ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 28 № 1 2022

УДК 512.554

МЕТОД РЕГУЛЯРНОГО МНОЖЕСТВА ПОСТРОЕНИЯ КОНЕЧНЫХ КВАЗИПОЛЕЙ[1]

О. В. Кравцова, Д. С. Скок

Ослабление аксиом поля приводит к более общим алгебраическим системам: почти-полям, полуполям, квазиполям. Инструментарий для исследования этих систем более сложен в использовании. Метод регулярного множества основан на записи умножения в квазиполе как линейного преобразования в ассоциированном линейном пространстве. Переход к матричным операциям позволяет эффективно применять метод для исследования конечных плоскостей трансляций и их координатизирующих квазиполей. В статье получено характеристическое свойство регулярного множества почти-поля размерности два над ядром. Полученный результат применен к двум неизоморфным почти-полям порядка 25 и квазиполям порядка 9. Обсуждается вопрос существования квазиполей с мультипликативной лупой Муфанг. Методом регулярного множества доказано, что неассоциативных квазиполей Муфанг порядка 25 не существует. Перечислены некоторые вопросы теории конечных полуполей и полуполевых проективных плоскостей, в решении которых может быть использован метод регулярного множества. Указана эффективность метода при компьютерных построениях квазиполей и плоскостей трансляций.

Ключевые слова: квазиполе, почти-поле, полуполе, регулярное множество, плоскость трансляций.

O. V. Kravtsova, D. S. Skok. The spread set method for the construction of finite quasifields.

The weakening of the field axioms leads to more general algebraic systems such as near-fields, semifields, and quasifields. The tools for studying these systems are more difficult to use. The spread set method is based on recording multiplication in a quasi-field as a linear transform in the associated linear space. The transition to matrix operations enables the effective application of the method for studying the finite translation planes and their coordinatizing quasifields. We obtain a characteristic property of a spread set for a near-field of dimension two over the kernel. The result is applied to two non-isomorphic near-fields of order 25 and quasifields of order 9. The existence of quasifields with a multiplicative Moufang loop is also discussed. It is proved by the spread set method that a non-associative Moufang quasifield of order 25 does not exist. We list some questions of the theory of finite semifields and semifield projective planes where the spread set method may be useful. This method is also effective in computer constructions of quasifields and translation planes.

Keywords: quasifield, near-field, semifield, spread set, translation plane.

MSC: 17D99, 16K20, 15A04, 51E15

DOI: 10.21538/0134-4889-2022-28-1-164-181

Введение

Наиболее изученными алгебраическими системами с двумя бинарными операциями являются, бесспорно, конечные поля (поля Галуа). Ослабление или исключение некоторых аксиом поля приводит к появлению более общих алгебраических систем, обладающих, в сравнении с полями, аномальными свойствами, но также имеющих широкое применение в проективной геометрии, теории кодирования, комбинаторике. Так, отказ от ассоциативности умножения позволяет получить конечные полуполя, а ослабляя далее двустороннюю дистрибутивность до односторонней, приходим к понятию квазиполя — левого или правого.

Напомним, что непустое множество L с бинарной операцией "$\cdot$" называется *лупой*, если: уравнения $ax = b$ и $ya = b$ однозначно разрешимы в L для любых $a, b \in L$, L содержит такой элемент e, что $ex = xe = x$ для всех $x \in L$ (т. е. *единицу*).

[1]Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-01-00566 А.

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) $(Q, +)$ — 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. Далее, говоря о квазиполе, мы будем иметь в виду именно правое квазиполе. Все тела представляют тривиальные примеры квазиполей. Квазиполе, не являющееся телом, будем называть нетривиальным или собственным.

Нетривиальные конечные квазиполя изучаются с начала XX в. взаимосвязанно с конечными плоскостями трансляций (работы Л. Диксона 1906 г. [1], О. Веблена и Д. Маклагана-Веддерберна 1907 г. [2]). В литературе до 1975 г. для квазиполей, как правило, использовался термин "системы Веблена — Веддерберна" [3, 20.4].

О п р е д е л е н и е 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. 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; хорошо известно, что квазиполе порядка 4 либо 8 — также поле. Минимальный порядок нетривиального квазиполя равен 9, квазиполей такого порядка точно четыре.

Если в квазиполе выполняются оба дистрибутивных закона, то оно называется *полуполем*. 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. [5], все конечные почти-поля полностью классифицировал Х. Цассенхауз в 1936 г. [6].

Первые примеры конечных квазиполей, не являющихся ни полуполями, ни почти-полями, построил М. Холл [7] в 1943 г. (см. также [3, 20.4]), это *квазиполя Холла*.

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. Некоторые закономерности и полезные свойства устанавливают посредством методов компьютерной алгебры, широко применяемых с середины прошлого века.

Полезный инструментарий дает применение стандартных алгебраических операций для построения и исследования конечных квазиполей. Прежде всего, это использование матриц и многочленов над конечными полями, латинских квадратов для составления таблиц Кэли, семейств линейных подпространств в качестве согласованного расщепления абелевой группы и т. д. Настоящая статья описывает метод регулярного множества, позволяющий на основе специального семейства линейных преобразований строить квазиполя, в частности с заранее определенными свойствами. Первый раздел содержит основные определения и пример построения матричного представления регулярного множества квазиполя Холла. Во втором разделе предлагается необходимый признак регулярного множества почти-поля порядка q^2 с ядром порядка q. Третий раздел посвящен обсуждению вопроса существования конечного квазиполя с лупой Муфанг; показано, что нетривиального квазиполя Муфанг порядка 25 не существует. В четвертом разделе представлен краткий обзор проблем в теории конечных полуполей, к решению которых может быть применен метод регулярного множества.

1. Определения и примеры. Квазиполя Холла

Пусть $Q = (Q, +, \cdot)$ — (правое) квазиполе порядка q^n ($q = p^l$, p — простое число) с ядром $K \simeq GF(q)$. Тогда Q есть (левое) векторное пространство размерности n 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

$$\Sigma = \{\rho_m \mid m \in Q\}$$

будем называть *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 R есть обратимое преобразование. Зафиксируем некоторый базис $e_1, e_2, \ldots, e_n$ квазиполя Q над K и рассмотрим матрицу каждого из указанных линейных преобразований; естественным образом возникает инъективное отображение θ из Q в $GL_n(K) \cup \{0\}$, сопоставляющее каждому элементу $m \in Q$ отображение ρ_m. Множество матриц

$$R = \{\theta(m) \mid m \in Q\} \subset GL_n(q) \cup \{0\} \tag{1.1}$$

— это матричное представление регулярного множества Σ; в дальнейшем для сокращения записи мы часто будем называть R регулярным множеством. Перечислим очевидные свойства множества R:

1) R содержит q^n матриц размерности $n \times n$ с элементами из поля $GF(q)$;

2) R содержит нулевую матрицу 0 и единичную матрицу E;

3) для любых двух различных матриц $A, B \in R$ их разность является невырожденной матрицей, $\det(A - B) \neq 0$.

Обратно, если Q — n-мерное линейное пространство над $GF(q)$,

$$Q = \{x = (x_1, \ldots, x_n) \mid x_i \in GF(q),\ i = 1, \ldots, n\},$$

множество матриц R (1.1) удовлетворяет условиям 1–3 выше, то определение операции умножения "$*$" правилом

$$x * y = x \cdot \theta(y), \quad x, y \in Q,$$

превращает $(Q, +, *)$ в правое квазиполе. Доказательство представляет непосредственную проверку аксиом квазиполя.

Ясно, что матричное представление R регулярного множества Σ зависит от выбора базиса линейного пространства Q. Переход к другому базису с матрицей перехода T приводит к новому множеству TRT^{-1}, поэтому разные регулярные множества могут задавать изоморфные квазиполя. Будем считать для определенности, что мы отождествляем векторы из Q со *строками* их координат в выбранном базисе. Удобен для рассуждений и вычислений базис, где первый, например, элемент e_1 есть единица e квазиполя Q. Тогда первой строкой матрицы $\theta(m)$ является строка координат вектора m в данном базисе, а остальные строки однозначно определяются первой строкой. Отметим также возможность построения *левого* квазиполя по данному регулярному множеству: достаточно заменить строки координат столбцами и изменить порядок умножения элементов.

Таким образом, каждому регулярному множеству матриц в $GL_n(q) \cup \{0\}$ соответствует правое квазиполе порядка q^n с ядром K, содержащим $GF(q)$. Поэтому в качестве основного поля можно выбирать не только ядро, но и любое его подполе. В частности, удобно матричное представление регулярного множества над простым подполем $\mathbb{Z}_p$ в силу линейности всех используемых функций и простоты вычислений, в том числе компьютерных (см. [9, лемма 1]).

Метод построения проективной плоскости трансляций на основе регулярного множества подробно описан в [4]; см. также [10]. Пусть Q — квазиполе порядка q^n с регулярным множеством $R \subset GL_n(q) \cup \{0\}$, $V = Q \oplus Q$ — линейное пространство размерности $2n$ над $GF(q)$.

Аффинными точками плоскости π назовем элементы $(x, y) \in V$, аффинными прямыми — смежные классы в аддитивной группе V по подгруппам

$$V_\infty = \{(0, y) \mid y \in Q\}, \quad V_m = \{(x, x\theta(m)) \mid x \in Q\}, \quad m \in Q.$$

Множество всех смежных классов по одной подгруппе считаем особой точкой (∞) или (m) соответственно, множество всех особых точек — особой прямой $[\infty]$. Построенная конфигурация π есть проективная плоскость трансляций с осью трансляций $[\infty]$. Результаты об изоморфизме плоскостей трансляций с различными регулярными множествами приведены в статьях [11; 12]. Тесная взаимосвязь группы коллинеаций плоскости трансляций и свойств координатизирующего квазиполя описана в [4, гл. VI].

Следующие простые результаты о связи регулярного множества и свойств операций в квазиполе можно найти, например, в [8, гл. 5, 8] в другой системе обозначений и в разрозненном виде; многие источники ссылаются на эти факты как известные. Доказательство их несложно и представляет непосредственную проверку определений. Запишем эти результаты в виде предложения для удобства использования далее.

Предложение 1. *Пусть Q — квазиполе порядка q^n с ядром $K \simeq GF(q)$ и регулярным множеством R (1.1). Q является*

1) *полуполем тогда и только тогда, когда R замкнуто по сложению*;
2) *почти-полем тогда и только тогда, когда R замкнуто по умножению (и $Q^* \simeq R^*$)*;
3) *полем тогда и только тогда, когда R — поле.*

Рассмотрим некоторые примеры квазиполей и их регулярные множества. Если квазиполе Q имеет порядок q^2 и ядро $K \simeq GF(q)$ ($q = p^l$, p — простое), то матрицы регулярного множества R размерности 2×2 могут быть записаны в виде

$$\theta(x, y) = \begin{pmatrix} x & y \\ f(x, y) & g(x, y) \end{pmatrix}, \quad x, y \in GF(q), \tag{1.2}$$

где (x, y) — координаты вектора $m \in Q$ в выбранном базисе $e_1 = e$, e_2, а f, g — многочлены от двух переменных с коэффициентами из $GF(q)$. Заметим, что легко доказать следующий полезный факт: регулярное множество R из матриц вида (1.2) является полем тогда и только тогда, когда функции f и g линейны,

$$f(x, y) = ax + by, \quad g(x, y) = x + cy, \quad a, b, c \in GF(q),$$

квадратный многочлен $t^2 + (c - a)t - b$ неприводим над $GF(q)$. Для полуполя Q функции f и g должны быть аддитивны:

$$f(x, y) = \sum_{i=0}^{l-1} \left(a_i x^{p^i} + b_i y^{p^i} \right), \quad g(x, y) = \sum_{i=0}^{l-1} \left(c_i x^{p^i} + d_i y^{p^i} \right), \quad a_i, b_i, c_i, d_i \in GF(q).$$

Непосредственным следствием имеем известный результат: полуполе порядка p^2 есть поле (см., например, [8, замечание 5.57]). В следующем разделе мы обсудим вид функций, ассоциированных с нетривиальным почти-полем.

П р и м е р 1. Рассмотрим регулярные множества всех квазиполей порядка 9. Для этого выберем $q = 3$ и найдем все многочлены $f, g \in \mathbb{Z}_3[x, y]$:

$$f(x, y) = \sum_{i=0}^{q-1} \sum_{j=0}^{q-1} f_{ij} x^i y^j, \quad g(x, y) = \sum_{i=0}^{q-1} \sum_{j=0}^{q-1} g_{ij} x^i y^j, \tag{1.3}$$

$f_{ij}, g_{ij} \in \mathbb{Z}_3$, с условием $\det(\theta(x, y) - \theta(u, v)) \neq 0$ для матриц вида (1.2) и всех пар $(x, y) \neq (u, v)$. Непосредственный компьютерный перебор предоставляет 12 вариантов подходящих многочленов f и g; список приведен в табл. 1.

Т а б л и ц а 1

Ассоциированные функции правых квазиполей порядка 9

№	$f(x,y)$	$g(x,y)$
1	y	$x+y$
2	y	$x+2y$
3	$y+xy+2x^2y$	$x+y^2+xy^2$
4	$y+2xy+2x^2y$	$x+2y^2+xy^2$
5	$2y$	x
6	$2y+2x^2y$	$x+xy^2$
7	$x+2x^2+y+x^2y$	$x+y+2xy+2xy^2$
8	$x+2x^2+2y+xy+x^2y$	$x+y^2+2xy+2xy^2$
9	$x+2x^2+2y+2xy+x^2y$	$x+2y+2y^2+2xy+2xy^2$
10	$2x+x^2+y+x^2y$	$x+2y+xy+2xy^2$
11	$2x+x^2+2y+xy+x^2y$	$x+y^2+xy+2xy^2$
12	$2x+x^2+2y+2xy+x^2y$	$x+y+2y^2+xy+2xy^2$

Ясно, что функции 1, 2 и 5 задают поле порядка 9; других аддитивных функций мы в списке не наблюдаем, что соответствует рассуждениям выше.

П р и м е р 2. *Квазиполя Холла* — первые примеры конечных квазиполей, не являющихся ни полуполями, ни почти-полями. Пусть многочлен $\varphi(x)=x^2-rx-s$ неприводим над $GF(q)$ и Q — левое квазиполе порядка q^2 с ядром $K\simeq GF(q)$, в котором умножение определяется 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 [13, следствие 14.3.9]. Мы рассмотрим правое квазиполе с такими условиями и найдем матричное представление регулярного множества.

Как указано ранее, в качестве первого базисного элемента выберем единицу e квазиполя Q, тогда все элементы центра (ядра) K имеют координаты $(x,0)$,

$$(x,0)\theta(u,v)=(u,v)\theta(x,0)\quad\forall x,u,v\in K.$$

Отсюда

$$(xu,xv)=(ux+f(x,0)v,vg(x,0)),\quad f(x,0)=0,\ g(x,0)=x,\quad \theta(x,0)=\begin{pmatrix}x&0\\0&x\end{pmatrix}.$$

Произвольный элемент (x,y) из $Q\setminus K$ $(y\neq 0)$ является корнем многочлена $\varphi(x)$:

$$(x,y)^2-r(x,y)-s(1,0)=0,$$
$$(x,y)\begin{pmatrix}x&y\\f(x,y)&g(x,y)\end{pmatrix}-r(x,y)-s(1,0)=0,$$
$$\begin{cases}x^2+yf(x,y)-rx-s=0,\\xy+yg(x,y)-ry=0.\end{cases}$$

Следовательно,

$$f(x,y)=\begin{cases}0, & y=0,\\ -y^{-1}\varphi(x), & y\neq 0,\end{cases}\quad\text{или}\quad f(x,y)=-y^{p^l-2}\varphi(x);$$

$$g(x,y)=\begin{cases}x, & y=0,\\ r-x, & y\neq 0,\end{cases}\quad \text{или}\quad g(x,y)=y^{p^l-1}(r-2x)+x;$$

$$\theta(x,y)=\begin{pmatrix} x & y\\ -y^{p^l-2}\varphi(x) & y^{p^l-1}(r-2x)+x\end{pmatrix},\quad x,y\in GF(q). \tag{1.4}$$

Однозначность определения функций $f(x,y)$ и $g(x,y)$ показывает, что запись закона умножения в координатной форме в квазиполе Холла Q при $e_1=e$ не зависит от выбора элемента $e_2\notin K$. Разные неприводимые над $GF(p^l)$ квадратичные многочлены $\varphi(x)$ и $\psi(x)$ ассоциированы с неизоморфными квазиполями Холла, которые, в свою очередь, задаются разными регулярными множествами (1.4).

Конечное квазиполе Холла является полем тогда и только тогда, когда оно имеет порядок 4. Рассмотрим все нетривиальные квазиполя Холла минимального порядка 9; в этом случае

$$\theta(x,y)=\begin{pmatrix} x & y\\ -y\varphi(x) & y^2(r-2x)+x\end{pmatrix},\quad x,y\in\mathbb{Z}_3.$$

Неприводимых многочленов в $\mathbb{Z}_3[x]$ точно три:

$$\varphi_1(x)=x^2-x-1,\quad \varphi_2(x)=x^2-2x-1,\quad \varphi_3(x)=x^2-2,$$

поэтому существуют три неизоморфных квазиполя Холла, регулярные множества которых состоят из матриц вида

$$\theta_1(x,y)=\begin{pmatrix} x & y\\ -y(x^2-x-1) & y^2(1-2x)+x\end{pmatrix}=\begin{pmatrix} x & y\\ y+xy+2x^2y & x+y^2+xy^2\end{pmatrix},$$

$$\theta_2(x,y)=\begin{pmatrix} x & y\\ -y(x^2-2x-1) & y^2(2-2x)+x\end{pmatrix}=\begin{pmatrix} x & y\\ y+2xy+2x^2y & x+y^2+xy^2\end{pmatrix},$$

$$\theta_3(x,y)=\begin{pmatrix} x & y\\ -y(x^2-2) & -2y^2x+x\end{pmatrix}=\begin{pmatrix} x & y\\ 2y+2x^2y & x+xy^2\end{pmatrix}.$$

Это варианты 3, 4 и 6 в табл. 1. Нетрудно проверить, что в случае выбора многочлена $\varphi_3(x)$ умножение ассоциативно, т. е. Q является почти-полем Диксона порядка 9.

Добавим, что множество матриц $\theta(x,y)$ регулярного множества квазиполя Холла при $y\neq 0$ составляет класс сопряженности в $GL_2(q)$ с характеристическим многочленом $\varphi(x)$ [14]. Квазиполя Холла над одним конечным полем K координатизируют изоморфные плоскости трансляций — *плоскости Холла* [15, теоремы 3.2 и 4.2].

2. Регулярное множество почти-поля

Все конечные почти-поля, кроме семи, могут быть построены единообразно на основе конечного поля. Пусть $q=p^l$, p — простое число, n — натуральное число. Пара (q,n) называется *парой Диксона*, если выполнены условия:

1) каждый простой делитель числа n делит $q-1$;

2) если $q\equiv 3(\mathrm{mod}\,4)$, то n не делится на 4.

Почти-поле порядка q^n с центром $GF(q)$, где (q,n) — пара Диксона, строится как специальное расширение центра. Метод Диксона — Цассенхауза [3, 20.8] заключается во введении новой операции $\circ$ на множестве элементов $Q=\{0,1,\beta,\beta^2,\ldots,\beta^{q^n-2}\}$, где β – фиксированный первообразный корень поля $GF(q^n)$. Произведение $w\circ u$ в почти-поле Q определяется в терминах произведения xy поля $GF(q^n)$ следующим образом. Если $u=\beta^{kn+j}$, то сравнением

$$q^i\equiv 1+j(q-1)(\mathrm{mod}\,n(q-1))$$

однозначно выбирается натуральное число i по модулю n. Тогда произведение $w \circ u$ задаем как $w \circ u = u \cdot w^{q^i}$. Построенные таким способом почти-поля называют *почти-полями Диксона*, в отличие от семи исключительных *почти-полей Цассенхауза*, порядки которых равны p^2 для простых чисел $p = 5, 7, 11$ (два почти-поля), 23, 29, 59. Класс всех почти-полей Диксона порядка q^n с ядром порядка q обозначается $DF(q, n)$.

Предложение 2. *Регулярное множество почти-поля Диксона $Q \in DF(q, 2)$ в базисе $e_1 = 1$, $e_2 = \beta$ состоит из матриц вида*

$$\theta(\beta^{2k}) = \begin{pmatrix} [\beta^{2k}] \\ [\beta^{2k+1}] \end{pmatrix}, \quad \theta(\beta^{2k+1}) = \begin{pmatrix} [\beta^{2k+1}] \\ [\beta^{2k+1+q}] \end{pmatrix},$$

где $[\beta^j]$ — строка координат элемента β^j в выбранном базисе.

Доказательство. Для составления матрицы преобразования $\rho_m : x \to xm$ умножим поочередно базисные элементы на фиксированный элемент $m = \beta^i$. Так как $x \circ \beta^{2k} = \beta^{2k} \cdot x$, $x \circ \beta^{2k+1} = \beta^{2k+1} \cdot x$, то

$$e_1 \circ \beta^{2k} = \beta^{2k} \cdot 1 = \beta^{2k}, \quad e_2 \circ \beta^{2k} = \beta^{2k} \cdot \beta = \beta^{2k+1};$$

$$e_1 \circ \beta^{2k+1} = \beta^{2k+1} \cdot 1^q = \beta^{2k+1}, \quad e_2 \circ \beta^{2k+1} = \beta^{2k+1} \cdot \beta^q = \beta^{2k+1+q}.$$

Предложение доказано.

Предложение 2 дает метод поэлементного построения регулярного множества почти-поля Диксона фиксированного порядка, однако более удобна общая (функциональная) запись (1.2). Она выявляет закономерности во всех матрицах регулярного множества данного почти-поля и поэтому позволяет выделить это почти-поле в классе всех построенных квазиполей данного порядка.

Рассмотрим почти-поле Q порядка q^2 с ядром $K \simeq GF(q)$, $q = p^l$, $p > 2$ — простое. Выберем базис $e_1 = 1$, $e_2 \notin K$ и найдем матричное представление регулярного множества вида (1.2), записывая многочлены f и g с коэффициентами из $GF(q)$ как

$$f(x, y) = \sum_{i=0}^{q-1} \sum_{j=0}^{q-1} f_{ij} x^i y^j, \quad g(x, y) = \sum_{i=0}^{q-1} \sum_{j=0}^{q-1} g_{ij} x^i y^j.$$

Ясно, что из невырожденности всех ненулевых матриц вытекает $f_{00} \neq 0$, $g_{00} \neq 0$.

Известно, что только четыре исключительных почти-поля Цассенхауза имеют центр, отличный от ядра ([16, гл. IV, 5.1 и 6.1]; см. также [17]). В зависимости от порядка центра почти-поля уточним вид функций f и g.

Теорема 1. *Пусть Q — почти-поле порядка q^2 с ядром $K \simeq GF(q)$ ($q = p^l$) и центром Z, матрицы $\theta(x, y)$ вида (1.2) образуют его регулярное множество.*

1. *Если $Z = K$, то*

$$f(x, y) = ay + xy\varphi(x, y), \quad g(x, y) = x + by + xy\psi(x, y),$$

где φ и ψ — однородные многочлены степени $q - 2$ от переменных x, y с коэффициентами из $GF(q)$; $b\varphi(a, b) = b\psi(a, b) = 0$.

2. *Если $Z \neq K$, то $q = p = 5, 7, 11$ или 29,*

$$f(x, y) = ax + (-a + d_1 y^{p-1})x^m + (b + d_2 x^{p-1})y^m + xy\varphi(x, y),$$
$$g(x, y) = ay + (1 + h_1 y^{p-1})x^m + (c + h_2 x^{p-1})y^m + xy\psi(x, y),$$

где $(m, p - 1) = 1$, $m > 1$; φ и ψ — однородные многочлены степени $m - 2$ от переменных x, y с коэффициентами из $GF(q)$.

Д о к а з а т е л ь с т в о. Рассмотрим сначала все почти-поля порядка q^2 с центром $Z = K \simeq GF(q)$. Это регулярные почти-поля Диксона из класса $DF(p^l, 2)$ и три из семи исключительных почти-полей Цассенхауза — порядков 11^2, 23^2 и 59^2. Так как

$$K = \{(x, 0) \mid x \in GF(q)\},$$

то для любых $u, v \in GF(q)$ имеем

$$(x,0)\theta(u,v) = (u,v)\theta(x,0) \Rightarrow (xu, xv) = (xu + vf(x,0), vg(x,0)),$$

откуда $f(x,0) = 0$, $g(x,0) = x$, матрица $\theta(x,0) = xE$ — скалярная.

Обратимся к условию замкнутости регулярного множества по умножению (предложение 1). Так как $\theta(x,0)\theta(0,y) \in R$ для всех $x, y \in GF(q)$, то $f(0,xy) = xf(0,y)$, $g(0,xy) = xg(0,y)$, поэтому $f(0,y)$ и $g(0,y)$ — линейные функции, $f(0,y) = f_{01}y$, $g(0,y) = g_{01}y$. Умножая теперь матрицы $\theta(x,0)$ и $\theta(u,v)$, получим $f(xu,xv) = xf(u,v)$, $g(xu,xv) = xg(u,v)$, следовательно, каждый из многочленов есть сумма линейной функции и однородного многочлена степени q от переменных x и y:

$$f(x,y) = f_{01}y + \sum_{i=1}^{q-1} f_{i,q-i}x^i y^{q-i} = f_{01}y + xy\varphi(x,y),$$
$$g(x,y) = x + g_{01}y + \sum_{i=1}^{q-1} g_{i,q-i}x^i y^{q-i} = x + g_{01}y + xy\psi(x,y).$$

Кроме того, из условия

$$\theta(0,1)\theta(0,1) = \begin{pmatrix} f_{01} & g_{01} \\ f_{01}g_{01} & f_{01} + g_{01}^2 \end{pmatrix} = \theta(f_{01}, g_{01})$$

вытекает $g_{01}\varphi(f_{01}, g_{01}) = g_{01}\psi(f_{01}, g_{01}) = 0$. Остальные произведения матриц регулярного множества мы не рассматриваем, поскольку они предоставляют более сложные в использовании условия на коэффициенты однородных многочленов φ и ψ. Переобозначая, для краткости записи, коэффициенты, приходим к первому утверждению теоремы.

Пусть теперь Q — одно из четырех исключительных почти-полей Цассенхауза порядка p^2 ($p = 5, 7, 11$ или 29), имеющих центр $Z \neq K$. Из условия замкнутости следует

$$\theta(x,0)\theta(y,0) = \begin{pmatrix} xy & 0 \\ f(x,0)y + g(x,0)f(y,0) & g(x,0)g(y,0) \end{pmatrix} = \begin{pmatrix} xy & 0 \\ f(xy,0) & g(xy,0) \end{pmatrix},$$

поэтому отображение $x \to g(x,0)$ является автоморфизмом мультипликативной группы поля $GF(p)$. Тогда $g(x,0) = x^m$, где $(m, p-1) = 1$. Если $m = 1$, то из

$$f(x,0)y + g(x,0)f(y,0) = f(xy,0) \tag{2.1}$$

имеем $f(x,0) = 0$, тогда $Z = K$. С учетом этого $m > 1$ и условие (2.1) дает $f(x,0) = f_{10}(x - x^m)$. Умножим теперь $\theta(x,0)$ на $\theta(0,y)$ и получим пару условий

$$\begin{cases} f(0,xy) = x^m f(0,y), \\ g(0,xy) = f_{10}(x - x^m)y + x^m g(0,y), \end{cases}$$

откуда $f(0,y) = f_{0m}y^m$, $g(0,y) = f_{10}y + g_{0m}y^m$. Запишем более подробно функции f и g:

$$f(x,y) = f_{10}(x - x^m) + f_{0m}y^m + \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} f_{ij}x^i y^j, \quad g(x,y) = x^m + f_{10}y + g_{0m}y^m + \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} g_{ij}x^i y^j,$$

рассмотрим произведение $\theta(x,0)\theta(u,v)$; из условия замкнутости вытекает

$$\begin{cases} f(xu,xv) = f_{10}(x-x^m)u + x^m f(u,v), \\ g(xu,xv) = f_{10}(x-x^m)v + x^m g(u,v); \end{cases}$$

это приведет к равенствам

$$\sum_{i=1}^{p-1}\sum_{j=1}^{p-1} f_{ij}u^i v^j x^{i+j} = \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} f_{ij}u^i v^j x^m, \quad \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} g_{ij}u^i v^j x^{i+j} = \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} g_{ij}u^i v^j x^m.$$

Следовательно, коэффициенты f_{ij} и g_{ij} $(ij \neq 0)$ могут быть отличны от нуля только при $i+j \equiv m \pmod{(p-1)}$. Группируя слагаемые, окончательно имеем

$$f(x,y) = f_{10}x + (-f_{10} + f_{m,p-1}y^{p-1})x^m + (f_{0m} + f_{p-1,m}x^{p-1})y^m + xy\varphi(x,y),$$
$$g(x,y) = f_{10}y + (1 + g_{m,p-1}y^{p-1})x^m + (g_{0m} + g_{p-1,m}x^{p-1})y^m + xy\psi(x,y).$$

Здесь φ и ψ — однородные многочлены степени $m-2$. Для упрощения записи изменяем обозначения коэффициентов и приходим ко второму утверждению теоремы.

Теорема полностью доказана.

Заметим, что, уточняя вид функций f и g, мы использовали условия замкнутости регулярного множества относительно умножения не для всех матриц $\theta(x,y)\theta(u,v)$. Эти условия приводят к слишком громоздким соотношениям коэффициентов, их сложно использовать практически. Таким образом, доказанная теорема не является критерием, она представляет *необходимый признак*, по которому можно выделить почти-поля в классе квазиполей порядка q^2 с ядром порядка q.

П р и м е р 3. Обратимся снова к табл. 1 для квазиполей порядка 9. В соответствии с доказанной теоремой регулярное множество № 6 задает почти-поле, как и указано в предыдущем разделе. Существует точно пять неизоморфных квазиполей порядка 9; одно из них — поле $GF(9)$, другое — почти-поле Диксона, еще два — квазиполя Холла. Пятое — "странное" квазиполе с центром $\{0,1\}$ [7, приложение II]. Этому квазиполю соответствуют в табл. 1 варианты 7–12, отличающиеся выбором второго базисного элемента.

П р и м е р 4. Применим теорему 1 для записи матричного представления почти-полей порядка 25: это единственное почти-поле Диксона $Q \in DF(5,2)$ с центром $\mathbb{Z}_5$ и исключительное почти-поле Цассенхауза W с центром порядка 3.

Выберем многочлен $\varphi(x) = x^2+3x+3$, неприводимый над $\mathbb{Z}_5$, и его корень β. Произведение $w \circ u$ определяем так: $w \circ \beta^{2k} = \beta^{2k} \cdot w$, $w \circ \beta^{2k+1} = \beta^{2k+1} \cdot w^5$. Используя предложение 2, найдем все матрицы регулярного множества. Например,

$$\theta(\beta) = \begin{pmatrix} [\beta] \\ [\beta^6] \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix},$$

так как $\beta^6 = (2\beta+2)^3 = 3$. Тогда по первому утверждению теоремы 1 имеем $a=3$ и $b=0$,

$$f(x,y) = 3y + f_{14}xy^4 + f_{23}x^2y^3 + f_{32}x^3y^2 + f_{41}x^4y,$$

$$g(x,y) = x + g_{14}xy^4 + g_{23}x^2y^3 + g_{32}x^3y^2 + g_{41}x^4y.$$

Используя все найденные матрицы $\theta(\beta^k)$, составим и решим две системы из 16 линейных уравнений на 4 неизвестных f_{ij}, g_{ij} соответственно. В результате получаем функции, ассоциированные с почти-полем Диксона порядка 25:

$$f(x,y) = 3y + 3x^2y^3 + 3x^3y^2 + 3x^4y, \quad g(x,y) = x + xy^4 + 2x^2y^3 + 4x^3y^2.$$

Исключительное почти-поле Цассенхауза W порядка 25 построим, учитывая предложение 1: мультипликативная группа почти-поля изоморфна мультипликативной группе его регулярного множества. Известно [3, 20.7], что $W^* \simeq SL(2,3)$; с помощью этого множества матриц найдем коэффициенты функций f и g.

Прежде всего матрицу $\theta(x,0)$ сравним с матрицами

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}2&0\\0&3\end{pmatrix}, \begin{pmatrix}3&0\\0&2\end{pmatrix}, \begin{pmatrix}4&0\\0&4\end{pmatrix} \in SL(2,3).$$

По второму утверждению теоремы 1 $(m, p-1) = (m,4) = 1$, $m \neq 1$ и $a(x - x^m) = 0$, тогда $m = 3$ и $a = 0$. Сравнение матрицы $\theta(0,y)$ с

$$\begin{pmatrix}0&1\\4&0\end{pmatrix}, \begin{pmatrix}0&2\\2&0\end{pmatrix}, \begin{pmatrix}0&3\\3&0\end{pmatrix}, \begin{pmatrix}0&4\\1&0\end{pmatrix} \in SL(2,3)$$

дает $c = 0$ и $b = 4$, откуда

$$f(x,y) = 4y^3 + d_1x^3y^4 + d_2x^4y^3 + f_{12}xy^2 + f_{21}x^2y, \quad g(x,y) = x^3 + h_1x^3y^4 + h_2x^4y^3 + g_{12}xy^2 + g_{21}x^2y.$$

Рассматривая остальные матрицы группы $SL(2,3)$, составим и решим систему линейных уравнений на коэффициенты функций, в результате получим функции, ассоциированные с исключительным почти-полем Цассенхауза порядка 25:

$$f(x,y) = 4y^3 + 3x^4y^3, \quad g(x,y) = x^3 + 2x^3y^4.$$

З а м е ч а н и е. Предлагаем изучить возможность применения первого утверждения теоремы 1 для построения примеров нетривиальных бесконечных почти-полей. Для этого, учитывая равенство $y^{q-i} = y \cdot y^{-i}$ для любого ненулевого элемента $y \in GF(q)$, перепишем функции f и g в виде

$$f(x,y) = y\sum_{i=0}^{m} f_i \left(\frac{x}{y}\right)^i, \quad g(x,y) = x + y\sum_{i=0}^{n} g_i \left(\frac{x}{y}\right)^i.$$

Пусть K — бесконечное поле, $\Phi(x)$ и $\Psi(x)$ — два многочлена с коэффициентами из K,

$$\theta(x,0) = \begin{pmatrix}x&0\\0&x\end{pmatrix}, \quad \theta(x,y) = \begin{pmatrix} x & y \\ y\Phi\left(\dfrac{x}{y}\right) & x + y\Psi\left(\dfrac{x}{y}\right)\end{pmatrix}, \ y \neq 0.$$

Если найдутся такие многочлены $\Phi(x)$ и $\Psi(x)$, что для любых пар $(x,y) \neq (u,v)$ элементов из K матрица $\theta(x,y) - \theta(u,v)$ является невырожденной, то при некоторых дополнительных условиях матрицы $\theta(x,y)$ образуют регулярное множество почти-поля размерности 2 над своим центром K. Требование изучения дополнительных ограничений вызвано тем, что теорема 1 дает лишь необходимое условие для регулярного множества почти-поля. Задача представляется нетривиальной и заслуживающей исследования.

3. Квазиполя Муфанг

Будем называть неассоциативное квазиполе Q *квазиполем Муфанг*, если его мультипликативная лупа Q^* является *лупой Муфанг*, т. е. для всех $x, y, z \in Q^*$ выполняется одно из (эквивалентных) тождеств:

$$(xy)(zx) = (x(yz))x, \quad ((xy)z)y = x(y(zy)), \quad x(y(xz)) = ((xy)x)z. \tag{3.1}$$

Лупа Муфанг удовлетворяет также тождествам

$$(xx)y = x(xy), \quad (xy)x = x(yx), \quad (yx)x = y(xx),$$

в силу которых она *диассоциативна*, любые два ее элемента порождают группу. На лупы Муфанг удается переносить теоретико-групповые результаты — теоремы Лагранжа, Силова и другие важные результаты [18; 19].

В статье [20] перечислены возможные малые порядки квазиполей Муфанг: квазиполя Муфанг порядка ≤ 100 могут существовать лишь для порядков 25, 49, 64 и 81. Возникает естественный вопрос (А. В. Заварницин, Мальцевские чтения, 2020):

Существуют ли конечные квазиполя Муфанг?

Цель настоящего исследования — применение метода регулярного множества к решению данного вопроса. Первый шаг приводит к следующему результату.

Теорема 2. *Не существует квазиполей Муфанг порядка* 25.

Используем описание луп Муфанг порядка 24, полученное О. Чейном [21].

Лемма 1. *Если Q — квазиполе Муфанг порядка* 25*, то его мультипликативная лупа Q^* содержит циклическую подгруппу порядка 6, остальные элементы имеют порядок* 4.

Доказательство. Чейн перечислил все лупы Муфанг порядков менее 31, среди них — пять луп порядка 24. В табл. 2 приведем необходимые нам данные из [21, табл. 3].

Мультипликативная лупа квазиполя содержит только один элемент порядка два — это $-e$. Действительно, пусть $a^2 = e$, $a \neq \pm e$. Тогда $a^2 + a = a + e$, $(a + e)a = a + e$ (для правого квазиполя), т. е. уравнение $(a + e)x = a + e$ имеет более одного корня, что противоречит определению лупы.

Таким образом, если Q — квазиполе Муфанг порядка 25, то $Q^* \simeq M_{24}(G_{12}, Q)$. Данные из табл. 2 о порядках элементов доказывают лемму 1.

Лемма 2. *Пусть Q — квазиполе Муфанг порядка* 25*. Тогда при некотором выборе базиса e_1, e_2 его регулярное множество состоит из матриц вида*

$$\theta(x,y) = \begin{pmatrix} x & y \\ f_{10}(x - x^3) - y^3 + xy\varphi(x,y) & x^3 + f_{10}(y - y^3) + xy\psi(x,y) \end{pmatrix}, \quad x, y \in \mathbb{Z}_5,$$

где $f_{10} \in \{0, 1, -1\}$, $\varphi, \psi \in \mathbb{Z}_5[x, y]$.

Доказательство. В качестве первого базисного элемента выберем единицу квазиполя: $e_1 = e$, в качестве второго — элемент порядка 4. По лемме 1 такой выбор возможен, так как ядро $K = \langle e_1 \rangle$ содержит только два элемента порядка 4 из 18. Тогда далее считаем $e_2^2 = -e$. Для $\theta(x, y)$ вида (1.2) имеем

$$(0,1)\theta(0,1) = (0,1)\begin{pmatrix} 0 & 1 \\ f(0,1) & g(0,1) \end{pmatrix} = (-1,0) \quad \Rightarrow \quad f(0,1) = -1,\ g(0,1) = 0.$$

Таблица 2

Порядки элементов луп Муфанг порядка 24

Лупа	Число элементов порядка			
	2	**3**	**4**	**6**
$M_{24}(A_4, 2)$	15	8	-	-
$M_{24}(D_6, 2)$	19	2	-	2
$M_{24}(G_{12}, 2)$	13	2	6	2
$M_{24}(G_{12}, C_2 \times C_4)$	7	2	12	2
$M_{24}(G_{12}, Q)$	1	2	18	2

Запишем очевидное $f(1,0)=0$, $g(1,0)=1$ и применим альтернативный закон $(yx)x=y(xx)$:

$$(u,v)\theta(x,0)\theta(x,0)=(u,v)\theta((x,0)\theta(x,0)) \quad \forall u,v,x\in\mathbb{Z}_5,$$

$$\theta(x,0)\theta(x,0)=\theta((x,0)\theta(x,0)) \quad \forall x\in\mathbb{Z}_5,$$

$$\begin{pmatrix} x & 0 \\ f(x,0) & g(x,0)\end{pmatrix}^2=\begin{pmatrix} x^2 & 0 \\ f(x^2,0) & g(x^2,0)\end{pmatrix}.$$

Из условий $f(x,0)(x+g(x,0)=f(x^2,0)$ и $g^2(x,0)=g(x^2,0)$ при $x=-1$ следует $f(-1,0)=0$ и $g(-1,0)=-1$. В обозначениях (1.3) для коэффициентов многочленов f и g верно $f_{00}=g_{00}=0$,

$$f(x,0)=f_{10}x+f_{20}x^2-f_{10}x^3-f_{20}x^4, \quad g(x,0)=g_{10}x+g_{20}x^2+(1-g_{10})x^3-g_{20}x^4$$

и $f(x^2,0)=0$. Из тождества $g^2(x,0)=g(x^2,0)$ вытекает, что возможны только четыре варианта функции $g(x,0)$:

$$\begin{aligned}
&(1)\ \ g(x,0)=x,\\
&(2)\ \ g(x,0)=x^3,\\
&(3)\ \ g(x,0)=3x+x^2+3x^3-x^4,\\
&(4)\ \ g(x,0)=3x-x^2+3x^3+x^4.
\end{aligned}$$

Тогда из $f(x,0)(x+g(x,0))=0$ получаем соответствующие варианты функции $f(x,0)$;

$$\begin{aligned}
&(1)\ \ f(x,0)=0,\\
&(2)\ \ f(x,0)=(f_{10}+f_{20}x)(x-x^3),\\
&(3)\ \ f(x,0)=f_{10}(1-2x)(x-x^3),\\
&(4)\ \ f(x,0)=f_{10}(1+2x)(x-x^3).
\end{aligned}$$

Применим второй альтернативный закон $(xy)x=x(yx)$:

$$(0,y)\theta(x,0)\theta(0,y)=(0,y)\theta((x,0)\theta(0,y)) \quad \forall x,y\in\mathbb{Z}_5,$$

отсюда $g(x,0)f(0,y)=f(0,xy)$, $f(x,0)y+g(x,0)g(0,y)=g(0,xy)$ для $y\neq 0$. При $x=-1$ имеем $f(0,-y)=-f(0,y)$ и $g(0,-y)=-g(0,y)$, поэтому многочлены $f(0,y)$ и $g(0,y)$ содержат только нечетные степени переменной.

В случае (1) находим $f(0,y)=-y$, $g(0,y)=0$, но разность матриц

$$\theta(x,0)-\theta(0,y)=\begin{pmatrix} x & -y \\ y & x\end{pmatrix}$$

является вырожденной, например, при $x=1$, $y=2$, что противоречит определению регулярного множества. Случай (1) невозможен.

В случае (2) получим $f(0,y)=-y^3$, $g(0,y)=f_{10}(y-y^3)$ и уточним $f(x,0)=f_{10}(x-x^3)$. Отметим, что все расчеты единообразные и несложные, поэтому мы их не приводим. Итак,

$$\theta(x,0)=\begin{pmatrix} x & 0 \\ f_{10}(x-x^3) & x^3\end{pmatrix}, \quad \theta(0,y)=\begin{pmatrix} 0 & y \\ -y^3 & f_{10}(y-y^3)\end{pmatrix},$$

разность таких матриц нулевая либо невырожденная тогда и только тогда, когда уравнение $f_{10}(t^3-t)=2$ не имеет корней в $\mathbb{Z}_5$. Следовательно, $f_{10}=\pm 1$ или $f_{10}=0$.

В случаях (3) и (4) снова противоречие, поскольку при $x=\pm 2$ получаем $f(0,\pm 2y)=2f(0,y)$ или $f(0,\pm 2y)=-2f(0,y)$, откуда $f(0,y)=0$, матрица $\theta(0,y)\neq 0$ вырожденная.

Таким образом, возможен только случай (2), лемма 2 доказана.

Д о к а з а т е л ь с т в о теоремы 2. По лемме 2

$$\theta(0,4) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Кроме того, можем считать, что не только $|e_2| = 4$, но и $|e_2 + e| = 4$. Действительно, множество $Q \setminus K$ содержит 16 элементов порядка 4, два элемента порядка 3 и два элемента порядка 6. Соответственно, $(1,1)^2 = (-1,0)$. Обозначим $a = (1,1)$ и вычислим два произведения:

$$(1,2)(0,4) = (1,2)\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = (2,4),$$

$$(1,2)(1,1) = (4e + 2a)a = 4a + 2a^2 = 4a - 2e = (2,4).$$

Таким образом, уравнение $(1,2)x = (2,4)$ имеет в лупе Q^* два решения, что невозможно. Полученное противоречие доказывает теорему 2.

Применяемый метод позволил избежать компьютерного перебора всех квазиполей порядка 25 с проверкой выполнения условий (3.1). Для доказательства существенно использованы структурные результаты О. Чейна для луп Муфанг порядка 24, поэтому метод не переносится на другие порядки непосредственно. Тем не менее метод регулярного множества представляется перспективным для решения вопроса существования квазиполей Муфанг — положительного либо отрицательного.

4. Вопросы теории конечных полуполей

Первые примеры нетривиальных конечных полуполей, т. е. квазиполей с двусторонней дистрибутивностью, указаны Л. Диксоном в 1906 г. В ранней литературе для них было принято понятие "неассоциативное кольцо с делением" ("квазитело", в терминологии А. Г. Куроша). Современное "semifield", предложенное Д. Кнутом для упрощения терминологии, используется с 1965 г. Целью авторов в настоящем разделе не является полный обзор теории конечных полуполей ввиду обширности материала. Будут перечислены лишь некоторые вопросы, напрямую связанные с методом регулярного множества.

Рассматривая полуполе $Q = (Q, +, *)$ порядка p^n как линейное пространство над простым подполем $\mathbb{Z}_p$, отметим, что его регулярное множество $R \subset GL_n(p) \cup \{0\}$ в силу замкнутости по сложению (предложение 1) также является n-мерным линейным пространством над $\mathbb{Z}_p$. Закон умножения $x * y = x\theta(y)$ достаточно определить только для базисных элементов $e_1, \ldots, e_n$ полуполя Q:

$$e_i * e_j = a_{ij1}e_1 + a_{ij2}e_2 + \cdots + a_{ijn}e_n, \quad i, j = 1, 2, \ldots, n.$$

Все коэффициенты a_{ijk} $(i, j, k = 1, \ldots, n)$ образуют кубический массив (*гиперкуб Кнута*), т. е. совокупность $(n \times n)$-матриц $A_1, \ldots, A_n$, составляющих базис R.

Ясно, что полная классификация полуполей — это классификация с точностью до изоморфизма. Взаимосвязь полуполей и полуполевых проективных плоскостей указывает также на важность классификации с точностью до изотопизма.

О п р е д е л е н и е 3. Изотопизмом квазиполей Q и W (автотопизмом, если $Q = W$) называется тройка изоморфизмов α, β, γ аддитивной группы $(Q, +)$ на $(W, +)$, если для всех $x, y \in S$ верно $x^\alpha \cdot y^\beta = (x \circ y)^\gamma$.

В 1960 г. А. Альбертом показана (см. также [22, теорема 3.4.3]) эквивалентность класса изоморфизма полуполевых проективных плоскостей и класса изотопизма полуполей: *полуполевые плоскости изоморфны тогда и только тогда, когда их координатизирующие полуполя изотопны.* Принято группировать конечные полуполя и в более крупные семейства — так называемые *орбиты Кнута*, получаемые при всевозможных перестановках индексов i, j, k элементов гиперкуба Кнута.

В отличие от конечных почти-полей, ни полуполя, ни тем более квазиполя не получили к настоящему времени исчерпывающей классификации. В 2003 г. У. Кантор [23] записал: “Исследование конечных коммутативных полуполей было начато Диксоном почти столетие назад ... Удивительно, что до сих пор о них так мало известно”. В обзоре М. Лаврау и О. Полверино [24] перечислены некоторые классификационные результаты, указаны 28 классов известных на текущий момент конечных полуполей, приведен список из девяти открытых вопросов в классификации полуполей с точностью до изотопизма. Полуполя малых порядков 2^4, 2^5, 2^6, 3^4 и 3^5 полностью классифицированы с использованием компьютерной техники (Э. Клейнфелд, Р. Уолкер, И. Руа и др.; см. подробнее в [10]).

В 2013 г. В. М. Левчук в своем докладе на научно-исследовательском семинаре кафедры высшей алгебры ММФ МГУ предложил несколько вопросов о строении конечных квазиполей и полуполей, они перечислены также в [10;17]. Эти вопросы о спектрах, максимальных подполях и группе автоморфизмов конечного квазиполя привлекали внимание исследователей и ранее. Г. Венэ в 1991 г. была выдвинута гипотеза, связанная со степенями и порядками элементов мультипликативной лупы.

Неассоциативное умножение элементов квазиполя приводит к необходимости учитывать порядок расстановки скобок даже при записи произведения одинаковых множителей. *Правоупорядоченная n-я степень* элемента a мультипликативной лупы L определяется индуктивно:

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

левоупорядоченная n-я степень — аналогично.

О п р е д е л е н и е 4. Пусть $(Q, +, \cdot)$ — конечное квазиполе. Элемент $a \in Q^*$ называется правопримитивным, если мультипликативная лупа Q^* исчерпывается правоупорядоченными степенями этого элемента: $Q^* = \{e, a, a^{2)}, a^{3)}, \dots\}$. Квазиполе Q, содержащее правопримитивный элемент, также называется правопримитивным.

Г. Венэ сформулировал предположение [25]:

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. (см. подробно в [10]). К настоящему времени исследование проблемы примитивности полностью завершено для всех полуполей до порядка 125 включительно. Новых примеров непримитивных полуполей не обнаружено; не найдены до сих пор и контрпримеры нечетного порядка.

Изучение проблемы примитивности основано на свойствах регулярного множества (см. [26, предложение 2]). Переформулируем в наших обозначениях: *если Q — конечное полуполе размерности n над своим центром Z, то $a \in Q$ является правопримитивным элементом Q тогда и только тогда, когда характеристический многочлен матрицы $\theta(a)$ регулярного множества есть неприводимый примитивный многочлен степени n над Z.* На текущий момент доказана примитивность полуполей размерности 3 над центром, а также размерности 4 над центром достаточно большого порядка.

Полное решение вопросов В. М. Левчука для исключительных непримитивных полуполей Кнута — Руа порядка 32 и Хентзела — Руа порядка 64 получено методом регулярного множества и представлено в [10] (для почти-полей — в [17]).

Отметим еще одно предположение, связанное с конечными полуполями и полуполевыми плоскостями. Хорошо известна неразрешимость группы коллинеаций (автоморфизмов) конечной дезарговой проективной плоскости, координатизируемой полем. Однако все примеры конечных недезарговых полуполевых плоскостей, построенных к середине 1950-х гг., имели разрешимую группу коллинеаций. Это позволило Д. Хьюзу в 1959 г. предположить, что данное свойство может быть присуще всем недезарговым полуполевым плоскостям. Гипотеза о разрешимости группы автотопизмов конечного (неассоциативного) полуполя (эквивалентно, группы

коллинеаций недезарговой полуполевой проективной плоскости) была записана Д. Хьюзом в монографии 1973 г. ([4, гл. VIII]; см. также вопрос 11.76 Н.Д. Подуфалова 1990 г. в Коуровской тетради).

Общего подхода к решению проблемы до сих пор не найдено, несмотря на продвижения для отдельных классов полуполевых плоскостей, полученные широким рядом исследователей. Значительное количество поздних результатов о разрешимости доказано с помощью вычислительной техники в ходе перечисления полуполей фиксированных малых порядков.

Представляется возможным использовать для изучения проблемы Хьюза метод регулярного множества, применяя его для выделения конечных простых групп, которые не могут содержаться в группе автотопизмов конечной недезарговой полуполевой проективной плоскости. Учитывая теорему Д. Г. Томпсона о минимальных простых группах, предлагаем строить регулярное множество полуполевой плоскости в предположении, что плоскость допускает группу коллинеаций G из списка Томпсона. Детальное изучение регулярного множества позволит, при определенных ограничениях на порядок плоскости, либо установить противоречие с наличием G в группе коллинеаций, либо построить пример. Наиболее общий результат первого автора, полученный методом регулярного множества, пока следующий: *недезаргова полуполевая плоскость произвольного нечетного порядка не может допускать подгруппу автотопизмов, изоморфную знакопеременной группе* A_5 [27, теорема 2].

Говоря в заключение о примерах полуполевых плоскостей с фиксированными группами коллинеаций, отметим также широкие возможности применения метода регулярного множества, в том числе посредством компьютерных вычислений. Первые такие примеры были построены Х. Хуангом и Н. Л. Джонсоном в 1990 г., что доказало существование недезарговых полуполевых плоскостей четного порядка с инволютивными автотопизмами [8, 37.9].

С другими способами представления конечных квазиполей можно ознакомиться в монографии [8], обзорах [23; 24], см. также метод Оямы [28].

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.: Изд-во иностр. лит., 1962. 468 с.
4. **Hughes D.R., Piper F.C.** Projective planes. NY: Springer-Verlag, 1973. 292 p.
5. **Dickson L.E.** On finite algebras // Nachr. Akad. Wiss. Göttingen, Math.-Phys. 1905. Kl. II. P. 358–393. URL: https://eudml.org/doc/58621 .
6. **Zassenhaus H.** Uber endliche Fastkörper // Abh. Math. Sem. Hamburg. 1936. Vol. 11. P. 187–220. doi: 10.1007/BF02940723 .
7. **Hall M., Jr.** Projective planes // Trans. Amer. Math. Soc. 1943. Vol. 54. P. 229–277. doi: 10.1090/S0002-9947-1943-0008892-4 .
8. **Johnson N.L., Jha V., Biliotti M.** Handbook of finite translation planes. London; NY: Chapman Hall/CRC, 2007. 888 p.
9. **Kravtsova O.V.** On automorphisms of semifields and semifield planes // Sib. Elektron. Mat. Izv. 2016. Vol. 13. P. 1300–1313. doi: 10.17377/semi.2016.13.102 .
10. **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 .
11. **Maduram D.M.** Matrix representation of translation planes // Geom. Dedicata. 1975. Vol. 4. P. 485–492. doi: 10.1007/BF00148776 .
12. **Podufalov N.D.** On spread sets and collineations of projective planes // Contem. Math. 1992. Vol. 131, part 1. P. 697–705. doi: 10.1090/conm/131.1/1175813 .
13. **Biliotti M., Jha V., Johnson N.L.** Foundations of translation planes. NY, Basel: Marcel Dekker Inc., 2001, 542 p.

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. URL: https://eudml.org/doc/137191 .
15. **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. URL: http://rivista.math.unipr.it/fulltext/1986-12/1986-12-241.pdf .
16. **Wähling H.** Theorie der Fastkörper. Ser. Thales Monographs, vol. 1. Essen: Thales-Verlag, 1987. 393 p.
17. **Кравцова О.В., Левчук В.М.** Вопросы строения конечных почти-полей // Тр. Ин-та математики и механики УрО РАН. 2019. Т. 25, № 4. С. 107–117. doi: 10.21538/0134-4889-2019-25-4-107-117 .
18. **Grishkov A.N., Zavarnitsyn A.V.** Lagrange's theorem for Moufang loops // Math. Proc. Phil. Soc. 2005. Vol. 139. P. 41–57. doi: 10.1017/S0305004105008388 .
19. **Grishkov A.N., Zavarnitsyn A.V.** Sylow's theorems for Moufang loops // J. Algebra. 2009. Vol. 321, no. 7. P. 1813–1825. doi: 10.1016/j.jalgebra.2008.08.035 .
20. **Яковлева Т.Н.** Вопросы строения квазиполей с ассоциативными степенями // Изв. Иркут. гос. ун-та. Сер. "Математика". 2019. Т. 29. С. 107–119. doi: 10.26516/1997-7670.2019.29.107 .
21. **Chein O.** Moufang loops of small order. I // Trans. of the Amer. Math. Soc. 1974. Vol. 188, iss. 2. P. 31–51. doi: 10.1090/S0002-9947-1974-0330336-3 .
22. **Knuth D.E.** Finite semifields and projective planes // J. Algebra. 1965. Vol. 2. P. 182–217. doi: 10.1016/0021-8693(65)90018-9 .
23. **Kantor W.M.** Commutative semifields and symplectic spreads // J. Algebra. 2003. Vol. 270, no. 1. P. 96–114. doi: 10.1016/S0021-8693(03)00411-3 .
24. **Lavrauw M., Polverino O.** Finite semifields // Current research topics in Galois Geometry / eds. L. Storme and J. De Beule. Chapter 6. NY: NOVA Acad. Publ., 2011. P. 131–160. URL: http://hdl.handle.net/1854/LU-2152960 .
25. **Wene G.P.** On the multiplicative structure of finite division rings // Aequationes Math. 1991. Vol. 41. P. 222–233. doi: 10.1007/BF02227457 .
26. **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 .
27. **Kravtsova O.V.** On alternating subgroup A_5 in autotopism group of finite semifield plane // Sib. Elektron. Mat. Izv. 2020. Vol. 17. P. 47–50. doi: 10.33048/semi.2020.17.004 .
28. **Oyama T.** On quasifields // Osaka J. Math. 1985. Vol. 22. P. 35–54. URL: https://projecteuclid.org/journals/osaka-journal-of-mathematics/volume-22/issue-1/On-quasifields/ojm/1200778033.full .

Поступила 10.11.2021
После доработки 20.12.2021
Принята к публикации 27.12.2021

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

Скок Дарья Сергеевна
магистрант
Институт математики и фундаментальной информатики
Сибирский федеральный университет
г. Красноярск
e-mail: skokdarya@yandex.ru

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*. Providence: AMS Chelsea, 1959, 434 p. ISBN: 978-0-8218-1967-8 . Translated to Russian under the title *Teoriya grupp*. Moscow: Inostr. Lit. Publ., 1962, 468 p.
4. Hughes D.R., Piper F.C. *Projective planes*. NY: Springer, 1973, 292 p. ISBN: 0387900438 .
5. Dickson L.E. On finite algebras. *Nachr. Akad. Wiss. Göttingen, Math.-Phys.*, 1905, vol. 1905, pp. 358–393. Available on: https://eudml.org/doc/58621 .
6. Zassenhaus H. Uber endliche Fastkörper. *Abh. Math. Sem. Hamburg*, 1935, vol. 11, pp. 187–220. doi: 10.1007/BF02940723 .
7. Hall M. Projective planes. *Trans. Amer. Math. Soc.*, 1943, vol. 54, no. 2, pp. 229–277. doi: 10.1090/S0002-9947-1943-0008892-4 .
8. Johnson N., Jha V., Biliotti M. *Handbook of finite translation planes*. NY: Chapman and Hall/CRC, 2007, 888 p. doi: 10.1201/9781420011142 .
9. Kravtsova O.V. On automorphisms of semifields and semifield planes. *Siberian Electronic Mathematical Reports*, 2016, vol. 13, pp. 1300–1313. doi: 10.17377/semi.2016.13.102 .
10. 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 .
11. Maduram D.M. Matrix representation of translation planes. *Geom. Dedicata*, 1975, vol. 4, no. 2, pp. 485–492. doi: 10.1007/BF00148776 .
12. Podufalov N.D. On spread sets and collineations of projective planes. *Contem. Math.*, 1992, vol. 131, part 1, pp. 697–705. doi: 10.1090/conm/131.1/1175813 .
13. Biliotti M., Jha V., Johnson N.L. *Foundations of translation planes*. Boca Raton: CRC Press, 2001, 558 p. doi: 10.1201/9781482271003 .
14. Mäurer H. Die affine projektivitätengruppe der Hallebenen [The affine group of projectivities of the Hall planes]. *Aequationes mathematicae*, 1987, vol. 32, no. 1, pp. 271–273. Available on: https://eudml.org/doc/137191 .
15. 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. Available on: http://rivista.math.unipr.it/fulltext/1986-12/1986-12-241.pdf .
16. Wähling H. *Theorie der fastkörper*. Ser. Thales Monographs, vol. 1. Essen: Thales-Verlag, 1987, 393 p. ISBN: 3889082319 .
17. Kravtsova O.V., Levchuk V.M. Questions of the structure of finite near-fields. *Trudy Inst. Mat. i Mekh. UrO RAN*, 2019, vol. 25, no. 4, pp. 107–117 (in Russian). doi: 10.21538/0134-4889-2019-25-4-107-117 .
18. Grishkov A.N., Zavarnitsyn A.V. Lagrange's theorem for Moufang loops. *Math. Proc. Phil. Soc.*, 2005, vol. 139, no. 1, pp. 41–57. doi: 10.1017/S0305004105008388 .
19. Grishkov A.N., Zavarnitsyn A.V. Sylow's theorems for Moufang loops. *J. Algebra*, 2009, vol. 321, no. 7, pp. 1813–1825. doi: 10.1016/j.jalgebra.2008.08.035 .
20. Yakovleva T.N. Questions of construction of quasifields with associative powers. *The Bulletin of Irkutsk State University. Series Mathematics*, 2019, vol. 29, pp. 107–119 (in Russian). doi: 10.26516/1997-7670.2019.29.107 .
21. Chein O. Moufang loops of small order. I. *Trans. Amer. Math. Soc.*, 1974, vol. 188, no. 2, pp. 31–51. doi: 10.1090/S0002-9947-1974-0330336-3 .
22. Knuth D. Finite semifields and projective planes. *J. Algebra*, 1965, vol. 2, no. 2, pp. 182–217. doi: 10.1016/0021-8693(65)90018-9 .
23. Kantor W. Commutative semifields and symplectic spreads. *J. Algebra*, 2003, vol. 270, no. 1, pp. 96–114. doi: 10.1016/S0021-8693(03)00411-3 .
24. Lavrauw M., Polverino O. Finite semifields. In: *Current research topics in Galois geometry*, L. Storme and J. De Beule (eds), NOVA Academic Publishers, 2011, chapter 6, pp. 131–160. Available on: http://hdl.handle.net/1854/LU-2152960 .
25. Wene G.P. On the multiplicative structure of finite division rings. *Aeq. Math.*, 1991, vol. 41, pp. 222–233. doi: 10.1007/BF02227457 .
26. 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, pp. 1411–1429. doi: 10.1142/S0218196707004220 .

27. Kravtsova O.V. On alternating subgroup A_5 in autotopism group of finite semifield plane. *Sib. Elektron. Mat. Izv.*, 2020, vol. 17, pp. 47–50. doi: 10.33048/semi.2020.17.004 .
28. Oyama T. On quasifields. *Osaka J. Math.*, 1985, vol. 22, no. 1, pp. 35–54. Available on: https://projecteuclid.org/journals/osaka-journal-of-mathematics/volume-22/issue-1/On-quasifields/ojm/1200778033.full .

Received November 10, 2021
Revised December 20, 2021
Accepted December 27, 2021

Funding Agency: This work was supported by the Russian Foundation for Basic Research (project no. 19-01-00566 A).

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

Daria Sergeevna Skok, Siberian Federal University, Krasnoyarsk, 660041 Russia, e-mail: skokdarya@yandex.ru .

Cite this article as: O. V. Kravtsova, D. S. Skok. The spread set method for the construction of finite quasifields, *Trudy Instituta Matematiki i Mekhaniki UrO RAN*, 2022, vol. 28, no. 1, pp. 164–181 .