ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 30 № 1 2024

УДК 512.554

ВОПРОСЫ СТРОЕНИЯ КОНЕЧНЫХ КВАЗИПОЛЕЙ ХОЛЛА[1]

О. В. Кравцова, В. С. Логинова

Конечные квазиполя изучаются взаимосвязанно с проективными плоскостями трансляций уже более века. Выявление особенностей строения и аномальных свойств представляет важный шаг в решении проблемы классификации конечных квазиполей. В статье решаются структурные вопросы для конечных квазиполей Холла. Это двумерные над центром квазиполя, все нецентральные элементы которых удовлетворяют одному квадратному уравнению. Группа автоморфизмов действует транзитивно на нецентральных элементах. Все квазиполя Холла одного порядка координатизируют одну плоскость трансляций — плоскость Холла. Метод регулярного множества, основанный на записи умножения как линейного преобразования, применяется для описания подполей и подквазиполей, спектров и автоморфизмов. Приводится алгоритм вычисления количества попарно неизоморфных квазиполей Холла одного порядка. Уточняется теорема М. Кордеро и В. Джа 2009 г. о покрытии и примитивности, с контрпримерами примитивных квазиполей Холла. Указаны квазиполя порядка 16 с покрытием подполями порядка 4, не содержащиеся в квазиполях Холла. В связи с примерами перечислены вопросы дальнейшего исследования.

Ключевые слова: квазиполе, квазиполе Холла, регулярное множество, спектр, автоморфизм, правопримитивное квазиполе.

O. V. Kravtsova, V. S. Loginova. Questions of the structure of finite Hall quasifields.

The finite quasifields have been studied together with projective translation planes for more than a century. The identification of structural features and anomalous properties is an important step in solving the classification problem of finite quasifields. The article solves the structural problems for finite Hall quasifields. These are quasifields two-dimensional over the center such that all non-central elements are the roots of a unique quadratic equation. The automorphism group acts transitively on non-central elements. All Hall quasifields of the same order coordinatize one isomorphic translation plane, which is the Hall plane. The spread set method allows to present the multiplication rule as a linear transformation. The method is used to describe subfields, subquasifields, spectra, and automorphisms. An algorithm to calculate the number of pairwise non-isomorphic Hall quasifields of the same order is given. The covering and primitivity theorem by M. Cordero and V. Jha (2009) is clarified, with the primitive Hall quasifields counter-examples. The quasifields of order 16 covered by subfields of order 4 not contained in any Hall quasifield are presented. The examples also raise the questions for further investigation.

Keywords: quasifield, Hall quasifield, spread set, spectrum, automorphism, right-primitive quasifield.

MSC: 12K99, 15A04, 17A35, 17D99

DOI: 10.21538/0134-4889-2024-30-1-128-141

Памяти профессора Владимира Михайловича Левчука

Введение

Координатизиция точек и прямых проективной плоскости элементами алгебраической системы устанавливает связь геометрических свойств плоскости с алгебраическими свойствами координатизирующего множества. С начала прошлого века взаимосвязанно изучаются плоскости трансляций и координатизирующие их квазиполя. К понятию квазиполя приходят, исключив из списка аксиом тела ассоциативность умножения и один из дистрибутивных законов.

О п р е д е л е н и е 1. Алгебраическая система $Q = (Q, +, \cdot)$ с бинарными операциями $+$ и $\cdot$ называется правым квазиполем, если

[1]Работа поддержана Красноярским математическим центром, финансируемым Минобрнауки РФ (Соглашение 075-02-2023-936).

1) $(Q,+)$ — абелева группа;
2) $Q^* = (Q \setminus \{0\}, \cdot)$ — лупа;
3) выполнен правый дистрибутивный закон $(a+b)c = ac + bc$ $(a,b,c \in Q)$;
4) $a \cdot 0 = 0$ для всех $a \in Q$;
5) уравнение $xa = xb + c$ однозначно разрешимо для всех $a,b,c \in Q$, $a \neq b$.

Левое квазиполе определяют аналогично.

Первые примеры конечных квазиполей, не являющихся полями, представлены в 1906–1907 гг. в работах Л. Диксона [1], О. Веблена и Д. Маклагана-Веддерберна [2]. В литературе до 1975 г. для квазиполей, как правило, использовался термин "системы Веблена — Веддерберна" [3, 20.4]. Квазиполя обладают, в сравнении с полями, аномальными свойствами, но также имеют широкое применение в проективной геометрии, теории кодирования, комбинаторике.

Определение 2. Ядром правого квазиполя Q называется множество элементов $k \in Q$, удовлетворяющих условиям:
1) $k(a+b) = ka + kb$;
2) $k(ab) = (ka)b$ для всех $a,b \in Q$.

Ядро квазиполя всегда есть тело, поэтому обязательно содержит простое подполе, образованное целочисленными кратными единицы. Квазиполе можно рассматривать как векторное пространство над своим ядром [4, теорема 7.2]. Таким образом, конечное квазиполе имеет порядок p^m, где p — простое число. Ясно, что квазиполе простого порядка p является полем; минимальный порядок нетривиального квазиполя равен 9.

Если в квазиполе выполняются оба дистрибутивных закона, то оно называется *полуполем* (квазитело, по терминологии А. Г. Куроша [5]). Первые примеры нетривиальных конечных полуполей указаны Л. Диксоном в 1906 г.

Если в (правом) квазиполе умножение ассоциативно, то такое квазиполе называют (правым) *почти-полем*. Первые примеры почти-полей были построены Л. Диксоном в 1905 г. [6], все конечные почти-поля полностью классифицировал Х. Цассенхауз в 1936 г. [7].

Строение даже известных собственных конечных квазиполей изучено мало, как показывает обзор 2007 г. [8]. В частности, не решена задача классификации всех конечных квазиполей и даже полуполей, в связи с чем любые классификационные результаты в этой области имеют значительную ценность.

Первые примеры конечных квазиполей, не являющихся ни полуполями, ни почти-полями, построил М. Холл [9] в 1943 г. (см. также [3, 20.4]).

Пусть многочлен $\varphi(x) = x^2 - rx - s$ неприводим над $GF(q)$ $(q = p^n$, p — простое). Левое квазиполе Q порядка q^2 с ядром $K \simeq GF(q)$ называется *квазиполем Холла*, если закон умножения в нем определен правилом (1, λ — базис, $x,y,z,t \in GF(q)$):

$$(x+\lambda y)(z+\lambda t) = xz - y^{-1}t\varphi(x) + \lambda(yz - xt + rt) \quad \text{при} \quad y \neq 0,$$

$$x(z+\lambda t) = xz + \lambda(xt).$$

Тогда каждый элемент из $Q \setminus K$ — это корень многочлена $\varphi(x)$, каждый элемент из K коммутирует со всеми элементами из Q (т. е. K — *центр* квазиполя Q). Эти свойства, вытекающие из определения операции, могут служить эквивалентным определением квазиполя Холла. Более точно они описаны М. Билиотти с соавторами.

Следствие 1 [10, следствие 14.3.9]. *Пусть Q — конечное квазиполе размерности 2 над ядром K. Тогда следующие утверждения эквивалентны*:
(1) *Q — квазиполе Холла*;
(2) *группа $\mathrm{Aut}_K Q$ транзитивна на $Q \setminus K$*;
(3) *Q — квазиполе Холла с центром K*;

(4) *каждый элемент из* $Q \setminus K$ *является корнем одного квадратного многочлена над* K;

(5) *каждый элемент из* $Q \setminus K$ *— это корень одного неприводимого квадратного многочлена над* K.

Здесь и далее $\mathrm{Aut}_K Q$ обозначает подгруппу автоморфизмов квазиполя Q, фиксирующих элементы ядра K. Мы будем рассматривать правое квазиполе с такими условиями, выбирая запись его элементов векторами-строками.

Конечное квазиполе Холла является а) полем тогда и только тогда, когда оно имеет порядок 4; б) нетривиальным почти-полем, если $K = GF(3)$ и $\varphi(x) = x^2 + 1$ [4, лемма 9.2]. Квазиполя Холла над одним конечным полем K *изотопны* и координатизируют изоморфные плоскости трансляций — *плоскости Холла* [11, теоремы 3.2 и 4.2]. Так, все три неизоморфных квазиполя Холла порядка 9 изотопны почти-полю Диксона порядка 9.

Следующие вопросы строения конечных полуполей и квазиполей рассматривались в различных ситуациях уже давно и записаны В. М. Левчуком в [12].

(A) *Перечислить максимальные подполя, найти их число и возможные порядки.*

(B) *Выявить конечные квазиполя* Q *с неоднопорожденной лупой* Q^*.

(C) *Выявить, какие возможны спектры лупы* Q^* *конечного полуполя и квазиполя* Q.

(D) *Найти порядок группы автоморфизмов.*

В настоящей статье мы приводим исследование проблем **(A)–(D)** для конечных квазиполей Холла, перечисляя известные результаты вместе с доказательством новых. Квазиполя Холла давно известны и хорошо изучены, тем не менее некоторые вопросы заслуживают внимательного рассмотрения, как показывает обсуждение проблемы примитивности в разд. 3.

Решение вопросов **(A)–(D)** для конечных квазиполей Холла было инициировано Владимиром Михайловичем Левчуком. Мы посвящаем статью его памяти.

1. Регулярное множество, автоморфизмы, изоморфизм

Для решения вопросов, указанных выше, применим метод регулярного множества (подробнее см. [13]).

Пусть $Q = (Q, +, \cdot)$ — (правое) квазиполе порядка q^d ($q = p^n$, p — простое число) с ядром $K \simeq GF(q)$. Тогда Q есть (левое) векторное пространство размерности d над полем K и для любого фиксированного элемента $m \in Q$ правое умножение $\rho_m : x \to xm$ является линейным преобразованием Q (согласно определению ядра). Множество всех таких преобразований $\Sigma = \{\rho_m \mid m \in Q\}$ называют *регулярным множеством* квазиполя Q (термин предложен Н. Д. Подуфаловым), в иностранной литературе — *spread set.* Из определения квазиполя следует, что множество Σ содержит нулевое и тождественное преобразования; разность любых двух различных элементов множества Σ есть обратимое преобразование. Множество матриц

$$R = \{\theta(m) \mid m \in Q\} \subset GL_d(q) \cup \{0\}$$

всех указанных линейных преобразований при определенном выборе базиса линейного пространства Q над K также будем называть регулярным множеством — для упрощения терминологии.

Пусть Q — правое квазиполе Холла порядка q^2 с ядром (центром) $K \simeq GF(q)$ и ассоциированным многочленом $\varphi(x) = x^2 - rx - s$. Будем записывать элементы Q как строки (x, y), $x, y \in K$, и выберем базис e_1, e_2 линейного пространства Q, где $e_1 = 1$ — единица квазиполя, $e_2 \notin K$. Тогда матрицы регулярного множества имеют вид [13]

$$\theta(x,y) = \begin{pmatrix} x & y \\ -y^{-1}\varphi(x) & r - x \end{pmatrix}, \quad y \neq 0, \qquad \theta(x,0) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}, \tag{1.1}$$

умножение векторов-строк выполняется по правилу

$$(u, v) \cdot (x, y) = (u, v)\, \theta(x, y), \quad u, v, x, y \in K.$$

Отметим, что запись закона умножения в координатной форме в квазиполе Холла Q при $e_1 = 1$ не зависит от выбора второго базисного элемента. Это объясняется транзитивностью группы $\mathrm{Aut}_K Q$ на $Q \setminus K$. Множество матриц $\theta(x, y)$ при $y \neq 0$ составляет класс сопряженности в $GL_2(q)$ с характеристическим многочленом $\varphi(x)$ [14].

Дополним следствие 1 информацией о группах $\mathrm{Aut}\, Q$ и $\mathrm{Aut}_K Q$. Обозначим через P минимальное подполе в K, содержащее коэффициенты r, s многочлена $\varphi(x)$. Пусть $|P| = p^t$; ясно, что $t|n$ и n/t — нечетное число, иначе K содержит поле разложения $\varphi(x)$. В частности, если $n = 2^k$, то $P = K$.

Теорема 1. *Группа автоморфизмов* $\mathrm{Aut}\, Q$ *квазиполя Холла* Q *имеет порядок* $(q^2 - q)n/t$ *и состоит из всех полулинейных преобразований*

$$(x, y) \to (x^\sigma, y^\sigma) \begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix}, \tag{1.2}$$

где $a, b \in K$, $b \neq 0$, $\sigma \in \mathrm{Aut}_P K$. *Стабилизатор ядра* $\mathrm{Aut}_K Q$ *имеет порядок* $q^2 - q$ *и состоит из всех линейных преобразований* (1.2) *при* $\sigma = 1$.

Д о к а з а т е л ь с т в о. Пусть α — автоморфизм квазиполя Q. Тогда α является полулинейным преобразованием двумерного векторного пространства:

$$(x, y)^\alpha = (x^\sigma, y^\sigma)A,$$

где $\sigma \in \mathrm{Aut}\, K$, $A \in GL_2(q)$. Из выбора первого базисного элемента $e_1 = 1$ следует, что

$$A = \begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix}, \quad a, b \in K.$$

Рассмотрим условие сохранения операции умножения:

$$(u, v)^\alpha \cdot (x, y)^\alpha = ((u, v)(x, y))^\alpha,$$

$$(u^\sigma, v^\sigma)A\theta((x^\sigma, y^\sigma)A) = (u^\sigma, v^\sigma)\theta^\sigma(x, y)A,$$

$$A\theta((x^\sigma, y^\sigma)A) = \theta^\sigma(x, y)A \qquad \forall x, y \in K$$

(в правой части поэлементное действие автоморфизма на матрицу). Если $\alpha \in \mathrm{Aut}_K Q$, то $\sigma = 1$ и матрица A должна удовлетворять условию $A\theta((x, y)A) = \theta(x, y)A$ при любых $x, y \in K$. Легко видеть, что при $y = 0$ условие выполнено. При $y \neq 0$ для матрицы $\theta(x, y)$ вида (1.1) получим

$$\begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix} \begin{pmatrix} x + ay & by \\ -(by)^{-1}\varphi(x + ay) & r - x - ay \end{pmatrix} = \begin{pmatrix} x & y \\ -y^{-1}\varphi(x) & r - x \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix},$$

равенство верно при любых $a, b, x, y \in K$, $b \neq 0$. Из доказанной транзитивности группы

$$\mathrm{Aut}_K Q = \{(x, y) \to (x + ay, by) \mid a, b \in K,\ b \neq 0\}$$

на $Q \setminus K$ вытекает, что полулинейное преобразование $\alpha \in \mathrm{Aut}\, Q$ достаточно рассмотреть для $A = E$. Из условия $\theta(x^\sigma, y^\sigma) = \theta^\sigma(x, y)$ имеем $\varphi(x^\sigma) = \varphi^\sigma(x)$ и $r - x^\sigma = (r - x)^\sigma$, откуда $r^\sigma = r$, $s^\sigma = s$, т. е. $\sigma \in \mathrm{Aut}_P K$.

Теорема доказана.

Непосредственным следствием доказанной теоремы является критерий изоморфизма квазиполей Холла одного порядка, уточняющий результат [11, лемма 1.1].

Следствие 2. *Два квазиполя Холла Q_1 и Q_2 порядка q^2 с центром $K \simeq GF(q)$ и ассоциированными многочленами $\varphi_1(x) = x^2 - r_1x - s_1$ и $\varphi_2(x) = x^2 - r_2x - s_2$ изоморфны тогда и только тогда, когда существует автоморфизм σ поля K с условием $r_1^\sigma = r_2$, $s_1^\sigma = s_2$.*

Таким образом, для определения количества попарно неизоморфных квазиполей Холла одного порядка следует группировать неприводимые многочлены в $K[x]$ в зависимости от поля их коэффициентов P. В частности, все квазиполя Холла порядка p^2 с разными ассоциированными многочленами попарно неизоморфны.

П р и м е р 1. Найдем количество попарно неизоморфных квазиполей Холла порядка 3^{60},

$$|K| = 3^{30}, \quad p = 3, \quad n = 30 = 2 \cdot 3 \cdot 5.$$

Общее количество неприводимых многочленов второй степени над K определяется следующим образом:

$$\frac{q^2 - q}{2} = \frac{3^{30}(3^{30} - 1)}{2}.$$

Подполе коэффициентов P имеет порядок p^t, где n/t — нечетное число. Значит, возможные варианты порядков $P \neq K$ — это 3^{10}, 3^6, 3^2. Обозначим соответствующие подполя K_{10}, K_6, K_2.

Число квадратных неприводимых многочленов в $K_2[x]$ равно $3^2(3^2-1)/2$. Они разбиваются на пары за счет $\operatorname{Aut} K_2 \simeq \mathbb{Z}_2$, число таких пар

$$m_1 = \frac{3^2(3^2 - 1)}{2 \cdot 2} \in \mathbb{N}.$$

Число квадратных неприводимых многочленов в $K_6[x]$ равно $3^6(3^6 - 1)/2$. Сюда входят и многочлены из $K_2[x]$; исключим их и получим

$$\frac{3^6(3^6 - 1)}{2} - \frac{3^2(3^2 - 1)}{2}.$$

Так как $\operatorname{Aut} K_6 \simeq \mathbb{Z}_6$, разобъем эти многочлены на шестерки; имеем

$$m_2 = \frac{1}{6}\left(\frac{3^6(3^6 - 1)}{2} - \frac{3^2(3^2 - 1)}{2}\right) \in \mathbb{N}.$$

Для многочленов из $K_{10}[x]$ и автоморфизмов из $\operatorname{Aut} K_{10} \simeq \mathbb{Z}_{10}$ аналогично получим число

$$m_3 = \frac{1}{10}\left(\frac{3^{10}(3^{10} - 1)}{2} - \frac{3^2(3^2 - 1)}{2}\right) \in \mathbb{N}.$$

Все оставшиеся в $K[x]$ неприводимые квадратные многочлены разобьем по 30:

$$m_4 = \frac{1}{30}\left(\frac{3^{30}(3^{30} - 1)}{2} - \frac{3^{10}(3^{10} - 1)}{2} - \frac{3^6(3^6 - 1)}{2} + \frac{3^2(3^2 - 1)}{2}\right) \in \mathbb{N}.$$

Общее количество попарно неизоморфных квазиполей Холла порядка 3^{60} равно $m_1 + m_2 + m_3 + m_4$.

2. Подквазиполя Холла и подполя

В квазиполе Холла Q определим *централизатор* элемента $a \in Q$ как множество

$$C(a) = \{b \in Q \mid ab = ba\}.$$

Лемма 1. *Централизатор элемента $a \in Q \setminus K$ равен $K \cup \{a, r - a\}$.*

Д о к а з а т е л ь с т в о. Выберем 1, a в качестве базиса Q над K и найдем элементы централизатора вне K; для этого решим уравнение $(x1+ya)a = a(x1+ya)$ при $y \neq 0$:

$$(x,y)\theta(0,1) = (0,1)\theta(x,y), \quad (x,y)\begin{pmatrix} 0 & 1 \\ s & r \end{pmatrix} = (0,1)\begin{pmatrix} x & y \\ -y^{-1}\varphi(x) & r-x \end{pmatrix}, \quad \begin{cases} -y^{-1}\varphi(x) = ys, \\ r-x = x+yr. \end{cases}$$

Если $r \neq 0$, то $y = 1-2xr^{-1}$ и $(r^2+4s)x(x-r) = 0$. Так как r^2+4s — это дискриминант неприводимого многочлена $\varphi(x)$, то $x = 0$ или $x = r$, отсюда $x1+ya = a$ или $x1+ya = r-a$.

Если $r = 0$, то $2x = 0$, но характеристика поля не может быть 2, поскольку $\varphi(x) = x^2 - s$ приводим над полем четного порядка. Значит, $x = 0$ и $y = \pm 1$; получаем тот же результат.

Лемма доказана.

Теорема 2. *Центр K конечного квазиполя Холла Q является единственным его максимальным подполем, за исключением случая $K \simeq GF(2^{2m+1})$, $\varphi(x) = x^2+x+1$, когда Q есть объединение K и подполей порядка* 4.

Д о к а з а т е л ь с т в о. Пусть $F \not\subset K$ — подполе в Q. Тогда для $a \in F \setminus K$ подполе F содержится в централизаторе $C(a)$ и по лемме 1 имеем $F \subseteq (K \cap F) \cup \{a, r-a\}$. Если $F \simeq GF(p^s)$ и $K \cap F \simeq GF(p^k)$, то $p^s \leq p^k + 2$, откуда $p = 2$, $s = 2$, $k = 1$. В этом случае $\varphi(x) = x^2+x+1$ и $F = \{0, 1, a, a+1 = a^2\} \simeq GF(4)$. При этом K не может содержать поле разложения многочлена $\varphi(x)$, отсюда число $n = 2m+1$ нечетно. Любой нецентральный элемент в данном случае содержится в единственном подполе порядка 4, количество таких подполей $(q^2-q)/2$.

Теорема доказана.

Для простоты изложения особый случай, выделенный в теореме 2, будем называть *специальным* квазиполем Холла.

Лемма 2. *Если F — подквазиполе квазиполя Холла Q, то его ядро K_F равно $K \cap F$.*

Д о к а з а т е л ь с т в о. Ясно, что пересечение $K \cap F$ содержится в ядре K_F квазиполя Q.

Пусть квазиполе Холла Q не является специальным. Так как K_F есть подполе в F, то $K_F \subset K$ и поэтому $K_F = K \cap F$.

Пусть Q — специальное квазиполе Холла и $K_F \not\subset K$. Тогда $K_F = \{0, 1, a, a+1\}$ для некоторого $a \in F \setminus K$. Выберем 1, a в качестве базиса Q и рассмотрим произвольный элемент $b = x1+ya \in F \setminus K_F$, $y \neq 0$. Поскольку $a \in K_F$, то $a(a+b) = a^2+ab$. Запишем в матричном виде:

$$(0,1)\,\theta(x, y+1) = (0,1)\,\theta(0,1) + (0,1)\,\theta(x,y).$$

Если $y+1 \neq 0$, то получим

$$(0,1)\begin{pmatrix} x & y+1 \\ (y+1)^{-1}\varphi(x) & x+1 \end{pmatrix} = (0,1)\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + (0,1)\begin{pmatrix} x & y \\ y^{-1}\varphi(x) & x+1 \end{pmatrix},$$

откуда $x+1 = 1+x+1$; это неверно.

Если $y = 1$, то

$$(0,1)\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} = (0,1)\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + (0,1)\begin{pmatrix} x & y \\ y^{-1}\varphi(x) & x+1 \end{pmatrix},$$

имеем $\varphi(x) = 1$, $x = 0$ или $x = 1$, тогда $b = (0,1) = a$ или $b = (1,1) = 1+a$, $b \in K_F$. Полученное противоречие показывает невозможность $K_F \simeq GF(4)$ в специальном случае.

Лемма доказана.

Если подквазиполе F квазиполя Холла Q имеет размерность более 2 над своим ядром K_F, то F не удовлетворяет определению квазиполя Холла. Это произойдет в случае, когда F не содержит коэффициенты r, s многочлена $\varphi(x)$, $P \not\subset F$. Вопрос о существовании таких подквазиполей в квазиполе Холла мы считаем открытым.

Утверждение 1. *Пусть F — подквазиполе квазиполя Холла Q с ядром $K_F = K \cap F$ и $K_F(r,s)$ — минимальное подполе, содержащее K_F и коэффициенты $\varphi(x)$. Если $K_F(r,s) \neq K$, то F содержится в подквазиполе Холла $F' \neq Q$.*

Доказательство. Выберем произвольный элемент $a \in F \setminus K$ и расмотрим двумерное линейное пространство с базисом 1, a и полем скаляров $K_F(r,s)$,

$$F' = \{x1 + ya \mid x, y \in K_F(r,s)\}.$$

Элементы матрицы $\theta(x,y)$ регулярного множества при $x, y \in K_F(r,s)$ также принадлежат данному полю, поэтому F' замкнуто относительно умножения в Q. Это минимальное подквазиполе Холла, содержащее F, его порядок равен $|K_F(r,s)|^2$.

Утверждение доказано.

Рассмотрим более внимательно подквазиполя, удовлетворяющие определению квазиполя Холла. Они будут существовать только при условии $P \neq K$, т. е. $t < n$.

Теорема 3. *Для любого числа $k \in \mathbb{N}$ с условием $(kt)|n$ в квазиполе Холла Q существует подквазиполе Холла порядка p^{2kt}. И обратно, если Q содержит подквазиполе Холла порядка p^{2m}, то $t|m$ и $m|n$. Два таких подквазиполя либо совпадают, либо пересекаются по общему центру порядка p^m, Q является объединением центра K и $p^{n-m}(p^n-1)/(p^m-1)$ подквазиполей порядка p^{2m}.*

Доказательство. Случай $kt = n$ тривиален, подквазиполе совпадает с Q. Пусть $(kt)|n$ и $kt < n$. Тогда в K есть единственное подполе K_F порядка p^{kt}, оно содержит P. Аналогично доказательству утверждения 1, можно говорить, что для произвольного элемента $a \in Q \setminus K$ множество $F = \{x1 + ya \mid x, y \in K_F\}$ есть подквазиполе Холла порядка p^{2kt}.

Обратно, пусть F — подквазиполе Холла порядка p^{2m}. Тогда по лемме 2 его ядро K_F является подполем в K, отсюда $m|n$. Кроме того, из определения следует, что $P \subset K_F$, поэтому $t|m$. Рассуждения остаются верными и в случаях $m = n$ или $m = t$, и для специального квазиполя Холла, так как $GF(4)$ можно считать квазиполем Холла. Заметим также, что частные n/m и m/t суть нечетные числа.

Если F и H — два различных подквазиполя Холла порядка p^{2m}, то

$$K_F = K_H = K \cap F = K \cap H \simeq GF(p^m).$$

Предположим, что существует общий нецентральный элемент $a \in (F \cap H) \setminus K$. Тогда 1, a составляют одновременно базис F и H над K_F, поэтому $F = H$. Утверждение о количестве подквазиполей Холла одного порядка очевидно.

Теорема доказана.

Рассмотрим вопрос о пересечении подквазиполей Холла разных порядков.

Теорема 4. *Пусть F и H — два подквазиполя Холла порядков p^{2m} и p^{2l} соответственно квазиполя Холла Q при*

$$t \leq m < l < n, \quad t|m, \quad t|l, \quad m|n, \quad l|n.$$

Тогда пересечение $F \cap H$ совпадает либо с F, либо с $K_F \cap K_H \simeq GF(p^s)$, $s = \text{НОД}(m,l)$, или является подквазиполем Холла порядка p^{2s}.

Доказательство. Ядра K_F и K_H подквазиполей — это подполя в K порядков p^m и p^l; обозначим их пересечение как $K_T = K_F \cap K_H \simeq GF(p^s)$. Пусть $(F \cap H) \setminus K \neq \varnothing$. Выберем в этом множестве произвольный элемент a и составим подквазиполе Холла порядка p^{2s}

$$T = \{x1 + ya \mid x, y \in K_T\}, \quad T \subset F, \quad T \subset H.$$

Если $s = m$, то $T = F \subset H$. Рассмотрим случай $s < m$ и предположим, что существует элемент $b \in (F \cap H) \setminus T$. Тогда пара элементов 1, b является базисом F над K_F и базисом H над K_H. Следовательно, элемент $a \in F \cap H$ представим в виде

$$a = x1 + yb, \quad x, y \in K_F, \quad a = u1 + vb, \quad u, v \in K_H.$$

Так как 1, b — базис Q над K, то из равенства $(x - u)1 + (y - v)b = 0$ следует $x = u \in K_T$, $y = v \in K_T$. Поскольку, очевидно, $y \neq 0$, то $b = -y^{-1}x1 + y^{-1}a \in T$, что противоречит выбору b. Таким образом, утверждение теоремы перечисляет все возможные случаи пересечения подквазиполей Холла разных порядков.

Теорема доказана.

Отметим, что описание пересечения подквазиполя Холла $F \neq Q$ с подполем ядра K сложности не представляет.

3. Спектры, примитивность

Неассоциативное умножение элементов квазиполя приводит к необходимости учитывать порядок расстановки скобок даже при записи произведения одинаковых множителей.

Определение 3. *Правоупорядоченная n-я степень* элемента $a \in Q^*$ определяется индуктивно:

$$a^{1)} = a, \quad a^{i+1)} = a^{i)} \cdot a, \quad i = 1, 2, \ldots.$$

Наименьшее натуральное m с условием $a^{m)} = 1$ называется *правым порядком* элемента a, множество правых порядков всех элементов лупы Q^* — ее *правым спектром.*

Определение 4. Элемент $a \in Q^*$ называется *правопримитивным*, если мультипликативная лупа Q^* исчерпывается правоупорядоченными степенями этого элемента:

$$Q^* = \{1, a, a^{2)}, a^{3)}, \ldots\}.$$

Квазиполе Q, содержащее правопримитивный элемент, также называется *правопримитивным.*

Левоупорядоченная степень, левый порядок, левый спектр и левопримитивный элемент определяются аналогично. Как доказано в [12, лемма 5], правый и левый порядки элемента не превышают порядка лупы Q^*. Используя метод регулярного множества, для правого порядка дадим более удобную оценку.

Утверждение 2. *Пусть Q — правое квазиполе порядка q^d с ядром $K \simeq GF(q)$, $A = \theta(a) \in GL_d(q)$ — матрица регулярного множества элемента $a \in Q^*$. Тогда правый порядок элемента a делит порядок матрицы A в группе $GL_d(q)$.*

Доказательство. С использованием матрицы A правоупорядоченные степени элемента a запишутся так:

$$a^2 = a\theta(a) = aA, \quad a^{3)} = a^2\theta(a) = aA^2, \ \ldots, \ a^{k)} = aA^{k-1}.$$

Пусть порядок матрицы $A \in GL_d(q)$ равен k, $A^k = E$. Тогда $a^{k+1)} = a^{k)} \cdot a = aA^k = a$, отсюда по определению лупы $a^{k)} = 1$. Если m — правый порядок элемента a, то $m \leq k$. Выполним деление с остатком: $k = mu + r$, $0 \leq r < m$, получим

$$a^{k)} = (\ldots(a^{m)} \cdot a) \cdot a \ldots) \cdot a = a^{k-m)} = \cdots = a^{r)} = 1,$$

откуда $r = 0$, иначе имеем противоречие с минимальностью m.

Утверждение доказано.

Для квазиполя Холла Q из транзитивности группы автоморфизмов на $Q \setminus K$ следует, что все нецентральные элементы имеют одинаковый правый порядок и одинаковый левый порядок. Выберем базис 1, $a \in Q \setminus K$ и составим при $A = \theta(A)$ множество матриц

$$S = \{xE + yA \mid x, y \in K\}. \tag{3.3}$$

Теорема 5. *Правый спектр квазиполя Холла Q равен $M \cup \{m\}$, где M — множество всех делителей числа $q-1$, m — делитель числа q^2-1, не делящий $q-1$. И обратно, для любого множества $M \cup \{m\}$ описанного вида существует квазиполе Холла с таким правым спектром. Левый порядок любого нецентрального элемента в квазиполе Холла равен трем при $r = s$, четырем при $r = 0$, и он больше четырех в остальных случаях.*

Доказательство. Очевидно, множество M — (правый, левый) спектр мультипликативной группы K^* ядра. Множество матриц S замкнуто относительно сложения и умножения, содержит 0 и E, все ненулевые матрицы невырожденные, так как

$$\det(xE + yA) = \begin{vmatrix} x & y \\ sy & x+ry \end{vmatrix} = y^2 \varphi\left(-\frac{x}{y}\right), \quad y \neq 0.$$

Значит, S — поле порядка q^2, содержащее все степени матрицы A. Ее порядок m делит q^2-1, но не делит $q-1$, так как A не принадлежит подполю $\{xE \mid x \in K\} \subset S$ порядка q.

Обратно, выберем в поле $GF(q^2)$ элемент c порядка m, не делящего $q-1$, и составим многочлен $\varphi(-x) = (x-c)(x-c^q) = x^2 + rx - s$ $(r, s \in GF(q))$. Тогда квазиполе Холла порядка q^2 с ассоциированным многочленом $\varphi(x)$ имеет правый спектр $M \cup \{m\}$.

Вычисление левого порядка элемента a квазиполя затруднено:

$$a^{(3} = a \cdot a^2 = a\,\theta(aA), \quad a^{(4} = a \cdot a^{(3} = a\,\theta(a\theta(aA)), \ldots$$

Утверждение о левом порядке элемента квазиполя Холла проверяется непосредственными расчетами. Действительно,

$$a^2 = aA = (0,1)\begin{pmatrix} 0 & 1 \\ s & r \end{pmatrix} = (s, r), \quad a^{(3} = (0,1)\theta(s,r).$$

Если $r = 0$, то $\theta(s,r) = sE$, $a^{(3} = (0,s)$ и $a^{(4} = (0,1)\,\theta(0,s) = (1,0) = 1$. Если $r \neq 0$, то

$$a^{(3} = (0,1)\begin{pmatrix} s & r \\ -r^{-1}\varphi(s) & r-s \end{pmatrix} = (-r^{-1}\varphi(s), r-s) = (1,0) = 1$$

при $r = s$. Напомним [13], что порядок элемента квазиполя равен 2 только для -1 в квазиполе нечетного порядка.

Теорема доказана.

Замечание. Выбрав для множества (3.3) подполе коэффициентов $P \simeq GF(p^t)$ вместо ядра K, уточняем, что правый порядок m нецентрального элемента делит $p^{2t}-1$.

Пример 2. Перечислим все попарно неизоморфные квазиполя Холла порядка 64 и укажем их правые и левые спектры. В качестве ядра используем алгебраическое расширение $K \simeq \mathbb{Z}_2(\alpha)$, где $\alpha^3 + \alpha + 1 = 0$. Если $P = \mathbb{Z}_2$, то $\varphi(x) = x^2 + x + 1$ и Q — специальное квазиполе Холла, нецентральные элементы имеют порядок 3. Для $P = K$ составляем $-1 + (8^2 - 8)/2 = 27$ неприводимых многочленов и разбиваем их на тройки, $|\mathrm{Aut}\,P| = 3$. Следовательно, существует ровно 10 попарно неизоморфных квазиполей Холла порядка 64. В таблице перечислены их ассоциированные многочлены, правые и левые спектры.

В 1991 г. Г. Венэ выдвинул следующую гипотезу [15]:

Всякое конечное полуполе является левопримитивным либо правопримитивным.

Предположение Г. Венэ опровергнуто в 2004 г. И. Руа, представившим контрпример порядка 32. Это коммутативное *полуполе Кнута — Руа* не является ни право-, ни левопримитивным. Второй контрпример — *полуполе Хентзела — Руа* порядка 64, построенное в 2007 г. ([16], подробно также в [12]). М. Кордеро и В. Джа изучали проблему примитивности для квазиполей, обращая внимание на непримитивность квазиполей Холла с покрытием собственными подквазиполями [17]. Одним из результатов явилась следующая теорема.

Спектры квазиполей Холла порядка 64

№	$\varphi(x)$	Правый спектр	Левый спектр
1	x^2+x+1	{1,3,7}	{1,3,7}
2	$x^2+\alpha x+1$	{1,7,9}	{1,7,15}
3	$x^2+\alpha^4x+\alpha$	{1,7,21}	{1,7,9}
4	$x^2+\alpha^5x+\alpha^3$	{1,7,21}	{1,7,11}
5	$x^2+\alpha x+\alpha$	{1,7,63}	{1,3,7}
6	$x^2+\alpha^5x+\alpha$	{1,7,63}	{1,7,8}
7	$x^2+\alpha^6x+\alpha$	{1,7,63}	{1,7,8}
8	$x^2+x+\alpha^3$	{1,7,63}	{1,7,15}
9	$x^2+\alpha^2x+\alpha^3$	{1,7,63}	{1,5,7}
10	$x^2+\alpha^6x+\alpha^3$	{1,7,63}	{1,7,11}

Теорема 6 [17, теорема 22]. *Квазиполе Холла Q порядка q^2, $q=p^n$, где $n>1$ и не является степенью 2, допускает покрытие собственными подквазиполями Холла, такими, что любые два из этих подквазиполей пересекаются в точности по собственному подполю ядра.*

Тем не менее согласно доказанной выше теореме 3 в случае $P=K$ такое покрытие невозможно. Более того, при любом q можем выбрать в качестве $\varphi(x)$ примитивный многочлен, корни которого — это порождающие элементы мультипликативной группы поля порядка q^2. Тогда квазиполе Холла правопримитивно, поэтому не является объединением подквазиполей. Так, квазиполя 5–10 порядка 64 (см. таблицу) правопримитивны и представляют контрпримеры к теореме 6, поскольку $n=6>1$ и не степень 2. Из теорем 3 и 5 вытекает иная формулировка результата выше.

Следствие 3. *Если $n>1$ и не является степенью 2, то для любого простого p существует квазиполе Холла Q порядка q^2, $q=p^n$, допускающее покрытие собственными подквазиполями Холла, любые два из которых пересекаются в точности по собственному подполю ядра.*

Можно предположить, что всеобщность вместо существования в результате (см. [17]) связана с его геометрическим доказательством — для координатизируемых плоскостей трансляций. Несмотря на изоморфизм плоскостей Холла одного порядка, их координатизирующие изотопные квазиполя обладают разными спектрами. Завершим обсуждение примитивности следующей теоремой, где $\boldsymbol{\varphi}$ — функция Эйлера.

Теорема 7. *Квазиполе Холла Q правопримитивно тогда и только тогда, когда $P=K$ и $\varphi(x)$ — примитивный неприводимый многочлен. Для любого $q=p^n$ существует $\boldsymbol{\varphi}(q^2-1)/(2n)$ правопримитивных квазиполей Холла порядка q^2.*

Доказательство проводится по схеме доказательства теоремы 5. Количество попарно неизоморфных правопримитивных квазиполей Холла равно числу примитивных неприводимых квадратных многочленов, деленному на порядок группы $\operatorname{Aut} K$. Для примера 2 и $q=64$ получаем $\boldsymbol{\varphi}(63)/(2\cdot 3)=36/6=6$, что соответствует данным таблицы.

4. Обобщения, открытые вопросы

Квазиполя Холла как важный особый класс конечных квазиполей привлекают внимание исследователей и открывают простор для приложений и обобщений. Уже упоминались проективные плоскости Холла, свойства которых представлены, например, в [10, гл. 14]. Г. Наги выделяет в [18] квазиполя Холла, допускающие дважды транзитивные множества четных подстановок. Ю. Хирамин предлагает к рассмотрению [19] *обобщенное квазиполе Холла* Q с базисом 1, λ над ядром K, каждый элемент которого $\xi = a + b\lambda$ из $Q \setminus K$ удовлетворяет уравнению $\xi^2 - r(b)\xi - s(b) = 0$, где r и s — отображения из K^* в K.

М. Билиотти и соавторы в [10, 14.3.11] формулируют следующие вопросы о существовании бесконечных обобщений квазиполей Холла:

(1) *Может ли квазиполе Холла быть некоммутативным телом?*

(2) *Может ли система Холла иметь в качестве ядра алгебраически замкнутое поле?*

Меняя в определении квазиполя Холла степень многочлена либо размерность квазиполя над ядром, получим квазиполя, свойства которых еще предстоит описать. Мы считаем полезным изучение следующих связанных вопросов.

(3) *Пусть* $K \simeq GF(q)$, $\varphi(x) \in K[x]$ *— неприводимый многочлен степени* s*. При каких* $m, s \in \mathbb{N}$ *существует (правое) квазиполе* Q *порядка* q^m *с ядром* K*, каждый элемент которого* $a \in Q \setminus K$ *является корнем многочлена* $\varphi(x)$*?*

(4) *Может ли конечное квазиполе Холла содержать подквазиполе размерности более* 2 *над своим ядром?*

С одной стороны, как обсуждалось выше, предположение о существовании не-холлова подквазиполя в квазиполе Холла не содержит очевидных противоречий. С другой стороны, можно указать примеры “почти-холловых” квазиполей, не содержащихся ни в одном конечном квазиполе Холла. Это квазиполя порядка 16, регулярные множества которых записал, в числе прочих, У. Демпволф (см., например,[20]). В. М. Левчук и П. К. Штуккерт в [21, теорема 3.3] показали, что каждое из этих квазиполей, Q_1, Q_3, Q_4, есть теоретико-множественное объединение семи максимальных подполей порядка 4. Эти квазиполя не являются квазиполями Холла, так как имеют размерность 4 над центром $\mathbb{Z}_2$, хотя все их нецентральные элементы суть корни одного многочлена $\varphi(x) = x^2 + x + 1$.

Теорема 8. *Не существует конечных квазиполей Холла, содержащих квазиполя* Q_1*,* Q_3*,* Q_4*.*

Д о к а з а т е л ь с т в о. Регулярные множества квазиполей Q_i списка У. Демпволфа обозначим через $R_i = \{\theta_i(x) \mid x \in Q_i\}$. Введем обозначения для базисных векторов:

$$e = (1,0,0,0), \quad b = (0,1,0,0), \quad c = (0,0,1,0), \quad d = (0,0,0,1);$$

выпишем соответствующие матрицы регулярных множеств, перечисленные в [20]. Для доказательства нам понадобятся только образы базисных элементов квазиполей Q_1, Q_3, Q_4:

$$\theta_1(b) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad \theta_1(c) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \quad \theta_1(d) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix};$$

$$\theta_3(b) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad \theta_3(c) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \quad \theta_3(d) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix};$$

$$\theta_4(b) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \quad \theta_4(c) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \quad \theta_4(d) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Если Q — квазиполе Холла порядка 2^{2n} с ядром $K \simeq GF(2^n)$, содержащее подквазиполе Q_0 порядка 16, изоморфное Q_1, Q_3 или Q_4, то n нечетно, $Q_0 \cap K = \{0, 1\}$.

Пусть σ — изоморфизм из Q_i на Q_0 ($i = 1, 3, 4$). Определим образы базисных элементов e, b, c, d в Q_0. Ясно, что $e^\sigma = 1$ — единица квазиполя Q. Выберем в качестве второго базисного элемента квазиполя Холла Q как линейного пространства над K образ $b^\sigma = a \in Q \setminus K$: $a \notin K$, иначе K содержит подполе порядка 4 и многочлен $\varphi(x)$ приводим над K; обозначим $a = b^\sigma = (0, 1)$.

Вычислим произведения базисных элементов b и c в квазиполях Q_i:

$$bc = b\,\theta_i(c) = (0, 0, 1, 1) = c + d, \quad i = 1, 3, 4;$$

в Q_1 верно $cb = c\,\theta_1(b) = (1, 0, 1, 1) = e + c + d$; в Q_3 получим $cb = c\,\theta_3(b) = d$; в Q_4 имеем $cb = c\,\theta_4(b) = b + c + d$.

Пусть $c^\sigma = (x, y) \in Q$. Если $y = 0$, то $c^\sigma \in K$, что противоречит условию $bc \neq cb$ в Q_i. Значит, $y \neq 0$ и

$$\theta(c^\sigma) = \theta(x, y) = \begin{pmatrix} x & y \\ -y^{-1}\varphi(x) & r - x \end{pmatrix} = \begin{pmatrix} x & y \\ y^{-1}(x^2 + x + 1) & 1 + x \end{pmatrix}.$$

Найдем образ d^σ из условия $bc = c + d$:

$$b^\sigma c^\sigma = (0, 1)\theta(x, y) = (y^{-1}(x^2 + x + 1), 1 + x),$$

$$d^\sigma = b^\sigma c^\sigma + c^\sigma = (x + y^{-1}(x^2 + x + 1), 1 + x + y).$$

Вычислим $(cb)^\sigma$:

$$c^\sigma b^\sigma = (x, y)\theta(0, 1) = (x, y)\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = (y, x + y).$$

Если $Q_0 \simeq Q_1$, то $c^\sigma b^\sigma = (e + c + d)^\sigma = 1 + c^\sigma + d^\sigma = (1 + y^{-1}(x^2 + x + 1), x + 1)$; получим систему уравнений

$$\begin{cases} y = 1 + y^{-1}(x^2 + x + 1), \\ x + y = x + 1, \end{cases} \qquad \begin{cases} x^2 + x + 1 = 0, \\ y = 1, \end{cases}$$

противоречие с неприводимостью $\varphi(x)$ над K.

В случаях $Q_0 \simeq Q_3$ и $Q_0 \simeq Q_4$ аналогичные расчеты также приводят к противоречию.

Теорема доказана.

Обсуждение вопроса о правопримитивности показывает также необходимость внимательного изучения возможности покрытия квазиполя Холла не-холловыми квазиполями. Остается открытым и вопрос о квазиполях Холла, мультипликативная лупа которых исчерпывается степенями одного элемента, но не обязательно правоупорядоченными.

СПИСОК ЛИТЕРАТУРЫ

1. **Dickson L.E.** Linear algebras in which division is always uniquely possible // Trans. Amer. Math. Soc. 1906. Vol. 7, no. 3. P. 370–390. doi: 10.1090/S0002-9947-1906-1500755-5
2. **Veblen O., Maclagan–Wedderburn J.H.** Non-Desarguesian and Non-Pascalian geometries // Trans. Amer. Math. Soc. 1907. Vol. 8, no. 3. P. 379–388. doi: 10.1090/S0002-9947-1907-1500792-1
3. **Холл М.** Теория групп. М.: ИЛ, 1962. 468 с.
4. **Hughes D.R., Piper F.C.** Projective planes. NY Inc.: Springer-Verlag, 1973. 292 p.
5. **Курош А.Г.** Лекции по общей алгебре. М.: Физматгиз, 1962. 396 с.
6. **Dickson L.E.** On finite algebras // Nachr. Akad. Wiss. Göttingen, Math.-Phys. 1905. Kl. II. P. 358–393. URL: http://eudml.org/doc/58621
7. **Zassenhaus H.** Uber endliche Fastkörper // Abh. Math. Sem. Hamburg. 1936. Vol. 11. P. 187–220. doi: 10.1007/BF02940723
8. **Johnson N.L., Jha V., Biliotti M.** Handbook of finite translation planes. London; NY: Chapman Hall/CRC, 2007. 888 p.

9. **Hall M., Jr.** Projective planes // Trans. Amer. Math. Soc. 1943. Vol. 54. P. 229–277. doi: 10.1090/S0002-9947-1943-0008892-4
10. **Biliotti M., Jha V., Johnson N.L.** Foundations of translation planes. NY; Basel: Marcel Dekker Inc., 2001. 542 p.
11. **Nesbitt–Stobert S.B., Garner C.W.L.** A direct proof that all Hall planes of the same finite order are isomorphic // Riv. Mat. Univ. Parma. 1986. Vol. 12, no. 4. P. 241–247.
12. **Levchuk V.M., Kravtsova O.V.** Problems on structure of finite quasifields and projective translation planes // Lobachevskii J. Math. 2017. Vol. 38, no. 4. P. 688–698. doi: 10.1134/S1995080217040138
13. **Кравцова О.В., Скок Д.С.** Метод регулярного множества построения конечных квазиполей // Тр. И-та математики и механики УрО РАН. 2022. Т. 28, № 1. С. 164–181. doi: 10.21538/0134-4889-2022-28-1-164-181 .
14. **Mäurer H.** Die affine Projektivitätengruppe der Hallebenen [The affine group of projectivities of the Hall planes] // Aequationes Math. 1987. Vol. 32. P. 271–273.
15. **Wene G.P.** On the multiplicative structure of finite division rings // Aequationes Math. 1991. Vol. 41. P. 222–233. doi: 10.1007/BF02227457
16. **Hentzel I.R., Rúa I.F.** Primitivity of finite semifields with 64 and 81 elements // International J. Algebra and Computation. 2007. Vol. 17, no. 7. P. 1411–1429. doi:10.1142/S0218196707004220
17. **Cordero M., Jha V.** On the multiplicative structure of quasifields and semifields: cyclic and acyclic loops // Note di Matematica. 2009. Vol. 29, no. 1. P. 45–59. doi:10.1285/i15900932v29n1supplp45
18. **Nagy G.P.** Doubly transitive sete of even permutations // Bul. Acad. Ştiinţe. Repub. Mold. Mat. 2016. No. 1. P. 78–82.
19. **Hiramine Y.** A generalization of Hall quasifields// Osaka J. Math. 1985. Vol. 22. P. 61–69. doi: 10.18910/7798
20. **Dempwolff U., Reifart A.** The Classification of the translation planes of order 16. Universität Stuttgart / Fachbereich Mathematik: Preprint (Vol. 42). 1982.
21. **Levchuk V.M., Shtukkert P.K.** Problems on structure for quasifields of orders 16 and 32 // J. Sib. Federal University. Ser. Mathematics & Physics. 2014. Vol.7, no. 3. P. 362–372.

Поступила 14.08.2023
После доработки 15.11.2023
Принята к публикации 20.11.2023

Кравцова Ольга Вадимовна
д-р. физ.-мат. наук, доцент
профессор кафедры высшей математики №2
Институт математики и фундаментальной информатики
Сибирский федеральный университет
г. Красноярск
e-mail: ol71@bk.ru

Логинова Валерия Сергеевна
магистрант
Институт математики и фундаментальной информатики
Сибирский федеральный университет
г. Красноярск
e-mail: yui5432188@gmail.com

REFERENCES

1. Dickson L.E. Linear algebras in which division is always uniquely possible. *Trans. Amer. Math. Soc.*, 1906, vol. 7, no. 3, pp. 370–390. doi: 10.1090/S0002-9947-1906-1500755-5
2. Veblen O., Maclagan–Wedderburn J.H. Non-Desarguesian and Non-Pascalian geometries. *Trans. Amer. Math. Soc.*, 1907, vol. 8, no. 3, pp. 379–388. doi: 10.1090/S0002-9947-1907-1500792-1
3. Hall M. *The theory of groups*, NY, Macmillan, 1959, 434 p. Translated to Russian under the title *Teoriya grupp*, Moscow, Inostr. Liter. Publ., 1962, 467 p.
4. Hughes D.R., Piper F.C. *Projective planes.* NY Inc.: Springer-Verlag, 1973, 292 p.

5. Kurosh A.G. *Lectures on general algebra.* International Ser. Monographs on Pure and Applied Math., vol. 70, NY Inc.: Elsevier Ltd., 1965, 374 p. doi: 10.1016/C2013-0-01775-6 . Original Russian text published in Kurosh A.G. *Lektsii po obshchei algebre*, Moscow: Fizmatgiz Publ., 1962, 396 p.
6. Dickson L.E. On finite algebras. *Nachr. Akad. Wiss.*, Göttingen, Math.-Phys, 1905, Kl. II, pp. 358–393. Available at: http://eudml.org/doc/58621 .
7. Zassenhaus H. Uber endliche Fastkörper. *Abh. Math. Sem. Hamburg*, 1936, vol. 11, pp. 187–220. doi: 10.1007/BF02940723
8. Johnson N.L., Jha V., Biliotti M. *Handbook of finite translation planes.* London; NY: Chapman Hall/CRC, 2007, 888 p. ISBN: 9781420011142 .
9. Hall M., Jr. Projective planes. *Trans. Amer. Math. Soc.*, 1943, vol. 54, pp. 229–277. doi: 10.1090/S0002-9947-1943-0008892-4 .
10. Biliotti M., Jha V., Johnson N.L. *Foundations of translation planes.* NY, Basel: Marcel Dekker Inc., 2001, 542 p. ISBN: 9780824706098 .
11. Nesbitt–Stobert S.B., Garner C.W.L. A direct proof that all Hall planes of the same finite order are isomorphic. *Riv. Mat. Univ. Parma.*, 1986, vol. 12, no. 4, pp. 241–247.
12. Levchuk V.M., Kravtsova O.V. Problems on structure of finite quasifields and projective translation planes. *Lobachevskii J. Math.*, 2017, vol. 38, no. 4, pp. 688–698. doi: 10.1134/S1995080217040138
13. Kravtsova O.V., Skok D.S. The spread set method for the construction of finite quasifields. *Trudy Instituta Matematiki i Mekhaniki UrO RAN*, 2022. Vol. 28, no. 1. P. 164–181. doi: 10.21538/0134-4889-2022-28-1-164-181
14. Mäurer H. Die affine Projektivitätengruppe der Hallebenen [The affine group of projectivities of the Hall planes]. *Aequationes Math.*, 1987, vol. 32, pp. 271–273.
15. Wene G.P. On the multiplicative structure of finite division rings. *Aequationes Math.*, 1991, vol. 41, pp. 222–233. doi: 10.1007/BF02227457
16. Hentzel I.R., Rúa I.F. Primitivity of finite semifields with 64 and 81 elements. *Internat. J. Algebra and Computation*, 2007, vol. 17, no. 7. P. 1411–1429. doi: 10.1142/S0218196707004220
17. Cordero M., Jha V. On the multiplicative structure of quasifields and semifields: cyclic and acyclic loops. *Note di Matematica*, 2009, vol. 29, no. 1, pp. 45–59. doi: 10.1285/i15900932v29n1supplp45
18. Nagy G.P. Doubly transitive sete of even permutations. *Bul. Acad. Ştiinţe. Repub. Mold. Mat.*, 2016, no. 1, pp. 78–82.
19. Hiramine Y. A generalization of Hall quasifields. *Osaka J. Math.*, 1985, vol. 22, pp. 61–69. doi: 10.18910/7798
20. Dempwolff U., Reifart A. The Classification of the translation planes of order 16. Universität Stuttgart / Fachbereich Mathematik: Preprint (Vol. 42). 1982.
21. Levchuk V.M., Shtukkert P.K. Problems on structure for quasifields of orders 16 and 32. *J. of Siberian Federal University. Ser. Mathematics & Physics*, 2014, vol. 7, no. 3, pp. 362–372.

Received August 14, 2023
Revised November 15, 2023
Accepted November 20, 2023

Funding Agency: This work was supported by the Krasnoyarsk Mathematical Center, which is financed by the Ministry of Science and Higher Education of the Russian Federation (agreement no. 075-02-2023-936).

Olga Vadimovna Kravtsova, Dr. Phys.-Math. Sci., Prof., Siberian Federal University, Krasnoyarsk, 660041 Russia, e-mail: ol71@bk.ru .

Valeria Sergeevna Loginova, graduate student, Siberian Federal University, Krasnoyarsk, 660041 Russia, e-mail: yui5432188@gmail.com .

Cite this article as: O. V. Kravtsova, V. S. Loginova. Questions of the structure of finite Hall quasifields. *Trudy Instituta Matematiki i Mekhaniki UrO RAN*, 2024, vol. 30, no. 1, pp. 128–141 .