Федеральное государственное автономное
образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт математики и фундаментальной информатики
Кафедра алгебры и математической логики

УТВЕРЖДАЮ
Заведующий кафедрой
/ В.М.Левчук
« 16 » июня 2016г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

ВОПРОСЫ СТРОЕНИЯ КВАЗИПОЛЕЙ С ФИКСИРОВАННЫМИ ОГРАНИЧЕНИЯМИ

Направление 01.04.01 Математика

Магистерская программа 01.04.01.02 Алгебра, логика и дискретная математика

Научный руководитель
доктор физико–математических наук,
профессор / В.М. Левчук
16.06.2016

Выпускник / Т.Н. Яковлева
16.06.2016

Красноярск 2016

АННОТАЦИЯ

Цель работы — исследование строения и классификации некоторых классов конечных квазиполей, в том числе, полуполей и квазиполей с ассоциативными степенями. Построение квазиполей тесно связано с построением проективных плоскостей трансляций. Рассматривается схема Оямы построения регулярного множества плоскости и координатизирующего ее квазиполя. С использованием известных аналогов теорем Лагранжа и Силова для луп Муфанг, в работе перечисляются возможные порядки собственных квазиполей Муфанг порядков ≤ 100.

Ключевые слова: конечное квазиполе, проективная плоскость трансляций, лупа Муфанг, квазиполе Муфанг, почти-поле.

ANNOTATION

Our goal is to study the structure and the classification of some classes of a finite quasifields including semifields and quasifield with associative powers. Construction of quasifields it is closely linked with the construction of projective translation planes. We consider the scheme of Oyama's construction spread set of plane and its coordinatizing quasifields. Using the known analogues Lagrange's and Sylow's theorems for Moufang loops, we list the possible orders of own Moufang quasifields of orders ≤ 100.

Keywords: finite quasifield, projective translation plane, Moufang loop, Moufang quasifield, nearfield.

СОДЕРЖАНИЕ

Введение 3
1 Полуполя и квазиполя 4
2 Квазиполя и проективные плоскости трансляций 7
3 Схема Оямы построения квазиполей 10
4 Квазиполя с ассоциативными степенями 16
5 Квазиполя и лупы Муфанг 18
Заключение 21
Список использованных источников 22

ВВЕДЕНИЕ

Проводимые уже более века исследования квазиполей тесно связаны с исследованиями проективных плоскостей, [1, 2, 3]. Эти исследования используют с середины прошлого века компьютерные вычисления. Их отражает обзор [4] 2007 года показывающий, что строение даже известных собственных (или не являющихся полем) конечных полуполей и квазиполей и их луп ненулевых элементов изучено мало.

Построение квазиполей тесно связано с построением проективных плоскостей трансляций. В § 2 приводятся основные определения, связанные с проективными плоскостями трансляций, в том числе определение регулярного множества плоскости, позволяющее сопоставить координатизирующее квазипле. В § 3 детально рассматривается схема построения квазиполей из работы Оямы [5] и представление регулярного множества.

В § 1 приводятся основные определения, связанные с полуполями и квазиполями. Доказано существование в любом конечном квазиполе Q простого подполя (лемма 1.2). Показано, что квазиполе Q над ним всегда является односторонним модулем, а двусторонним — не всегда. На примере почти-поля порядка 25 показывается также, что простое подполе не обязано лежать в центре квазиполя (§ 4).

В §§ 4 и 5 рассматриваются конечные квазиполя с ассоциативными степенями, а именно ассоциативные квазиполя, называемые почти-полями, и квазиполя Муфанг. Приводятся аналоги теорем Лагранжа и Силова для конечных луп Муфанг из работ [6, 7, 8]. С их помощью Чейн [9] перечислил собственные лупы Муфанг порядка < 32. Аналогично, в § 5 мы перечисляем возможные порядки собственных квазиполей Муфанг порядков ≤ 100.

1 Полуполя и квазиполя

Напомним, что множество L с бинарной операцией $\circ$ называется *лупой*, если в $(L, \circ)$ существует нейтральный элемент и уравнения $a \circ x = b$ и $y \circ a = b$ однозначно разрешимы при любых a,$b \in L$, [1, 10]. В частности, группа — это ассоциативная лупа. Простое кольцо, в котором ненулевые элементы образуют лупу по умножению, называют *полуполем* S. Более подробно,

Определение 1.1. Система $(S, +, \circ)$ является полуполем, если выполняются следующие аксиомы:

1. $(S, +)$ — абелева группа;
2. $S^* = (S \backslash \{0\}, \circ)$ — лупа;
3. для любого $x, y, z \in S$ выполняются левый и правый дистрибутивные законы, соответственно,

$$x \circ (y + z) = x \circ y + x \circ z, \quad (y + z) \circ x = y \circ x + z \circ x.$$

Таким образом, отказываясь в определении поля от коммутативности, приходят к понятию тела. Отбрасывая также требование ассоциативности, приходим к понятию полуполя. Более общее понятие дает ослабление дистрибутивности, см. [2, 3].

Определение 1.2. Множество $Q = (Q, +, \circ)$ с бинарными операциями сложения $+$ и умножения $\circ$ называют *правым квазиполем*, если выполняются следующие условия:

1. $(Q, +)$ – абелева группа;
2. $Q^* = (Q \backslash \{0\}, \circ)$ — лупа;
3. $x \circ 0 = 0$ для любого $x \in Q$;
4. выполняется правый дистрибутивный закон $(x + y) \circ z = x \circ$ $\circ z + y \circ z$ для любых $x, y, z \in Q$;
5. если $a, b, c \in Q$ и $a \neq b$, то уравнения $x \circ a = x \circ b + c$ однозначно разрешимы в Q.

Левое квазиполе определяют аналогично. Согласно теореме 7.3 Д. Хьюгеса и Ф. Пайпера [3], для конечного правого квазиполя аксиома 5 вытекает из аксиом 1-4, то есть является излишней. Далее, говорим „квазиполе“ вместо „правое квазиполе“.

Нам потребуются леммы о простом подполе.

Лемма 1.1. *Любая абелева аддитивная группа $A = (A, +)$ превращается в двусторонний $\mathbb{Z}$-модуль, если для элементов $x \in A$ и целых чисел $k > 0$ полагать $0x := 0 = x0$ и*

$$kx := \underbrace{x + x + \ldots + x}_{k \text{ раз}} = xk, \quad (-k)x := -(kx) = x(-k).$$

Доказательство. Из ассоциативности сложения в группе A и соотношения $kx = xk$ для любых $x, y \in Q$ и $k, m \in \mathbb{Z}$ вытекают следующие равенства:

$$k(mx) = (km)x = x(km) = (xk)m,$$
$$(k + m)x = kx + mx = x(k + m).$$

Используя также коммутативность сложения для любых $x, y \in Q$ и $k, m \in \mathbb{Z}$ получаем

$$k(x + y) = kx + ky = (x + y)k.$$

Лемма доказана.

Лемма 1.2. *Пусть Q — правое квазиполе с единицей e. Тогда:*

а) отображение $\pi : k \to ke \quad (k \in \mathbb{Z})$ есть гомоморфизм в Q кольца $\mathbb{Z}$ целых чисел;

б) Q — левый $\pi(\mathbb{Z})$-модуль и либо $\pi(\mathbb{Z}) \cong \mathbb{Z}$, либо $\pi(\mathbb{Z}) \cong \mathbb{Z}_p$ для простого числа p.

Доказательство. Очевидно, что для любых $k, m \in \mathbb{Z}$ имеем:

$$\pi(k + m) = (k + m)e = ke + me = \pi(k) + \pi(m).$$

Отображение π сохраняет также операцию умножения целых чисел — $\pi(km) = \pi(k)\pi(m)$, так как

$$ke \cdot me = k\big(e \cdot (me)\big) = \underbrace{e \cdot me + e \cdot me + \ldots + e \cdot me}_{k \text{ раз}} =$$

$$= \underbrace{me + me + \ldots + me}_{k \text{ раз}} = k(me) = (km)e \quad (k, m \in \mathbb{Z}).$$

Поэтому π является гомоморфизмом в Q кольца $\mathbb{Z}$ целых чисел, и первое утверждение леммы доказано.

Свойства коммутативности, ассоциативности и дистрибутивности кольца при гомоморфизмах сохраняются. Следовательно, $\pi(\mathbb{Z}) = \{ke | k \in \mathbb{Z}\}$ — ассоциативно коммутативное подкольцо в Q, причем ненулевое, так как $e \neq 0$.

В силу известной теоремы о гомоморфизмах колец, кольцо $\pi(\mathbb{Z})$ изоморфно фактор-кольцу кольца $\mathbb{Z}$ по ядру гомоморфизма $Ker(\pi)$. Если ядро гомоморфизма π нулевое, то $\pi(\mathbb{Z}) \cong \mathbb{Z}$. Когда $Ker(\pi) \neq 0$, подкольцо $\pi(\mathbb{Z})$ изоморфно конечному кольцу вычетов кольца $\mathbb{Z}$ и не имеет делителей нуля, как подмножество в Q. Следовательно, $\pi(\mathbb{Z})$ изоморфно простому подполю $\mathbb{Z}_p$ для некоторого простого числа p.

Наконец, следующие равенства показывают, что Q есть левый $\pi(\mathbb{Z})$-модуль и завершают доказательство:

$$me \cdot x = m(ex) = mx,$$
$$(ke) \cdot (me \cdot x) = k(e \cdot (me \cdot x)) = (km)x = (ke \cdot me) \cdot x,$$
$$me \cdot (x + y) = m(x + y) = mx + my = (me \cdot x) + (me \cdot y),$$
$$(ke + me)x = (ke)x + (me)x = k(ex) + m(ex) = ((k + m)e)x.$$

Из доказанного утверждения б) сразу же вытекает

Следствие 1.1. Порядок $|Q|$ всякого конечного квазиполя Q является примарным, то есть равен степени простого числа.

По аналогии с леммой 1.2 можно показать, что произвольное полуполе является также правым модулем, а поэтому и двусто-

ронним модулем над $\pi(\mathbb{Z})$. В случае конечного полуполя, выполняется более сильное утверждение.

Лемма 1.3. *Простое подполе P всякого конечного полуполя S содержится в центре S.*

Доказательство. Пусть S — полуполе и P – его простое подполе, то есть

$$P = \pi(\mathbb{Z}) = \{e, 2e, \dots\ , (p-1)e, pe = 0\}.$$

Докажем, что $P \subset Z(S)$, где $Z(S)$ — это центр S. Другими словами, нужно показать, что при любых $ke \in P^*$ и $x \in S$ всегда имеем, что $(ke)x = x(ke)$. Это показывают следующие равенства:

$$(ke)x = \underbrace{(e + \dots\ + e)}_{k\ \text{раз}} x = \underbrace{ex + \dots\ + ex}_{k\ \text{раз}} = \underbrace{x + \dots\ + x}_{k\ \text{раз}},$$

$$x(ke) = x\underbrace{(e + \dots\ + e)}_{k\ \text{раз}} = \underbrace{xe + \dots\ + xe}_{k\ \text{раз}} = \underbrace{x + \dots\ + x}_{k\ \text{раз}}.$$

Доказательство завершено.

Известно (§ 4), что существует квазиполе порядка 25, простое подполе которого не содержится в центре этого квазиполя.

2 Квазиполя и проективные плоскости трансляций

Построение квазиполей и проективных плоскостей трансляций тесно связаны. Согласно [1, § 20.1] и [11], *проективная плоскость* — это множество точек, определенные подмножества которого называются прямыми и которое удовлетворяет следующим свойствам: 1) две произвольные различные точки лежат на одной и только на одной прямой, 2) две произвольные различные прямые пересекаются в одной и только одной точке и 3) существуют четыре точки, никакие три из которых не лежат на одной прямой.

Всякой проективной плоскости π соответствует двойственная плоскость π^α. По определению, ее точки — это прямые из π,

а прямые — это точки плоскости π; прямую и точку в π^α считают инцидентными тогда и только тогда, когда они инцидентны в π.

Биективное отображение точек и прямых плоскости π, соответственно, на точки и прямые другой называют *изоморфизмом плоскостей*, если оно сохраняет инцидентность. Всякую коллинеацию (или автоморфизм) плоскости π, фиксирующую каждую точку прямой $l \in \pi$ и каждую прямую, проходящую через точку P, называют (P, l) – перспективной. Если существует прямая $l \in \pi$ такая, что для любой точки $P \in l$ группа (P, l) – перспективных коллинеаций действует транзитивно на точках аффинной плоскости $\pi \backslash l$, то π называют *плоскостью трансляций*, а если также двойственная к π плоскость есть плоскости трансляций, — полуполевой плоскостью.

Известно [3], что проективную плоскость трансляций любого примарного порядка p^n с простым p удается построить, координатизируя ее n-мерным линейным пространством W над полем Z_p и снабжая W структурой квазиполя порядка p^n с помощью определенного регулярного множества.

Для построения плоскостей трансляций ранга n выбирают n-мерное линейное пространство W над полем F (*координатизирующее множество*), внешнюю прямую сумму $V = W \oplus W = \{(x, y) | x, y \in W\}$ двух копий W и *расщепление* μ аддитивной группы $(V, +)$ такое, что $V = M \oplus N$ для любых $M \neq N$ из μ. По определению, точки проективной плоскости трансляций $\pi = \pi(V, \mu)$ есть 1-мерные подпространства из V, а прямые —это подгруппы из μ и смежные классы по ним; смежные классы по одной и той же подгруппе, по определению, пересекаются в одной и той же точке (∞), называемой особой, а особую прямую $[\infty]$ в π составляют все особые точки, [2, 3].

Далее мы введем определение регулярного множества плоскости и установим соответствующее ему квазиполе на W. Напомним, что *расщеплением аддитивной группы* называют набор ее подгрупп (компоненты расщепления), имеющих попарно нулевые

пересечения и дающих в теоретико-множественном объединении всю группу, [2].

Компоненты выбранного расщепления μ группы $(V,+)$ есть n-мерные подпространства в V. Более точно, согласно Люнебургу [2], верна следующая лемма, где полагаем, по определению,

$$V(\sigma)=\big\{(v,v^{\sigma})|v\in W\big\}$$
$$\big(\sigma\in GL(W)\big),\quad V(0)=(W,0),\quad V(\infty)=(0,W).$$

Пусть θ — биективное отображение пространства W в кольцо $M(n,F)$ всех $n\times n$ – матриц над F. Образ $R=\theta(W)$ называют *регулярным множеством*, если:

1) единичная и нулевая матрицы E и O лежат в R,

2) $R\backslash\{O\}$ и матрицы $\theta(u)-\theta(v)$ лежат в $GL(n,F)$ при любых $u,v\in W$, $u\neq v$.

В этом случае приходим к квазиполю $(W,+,\circ)$ с умножением

$$x\circ y=x\cdot\theta(y)\quad(x=(x_1,x_2,\ldots,x_n),y=(y_1,y_2,\ldots,y_n)\in W).$$

Будем обозначать $W=W(n,q^n,\theta)$ квазиполе порядка q^n с регулярным множеством в $GL(n,q)\cup\{0\}$, заданным отображением θ. Если π — плоскость трансляций, координатизируемая квазиполем W, то далее обозначаем $\pi=\pi(W)$.

Согласно Каллахеру [12, Теорема 6.1], аффинная плоскость является трансляционной тогда и только тогда, когда она координатизируется квазиполем. В случае полуполя — это полуполевая плоскость. Известна [13]

Теорема 2.1. *Две полуполевые плоскости изоморфны тогда и только тогда, когда их координатизирующие полуполя изотопны.*

Напомним, что тройку биективных отображений α,β,γ группоида $(S,\circ)$ на $(V,\cdot)$ называют *изотопизмом*, если $\alpha(x\circ y)=$ $=\beta(x)\cdot\gamma(y)\quad(x,y\in S)$. Изотопизмом квазиполей Q и W называют тройку изоморфизмов аддитивной группы $(Q;+)$ на $(W;+)$, если их ограничения на лупе Q^* — ее изотопизм на W^*.

3 Схема Оямы построения квазиполей

Вначале рассмотрим представление Оямы [5] регулярного множества проективной плоскости.

Пусть $GF(q)$ есть конечное поле порядка q. Для элемента x из расширения $GF(q^n)$ степени n поля $GF(q)$ элемент $\bar{x} = x^q$ назовем сопряженным к x. Положим

$$x = x^{(0)}, \quad \overline{x} = x^{(1)} = x^q, \quad x^{(i)} = x^{(q^i)}, \quad i = 2, 3, \ldots, n-1.$$

Тогда отображение $x \to x^{(i)}$ есть автоморфизм поля $GF(q^n)$, действующий тождественно на подполе $GF(q)$. Если $\alpha = (\alpha_{ij}) \in$ $\in GL(n, q^n)$, то полагая

$$\overline{\alpha} = \overline{(\alpha_{ij})}, \quad w = \begin{pmatrix} 0 & \ldots & \ldots & 0 & 1 \\ 1 & 0 & \ldots & \ldots & 0 \\ 0 & \ddots & \ddots & & \\ \vdots & \ddots & \ddots & \ddots & \\ 0 & \ldots & 0 & 1 & 0 \end{pmatrix},$$

где w – $n \times n$-матрица, введем множество

$$\mathfrak{A} = \{\alpha \in GL(n, q^n) | \overline{\alpha} = \alpha w\}. \tag{3.1}$$

Лемма 3.1. *Для любого $\alpha_0 \in \mathfrak{A}$ верно равенство $\mathfrak{A} =$ $= GF(n, q)\alpha_0$. Кроме того, $n \times n$ – матрица α над $GF(q^n)$ лежит в $\mathfrak{A}$ тогда и только тогда, когда существуют линейно независимые над $GF(q)$ элементы $\alpha_0, \alpha_1, \ldots, \alpha_{(n-1)}$ с условием, что*

$$\alpha = \begin{pmatrix} \alpha_0 & \alpha_0^{(1)} & \ldots & \alpha_0^{(n-1)} \\ \alpha_1 & \alpha_1^{(1)} & \ldots & \alpha_1^{(n-1)} \\ \vdots & \vdots & \ldots & \vdots \\ \alpha_{n-1} & \alpha_{n-1}^{(1)} & \ldots & \alpha_{n-1}^{(n-1)} \end{pmatrix}.$$

Доказательство. Для любого элемента δ из $GL(n, q)$ выполняются равенства $\overline{\delta\alpha_0} = \delta\overline{\alpha_0} = \delta\alpha_0 w$, следовательно $\delta\alpha_0 \in \mathfrak{A}$. Иначе, для любого элемента α из $\mathfrak{A}$, $\overline{\alpha\alpha_0^{-1}} = \alpha w w^{-1}\alpha_0^{-1} = \alpha\alpha_0^{-1} \in$

$\in GL(n,q)$ и поэтому $\alpha \in GL(n,q)\alpha_0$. Таким образом $\mathfrak{A} \in$ $\in GL(n,q)\alpha_0$.

Пусть $\alpha = (\alpha_{ij})$ — это любой элемент из множества $\mathfrak{A}$, заданного формулой (3.1). Так как

$$\overline{\alpha} = \alpha w, \overline{\alpha_{ij}} = \alpha_{i2},$$
$$\overline{\alpha_{i1}} = \alpha_{i3}, \ldots, \overline{\alpha_{in-1}} = \alpha_{in}, \quad i = 1, 2, \ldots, n,$$

то

$$\alpha_{ij} = \alpha_{i1}^{(j-1)}, \quad i = 1, 2, \ldots, n; \quad j = 2, 3, \ldots, n.$$

В силу невырожденности матрицы α, элементы $\alpha_{11}, \alpha_{21}, \ldots, \alpha_{n1}$ линейно независимы над $GF(q)$.

Обратное утверждение очевидно и поэтому доказательство завершено.

Сейчас несложно доказывается

Лемма 3.2. *Если* $\alpha \in \mathfrak{A}$, *то*

$$\alpha^{-1} = \begin{pmatrix} \alpha_0 & \alpha_1 & \ldots & \alpha_{n-1} \\ \alpha_0^{(1)} & \alpha_1^{(1)} & \ldots & \alpha_{n-1}^{(1)} \\ \vdots & \vdots & \ldots & \vdots \\ \alpha_0^{(n-1)} & \alpha_1^{(n-1)} & \ldots & \alpha_{n-1}^{(n-1)} \end{pmatrix} \in GL(n, q^n).$$

Оказывается, в матричном представлении в регулярном множестве R все ненулевые матрицы имеют вид, описанный в лемме 3.1. Кроме того, регулярное множество содержит нулевую и единичную матрицу, а разность любых различных матриц из R всегда есть невырожденная матрица.

Для построения квазиполей зафиксируем базу в векторном пространстве $V(n,q)$, то есть n-мерном над $GF(q)$. Вектор $\upsilon \in V(n,q)$ представляем координатной строкой $(x_0, x_1, \ldots, x_{n-1})$.

Пусть α — фиксированный элемент из множества $\mathfrak{A}$ (3.1).

Тогда

$$\alpha = \begin{pmatrix} \alpha_0 & \alpha_0^{(1)} & \dots & \alpha_0^{(n-1)} \\ \alpha_1 & \alpha_1^{(1)} & \dots & \alpha_1^{(n-1)} \\ \dots & \dots & \dots & \dots \\ \alpha_{n-1} & \alpha_{n-1}^{(1)} & \dots & \alpha_{n-1}^{(n-1)} \end{pmatrix},$$

$$\upsilon\alpha = x, x^{(1)}, \dots, x^{(n-1)} \in V(n, q^n), \qquad x = \sum_{i=0}^{n-1} x_i\alpha_i.$$

Обратно, пусть υ^* принадлежит векторному пространству $V(n, q^n)$ и $\upsilon^* = (x, x^{(1)}, \dots, x^{(n-1)})$, где $x \in GF(q^n)$. Так как $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ линейно независимые над $GF(q)$, то x однозначно представляется $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ так, что $x = \sum\limits_{i=0}^{n-1} x_i\alpha_i$, $x_i \in GF(q)$. Следовательно, $\upsilon^{*\alpha^{-1}} = (x_0, x_1, \dots, x_{n-1}) \in V(2n, q)$. Таким образом, $V(n, q)^\alpha = \left\{(x, x^{(1)}, \dots, x^{(n-1)}) | x \in GF(q^n)\right\}$ и $V(n, q)^\alpha$ являются $GF(q)$ – векторным пространством изоморфным $V(n, q)$.

Очевидно, $V(2n, q)^\alpha = \left\{(u\alpha, \upsilon\alpha) | u, \upsilon \in V(n, q)\right\}$ есть $GF(q)$ – векторное пространство, изоморфное $V(2n, q)$.

Обозначим вектор $(x, x^{(1)}, \dots, x^{(n-1)})$ как $((x))$, где $((x)) \in \in V(n, q)^\alpha$. Тогда любой вектор из $V(2n, q)^\alpha$ обозначим как $\big(((x)), ((y))\big)$. Аддитивная группа из $GF(q^n)$ изоморфна $V(n, q)^\alpha$ согласно отображению $x \to ((x))$. В этом отображении прообраз $\upsilon^* \in V(n, q)^\alpha$ обозначим как $\widehat{\upsilon}^*$.

Пусть M любой элемент из $GL(n, q)$. Тогда

$$M^\alpha = \begin{pmatrix} x_0 & x_{n-1}^{(1)} & \dots & x_1^{(n-1)} \\ x_1 & x_0^{(1)} & \dots & x_2^{(n-1)} \\ \dots & \dots & \dots & \dots \\ x_{n-1} & x_{n-2}^{(1)} & \dots & x_0^{(n-1)} \end{pmatrix},$$

однозначно определяется первым столбцом. Следовательно, M^α

можно обозначить как

$$\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{bmatrix}.$$

Пусть $\mu = \{V(\infty)\} \cup \{V(M) | \in \sum\}$ расщепление из $V(2n, q)$, где $\sum$ это объединение подмножеств из $GL(n, q)$ и $\{0\}$. Тогда

$$\mu^\alpha = \left\{V^*(\infty)\right\} \cup \left\{V^*(M^\alpha) | M \in \sum\right\}, \tag{3.2}$$

где

$$V^*(\infty) = \left\{\big(((0)), ((x))\big) | ((x)) \in V(n, q)^\alpha\right\},$$
$$V^*(M^\alpha) = \left\{\big(((x)), ((x))M^\alpha\big) | ((x)) \in V(n, q)^\alpha\right\}.$$

Так как $(\upsilon\alpha)M^\alpha = (\upsilon M)\alpha$, то μ^α это расщепление из $V(2n, q)^\alpha$. Следовательно, μ^α определяет плоскость трансляций, которую обозначим как Π^*. Мы можем считать, согласно Люнебургу [2, Лемма 2.1], что расщепление μ^α содержит

$$V^*(1) = \left\{\big(((x)), ((x))\big) | ((x)) \in V(n, q)^\alpha\right\}. \tag{3.3}$$

Для любых двух векторов $((x)) \neq ((0))$ и $((y))$ из $V(n, q)^\alpha$ существует единственная матрица $M^\alpha = \sum^\alpha$ такая, что $((x))M^\alpha = ((y))$, $((x)) = ((1)) = (1, 1, \ldots, 1)$. Тогда любой элемент y из $GF(q^n)$ однозначно определяется

$$M^\alpha = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix} \in \sum^\alpha$$

так, что $((1))M^\alpha = ((y))$. Это означает, что $y = \sum_{i=0}^{n-1} y_i$.

Обратно, (3.3) однозначно определено как $y = GF(q^n)$ таким образом, что $((1))M^\alpha = ((y))$. Исходя из этого, можем обозначить

$$M^\alpha = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix} = [y]\,,$$

где $y = \sum_{i=0}^{n-1} y_i$. Тогда отображение $GF(q^n) \to \sum^\alpha$ является биекцией согласно $y \to [y]$. Следовательно, $\sum^\alpha = \{[x]\,|x \in GF(q^n)\}$. В этом отображении прообраз $M^* \in \sum^\alpha$ обозначим как $\widehat{M^*}$.

Далее сформулируем две теоремы, в которых отражено построение квазиполей с помощью регулярных множеств.

Теорема 3.1. *Пусть* $\sum^* = \{[x]\,|x \in GF(q^n)\}$ *— это регулярное множество степени* n *над конечным полем* $GF(q^n)$. *Тогда имеем квазиполе* Q *с двумя бинарными операциями* $+$ *и* $\circ$, *удовлетворяющее следующим условиям:*

(1) $Q = GF(q^n)$ *как множество;*

(2) сложение $+$ *является обычным сложением поля* $GF(q^n)$;

(3) умножение $\circ$ *получается как* $x \circ y = \widehat{((x))\,[y]}$, *где* $((x)) = (x, x^{(1)}, \ldots, x^{(n-1)}) \in V(n, q^n)$ *и* $[y] \in \sum^*$.

Доказательство. Известно, что аффинная плоскость является плоскостью трансляций тогда и только тогда, когда она координатизированна квазиполем [3, Теорема 6.1]. Используя это, можно построить квазиполе.

Пусть Π^* — это плоскость трансляций с расщеплением μ^α, определенная в $V(2n, q)^\alpha$. Если точка из Π^* представлена вектором $\big(((x)), ((y))\big)$ из $V(2n, q)^\alpha$, то этой точки дадим координаты (x, y), где $x, y \in GF(q^n)$. Тогда Q состоит из всех элементов координат плоскости Π из поля $GF(q^n)$, и является квазиполем со следующими двумя бинарными операциями $+$ и $\circ$:

(1) сложение + является обычным сложением поля;

(2) умножение $\circ$ получается как

$$x \circ y = \widehat{((x))\,[y]} = \sum_{i=0}^{n-1} x^{(i)} y_i, \quad \text{если} \quad [y] = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix}.$$

Используя эти координаты, мы можем записать линии плоскости Π^* следующими образом:

$$V^*(m) + k = \big\{(x, x \circ m + k) | x \in GF(q^n)\big\} \cup \big\{(m)\big\},$$
$$V^*(\infty) + k = \big\{(k, y) | y \in GF(q^n)\big\} \cup \big\{(\infty)\big\},$$
$$l_\infty = \big\{(m) | m \in GF(q^n)\big\} \cup \big\{(\infty)\big\}.$$

Считая, что $\sum^*$ содержит $q^n - 1$ матрицу из $GL(n,q)^\alpha$ и 0, назовем $\sum^*$ регулярным множеством степени n над $GF(q^n)$, если $\sum^*$обладает следующими свойствами:

а) для $m = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix} \in \sum^*$, положим $\beta(m) = \sum_{i=0}^{n-1} y_i$. Тогда $\big\{\beta(m) | m \in \sum^*\big\} = GF(q^n)$, следовательно $m = [\beta(m)]$;

б) если $m_1, m_2 \in \sum^*$ и $m_1 \neq m_2$, то $m_1 - m_2 \in GL(n,q)^\alpha$.

Очевидно, что для любого вектора $((x)) \neq 0 \in V(n,q)^\alpha$ имеем $\big\{((x))m | m \in \sum^*\big\} = V(n,q)^\alpha$.

Пусть (3.2) и

$$V^*(m) = \Big\{\big(((x)), ((x))m\big) | ((x)) \in V(n,q)^\alpha\Big\},$$

тогда $\big\{V^*(\infty)\big\} \cup \big\{V^*(m) | m \in \sum^*\big\}$ является расщеплением μ из $V(2n,q)^\alpha$ и поэтому определяет плоскость трансляций Π^*.

Теорема 3.2. *Любое конечное квазиполе Q с двумя бинарными операциями + и $\circ$ можно построить с помощью метода, изложенного в теореме 3.1.*

Доказательство. Ядро из Q является множеством $K(Q)$, состоящее из всех элементов $k \in Q$ таких, что $(k \circ a) \circ b = k \circ (a \circ b)$ и $k \circ (a + b) = k \circ a + k \circ b$ для всех $a, b \in Q$. Тогда $K(Q)$ — это конечное поле, и Q является $K(Q)$ – векторным пространством. Пусть $K(Q)$ имеет порядок q и пусть Q имеет размерность n над $K(Q)$.

Холл [1] доказал следующее. Пусть $V(2n, q) = Q \oplus Q$ внешняя прямая сумма двух копий из $K(Q)$ — векторного пространства Q. Если

$$V(m) = \big\{(x, x \circ m) | x \in Q\big\},$$
$$V(\infty) = \big\{(0, x) | x \in Q\big\},$$

то $\mu = \big\{V(m) | m \in Q \cup \{\infty\}\big\}$ является расщеплением из $V(2n, q)$. Кроме того, $\sum = \{(x \to x \circ m) | m \in Q\}$.

Следовательно, снабжая координатизирующее множество структурой квазиполя Q, мы полностью определяем плоскость трансляций.

4 Квазиполя с ассоциативными степенями

Наиболее изучены квазиполя с ассоциативными степенями: ассоциативные квазиполя или почти-поля [1].

Известен единообразный способ построения конечного почти-поля как специального расширения степени n центра $GF(q)$ с аддитивной группой $(GF(q^n), +)$. Это расширение порядка p^{ln}, называемое почти-полем Диксона, характеризуют порядком $q = p^l$ центра и степенью n, которое можно выбирать произвольно с условиями:

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

2) если $q \equiv 3 \pmod 4$, то $n \not\equiv 0 \pmod 4$.

Как доказал в 1936 году Цассенхауз [14], конечные почти-поля исчерпываются почти-полями Диксона и, кроме того, семью

исключительными почти-полями порядка p^2 с простыми $p = 5, 7, 11, 23, 29, 59$. (Они выписаны в [1].)

Отметим, что в лемме 1.2 нельзя заменить левый модуль над простым подполем $\pi(\mathbb{Z})$ на правый. Это можно показать на примере почти-поля NQ порядка 25 из списка названных выше 7 исключительных почти-полей. Лупа NQ^* выписана в [1] явно, как матричная группа

$$NQ^* = \left\langle A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & -2 \\ -1 & -2 \end{pmatrix} \right\rangle,$$

которая изоморфна группе $SL(2,3)$ порядка 24. Группа $SL(2,3)$ имеет центр $\{E, -E\}$ порядка 2. Поэтому центр почти-поля NQ имеет порядок 3 и не содержит простое подполе. Доказана

Лемма 4.1. *Существует почти-поле NQ порядка 25 с простым подполем*

$$Z_5E = \{0, E, -E, 2E, -2E\},$$

не лежащим в центре NQ.

Можно показать, что если S — полуполе и почти-поле, то S есть тело, а при условии конечности, даже конечное поле, по известной теореме Веддерберна — Артина; в частности, лупа S^* будет циклической группой.

К квазиполям с ослабленной ассоциативностью приводят квазиполя Муфанг с лупой Муфанг ненулевых элементов, по определению. Согласно [15], *лупа Муфанг* — это лупа M такая, что для всех $x, y, z \in M$ выполняется одно из (эквивалентных) тождеств:

$$(xy)(zx) = \big(x(yz)\big)x, \tag{4.1}$$
$$\big((xy)z\big)y = x\big(y(zy)\big), \tag{4.2}$$
$$x\big(y(xz)\big) = \big((xy)x\big)z. \tag{4.3}$$

Если квазиполе удовлетворяет тождеству Муфанг 4.1, то его называют *квазиполем Муфанг*, [16].

Замечание 4.1. *Из определений квазиполя Муфанг и почти-поля сразу же следует, что все квазиполя Муфанг являются обобщением почти-полей.*

Проективную плоскость называют *плоскостью Муфанг*, если каждая прямая является трансляционной. Плоскость Муфанг координатизируется полуполем D с альтернативными законами:

$$x(xy) = x^2y, \qquad (xy)y = xy^2 \quad (x, y \in D),$$

или, что равносильно, полуполем с обратными свойствами:

$$(yx)x^{-1} = y, \qquad x^{-1}(xy) = y \quad (x, y \in D).$$

Хорошо известно, что проективная плоскость трансляций дезаргова тогда и только тогда, когда ее координатизирующее квазиполе является полем. В силу следующей теоремы, конечная плоскость Муфанг является папповой и дезарговой.

Теорема 4.1. *[3, Теорема 6.20 (Артин — Цорн)] Каждое конечное альтернативное полуполе является полем.*

5 Квазиполя и лупы Муфанг

Лупы Муфанг были введены и изучались Р. Муфанг [17] в 1930-х годах, и обсуждались детально в книге Р. Брука [15].

Тождества 4.1 – 4.3 называются *тождествами Муфанг*. Их эквивалентность устанавливает лемма 3.1 в [15].

В силу этой же леммы, лупа Муфанг M удовлетворяет также тождествам

$$(xx)y = x(xy) \quad (xy)x = x(yx) \quad (yx)x = y(xx). \tag{5.1}$$

Циклические и двупорожденные лупы Муфанг — ассоциативны, и поэтому являются группами. В частности, циклические лупы Муфанг — это хорошо известные циклические группы.

Р. Муфанг [17] доказала теорему, что каждая лупа Муфанг M, является *ди-ассоциативной*, то есть любые два элемента порождают подгруппу в M. Более того, если $(x, y, z) = 1$ для некоторых $x, y, z \in L$, то $< x, y, z >$ является группой [15, с. 117].

Так как тождество (5.1) выполняется в каждой лупе Муфанг, то второе утверждение теоремы следует из первой. Эта теорема была доказана Р. Муфанг одновременно для луп Муфанг и альтернативных колец с делением, с помощью математической индукции.

Ди-ассоциативность луп Муфанг подразумевает следующие свойства [15]:

1) если $ab = 1$, то $ba = 1$ для $\forall a, b \in M$;

2) b можно обозначить как a^{-1};

3) $\forall c \in M$, $(ca)a^{-1} = c$, $a^{-1}(ac) = c$ и $(ac)^{-1} = c^{-1}a^{-1}$.

Р. Брук в [9] для конечных луп выделил следующие свойства:

1) порядок каждой подлупы K конечной лупы L делится на порядок L;

2) если H есть подподлупа подлупы K конечной лупы L, то порядок H делится на порядок K. Другими словами, каждая подлупа из лупы L обладает свойством (2).

Для луп Муфанг также выполняются различные свойства, которые имеют место для групп. В работе [6] было доказано, что теорема Лагранжа имеет место не только для групп, но и для конечных луп Муфанг. Для доказательства этой теоремы Гришков и Заварницин использовали связь между лупами Муфанг и группами с тройственностью. Аналог теоремы Силова для луп Муфанг был доказан в [7, 8].

Ниже приведем эти теоремы.

Теорема 5.1. *Порядок любой конечной лупы Муфанг M делится на порядок любой ее подлупы.*

Определение 5.1. p-подлупа P лупы Муфанг M называется силовской p-подлупой, если показатель(индекс) не делится на простое число p. Множество всех силовских p-подлуп M обозначим как $Syl_p(M)$.

Теорема 5.2. *Если M — конечная лупа Муфанг, p — силовское простое число для M и P является p-подлупой M, то существует p-подлупа для M, которая содержит P.*

Теорема 5.3. *Если M — конечная лупа Муфанг и p — силовское простое число для M, то $|Syl_p(M)| \equiv 1 \pmod{p}$).*

Также для конечных луп Муфанг С. Гагола в [18] доказал аналог теоремы Холла .

В статье Орина Чейна [9] были приведены следующие свойства о лупах Муфанг:

Лемма 5.1. *Если p — простое число, то лупа Муфанг M порядка p^3 является группой.*

Лемма 5.2. *Если p — простое число, то каждая лупа Муфанг M порядка p или p^2 является группой.*

Лемма 5.3. *Если p и q — различные простые числа и $p < q$, то каждая лупа Муфанг M порядка pq является группой.*

В статье Орина Чейна [9] были перечислены все неассоциативные лупы Муфанг порядков ≤ 32. Он показал, что существует 13 таких луп: одна из которых имеет порядок 12, пять – порядка 16, одна – порядка 20, пять – порядка 24 и одна – порядка 28. А значит собственное квазиполе Муфанг Q порядка 25 имеет лупу Муфанг M порядка 24 и, следовательно, известную.

Используя леммы 5.1 – 5.3, а также теоремы 5.1, 5.2 и 5.3, получаем описание возможных порядков собственных квазиполей Муфанг порядков ≤ 100.

Теорема 5.4. *Собственные квазиполя Муфанг порядка ≤ 100 могут существовать лишь для порядков 25, 49, 64 и 81.*

ЗАКЛЮЧЕНИЕ

В магистерской диссертации получены следующие результаты.

1. Доказано, что в любом конечном квазиполе существует простое подполе, и над ним правое квазиполе есть левый модуль.
2. Показано, что простое подполе не обязано лежать в центре квазиполя.
3. Доказано, что простое подполе всякого конечного полуполя содержится в центре этого полуполя.
4. Построен пример почти-поля, являющегося односторонним, но не двусторонним модулем над своим простым подполем.
5. Рассмотрена схема Оямы [5] построения регулярного множества плоскости и координатизирующего ее квазиполя.
6. С помощью известных аналогов теорем Лагранжа и Силова для луп Муфанг, перечислены возможные порядки собственных квазиполей Муфанг порядков ≤ 100.

Полученные результаты имеют теоретическое значение и могут быть использованы при разработке криптографических методов.

Апробация работы. Основные результаты исследования докладывались в СФУ в 2014 и 2016 годах на научно-технических конференциях студентов, аспирантов и молодых ученых «МОЛОДЕЖЬ И НАУКА».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Холл, М. Теория групп / М. Холл. — Москва : Издательство иностранной литературы, 1962. — 468 p.

2 Luneburg, H. Translation planes / H. Luneburg. — Berlin–Heidelberg–New York : Springer, 1980.

3 Hughes, D. R. Projective planes / D. R. Hughes, F. C. Piper. — New-York Inc : Springer–Verlag, 1973. — 291 p.

4 Johnson, N. L. Handbook of finite translation planes / N. L. Johnson, V. Jha, M. Biliotti. — London New York: Chapman Hall/CRC, 2007. — 861 p.

5 Oyama, T. On quasifields / T. Oyama // Osaka Journal of Mathematics. — 1985. — № 22(1). — P. 35–54.

6 Grishkov, A. N. Lagrange's theorem for Moufang Loops / A. N. Grishkov, A. V. Zavarnitsine // Math. Proc. Camb. Phil. Soc. — 2005. — № 1(139). — P. 41—57.

7 Gagola, S. M. The conjugacy of triality subgroups of Sylow subloops of Moufang loops / S. M. Gagola // Journal of Group Theory. — 2010.

8 Grishkov, A. N. Sylow's theorem for Moufang loops / A. N. Grishkov, A. V. Zavarnitsine // J. Algebra 321. — 2009 (7). — P. 1813–1825.

9 Chein, O. Moufang loops of small order / O. Chein // Transactions of the American mathematical society. — Vol.188, issue 2. —1974.

10 Курош, А. Г. Лекции по общей алгебре / А. Г. Курош. — Санкт-Петербург : Лань, 2007. — 560 с.

11 Veblen, O. Non-Desarguesian and Non-Pascalian Geometries / O. Veblen, J. H. Maclagan-Wedderburn // Trans. Amer. Math. Soc. — 1907. — Vol. 8, №3. — P. 307–388.

12 Kallaher, M. Affine planes with transitive collineation groups / M. Kallaher. — North-Holland. — 1982.

13 Albert, A. A. Finite division algebras and finite planes / A. A. Albert // Proc. Sympos. Appl. Math. AMS, Provid. R.I — 1960. — Vol.10. — P. 53-70.

14 Zassenhaus, H. Uber endliche Fastkorper / H. Zassenhaus // Abh. Math. Sem. Hamburg. — 1936. — 11. — P. 187–220.

15 Bruck, R. H. A survey of binary systems / R. H. Bruck. — Springer-Verlag, 1971. — 188 p.

16 Kallaher, M. J. Right Bol quasi-fields / M. J. Kallaher // Canadian journal of mathematics. — 1969. —P. 1409–1420.

17 Moufang, R. Zur Struktur von Alternativkorpern / R. Moufang // Math. Ann. — 1935. — 110. — P. 416–430.

18 Gagola, S. M. Hall's Theorem for Moufang loops / S. M. Gagola // J. Algebra 323. — 2010. — P. 3252–3262.

19 Левчук, В. М. Строение квазиполей малых четных порядков / В. М. Левчук, П. К. Штуккерт // Труды ИММ УрО РАН. — 2015. — Т. 21, № 3. — С. 197–212.