ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 21 № 3 2015

УДК 512.554

СТРОЕНИЕ КВАЗИПОЛЕЙ МАЛЫХ ЧЕТНЫХ ПОРЯДКОВ[1]

В. М. Левчук, П. К. Штуккерт

Изучаются вопросы строения конечного квазиполя: максимальные подполя, порядки элементов его мультипликативной лупы и гипотеза об однопорожденности лупы конечного полуполя. Исследовано строение полуполей порядка 16, полуполя Кнута — Руа порядка 32, опровергающего гипотезу Венэ, и представителей изотопных классов квазиполей порядков 16 и 32.

Ключевые слова: конечное квазиполе, максимальное подполе, порядок ненулевого элемента, гипотеза об однопорожденности мультипликативной лупы конечного полуполя.

V. M. Levchuk, P. K. Shtukkert. The structure of quasifields of small even orders.

We study the structure of a finite quasifield: maximal subfields, the orders of nonzero elements of its multiplicative loop, and the conjecture that the multiplicative loop of any finite semifield is one-generated. We consider the structure of all semifields of order 16; the Knuth–Rua semifield of order 32, which disproves Wene's conjecture; and representatives of isotope classes of quasifields of orders 16 and 32.

Keywords: finite quasifield, maximal subfield, order of a nonzero element, conjecture that the multiplicative loop of any finite semifield is one-generated.

Введение

Ослабление свойств коммутативности и ассоциативности полей приводит к понятию полуполя (“квазитело” в терминологии А. Г. Куроша [1, II.6.1]); это кольцо S, в котором ненулевые элементы по умножению образуют лупу S^*. С другой стороны, исследования недезарговых проективных плоскостей трансляций, восходящие к работам О. Веблена – Дж. Веддерберна [2] и Л. Диксона [3] начала 1900-х гг., опираются на более общее понятие квазиполя, ослабляющее также двустороннюю дистрибутивность до односторонней (см. разд. 1). В исследованиях, начиная с середины прошлого века, используются компьютерные вычисления.

Строение даже известных *собственных* (или не являющихся полем) конечных полуполей и квазиполей и их луп ненулевых элементов изучено мало (см. обзор [4]). Более изучены квазиполя с ассоциативными степенями: ассоциативные квазиполя или *почти-поля* [5], альтернативные кольца [1]; на лупы Муфанг теоретико-групповые теоремы переносят М. Либек [6], А. Н. Гришков и А. В. Заварницын [7; 8], С. М. Гагола [9] и др.

Г. Венэ [10] высказал в 1991 г. *гипотезу о правоцикличности конечных полуполей*, т. е. о представимости ненулевых элементов правоупорядоченными степенями одного элемента. На основе перечисления Д. Кнута полуполевых плоскостей порядка 32 [11; 12] И. Руа [13] указал в 2004 г. полуполе порядка 32 (*полуполе Кнута — Руа*), опровергающее гипотезу Венэ, а также изотопное с ним полуполе порядка 2^5 с подполем порядка 4.

Аналогично спектру лупы [14; 15] в разд. 2 введены левый и правый спектры с помощью наименьших лево- и правоупорядоченных степеней элементов, равных единице.

Для конечных полуполей и квазиполей в [14; 15] записаны следующие задачи.

(А) *Перечислить максимальные подполя и их порядки.*

(Б) *Выявить конечные квазиполя S с неоднопорожденной лупой S^*.*

Г и п о т е з а. *Лупа S^* всякого конечного полуполя S однопорождена.*

[1]Работа выполнена при поддержке РФФИ (проект 12-01-00968).

(B) *Определить, какие возможны спектры лупы S^* конечного полуполя и квазиполя.*

Решение задач для полуполя Кнута — Руа $\Re$ порядка 32 дает в разд. 2 теорема 1, выявившая порождаемость лупы $\Re^*$ любым неединичным элементом, ее спектр $\{1, 5, 6, 7, 8, 10\}$, а также правый и левый спектры $\{1, 21\}$. В разд. 4 найдено строение представителей всех изотопных классов собственных квазиполей порядка 32. Их выбираем с помощью регулярных множеств плоскостей трансляций порядка 32, классификация которых завершена в 2011 г. (У. Демпвольф [26] и Р. Рокенфеллер [28]). Ранее [16] был изучен случай представителей, являющихся полуполем (см. теоремы 4 и 5). Теорема 6 посвящена оставшимся случаям.

В разд. 3 задачи решены для всех собственных полуполей порядка 16. Е. Клейнфилд [24] классифицировал их, с точностью до изоморфизмов (предложение 4), разрабатывая алгоритм построения таблицы Кэли лупы. Мы сокращаем его список до 16 полуполей, с точностью до изоморфизмов и антиизоморфизмов, и для каждого указываем явную формулу умножения (теорема 2). Формулы для двух неизотопных полуполей выписал ранее Д. Кнут [12]; таблицы Кэли лупы и формулы в некоторых других случаях см. [15], а также [27]. Результаты о строении полуполей сведены в табл. 4, анонсированную (без правого и левого спектров) в [15].

Собственные квазиполя наименьшего четного порядка 16 образуют семь изотопных классов. Из них пять классов не содержат полуполей; в [15, теоремы 3.1–3.3] выявлено строение их представителей, выбранных с помощью [25]. Его резюмирует теорема 3 в разд. 3; в частности, три из них являются теоретико-множественным объединением семи своих подполей порядка 4.

1. Координатизация плоскостей трансляций квазиполями

По определению полуполе — это (простое) кольцо $S = (S, +, \cdot)$, в котором $(S \setminus \{0\}, \cdot)$ есть лупа. Напомним, что группоид L с бинарной операцией $\cdot$ называют *квазигруппой*, если при любых $a, b \in L$ каждое из уравнений $ax = b$ и $xa = b$ однозначно разрешимо в L, и называют *лупой*, если также существует единица e (нуль, “0”, в аддитивной терминологии) [1; 5]; группа — это ассоциативная лупа. К понятию квазиполя приходят, ослабляя также двустороннюю дистрибутивность до односторонней [17; 18]. Ясно, что левая дистрибутивность $x(y + z) = xy + xz \ \ (x, y, z \in S)$ дает (при $y = z = 0$) условие $x0 = 0$.

О п р е д е л е н и е 1. Конечное множество Q с бинарными операциями сложения $+$ и умножения $\cdot$ называют *левым квазиполем*, если выполняются следующие условия: 1) $(Q, +)$ — абелева группа, 2) $Q^* := (Q \setminus \{0\}, \cdot)$ — лупа, 3) выполнен левый дистрибутивный закон, 4) $0x = 0$ $(x \in Q)$.

Конечное *правое квазиполе* определяют аналогично с соответствующими изменениями свойств 3) и 4) [18]. Далее говорим “квазиполе” вместо “правое квазиполе”.

З а м е ч а н и е 1. Д. Хьюз и Ф. Пайпер [17] называют $(Q, +, \cdot)$ с произвольным Q и условиями 1)–4) *слабым квазиполем* и *квазиполем* — при дополнительном условии

уравнение $ax = bx + c$ однозначно разрешимо при любых $a, b, c \in Q$, $a \neq b$.

Согласно [17, теорема 7.3] конечное слабое квазиполе есть квазиполе.

О п р е д е л е н и е 2. Тройку биективных отображений α, β, γ группоида $(S; \circ)$ на $(V; \cdot)$ называют *изотопизмом*, если $\alpha(x \circ y) = \beta(x) \cdot \gamma(y)$ $(x, y \in S)$. *Изотопизмом квазиполей* Q и W (*автотопизмом* при $Q = W$) называют тройку изоморфизмов аддитивной группы $(Q, +)$ на $(W, +)$, если их ограничения на квазигруппе Q^* — ее изотопизмы на W^*.

Построение квазиполей тесно связано с построениями проективных плоскостей трансляций. Согласно [2; 5, § 20.1] проективная плоскость — это множество точек с определенными подмножествами, называемыми прямыми, и следующими свойствами: 1) две различные точки лежат на одной и только одной прямой; 2) две различные прямые пересекаются в единственной точке и 3) существуют четыре точки, никакие три из которых не лежат на одной прямой.

Биективное отображение точек и прямых одной проективной плоскости соответственно на точки и прямые другой называют *изоморфизмом плоскостей,* если оно сохраняет инцидентность. *Порядком конечной плоскости* называют число n такое, что число точек какой-либо (равносильно [5, теорема 20.1.1], любой) ее прямой равно $n+1$.

Напомним, что *расщепление группы* — это набор ее подгрупп (компоненты расщепления) с тривиальными попарными пересечениями, дающих в теоретико-множественном объединении всю группу. Абелевой группе G с расщеплением μ сопоставляют аффинную плоскость, точки которой есть элементы группы G, прямые — смежные классы группы G по подгруппам из μ, инцидентность теоретико-множественная. Проективную плоскость получают из аффинной, считая по определению, что смежные классы по одной и той же подгруппе пересекаются (как прямые аффинной плоскости) в одной и той же *особой точке*; множество всех особых точек считают *особой прямой.*

Расщепление μ аддитивной группы $2n$-мерного пространства V над полем F называют *спредом* (*spread*) в V, если $V = M \oplus N$ для любых различных $M, N \in \mu$. В этом случае согласно Дж. Андрэ [19] компоненты являются n-мерными подпространствами; мы получаем плоскость трансляций $\mu(V)$, считая ее точками векторы из V, прямыми — все смежные классы по компонентам из μ, а инцидентностью — отношение включения. Обратно, всякая плоскость трансляций изоморфна подходящей плоскости $\mu(V)$.

Для построения проективной плоскости трансляций π ранга n над полем F выбирают n-мерное линейное пространство W над F (*координатизирующее множество*), внешнюю прямую сумму $V = W \oplus W = \{(x, y) \mid x, y \in W\}$ двух его копий и спред μ в V, содержащий $V(0) := (W, 0)$ и $V(\infty) := (0, W)$. Тогда оставшиеся компоненты из μ имеют вид $V(\sigma) = \{(v, v^\sigma) \mid v \in W\}$ для подходящих $\sigma \in GL(W)$.

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) $R \setminus \{O\}$ 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

$$x \circ y := x \cdot \theta(y) \quad (x = (x_1, x_2, \dots, x_n),\ y = (y_1, y_2, \dots, y_n) \in W). \tag{1.1}$$

Согласно М. Каллахеру [20, теорема 6.1] аффинная плоскость является *трансляционной*, если и только если она координатизируется квазиполем. Соответствующая проективная плоскость трансляций *дезаргова* тогда и только тогда, когда координатизирующее квазиполе есть поле. Когда квазиполе является полуполем, плоскость π называют *полуполевой.* Известно, что это равносильно замкнутости регулярного множества R по сложению.

Предложение 1 (А. Альберт, [21]). *Две полуполевые плоскости изоморфны тогда и только тогда, когда координатизирующие их полуполя изотопны.*

Нам потребуются правое и левое ядра N_r и N_l квазиполя Q, в частности

$$N_r(Q) = \{a \in Q \mid x \circ (y \circ a) = (x \circ y) \circ a,\ (x + y) \circ a = x \circ a + y \circ a \ \ (x, y \in Q)\}.$$

Для любого элемента $x \in Q$ квазиполя $Q = (Q; +, \cdot)$ полагаем

$$0x := 0 = x0, \quad kx := \underbrace{x + x + \ldots + x}_{k \text{ раз}} = xk, \quad (-k)x := -(kx) = k(-x) \quad (k \in \mathbb{Z},\ k > 0).$$

Ассоциативность сложения и левая дистрибутивность дают

$$(x \cdot me) \cdot (ke) = k((x \cdot me) \cdot e) = (km)x = x \cdot (me \cdot ke) \quad (k, m \in \mathbb{Z}).$$

Существование простого подполя в конечном квазиполе устанавливает (см. [16, лемма 1]) следующее предложение.

Предложение 2. *Пусть Q — левое квазиполе с единицей e. Тогда $\pi:\ k\to ke\ \ (k\in\mathbb{Z})$ есть гомоморфизм кольца $\mathbb{Z}$ целых чисел в квазиполе Q, причем Q есть правый $\pi(\mathbb{Z})$-модуль и либо $\pi(\mathbb{Z})\simeq\mathbb{Z}$, либо $\pi(\mathbb{Z})\simeq\mathbb{Z}_p$ для некоторого простого числа p. Число 0 или p здесь соответственно называют характеристикой квазиполя Q.*

Из предложения 2 вытекает

Следствие. *Порядок $|Q|$ всякого конечного квазиполя Q является примарным, т. е. равен степени простого числа.*

Собственное квазиполе порядка p^2 построил Л. Диксон [3] при любом простом $p>2$. Квазиполе порядка 4 или 8 всегда есть поле [22]. Известно также

Предложение 3 [11, теорема 6.1 и следствие 8.2.2]. *Собственное полуполе порядка p^n (p — простое число) существует тогда и только тогда, когда $n\geq 3$ и $p^n\geq 16$.*

2. Порядки элементов и полуполе Кнута — Руа

Произведение с m сомножителями (мультипликативного) группоида называем m-й степенью элемента v (независимо от расстановки скобок), если все сомножители равны v.

О п р е д е л е н и е 3. Порядком $|v|$ элемента v лупы называем наименьшее натуральное число m такое, что существует m-я степень v, равная e; порядок бесконечен, если такое m не существует. Множество порядков всех элементов лупы назовем ее *спектром.*

По аналогии со спектром, введенным в [14], определяем правый порядок $|v|_r$ элемента v лупы по наименьшей правоупорядоченной степени $v^{m)}$, равной e, и *правый спектр* лупы; аналогично вводим левый порядок $|v|_l$ и *левый спектр* лупы. Напомним, что согласно [10]

$$v^{1)}:=v,\ v^{i+1)}=v^{i)}\circ v;\quad v^{(1}=v,\ v^{(i+1}=v\circ v^{(i}\quad (i\geq 1).$$

Конечное полуполе S и лупу S^* называют *правоциклическими* или *правопримитивными*, если все элементы лупы S^* есть правоупорядоченные степени фиксированного элемента.

В 1991 г. Г. Венэ [10] высказал *гипотезу о правоцикличности любого конечного полуполя.* Коммутативное полуполе $\Re$ порядка 32, опровергающее гипотезу Венэ, указал в 2004 г. И. Руа [13], основываясь на координатизирующем полуполе плоскости, построенной Д. Кнутом [11]. Его назовем *полуполем Кнута — Руа.* В этом разделе доказана следующая теорема.

Теорема 1. *В полуполе Кнута — Руа $\Re$ порядка 32 с тождеством $x^{(22}=x$ лупа $\Re^*$ однопорождена и, более того, порождается любым своим неединичным элементом. Ее правый и левый спектры равны $\{1,21\}$, а спектр — $\{1,5,6,7,8,10\}$.*

Д о к а з а т е л ь с т в о. Д. Кнут [11] построил проективные плоскости $\pi(i)$ $(1\leq i\leq 5)$ порядка 32 и показал, что они исчерпывают, с точностью до изоморфизмов, все недезарговы проективные полуполевые плоскости порядка 32. Каждая такая плоскость координатизируется 5-мерным пространством W над $\mathbb{Z}_2$. Оно снабжается структурой полуполя $(W,+,\circ)$ порядка 32 с помощью регулярного множества $\theta(W)$, где аддитивное отображение $\theta:\ W\to M(5,\mathbb{Z}_2)$ (кольцо 5×5-матриц над $\mathbb{Z}_2$) определяет умножение по формуле (1.1). И. Руа [13] использует полуполе порядка 32, соответствующее плоскости $\pi(3)$. Регулярное множество Д. Кнута здесь представляется θ-образом $\theta(W)$, где

$$\theta(x,y,z,w,s)=\begin{pmatrix} x & y & z & w & s\\ s & x+s & y & z & w\\ z & z+w & x+s & y+w+s & z+s\\ w+s & z+w+s & s & x+z+w & y+w\\ y+w+s & y+w & z+w+s & z+s & x+z+s\end{pmatrix}.$$

Тогда умножение $\circ$ полуполя $\Re = (W, +, \circ)$ записывается в виде

$$(u,v,k,l,m)\circ(x,y,z,w,s) = \big(ux+vs+kz+lw+ls+my+mw+ms,$$

$$uy+vx+vs+kz+kw+lz+lw+ls+my+mw,\ uz+vy+kx+ks+ls+mz+mw+ms,$$

$$uw+vz+ky+kw+ks+lx+lz+lw+mz+ms,$$

$$us+vw+kz+ks+ly+lw+mx+mz+ms\big).$$

В частности, $\Re$ — коммутативное полуполе, так что в нем $v^{(i} = v^{i)}$ для всех $i \geq 0$. Далее полезна следующая, доказываемая индукцией, лемма.

Лемма 1. *Пусть α есть m-я степень элемента v коммутативной лупы. Если v^2 входит в α как подпроизведение не более одного раза, то $\alpha = v^{(m}$.*

В коммутативной лупе правый и левый обратные к ее элементу совпадают, а для элемента порядка 3 равны его квадрату. Квадраты элементов лупы всегда расположены на главной диагонали ее таблицы Кэли.

Теперь легко проверить, что лупа $\Re^*$ не имеет элементов порядка 3. Таблица Кэли лупы $\Re^*$ симметрична относительно главной диагонали (табл. 1). Представим ее блоками, разбив столбцы на 4 группы. (Умножение на единицу $e = (1,0,0,0,0)$ в таблице опускаем.)

Несложно доказывается, что для любой конечной лупы L выполняются неравенства

$$|v| \leq |v|_l \leq |L|, \quad |v| \leq |v|_r \leq |L| \qquad (v \in L).$$

Таблица Кэли показывает, что $x^{21)} = e$ — тождество лупы $\Re^*$, как и в [13]. По лемме 1 $x^{(21} = e$ — также тождество. Более того, $|v|_l = |v|_r = 21$ для каждого элемента $v \neq e$ лупы $\Re^*$. Следовательно, ее правый и левый спектры совпадают и равны $\{1, 21\}$.

В лупе $\Re^*$ при любом $v \neq e$ элементы $v^2 \cdot v^2$ и $v^{(4}$ неединичны и различны, так что $|v| > 4$. Отсюда вытекает также максимальность подполя $\mathbb{Z}_2 e$ в полуполе $\Re$.

Т а б л и ц а 1

Таблица Кэли лупы $\Re^*$ полуполя Кнута — Руа

	00001	00010	00011	00100	00101	00110	00111	01000
00001	10111	11100	01011	00111	10000	11011	01100	11000
00010	11100	11011	00111	01010	10110	10001	01101	00001
00011	01011	00111	01100	01101	00110	01010	00001	11001
00100	00111	01010	01101	11001	11110	10011	10100	00010
00101	10000	10110	00110	11110	01110	01000	11000	11010
00110	11011	10001	01010	10011	01000	00010	11001	00011
00111	01100	01101	00001	10100	11000	11001	10101	11011
01000	11000	00001	11001	00010	11010	00011	11011	00100
01001	01111	11101	10010	00101	01010	11000	10111	11100
01010	00100	11010	11110	01000	01100	10010	10110	00101
01011	10011	00110	10101	01111	11100	01001	11010	11101
01100	11111	01011	10100	11011	00100	10000	01111	00110
01101	01000	10111	11111	11100	10100	01011	00011	11110
01110	00011	10000	10011	10001	10010	00001	00010	00111
01111	10100	01100	11000	10110	00010	11010	01110	11111
10001	10110	11110	01000	00011	10101	11101	01011	10000
10010	11101	11001	00100	01110	10011	10111	01010	01001
10011	01010	00101	01111	01001	00011	01100	00110	10001
10100	00110	01000	01110	11101	11011	10101	10011	01010
10101	10001	10100	00101	11010	01011	01110	11111	10010
10110	11010	10011	01001	10111	01101	00100	11110	01011
10111	01101	01111	00010	10000	11101	11111	10010	10011
11000	11001	00011	11010	00110	11111	00101	11100	01100
11001	01110	11111	10001	00001	01111	11110	10000	10100
11010	00101	11000	11101	01100	01001	10100	10001	01101
11011	10010	00100	10110	01011	11001	01111	11101	10101
11100	11110	01001	10111	11111	00001	10110	01000	01110
11101	01001	10101	11100	11000	10001	01101	00100	10110
11110	00010	10010	10000	10101	10111	00111	00101	01111
11111	10101	01110	11011	10010	00111	11100	01001	10111

	01001	01010	01011	01100	01101	01110	01111
00001	01111	00100	10011	11111	01000	00011	10100
00010	11101	11010	00110	01011	10111	10000	01100
00011	10010	11110	10101	10100	11111	10011	11000
00100	00101	01000	01111	11011	11100	10001	10110
00101	01010	01100	11100	00100	10100	10010	00010
00110	11000	10010	01001	10000	01011	00001	11010
00111	10111	10110	11010	01111	00011	00010	01110
01000	11100	00101	11101	00110	11110	00111	11111
01001	10011	00001	01110	11001	10110	00100	01011
01010	00001	11111	11011	01101	01001	10111	10011
01011	01110	11011	01000	10010	00001	10100	00111
01100	11001	01101	10010	11101	00010	10110	01001
01101	10110	01001	00001	00010	01010	10101	11101
01110	00100	10111	10100	10110	10101	00110	00101
01111	01011	10011	00111	01001	11101	00101	10001
10001	00110	01110	11000	10011	00101	01101	11011
10010	10100	10000	01101	00111	11010	11110	00011
10011	11011	10100	11110	11000	10010	11101	10111
10100	01100	00010	00100	10111	10001	11111	11001
10101	00011	00110	10111	01000	11001	11100	01101
10110	10001	11000	00010	11100	00110	01111	10101
10111	11110	11100	10001	00011	01110	01100	00001
11000	10101	01111	10110	01010	10011	01001	10000
11001	11010	01011	00101	10101	11011	01010	00100
11010	01000	10101	10000	00001	00100	11001	11100
11011	00111	10001	00011	11110	01100	11010	01000
11100	10000	00111	11001	10001	01111	11000	00110
11101	11111	00011	01010	01110	00111	11011	10010
11110	01101	11101	11111	11010	11000	01000	01010
11111	00010	11001	01100	00101	10000	01011	11110

	10001	10010	10011	10100	10101	10110	10111	11000
00001	10110	11101	01010	00110	10001	11010	01101	11001
00010	11110	11001	00101	01000	10100	10011	01111	00011
00011	01000	00100	01111	01110	00101	01001	00010	11010
00100	00011	01110	01001	11101	11010	10111	10000	00110
00101	10101	10011	00011	11011	01011	01101	11101	11111
00110	11101	10111	01100	10101	01110	00100	11111	00101
00111	01011	01010	00110	10011	11111	11110	10010	11100
01000	10000	01001	10001	01010	10010	01011	10011	01100
01001	00110	10100	11011	01100	00011	10001	11110	10101
01010	01110	10000	10100	00010	00110	11000	11100	01111
01011	11000	01101	11110	00100	10111	00010	10001	10110
01100	10011	00111	11000	10111	01000	11100	00011	01010
01101	00101	11010	10010	10001	11001	00110	01110	10011
01110	01101	11110	11101	11111	11100	01111	01100	01001
01111	11011	00011	10111	11001	01101	10101	00001	10000
10001	00111	01111	11001	10010	00100	01100	11010	00001
10010	01111	01011	10110	11100	00001	00101	11000	11011
10011	11001	10110	11100	11010	10000	11111	10101	00010
10100	10010	11100	11010	01001	01111	00001	00111	11110
10101	00100	00001	10000	01111	11110	11011	01010	00111
10110	01100	00101	11111	00001	11011	10010	01000	11101
10111	11010	11000	10101	00111	01010	01000	00101	00100
11000	00001	11011	00010	11110	00111	11101	00100	10100
11001	10111	00110	01000	11000	10110	00111	01001	01101
11010	11111	00010	00111	10110	10011	01110	01011	10111
11011	01001	11111	01101	10000	00010	10100	00110	01110
11100	00010	10101	01011	00011	11101	01010	10100	10010
11101	10100	01000	00001	00101	01100	10000	11001	01011
11110	11100	01100	01110	01011	01001	11001	11011	10001
11111	01010	10001	00100	01101	11000	00011	10110	01000

	11001	11010	11011	11100	11101	11110	11111
00001	01110	00101	10010	11110	01001	00010	10101
00010	11111	11000	00100	01001	10101	10010	01110
00011	10001	11101	10110	10111	11100	10000	11011
00100	00001	01100	01011	11111	11000	10101	10010
00101	01111	01001	11001	00001	10001	10111	00111
00110	11110	10100	01111	10110	01101	00111	11100
00111	10000	10001	11101	01000	00100	00101	01001
01000	10100	01101	10101	01110	10110	01111	10111
01001	11010	01000	00111	10000	11111	01101	00010
01010	01011	10101	10001	00111	00011	11101	11001
01011	00101	10000	00011	11001	01010	11111	01100
01100	10101	00001	11110	10001	01110	11010	00101
01101	11011	00100	01100	01111	00111	11000	10000
01110	01010	11001	11010	11000	11011	01000	01011
01111	00100	11100	01000	00110	10010	01010	11110
10001	10111	11111	01001	00010	10100	11100	01010
10010	00110	00010	11111	10101	01000	01100	10001
10011	01000	00111	01101	01011	00001	01110	00101
10100	11000	10110	10000	00011	00101	01011	01101
10101	10110	10011	00010	11101	01100	01001	11000
10110	00111	01110	10100	01010	10000	11001	00011
10111	01001	01011	00110	10100	11001	11011	10110
11000	01101	10111	01110	10010	01011	10001	01000
11001	00011	10010	11100	01100	00010	10011	11101
11010	10010	01111	01010	11011	11110	00011	00110
11011	11100	01010	11000	00101	10111	00001	10011
11100	01100	11011	00101	01101	10011	00100	11010
11101	00010	11110	10111	10011	11010	00110	01111
11110	10011	00011	00001	00100	00110	10110	10100
11111	11101	00110	10011	11010	01111	10100	00001

Т а б л и ц а 2

Порядки элементов лупы $\Re^*$

y	(1,0,0,0,0)	(0,0,0,0,1)	(0,0,0,1,0)	(0,0,0,1,1)	(0,0,1,0,0)	(0,0,1,0,1)	(0,0,1,1,0)	(0,0,1,1,1)
|y|	1	5	7	10	6	7	8	10

y	(0,1,0,0,0)	(0,1,0,0,1)	(0,1,0,1,0)	(0,1,0,1,1)	(0,1,1,0,0)	(0,1,1,0,1)	(0,1,1,1,0)	(0,1,1,1,1)
|y|	10	5	8	7	6	5	5	6

y	(1,0,0,0,1)	(1,0,0,1,0)	(1,0,0,1,1)	(1,0,1,0,0)	(1,0,1,0,1)	(1,0,1,1,0)	(1,0,1,1,1)	(1,1,0,0,0)
|y|	7	6	8	7	6	10	8	8

y	(1,1,0,0,1)	(1,1,0,1,0)	(1,1,0,1,1)	(1,1,1,0,0)	(1,1,1,0,1)	(1,1,1,1,0)	(1,1,1,1,1)
|y|	7	10	5	7	7	7	7

Найдем спектр лупы $\Re^*$. Элементами порядка 5 являются элементы m_i, $1 \leq i \leq 5$:

$$m_1 = (0,0,0,0,1),\ m_2 = (0,1,0,0,1),\ m_3 = (0,1,1,0,1),\ m_4 = (0,1,1,1,0),\ m_5 = (1,1,0,1,1).$$

Действительно, обратный к элементу m_i совпадает с $m_i^2 \cdot m_i^2$. Далее, степени ≤ 5 элементов

$$n_1 = (0,0,1,0,0),\ n_2(0,1,1,0,0),\ n_3 = (0,1,1,1,1),\ n_4 = (1,0,0,1,0),\ n_5 = (1,0,1,0,1)$$

неединичны и, кроме того, $n_j^2 \cdot n_j^{4)} = e$. Отсюда $|n_j| = 6\ \ (1 \leq j \leq 5)$.

Аналогично неединичные степени ≤ 6 имеют все элементы:

$$k_1 = (0,0,0,1,0),\ k_2 = (0,0,1,0,1),\ k_3 = (0,1,0,1,1),\ k_4 = (1,0,0,0,1),\ k_5 = (1,0,1,0,0),$$

$$k_6 = (1,1,0,0,1),\ \ k_7 = (1,1,1,0,0),\ k_8 = (1,1,1,0,1),\ k_9 = (1,1,1,1,0),\ k_{10} = (1,1,1,1,1),$$

причем хотя бы одно из произведений $k_r^2 \cdot (k_r^2 \cdot k_r^2)$ или $k_r^{3)} \cdot k_r^{3)}$ совпадает с обратным к элементу k_r $(1 \leq r \leq 10)$. Таким образом, порядки этих элементов равны 7.

Аналогичной процедурой находим порядки оставшихся элементов лупы $\Re^*$.

Сводная табл. 2 показывает, что спектр лупы $\Re^*$ равен $\{1,5,6,7,8,10\}$.

Докажем, что лупу $\Re^*$ порождает ее элемент $a_1 = (0,0,0,0,1)$. Вначале находим

$$a_1^2 = (1,0,1,1,1) := a_2, \quad a_1^{3)} = a_1 \cdot a_1^2 = (0,1,1,0,1) := a_3.$$

Правоупорядоченные j-е степени элемента a_1, $4 \leq j \leq 21$, дают соответственно элементы

$$a_4 = (1,0,1,1,1),\ a_5 = (1,1,0,0,0),\ a_6 = (1,1,0,0,1),\ a_7 = (0,1,1,1,0),$$

$$a_8 = (0,0,0,1,1),\ a_9 = (0,1,0,1,1),\ a_{10} = (1,0,0,1,1),\ a_{11} = (0,1,0,1,0),$$

$$a_{12} = (0,0,1,0,0),\ a_{13} = (0,0,1,1,1),\ a_{14} = (0,1,1,0,0),\ a_{15} = (1,1,1,1,1),$$

$$a_{16} = (1,0,1,0,1),\ a_{17} = (1,0,0,0,1),\ a_{18} = (1,0,1,1,0),\ a_{19} = (1,1,0,1,0),$$

$$a_{20} = (0,0,1,0,1),\ a_{21} = (1,0,0,0,0).$$

Используя уже найденные элементы, получаем оставшиеся десять элементов лупы:

$$a_{22} = a_2 \cdot a_4 = (1,1,1,1,0),\ a_{23} = a_{22} \cdot a_1 = (0,0,0,1,0),\ a_{24} = a_{22} \cdot a_2 = (1,1,0,1,1),$$

$$a_{25} = a_{22} \cdot a_4 = (0,1,1,1,1),\ a_{26} = a_{23} \cdot a_1 = (1,1,1,0,0),\ a_{27} = a_{24} \cdot a_2 = (0,0,1,1,0),$$

$$a_{28} = a_6 \cdot a_2 = (0,1,0,0,1),\ a_{29} = a_3 \cdot a_{10} = (1,0,0,1,0),\ a_{30} = a_3 \cdot a_{20} = (1,0,1,0,0),$$
$$a_{31} = a_2 \cdot a_{20} = (1,1,1,0,1).$$

Поэтому все элементы лупы являются различными степенями элемента a_1, так что однопорожденность лупы $\Re^*$ доказана. Более сильное утверждение устанавливает

Лемма 2. *Лупа $\Re^*$ порождается любым ее неединичным элементом.*

Доказательство. Лупу $\Re^*$ порождает элемент $b_1 := (0,0,0,0,1)$ согласно доказанному выше, а также любой из элементов $b_2 = (1,1,1,1,1)$, $b_3 = (0,0,1,0,0)$ и $b_4 = (0,0,0,1,0)$, поскольку $b_2^2 = b_3^3 = b_1$ и $b_4^{(19} = b_2$. Далее удается аналогично выражать найденные элементы b_i правоупорядоченными степенями оставшихся неединичных элементов:

$$b_5^2 = b_6^{(12} = b_4, \quad b_5 := (0,0,1,1,0), \quad b_6 := (0,0,0,1,1);$$

$$b_7^{(5} = b_8^2 = b_6, \quad b_7 := (0,0,1,0,1), \quad b_8 := (1,1,0,0,1)$$

и т. д. Таким образом, лупа $\Re^*$ полуполя Кнута — Руа порождается всяким своим неединичным элементом. Доказательство леммы и вместе с тем теоремы 1 завершено. □

3. Полуполя и квазиполя порядка 16

Алгоритм построения полуполей и квазиполей порядка 16 разрабатывал в 1960 г. Е. Клейнфилд [24], рассматривая таблицу Кэли лупы как латинский квадрат. Когда квазиполе имеет ядро порядка 4, ключевой в ней (помимо умножений на элементы ядра) является 4-я строка; для ее выбора и построения латинского 4×15-прямоугольника существуют 1264 возможности [24, с. 333]. Изоморфными преобразованиями это число удается уменьшить до 76, построив два класса изотопных попарно неизоморфных собственных квазиполей: один класс из 50 квазиполей T_i, $1 \le i \le 50$, включая полуполя T_{24}, T_{25}, T_{35}, T_{45} и T_{50}; второй изотопный класс составляют 25 квазиполей, не являющиеся полуполями.

Громоздкость вычислений, как отметил Е. Клейнфилд, не позволила перечислить также квазиполя порядка 16 с ядром порядка 2; они классифицированы для случая полуполей.

Предложение 4 (Е. Клейнфилд, [24]). *Собственные полуполя порядка* 16 *образуют два класса изотопных попарно неизоморфных полуполей. Один из* 18 *полуполей V_i*, $1 \le i \le 18$, *с ядром порядка* 2, *а другой из* 5 *полуполей T_{24}, T_{25}, T_{35}, T_{45} и T_{50} с ядром порядка* 4.

Отсюда и из предложения 1 следует, что число неизоморфных недезарговых полуполевых плоскостей порядка 16 равно двум. Применяя компьютерные вычисления, Д. Кнут [11; 12] подтвердил перечисления из [24] (с оценкой ≤ 6 порядков групп автоморфизмов полуполей) и координатизировал обе плоскости полуполями с явными формулами умножения:

$$(u,v) \circ (x,y) = (ux + \omega v^2 y, vx + u^2 y) \qquad (u,v,x,y \in GF(4) = \{0,1,\omega,\omega^2 = \omega+1\}),$$

$$(u,v) \circ (x,y) = (ux + v^2 y, vx + u^2 y + v^2 y^2).$$

Ясно, что кольцо (или квазиполе) $R = (R,+,\cdot)$ антиизоморфно его *противоположному* $R^{op} := (R,+,\circ)$, где $a \circ b = b \cdot a$ $(a,b \in R)$, по определению. Сокращая список Клейнфилда, мы классифицируем полуполя порядка 16, с точностью (достаточной для решения вопросов **(A)**–**(B)**) до изоморфизмов и антиизоморфизмов, с явными формулами умножения.

Теорема 2. *Всякое собственное полуполе порядка 16 либо антиизоморфно или изоморфно одному из семи полуполей $V_1, V_3, V_4, V_8, V_{11}, V_{15}, T_{25}$, не изоморфных противоположному полуполю, либо изоморфно одному из девяти полуполей V_2, V_{10}, V_{12}, V_{13}, V_{17}, V_{18}, T_{24}, T_{35}, T_{45}. Формулы умножения в полуполях определяет табл.* 3.

Таблица 3

Формулы умножения в полуполях порядка 16

Полуполе	Произведение $(a,b,c,d)\circ(x,y,z,w)$
$V_1 \simeq V_6^{op}$	$(ax+bw+cz+dy+dz,\ ay+bx+cy+cz+dy+dw,$ $az+by+bw+cx+cw+dy,\ aw+bz+cy+cw+dx+dy+dw)$
V_2	$(ax+bw+cz+dy+dz+dw, ay+bx+bw+cw+dy+dz,$ $az+by+bw+cx+cy+cz+dy+dw, aw+bz+cy+cw+dx+dy+dz+dw)$
$V_3 \simeq V_7^{op}$	$(ax+bw+cy+cz+dz, ay+bx+cz+dy+dw,$ $az+by+cx+cy+cw+dw, aw+bz+bw+cy+cw+dx+dy+dz+dw)$
$V_4 \simeq V_5^{op}$	$(ax+bw+cy+cw+dz, ay+bx+bw+cz+cw+dw,$ $az+by+bw+cx+cy+cz+dy, aw+bz+bw+cy+dx+dy+dz+dw)$
$V_8 \simeq V_9^{op}$	$(ax+bw+cz+dy, ay+bx+bw+cy+cw+dz,$ $az+by+bw+cx+cz+cw+dw, aw+bz+bw+cy+dx+dz)$
V_{10}	$(ax+bw+cy+cz+cw+dy+dw, ay+bx+cz+cw+dy+dz,$ $az+by+bw+cx+cz+cw+dy, aw+bz+cy+cw+dx+dz+dw)$
$V_{11} \simeq V_{14}^{op}$	$(ax+bw+cz+dy+dw, ay+bx+bw+cz+cw+dz,$ $az+by+cx+cz+dw, aw+bz+cy+cz+cw+dx+dy+dz)$
V_{12}	$(ax+bw+cz+dy+dw, ay+bx+bw+cy+cz+cw+dz,$ $az+by+bw+cx+cw+dz+dw, aw+bz+bw+cy+dx+dy+dz+dw)$
V_{13}	$(ax+bw+cz+cw+dy+dw, ay+bx+bw+cy+cw+dz,$ $az+by+cx+cy+cz+cw+dw, aw+bz+cy+dy+dz)$
$V_{15} \simeq V_{16}^{op}$	$(ax+bw+cz+cw+dy+dw, ay+bx+cy+cz+cw+dy+dz,$ $az+by+bw+cx+cz+cw+dy, aw+bz+cy+cz+dx+dz+dw)$
V_{17}	$(ax+bw+cz+cw+dy+dw, ay+bx+bw+cy+cw+dz,$ $az+by+bw+cx+cz+dz+dw, aw+bz+bw+cy+dx+dy+dz+dw)$
V_{18}	$(ax+bw+cz+dy+dz, ay+bx+cy+cw+dy+dz+dw,$ $az+by+bw+cx+cy+cz+cw+dy, aw+bz+cy+dx+dy+dz)$
T_{24}	$(ax+by+bz+cy+cw+dw, ay+bx+by+bz+cy+cz+cw+dy+dz,$ $az+by+bz+bw+cx+cw+dy, aw+bz+bw+cy+cz+dx+dw)$
$T_{25} \simeq T_{50}^{op}$	$(ax+by+cz+cw+dw, ay+bx+by+cw+dz,$ $az+bw+cx+cy+cz+cw+dy+dw, aw+bz+bw+cy+cw+dx+dz)$
T_{35}	$(ax+bz+cy+cw+dw, ay+bx+by+cw+dy+dz,$ $az+bw+cx+cy+cw+dy, aw+by+bz+bw+cz+dw)$
T_{45}	$(ax+by+bz+bw+cy+cw+dw, ay+bx+by+bz+bw+cz+cw+dy+dz,$ $az+bz+bw+cx+cy+dy, aw+bz+cy+cz+cw+dw)$

Доказательство. Е. Клейнфилд [24] характеризует специальной порождающей последовательностью таблицу Кэли лупы W^* каждого из 76 квазиполей $W = T_j$ с ядром порядка 4 и каждого из 18 полуполей V_i с ядром порядка 2. Построив таблицы Кэли 23 полуполей Клейнфилда, находим (используя общую формулу (1.1)) аддитивные отображения $\theta : W \to M(4,\mathbb{Z}_2)$ такие, что $R = \theta(W)$ – регулярное множество проективной плоскости ранга 4 над полем $\mathbb{Z}_2$. Полуполя Клейнфилда удается восстановить, вместе с формулами умножения, как координатизирующие полуполя таких плоскостей. (Тогда последовательности Клейнфилда легко восстанавливаются.) Ранее авторами [15] формулы умножения были выписаны (помимо двух полуполей Кнута), вместе с таблицами Кэли, для полуполей V_3, V_7, T_{25} и T_{50}.

Таблица 4

Строение полуполей порядка 16

Полуполе	$\|N_l\|$	Число подполей порядка 4	Спектр	Правый спектр	Левый спектр
V_1	2	0	$\{1,4,5\}$	$\{1,5,6,15\}$	$\{1,6,15\}$
V_2	2	1	$\{1,3,4,5,6\}$	$\{1,3,6,15\}$	$\{1,3,6,15\}$
V_3	2	0	$\{1,4,5,6\}$	$\{1,5,6,15\}$	$\{1,5,6,15\}$
V_4	2	1	$\{1,3,4,5,6\}$	$\{1,3,6,15\}$	$\{1,3,5,6,15\}$
V_8	2	2	$\{1,3,4,5,6\}$	$\{1,3,6,15\}$	$\{1,3,5,6,15\}$
V_{10}	2	1	$\{1,3,5,6\}$	$\{1,3,6,15\}$	$\{1,3,6,15\}$
V_{11}	2	1	$\{1,3,4,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,6,15\}$
V_{12}	2	0	$\{1,4,5,6\}$	$\{1,5,6,15\}$	$\{1,5,6,15\}$
V_{13}	2	4	$\{1,3,5\}$	$\{1,3,15\}$	$\{1,3,15\}$
V_{15}	2	2	$\{1,3,4,5\}$	$\{1,3,6,15\}$	$\{1,3,6,15\}$
V_{17}	2	1	$\{1,3,4,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,5,6,15\}$
V_{18}	2	2	$\{1,3,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,5,6,15\}$
T_{24}	4	2	$\{1,3,4,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,5,6,15\}$
T_{25}	4	2	$\{1,3,4,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,6,15\}$
T_{35}	4	1	$\{1,3,4,5,6\}$	$\{1,3,6,15\}$	$\{1,3,6,15\}$
T_{45}	4	3	$\{1,3,5\}$	$\{1,3,5,15\}$	$\{1,3,5,15\}$

В силу предложения 4 каждое собственное полуполе порядка 16 изоморфно либо одному из 16 полуполей табл. 3, либо противоположному к одному из семи указанных в таблице полуполей полуполю. Формула умножения в произвольном полуполе R позволяет сразу же записать формулу умножения в полуполе R^{op}, причем $(R^{op})^{op} \simeq R$. Все семь случаев, когда $R^{op} \not\simeq R$, отражены в табл. 3 явно. Это завершает доказательство теоремы. $\square$

Теорема 2 анонсирована (без формул) в [15, теорема 2.3]; подробнее см. [27, теорема 2.1.1].

Очевидно, левый и правый спектры любого полуполя совпадают соответственно с правым и левым спектрами противоположного полуполя. Таблицы Кэли и формулы умножения позволяют выявить строение полуполей порядка 16 и доказать, что *лупа ненулевых элементов всякого полуполя порядка* 16 *однопорождена*. Таблица 4 резюмирует решение вопросов **(A)**–**(B)** для полуполей порядка 16, в частности, выявляя их право- и левоцикличность. Она анонсировалась (без правого и левого спектров) ранее в [15, табл. 4].

Число всех недезарговых проективных плоскостей трансляций порядка 16 равно 7, как показали У. Демпвольф и А. Рейфарт [25; 26]. По найденным там же регулярным множествам выбираем представители Q_j, $1 \le j \le 5$, изотопных классов квазиполей, не содержащих полуполя. Их строение, выявленное в [16, теорема 2; 15, теоремы 3.1–3.3], резюмирует следующая теорема.

Теорема 3. *Каждое из квазиполей Q_j при $j = 1,2,3$ есть теоретико-множественное объединение 7 максимальных подполей порядка 4, спектр лупы Q_j^* совпадает с $\{1,3\}$ и любой ее элемент лежит в циклической подгруппе порядка 3. В квазиполях Q_j при $j = 4,5$ любой элемент, не лежащий в подполе порядка 4, порождает лупу Q_j^* и имеет порядок 5, причем в Q_4 ядро есть единственное максимальное подполе порядка 4, а Q_5 имеет 3 максимальных подполя порядка 4 и $|N_l(Q_5)| = 2$.*

4. Полуполя и квазиполя порядка 32

Д. Кнут [11] построил проективные плоскости $\pi(i)$ $(1 \leq i \leq 5)$ порядка 32 и показал, что они исчерпывают, с точностью до изоморфизмов, все недезарговы проективные полуполевые плоскости порядка 32. Тем самым собственные полуполя порядка 32 были описаны, с точностью до изотопизмов, как соответствующие координатизирующие полуполя P_j $(1 \leq j \leq 5)$. Полуполя порядка 32 классифицировал также Р. Волкер [23].

Очевидно, порядок конечного полуполя равен степеням порядков правого и левого ядра. Поэтому ядра собственных полуполей порядка $32 = 2^5$ совпадают с простым подполем. В полуполе Кнута — Руа в силу теоремы 1 простое подполе — единственное его подполе.

Оказывается, такие полуполя могут содержать подполе порядка 4 (см. также [13].) Выберем представители P_i изотопных классов полуполей порядка 32, построенные на основе регулярных множеств из [26] плоскостей $\pi(i)$, выписанных как в [16].

Строение полуполей P_i выявляют следующие две теоремы.

Теорема 4 [16, теорема 5]. *Каждое полуполе P_i, $1 \leq i \leq 4$, имеет единственное подполе — подполе порядка 2. Лупу P_i^* порождает всякий неединичный элемент, а спектр лупы совпадает с $\{1, 4, 5, 6, 7, 8\}$ при $i = 3$, с $\{1, 5, 6, 7, 8, 9\}$ при $i = 4$ и с $\{1, 4, 5, 6, 7\}$ при $i = 1, 2$.*

Теорема 5 [16, теорема 4]. *В полуполе P_5 существует подполе H порядка 4, являющееся единственным максимальным подполем. Каждый элемент из $P_5 \setminus H$ порождает лупу P_5^* и имеет порядок > 3, а спектр лупы совпадает с $\{1, 3, 4, 5, 6, 7, 8\}$.*

Классификацию проективных плоскостей трансляций порядка 32 завершили в 2011 г. У. Демпвольф [26] и Р. Рокенфеллер [28]. С точностью до изоморфизмов, помимо шести полуполевых плоскостей существует точно 3 плоскости трансляций порядка 32, не являющихся полуполевыми. Координатизирующие квазиполя Q_i, $i = 1, 2, 3$, построим на основе регулярных множеств плоскостей из [26]. Вместе с полуполями P_i, $1 \leq i \leq 5$, они исчерпывают все собственные квазиполя порядка 32 с точностью до изотопизмов.

Оказывается, строение квазиполей Q_i, $i = 1, 2, 3$, допускает единообразное описание.

Теорема 6. *В каждом квазиполе Q_i, $i = 1, 2, 3$, простое подполе максимально, лупа Q_i^* является правоциклической, а ее спектр совпадает с $\{1, 4, 5, 6, 7\}$.*

Д о к а з а т е л ь с т в о. Квазиполя Q_1, Q_2 и Q_3 построены на основе регулярных множеств плоскостей трансляций с номерами 7, 8 и 9 из [26] соответственно. С их помощью восстанавливаем умножение (1.1) и таблицу Кэли лупы Q_i^*. Для Q_1 получаем регулярное множество

$$\left\{ O, E, \begin{pmatrix} 0&0&0&0&1\\ 1&1&1&1&0\\ 0&1&0&1&0\\ 0&1&1&1&1\\ 0&1&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&0&1&0\\ 1&0&0&1&1\\ 1&0&0&0&0\\ 1&1&1&0&1\\ 0&0&1&1&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&1&1\\ 1&1&1&0&1\\ 1&0&1&0&0\\ 1&1&0&1&1\\ 1&1&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&0&0\\ 0&0&0&1&1\\ 1&1&1&1&1\\ 0&1&0&0&0\\ 1&1&1&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&0&1\\ 0&1&1&0&1\\ 1&1&0&1&1\\ 1&1&1&1&1\\ 1&0&1&0&1 \end{pmatrix}, \right.$$

$$\begin{pmatrix} 0&0&1&1&0\\ 1&0&1&1&0\\ 0&1&1&1&0\\ 0&1&1&0&1\\ 1&0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&1&1&1\\ 0&0&1&1&0\\ 0&1&1&0&1\\ 0&0&0&1&1\\ 1&0&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0\\ 0&1&0&1&0\\ 0&0&1&0&1\\ 1&1&1&0&0\\ 1&0&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&1\\ 0&0&1&0&1\\ 0&1&1&1&1\\ 1&1&0&1&0\\ 0&1&1&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&1&0\\ 0&1&1&1&0\\ 1&0&1&0&1\\ 0&0&1&1&1\\ 0&1&0&0&0 \end{pmatrix},$$

$$\begin{pmatrix} 0&1&0&1&1\\ 1&0&1&1&1\\ 0&0&1&1&1\\ 1&0&1&1&0\\ 1&1&1&1&1 \end{pmatrix}, \begin{pmatrix} 0&1&1&0&0\\ 1&0&0&0&1\\ 0&1&0&1&1\\ 1&0&1&0&1\\ 0&1&1&0&1 \end{pmatrix}, \begin{pmatrix} 0&1&1&0&1\\ 0&0&1&1&1\\ 1&1&0&0&0\\ 1&0&0&1&1\\ 0&0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&1&1&1&0\\ 1&1&1&0&0\\ 1&1&1&0&1\\ 0&0&1&1&0\\ 0&0&0&1&1 \end{pmatrix}, \begin{pmatrix} 0&1&1&1&1\\ 1&0&1&0&0\\ 1&1&0&0&1\\ 0&1&0&0&1\\ 1&0&0&1&1 \end{pmatrix},$$

$$\begin{pmatrix} 1&0&0&0&1\\ 1&1&1&1&1\\ 0&1&0&0&0\\ 1&0&0&1&0\\ 0&1&1&1&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&1&0\\ 1&1&0&1&1\\ 0&0&0&1&0\\ 0&1&1&1&0\\ 1&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&1&1\\ 1&0&1&0&1\\ 1&0&0&0&1\\ 1&1&0&0&1\\ 1&1&0&0&0 \end{pmatrix}, \begin{pmatrix} 1&0&1&0&0\\ 0&0&0&1&0\\ 0&1&1&0&0\\ 0&0&1&0&1\\ 1&1&0&1&1 \end{pmatrix}, \begin{pmatrix} 1&0&1&0&1\\ 0&1&1&0&0\\ 0&1&0&0&1\\ 1&0&1&0&0\\ 0&0&0&1&0 \end{pmatrix},$$

$$\begin{pmatrix} 1&0&1&1&0\\ 0&0&0&0&1\\ 1&0&0&1&1\\ 1&0&0&0&1\\ 1&1&1&0&0 \end{pmatrix}, \begin{pmatrix} 1&0&1&1&1\\ 1&1&0&0&0\\ 0&0&1&1&0\\ 0&0&0&0&1\\ 0&1&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&1&0&0&0\\ 0&1&0&1&1\\ 1&0&1&1&0\\ 1&0&1&1&1\\ 0&0&1&1&1 \end{pmatrix}, \begin{pmatrix} 1&1&0&0&1\\ 1&0&0&1&0\\ 0&0&0&1&1\\ 1&0&0&0&0\\ 1&0&1&1&1 \end{pmatrix}, \begin{pmatrix} 1&1&0&1&0\\ 1&1&0&0&1\\ 1&1&1&1&0\\ 0&1&0&1&0\\ 1&0&1&1&0 \end{pmatrix},$$

$$\left.\begin{pmatrix} 1&1&0&1&1\\ 0&1&1&1&1\\ 1&1&0&1&0\\ 0&1&1&0&0\\ 1&1&1&1&0 \end{pmatrix}, \begin{pmatrix} 1&1&1&0&0\\ 0&1&0&0&1\\ 0&0&0&0&1\\ 1&1&1&1&0\\ 1&1&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&1&1&0&1\\ 1&0&0&0&0\\ 1&0&0&1&0\\ 1&1&0&0&0\\ 0&1&0&1&1 \end{pmatrix}, \begin{pmatrix} 1&1&1&1&0\\ 0&0&1&0&0\\ 1&0&1&1&1\\ 0&1&0&1&1\\ 0&0&1&0&1 \end{pmatrix}, \begin{pmatrix} 1&1&1&1&1\\ 1&1&0&1&0\\ 1&1&1&0&0\\ 0&0&1&0&0\\ 0&1&1&0&0 \end{pmatrix}\right\}$$

и таблицу Кэли лупы Q_1^* (умножение на единичный элемент (1,0,0,0,0) опускаем).

В квазиполе Q_i, как показывает его таблица Кэли, правоупорядоченные степени элемента $(0,0,0,1,0)$ дают все ненулевые элементы; его правоупорядоченный порядок равен 31. В частности, лупа Q_i^* $(i = 1, 2, 3)$ является однопорожденной и даже правоциклической.

Таблица Кэли показывает также, что все неединичные элементы лупы Q_i^* имеют различные правый и левый обратные элементы и поэтому их порядок больше 3, а квазиполе Q_i не имеет подполей, отличных от простого подполя порядка 2.

Т а б л и ц а 5

Таблица Кэли лупы Q_1^*

	00001	00010	00011	00100	00101	00110	00111	01000
00001	01001	00110	11001	11101	10101	10100	10010	10000
00010	01111	11101	11011	01000	11111	01101	00011	11100
00011	00110	11011	00010	10101	01010	11001	10001	01100
00100	01010	10000	10100	11111	11011	01110	01101	00101
00101	00011	10110	01101	00010	01110	11010	11111	10101
00110	00101	01101	01111	10111	00100	00011	01110	11001
00111	01100	01011	10110	01010	10001	10111	11100	01001
01000	11110	10011	11101	00011	01101	10110	00110	01010
01001	10111	10101	00100	11110	11000	00010	10100	11010
01010	10001	01110	00110	01011	10010	11011	00101	10110
01011	11000	01000	11111	10110	00111	01111	10111	00110
01100	10100	00011	01001	11100	10110	11000	01011	01111
01101	11101	00101	10000	00001	00011	01100	11001	11111
01110	11011	11110	10010	10100	01001	10101	01000	10011
01111	10010	11000	01011	01001	11100	00001	11010	00011
10001	01000	00100	11010	11001	10000	10010	10101	11000
10010	01110	11111	11000	01100	11010	01011	00100	10100
10011	00111	11001	00001	10001	01111	11111	10110	00100
10100	01011	10010	10111	11011	11110	01000	01010	01101
10101	00010	10100	01110	00110	01011	11100	11000	11101
10110	00100	01111	01100	10011	00001	00101	01001	10001
10111	01101	01001	10101	01110	10100	10001	11011	00001
11000	11111	10001	11110	00111	01000	10000	00001	00010
11001	10110	10111	00111	11010	11101	00100	10011	10010
11010	10000	01100	00101	01111	10111	11101	00010	11110
11011	11001	01010	11100	10010	00010	01001	10000	01110
11100	10101	00001	01010	11000	10011	11110	01100	00111
11101	11100	00111	10011	00101	00110	01010	11110	10111
11110	11010	11100	10001	10000	01100	10011	01111	11011
11111	10011	11010	01000	01101	11001	00111	11101	01011

	01001	01010	01011	01100	01101	01110	01111
00001	01110	01000	11111	01101	00100	00011	10011
00010	11010	00111	10110	10101	10011	00110	01001
00011	10100	01111	01001	11000	10111	00101	11010
00100	01111	10101	00111	01011	11000	11101	11001
00101	00001	11101	11000	00110	11100	11110	01010
00110	10101	10010	10001	11110	01011	11011	10000
00111	11011	11010	01110	10011	01111	11000	00011
01000	00101	01110	10111	10001	00111	11100	10100
01001	01011	00110	01000	11100	00011	11111	00111
01010	11111	01001	00001	00100	10100	11010	11101
01011	10001	00001	11110	01001	10000	11001	01110
01100	01010	11011	10000	11010	11111	00001	01101
01101	00100	10011	01111	10111	11011	00010	11110
01110	10000	11100	00110	01111	01100	00111	00100
01111	11110	10100	11001	00010	01000	00100	10111
10001	00111	00010	10100	00001	01001	01101	11100
10010	10011	01101	11101	11001	11110	01000	00110
10011	11101	00101	00010	10100	11010	01011	10101
10100	00110	11111	01100	00111	10101	10011	10110
10101	01000	10111	10011	01010	10001	10000	00101
10110	11100	11000	11010	10010	00110	10101	11111
10111	10010	10000	00101	11111	00010	10110	01100
11000	01100	00100	11100	11101	01010	10010	11011
11001	00010	01100	00011	10000	01110	10001	01000
11010	10110	00011	01010	01000	11001	10100	10010
11011	11000	01011	10101	00101	11101	10111	00001
11100	00011	10001	11011	10110	10010	01111	00010
11101	01101	11001	00100	11011	10110	01100	10001
11110	11001	10110	01101	00011	00001	01001	01011
11111	10111	11110	10010	01110	00101	01010	11000

	10001	10010	10011	10100	10101	10110	10111	11000
00001	01111	10001	11000	11011	00010	11100	01010	00111
00010	10010	01110	11001	00101	10100	10001	00001	10111
00011	11101	11111	00001	11110	10110	01101	01011	10000
00100	01000	00010	10001	01100	01001	10011	00110	10110
00101	00111	10011	01001	10111	01011	01111	01100	10001
00110	11010	01100	01000	01001	11101	00010	00111	00001
00111	10101	11101	10000	10010	11111	11110	01101	00110
01000	11111	11011	10101	00010	01100	00001	11000	01011
01001	10000	01010	01101	11001	01110	11101	10010	01100
01010	01101	10101	01100	00111	11000	10000	11001	11100
01011	00010	00100	10100	11100	11010	01100	10011	11011
01100	10111	11001	00100	01110	00101	10010	11110	11101
01101	11000	01000	11100	10101	00111	01110	10100	11010
01110	00101	10111	11101	01011	10001	00011	11111	01010
01111	01010	00110	00101	10000	10011	11111	10101	01101
10001	11110	00011	01011	01111	10111	01010	11101	11111
10010	00011	11100	01010	10001	00001	00111	10110	01111
10011	01100	01101	10010	01010	00011	11011	11100	01000
10100	11001	10000	00010	11000	11100	00101	10001	01110
10101	10110	00001	11010	00011	11110	11001	11011	01001
10110	01011	11110	11011	11101	01000	10100	10000	11001
10111	00100	01111	00011	00110	01010	01000	11010	11110
11000	01110	01001	00110	10110	11001	10111	01111	10011
11001	00001	11000	11110	01101	11011	01011	00101	10100
11010	11100	00111	11111	10011	01101	00110	01110	00100
11011	10011	10110	00111	01000	01111	11010	00100	00011
11100	00110	01011	10111	11010	10000	00100	01001	00101
11101	01001	11010	01111	00001	10010	11000	00011	00010
11110	10100	00101	01110	11111	00100	10101	01000	10010
11111	11011	10100	10110	00100	00110	01001	00010	10101

	11001	11010	11011	11100	11101	11110	11111
00001	10111	10110	11110	11010	01011	00101	01100
00010	10000	01010	01100	11110	11000	01011	00100
00011	00111	11100	10010	00100	10011	01110	01000
00100	00011	11110	11010	00001	10010	10111	11100
00101	10100	01000	00100	11011	11001	10010	10000
00110	10011	10100	10110	11111	01010	11100	11000
00111	00100	00010	01000	00101	00001	11001	10100
01000	10010	11001	01111	01001	10000	00100	11010
01001	00101	01111	10001	10011	11011	00001	10110
01010	00010	10011	00011	10111	01000	01111	11110
01011	10101	00101	11101	01101	00011	01010	10010
01100	10001	00111	10101	01000	00010	10011	00110
01101	00110	10001	01011	10010	01001	10110	01010
01110	00001	01101	11001	10110	11010	11000	00010
01111	10110	11011	00111	01100	10001	11101	01110
10001	01110	01100	00101	00110	10110	11011	10011
10010	01001	10000	10111	00010	00101	10101	11011
10011	11110	00110	01001	11000	01110	10000	10111
10100	11010	00100	00001	11101	01111	01001	00011
10101	01101	10010	11111	00111	00100	01100	01111
10110	01010	01110	01101	00011	10111	00010	00111
10111	11101	11000	10011	11001	11100	00111	01011
11000	01011	00011	10100	10101	01101	11010	00101
11001	11100	10101	01010	01111	00110	11111	01001
11010	11011	01001	11000	01011	10101	10001	00001
11011	01100	11111	00110	10001	11110	10100	01101
11100	01000	11101	01110	10100	11111	01101	11001
11101	11111	01011	10000	01110	10100	01000	10101
11110	11000	10111	00010	01010	00111	00110	10001
11111	01111	00001	11100	10000	01100	00011	11101

С учетом табл. 5 в лупе Q_1^* одна из третьих степеней каждого из элементов

$$(0,0,1,1,0),\ (0,1,0,0,1),\ (0,1,0,1,1),\ (0,1,1,0,1),\ (1,1,0,0,0),\ (1,1,1,1,0)$$

совпадает с его правым или левым обратным, так что их порядки равны 4. Для элементов

$$(0,0,0,0,1),\ (0,0,1,0,0),\ (0,0,1,0,1),\ (1,0,1,0,1),\ (1,1,1,0,1)$$

лупа Q_1^* совпадает с левым или правым обратным квадрата элемента и порядки равны 5. Также порядок 5 имеют элементы $(0,0,1,1,1)$, $(0,1,0,0,0)$, $(0,1,1,0,0)$, $(1,0,0,0,1)$, $(1,0,0,1,0)$, $(1,0,1,1,0)$, $(1,0,1,1,1)$ и $(1,1,1,0,0)$, поскольку одна из четвертых степеней каждого из них совпадает с левым или правым обратным квадрата элемента.

Продолжая, найдем 10 элементов порядка 6, единственный элемент $(1,1,1,1,1)$ наивысшего порядка 7 и вместе с тем спектр лупы Q_1^* (табл. 6).

Аналогично получаем (табл. 7) спектры луп Q_2^* и Q_3^*. (Во всех трех лупах единствен неединичный элемент либо наименьшего, либо наибольшего порядка.) В частности, лупа Q_i^* $(i = 1, 2, 3)$ является однопорожденной и даже правоциклической.

Тем самым доказательство теоремы завершается. □

Согласно [11; 13; 23, с. 802] число собственных полуполей порядка 32, с точностью до изоморфизма, равно 2501. Они образуют 5 изотопных классов: 2 класса по 961 лево- и правоциклических полуполей, 2 класса по 186 аналогичных полуполей и еще по 7 с односторонней цикличностью. Оставшийся класс дают единственное ни лево-, ни правоциклическое полуполе и еще 192 полуполя с различными вариантами цикличности.

Т а б л и ц а 6

Обратные к элементам и спектр лупы Q_1^*

Элемент y	Левый обратный	Правый обратный	Порядок $\vert y\vert$
(1,0,0,0,0)	**(1,0,0,0,0)**	**(1,0,0,0,0)**	1
(0,0,0,0,1)	(1,1,0,1,0)	(0,1,0,0,0)	5
(0,0,0,1,0)	(0,0,1,0,0)	(1,1,0,0,1)	6
(0,0,0,1,1)	(0,1,1,0,1)	(1,1,0,0,0)	6
(0,0,1,0,0)	(1,1,1,1,0)	(0,0,0,1,0)	5
(0,0,1,0,1)	(1,0,0,0,1)	(1,1,1,1,1)	5
(0,0,1,1,0)	(1,1,0,0,0)	(0,1,1,1,1)	4
(0,0,1,1,1)	(1,1,0,1,1)	(1,0,0,1,1)	5
(0,1,0,0,0)	(0,0,0,0,1)	(1,1,1,0,1)	5
(0,1,0,0,1)	(0,1,1,1,0)	(1,0,0,0,1)	4
(0,1,0,1,0)	(1,0,1,1,1)	(1,0,1,1,0)	6
(0,1,0,1,1)	(0,1,1,0,0)	(0,1,1,0,1)	4
(0,1,1,0,0)	(1,1,0,0,1)	(0,1,0,1,1)	5
(0,1,1,0,1)	(0,1,0,1,1)	(0,0,0,1,1)	4
(0,1,1,1,0)	(1,0,1,0,1)	(0,1,0,0,1)	6
(0,1,1,1,1)	(0,0,1,1,0)	(1,0,1,0,0)	6
(1,0,0,0,1)	(0,1,0,0,1)	(0,0,1,0,1)	5
(1,0,0,1,0)	(1,0,1,0,0)	(1,1,0,1,0)	5
(1,0,0,1,1)	(0,0,1,1,1)	(1,1,1,1,0)	6
(1,0,1,0,0)	(0,1,1,1,1)	(1,0,0,1,0)	6
(1,0,1,0,1)	(1,1,1,0,0)	(0,1,1,1,0)	5
(1,0,1,1,0)	(0,1,0,1,0)	(1,0,1,1,1)	5
(1,0,1,1,1)	(1,0,1,1,0)	(0,1,0,1,0)	5
(1,1,0,0,0)	(0,0,0,1,1)	(0,0,1,1,0)	4
(1,1,0,0,1)	(0,0,0,1,0)	(0,1,1,0,0)	6
(1,1,0,1,0)	(1,0,0,1,0)	(0,0,0,0,1)	6
(1,1,0,1,1)	(1,1,1,0,1)	(0,0,1,1,1)	6
(1,1,1,0,0)	(1,1,1,1,1)	(1,0,1,0,1)	5
(1,1,1,0,1)	(0,1,0,0,0)	(1,1,0,1,1)	5
(1,1,1,1,0)	(1,0,0,1,1)	(0,0,1,0,0)	4
(1,1,1,1,1)	(0,0,1,0,1)	(1,1,1,0,0)	7

Т а б л и ц а 7

Спектры луп Q_2^* и Q_3^*

Элемент y	Порядок $\vert y\vert$ в Q_2^*	Порядок $\vert y\vert$ в Q_3^*
(1,0,0,0,0)	1	1
(0,0,0,0,1)	6	5
(0,0,0,1,0)	5	6
(0,0,0,1,1)	5	6
(0,0,1,0,0)	6	6
(0,0,1,0,1)	5	5
(0,0,1,1,0)	5	5
(0,0,1,1,1)	5	5
(0,1,0,0,0)	5	7
(0,1,0,0,1)	6	7
(0,1,0,1,0)	5	5
(0,1,0,1,1)	5	5
(0,1,1,0,0)	5	6
(0,1,1,0,1)	5	6
(0,1,1,1,0)	6	6
(0,1,1,1,1)	6	5
(1,0,0,0,1)	6	5
(1,0,0,1,0)	4	6
(1,0,0,1,1)	5	5
(1,0,1,0,0)	6	7
(1,0,1,0,1)	5	7
(1,0,1,1,0)	5	5
(1,0,1,1,1)	7	6
(1,1,0,0,0)	6	4
(1,1,0,0,1)	6	6
(1,1,0,1,0)	5	7
(1,1,0,1,1)	4	7
(1,1,1,0,0)	6	6
(1,1,1,0,1)	5	5
(1,1,1,1,0)	6	5
(1,1,1,1,1)	5	6

СПИСОК ЛИТЕРАТУРЫ

1. **Курош А.Г.** Лекции по общей алгебре. СПб: Лань, 2007. 560 с.
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.
3. **Dickson L.E.** Linear algebras in which division is always uniquely possible // Trans. Amer. Math. Soc. 1906. Vol. 7, no. 3. P. 370–390.
4. **Johnson N.L., Jha V., Biliotti M.** Handbook of finite translation planes. London; New York, 2007. 861 p.
5. **Холл М.** Теория групп. М.: ИЛ, 1962. 460 с.
6. **Liebeck M.** The classification of finite simple Moufang loops // Math. Proc. Camb. Phil. Soc. 1987. Vol. 102. P. 33–47.
7. **Grishkov A.N., Zavarnitsine A.V.** Lagrange's theorem for Moufang loops // Math. Proc. Camb. Phil. Soc. 2005. Vol. 139. P. 101–116.
8. **Grishkov A.N., Zavarnitsine A.V.** Sylow's theorems for Moufang loops // J. Algebra. 2009. Vol. 321, no. 7. P. 1813–1825.
9. **Gagola S. M. III** Hall's theorem for Moufang loops // J. Algebra. 2010. Vol. 323, no. 12. P. 3252–3262.
10. **Wene G.P.** On the multiplicative structure of finite division rings //Aequationes Math. 1991. Vol. 41, iss. 1. P. 222–233.
11. **Knuth D.E.** Finite semifields and projective planes (PhD dissertation). Pasadena: California Inst. Technology, 1963. 70 p.
12. **Knuth D.E.** Finite semifields and projective planes // J. Algebra. 1965. Vol. 2. P. 182–217.
13. **Rua I.F.** Primitive and non-primitive finite semifields // Commun. Algebra. 2004. Vol. 32, no. 2. P. 793–803.
14. **Levchuk V.M., Panov S.V., Shtukkert P.K.** The structure of finite quasifields and their projective translation planes // Proc. XII Intern. Conf. on Algebra and Number Theory. Tula, 2014. P. 106–108.
15. **Levchuk V.M., Shtukkert P.K.** Problems on structure for quasifields of orders 16 and 32 // J. Sib. Fed. Univ. Ser. Math. Phys. 2014. Vol.7, no. 3. P. 362–372.
16. **Штуккерт П.К.** Квазиполя и проективные плоскости трансляций малых четных порядков // Изв. Иркут. гос. ун-та. 2014. Т. 7, № 1. С. 144–159.
17. **Hughes D.R., Piper F.C.** Projective planes. New-York: Springer-Verlag, 1973. 291 p.
18. **Lüneburg H.** Translation planes. New-York: Springer-Verlag, 1980. 278 p.
19. **Andre J.** Uber nicht-Desarguesche Ebenen mit transitiver Translationgruppe // Math. Z. 1954. Vol. 60. P. 156–186.
20. **Kallaher M.** Affine planes with transitive collineation groups. New York: North-Holland, 1982. 155 p.
21. **Albert A.A.** Finite division algebras and finite planes // Proc. Sympos. Appl. Math. Providence: Amer. Math. Soc, 1960. Vol. 10. P. 53–70.
22. **Wesson J.R.** On Veblen-Wedderburn systems // Amer. Math. Monthly. 1957. Vol. 64, no. 9. P. 631–635.
23. **Walker R.J.** Determination of division algebras with 32 elements // Proc. Symp. Appl. Math. 1962. Vol. 15. P. 83–85.
24. **Kleinfeld E.** Techniques for enumerating Veblen-Wedderburn systems // J. Assoc. Comput. Mach. 1960. Vol. 7. P. 330–337.
25. **Dempwolff U., Reifart A.** The Classification of the translation planes of order 16, Part I // Geom. Dedic. 1983. Vol. 15. P. 137–153.
26. **Dempwolff U.** Translation Planes of Small Order: [e-resource]. URL: http://www.mathematik.uni-kl.de/~dempw/dempw_Plane.html .

27. **Штуккерт П.К.** Квазиполя и проективные плоскости трансляций малых четных порядков: дисс. ... канд. физ.-мат. наук / Сиб. федер. ун-т. Красноярск, 2014. 83 с.
28. **Rockenfeller R.** Translationsebenen der Ordnung 32 (Diploma Thesis) / FB Mathematik. University of Kaiserslautern. 2011. 93 p.

Левчук Владимир Михайлович
д-р физ.- мат. наук, профессор
зав. кафедрой
Сибирский федеральный университет,
Институт математики и фундаментальной информатики
e-mail: vlevchuk@sfu-kras.ru

Поступила 25.02.15

Штуккерт Полина Константиновна
канд. физ.- мат. наук
старший преподаватель
Норильский федеральный университет – Сибирский федеральный университет,
Институт математики и фундаментальной информатики
e-mail: Poli422@yandex.ru