгебра, теория чисел, дискретная геометрия и многомасштабное моделирование. Современные проблемы, приложения и проблемы истории”, посвященная 110-летию со дня рождения академика Ю.В. Линника и 110-летию со дня рождения профессора А.Б. Шидловского и 80-летию со дня рождения профессора Г.И. Архипова**
ТГПУ им. Л. Н. Толстого, г. Тула, Россия, 14–17 мая 2025 г.
Сайт: <https://poivs.tsput.ru/conf/international/XXIV>
Регистрация и прием тезисов завершены.
- **XIV Всероссийская научно-методическая конференция “Актуальные проблемы преподавания математики в техническом вузе”**
г. Омск, Россия, 16–17 мая 2025 г.
Сайт: <https://conferences.omgtu.ru/conference/APPM2025>
Регистрация и прием тезисов завершены.
- **Всероссийская конференция “Дифференциальные игры, теория управления и оптимизация” (DGCTO-2025), посвященная памяти профессора В.И. Ухоботова**
Челябинский государственный университет, г. Челябинск, Россия, 19–21 мая 2025 г.
Сайт: <https://sites.google.com/view/dgcto2025>
Регистрация и прием тезисов завершены.

- **Международная конференция “Современные проблемы математики и её приложения”**

Институт математики им. А.Джураева Национальной академии наук Таджикистана, г. Душанбе, Таджикистан, 30–31 мая 2025 г.

Сайт: <https://mitas.tj>

Июнь 2025 г.

- **Конференция “Геометрия, топология и математическая физика” памяти Сергея Петровича Новикова**

МГУ, МИАН, г. Москва, Россия, 2–6 июня 2025 г.

Сайт: <http://www.mathnet.ru/rus/conf2561>

- **Теория функций, теория операторов и квантовая теория информации**

г. Коломна, Россия, 2–6 июня 2025 г.

Сайт: <https://www.mathnet.ru/rus/conf2585>

- **Международная конференция “Алгебраические методы в геометрии и теории чисел”, посвященная 85-летию академика В.П. Платонова**

МИАН, г. Москва, Россия, 16–20 июня 2025 г.

Сайт: <https://www.mathnet.ru/rus/conf2500>

- **Всероссийская конференция с международным участием “Теория управления и математическое моделирование” (СТММ 2025), посвященная памяти профессора Н.В. Азбелева и профессора Е.Л. Тонкова**

Удмуртский государственный университет, г. Ижевск, Россия, 16–20 июня 2025 г.

Сайт: <https://lomonosov-msu.ru/rus/event/9543>

Регистрация завершена.

- **16-ая Санкт-Петербургская конференция по спектральной теории и математической физике**

Песочная набережная, дом 10, г. Санкт-Петербург, Россия, 23–27 июня 2025 г.

Сайт: <https://www.mathnet.ru/rus/conf2579>

- **Летняя школа “Криптография, Статистика и Машинное Обучение”**

г. Цахкадзор, Армения, 29 июня–6 июля 2025 г.

Сайт: <http://mathschool.ysu.am/mss2025>

Срок регистрации – до 01 июня 2025 г.

- **34-ая Санкт-Петербургская летняя конференция по математическому анализу**

Международный математический институт им. Л. Эйлера, Песочная набережная, 10, г. Санкт-Петербург, Россия, 30 июня–5 июля 2025 г.

Сайт: <https://www.mathnet.ru/rus/conf2578>

Июль 2025 г.

- **Международная конференция “Теория функций и ее приложения”, посвященная 120-летию со дня рождения академика РАН Сергея Михайловича Никольского**

Конференция будет проходить 1-5 июля 2025 года в режиме онлайн.

Сайт: <https://www.mathnet.ru/rus/conf2526>

Срок регистрации – до 30 апреля 2025 г.

- **Алгебраические группы: сезон белых ночей V**

Международный математический институт им. Л. Эйлера, Песочная набережная, 10, г. Санкт-Петербург, Россия, 7–11 июля 2025 г.

Сайт: <https://www.mathnet.ru/rus/conf2577>

- **Elliptic curves and their applications**

Institute of Mathematics National Academy of Sciences of Armenia, Yerevan, Армения, 14–26 июля 2025 г.

Сайт: <https://sites.google.com/view/ecasummerschool2025>

Регистрация завершена.

- **21st International Geometry Symposium In Honor of Prof. Dr. Arif Salimov**

Erzurum Technical University, Erzurum, Турция, 17–19 июля 2025 г.

Сайт: <https://www.geometrysymposium.org>

Срок регистрации – до 27 июня 2025 г.

- **Международная школа “Передовые методы современной теоретической физики: интегрируемые и стохастические системы”**

Объединенный институт ядерных исследований, г. Дубна, Россия, 20–25 июля 2025 г.

Сайт: <https://indico.jinr.ru/event/5276>

Срок регистрации – до 15 июня 2025 г.

- **15-й Конгресс ISAAC**

Назарбаев Университет, г. Астана, Казахстан, 21–25 июля 2025 г.

Сайт: <https://isaac2025.org>

Срок регистрации – до 16 мая 2025 г.