МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

На правах рукописи

Штуккерт Полина Константиновна

КВАЗИПОЛЯ И ПРОЕКТИВНЫЕ ПЛОСКОСТИ ТРАНСЛЯЦИЙ МАЛЫХ ЧЕТНЫХ ПОРЯДКОВ

01.01.06 — математическая логика, алгебра и теория чисел

Диссертация на соискание ученой степени
кандидата физико-математических наук

Научный руководитель
доктор физ.-мат. наук, профессор
Левчук В. М.

Красноярск – 2014

Содержание

Введение

Кольцо $S = \langle S, +, \circ \rangle$ с единицей $e \neq 0$ называют *полуполем* (согласно А.Г. Курошу [2, II.6.1], *квазителом*), если $S^* = (S \setminus \{0\}, \circ)$ – лупа, то есть для любых $a \in S^*$ и $b \in S$ каждое уравнение $a \circ x = b$ и $y \circ a = b$ однозначно разрешимо в S. При конечном S ослабление двусторонней дистрибутивности до односторонней приводит к понятию *квазиполя* [18], [27]; его минимальное подполе единственно и простого порядка p, а порядок S – p-примарный.

Построения *собственных* (или не являющихся полем) квазиполей взаимосвязаны с построениями недезарговых проективных плоскостей трансляций с помощью координатизирующих и регулярных множеств (О. Веблен и Ж.М. Веддерберн [40], Л. Диксон [13], Д. Кнут [23] и др.) и с середины прошлого века опираются на компьютерные вычисления. См. также Н.Д. Подуфалов [4] и его вопросы 9.43, 10.48, 11.76, 11.77 и 12.66 в [39]. В отличие от конечных полей, конечные квазиполя изучены мало, см. [20].

В диссертации исследуются известные вопросы о строении конечных квазиполей для конечных квазиполей малых четных порядков.

В 2004 г. И. Руа [35] на основе известного перечисления полуполевых плоскостей порядка 32 (Д. Кнута, 1963 г.) выявил полуполе S порядка 32, в котором лупа S^* не является правоциклической, более точно, 21-я правоупорядоченная степень любого ее элемента равна e. Согласно [35], *гипотеза Г. Венэ [43] о правоцикличности лупы* S^*

конечного полуполя S остается открытой, когда $|S| > 32$.

Следующие вопросы для конечного собственного квазиполя выделил В.М. Левчук ([55] и доклад в МГУ, 2013 г.).

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

(Б) *Выявить конечные квазиполя S с не однопорожденной лупой S^*.* **Гипотеза:** *Верно ли, что для конечного полуполя S лупа S^* всегда однопорождена ?*

(В) *Какие возможны спектры лупы S^* конечного полуполя и квазиполя ?*

Спектром лупы в [55] названо множество порядков всех ее элементов. *Порядок $|v|$ элемента v лупы* обобщает понятие порядка элемента группы: это наименьшее целое число $m \geq 1$ такое, что хотя бы одна m-я степень элемента v при всевозможных расстановках скобок равна e; порядок бесконечен, когда такое m не существует.

Наименьшие четные порядки недезарговых проективных полуполевых плоскостей и плоскостей трансляций совпадают и равны 16; для нечетных p-примарных порядков они равны p^2 и p^3, соответственно (Л. Диксон [14], Ж. Вессон [44] и Д. Кнут [23]). Перечисление, с точностью до изоморфизмов, таких плоскостей завершено в 80-х годах (П. Лоример [26], У. Демпволф и А. Рейфарт [11], [12]), а порядка 32 – в работах Р. Волкера [41], для случая полуполевых плоскостей, и завершено в 2011 г., Р. Рокенфеллером и У. Демпволфом в [34] (см. также [12]).

Таблицу Кэли лупы S^* любого конечного квазиполя S естественно рассматривать, как латинский квадрат, и методы латинских прямоугольников для построения квазиполей порядка 16 применял Е. Клейнфилд [21].

Цель диссертации – исследовать вопросы **(A)** – **(B)** для квазиполей проективных плоскостей трансляций малых четных порядков.

Диссертация состоит из введения, двух глав по 4 параграфа и списка литературы, включающего 55 наименований. Номер теоремы, леммы и др. включает последовательно номер главы, параграфа и порядковый номер в параграфе.

Основные результаты диссертации направлены на решение вопросов **(A)** – **(B)** для квазиполей малых четных порядков.

1) Описано строение представителей изотопных классов квазиполей порядка 16, в частности, выявлено квазиполе, каждый элемент которого лежит в подполе порядка 4, а также квазиполе с элементами порядка 3, не лежащими в подполе порядка 4.

2) Для полуполей порядка 16 перечислены максимальные подполя, доказана однопорожденность лупы ненулевых элементов, и найден ее спектр.

3) Описано строение полуполей проективных полуполевых плоскостей порядка 32.

4) Доказана однопорожденность лупы полуполя Кнута – Руа, не являющегося правоциклическим.

Получен также ответ на вопросы В.В. Беляева о латинских пря-

моугольниках, записанных им для молодых исследователей в [1].

В § 1.1 главы 1, наряду с постановкой основных задач, приводятся основные определения и свойства квазиполей и плоскостей трансляций, показана их характеризуемость регулярным множеством.

С использованием известных регулярных множеств проективных плоскостей трансляций порядка 16 (У. Демпволф [12]), в § 1.2 построены квазиполя Q_i $(1 \leq i \leq 5)$, исчерпывающие, с точностью до изотопизмов, все квазиполя порядка 16. Теоремы 1.2.1 и 1.2.2 показывают, что квазиполя Q_2 и Q_5 имеют, соответственно, 1 и 3 максимальных подполя порядка 4, каждый, не лежащий в них элемент, порождает лупу Q_2^* или, соответственно, Q_5^*, а ее спектр в обоих случаях совпадают с $\{1, 3, 5\}$. Аномальные свойства выявляет

Теорема 1.2.3. *Каждое из квазиполей Q_i, $i = 1, 3, 4$, есть теоретико-множественное объединение 7 максимальных подполей порядка 4. В частности, лупа Q_i^* не однопорождена и ее спектр совпадает с $\{1, 3\}$.*

В § 1.3 приведены два метода Е. Клейнфилда построения квазиполей порядка 16 с помощью латинских прямоугольников и специальных порождающих последовательностей. В теореме 1.3.3 приведена классификация Е. Клейнфилда полуполей порядка 16, с точностью до изоморфизмов.

Ответы на вопросы В.В. Беляева о латинских $r \times 6$-прямоугольниках, записанные им в 2004 г. для молодых исследователей [1], приводятся в § 1.4.

Теорема 1.2.1 и результаты § 1.4 опубликованы автором в [46] и [49], соответственно. Теоремы 1.2.2 и 1.2.3 опубликованы в неразделном соавторстве (соавтор В.М. Левчук) в статье [47].

Глава 2 посвящена строению полуполей порядков 16 и 32.

Согласно теореме Е. Клейнфилда [21], число попарно неизоморфных собственных полуполей порядка 16 равно 23. Наряду с классификационной теоремой Е. Клейнфилда (теорема 1.3.3), в § 1.3 указан предложенный Е. Клейнфилдом алгоритм построения таблицы Кэли лупы S^* полуполя S порядка 16. Явные формулы умножения двух полуполей выписал Д. Кнут [22], [23].

В § 2.1 выписаны формулы умножения всех Клейнфилдовых полуполей. С их помощью в теореме 2.1.1 показано, что число полуполей порядка 16, с точностью до изоморфизмов и антиизоморфизмов, равно 16; именно для них строятся таблицы Кэли.

Теоремы 2.2.2 – 2.2.4 и сводная таблица 2.2.5 в § 2.2 решают вопросы **(A)** – **(B)** для полуполей порядка 16.

Строение опровергающего гипотезу Г. Венэ полуполя $\Re$ порядка 32, не являющегося правоциклическим (*полуполе Кнута – Руа*), исследуется в § 2.4. Основная теорема 2.4.1 показывает однопорожденность лупы $\Re^*$. Основные результаты § 2.2 и теорема 2.4.1 опубликованы автором в совместной статье [47] (соавтор В.М. Левчук).

Используя регулярные множества проективных плоскостей трансляций У. Демпвольфа [12], мы выписываем в § 2.3 представители всех изотопных классов собственных полуполей порядка 32.

Их строение выявляют опубликованные автором в [46] теорема 2.3.2 и

Теорема 2.3.3. *В полуполе P_5 существует подполе H порядка 4, являющееся единственным максимальным подполем и не являющееся ни правым, ни левым ядром. Каждый элемент из $P_5 \setminus H$ порождает лупу P_5^* и имеет порядок > 3; спектр лупы P_5^* совпадает с $\{1, 3, 4, 5, 6, 7, 8\}$.*

Основные результаты диссертации опубликованы в работах [46] – [55] и включают статьи [46] и [47] в изданиях из перечня ВАК.

Результаты диссертации докладывались автором на Красноярском алгебраическом семинаре (2014). Они апробировались на IV Российской школе-семинаре "Синтаксис и семантика логических систем" в Улан-Удэ (2012); "VII Всесибирский конгресс женщин-математиков" в Красноярске (2012); на международных конференциях в Киеве (Украина, 2012), "Мальцевские чтения" в Новосибирске (2012, 2013); "Алгебра и логика: теория и приложения" в Красноярске (2013); "Алгебра и теория чисел" в Туле (2014).

Автор благодарна доценту О.В. Кравцовой за постановку первой задачи и помощь в подготовке первой работы, и научному руководителю, профессору В.М. Левчуку, за предложенную тему. Признательна сотрудникам кафедры алгебры и математической логики и ИМиФИ СФУ за хорошие условия для научной работы.

Работа над диссертацией была поддержана грантом Российского фонда фундаментальных исследований (код проекта 12-01-00968).

1 Квазиполя проективных плоскостей трансляций и методы их построения

Классификацию недезарговых плоскостей трансляций порядка 16 завершили в 1983 г. У. Демпволф и А. Рейфарт [11], а порядка 32 – Р. Рокенфеллер и У. Демпволф в 2011 г. На основе их регулярных множеств в диссертации удается выписать представители всех изотопных классов квазиполей или полуполей заданных порядков.

В § 1.2 мы решаем вопросы **(A)** – **(B)** для представителей квазиполей порядка 16 (теоремы 1.2.1 – 1.2.3). В частности, выявлено квазиполе, каждый элемент которого лежит в подполе порядка 4, а также квазиполе с элементами порядка 3, не лежащими в подполе порядка 4.

В § 1.3 приведены два метода Е. Клейнфилда построения таблицы Кэли лупы ненулевых элементов квазиполя порядка 16 с помощью латинских прямоугольников и специальных порождающих последовательностей.

В § 1.4 получен ответ на вопросы В.В. Беляева о латинских прямоугольниках, записанных им для молодых исследователей в [1].

Предварительные сведения и постановка основных задач приводятся в § 1.1.

1.1 Квазиполя и регулярные множества проективных плоскостей трансляций. Постановка основных задач

Определение 1.1.1. *Конечное множество Q с бинарными операциями сложения $+$ и умножения $\circ$ называют левым квазиполем, если:*

1) $(Q,+)$ *– абелева группа;* *2)* $0 \circ x = 0$ $(x \in Q)$*;*

3) $(Q \setminus \{0\}, \circ)$ *– лупа;*

4) выполняется левый дистрибутивный закон

$$x \circ (y+z) = x \circ y + x \circ z \qquad (x,y,z \in Q).$$

Напомним, что множество L с бинарной операцией $\circ$ называют *лупой*, если в $(L,\circ)$ существует нейтральный элемент и уравнения $a \circ x = b$ и $x \circ a = b$ однозначно разрешимы при любых $a, b \in L$. В частности, группа – это ассоциативная лупа.

Конечное *правое квазиполе* определяется аналогично с соответствующими изменениями свойств 3) и 4). (Х. Люнебург [27] под "квазиполем" понимает "правое квазиполе".) Далее, как и Д. Хьюгес [18], говорим "квазиполе" вместо "левое квазиполе" , если не оговорено противное.

Замечание 1.1.2. *Д. Хьюгес [18] называет $(Q,+,\circ)$ с произвольным (не обязательно конечным) Q и условиями 1) – 4) слабым*

квазиполем, а квазиполем – при дополнительном условии однозначной разрешимости уравнения $a \circ x = b \circ x + c$ *при любых* $a, b, c \in Q$, $a \neq b$. *Согласно [18, Теорема 7.3], конечное слабое квазиполе есть квазиполе.*

Квазиполе с двусторонней дистрибутивностью называют *полуполем*. (В терминологии А.Г. Куроша [2, II.6.1] – это квазитело.)

Определение 1.1.3. *Квазиполя* $\langle S_1, +, \circ \rangle$ *и* $\langle S_2, +, \cdot \rangle$ *называют изотопными, если существуют изоморфизмы* F, G, H *аддитивных групп* $S_1 \to S_2$ *такие, что*

$$x^F \cdot y^G = (x \circ y)^H \qquad (x, y \in S_1).$$

Построения *собственных* (или не являющихся полем) квазиполей с начала прошлого века тесно связаны с построениями недезарговых проективных плоскостей трансляций с помощью координатизирующих и регулярных множеств.

Согласно [5, § 20.1], *проективная плоскость* π – это множество точек с определенными подмножествами, называемыми прямыми, и удовлетворяющими следующим аксиомам:

1) две различные точки лежат на одной и только одной прямой;

2) две различные прямые пересекаются в единственной точке;

3) существуют четыре точки, никакие три из которых не лежат на одной прямой.

Проективную плоскость называют *конечной*, если конечно число точек хотя бы одной ее прямой. Оказывается, тогда однозначно

определено число n, называемое *порядком проективной плоскости*, характеризуемое любым из следующих свойств [5, Теорема 20.1.1]:

1) некоторая прямая содержит точно $n+1$ точек;

2) некоторая точка принадлежит точно $n+1$ прямым;

3) каждая прямая содержит точно $n+1$ точек;

4) каждая точка лежит точно на $n+1$ прямых;

5) в плоскости π ровно n^2+n+1 точек;

6) в плоскости π ровно n^2+n+1 прямых.

Конечные плоскости порядка n существуют не для любого натурального числа $n \geq 2$. В связи со старой гипотезой Л. Эйлера о плоскостях порядка $n > 2$, $n \equiv 2 \mod 4$, Г. Тарри доказал в 1900 г. их несуществование при $n = 6$. См., например, [5].

Определение 1.1.4. *Изоморфизмом проективных плоскостей π_1 и π_2 называют биективное отображение точек и прямых плоскости π_1, соответственно, в точки и прямые плоскости π_2, сохраняющее инцидентность.*

Для построения плоскостей трансляций выбирают n-мерное линейное пространство W над полем F *(координатизирующее множество)*, внешнюю прямую сумму

$$V = W \oplus W = \{(x, y) \mid x, y \in W\}$$

двух копий W и расщепление μ аддитивной группы $(V, +)$ такое, что $V = M \oplus N$ для любых $M \neq N$ из μ. Точки проективной плоскости

трансляций $\pi = \pi(V, \mu)$ ранга n над F дают 1-мерные подпространства из V, а прямые – подгруппы из μ и смежные классы по ним, причем 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, [18], [27].

Напомним, что *расщеплением* аддитивной группы называют набор ее подгрупп (компоненты расщепления) с попарно нулевыми пересечениями, дающих в теоретико-множественном объединении всю группу. Компоненты расщепления μ есть n-мерные подпространства в V [27]. Известна [33] следующая лемма, где $V(\infty) = (0, W)$ и

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

Лемма 1.1.5. *Допустим, что* $V(0), V(\infty) \in \mu$. *Тогда:*

а) если $M \in \mu$ *и* $M \neq V(0), V(\infty)$, *то* $M = V(\sigma)$ *при единственном* $\sigma \in GL(W)$ *и, полагая* $R^* = \{\sigma \in GL(W) \mid V(\sigma) \in \mu\}$, *имеем*

$$\mu = \{V(\sigma) \mid \sigma \in R^* \cup \{0\}\} \cup \{V(\infty)\};$$

б) если $u, v \in W \setminus \{0\}$, *то* $u^\sigma = v$ *при единственном* $\sigma \in R^*$;

в) если $\tau, \rho \in R^*$ *и* $\tau \neq \rho$, *то* $\tau - \rho \in GL(W)$.

Верно и обратное: если подмножество R^* *в* $GL(W)$ *удовлетворяет условиям б) и в), то* $\mu = \{V(0),\ V(\infty)\} \cup \{V(\sigma) \mid \sigma \in R^*\}$ *есть расщепление группы* $(V, +)$ *такое, что* $V = M \oplus N$ *для любых* $M \neq N$ *из* μ. $\square$

Заметим, что свойство б) дает биективное отображение $\theta : W \to R^* \cup \{0\}$ по правилу:

$$\theta(u) = \sigma \quad (v \in W \setminus \{0\}, \quad u^\sigma = v), \quad \theta(0) = 0.$$

Совокупность R нулевого преобразования и подмножества R^* в $GL(W)$ с единицей и условиями б), в) называют *регулярным множеством* плоскости π. Записывая векторы из W координатными строками, полагаем

$$x \circ y := x \cdot \theta(y) \quad (x, y \in W). \tag{1.1}$$

Плоскость π называют *плоскостью трансляций*, если $(W, +, \circ)$ есть квазиполе. Плоскость называют *полуполевой*, если W – полуполе, [18], [27], [4]. Хорошо известны следующие утверждения.

Лемма 1.1.6. *Если координатизирующее множество есть поле, то и регулярное множество есть подполе кольца $M(n, F)$, а соответствующая плоскость – дезаргова.* □

Лемма 1.1.7. *Полуполевая плоскость дезаргова тогда и только тогда, когда соответствующее ей полуполе есть поле.* □

Теорема 1.1.8. (А. Альберт [7]) *Полуполевые плоскости изоморфны тогда и только тогда, когда соответствующие полуполя изотопны.* □

Теорема о минимальном подполе конечного поля переносится на конечные квазиполя, как показывает следующая известная лемма

для конечного квазиполя S с единицей e, где

$$ke = \underbrace{e + e + ... + e}_{k \text{ раз}}, \quad (-k)e = -ke \text{ при } k \in Z,\ k > 0.$$

Лемма 1.1.9. *Отображение* $\chi:\ k \to ke$ $(k \in Z)$ *есть гомоморфизм кольца* Z *целых чисел в квазиполе* S, *причем либо* $\chi(Z) \simeq Z$, *либо* $\chi(Z) \simeq Z_p$ *для некоторого простого числа* p. $\square$

Таким образом, характеристика произвольного квазиполя S также определена, причем порядок конечного квазиполя S всегда равен степени его характеристики p. Кроме того, справедлива [22]

Теорема 1.1.10. *Полуполе порядка* p^n *(*p *- простое число) существует тогда и только тогда, когда* $n \geq 3$ *и* $p^n \geq 16$.

Доказательство. См. [22, Теорема 6.1 и Следствие 8.2.2]. $\square$

Отметим, что квазиполя порядка p^2 с простым $p > 2$ построил Л. Диксон [14]. С другой стороны, квазиполя порядка 2^n при $n \leq 3$ являются полями (Ж. Вессон [44]). Таким образом, наименьшие четные порядки недезарговых проективных полуполевых плоскостей и плоскостей трансляций совпадают и равны 16. (Для нечетных p-примарных порядков они равны p^2 и p^3, соответственно.) Такие плоскости и их квазиполя классифицировали Е. Клейнфилд [21], У. Демпволф и А. Рейфарт [11].

В диссертации исследуются следующие вопросы для конечных квазиполей и полуполей, которые записал В.М. Левчук [55].

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

(Б) *Какие возможны спектры лупы S^* конечного полуполя и квазиполя ?*

(В) *Перечислить конечные квазиполя и, в частности, полуполя, у которых лупа S^* не является однопорожденной.*

См. также вопросы 9.43, 10.48, 11.76, 11.77 и 12.66 Н.Д. Подуфалова [39]. Остается открытой *гипотеза Г. Венэ о правоцикличности лупы S^** полуполя порядка > 32: всегда ли ее исчерпывают правоупорядоченные степени фиксированного элемента [43], [35].

1.2 Строение квазиполей проективных плоскостей трансляций порядка 16

Описанный в § 1.1 метод построения конечных квазиполей с помощью регулярных множеств проективных плоскостей трансляций является наиболее распространенным. Этот метод, называемый далее *классическим*, позволяет классифицировать квазиполя, с точностью до изотопизмов. См. также теорему А. Альберта 1.1.8.

Плоскости трансляций порядка 16 классифицировали полностью У. Демпволф и А. Рейфарт в работе [11]. С точностью до изоморфизмов, их всего 8, а число классов изоморфных полуполевых плоскостей равно 3. Полуполя порядка 16 мы исследуем в § 2.2.

Координатизирующее множество плоскостей трансляций порядка 16 есть пространство W строк длины 4 над Z_2. Регулярные множества представителей 5 изоморфных классов плоскостей трансля-

ций, не являющихся полуполевыми, приведены на сайте У. Демп-волфа [12]. Выпишем их в следующем порядке (через O и E обозначаются нулевая и единичная матрицы):

$$\{O, E, \begin{pmatrix} 0&0&0&1\\ 1&0&1&0\\ 1&1&1&1\\ 1&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&0\\ 0&0&1&1\\ 1&0&1&0\\ 1&1&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&1\\ 1&0&0&1\\ 0&1&0&1\\ 1&1&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0\\ 1&1&0&0\\ 1&0&1&1\\ 0&1&1&0 \end{pmatrix},$$
$$\begin{pmatrix} 0&1&0&1\\ 0&1&1&0\\ 0&1&0&0\\ 1&0&1&1 \end{pmatrix}, \begin{pmatrix} 0&1&1&0\\ 1&1&1&1\\ 0&0&0&1\\ 0&0&1&1 \end{pmatrix}, \begin{pmatrix} 0&1&1&1\\ 0&1&0&1\\ 1&1&1&0\\ 0&1&0&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&1\\ 1&1&1&0\\ 1&1&0&1\\ 1&0&0&0 \end{pmatrix}, \begin{pmatrix} 1&0&1&0\\ 0&1&1&1\\ 1&0&0&0\\ 1&1&0&0 \end{pmatrix},$$
$$\begin{pmatrix} 1&0&1&1\\ 1&1&0&1\\ 0&1&1&1\\ 1&1&1&1 \end{pmatrix}, \begin{pmatrix} 1&1&0&0\\ 1&0&0&0\\ 1&0&0&1\\ 0&1&1&1 \end{pmatrix}, \begin{pmatrix} 1&1&0&1\\ 0&0&1&0\\ 0&1&1&0\\ 1&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&1&1&0\\ 1&0&1&1\\ 0&0&1&1\\ 0&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&1&1&1\\ 0&0&0&1\\ 1&1&0&0\\ 0&1&0&1 \end{pmatrix}\};$$

$$\{O, E, \begin{pmatrix} 0&0&0&1\\ 0&1&1&0\\ 1&1&0&1\\ 0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&1&0\\ 0&0&1&1\\ 1&0&1&0\\ 1&1&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&1\\ 1&1&0&1\\ 0&1&1&1\\ 1&0&1&1 \end{pmatrix}, \begin{pmatrix} 0&1&0&0\\ 1&1&1&1\\ 0&0&1&1\\ 0&1&0&1 \end{pmatrix},$$
$$\begin{pmatrix} 0&1&0&1\\ 1&1&0&0\\ 1&1&1&0\\ 1&1&1&1 \end{pmatrix}, \begin{pmatrix} 0&1&1&0\\ 1&1&1&0\\ 1&0&0&1\\ 0&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&1&1\\ 0&1&0&1\\ 0&1&0&0\\ 1&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&1\\ 1&0&1&0\\ 1&1&1&1\\ 0&1&1&1 \end{pmatrix}, \begin{pmatrix} 1&0&1&0\\ 0&1&1&1\\ 1&1&1&1\\ 0&1&1&1 \end{pmatrix},$$
$$\begin{pmatrix} 1&0&1&1\\ 0&0&0&1\\ 0&1&0&1\\ 1&0&0&0 \end{pmatrix}, \begin{pmatrix} 1&1&0&0\\ 1&0&0&1\\ 0&0&0&1\\ 1&1&1&0 \end{pmatrix}, \begin{pmatrix} 1&1&0&1\\ 0&0&1&0\\ 1&1&0&0\\ 0&1&1&0 \end{pmatrix}, \begin{pmatrix} 1&1&1&0\\ 1&0&0&0\\ 1&0&1&1\\ 1&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&1&1&1\\ 1&0&1&1\\ 0&1&1&0\\ 0&0&1&1 \end{pmatrix}\};$$

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

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

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

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

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

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

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

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

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

Каждое из них дает умножение на W по формуле (1.1). Получаем 5 изотопных классов квазиполей с представителями Q_i, $i = 1, 2, 3, 4, 5$, соответственно. Исследуем для них вопросы **(A)** – **(B)**.

Следующие две теоремы выявляют строение квазиполей Q_2 и Q_5, наиболее близких по свойствам к конечным полям.

Теорема 1.2.1. *Квазиполе Q_2 имеет единственное максимальное подполе H, причем $|H| = 4$ и каждый элемент из $Q_2 \setminus H$ имеет порядок 5 и порождает лупу Q_2^*.*

Доказательство. Таблицу Кэли лупы Q_2^* строим по правилу (1.1); умножение на единичный элемент $e = (1, 0, 0, 0)$ опускаем.

Таблица 1.2.1. Таблица Кэли лупы Q_2^*

	(0,0,0,1)	**(0,0,1,0)**	**(0,0,1,1)**	**(0,1,0,0)**	**(0,1,0,1)**	**(0,1,1,0)**	**(0,1,1,1)**
(0,0,0,1)	(0,1,0,0)	(1,1,0,1)	(1,0,1,1)	(0,1,0,1)	(1,1,1,1)	(0,0,1,0)	(1,0,1,0)
(0,0,1,0)	(1,1,0,1)	(1,0,1,0)	(0,1,1,1)	(0,0,1,1)	(1,1,1,0)	(1,0,0,1)	(0,1,0,0)
(0,0,1,1)	(1,0,0,1)	(0,1,1,1)	(1,1,0,0)	(0,1,1,0)	(0,0,0,1)	(1,0,1,1)	(1,1,1,0)
(0,1,0,0)	(0,1,1,0)	(0,0,1,1)	(1,1,0,1)	(1,1,1,1)	(1,1,0,0)	(1,1,1,0)	(0,1,0,1)
(0,1,0,1)	(0,0,1,0)	(1,1,1,0)	(0,1,1,0)	(1,0,1,0)	(0,0,1,1)	(1,1,0,0)	(1,1,1,1)
(0,1,1,0)	(1,0,1,1)	(1,0,0,1)	(1,0,1,0)	(1,1,0,0)	(0,0,1,0)	(0,1,1,1)	(0,0,0,1)
(0,1,1,1)	(1,1,1,1)	(0,1,0,0)	(0,0,0,1)	(1,0,0,1)	(1,1,0,1)	(0,1,0,1)	(1,0,1,1)
(1,0,0,1)	(0,1,0,1)	(1,1,1,1)	**(1,0,0,0)**	(0,0,0,1)	(1,0,1,0)	(0,1,0,0)	(1,1,0,1)
(1,0,1,0)	(1,1,0,0)	**(1,0,0,0)**	(0,1,0,0)	(0,1,1,1)	(1,0,1,1)	(1,1,1,1)	(0,0,1,1)
(1,0,1,1)	**(1,0,0,0)**	(0,1,0,1)	(1,1,1,1)	(0,0,1,0)	(0,1,0,0)	(1,1,0,1)	(1,0,0,1)
(1,1,0,0)	(0,1,1,1)	(0,0,0,1)	(1,1,1,0)	(1,0,1,1)	(1,0,0,1)	**(1,0,0,0)**	(0,0,1,0)
(1,1,0,1)	(0,0,1,1)	(1,1,0,0)	(0,1,0,1)	(1,1,1,0)	(0,1,1,0)	(1,0,1,0)	**(1,0,0,0)**
(1,1,1,0)	(1,0,1,0)	(1,0,1,1)	(1,0,0,1)	**(1,0,0,0)**	(0,1,1,1)	(0,0,0,1)	(0,1,1,0)
(1,1,1,1)	(1,1,1,0)	(0,1,1,0)	(0,0,1,0)	(1,1,0,1)	**(1,0,0,0)**	(0,0,1,1)	(1,1,0,0)

	(1,0,0,1)	**(1,0,1,0)**	**(1,0,1,1)**	**(1,1,0,0)**	**(1,1,0,1)**	**(1,1,1,0)**	**(1,1,1,1)**
(0,0,0,1)	(0,1,1,1)	(1,1,0,0)	**(1,0,0,0)**	(1,1,1,0)	(0,1,1,0)	(1,0,0,1)	(0,0,1,1)
(0,0,1,0)	(1,1,1,1)	**(1,0,0,0)**	(0,1,0,1)	(0,0,0,1)	(1,1,0,0)	(1,0,1,1)	(0,1,1,0)
(0,0,1,1)	**(1,0,0,0)**	(0,1,0,0)	(1,1,0,1)	(1,1,1,1)	(1,0,1,0)	(0,0,1,0)	(0,1,0,1)
(0,1,0,0)	(1,0,1,0)	(0,1,1,1)	(0,0,0,1)	(1,0,0,1)	(0,0,1,0)	**(1,0,0,0)**	(1,0,1,1)
(0,1,0,1)	(1,1,0,1)	(1,0,1,1)	(1,0,0,1)	(0,1,1,1)	(0,1,0,0)	(0,0,0,1)	**(1,0,0,0)**
(0,1,1,0)	(0,1,0,1)	(1,1,1,1)	(0,1,0,0)	**(1,0,0,0)**	(1,1,1,0)	(0,0,1,1)	(1,1,0,1)
(0,1,1,1)	(1,1,1,0)	(0,0,1,1)	(1,1,0,0)	(0,1,1,0)	**(1,0,0,0)**	(1,0,1,0)	(1,1,1,0)
(1,0,0,1)	(1,1,1,0)	(0,1,1,0)	(0,0,1,1)	(0,0,1,0)	(1,0,1,1)	(0,1,1,1)	(1,1,0,0)
(1,0,1,0)	(0,1,1,0)	(0,0,1,0)	(1,1,1,0)	(1,1,0,1)	(0,0,0,1)	(0,1,0,1)	(1,0,0,1)
(1,0,1,1)	(0,0,0,1)	(1,1,1,0)	(0,1,1,0)	(0,0,1,1)	(0,1,1,1)	(1,1,0,0)	(1,0,1,0)
(1,1,0,0)	(0,0,1,1)	(1,1,0,1)	(1,0,1,0)	(0,1,0,1)	(1,1,1,1)	(0,1,1,0)	(0,1,0,0)
(1,1,0,1)	(0,1,0,0)	(0,0,0,1)	(0,0,1,0)	(1,0,1,1)	(1,0,0,1)	(1,1,1,1)	(0,1,1,1)
(1,1,1,0)	(1,1,0,0)	(0,1,0,1)	(1,1,1,1)	(0,1,0,0)	(0,0,1,1)	(1,1,0,1)	(0,0,1,0)
(1,1,1,1)	(1,0,1,1)	(1,0,0,1)	(0,1,1,1)	(1,0,1,0)	(0,1,0,1)	(0,1,0,0)	(0,0,0,1)

С помощью таблицы Кэли устанавливаем равенство левого и правого обратных элементов к любому элементу лупы Q_2^*. Кроме того, $(0,0,1,0), (1,0,1,0)$ исчерпывают элементы порядка 3; вместе с нулем и единицей образуют единственное максимальное подполе H.

Далее g^k обозначает $k-$ю степень элемента g с правильной (или с правонормированной) расстановкой скобок. Для вычисления порядков элементов заметим, что число различных неассоциативных произведений длины n элемента g, то есть с различными расстановками скобок, при $n = 1, 2, 3, 4, 5$ равно $1, 1, 2, 5, 14$, соответственно. В частности, все они при $n = 1, 2, 3, 4$ отличны от e для элемента $g = (0, 0, 0, 1)$, а $g^5 = e$. Аналогично, произведения длины < 5 лю-

бого элемента $f \in Q_1 \setminus H$ не равны e и $f^5 = e$. Проверка с помощью таблицы Кэли показывает, что f порождает лупу Q_2^*. $\square$

Отметим, что таблица Кэли лупы Q_i^* построена для всех квазиполей Q_i. В отличие от Q_2, квазиполе Q_5 имеет 3 подполя порядка 4:

$$G_1 = \{0, e, (0,0,1,0), (1,0,1,0)\},\ G_2 = \{0, e, (0,1,0,1), (1,1,0,1)\},$$

$$G_3 = \{0, e, (0,1,1,1), (1,1,1,1)\}.$$

Теорема 1.2.2. *Максимальные подполя квазиполя Q_5 исчерпываются подполями G_1, G_2, G_3. Каждый элемент из $Q_5 \setminus \{G_1 \cup G_2 \cup G_3\}$ имеет порядок 5 и порождает лупу Q_5^*, в частности, ее спектр совпадает с $\{1, 3, 5\}$.*

Доказательство. Вначале восстанавливаем таблицу Кэли лупы Q_5^* с помощью умножения (1.1). Она показывает, что левый и правый обратные к любому элементу лупы Q_5^* совпадают.

С помощью таблицы Кэли лупы Q_5^* устанавливаем, что степени ≤ 4 элемента $g = (0,1,0,0)$ при любых расстановках скобок отличны от e, причем $g^5 = e$. Аналогично, элемент $f = (0,0,1,1)$ имеет порядок 5. Порядки $|y|$ всех элементов $y \in Q_5^*$ перечисляет

Таблица 1.2.2. Порядки элементов лупы Q_5^*

y	(1,0,0,0)	(0,0,1,0)	(1,0,1,0)	(0,1,0,1)	(1,1,0,1)	(0,1,1,1)	(1,1,1,1)	(0,0,0,1)
|y|	1	3	3	3	3	3	3	5

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

Таблица Кэли и таблица 1.2.2 показывают, что G_1, G_2 и G_3 есть подполя порядка 4, содержащие все элементы порядка 3 из Q_5, каждый элемент из $Q_5 \setminus \{G_1 \cup G_2 \cup G_3\}$ имеет порядок 5 и порождает лупу

Q_5^*. Отсюда сразу же следует, что подполя $G_1,\ G_2,\ G_3$ исчерпывают все максимальные подполя квазиполя Q_5. Тем самым, завершено доказательство теоремы. $\square$

Существенно аномальными свойствами, по сравнению с конечными полями, обладают квазиполя $Q_1,\ Q_3$ и Q_4: любой элемент каждого из них лежит в каком-либо подполе порядка 4, как показывает

Теорема 1.2.3. *Каждое из квазиполей $Q_i,\ i = 1, 3, 4$, есть теоретико-множественное объединение 7 максимальных подполей порядка 4. В частности, лупа Q_i^* не однопорождена и ее спектр совпадает с $\{1, 3\}$.*

Доказательство. С помощью первого регулярного множества определяем умножение (1.1) в квазиполе Q_1 и находим таблицу Кэли умножения элементов лупы Q_1^*; умножение на единичный элемент $(1, 0, 0, 0)$ в ней опускаем.

Таблица 1.2.3. Таблица Кэли лупы Q_1^*

	(0,0,0,1)	**(0,0,1,0)**	**(0,0,1,1)**	**(0,1,0,0)**	**(0,1,0,1)**	**(0,1,1,0)**	**(0,1,1,1)**
(0,0,0,1)	(1,0,0,1)	(1,1,0,1)	(1,1,1,0)	(0,1,1,0)	(1,0,1,1)	(0,0,1,1)	(0,1,0,0)
(0,0,1,0)	(1,1,1,1)	(1,0,1,0)	(0,1,0,1)	(1,0,1,1)	(0,1,0,0)	(0,0,0,1)	(1,1,1,0)
(0,0,1,1)	(0,1,1,0)	(0,1,1,1)	(1,0,1,1)	(1,1,0,1)	(1,1,1,1)	(0,0,1,0)	(1,0,1,0)
(0,1,0,0)	(1,0,1,0)	(0,0,1,1)	(1,0,0,1)	(1,1,0,0)	(0,1,1,0)	(1,1,1,1)	(0,1,0,1)
(0,1,0,1)	(0,0,1,1)	(1,1,1,0)	(0,1,1,1)	(1,0,1,0)	(1,1,0,1)	(1,1,0,0)	(0,0,0,1)
(0,1,1,0)	(0,1,0,1)	(1,0,0,1)	(1,1,0,0)	(0,1,1,1)	(0,0,1,0)	(1,1,1,0)	(1,0,1,1)
(0,1,1,1)	(1,1,0,0)	(0,1,0,0)	(0,0,1,0)	(0,0,0,1)	(1,0,0,1)	(1,1,0,1)	(1,1,1,1)
(1,0,0,1)	**(1,0,0,0)**	(1,1,1,1)	(1,1,0,1)	(0,0,1,0)	(1,1,1,0)	(0,1,0,1)	(0,0,1,1)
(1,0,1,0)	(1,1,1,0)	**(1,0,0,0)**	(0,1,1,0)	(1,1,1,1)	(0,0,0,1)	(0,1,1,1)	(1,0,0,1)
(1,0,1,1)	(0,1,1,1)	(0,1,0,1)	**(1,0,0,0)**	(1,0,0,1)	(1,0,1,0)	(0,1,0,0)	(1,1,0,1)
(1,1,0,0)	(1,0,1,1)	(0,0,0,1)	(1,0,1,0)	**(1,0,0,0)**	(0,0,1,1)	(1,0,0,1)	(0,0,1,0)
(1,1,0,1)	(0,0,1,0)	(1,1,0,0)	(0,1,0,0)	(1,1,1,0)	**(1,0,0,0)**	(1,0,1,0)	(0,1,1,0)
(1,1,1,0)	(0,1,0,0)	(1,0,1,1)	(1,1,1,1)	(0,0,1,1)	(0,1,1,1)	**(1,0,0,0)**	(1,1,0,0)
(1,1,1,1)	(1,1,0,1)	(0,1,1,0)	(0,0,0,1)	(0,1,0,1)	(1,1,0,0)	(1,0,1,1)	**(1,0,0,0)**

	(1,0,0,1)	**(1,0,1,0)**	**(1,0,1,1)**	**(1,1,0,0)**	**(1,1,0,1)**	**(1,1,1,0)**	**(1,1,1,1)**
(0,0,0,1)	**(1,0,0,0)**	(1,1,0,0)	(1,1,1,1)	(0,1,1,1)	(1,0,1,0)	(0,0,1,0)	(0,1,0,1)
(0,0,1,0)	(1,1,0,1)	**(1,0,0,0)**	(0,1,1,1)	(1,0,0,1)	(0,1,1,0)	(0,0,1,1)	(1,1,0,0)
(0,0,1,1)	(0,1,0,1)	(0,1,0,0)	**(1,0,0,0)**	(1,1,1,0)	(1,1,0,0)	(0,0,0,1)	(1,0,0,1)
(0,1,0,0)	(1,1,1,0)	(0,1,1,1)	(1,1,0,1)	**(1,0,0,0)**	(0,0,1,0)	(1,0,1,1)	(0,0,0,1)
(0,1,0,1)	(0,1,1,0)	(1,0,1,1)	(0,0,1,0)	(1,1,1,1)	**(1,0,0,0)**	(1,0,0,1)	(0,1,0,0)
(0,1,1,0)	(0,0,1,1)	(1,1,1,1)	(1,0,1,0)	(0,0,0,1)	(0,1,0,0)	**(1,0,0,0)**	(1,1,0,1)
(0,1,1,1)	(1,0,1,1)	(0,0,1,1)	(0,1,0,1)	(0,1,1,0)	(1,1,1,0)	(1,0,1,0)	**(1,0,0,0)**
(1,0,0,1)	(0,0,0,1)	(0,1,1,0)	(0,1,0,0)	(1,0,1,1)	(0,1,1,1)	(1,1,0,0)	(1,0,1,0)
(1,0,1,0)	(0,1,0,0)	(0,0,1,0)	(1,1,0,0)	(0,1,0,1)	(1,0,1,1)	(1,1,0,1)	(0,0,1,1)
(1,0,1,1)	(1,1,0,1)	(1,1,1,0)	(0,0,1,1)	(0,0,1,0)	(0,0,0,1)	(1,1,1,1)	(0,1,1,0)
(1,1,0,0)	(0,1,1,1)	(1,1,0,1)	(0,1,1,0)	(0,1,0,0)	(1,1,1,1)	(0,1,0,1)	(1,1,1,0)
(1,1,0,1)	(1,1,1,1)	(0,0,0,1)	(1,0,0,1)	(0,0,1,1)	(0,1,0,1)	(0,1,1,1)	(1,0,1,1)
(1,1,1,0)	(1,0,1,0)	(0,1,0,1)	(0,0,0,1)	(1,1,0,1)	(1,0,0,1)	(0,1,1,0)	(0,0,1,0)
(1,1,1,1)	(0,0,1,0)	(1,0,0,1)	(1,1,1,0)	(1,0,1,0)	(0,0,1,1)	(0,1,0,0)	(0,1,1,1)

Аналогично находим таблицы Кэли лупы Q_3^* и Q_4^*. Как показывают таблицы Кэли, для любого элемента лупы Q_i^* при любом $i = 1, 3, 4$ левый и правый обратные элементы совпадают, и в каждом квазиполе Q_i^* выявляются следующие подполя:

$$F_1 = \{0, e, (0,0,0,1), (1,0,0,1)\},\ F_2 = \{0, e, (0,0,1,0), (1,0,1,0)\},$$

$$F_3 = \{0, e, (0,0,1,1), (1,0,1,1)\},\ F_4 = \{0, e, (0,1,0,0), (1,1,0,0)\},$$

$$F_5 = \{0, e, (0,1,0,1), (1,1,0,1)\},\ F_6 = \{0, e, (0,1,1,0), (1,1,1,0)\},$$

$$F_7 = \{0, e, (0,1,1,1), (1,1,1,1)\}.$$

Ясно, что теоретико-множественное объединение семи различных подполей порядка 4 совпадает с Q_i. Окончательно, лупа Q_i^* не однопорождена. □

Построенные Е. Клейнфилдом [21] квазиполя $S_i, 1 \leq i \leq 25$, исчерпывают все, с точностью до изоморфизмов, квазиполя порядка 16 с ядром порядка 4, неизотопные полуполю. Несложно доказывается

Предложение 1.2.4. *Каждое из квазиполей Клейнфилда S_3 и S_{10} имеет элемент порядка 3, не лежащий ни в одном подполе.*

Теорема 1.2.1 опубликована автором в [46].

Теоремы 1.2.2 и 1.2.3 опубликованы в нераздельном соавторстве в статье [47] (соавтор В.М. Левчук).

1.3 Латинские прямоугольники и порождающие последовательности в построении квазиполей Клейнфилда

Е. Клейнфилд [21] разработал в 1960 году алгоритм построения квазиполей порядка 16 с помощью латинских прямоугольников. С его помощью он классифицировал все (с точностью до изоморфизмов) квазиполя порядка 16 с ядром порядка 4.

На самом деле, для построения такого квазиполя Q с левым ядром порядка 4 – как квазиполя ранга 4 над Z_2 – Е. Клейнфилд вначале задает лупу Q^* частью ее таблицы Кэли. Нам потребуется

Определение 1.3.1. *Латинским $r \times n$-прямоугольником при $r \leq n$ называется $r \times n$-матрица, у которой строки являются перестановками первой строки и в каждой строке и в каждом столбце элементы попарно различны.*

Ясно, что таблица Кэли лупы Q^* есть латинский квадрат порядка 15. Первые его три строки заполняются произведениями элементов лупы Q^* на ненулевые элементы из левого ядра. Ключевая 4-ая строка заполняется с помощью введенного понятия *специальной порождающей последовательности*. Как отмечает Е. Клейнфилд [21, стр. 333], для ее выбора и построения латинского 4×15-прямоугольника существует 1264 возможностей, даже если счи-

тать квазиполя. Изоморфными преобразованиями это число удается уменьшить до 76 случаев. В каждом из них 5, 6 и 7-ю строки получаем как сумму 4-й строки, соответственно, с 1, 2 или 3-й строкой.

Теорема 1.3.2. [21, Теорема 2] *Построенная* 7×15*-матрица однозначно определяет таблицу Кэли лупы* Q^* *тогда и только тогда, когда она является латинским* 7×15*-прямоугольником.* $\square$

Таким образом, в [21] построены 75 собственных квазиполей порядка 16 с ядром порядка 4. Из них один изотопный класс составляют 25 попарно неизоморфных квазиполей $S_i,\ 1 \leq i \leq 25$; второй изотопный класс образуют 50 попарно неизоморфных квазиполей $T_i,\ 1 \leq i \leq 50$. Из перечисленных квазиполей полуполями являются только $T_{24},\ T_{25},\ T_{35},\ T_{45}$ и T_{50}.

Как отмечает Е. Клейнфилд, громоздкость вычислений не позволила ему перечислить все квазиполя порядка 16 с ядром порядка 2. Однако, полуполя порядка 16 в [21] классифицированы полностью с помощью специальных порождающих последовательностей. К перечисленным выше добавляются попарно неизоморфные полуполя V_i, $1 \leq i \leq 18$, с ядром порядка 2, образующие один изотопный класс.

Каждый из двух методов Е. Клейнфилда направлен на прямое построение лупы Q^* ненулевых элементов квазиполя Q и существенно отличается от классического метода (см. § 1.2). Итак, в [21] доказана

Теорема 1.3.3. *Собственные полуполя порядка 16 составляют 2 класса изотопных полуполей. Один составляют 5 попарно неизоморфных полуполей* T_{24}, T_{25}, T_{35}, T_{45} *и* T_{50} *с ядром порядка 4, а другой – 18 попарно неизоморфных полуполей* V_i, $1 \leq i \leq 18$, *с ядром порядка 2.* □

1.4 Вопросы В.В. Беляева о латинских прямоугольниках

В этом параграфе отмечаются некоторые известные связи латинских квадратов и проективных плоскостей и приводятся ответы на вопросы о латинских $r \times 6$-прямоугольниках, записанные В.В. Беляевым в 2004 г. для молодых исследователей [1].

Наряду с теоремой 1.3.2 Е. Клейнфилда, связи проективных плоскостей и латинских квадратов изучались в [18], [31] и др. С другой стороны, М. Гориссен [17, Теорема 10] исследовал связь отношения изоморфности проективных плоскостей и отношения изотопности латинских квадратов.

Отметим, что латинский $r \times n$-прямоугольник (определение 1.3.1) является латинским квадратом при $r = n$. Нам потребуется

Определение 1.4.1. *Латинский* $r \times n$*-прямоугольник называется редуцированным, если элементы его 1-й строки расположены по возрастанию, а элементы 1-го столбца возрастают от 1 до* r.

Связи проективных плоскостей и латинских квадратов выявляются в [18], [31] и др. Перечисления латинских квадратов порядка n даже для небольших n представляют собой трудную комби-

наторную задачу. Число R_n редуцированных латинских квадратов порядка $n \leq 5$ вычислили Л. Эйлер [15] и А. Кэли [10]. Другой подход к вычислению тех же чисел использовал П. МакМахон [28], но для R_5 он получил ошибочное значение. Б. МакКей, А. Мейнерт и В. Мирволд [31] отмечают: "История латинских квадратов длинна и наполнена многими опубликованными ошибками". Это вызывает потребность в новых подходах и новых правилах перечисления.

В.В. Беляев записал вопрос о числе L_n латинских квадратов порядков $n = 4, 5, 6$ и вопросы о числе латинских $r \times 6$-прямоугольников для случаев $r = 2, 3, 4$ и 5 (вопросы 1.1 – 1.4 из [1]).

Латинские квадраты порядка ≤ 6 со специальными свойствами выявляются в [31], [6]. Число R_6 исследовал М. Фролов [16], а уточнение дали М. Якобсон и П. Матевс [19] и Е. Шенхард [38]. Исследование Х. Нортона [32] числа R_7 уточняли А. Сэйд [36] и П. Саксена [37]. Далее, значение R_n находили М. Веллс [42] при $n = 8$, С. Баммел и Ж. Ростейн [9] при $n = 9$, Б. МакКей и Е. Рогойский [29] при $n = 10$, наконец, Б. МакКей и И. Ванлес [30] для $n = 11$. Перечисления редуцированных латинских квадратов порядка $4 \leq n \leq 11$ (он единствен, когда $n = 1, 2$ или 3) отражает

Таблица 1.4.1. Число R_n редуцированных латинских квадратов

n	R_n	год
4	4	1782
5	56	1782
6	9408	1890
7	16942080	1948
8	5352281401856	1967
9	377597570964258816	1975
10	7580721483160132811489280	1995
11	536393777327737129811967354077184O	2005

Хорошо известна связь чисел L_n и R_n.

Теорема 1.4.2. *Число L_n всех латинских квадратов порядка n равно $n! \cdot (n-1)! \cdot R_n$.* □

Исследования L_n к настоящему времени отражает

Таблица 1.4.2. Число L_n латинских квадратов порядка n

n	L_n
1	1
2	2
3	12
4	576
5	161280
6	812851200
7	614794199040000
8	108776032459082956800
9	5524751496156892842531225600
10	9982437658213039871725064756920332000
11	776966836171770144107444346734230682311065600000

С использованием компьютерных вычислений, число $R_{r\times n}$ редуцированных латинских $r \times n$-прямоугольников найдено в [31] для $r = 4 \leq n \leq 28$ и $r = 5 \leq n \leq 28$, а ранее Б. МакКей и И. Вонлес [30] получили следующую таблицу.

Таблица 1.4.3. Число $R_{r\times n}$ латинских прямоугольников

$r \times n$	$R_{r\times n}$
2×3	1
2×4	3
3×4	4
2×5	11
3×5	46
4×5	56
2×6	53
3×6	1064
4×6	6552
5×6	9408
2×7	309
3×7	35792
4×7	1293216
5×7	11270400
6×7	16942080

2×8	2119
3×8	1673792
4×8	420909504
5×8	27206658048
6×8	335390189568
7×8	535281401856
2×9	16687
3×9	103443808
4×9	207624560256
5×9	112681643083776
6×9	12952605404381184
7×9	224382697916691456
8×9	377597570964258816
2×10	148329
3×10	8154999232
4×10	147174521059584
5×10	746988383076286464
6×10	870735405591003709440
7×10	1771442969830541859225 60
8×10	429203942159185427300 3520
9×10	758072148316013281148 9280
2×11	1468457
3×11	798030483328
4×11	143968880078466048
5×11	75334923230479020933 12
6×11	96299552373292505158778880
7×11	24012321647517351550217355 2640
8×11	86108204357787266780858343751680
9×11	29059903100338826931139890275942 40
10×11	53639377732773712981196735407718 40

Оценки числа R_n редуцированных латинских квадратов порядка n для случаев $n = 12, 13, 14$ и 15 изучали Б. МакКей и Е. Рогойский [29]. В 2009 году Н.Ю. Кузнецов [24], К. Жанг и Ж. Ма [45] установили более точные оценки, которые резюмирует следующая таблица (через ξ_n обозначается погрешность в процентах оценки R_n).

Таблица 1.4.4. Оценка числа R_n редуцированных латинских квадратов

	C. Zhang – J. Ma	Н.Ю. Кузнецов		
n	R_n	R_n	Интервал	ξ_n
12	$1{,}622 \cdot 10^{44}$	$1{,}612 \cdot 10^{44}$	$(1{,}596 \cdot 10^{44},\ 1{,}629 \cdot 10^{44})$	1
13	$2\ 2{,}514 \cdot 10^{56}$	$2{,}489 \cdot 10^{56}$	$(2{,}465 \cdot 10^{56},\ 2{,}515 \cdot 10^{56})$	1
14	$2{,}332 \cdot 10^{70}$	$2{,}323 \cdot 10^{70}$	$(2{,}3 \cdot 10^{70},\ 2{,}347 \cdot 10^{70})$	1
15	$1{,}516 \cdot 10^{86}$	$1{,}516 \cdot 10^{86}$	$(1{,}499 \cdot 10^{86},\ 1{,}531 \cdot 10^{86})$	1
16	$7{,}898 \cdot 10^{103}$	$8{,}081 \cdot 10^{103}$	$(7{,}92 \cdot 10^{103},\ 8{,}242 \cdot 10^{103})$	2
17	$3{,}768 \cdot 10^{123}$	$3{,}717 \cdot 10^{123}$	$(3{,}642 \cdot 10^{123},\ 3{,}791 \cdot 10^{123})$	2
18	$1{,}869 \cdot 10^{145}$	$1{,}828 \cdot 10^{145}$	$(1{,}773 \cdot 10^{145},\ 1{,}883 \cdot 10^{145})$	3
19	$1{,}073 \cdot 10^{169}$	$1{,}103 \cdot 10^{169}$	$(1{,}059 \cdot 10^{169},\ 1{,}147 \cdot 10^{169})$	4
20	$7{,}991 \cdot 10^{194}$	$7{,}647 \cdot 10^{194}$	$(7{,}264 \cdot 10^{194},\ 8{,}028 \cdot 10^{194})$	5
50	$3{,}06 \cdot 10^{2123}$			
100	$1{,}78 \cdot 10^{11139}$			

Классический результат Ж. Линта и Р. Вильсона [25] дает оценку:

$$\prod_{k=1}^{n}(k!)^{\frac{n}{k}} \geq L_n \geq \frac{(n!)^{2n}}{n^{n^2}}.$$

Установим связь чисел $L_{r\times n}$ и $R_{r\times n}$. Теорему 1.4.2 обобщает

Теорема 1.4.3. *Число $L_{r\times n}$ всех латинских $r \times n$-прямоугольников при $1 \leq r \leq n$ равно*

$$L_{r\times n} = \frac{n!(n-1)!}{(n-r)!} \cdot R_{r\times n}.$$

Доказательство. Зафиксируем редуцированный латинский $r \times n$-прямоугольник. Тогда всевозможные перестановки его строк, кроме первой, дают $(r-1)!$ различных латинских $r \times n$-прямоугольников, у которых первые элементы 2-й, 3-й, $\cdots$, r-й строк образуют множество $\{2, 3, \cdots, r\}$.

Ясно, что мы получаем столько же различных латинских $r \times n$-прямоугольников с аналогичной первой строкой, у которых первые элементы 2-й, 3-й, $\cdots$, r-й строк образуют фиксированное произвольно $(r-1)$-элементное подмножество во множестве $\{2, 3, \cdots, n\}$. Следовательно, число всех латинских $r \times n$-прямоугольников, у которых элементы первой строки расположены по возрастанию, равно

$$\begin{pmatrix} \text{n-1} \\ \text{r-1} \end{pmatrix} \cdot (r-1)! \cdot R_{r\times n} = \frac{(n-1)!}{(n-r)!} \cdot R_{r\times n}.$$

Применяя далее к полученным латинским $r\times n$-прямоугольникам всевозможные $n!$ перестановок столбцов, очевидно, получаем все латинские $r \times n$-прямоугольники. $\square$

Следующая теорема выявляет число $L_{2\times n}$.

Теорема 1.4.4. *Число латинских* $2 \times n$*-прямоугольников равно*

$$L_{2\times n} = (n!)^2 \cdot \sum_{k=2}^{n} \frac{(-1)^k}{k!}.$$

Доказательство. Ясно, что 1-ю строку в латинских $2 \times n$-прямоугольниках можно выбрать $n!$ способами. Фиксируя 1-ю строку, мы сводим задачу выбора второй строки к следующей известной комбинаторной задаче.

Задача о беспорядках. Пусть даны n предметов $a_1, a_2, \cdots, a_n$ и n ячеек $b_1, b_2, ..., b_n$. Какое число N способов возможно для размещения всех предметов одновременно по ячейкам (считаем, что каждая ячейка вмещает один предмет) так, чтобы каждый предмет a_i не попал в ячейку b_i?

По комбинаторной формуле включений и исключений [5, § 2.1] находим:

$$N = n! + \sum_{k=1}^{n} (-1)^k \frac{n!}{k!} = n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!} = n! \cdot (1 - 1 + \frac{1}{2!} - \frac{1}{3!} + ... + \frac{(-1)^k}{n!}).$$

Поэтому число различных латинских $2 \times n$-прямоугольников равно

$$n! \cdot N = n! \cdot n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!} = (n!)^2 \sum_{k=2}^{n} (-1)^k \frac{1}{k!}$$

и теорема доказана. □

Рассмотрим сейчас вопросы 1.1 – 1.4 из [1].

Заметим, что любые две строки произвольного латинского квадрата (аналогично, $r \times n$-прямоугольника с $r \leq n$) образуют латинский $2 \times n$-прямоугольник. С другой стороны, они дают подстановку

n-ой степени, в циклической записи которой нет циклов длины 1, а, следовательно, и циклов длины $n-1$. Зафиксируем произвольный редуцированный латинский прямоугольник.

При $n=4$ второй элемент 2-й строки можно выбирать любым $\neq 2$, и тогда 2-я строка определяется однозначно. Когда этот элемент равен 1, 3-ю строку со вторым элементом 4 можно выбрать двумя способами; в остальных случаях 3-я строка определена выбором второго элемента однозначно. Отсюда $R_{3\times 4}=R_4$ и, с учетом теоремы 1.4.2, получаем $L_4=4!3!\cdot R_4=576$.

При $n=5$ первая строка с любой другой строкой образует подстановку, которая либо циклическая (6 возможностей), либо подстановка с двумя независимыми циклами длины 2 и 3 (5 возможностей). При этом учитываем, что в силу теоремы 1.4.3 имеем,

$$L_{2\times 5}=5280=\frac{R_{2\times 5}\cdot 5!4!}{3!},\quad R_{2\times 5}=11.$$

Аналогичными рассуждениями устанавливаются равенства:

$$R_5=56,\quad L_5=5!4!\cdot R_5=161280.$$

При $n=6$, в силу теорем 1.4.2 и 1.4.3,

$$L_{2\times 6}=190800=\frac{6!5!}{4!}\cdot R_{2\times 6},\quad R_{2\times 6}=53.$$

Таким образом, число возможностей для второй строки равно 53. Из них приводят (вместе с первой строкой):

a) 24 к циклической подстановке вида (12...);

b) 3 к произведению трех (независимых) двойных циклов, включая

(12...);

c) 8 к произведению двух тройных циклов;

d) 18 к подстановке вида (12)(...) или (...)(12...) с четверным циклом.

Оказывается, при любом выборе редуцированного латинского 2×6-прямоугольника в случаях a), b) и d) существует точно 20 способов присоединения 3-й строки до редуцированного латинского 3×6-прямоугольника, то есть $(24 + 18 + 3) \cdot 20 = 900$ всего. Аналогично, в случае c): ровно 3 таких подстановки имеют по 19 способов присоединения 3-й строки, 3 - по 21 способу и 2 - по 22 способа. Таким образом получаем $3 \cdot 19 + 3 \cdot 21 + 2 \times 22 = 164$. Нетрудно посчитать число латинских $R_{3\times 6} = 900 + 164 = 1064$.

Непосредственное перечисление показывает, что общее число возможных вариантов присоединения 3-й строки к первым двум, образующим подстановки типов a), b) и d) равно 80, в случае c) - 82. Это дает ответ на вопрос 1.3 В.В. Беляева.

Число $L_{3\times 6}$ латинских 3×6-прямоугольников, полученных добавлением 3-й строки к первым двум, образующим подстановку первого типа, равно 9440. При этом имеем 4248, 472, 1534 и 3186 случаев, когда 2-я и 3-я строки образуют подстановку, соответственно, первого, второго, третьего или четвертого типа. Добавлением 3-й строки, когда 1-я и 2-я образуют подстановку второго типа, дает 1200 случаев. Из них имеем 540, 60, 180 и 420 случаев, когда 2-я и 3-я строки образуют подстановку, соответственно, первого, второго, третьего или четвертого типа. Аналогично, если 1-я и 2-я строки образуют подста-

новку третьего типа, то 3-ю строку можно добавить 3280 способами. Из них 1600, 240, 400 и 1040 случаев, когда 2-я и 3-я строки образуют подстановку, соответственно, первого, второго, третьего или четвертого типа. Если 1-я и 2-я строки образуют подстановку четвертого типа, то 3-ю строку можно добавить 7360 способами. Из них 3312, 368, 1104 и 2576 случаев, когда 2-я и 3-я строки образуют подстановку, соответственно, первого, второго, третьего или четвертого типа. Отсюда получаем равенство $L_{3\times 6} = 15321600$. По теореме 1.4.3,

$$L_{3\times 6} = 15321600 = \frac{6!5!}{3!} \cdot R_{3\times 6}, \quad R_{3\times 6} = 1064.$$

Присоединим 4-ю строку к перечисленным латинским 3×6-прямоугольникам. Если 2-я и 3-я строки образуют подстановку первого типа, то в каждом случае 4-ю строку можно задать только 20 вариантами; во всех остальных случаях 4-ю строку можно задать 17, 18, 19, 20 или 21 способами. Таким образом, с учетом теоремы 1.4.3, получаем:

$$L_{4\times 6} = 283086400 = \frac{6!5!}{2!} \cdot R_{4\times 6}, \quad R_{4\times 6} = 6552.$$

Для дальнейшего построения определяем число циклов типов a), b), c), d) в подстановке, образованной 3-й и 4-й строками. Число возможностей задания 5-й строки в случаях латинских 5×6-прямоугольниках первого, второго и четвертого типов равно 2 или 4, а в случае третьего типа - 2, 4 или 8. Итак,

$$L_{5\times 6} = 812851200 = \frac{6!5!}{1!} \cdot R_{5\times 6}, \quad R_{5\times 6} = 9408.$$

6-я строка задается однозначно, так что число латинских квадратов порядка 6 равно 812851200; это ответ на вопрос 1.4 В.В. Беляева.

Перечислим редуцированные латинские квадраты порядка $n = 6$. Число возможностей выбора 2-й строки равно 53. Полученные 2×6 редуцированные латинские прямоугольники можно представлять циклическими подстановками с наборами длин циклов:

a) 6 – 24 подстановки; b) 2,2,2 – 2 подстановки;

c) 3, 3 – 8 подстановок; d) 2, 4 – 19 подстановок.

Соответственно получаем:

$$\begin{bmatrix} 1&2&3&4&5&6\\ 2&1&4&6&3&5 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&1&4&3&6&5 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&1&4&5&6&3 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&1&5&6&3&4 \end{bmatrix},$$

$$\begin{bmatrix} 1&2&3&4&5&6\\ 2&1&5&6&4&3 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&1&5&3&6&4 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&1&6&5&3&4 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&1&6&3&4&5 \end{bmatrix},$$

$$\begin{bmatrix} 1&2&3&4&5&6\\ 2&1&6&5&4&3 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&3&1&6&4&5 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&3&1&5&6&4 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&3&4&5&6&1 \end{bmatrix},$$

$$\begin{bmatrix} 1&2&3&4&5&6\\ 2&3&4&5&1&5 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&3&4&1&6&5 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&3&5&1&6&4 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&3&5&6&1&4 \end{bmatrix},$$

$$\begin{bmatrix} 1&2&3&4&5&6\\ 2&3&5&6&4&1 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&3&6&1&4&5 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&3&6&5&1&4 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&3&6&5&4&1 \end{bmatrix},$$

$$\begin{bmatrix} 1&2&3&4&5&6\\ 2&4&1&3&6&5 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&4&1&5&6&3 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&4&1&6&3&5 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&4&5&1&6&3 \end{bmatrix},$$

$$\begin{bmatrix} 1&2&3&4&5&6\\ 2&4&5&3&6&1 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&4&5&6&1&3 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&4&5&6&3&1 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&4&6&1&3&5 \end{bmatrix},$$

$$\begin{bmatrix} 1&2&3&4&5&6\\ 2&4&6&3&1&5 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&4&6&5&1&3 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&4&6&5&3&1 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&5&1&3&6&4 \end{bmatrix},$$

$$\begin{bmatrix} 1&2&3&4&5&6\\ 2&5&1&6&3&4 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&5&1&6&4&3 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&5&4&1&6&3 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&5&4&3&6&1 \end{bmatrix},$$

$$\begin{bmatrix} 1&2&3&4&5&6\\ 2&5&4&6&1&3 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&5&4&6&3&1 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&5&6&1&3&4 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&5&6&1&4&3 \end{bmatrix},$$

$$\begin{bmatrix} 1&2&3&4&5&6\\ 2&5&6&3&1&4 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&5&6&3&4&1 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&6&1&3&4&5 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&6&1&5&4&3 \end{bmatrix},$$

$$\begin{bmatrix} 1&2&3&4&5&6\\ 2&6&1&5&3&4 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&6&4&1&3&5 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&6&4&3&1&5 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&6&4&5&1&3 \end{bmatrix},$$

$$\begin{bmatrix} 1&2&3&4&5&6\\ 2&6&4&5&3&1 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&6&5&1&3&4 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&6&5&1&4&3 \end{bmatrix}, \begin{bmatrix} 1&2&3&4&5&6\\ 2&6&5&3&1&4 \end{bmatrix},$$

$$\begin{bmatrix} 1&2&3&4&5&6\\ 2&6&5&3&4&1 \end{bmatrix}.$$

Каждый редуцированный латинский 2×6-прямоугольник типов a), b) или d) имеет по 20 вариантов присоединения 3-й строки, а для типа c) - 19, 21 или 22 варианта. Таким образом,

$$R_{3\times 6} = 1064.$$

Ниже приведены результаты отдельно для некоторых видов подстановок (перечисляются после отдельной линии).

Тип a)	Тип b)	Тип d)
1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6
2 3 4 5 6 1	2 1 4 3 6 5	2 1 4 6 3 5
3 1 2 6 4 5	3 4 5 6 1 2	3 4 1 5 6 2
3 1 5 6 2 4	3 4 5 6 2 1	3 4 2 5 6 1
3 1 5 6 4 2	3 4 6 5 1 2	3 4 5 1 6 2
3 1 6 2 4 5	3 4 6 5 2 1	3 4 5 2 6 1
3 4 1 6 2 5	3 5 1 6 2 4	3 4 6 5 1 2
3 4 2 6 1 5	3 5 1 6 4 2	3 4 6 5 2 1
3 4 5 6 1 2	3 5 2 6 1 4	3 5 1 2 6 4
3 4 6 1 2 5	3 5 2 6 4 1	3 5 2 1 6 4
3 4 6 2 1 5	3 5 6 1 2 4	3 5 6 1 2 4
3 5 1 6 2 4	3 5 6 1 4 2	3 5 6 1 4 2
3 5 1 6 4 2	3 5 6 2 1 4	3 5 6 2 1 4
3 5 1 6 1 4	3 5 6 2 4 1	3 5 6 2 4 1
3 5 6 1 2 4	3 6 1 5 2 4	3 6 1 5 2 4
3 5 6 1 4 2	3 6 1 5 4 2	3 6 1 5 4 2
3 5 6 2 1 4	3 6 2 5 1 4	3 6 2 5 1 4
3 6 1 2 4 5	3 6 2 5 4 1	3 6 2 5 4 1
3 6 2 1 4 5	3 6 5 1 2 4	3 6 5 1 2 4
3 6 5 1 2 4	3 6 5 1 4 2	3 6 5 1 4 2
3 6 5 1 4 2	3 6 5 2 1 4	3 6 5 2 1 4
3 6 5 2 1 4	3 6 5 2 4 1	3 6 5 2 4 1

Аналогично перечисляем варианты выбора 3-х строк для типа c). Для дальнейшего присоединения 4-й строки необходимо разбить множество полученных редуцированных латинских 3×6-прямоугольников на подмножества, в каждом из которых 1-я и 3-я строки образуют подстановку описанных выше типов. Число способов присоединения 4-й строки для латинских 3×6-прямоугольников равно 5 для типов a), c) и d), и равно 5, 6 или 8 для b). Таким образом, $R_{4\times 6} = 6552$.

Число возможных вариантов присоединения 5-й строки равно 2 или 4 независимо от циклической записи подстановки, образованной 1 и 4 строками. Поэтому $R_{5\times 6} = 9408$.

Ниже приведены примеры присоединения 4-й и 5-й строк (перечисляются после отдельной линии) для различных типов подстановок.

Примеры присоединения четвертой строки для типов a), b), c):

Тип a)	Тип b)	Тип c)
1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6
2 1 4 3 6 5	2 1 4 3 6 5	2 1 4 3 6 5
3 4 5 6 2 1	3 5 1 6 2 4	3 4 5 6 1 2
4 3 6 5 1 2	4 3 6 5 1 2	4 3 6 5 2 1
4 5 6 1 3 2	4 6 2 5 1 3	4 5 6 1 2 3
4 5 6 2 1 3	4 6 2 5 3 1	4 5 6 2 3 1
4 6 1 5 3 2	4 6 5 1 3 2	4 6 1 5 2 3
4 6 2 5 1 3	4 6 5 2 1 3	4 6 2 5 3 1
	4 6 5 2 3 1	

Примеры присоединения пятой строки:

Тип a)	Тип b)	Тип c)	Тип d)
1 2 3 4 5 6		1 2 3 4 5 6	
2 1 4 3 6 5	1 2 3 4 5 6	2 1 4 3 6 5	1 2 3 4 5 6
3 4 5 6 1 2	2 1 4 3 6 5	3 4 5 6 1 2	2 1 4 3 6 5
4 3 6 5 2 1	3 5 1 6 2 4	4 3 5 6 2 1	3 4 5 6 1 2
5 6 1 2 3 4	4 6 5 1 3 2	5 6 1 2 3 4	4 5 6 1 2 3
5 6 1 2 4 3	5 3 6 2 4 1	5 6 1 2 4 3	5 6 1 2 3 4
5 6 2 1 3 4	5 4 6 2 1 3	5 6 2 1 3 4	5 6 2 1 3 4
5 6 2 1 4 3		5 6 2 1 4 3	

Ясно, что последняя строка определяется однозначно и поэтому

$$R_6 = 9408.$$

Вопросы 1.5 - 1.10 В.В. Беляева [1] заключаются в определении числа классов RC- и RCN- эквивалентных латинских квадратов порядков $n = 4, 5, 6$ и чисел редуцированных латинских квадратов в каждом эквивалентном классе. Нам потребуются определения.

Определение 1.4.5. *Два латинских квадрата называют R-(аналогично, C- или N-) эквивалентными, если любой из них получается из другого перестановками строк (соответственно, столбцов или элементов).*

Рассмотрим подробно преобразования RC- и RCN- эквивалентных латинских квадратов порядка $n = 4$. Для этого удобнее рассмотреть сначала более простые R- и C- преобразования.

Изучение R- и C- преобразований позволило построить 24 класса R-эквивалентных латинских квадратов порядка $n = 4$, и столько же C-эквивалентных классов. Каждый найденный класс имеет мощность 24. Оказалось, что некоторые латинские квадраты порядка 4 лежат одновременно и в R- и в C- эквивалентных классах. Значит, они образуют один RC-эквивалентный класс. Так как RC-преобразование - это одновременная перестановка строк и столбцов латинского квадрата, то некоторые R- и C- эквивалентные классы будут совпадать. Отсюда последовательно получаем следующие два предложения.

Предложение 1.4.6. *Полная система латинских квадратов порядка 4 имеет точно 4 RC-эквивалентных класса. Мощности классов равны 144, причем каждый класс RC-эквивалентности содержит точно 1 редуцированный латинский квадрат.*

Предложение 1.4.7. *Число классов RC-эквивалентных латинских квадратов порядка n совпадает с числом R_n.*

Доказательство. Ясно, что перестановки строк и столбцов не могут преобразовать редуцированный латинский квадрат в новый редуцированный латинский квадрат. Следовательно, в каждом RC-эквивалентном классе редуцированный латинский квадрат единственный. □

В силу предложения 1.4.7, число RC-эквивалентных классов латинских квадратов порядков $n = 5, 6$ равны 56 и 9408, соответственно. Для определения мощности RC-эквивалентных классов латинских квадратов порядков $n = 5, 6$ достаточно знать число редуцированных латинских квадратов заданных порядков. Нетрудно подсчитать, что эти мощности равны для $n = 5$ и $n = 6$, соответственно

$$\frac{L_5}{R_5} = \frac{161280}{56} = 2880 \quad \text{и} \quad \frac{L_6}{R_6} = \frac{812851200}{9408} = 86400$$

Таким образом, завершается ответ на вопрос 1.7 В.В. Беляева. Ответ на вопрос 1.8 явно следует из теоремы 1.4.2 и предложения 1.4.7.

Решение вопроса 1.6 из [1] об определении принадлежности двух латинских квадратов к одному RC-эквивалентному классу дает

Предложение 1.4.8. *Два латинских квадрата любого фиксированного порядка n лежат в одном RC-эквивалентном классе, если они приводятся к одному и тому же редуцированному виду.*

Понятно, что RCN-преобразования включают все RC-преобразования. Поэтому для определения числа классов RCN-эквивалентных латинских квадратов порядка n достаточно работать с RC-эквивалентными классами. Для установления принадлежности двух латинских квадратов из разных RC-эквивалентных классов к одному RCN-эквивалентному классу достаточно установить RCN-эквивалентность любого квадрата из одного RC-эквивалентного класса с квадратом из другого RC-эквивалентного класса.

Предложения 1.4.7, 1.4.8 и следующие 2 предложения дают ответ на вопросы 1.5, 1.9 и 1.10 из [1].

Предложение 1.4.9. *Все латинские квадраты порядка $n = 4$ образуют единственный RCN-эквивалентный класс.*

Предложение 1.4.10. *Латинские квадраты порядка $n = 5$ образуют 2 RCN-эквивалентных класса, мощности классов одинаковые и равны 80640.*

Заметим, что перечисление редуцированных латинских квадратов порядков $n = 4, 5, 6$ дает перечисление RC-эквивалентных классов латинских квадратов тех же порядков. Это завершает исследование последнего вопроса 1.9 из [1].

Решение вопросов В.В. Беляева опубликовано автором в [49].

2 Строение полуполей порядков 16 и 32

Согласно Е. Клейнфилду [21], число всех, с точностью до изоморфизмов, собственных полуполей порядка 16 равно 23. В главе 2 вопросы **(A)** – **(B)** решаются в § 2.2 для всех полуполей порядка 16 (теоремы 2.2.2 – 2.2.4 и таблица 2.2.5). Предварительно в § 2.1 показывается, что с точностью до изоморфизмов и антиизоморфизмов, число полуполей порядка 16 равно 16 (теорема 2.1.1) и выписаны формулы умножения.

Основная теорема 2.4.1 в § 2.4 показывает, что для опровергающего гипотезу Г. Венэ полуполя Кнута – Руа (не являющегося правоциклическим) лупа ненулевых элементов однопорождена.

С помощью известных регулярных множеств проективных плоскостей трансляций (У. Демпвольф и Р. Рокенфеллер, 2011 г.), в § 2.3 выписаны представители всех изотопных классов собственных полуполей порядка 32. Их строение выявляют теоремы 2.3.2 и 2.3.3.

2.1 Формулы умножения полуполей Клейнфилда

Перечисленные Е. Клейнфилдом собственные полуполя порядка 16 (теорема 1.3.3 в § 1.3) образуют два изотопных класса, составленные из 18 и 5 попарно не изоморфных полуполей с ядрами порядков 2 и 4, соответственно. Явные формулы умножения двух представителей изотопных классов полуполей указал Д. Кнут [22], [23].

Для исследования строения мы находим в этом параграфе формулы умножения всех 23-х Клейнфилдовых полуполей, а также их перечисление, с точностью до изоморфизмов и антиизоморфизмов.

Теорема 2.1.1. *Всякое собственное полуполе порядка 16, с точностью до изоморфизмов, есть либо одно из 9-и полуполей* $V_2, V_{10}, V_{12}, V_{13}, V_{17}, V_{18}, T_{24}, T_{35}, T_{45}$, *либо одно из 7-и полуполей* $V_1, V_3, V_4, V_8, V_{11}, V_{15}, T_{25}$ *или одно из противоположных к ним полуполей* $V_6, V_7, V_5, V_9, V_{14}, V_{16}, T_{50}$, *соответственно.*

Напомним, что для любого кольца $R = (R, +, \cdot)$ *противоположное кольцо* $R^{op} = (R, +, \circ)$ получают, полагая $a \circ b = b \cdot a$ $(a, b \in R)$. (Аналогично определяют противоположные квазиполя.)

Для получения формул умножения и доказательства теоремы установим соответствие между полуполями Е. Клейнфилда и регулярными множествами проективных полуполевых плоскостей.

С помощью компьютерных вычислений Д. Кнут в работах [22] и [23] подтверждает результат Е. Клейнфилда: *число недезарговых полуполевых плоскостей порядка 16 равно двум и обе они координати-*

зируются полуполями, содержащими поле $GF(4) = \{0, 1, \omega, \omega^2\}$. Для указанных полуполей Д. Кнут [23] записал явно умножения:

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

$$(u, v) \circ (x, y) = (ux + \omega v^2 y, vx + u^2 y) \quad (u, v, x, y \in GF(4)).$$

Мы используем классический способ построения полуполей, основанный на перечислении полуполевых плоскостей и восстановлении полуполя с помощью регулярного множества и умножения (1.1) (см. § 1.1). Всякая такая плоскость π имеет ранг 4 над Z_2 и координатизируется 4-х мерным пространством W над Z_2. Регулярное множество $R = \theta(W)$ можно определять биективным (или Z_2-линейным) отображением $\theta : W \to M(4, Z_2)$, тождественным на $(1, 0, 0, 0)$. В общем случае, для подходящих линейных функций b_{ij}, c_{ij}, d_{ij} $(2 \le i \le 4,\ 1 \le j \le 4)$ от x_1, x_2, x_3, x_4 имеем:

$$\theta(x_1, x_2, x_3, x_4) = x_1 \cdot E + x_2 \cdot B + x_3 \cdot C + x_4 \cdot D \quad (B, C, D \in GL(4, Z_2)), \quad (2.1)$$

$$B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix}, \ C = \begin{pmatrix} 0 & 0 & 1 & 0 \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix}, \ D = \begin{pmatrix} 0 & 0 & 0 & 1 \\ d_{21} & d_{22} & d_{23} & d_{24} \\ d_{31} & d_{32} & d_{33} & d_{34} \\ d_{41} & d_{42} & d_{43} & d_{44} \end{pmatrix}.$$

В качестве базы полуполей $T_{24}, T_{25}, T_{35}, T_{45}$ и T_{50} над $Z_2 e$ Е. Клейнфилд выбирает векторы

$$(0, 0, 0, 1) = 1,\ (0, 0, 1, 0) = c,\ (0, 1, 0, 0) = b,\ (1, 0, 0, 0) = a.$$

Заметим, что если в каких-то базах двух полуполей таблицы Кэли лупы ненулевых элементов совпадают, то полуполя изоморфны. Для наших построений мы используем базу

$$(1,0,0,0) = 1', \ \ (0,1,0,0) = a', \ \ (0,0,1,0) = b', \ \ (0,0,0,1) = c'.$$

Рассмотрим подробно случай полуполя Е. Клейнфилда T_{24}. Метод Е. Клейнфилда [21], основанный на латинских прямоугольниках (см. также §1.3), позволяет восстановить таблицу Кэли лупы T_{24}^* (умножение на единичный элемент $e = (0,0,0,1)$ опускаем):

Таблица 2.1.1. Таблица Кэли лупы T_{24}^*

	(0,0,1,0)	**(0,0,1,1)**	**(0,1,0,0)**	**(0,1,0,1)**	**(0,1,1,0)**	**(0,1,1,1)**	**(1,0,0,0)**
(0,0,1,0)	(0,0,1,0)	(0,0,0,1)	(1,0,0,0)	(1,0,1,0)	(1,0,1,1)	(1,0,0,1)	(1,1,0,0)
(0,0,1,1)	(0,0,0,1)	(0,0,1,0)	(1,1,0,0)	(1,1,1,1)	(1,1,0,1)	(1,1,1,0)	(0,1,0,0)
(0,1,0,0)	(1,1,0,1)	(1,0,0,1)	(1,0,1,0)	(1,1,1,0)	(0,1,1,1)	(0,0,1,1)	(1,0,1,1)
(0,1,0,1)	(1,1,1,1)	(1,0,1,0)	(1,1,1,0)	(1,0,1,1)	(0,0,0,1)	(0,1,0,0)	(0,0,1,1)
(0,1,1,0)	(1,1,1,0)	(1,0,0,0)	(0,0,1,0)	(0,1,0,0)	(1,1,0,0)	(1,0,1,0)	(0,1,1,1)
(0,1,1,1)	(1,1,0,0)	(1,0,1,1)	(0,1,1,0)	(0,0,0,1)	(1,0,1,0)	(1,1,0,1)	(1,1,1,1)
(1,0,0,0)	(0,1,1,0)	(1,1,1,0)	(1,1,1,1)	(0,1,1,1)	(1,0,0,1)	(0,0,0,1)	(1,1,0,1)
(1,0,0,1)	(0,1,0,0)	(1,1,0,1)	(1,0,1,1)	(0,0,1,0)	(1,1,1,1)	(0,1,1,0)	(0,1,0,1)
(1,0,1,0)	(0,1,0,1)	(1,1,1,1)	(0,1,1,1)	(1,1,0,1)	(0,0,1,0)	(1,0,0,0)	(0,0,0,1)
(1,0,1,1)	(0,1,1,1)	(1,1,0,0)	(0,0,1,1)	(1,0,0,0)	(0,1,0,0)	(1,1,1,1)	(1,0,0,1)
(1,1,0,0)	(1,0,1,1)	(0,1,1,1)	(0,1,0,1)	(1,0,0,1)	(1,1,1,0)	(0,0,1,0)	(0,1,1,0)
(1,1,0,1)	(1,0,0,1)	(0,1,0,0)	(0,0,0,1)	(1,1,0,0)	(1,0,0,0)	(0,1,0,1)	(1,1,1,0)
(1,1,1,0)	(1,0,0,0)	(0,1,1,0)	(1,1,0,1)	(0,0,1,1)	(0,1,0,1)	(1,0,1,1)	(1,0,1,0)
(1,1,1,1)	(1,0,1,0)	(0,1,0,1)	(1,0,0,1)	(0,1,1,0)	(0,0,1,1)	(1,1,0,0)	(0,0,1,0)

	(1,0,0,1)	**(1,0,1,0)**	**(1,0,1,1)**	**(1,1,0,0)**	**(1,1,0,1)**	**(1,1,1,0)**	**(1,1,1,1)**
(0,0,1,0)	(1,1,1,0)	(1,1,1,1)	(1,1,0,1)	(0,1,0,0)	(0,1,1,0)	(0,1,1,1)	(0,1,0,1)
(0,0,1,1)	(0,1,1,1)	(0,1,0,1)	(0,1,1,0)	(1,0,0,0)	(1,0,1,1)	(1,0,0,1)	(1,0,1,0)
(0,1,0,0)	(1,1,1,1)	(0,1,1,0)	(0,0,1,0)	(0,0,0,1)	(0,1,0,1)	(1,1,0,0)	(1,0,0,0)
(0,1,0,1)	(0,1,1,0)	(1,1,0,0)	(1,0,0,1)	(1,1,0,1)	(1,0,0,0)	(0,0,1,0)	(0,1,1,1)
(0,1,1,0)	(0,0,0,1)	(1,0,0,1)	(1,1,1,1)	(0,1,0,1)	(0,0,1,1)	(1,0,1,1)	(1,1,0,1)
(0,1,1,1)	(1,0,0,0)	(0,0,1,1)	(0,1,0,0)	(1,0,0,1)	(1,1,1,0)	(0,1,0,1)	(0,0,1,0)
(1,0,0,0)	(0,1,0,1)	(1,0,1,1)	(0,0,1,1)	(0,0,1,0)	(1,0,1,0)	(0,1,0,0)	(1,1,0,0)
(1,0,0,1)	(1,1,0,0)	(0,0,0,1)	(1,0,0,0)	(1,1,1,0)	(0,1,1,1)	(1,0,1,0)	(0,0,1,1)
(1,0,1,0)	(1,0,1,1)	(0,1,0,0)	(1,1,1,0)	(0,1,1,0)	(1,1,0,0)	(0,0,1,1)	(1,0,0,1)
(1,0,1,1)	(0,0,1,0)	(1,1,1,0)	(0,1,0,1)	(1,0,1,0)	(0,0,0,1)	(1,1,0,1)	(0,1,1,0)
(1,1,0,0)	(1,0,1,0)	(1,1,0,1)	(0,0,0,1)	(0,0,1,1)	(1,1,1,1)	(1,0,0,0)	(0,1,0,0)
(1,1,0,1)	(0,0,1,1)	(0,1,1,1)	(1,0,1,0)	(1,1,1,1)	(0,0,1,0)	(0,1,1,0)	(1,0,1,1)
(1,1,1,0)	(0,1,0,0)	(0,0,1,0)	(1,1,0,0)	(0,1,1,1)	(1,0,0,1)	(1,1,1,1)	(0,0,0,1)
(1,1,1,1)	(1,1,0,1)	(1,0,0,0)	(0,1,1,1)	(1,0,1,1)	(0,1,0,0)	(0,0,0,1)	(1,1,1,0)

С помощью таблицы 2.1.1 нетрудно построить таблицу умножения базисных элементов Е. Клейнфилда полуполя T_{24}:

Таблица 2.1.2. Таблица умножения базиса Клейнфилда лупы T_{24}^*

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	a+b+1	a+b+c+1	b+c
b	b	a+c+1	a+c	a+b+1
c	c	a+b	a	c+1

Умножение $\circ$ элементов нового базиса считаем совпадающим с умножением в таблице 2.1.2. Тогда соотношение

$$a' \circ a' = a' \cdot \theta(a') = (0,1,0,0) \cdot \begin{pmatrix} 0 & 1 & 0 & 0 \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix}$$

$$= (b_{21}, b_{22}, b_{23}, b_{24}) = a' + b' + 1' = (1,1,1,0)$$

сразу определяет вторую строку матрицы B из (2.1) регулярного множества полуполевой плоскости. Аналогично, равенство

$$b' \circ a' = b' \cdot \theta(a') = (0,0,1,0) \cdot \begin{pmatrix} 0 & 1 & 0 & 0 \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix}$$

$$= (b_{31}, b_{32}, b_{33}, b_{34}) = a' + c' + 1' = (1,1,0,1)$$

дает третью строку матрицы B. 4-ю строку находим из равенства

$$c' \circ a' = (0,0,0,1) \cdot \begin{pmatrix} 0 & 1 & 0 & 0 \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix} = (b_{41}, b_{42}, b_{43}, b_{44}) = a' + b' = (0,1,1,0).$$

Аналогично, матрицу C из (2.1) дают соотношения

$$a' \circ b' = (0,1,0,0) \cdot \begin{pmatrix} 0 & 0 & 1 & 0 \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix} = (c_{21}, c_{22}, c_{23}, c_{24}) = a' + b' + c' + 1' = (1,1,1,1),$$

$$b' \circ b' = (0,0,1,0) \cdot \begin{pmatrix} 0 & 0 & 1 & 0 \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix} = (c_{31}, c_{32}, c_{33}, c_{34}) = a' + c' = (0,1,0,1),$$

$$c' \circ b' = (0,0,0,1) \cdot \begin{pmatrix} 0 & 0 & 1 & 0 \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix} = (c_{41}, c_{42}, c_{43}, c_{44}) = a' = (0,1,0,0),$$

а матрицу D – соотношения

$$a' \circ c' = (0,1,0,0) \cdot \begin{pmatrix} 0 & 0 & 0 & 1 \\ d_{21} & d_{22} & d_{23} & d_{24} \\ d_{31} & d_{32} & d_{33} & d_{34} \\ d_{41} & d_{42} & d_{43} & d_{44} \end{pmatrix} = (d_{21}, d_{22}, d_{23}, d_{24}) = b' + c' = (0,0,1,1),$$

$$b' \circ c' = (0,0,1,0) \cdot \begin{pmatrix} 0 & 0 & 0 & 1 \\ d_{21} & d_{22} & d_{23} & d_{24} \\ d_{31} & d_{32} & d_{33} & d_{34} \\ d_{41} & d_{42} & d_{43} & d_{44} \end{pmatrix} = (d_{31}, d_{32}, d_{33}, d_{34}) = a' + b' + 1' = (1,1,1,0),$$

$$c' \circ c' = (0,0,0,1) \cdot \begin{pmatrix} 0 & 0 & 0 & 1 \\ d_{21} & d_{22} & d_{23} & d_{24} \\ d_{31} & d_{32} & d_{33} & d_{34} \\ d_{41} & d_{42} & d_{43} & d_{44} \end{pmatrix} = (d_{41}, d_{42}, d_{43}, d_{44}) = c' + 1' = (1,0,0,1).$$

В силу (2.1), регулярное множество соответствующей полуполевой плоскости принимает вид:

$$\theta(x,y,z,w) = \begin{pmatrix} x & y & z & w \\ y+z & x+y+z & y+z+w & z+w \\ y+w & y+z+w & x+w & y+z \\ w & y+z & y & x+w \end{pmatrix} \quad (x,y,z,w \in Z_2).$$

Отсюда и из (1.1) получаем формулу умножения в полуполе T_{24}:

$$(a,b,c,d) \circ (x,y,z,w) = (ax+by+bz+cy+cw+dw,$$

$$ay+bx+by+bz+cy+cz+cw+dy+dz,$$

$$az+by+bz+bw+cx+cw+dy, aw+bz+bw+cy+cz+dx+dw).$$

Аналогичным образом выписываем явные умножения других полуполей Клейнфилда T_i из [21].

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	c	a+b+c+1	b+c
b	b	1	a+c	a+b+1
c	c	a+b	a	c+1

$T_{25}:\ (a,b,c,d) \circ (x,y,z,w) = (ax+by+cz+cw+dw, ay+bx+by+cw+dz,$

$$az+bw+cx+cy+cz+cw+dy+dw, aw+bz+bw+cy+cw+dx+dz).$$

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	a+c	c+1	b+c
b	b	b+1	c	a+b+1
c	c	a+b	a	c+1

$T_{35}:\quad (a,b,c,d) \circ (x,y,z,w) = (ax+bz+cy+cw+dw, ay+bx+by+cw+dy+dz,$

$$az+bw+cx+cy+cw+dy, aw+by+bz+bw+cz+dw).$$

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	a+1	a+b+c+1	a+b+1
b	b	b+c+1	a+c	a+c+1
c	c	a+b	a	c+1

$$T_{45}: \quad (a,b,c,d)\circ(x,y,z,w) = (ax+by+bz+bw+cy+cw+dw,$$

$$ay+bx+by+bz+bw+cz+cw+dy+dz, az+bz+bw+cx+cy+dy,$$

$$aw+bz+cy+cz+cw+dw).$$

Оставшееся полуполе T_{50} изоморфно полуполю T_{25}^{op}.

Обозначение $\{1,c,b,a\}$ базисного набора Е. Клейнфилда заменяем для полуполей V_i $(1 \le i \le 18)$ набором $\{1,a,b,c\}$. С учетом этой замены, находим формулы умножения полуполей V_i.

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	b+1
b	b	a+c	a+1	b+c
c	c	a+b+c+1	1	a+c

$$V_1: \ (a,b,c,d)\circ(x,y,z,w) = (ax+bw+cz+dy+dz, ay+bx+cy+cz+dy+dw,$$

$$az+by+bw+cx+cw+dy, aw+bz+cy+cw+dx+dy+dw).$$

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	a+1
b	b	b+c	b+1	a+c
c	c	a+b+c+1	a+c+1	b+c+1

$$V_2: \ (a,b,c,d)\circ(x,y,z,w) = (ax+bw+cz+dy+dz+dw, ay+bx+bw+cw+dy+dz,$$

$$az+by+bw+cx+cy+cz+dy+dw, aw+bz+cy+cw+dx+dy+dz+dw).$$

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	c+1
b	b	b+c+1	a+1	b+c
c	c	a+c	c+1	a+b+c

$$V_3: \ (a,b,c,d)\circ(x,y,z,w) = (ax+bw+cy+cz+dz, ay+bx+cz+dy+dw,$$

$$az+by+cx+cy+cw+dw, aw+bz+bw+cy+cw+dx+dy+dz+dw).$$

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	a+b+c+1
b	b	b+c+1	a+b	a+1
c	c	b+c	c+1	a+c

$$V_4 : \ (a,b,c,d) \circ (x,y,z,w) = (ax + bw + cy + cw + dz, ay + bx + bw + cz + cw + dw,$$

$$az + by + bw + cx + cy + cz + dy, aw + bz + bw + cy + dx + dy + dz + dw).$$

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	a+b+c+1
b	b	a+c	b+1	a+b
c	c	1	a+c	b

$$V_8 : \ (a,b,c,d) \circ (x,y,z,w) = (ax + bw + cz + dy, ay + bx + bw + cy + cw + dz,$$

$$az + by + bw + cx + cz + cw + dw, aw + bz + bw + cy + dx + dz).$$

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	b+1
b	b	c+1	a+b+1	a+b+c+1
c	c	a+b+1	a+c	c+1

$$V_{10} : \ (a,b,c,d) \circ (x,y,z,w) = (ax + bw + cy + cz + cw + dy + dw, ay + bx + cz + cw + dy + dz,$$

$$az + by + bw + cx + cz + cw + dy, aw + bz + cy + cw + dx + dz + dw).$$

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	a+1
b	b	c	a+b+c+1	a+c
c	c	c+1	a+c	b+1

$$V_{11} : \ (a,b,c,d) \circ (x,y,z,w) = (ax + bw + cz + dy + dw, ay + bx + bw + cz + cw + dz,$$

$$az + by + cx + cz + dw, aw + bz + cy + cz + cw + dx + dy + dz).$$

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	a+b+c+1
b	b	a+c	a+1	a+b
c	c	c+1	a+b+c	b+c+1

$$V_{12} : \ (a,b,c,d) \circ (x,y,z,w) = (ax + bw + cz + dy + dw, ay + bx + bw + cy + cz + cw + dz,$$

$$az + by + bw + cx + cw + dz + dw, aw + bz + bw + cy + dx + dy + dz + dw).$$

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	a+1
b	b	a+b+c	b+1	a+b+1
c	c	c+1	a+c	b+1

$V_{13}: \ (a,b,c,d)\circ(x,y,z,w) = (ax+bw+cz+cw+dy+dw, ay+bx+bw+cy+cw+dz,$

$az+by+cx+cy+cz+cw+dw, aw+bz+cy+dy+dz).$

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	b+1
b	b	a+c	a+b+c+1	a+b+1
c	c	a+b+1	a+c	c+1

$V_{15}: \ (a,b,c,d)\circ(x,y,z,w) = (ax+bw+cz+cw+dy+dw, ay+bx+cy+cz+cw+dy+dz,$

$az+by+bw+cx+cz+cw+dy, aw+bz+cy+cz+dx+dz+dw).$

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	a+b+c+1
b	b	a+c	b+1	a+1
c	c	c+1	a+b+c	b+c+1

$V_{17}: \ (a,b,c,d)\circ(x,y,z,w) = (ax+bw+cz+cw+dy+dw, ay+bx+bw+cy+cw+dz,$

$az+by+bw+cx+cz+dz+dw, aw+bz+bw+cy+dx+dy+dz+dw).$

$*$	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	b+1
b	b	a+b+c	b+1	a+b
c	c	a+b+c+1	a+c+1	a

$V_{18}: \ (a,b,c,d)\circ(x,y,z,w) = (ax+bw+cz+dy+dz, ay+bx+cy+cw+dy+dz+dw,$

$az+by+bw+cx+cy+cz+cw+dy, aw+bz+cy+dx+dy+dz).$

Для оставшихся полуполей используем изоморфизмы:

$$V_1^{op} \simeq V_6,\ V_3^{op} \simeq V_7,\ V_4^{op} \simeq V_5,\ V_8^{op} \simeq V_9,\ V_{11}^{op} \simeq V_{14},\ V_{15}^{op} \simeq V_{16}.$$

Построенные изоморфизмы полуполей завершают доказательство теоремы 2.1.1. $\square$

2.2 Теоремы о строении полуполей порядка 16

Д. Кнут [23] показал, что порядок группы автоморфизмов каждого из 23 Клейнфилдовых неизоморфных собственных полуполей порядка 16 равен 6, 4, 3, 2 или 1. Ясно, что для решения вопросов **(A)** – **(B)** для полуполей порядка 16 достаточно решить их для каждого из 16 полуполей S, перечисленных в теореме 2.1.1. С этой целью первоочередной становится задача построения таблицы Кэли лупы S^*.

Мы используем обозначения из § 2.1 координатизирующего множества W, как 4-х мерного пространства над Z_2, регулярного множества $R = \theta(W)$ и отображения $\theta : W \to M(4, Z_2)$, заданного по формуле (2.1).

Когда $(W, +, \circ)$ – конечное поле с умножением (1.1), по лемме 1.1.6, R есть подполе порядка 16 в $M(4, Z_2)$ и R^* – циклическая группа порядка 15. Она порождается матрицей $A \in GL(4, 2)$. Для построения матрицы A учитываем неприводимость над Z_2 ее характеристического многочлена (каждый ее характеристический корень порождает расширение степени 4 поля Z_2) и используем естественную нормальную форму матриц [3, § 15.5].

Формула (2.1) и компьютерные вычисления приводят точно к 19936 различным наборам B, C, D, и точно в 336 случаях регулярное множество $R = \theta(W)$ есть поле. В оставшихся 19600 недезарговых случаях выбор матриц B, C, D однозначно определяет и полуполевую плоскость π, и полуполе W с умножением (1.1).

Методами [48] перечисление неизоморфных плоскостей удается свести к двум случаям:

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

$$\theta(x,y,z,w) = \begin{pmatrix} x & y & z & w \\ w & x+z & z+w & y+w \\ z & w & x+y+z+w & y+z+w \\ y+z+w & z & y+z & x+w \end{pmatrix} \quad (x,y,z,w \in Z_2).$$

Учитывая (1.1) и теорему 1.1.8, получаем точно 2, с точностью до изотопизмов, собственных полуполя порядка 16 с умножениями

$$(a,b,c,d) \circ (u,v,z,w) = (au+bv+cz+dw, av+bu+bw+cz+cw+dz,$$

$$az+bz+bw+cu+cv+cw+dv+dw, aw+bv+bz+bw+cv+cw+du), \qquad (2.2)$$

$$(a,b,c,d) \circ (u,v,z,w) = (au+bv+cz+dv+dz+dw, av+bu+bz+cw+dz,$$

$$az+bz+bw+cu+cv+cz+cw+dv+dz, aw+bv+bw+cv+cz+cw+du+dw). \quad (2.3)$$

Таким образом, приходим к следующей теореме Е. Клейнфилда [21] (доказанной также с использованием компьютерных вычислений).

Теорема 2.2.1. *Существует точно две неизоморфных недезарговых полуполевых плоскости порядка 16.* □

Для исследования строения всех полуполей порядка 16 достаточно исследовать 16 полуполей из теоремы 2.1.1. Вначале рассмотрим строение представителей изотопных классов полуполей.

Теорема 2.2.2. *В полуполе S с умножением (2.2) минимальное подполе Z_2e является максимальным. Лупа S^* порождается любым ее неединичным элементом, и спектр лупы совпадает с* $\{1, 4, 5, 6\}$.

Доказательство. Вначале находим таблицу Кэли лупы S^*; умножение на единичный элемент $e = (1, 0, 0, 0)$ опускаем.

Таблица 2.2.1. Лупа S^* полуполя S с умножением (2.2)

	(0,0,0,1)	**(0,0,1,0)**	**(0,0,1,1)**	**(0,1,0,0)**	**(0,1,0,1)**	**(0,1,1,0)**	**(0,1,1,1)**
(0,0,0,1)	(0,0,1,0)	(0,1,0,0)	(0,1,1,0)	(1,0,1,0)	**(1,0,0,0)**	(1,1,1,0)	(1,1,0,0)
(0,0,1,0)	(0,1,1,1)	(1,1,0,0)	(1,0,1,1)	(0,0,1,1)	(0,1,0,0)	(1,1,1,1)	**(1,0,0,0)**
(0,0,1,1)	(0,1,0,1)	**(1,0,0,0)**	(1,1,0,1)	(1,0,0,1)	(1,1,0,0)	(0,0,0,1)	(0,1,0,0)
(0,1,0,0)	(1,1,1,1)	(0,0,1,1)	(1,1,0,0)	(0,0,0,1)	(1,1,1,0)	(0,0,1,0)	(1,1,0,1)
(0,1,0,1)	(1,1,0,1)	(0,1,1,1)	(1,0,1,0)	(1,0,1,1)	(0,1,1,0)	(1,1,0,0)	(0,0,0,1)
(0,1,1,0)	**(1,0,0,0)**	(1,1,1,1)	(0,1,1,1)	(0,0,1,0)	(1,0,1,0)	(1,1,0,1)	(0,1,0,1)
(0,1,1,1)	(1,0,1,0)	(1,0,1,1)	(0,0,0,1)	**(1,0,0,0)**	(0,0,1,1)	(0,0,1,1,)	(1,0,0,1)
(1,0,0,1)	(0,0,1,1)	(0,1,1,0)	(0,1,0,1)	(1,1,1,0)	(1,1,0,1)	**(1,0,0,0)**	(1,0,1,1)
(1,0,1,0)	(0,1,1,0)	(1,1,1,0)	**(1,0,0,0)**	(0,1,1,1)	(0,0,0,1)	(1,0,0,1)	(1,1,1,1)
(1,0,1,1)	(0,1,0,0)	(1,0,1,0)	(1,1,1,0)	(1,1,0,1)	(1,0,0,1)	(0,1,1,1)	(0,0,1,1)
(1,1,0,0)	(1,1,1,0)	(0,0,0,1)	(1,1,1,1)	(0,1,0,1)	(1,0,1,1)	(0,1,0,0)	(1,0,1,0)
(1,1,0,1)	(1,1,0,0)	(0,1,0,1)	(1,0,0,1)	(1,1,1,1)	(0,0,1,1)	(1,0,1,0)	(0,1,1,0)
(1,1,1,0)	(1,0,0,1)	(1,1,0,1)	(0,1,0,0)	(0,1,1,0)	(1,1,1,1)	(1,0,1,1)	(0,0,1,0)
(1,1,1,1)	(1,0,1,1)	(1,0,0,1)	(0,0,1,0)	(1,1,0,0)	(0,1,1,1)	(0,1,0,1)	(1,1,1,0)

	(1,0,0,1)	**(1,0,1,0)**	**(1,0,1,1)**	**(1,1,0,0)**	**(1,1,0,1)**	**(1,1,1,0)**	**(1,1,1,1)**
(0,0,0,1)	(0,0,1,1)	(0,1,0,1)	(0,1,1,1)	(1,0,1,1)	(1,0,0,1)	(1,1,1,1)	(1,1,0,1)
(0,0,1,0)	(0,1,0,1)	(1,1,1,0)	(1,0,0,1)	(0,0,0,1)	(0,1,1,0)	(1,1,0,1)	(1,0,1,0)
(0,0,1,1)	(0,1,1,0)	(1,0,1,1)	(1,1,1,0)	(1,0,1,0)	(1,1,1,1)	(0,0,1,0)	(0,1,1,1)
(0,1,0,0)	(1,0,1,1)	(0,1,1,1)	**(1,0,0,0)**	(0,1,0,1)	(1,0,1,0)	(0,1,1,0)	(1,0,0,1)
(0,1,0,1)	**(1,0,0,0)**	(0,0,1,0)	(1,1,1,1)	(1,1,1,0)	(0,0,1,1)	(1,0,0,1)	(0,1,0,0)
(0,1,1,0)	(1,1,1,0)	(1,0,0,1)	(0,0,0,1)	(0,1,0,0)	(1,1,0,0)	(1,0,1,1)	(0,0,1,1)
(0,1,1,1)	(1,1,0,1)	(1,1,0,0)	(0,1,1,0)	(1,1,1,1)	(0,1,0,1)	(0,1,0,0)	(1,1,1,0)
(1,0,0,1)	(1,0,1,0)	(1,1,1,1)	(1,1,0,0)	(0,1,1,1)	(0,1,0,0)	(0,0,0,1)	(0,0,1,0)
(1,0,1,0)	(1,1,0,0)	(0,1,0,0)	(0,0,1,0)	(1,1,0,1)	(1,0,1,1)	(0,0,1,1)	(0,1,0,1)
(1,0,1,1)	(1,1,1,1)	(0,0,0,1)	(0,1,0,1)	(0,1,1,0)	(0,0,1,0)	(1,1,0,0)	**(1,0,0,0)**
(1,1,0,0)	(0,0,1,0)	(1,1,0,1)	(0,0,1,1)	(1,0,0,1)	(0,1,1,1)	**(1,0,0,0)**	(0,1,1,0)
(1,1,0,1)	(0,0,0,1)	**(1,0,0,0)**	(0,1,0,0)	(0,0,1,0)	(1,1,1,0)	(0,1,1,1)	(1,0,1,1)
(1,1,1,0)	(0,1,1,1)	(0,0,1,1)	(1,0,1,0)	**(1,0,0,0)**	(0,0,0,1)	(0,1,0,1)	(1,1,0,0)
(1,1,1,1)	(0,1,0,0)	(0,1,1,0)	(1,1,0,1)	(0,0,1,1)	**(1,0,0,0)**	(1,0,1,0)	(0,0,0,1)

Таблица 2.2.1 показывает, что правильные (правонормированные) k-е степени $(1 \leq k \leq 15)$ каждого из элементов

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

дают все элементы лупы S^*, причем

$$(m_1)^{15} = (m_2)^{15} = (m_3)^{15} = (m_4)^{15} = e.$$

Для элемента $h = (0,0,0,1)$ все произведения длины < 5 отличны от e и $h^2 \cdot h^3 = e$, так что $|h| = 5$. С другой стороны, для элемента m_1 всевозможные произведения длины ≤ 5 также не равны e, а произведение $m_1^2 \cdot (m_1 \cdot (m_1)^3) = e$. Таким образом, $|m_1| = 6$. Аналогично доказывается, что порядок любого элемента лупы S^* не больше 6.

Порядки элементов лупы S^*, наряду с ее спектром, и левый и правый обратные элементы явно перечисляет

Таблица 2.2.2. Правый и левый обратные элементы к элементам лупы S^* полуполя S с умножением (2.2) и их порядки

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

В частности, аналог теоретико-групповой теоремы Лагранжа для лупы S^* не выполняется.

Порождаемость лупы S^* элементами $y = m_i$ $(1 \leq i \leq 4)$ доказана. Для любого другого неединичного элемента с помощью таблиц 2.2.1 и 2.2.2 нетрудно подобрать его подходящую степень (при всевозможных расстановках скобок), которая будет равна одному из

элементов m_i. Таким образом, лупа S^* порождается любым своим неединичным элементом.

Покажем, что полуполе S не имеет подполей, кроме Z_2e. Ясно, что если элемент лежит в подполе, то его левый и правый обратные элементы равны. Согласно таблице 2.2.2, это могут быть только элементы $(1,1,0,0)$ и $(1,1,1,0)$ порядка > 3. Следовательно, полуполе S не имеет подполей порядка > 2. $\square$

Строение полуполя с умножением (2.3) аналогично описывает

Теорема 2.2.3. *Полуполе S с умножением (2.3) имеет точно 2 максимальных подполя H_1 и H_2, и $|H_1| = |H_2| = 4$. Лупа S^* порождается любым элементом из $S \setminus \{H_1 \cup H_2\}$, и ее спектр совпадает с $\{1,3,4,5,6\}$.* $\square$

Несложно показывается, что полуполя из теорем 2.2.2 и 2.2.3 изоморфны полуполям Е. Клейнфилда V_7 и T_{25}, соответственно.

Аналогичное структурное описание получено для всех 16 собственных Клейнфилдовых полуполей порядка 16 из теоремы 2.1.1. Число подполей порядка 4 равно 1,2,3 и 4, соответственно, в 6,5,1 и 1 полуполях; в трех оставшихся полуполях минимальное подполе максимально. Описание и теорема 2.1.1 дают:

Лупа ненулевых элементов полуполя порядка 16 однопорождена.

Результаты описания резюмирует Таблица 2.2.5 в конце § 2.2. Подробнее рассмотрим еще случай с наибольшим числом подполей.

Теорема 2.2.4. *Полуполе V_{13} имеет точно 4 максимальных подполя. Они имеют порядок 4, а любой, не лежащий в них элемент, порождает лупу V_{13}^*. Спектр лупы совпадает с $\{1, 3, 5\}$.*

Доказательство. Вначале строим таблицу Кэли лупы V_{13}^* с единицей $e = (0, 0, 0, 1)$, используя алгоритм Е. Клейнфилда, основанный на специальных порождающих последовательностях. Умножение на единичный элемент в таблице опускаем.

Таблица 2.2.3. Таблица Кэли лупы V_{13}^*

	(0,0,1,0)	**(0,0,1,1)**	**(0,1,0,0)**	**(0,1,0,1)**	**(0,1,1,0)**	**(0,1,1,1)**	**(1,0,0,0)**
(0,0,1,0)	(0,1,0,0)	(0,1,1,0)	(1,0,0,0)	(1,0,1,0)	(1,1,0,0)	(1,1,1,0)	(0,0,1,1)
(0,0,1,1)	(0,1,1,0)	(0,1,0,1)	(1,1,0,0)	(1,1,1,1)	(1,0,1,0)	(1,0,0,1)	(1,0,1,1)
(0,1,0,0)	(1,1,1,0)	(1,0,1,0)	(0,1,0,1)	**(0,0,0,1)**	(1,0,1,1)	(1,1,1,1)	(0,1,1,1)
(0,1,0,1)	(1,1,0,0)	(1,0,0,1)	**(0,0,0,1)**	(0,1,0,0)	(1,1,0,1)	(1,0,0,0)	(1,1,1,1)
(0,1,1,0)	(1,0,1,0)	(1,1,0,0)	(1,1,0,1)	(1,0,1,1)	(0,1,1,1)	**(0,0,0,1)**	(0,1,0,0)
(0,1,1,1)	(1,0,0,0)	(1,1,1,1)	(1,0,0,1)	(1,1,1,0)	**(0,0,0,1)**	(0,1,1,0)	(1,1,0,0)
(1,0,0,0)	(1,0,0,1)	**(0,0,0,1)**	(1,0,1,0)	(0,0,1,0)	(0,0,1,1)	(1,0,1,1)	(0,1,0,1)
(1,0,0,1)	(1,0,1,1)	(0,0,1,0)	(1,1,1,0)	(0,1,1,1)	(0,1,0,1)	(1,1,0,0)	(1,1,0,1)
(1,0,1,0)	(1,1,0,1)	(0,1,1,1)	(0,0,1,0)	(1,0,0,0)	(1,1,1,1)	(0,1,0,1)	(0,1,1,0)
(1,0,1,1)	(1,1,1,1)	(0,1,0,0)	(0,1,1,0)	(1,1,0,1)	(1,0,0,1)	(0,0,1,0)	(1,1,1,0)
(1,1,0,0)	(0,1,1,1)	(1,0,1,1)	(1,1,1,1)	(0,0,1,1)	(1,0,0,0)	(0,1,0,0)	(0,0,1,0)
(1,1,0,1)	(0,1,0,1)	(1,0,0,0)	(1,0,1,1)	(0,1,1,0)	(1,1,1,0)	(0,0,1,1)	(1,0,1,0)
(1,1,1,0)	(0,0,1,1)	(1,1,0,1)	(0,1,1,1)	(1,0,0,1)	(0,1,0,0)	(1,0,1,0)	**(0,0,0,1)**
(1,1,1,1)	**(0,0,0,1)**	(1,1,1,0)	(0,0,1,1)	(1,1,0,0)	(0,0,1,0)	(1,1,0,1)	(1,0,0,1)

	(1,0,0,1)	**(1,0,1,0)**	**(1,0,1,1)**	**(1,1,0,0)**	**(1,1,0,1)**	**(1,1,1,0)**	**(1,1,1,1)**
(0,0,1,0)	**(0,0,0,1)**	(0,1,1,1)	(0,1,0,1)	(1,0,1,1)	(1,0,0,1)	(1,1,1,1)	(1,1,0,1)
(0,0,1,1)	(1,0,0,0)	(1,1,0,1)	(1,1,1,0)	(0,1,1,1)	(0,1,0,0)	**(0,0,0,1)**	(0,0,1,0)
(0,1,0,0)	(0,0,1,1)	(1,0,0,1)	(1,1,0,1)	(0,0,1,0)	(0,1,1,0)	(1,1,0,0)	(1,0,0,0)
(0,1,0,1)	(1,0,1,0)	(0,0,1,1)	(0,1,1,0)	(1,1,1,0)	(1,0,1,1)	(0,0,1,0)	(0,1,1,1)
(0,1,1,0)	(0,0,1,0)	(1,1,1,0)	(1,0,0,0)	(1,0,0,1)	(1,1,1,1)	(0,0,1,1)	(0,1,0,1)
(0,1,1,1)	(1,0,1,1)	(0,1,0,0)	(0,0,1,1)	(0,1,0,1)	(0,0,1,0)	(1,1,0,1)	(1,0,1,0)
(1,0,0,0)	(1,1,0,1)	(1,1,0,0)	(0,1,0,0)	(1,1,1,1)	(0,1,1,1)	(0,1,1,0)	(1,1,1,0)
(1,0,0,1)	(0,1,0,0)	(0,1,1,0)	(1,1,1,1)	(0,0,1,1)	(1,0,1,0)	(1,0,0,0)	**(0,0,0,1)**
(1,0,1,0)	(1,1,0,0)	(1,0,1,1)	**(0,0,0,1)**	(0,1,0,0)	(1,1,1,0)	(1,0,0,1)	(0,0,1,1)
(1,0,1,1)	(0,1,0,1)	**(0,0,0,1)**	(1,0,1,0)	(1,0,0,0)	(0,0,1,1)	(0,1,1,1)	(1,1,0,0)
(1,1,0,0)	(1,1,1,0)	(0,1,0,1)	(1,0,0,1)	(1,1,0,1)	**(0,0,0,1)**	(1,0,1,0)	(0,1,1,0)
(1,1,0,1)	(0,1,1,1)	(1,1,1,1)	(0,0,1,0)	**(0,0,0,1)**	(1,1,0,0)	(0,1,0,0)	(1,0,0,1)
(1,1,1,0)	(1,1,1,1)	(0,0,1,0)	(1,1,0,0)	(0,1,1,0)	(1,0,0,0)	(0,1,0,1)	(1,0,1,1)
(1,1,1,1)	(0,1,1,0)	(1,0,0,0)	(0,1,1,1)	(1,0,1,0)	(0,1,0,1)	(1,0,1,1)	(0,1,0,0)

Правильные k-ые степени $(1 \leq k \leq 15)$ каждого из элементов

$$l_1 = (0, 0, 1, 0),\ l_2 = (0, 0, 1, 1),\ l_3 = (1, 0, 0, 0),$$

$$l_4 = (1, 0, 0, 1),\ l_5 = (1, 1, 1, 0),\ l_6 = (1, 1, 1, 1)$$

дают все элементы лупы V_{13}^*, как показывает таблица 2.2.3, причем

$$(l_1)^{15} = (l_2)^{15} = (l_3)^{15} = (l_4)^{15} = (l_5)^{15} = (l_6)^{15} = e.$$

Все произведения длины ≤ 4 каждого элемента l_i $(1 \leq i \leq 6)$ отличны от e, однако, $(l_i \cdot l_i^3) \cdot l_i = e$ и $l_i \cdot ((l_i \cdot l_i^2) \cdot l_i)) = e$. Поэтому $|l_i| = 5$ $(1 \leq i \leq 6)$. Порядки всех элементов лупы V_{13}^* явно перечисляет

Таблица 2.2.4. Порядки элементов лупы V_{13}^*

y	(0,0,0,1)	(0,0,1,0)	(0,0,1,1)	(0,1,0,0)	(0,1,0,1)	(0,1,1,0)	(0,1,1,1)	(1,0,0,0)
|y|	1	5	5	3	3	3	3	5

y	(1,0,0,1)	(1,0,1,0)	(1,0,1,1)	(1,1,0,0)	(1,1,0,1)	(1,1,1,0)	(1,1,1,1)
|y|	5	3	3	3	3	5	5

Таблицы 2.2.3 и 2.2.4 показывают, что каждый элемент порядка 3 лежит в подходящем подполе порядка 4, и все такие подполя в V_{13} исчерпываются следующими:

$$D_1 = \{0, e, (0,1,0,0), (0,1,0,1)\}, \quad D_2 = \{0, e, (0,1,1,0), (0,1,1,1)\},$$

$$D_3 = \{0, e, (1,0,1,0), (1,0,1,1)\}, \quad D_4 = \{0, e, (1,1,0,1), (1,1,0,0)\}.$$

Объединение подполей содержит 10 элементов. Следовательно, любой из оставшихся элементов совпадает с одним из l_i и, по доказанному выше, порождает лупу V_{13}^*. Это завершает доказательство теоремы. $\square$

Таблица 2.2.5. Строение неизоморфных полуполей порядка 16

Полуполе	$\lvert N_l \rvert$	Число подполей порядка 4	Спектр лупы полуполя	Противоположное полуполе
V_1	2	–	$\{1,4,5\}$	$V_1^{op} \simeq V_6$
V_2	2	1	$\{1,3,4,5,6\}$	$V_2^{op} = V_2$
V_3	2	–	$\{1,4,5,6\}$	$V_3^{op} \simeq V_7$
V_4	2	1	$\{1,3,4,5,6\}$	$V_4^{op} \simeq V_5$
V_8	2	2	$\{1,3,4,5,6\}$	$V_8^{op} \simeq V_9$
V_{10}	2	1	$\{1,3,5,6\}$	$V_{10}^{op} = V_{10}$
V_{11}	2	1	$\{1,3,4,5,6\}$	$V_{11}^{op} \simeq V_{14}$
V_{12}	2	–	$\{1,4,5,6\}$	$V_{12}^{op} = V_{12}$
V_{13}	2	4	$\{1,3,5\}$	$V_{13}^{op} = V_{13}$
V_{15}	2	2	$\{1,3,4,5\}$	$V_{15}^{op} \simeq V_{16}$
V_{17}	2	1	$\{1,3,4,5,6\}$	$V_{17}^{op} = V_{17}$
V_{18}	2	2	$\{1,3,5,6\}$	$V_{18}^{op} = V_{18}$
T_{24}	4	2	$\{1,3,4,5,6\}$	$T_{24}^{op} = T_{24}$
T_{25}	4	2	$\{1,3,4,5,6\}$	$T_{25}^{op} \simeq T_{50}$
T_{35}	4	1	$\{1,3,4,5,6\}$	$T_{35}^{op} = T_{35}$
T_{45}	4	3	$\{1,3,5\}$	$T_{45}^{op} = T_{45}$

Теоремы 2.2.2 – 2.2.4 и таблица 2.2.5 опубликованы в нераздельном соавторстве (соавтор В.М. Левчук) в статье [47].

2.3 Строение полуполей проективных полуполевых плоскостей порядка 32

В 2011 году все плоскости трансляций порядка 32 классифицировали У. Демпволф и Р. Рокенфеллер [34], [12], наряду с описанием регулярных множеств. (Классификацию полуполевых плоскостей анонсировал в 1962 году Р. Волкер [41].) С точностью до изоморфизмов, таких плоскостей оказалось 9, включая 6 полуполевых. Координатизирующее множество представлено в [12] как 5-мерное пространство W над полем Z_2.

В [12] выписаны регулярные множества недезарговых полуполевых плоскостей порядка 32; это 5 множеств 5×5-матриц над Z_2,

по 32 матрицы в каждом. Основываясь на [12], мы запишем их как множества $R_i = \theta_i(W)$, $1 \leq i \leq 5$, матриц для всевозможных $x, y, z, w, s \in Z_2$ вида, соответственно,

$$R_1 : \begin{pmatrix} x & y & z & w & s \\ z & x+z & y+s & w+s & w \\ z+s & w & x+w & y+w & z \\ w & z+w & w+s & x+z & y+w \\ y+z+w+s & z+s & y+w+s & z+w & x+w \end{pmatrix},$$

$$R_2 : \begin{pmatrix} x & y & z & w & s \\ z+w+s & x+z+s & y+w & s & w+s \\ z+s & w & x+z+w & y+z & z \\ z+w & z+w+s & w+s & x+s & y+z+s \\ y+z+w & z+w & y+z+w+s & z+s & x+z+w+s \end{pmatrix},$$

$$R_3 : \begin{pmatrix} x & y & z & w & s \\ z+w & x & y+z+w & w+s & w \\ z+s & z+w & x+z+w & y+w & z \\ z & s & z+w+s & x+z+w+s & y+z+s \\ y+z+w & z & y+z+w+s & z+w & x+z+s \end{pmatrix},$$

$$R_4 : \begin{pmatrix} x & y & z & w & s \\ s & x & y+s & z & w \\ z+w & z+w+s & x+z & y+z & z \\ z+s & z+w & s & x+s & y \\ y+w+s & z & y+w & w+s & x \end{pmatrix},$$

$$R_5 : \begin{pmatrix} x & y & z & w & s \\ z & x+z+w & y+w & w+s & w \\ z+s & w & x & y+w & z+w \\ z+w+s & z+s & s & x+z+w & y+z+s \\ y+z+w & w+s & y & z & x+z \end{pmatrix}.$$

Обозначим полуполе W с умножением (1.1) при $R = R_i$ через P_i. В этих обозначениях из [34], [12] и теоремы 1.1.8 вытекает

Теорема 2.3.1. *Каждое собственное полуполе порядка 32 изотопно точно одному из полуполей* P_i, $1 \leq i \leq 5$. $\square$

Напомним, что *левым, средним* и *правым ядром полуполя* S (случай квазиполя см. [18, стр. 159]) называют, соответственно,

$$N_l(S) = \{x \in S \mid x \circ (y \circ z) = (x \circ y) \circ z, \quad \forall y, z \in S\},$$

$$N_m(S) = \{y \in S \mid x \circ (y \circ z) = (x \circ y) \circ z, \quad \forall x, z \in S\},$$

$$N_r(S) = \{z \in S \mid x \circ (y \circ z) = (x \circ y) \circ z, \quad \forall x, y \in S\}.$$

Для исследования строения полуполя P_i с помощью формулы (1.1) и регулярного множества R_i выписываем таблицу Кэли каждой лупы P_i^*. Структурное описание полуполя P_5 дает

Теорема 2.3.2. *В полуполе* P_5 *существует подполе* H *порядка 4, являющееся единственным максимальным подполем и не являющееся ни правым, ни левым ядром. Каждый элемент из* $P_5 \setminus H$ *порождает лупу* P_5^* *и имеет порядок* > 3*; спектр лупы* P_5^* *совпадает с* $\{1, 3, 4, 5, 6, 7, 8\}$.

Доказательство. С помощью формулы (1.1) и регулярного множества R_5 находим таблицу Кэли лупы P_5^*; умножение на единичный элемент $e = (1, 0, 0, 0, 0)$ в ней опускаем.

Таблица 2.3.1. Таблица Кэли лупы P_5^*

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

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

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

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

С ее помощью легко находим левые и правые обратные элементы к элементам лупы P_5^* (таблица 2.3.2). В лупе P_5^*, как показывает таблица 2.3.2, только у первых пяти элементов из нее правые и левые обратные элементы совпадают и поэтому полуполе P_5 не имеет подполей порядка больше 4.

Таблица Кэли показывает также, что все степени ≤ 3 каждого из элементов $(0,0,0,0,1)$, $(0,0,0,1,1)$, $(0,1,1,1,1)$ неединичны, а одна из третьих степеней совпадает с правым или левым обратным к этому элементу. Поэтому порядки этих элементов равны 4.

Аналогичной процедурой находим порядки всех элементов лупы P_5^* и ее спектр.

Таблица 2.3.2. Левый и правый обратный к элементам лупы P_5^*

Элемент y	Левый обратный	Правый обратный	Порядок $\|y\|$
(1,0,0,0,0)	**(1,0,0,0,0)**	**(1,0,0,0,0)**	1
(0,0,0,1,0)	**(1,0,0,1,0)**	**(1,0,0,1,0)**	3
(1,0,0,1,0)	**(0,0,0,1,0)**	**(0,0,0,1,0)**	3
(1,0,0,0,1)	**(1,1,1,1,0)**	**(1,1,1,1,0)**	7
(1,1,1,1,0)	**(1,0,0,0,1)**	**(1,0,0,0,1)**	7
(0,0,0,0,1)	(0,0,1,0,0)	(0,0,0,1,1)	4
(0,0,0,1,1)	(0,0,0,0,1)	(0,1,0,0,1)	4
(0,0,1,0,0)	(0,1,0,1,1)	(0,0,0,0,1)	7
(0,0,1,0,1)	(0,1,1,0,1)	(1,1,0,1,0)	6
(0,0,1,1,0)	(1,1,1,0,1)	(0,1,1,1,0)	6
(0,0,1,1,1)	(1,0,0,1,1)	(1,1,0,0,0)	5
(0,1,0,0,0)	(0,1,0,0,1)	(1,0,1,0,0)	6
(0,1,0,0,1)	(0,0,0,1,1)	(0,1,0,0,0)	7
(0,1,0,1,0)	(1,0,1,1,0)	(1,1,0,0,1)	6
(0,1,0,1,1)	(0,1,1,0,0)	(0,0,1,0,0)	5
(0,1,1,0,0)	(1,1,0,0,0)	(0,1,0,1,1)	5
(0,1,1,0,1)	(1,1,1,0,0)	(0,0,1,0,1)	5
(0,1,1,1,0)	(0,0,1,1,0)	(1,1,0,1,1)	5
(0,1,1,1,1)	(1,0,1,0,1)	(1,0,1,1,0)	4
(1,0,0,1,1)	(1,0,1,1,1)	(0,0,1,1,1)	7
(1,0,1,0,0)	(0,1,0,0,0)	(1,0,1,0,1)	7
(1,0,1,0,1)	(1,0,1,0,0)	(0,1,1,1,1)	6
(1,0,1,1,0)	(0,1,1,1,1)	(0,1,0,1,0)	6
(1,0,1,1,1)	(1,1,1,1,1)	(1,0,0,1,1)	6
(1,1,0,0,0)	(0,0,1,1,1)	(0,1,1,0,0)	6
(1,1,0,0,1)	(0,1,0,1,0)	(1,1,1,1,1)	7
(1,1,0,1,0)	(0,0,1,0,1)	(1,1,1,0,0)	7
(1,1,0,1,1)	(0,1,1,1,0)	(1,1,1,0,1)	5
(1,1,1,0,0)	(1,1,0,1,0)	(0,1,1,0,1)	8
(1,1,1,0,1)	(1,1,0,1,1)	(0,0,1,1,0)	5
(1,1,1,1,1)	(1,1,0,0,1)	(1,0,1,1,1)	6

Ясно, что $H = \{0, e, (0,0,0,1,0), (1,0,0,1,0)\}$ – подполе. Как показывает таблица 2.3.1, кубы 4 и 5-го элементов таблицы 2.3.2 не равны e. Поэтому H – единственное максимальное подполе в P_5. С помощью таблицы Кэли и определения ядер полуполя несложно показывается, что H не является ни левым, ни правым ядром.

Таблица 2.3.1 показывает, что правильные расстановки скобок 24 элементов из $P_5 \setminus H$ (кроме 4 элементов $g_1 = (0,1,0,0,1)$, $g_2 = (0,1,1,0,1)$, $g_3 = (1,1,0,0,1)$, $g_4 = (1,1,1,0,1)$) дают все ненулевые элементы полуполя P_5, причем их 31−я степень равна e. С другой стороны, вторые степени элементов g_i дают элементы, ко-

торые порождают лупу P_5^*: $g_1^2 = (0,0,1,1,0)$, $g_2^2 = (0,0,0,1,0)$, $g_3^2 = (1,1,0,1,0)$, $g_4^2 = (1,0,0,1,0)$. Поэтому лупа P_5^* порождается всяким элементом из $P_5 \setminus H$. $\square$

Таблицы Кэли луп оставшихся полуполей P_i $(1 \le i \le 4)$ также были найдены с помощью следующих формул умножения:

$$P_1: (u,v,k,l,m) \circ (x,y,z,w,s) = (ux+vz+kz+ks+lw+my+mz+mw+ms,$$
$$uy+vx+vz+kw+lz+lw+mz+ms, uz+vy+vs+kx+kw+lw+ls+my+mw+ms,$$
$$uw+vw+vs+ky+kw+lx+ly+mz+mw, us+vw+kz+ly+lw+mx+mw);$$

$$P_2: (u,v,k,l,m) \circ (x,y,z,w,s) = (ux+vz+vw+vs+kz+ks+lz+lw+my+mz+mw,$$
$$uy+vx+vz+vs+kw+lz+lw+ls+mz+mw,$$
$$uz+vy+vw+kx+kz+kw+lw+ls+my+mz+mw+ms,$$
$$uw+vs+ky+kz+lx+lz+mz+ms, us+vw+vs+kz+ly+lz+ls+mx+mz+mw+ms);$$

$$P_3: (u,v,k,l,m) \circ (x,y,z,w,s) = (ux+vz+vw+kz+ks+lz+my+mz+mw,$$
$$uy+vx+kz+kw+ls+mz, uz+vy+vz+vw+kx+kz+kw+lz+lm+ls+my+mz+mw+ms,$$
$$uw+vw+vs+ky+kw+lx+lz+lw+ls+mz+mw, us+vw+kz+ly+lz+ls+mx+mz+ms);$$

$$P_4: (u,v,k,l,m) \circ (x,y,z,w,s) = (ux+vs+kz+kw+lz+ls+my+mw+ms,$$
$$uy+vx+kz+kw+ks+lz+lw+mz, uz+vy+vs+kx+kz+ls+my+mw,$$
$$uw+vz+ky+kz+lx+ls+mw+ms, us+vw+kz+ly+mx);$$

Теорема 2.3.3. *В каждом полуполе P_i, $i = 1,2,3,4$, подполе порядка 2 есть единственное подполе. Всякий элемент порядка > 1 пороождает лупу P_i^*, а спектр лупы P_i^* совпадает с $\{1,4,5,6,7\}$ при $i = 1,2$, с $\{1,4,5,6,7,8\}$ при $i = 3$, и с $\{1,5,6,7,8,9\}$ при $i = 4$.*

Доказательство теоремы проводится аналогично предыдущей теореме. Правый и левый обратный элементы совпадают в лупе P_1^* только для единичного элемента, в лупах P_2^* и P_3^* – для 3-х элементов. Сейчас легко получаем максимальность подполя порядка 2 в этих полуполях. Это же верно и для коммутативной лупы P_4^*, поскольку она не имеет элементов порядка 3. Спектр и порядки элементов выявляют следующие таблицы.

Таблица 2.3.4. Порядки элементов лупы P_1^*

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)
|y|	1	4	7	5	6	6	6

y	(0,0,1,1,1)	(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)
|y|	5	6	6	5	6	6	5

y	(0,1,1,1,0)	(0,1,1,1,1)	(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)
|y|	6	6	5	6	5	6	6

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

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

Таблица 2.3.5. Порядки элементов лупы P_2^*

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)
|y|	1	5	4	6	7	6	5

y	(0,0,1,1,1)	(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)
|y|	6	6	6	6	6	6	5

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

y	(1,0,1,1,0)	(1,0,1,1,1)	(1,1,0,0,0)	(1,1,0,0,1)	(1,1,0,1,0)	(1,1,0,1,1)	(1,1,1,0,0)
|y|	6	6	5	6	5	6	6

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

Таблица 2.3.6. Порядки элементов лупы P_3^*

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)
|y|	1	7	6	6	5	8	6

y	(0,0,1,1,1)	(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)
|y|	7	6	6	7	5	7	4

y	(0,1,1,1,0)	(0,1,1,1,1)	(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)
|y|	5	4	7	7	5	5	7

y	(1,0,1,1,0)	(1,0,1,1,1)	(1,1,0,0,0)	(1,1,0,0,1)	(1,1,0,1,0)	(1,1,0,1,1)	(1,1,1,0,0)
|y|	4	7	6	8	5	6	6

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

Таблица 2.3.7. Порядки элементов лупы P_4^*

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)
|y|	1	8	9	7	8	9	8

y	(0,0,1,1,1)	(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)
|y|	7	7	7	8	9	9	9

y	(0,1,1,1,0)	(0,1,1,1,1)	(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)
|y|	9	7	8	8	8	8	5

y	(1,0,1,1,0)	(1,0,1,1,1)	(1,1,0,0,0)	(1,1,0,0,1)	(1,1,0,1,0)	(1,1,0,1,1)	(1,1,1,0,0)
|y|	8	6	8	9	8	7	5

y	(1,1,1,0,1)	(1,1,1,1,0)	(1,1,1,1,1)
|y|	7	9	6

Пользуясь таблицами Кэли несложно доказать однопорожденность каждой лупы $P_i^*,\ 1 \leq i \leq 4$. $\square$

Замечание 2.3.4. *Теорема 2.3.2 выявляет полуполе порядка 32 с аномальным (по сравнению с конечными полями) свойством для подполей: полуполе P_5 порядка 2^5 содержит подполе порядка 2^2. Полуполе порядка 32 с аналогичным свойством указывает И. Руа [35, Следствие 1], основываясь на [7].*

Теоремы 2.3.2 и 2.3.3 опубликованы автором в [46].

2.4 Классификация и полуполе Кнута – Руа

Г. Венэ [43] называет полуполе P *правоциклическим или правопримитивным*, если лупу P^* исчерпывают правоупорядоченные степени ее фиксированного элемента. (Аналогично вводят левоциклические полуполя.)

Там же высказана *гипотеза о правоцикличности конечных полуполей*. Полуполе порядка 32, для которого гипотеза Г. Венэ не выполняется, указал в 2004 г. И. Руа [35] на основе работы [22].

Проблема описания строения полуполей порядка 32 сложнее, чем для порядка 16. Согласно [41] и [23], с точностью до изоморфизмов, их число равно 2502; они образуют 6 изотопных классов, соответствующих 6 попарно неизоморфным полуполевым плоскостям $P(i)$ $(0 \leq i \leq 5)$ (включая дезаргову плоскость $P(0)$).

Классификацию резюмирует следующая таблица из [35].

Таблица 2.4.1. Классы изоморфных полуполей порядка 32

Полуполе \ Плоскость	$P(0)$	$P(1)$	$P(2)$	$P(3)$	$P(4)$	$P(5)$
Лево- и право- примитивные	1	961	961	180	186	186
Только левопримитивные	0	0	0	6	0	7
Только правопримитивные	0	0	0	6	7	0
Ни лево-, ни право- примитивные	0	0	0	1	0	0

Исследуем пример И. Руа детальнее. Все недезарговы проективные полуполевые плоскости порядка 32 исчерпываются, с точностью до изоморфизмов, плоскостями $P(i)$ $(1 \leq i \leq 5)$ над Z_2 [22]. Для

плоскости $P(3)$ регулярное множество

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

наряду с формулой (1.1), дает полуполе $(W,+,\circ) = \Re$ порядка 32, которое назовем *полуполем Кнута – Руа.*

И. Руа [35] доказал тождество $g^{21} = e$ для правоупорядоченных степеней лупы $\Re^*$. Отсюда сразу же следует, что лупа $\Re^*$ не является правопримитивной. Основной в этом параграфе является

Теорема 2.4.1. *Лупа $\Re^*$ полуполя $\Re$ однопорождена.*

Доказательство. Регулярное множество $\theta(W)$ плоскости $P(3)$ позволяет записать умножение $\circ$ в полуполе $\Re$ в виде формулы:

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

$$uy+vx+vs+kz+kw+lz+lw+ls+my+mw,$$

$$uz+vy+kx+ks+ls+mz+mw+ms,$$

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

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

Формула сразу же показывает коммутативность умножения. С ее помощью восстанавливаем таблицу Кэли лупы $\Re^*$.

Таблица 2.4.2. Лупа $\Re^*$ полуполя $\Re$ 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

Для доказательства однопорожденности лупы $\Re^*$ выбираем ее элемент $a = (0, 0, 0, 0, 1)$. Его степени ≤ 3, в частности, куб c определены однозначно:

$$a^2 = (1, 0, 1, 1, 1),\ a^3 = a \cdot a^2 = (0, 1, 1, 0, 1) := c.$$

Далее вычисляем его степени с различными расстановками скобок.

$$a^4 = a \cdot a^3 = (0, 1, 0, 0, 0) := d, \quad a^2 \cdot a^2 = (0, 0, 1, 0, 1) := f,$$

$$(a \cdot a^3) \cdot a = a \cdot (a \cdot a^3) = (1, 1, 0, 0, 0),$$

$$a^3 \cdot a^2 = a^2 \cdot a^3 = (0, 1, 1, 1, 0), \quad a \cdot (a^2 \cdot a^2) = (1, 0, 0, 0, 0).$$

Мы выписываем только те степени элемента a, которые различные новые элементы лупы $\Re^*$.

$$c^2 = (0,1,0,1,0), \quad c^3 = (0,1,0,0,1) := n, \quad c^2 \cdot c^2 = (1,1,1,1,1);$$

$$c \cdot c^3 = (1,0,1,1,0), \quad f^3 = (1,0,0,1,0);$$

$$f \cdot f^3 = (1,0,0,1,1) := g, \quad g \cdot f = (0,0,0,1,1) := k;$$

$$f^3 \cdot f^2 = (1,1,1,1,0), \quad (f^3)^2 = (0,1,0,1,1), \quad k^2 = (0,1,1,0,0) := m;$$

$$k^3 = (1,0,1,0,0), \quad k^2 \cdot k^2 = (1,1,1,0,1);$$

$$(c \cdot c^3) \cdot c = (0,0,1,1,0) := l, \quad d^2 = (0,0,1,0,0);$$

$$(d^2)^2 = (1,1,0,0,1), \quad l^2 = (0,0,0,1,0).$$

Продолжая выписывать без повторов степени элемента a либо по возрастанию степеней, либо с различными расстановками скобок, находим оставшиеся 7 элементов лупы $\Re^*$ порядка 31:

$$g^2 = (1,1,1,0,0), \quad l^3 = (1,0,0,0,1), \quad l^2 \cdot l^2 = (1,1,0,1,1);$$

$$m^2 \cdot m^2 = (1,1,0,1,0), \quad (m^2 \cdot m^2)^2 = (0,1,1,1,1);$$

$$n \cdot n^3 = (0,0,1,1,1), \ (n \cdot n^3)^2 = (1,0,1,0,1).$$

Таким образом, все элементы лупы $\Re^*$ получаем как различные степени элемента a с различными расстановками скобок. $\square$

Ясно, что квадраты элементов лупы расположены по главной диагонали таблицы Кэли. Используя таблицу Кэли легко убедиться, что лупа $\Re^*$ не имеет элементов порядка 3 и подполе $Z_2 e$ максимально в полуполе $\Re$.

Список литературы

[1] *Енисейская тетрадь (математические вопросы и задачи для молодых исследователей). Выпуск I* // Красноярск: КГУ. 2004. 32 с.

[2] *Курош А.Г.* Лекции по общей алгебре // С.-Петербург: Лань. 2007.

[3] *Мальцев А.И.* Основы линейной алгебры // М.: Наука. 1979.

[4] *Подуфалов Н.Д.* О функциях на линейных пространствах, связанных с конечными проективными плоскостями // Алгебра и логика. 2002. Т. 41. №1. С. 83–103.

[5] *Холл М.* Теория групп // М.: ИЛ. 1962.

[6] *Adams P., Bean R., Khodkar A.* A census of critical sets in the latin squares of order at most six // Ars Combin. 2003. Vol. 68. P. 203–223.

[7] *Albert A.A.* Finite division algebras and finite planes // Proc. Sympos. Appl. Math., Vol.10, AMS, Provid. R.I. 1960. P. 53–70.

[8] *André J.* Über nicht-Desarguesche Ebenen mit transitiver Translationgruppe // Math. Z. 1954. Vol. 60. P. 156–186.

[9] *Bammel S.E., Rothstein J.* The number of 9×9 Latin squares // Discrete Math. 1975. Vol. 11. P. 93–95.

[10] *Cayley A.* On latin squares // Oxford Camb. Dublin Messenger of Math. 1890. Vol. 19. P. 85–239.

[11] *Dempwolff U., Reifart A.* The Classification of the translation planes of order 16, Part I // Geom. Dedic. 1983. Vol. 15. P. 137–153.

[12] *Dempwolff U.* File of Translation Planes of Small Order *http* : *//www.mathematik.uni−kl.de/* ∼ *dempw/dempw_Plane.html*.

[13] *Dickson L.E.* On finite algebras // Nachrichten der Gesellschaften der Wissenschaften zu Göttingen. 1905. P. 358–393.

[14] *Dickson L.E.* Linear algebras in which division is always uniquely possible // Trans. Amer. Math. Soc. 1906. Vol. 7. P. 370–390.

[15] *Euler L.* Rechercher sur une nouvelle espece de quarres magiques // Verhandelingen / uingegeven doorhet zeeuwsch Genootschap der Wetenschappen te Vlissingen. 1782. Vol. 9. P. 85–239.

[16] *Frolov M.* Sur les permutations carrees // J. de Math. spec. IV. 1890. P. 8–11. P. 25–30.

[17] *Gorissen M.J.G.* Generating finite projective planes from non-paratopic latin squares // Radboud University Nijmegen. Wiskunde en Informatica. IMAPP Computer Algebra. 6525 ED Nijmegen.

[18] *Hughes D.R., Piper F.C.* Projective planes // Springer - Verlag: New-York Inc. 1973.

[19] *Jacobson M.T., Matthews P.* Generating uniformly distributed random Latin squares // J. Combin. Des. 1996. Vol. 4. P. 405–437.

[20] *Johnson N.L., Jha V., Biliotti M.* Handbook of finite translation planes // London New York. 2007. 861 p.

[21] *Kleinfeld E.* Techniques for enumerating Veblen-Wedderburn systems // J. Assoc. Comput. Mach. 1960. Vol. 7. P. 330–337.

[22] *Knuth D.E.* Finite semifields and projective planes (PhD dissertation) // Pasadena: California Inst. of Thechnology. 1963. P. 1–70.

[23] *Knuth D.E.* Finite semifields and projective planes // J. Algebra. 1965. Vol. 2. P. 182–217.

[24] *Kuznetsov N.Y.* Estimating number of latin rectangles by the fast simulation metod // Cybern. Syst. Anal. 2009. Vol. 45. P. 69–75.

[25] *Lint J.H., Wilson R.M.* A Course in Combinatorics // Cambridge University Press. 1992. ISBN 0-521-42260-4. 157 p.

[26] *Lorimer P.* A Projective Plane of Order 16 // J. Combin. theory (A). 1974. 16. P. 334–347.

[27] *Lüneburg H.* Translation planes // Springer - Verlag: Berlin Heidelberg New-York Inc. 1980.

[28] *MacMahon P.A.* Combinatory analisis // Cambridge. 1915.

[29] *McKay B.D., Rogoyski E.* Latin squares of order ten // Electron. J. Combin. 1995. Vol. 2, No. 3. P. 1–4.

[30] *McKay B.D., Wanless I.M.* On the number of latin squares // Ann. Combin. 2005. Vol. 9. P. 335–344.

[31] *McKay B.D., Meynert A., Myrvold W.* Small latin squares, Quasigroups and Loops // J. Combin. Designs. 2007. Vol. 15. No. 2. P. 98–119.

[32] *Norton H.W.* The 7×7 squares // Ann. Eugenics. 1939. Vol. 9. P. 269–307.

[33] *Oyama T.* On quasifields // Osaka J. Math. 1985. Vol. 22. P. 35–54.

[34] *Rockenfeller R.* Translationsebenen der Ordnung 32 (Diploma Thesis) // FB Mathematik. University of Kaiserslautern. 2011.

[35] *Rua I.F.* Primitive and Non-Primitive Finite Semifields // Commun. Algebra. 2004. Vol. 22. P. 223–233.

[36] *Sade A.* An omission in Norton's list of 7×7 squares // Ann. Math. Stat. 1951. Vol. 22. P. 306–307.

[37] *Saxena P.N.* A simplified mathod of enumerating Latin squares by MacMahon's differential operators, Part II. The 7×7 latin squares // J. Indian Soc. Agric. Statistics. 1951. Vol. 3. P. 24–79.

[38] *Shonhardt E.* Uber lateinisch Quadrate und Uneonen // J. Reine Angew. Math. 1953. Vol. 163. P. 24–79.

[39] The Kourovka Notebook (unsolved problems in group theory), 15-th Ed. // Novosibirsk. Inst. Math. SO RAN. 1992.

[40] *Veblen O., Maclagan-Wedderburn J.H.* Non-Desarguesian and Non-Pascalian Geometries // Trans. Amer. Math. Soc. 1907. Vol. 8. No. 3. P. 379–388.

[41] *Walker R.J.* Determination of Division Algebras with 32 Elements // Proc. Symp. Appl. Math. XV, AMS. 1962. P. 83–85.

[42] *Wells M.B.* The number of Latin squares of order 8 // J. Combin. Theory. 1967. Vol. 3. P. 98–99.

[43] *Wene G.P.* On the multiplicative structure of finite division rings // A equationes Math. 1991. Vol. 41. P. 791–803.

[44] *Wesson J.R.* On Veblen-Wedderburn Systems // Amer. Math. Monthly. 1957. Vol. 64. No. 9. P. 631–635.

[45] *Zhang C., Ma J.* Counting solutions for the N-queens and latin square problems by Monte Carlo simulations // Phys. Rev. E 79. 2009.

РАБОТЫ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

[46] *Штуккерт П.К.* Квазиполя и проективные плоскости трансляций малых четных порядков // Известия Ирк.ГУ. 2014. Т.7. №1. С. 144–159.

[47] *Levchuk V.M., Shtukkert P.K.* Problems on structure for quasifields of orders 16 and 32 // J. of Siberian Federal University. Ser. Mathematics & Physics. 2014. Vol.7. No. 3. P. 362–372.

[48] *Кравцова О.В., Куршакова (Штуккерт) П.К.* К вопросу об изоморфизме полуполевых плоскостей // Красноярск: Вестник КГТУ. 2006. Т.42. С. 13–19.

[49] *Левчук В.М., Панов С.В., Штуккерт П.К.* Вопросы перечисления проективных плоскостей и латинских прямоугольников // В сб. научных статей "Моделирование и механика". Красноярск: СибГАУ. 2012. С. 56–70.

[50] *Штуккерт П.К.* Перечисление полуполевых плоскостей порядка 16 // Электронный сборник тез. докл. международной науч. конф. "Мальцевские чтения". Новосибирск: ИМ СО РАН. 2012. С. 53–54.

[51] *Штуккерт П.К.* Проективные плоскости и латинские квадраты // Материалы IV Российской школы-семинара "Синтаксис и семантика логических систем". Улан-Удэ: БГУ. 2012. С. 151–152.

[52] *Штуккерт П.К.* Перечисление полуполевых плоскостей и латинских квадратов малых порядков // Матерериалы Всерос. конф. "VII всесибирский конгресс женщин-математиков". Красноярск: СФУ. 2012. С. 235–237.

[53] *Polina K. Shtukkert* Semifields planes and Latin squares // Intern. Conf. on Algebra. Kiev: Ukrainian Nat. Acad. Sci. 2012. P. 145.

[54] *Штуккерт П.К.* О свойствах полуполей четного порядка // Электронный сборник тез. докл. международной науч. конф. "Мальцевские чтения". Новосибирск: ИМ СО РАН. 2013. С. 114.

[55] *Levchuk V.M., Panov S.V., Shtukkert P.K.* The structure of finite quasifields and their projective translation planes // Proceed. XII Intern. Conf. on Alg. and Number Theory. Tula. 2014. P. 106–108.

Наиболее употребительные обозначения

$Q^* = Q \setminus \{0\}$ – лупа ненулевых элементов квазиполя Q;

$|y|$ – порядок элемента лупы;

W – координатизирующее множество плоскости;

$R, \theta(W)$ – регулярное множество плоскости;

$GF(q)$ – поле Галуа порядка q;

$M(n, F)$ – кольцо всех $n \times n$-матриц над F;

$GL(n, F)$ – группа всех обратимых над F $n \times n$-матриц;

$R_{r \times n}$ — число редуцированных латинских $r \times n$-прямоугольников;

$L_{r \times n}$ — число всех латинских $r \times n$-прямоугольников.