ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

На правах рукописи

Кравцова Ольга Вадимовна

ВОПРОСЫ СТРОЕНИЯ КОНЕЧНЫХ КВАЗИПОЛЕЙ И ГРУПП КОЛЛИНЕАЦИЙ ПОЛУПОЛЕВЫХ ПРОЕКТИВНЫХ ПЛОСКОСТЕЙ

01.01.06 — математическая логика, алгебра и теория чисел

Диссертация на соискание ученой степени
доктора физико-математических наук

Научный консультант:
доктор физ.-мат. наук, профессор,
академик РАО
Подуфалов Николай Дмитриевич

Красноярск – 2022

Содержание

Введение

Диссертация посвящена изучению вопросов строения групп коллинеаций конечных недезарговых проективных плоскостей и их координатизирующих алгебраических систем.

Исследования проективных плоскостей трансляций и координатизирующих квазиполей восходят к началу 20-го века (О. Веблен, Д. Маклаган–Веддерберн [113], Л. Диксон [47]). Взаимосвязь обусловлена координатизацией конечной проективной плоскости элементами алгебраической системы, что приводит к зависимости геометрических свойств плоскости от алгебраических свойств координатизирующего множества, и наоборот.

Начиная с работ Д. Кнута и Э. Клейнфелда [81, 80] 1960-х годов, исследования конечных квазиполей и ассоциированных плоскостей трансляций систематически используют методы компьютерной алгебры. Эти исследования отражены в обширном обзоре Н. Джонсона, В. Джа и М. Билиотти [72], см. также монографию Д. Хьюза и Ф. Пайпера [68].

Хорошо известна неразрешимость группы коллинеаций дезарговой проективной плоскости. В 1959 г. Д. Хьюз выдвинул [65] гипотезу о разрешимости группы коллинеаций конечной недезарговой полуполевой плоскости, см. также монографию [68], 1973 г. Напомним, что плоскость трансляций является полуполевой, если дуальная к ней также является плоскостью трансляций.

Общего подхода к решению проблемы до сих пор не найдено. Продвижение для отдельных классов полуполевых плоскостей с 1960-х годов получали Д. Кнут [82], Д. Хьюз и М. Каллахер [69], Т. Остром [95], М. Ганли [51], М. Ганли и В. Джа [53], М. Билиотти, Н. Джонсон, В. Джа и Д. Меничетти [29], Х. Хуанг и Н. Джонсон [64], М. Кордеро [35].

В 1990 г. Н. Д. Подуфалов записал проблему разрешимости группы коллинеаций полуполевой плоскости в Коуровскую тетрадь [10, Вопрос 11.76]. В период 1990–2000 гг. под его руководством получено несколько значимых результатов.

Значительное количество более поздних результатов о разрешимости получено для плоскостей малого порядка с использованием вычислительной техники. К результатам такого рода следует отнести работы И. Руа и других о полуполях и полуполевых плоскостях порядков 64, 81, 243 [102, 101, 103].

Взаимосвязанно с полуполевыми проективными плоскостями изучаются координатизирующие их полуполя. *Полуполем* называют алгебраическую систему, удовлетворяющую аксиомам тела, за исключением ассоциативности умножения. Первые примеры нетривиальных (не являющихся полями) конечных полуполей предложил в 1906 г. Л. Диксон. Ослабляя в определении полуполя двустороннюю дистрибутивность до односторонней, приходим к понятию *ква-*

зиполя. Квазиполе с ассоциативным умножением есть *почти-поле*. В отличие от конечных почти-полей, полностью классифицированных [121] Х. Цассенхаузом в 1936 г., ни полуполя, ни тем более квазиполя не получили к настоящему времени исчерпывающей классификации. В 2003 г. У. Кантор [77] записал: «Исследование конечных коммутативных полуполей было начато Диксоном почти столетие назад ... Удивительно, что до сих пор о них так мало известно».

В различных ситуациях вопросы строения конечных квазиполей изучались уже давно. Прежде всего, это вопрос

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

Следует подчеркнуть существование конечных квазиполей, центр которых не является подполем: например, четыре из семи исключительных почти-полей Цассенхауза. Отметим также, что для конечных почти-полей ранее устанавливалась единственность максимального подполя, содержащего центр [49]. Удается, тем не менее, привести примеры почти-полей с более чем одним максимальным подполем. Естественно исследовать предположение о возможной неограниченности их числа в целом.

(A1) *Существует ли такое натуральное число N, что количество максимальных подполей в произвольном конечном почти-поле меньше, чем N?*

Г. Венэ выдвинул в 1991 г. предположение [119]:

Всякое конечное полуполе является левопримитивным либо правопримитивным, то есть его мультипликативная лупа исчерпывается лево- либо, соответственно, правоупорядоченными степенями одного элемента.

Предположение Г. Венэ опровергнуто в 2004 г. И. Руа [100], представившим контрпример порядка 32. Это коммутативное *полуполе Кнута–Руа* не является ни право-, ни левопримитивным. Второй контрпример представляет *полуполе Хентзела–Руа* [61] порядка 64, построенное в 2007 г. К настоящему времени исследования проблемы примитивности полностью завершены для всех полуполей до порядка 125 включительно. Кроме двух указанных непримитивных полуполей, не обнаружено новых примеров. Контрпримеры нечетного порядка до сих пор не найдены. Естественным образом обобщают предположение Венэ следующие вопрос и гипотеза.

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

Гипотеза: *лупа Q^* всякого конечного полуполя Q однопорождена.*

С учетом неассоциативности умножения, для квазиполя выделяют три множества, аналогичные теоретико-групповому понятию спектра. Это левый и пра-

вый спектры как множества левых (соответственно, правых) порядков элементов и спектр как множество порядков. Изучается вопрос

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

Безусловный интерес вызывает строение группы автоморфизмов конечного квазиполя и вопрос

(D) *Найти порядок группы автоморфизмов.*

Вопросы **(A), (B), (C)** формулировал В. М. Левчук в 2013 г. в своем докладе на научно-исследовательском семинаре кафедры высшей алгебры ММФ МГУ, также см. [6, 85], полностью вопросы записывались в [134]. Вопрос **(A1)** В. М. Левчук поставил в 2019 г. (семинар кафедры высшей алгебры ММФ МГУ), записан в [141].

Целью диссертационного исследования является получение значимых результатов о строении групп коллинеаций конечных недезарговых полуполевых проективных плоскостей, обеспечивающих продвижение в решении проблемы Хьюза, а также решение вопросов **(A)**–**(D)** для широкого класса конечных квазиполей, координатизирующих конечные проективные плоскости трансляций.

Диссертация состоит из введения, семи глав и списка литературы. Номер теоремы, леммы и др. включает номер главы, параграфа и порядковый номер, таблицы имеют сквозную нумерацию.

В решении поставленных задач получил развитие метод регулярных множеств взаимосвязанного построения конечных проективных плоскостей трансляций и, как координатизирующих множеств, конечных квазиполей.

Пусть π – недезаргова проективная полуполевая плоскость порядка p^N, где p – простое число. Размерность N координатизирующего полуполя над его простым подполем в дальнейшем часто называется *рангом*. К основным результатам относятся следующие.

1. Доказано, что в группе коллинеаций $Aut\ \pi$ при нечетном $|\pi|$ нет подгрупп, изоморфных знакопеременной группе A_5.

2. Если $p \equiv 1 \pmod 4$, то в группе автотопизмов плоскости π нет диэдральной группы порядка 8 без гомологий.

3. Если $p > 2$ и N не делится на 2^{2m+1}, то в группе коллинеаций $Aut\ \pi$ нет подгрупп, изоморфных группе Судзуки $Sz(2^{2n+1})$ для всех $n \geq m$.

4. Если $p \not\equiv -1 \pmod 4$, $N = 2^m \cdot s$, s нечетно, то группа коллинеаций $Aut\ \pi$ не содержит подгрупп, изоморфных $PSL(2, q)$, где $q \equiv 1 \pmod{2^{m+2}}$.

5. Если $p \equiv 1 (\mathrm{mod}\, 4)$, N не делится на 4 или $N = 4$, то в группе автотопизмов плоскости π нет подгрупп, изоморфных группе $SL(2, 5)$.

6. Вопросы **(A)**–**(D)** строения конечных квазиполей решены для известных контрпримеров к гипотезе Венэ – полуполя Кнута–Руа порядка 32, полуполя Хентзела–Руа порядка 64, некоторых полуполей порядков 3^4, 5^4, 13^4, а также завершены для всех полуполей порядка 16.

7. Вопросы **(A)**–**(D)**, в основном, решены для всех конечных почти-полей. Гипотеза к вопросу **(A)** о неограниченности, в целом, числа максимальных подполей конечного почти-поля подтверждена даже в классе минимальных собственных почти-полей.

Другие результаты, имеющие самостоятельное значение, следующие.

8. Ранг N плоскости π представляет естественные ограничения на порядок элементарной абелевой 2-подгруппы и на порядок 2-элемента в группе автотопизмов, при дополнительных условиях на их геометрический смысл.

9. Построено матричное представление регулярного множества полуполевой проективной плоскости порядка p^N в предположении, что группа автотопизмов содержит:

а) бэровскую инволюцию, автотопизм порядка 4;

б) подгруппу, изоморфную знакопеременной группе A_4 (для $p > 2$);

в) подгруппу, изоморфную группе кватернионов Q_8 (для $p \equiv 1 \pmod 4$));

г) подгруппу, изоморфную симметрической группе S_3 (если плоскость имеет ранг 2 над ядром).

10. Построены примеры конечных недезарговых полуполевых проективных плоскостей, допускающих:

а) бэровскую инволюцию, автотопизм порядка 4;

б) подгруппу автотопизмов, изоморфную Q_8;

в) подгруппу автотопизмов, изоморфную S_3.

11. Построены новые примеры 3-примитивных полуполевых плоскостей порядка 81, дополняющие список М. Кордеро.

12. Разработан метод односторонне упорядоченных минимальных многочленов в конечных полуполях, обобщающих классическое понятие минимального многочлена элемента конечного поля.

13. Разработаны пакеты прикладных компьютерных программ для построения и исследования конечных полуполей и полуполевых проективных плоскостей.

14. Доказано существование минимальных собственных почти-полей произвольной простой степени расширения $n > 2$ над своим центром.

15. Построено матричное представление регулярного множества конечного почти-поля, двумерного над центром, допускающее обобщение на бесконечный случай.

16. Доказано, что не существует неассоциативных квазиполей порядка 25 с мультипликативной лупой Муфанг.

Глава 1 содержит, главным образом, основные определения и технические результаты, необходимые для дальнейшей работы.

В § 1.1 вводятся определения квазиполя, полуполя, почти-поля, лево- и правоупорядоченных степеней элементов мультипликативной лупы, левых и правых порядков, левых и правых спектров.

В § 1.2 приводится используемая терминология, в соответствии, в основном, с монографией Д. Хьюза и Ф. Пайпера [68]. Перечисляются основные понятия проективной геометрии, кратко описывается схема координатизации конечной проективной плоскости, устанавливается связь геометрических свойств плоскости и алгебраических свойств координатизирующего множества.

В § 1.3 перечисляются основные задачи диссертационной работы.

Глава 2 содержит предварительное обсуждение предлагаемой программы решения проблемы Хьюза и описание основного применяемого метода.

В § 2.1 вводится основное для дальнейших исследований понятие регулярного множества (spread set) плоскости трансляций и, соответственно, координатизирующего квазиполя. Устанавливается естественная взаимосвязь между свойствами регулярного множества и свойствами квазиполя. Приводится обоснование представления регулярного множества над простым подполем квазиполя (так называемого «гиперкуба», в случае полуполя).

В § 2.2 кратко описываются особенности строения группы коллинеаций полуполевой проективной плоскости. Вводятся понятия ядер полуполя, группы автотопизмов, приводится матричное представление центральных коллинеаций в группе автотопизмов.

§ 2.3 посвящен обсуждению гипотезы разрешимости недезарговой полуполевой проективной плоскости конечного порядка, с обоснованием редукции к разрешимости группы автотопизмов и, далее, к случаю существования бэровской инволюции в группе автотопизмов. Перечислены некоторые известные результаты, в том числе доказанные автором в кандидатской диссертации (теорема 2.3.2, подробно обзор [125]). Предложена программа дальнейшего исследования проблемы.

Результаты, приведенные в главах 1–2, являются, в-основном, известными фактами. Лемма 2.1.5 доказана автором в [132], лемма 2.2.6 опубликована в совместной работе [125] (соавторы Н. Д. Подуфалов, Б. К. Дураков, Е. Б. Дураков) в нераздельном соавторстве.

В **главе 3** рассматривается проблема Хьюза. В предположении неразрешимости группы коллинеаций недезарговой полуполевой плоскости конечного порядка композиционные факторы должны быть изоморфны известным простым неабелевым группам [3, гл. 5, § 16]. Представленная программа исследований заключается в исключении из списка возможных подгрупп группы автотопизмов бесконечных серий простых групп, при особом внимании к минимальным простым группам из списка Д. Г. Томпсона. Основным результатом главы 3 является доказательство для любой недезарговой полуполевой плоскости нечетного порядка отсутствия в группе коллинеаций подгруппы, изоморфной A_5, и при условии на характеристику основного поля – изоморфной D_8. Для доказательства потребовалось построить матричное представление регулярного множества для полуполевых плоскостей с ограничениями на группу автотопизмов.

В § 3.1 построено матричное представление бэровской инволюции в группе автотопизмов полуполевой плоскости конечного порядка, а также матричное представление регулярного множества плоскости, допускающей бэровскую инволюцию – отдельно для четного и для нечетного порядков.

Основными результатами этого параграфа являются теоремы 3.1.2, 3.1.3, 3.1.5, обобщающие двумерный случай, рассмотренный М. Билиотти и другими в [29], на случай линейного пространства произвольной размерности над полем простого порядка.

В § 3.2 получено матричное представление элементарной абелевой 2-подгруппы в группе автотопизмов полуполевой плоскости, единообразное для случаев четного и нечетного порядка (теорема 3.2.1). Если такая подгруппа порядка 2^m порождена бэровскими инволюциями, фиксирующими поточечно различные бэровские подплоскости, то ранг N плоскости π делится на 2^m. К основным результатом параграфа также относится

Теорема 3.2.4. *Пусть π – недезаргова полуполевая плоскость порядка p^N ($p > 2$ – простое). Если N не делится на 2^{2m+1}, то группа автотопизмов плоскости π не содержит подгрупп, изоморфных $Sz(2^{2n+1})$ для всех $n \geq m$.*

Для случая полуполевой плоскости четного порядка теорема 3.2.8 и предложение 3.2.9 обсуждают возможность существования подгруппы, изоморфной знакопеременной группе A_4, в группе автотопизмов.

Метод регулярного множества применен в § 3.3 для установления естественного ограничения на порядок 2-элементов в группе автотопизмов, а также для записи матричного представления автотопизмов порядка 4. Основной результат представлен в следующей теореме.

Теорема 3.3.3. *Пусть π – полуполевая плоскость порядка p^N, p – простое, $p \not\equiv -1 \pmod 4$. Если α – автотопизм порядка 2^n плоскости π и группа $\langle\alpha\rangle$ не содержит гомологий, то N делится на 2^n.*

Следствие 3.3.8 выделяет группы $PSL(2,q)$, которые не могут быть подгруппами автотопизмов полуполевой плоскости данного порядка.

Следствие 3.3.8. *Пусть π – недезаргова полуполевая плоскость порядка p^N, где $p=2$ или $p\equiv 1 \pmod 4$, $N=2^m\cdot s$, s нечетно. Группа автотопизмов Λ плоскости π не содержит подгрупп, изоморфных $PSL(2,q)$, где $q-1$ делится на 2^{m+2}.*

Сочетание с результатами предыдущего параграфа выявляет еще один класс полуполевых плоскостей с разрешимой группой коллинеаций (следствие 3.3.7).

Матричное представление регулярного множества полуполевой плоскости нечетного порядка, допускающей подгруппу автотопизмов, изоморфную A_4, найдено в § 3.4 (теорема 3.4.2). Для плоскости нечетного порядка ранга 2 над ядром показано, что такая подгруппа автотопизмов отсутствует (лемма 3.4.1).

Параграф 3.5 посвящен доказательству основного результата.

Теорема 3.5.2. *Пусть π – недезаргова полуполевая плоскость нечетного порядка p^N ($p>2$ – простое). Тогда ее группа автотопизмов Λ не может содержать подгруппу, изоморфную знакопеременной группе A_5.*

Эта теорема доказана на основе матричного представления регулярного множества, полученного в теореме 3.5.1. Непосредственно из теоремы 3.5.2 следует, что группа автотопизмов недезарговой полуполевой плоскости произвольного нечетного порядка не может содержать также знакопеременные и симметрические группы A_n и S_n для всех $n\geq 5$, а также и некоторые другие неабелевы группы.

Основные результаты § 3.6 доказаны с применением теорем из § 3.2 и 3.3.

Теорема 3.6.1. *Недезаргова полуполевая плоскость π порядка p^N, где $p>2$ – простое, $p\equiv 1 \pmod 4$, не допускает подгруппы автотопизмов, изоморфной диэдральной группе порядка 8 и не содержащей гомологий.*

К числу основных относится и вытекающая из этого результата теорема 3.6.3. Диэдральная группа D_8 содержится почти в каждой конечной простой неабелевой группе. Результаты Д. Голдшмидта о сильно замкнутых подгруппах ([54], см. также Д. Горенстейн [55]) перечисляют исключения.

Теорема 3.6.3 *Пусть π – недезаргова полуполевая плоскость порядка p^N, где $p>2$ – простое, $p\equiv 1 \pmod 4$. Тогда ее группа автотопизмов Λ не содержит простых неабелевых подгрупп, за исключением, возможно, следующих: $PSL(2,2^n)$, $n\geq 2$, $PSU(3,2^n)$, $n\geq 2$, $Sz(2^n)$, n нечетно, $n>1$, $PSL(2,q)$, $q\equiv\pm 3 \pmod 8$, J_1 или ${}^2G_2(3^n)$, n нечетно, $n>1$.*

Параграф 3.7 посвящен обсуждению возможности существования A_5 как фактор-группы в группе автотопизмов недезарговой полуполевой плоскости

нечетного порядка. Так как A_5 изоморфна фактор-группе группы $SL(2,5)$ по центру, и силовская 2-подгруппа в $SL(2,5)$ изоморфна группе кватернионов Q_8, то поставлена задача построения матричного представления регулярного множества полуполевой плоскости, допускающей Q_8 в группе автотопизмов. Задача решена в теореме 3.7.1 для полуполевой плоскости нечетного порядка p^N, где $p-1$ делится на 4. Изучение случая $N=4$ приводит к следующему важному результату.

Теорема 3.7.2. *Пусть π – недезаргова полуполевая плоскость нечетного порядка p^N, $p>2$ – простое, $p \equiv 1 \pmod 4$. Если $N=4$ или N не делится на 4, то ее группа автотопизмов Λ не может содержать подгруппу, изоморфную $SL(2,5)$.*

В § 3.8 метод регулярного множества применяется для изучения полуполевых плоскостей ранга 2 над ядром, допускающих подгруппу автотопизмов, изоморфную S_3. Основные результаты этого параграфа (теоремы 3.8.1, 3.8.3 и 3.8.4) допускают дальнейшее обобщение на многомерный случай.

Результаты третьей главы, относящиеся к бэровской инволюции и группе A_4, опубликованы автором в [129] и [131]; относящиеся к двумерному случаю для A_4 – совместно с дипломницей В. О. Прамзиной в [127], автору принадлежит идея доказательства для группы автотопизмов, дипломнице – доказательство для трансляционного дополнения. Основные результаты, связанные с группой A_5, опубликованы совместно с Б. К. Дураковым в [136], а также в [142] без соавторов. Б. К. Дуракову в [136] принадлежит постановка задачи и обсуждение результатов, все результаты доказаны диссертантом лично. Результаты, относящиеся к группе Q_8, опубликованы автором в [143]; об элементарной абелевой 2-подгруппе и группах Судзуки – в [144], о 2-элементах в группе автотопизмов – в [145]. Теоремы о диэдральной группе D_8 представлены в [147]. Результаты, связанные с группой S_3, опубликованы в [138] (соавтор Т. В. Моисеенкова) в нераздельном соавторстве.

В **главе 4** рассматриваются примеры полуполевых плоскостей, иллюстрирующие теоретические результаты главы 3. Запись в общем виде матричного представления регулярного множества полуполевой плоскости при определенных ограничениях на коллинеации не является достаточным условием существования таких плоскостей. Поэтому важно показать, что множество изучаемых объектов не пусто либо, напротив, доказать его пустоту (см. теоремы о подгруппе, изоморфной A_5, 3.5.1 и 3.5.2).

В § 4.1 перечислены минимальные примеры полуполевых плоскостей ранга 2 над ядром, допускающие S_3 в группе автотопизмов (примеры к теоремам 3.8.1 и 3.8.4.) Представлены примеры к теореме 3.1.2 полуполевых плоскостей четного порядка, допускающих бэровскую инволюцию (теорема 4.1.1). Приложениями

к теореме 3.7.1 являются примеры полуполевых плоскостей порядков 5^4 и 13^4, допускающих подгруппу автотопизмов, изоморфную группе кватернионов Q_8 (теорема 4.1.2). Кратко описан алгоритм построения полуполевых плоскостей на основе матричного представления их регулярного множества с применением вычислительной техники.

В § 4.2 также обсуждается использование методов компьютерной алгебры для доказательства изоморфизма двух полуполевых плоскостей. Описана возможность оптимизации алгоритма проверки, за счет сокращения перебора, в случае, когда хотя бы одно из ядер координатизирующего полуполя отлично от простого подполя.

Параграф 4.3 посвящен построению примеров полуполевых плоскостей порядка 81, допускающих бэровскую инволюцию (к теореме 3.1.2). Основной результат (теорема 4.3.1) показывает, что все построенные примеры являются 3-примитивными плоскостями. Понятие p-примитивных полуполевых плоскостей возникло в работе Й. Хирамин, М. Мацумото и Т. Ояма [62]. Исследование было продолжено М. Кордеро [37], построившей примеры четырех 3-примитивных плоскостей порядка 81. С использованием результатов И. В. Шевелевой (Бусаркиной) [12] показано существование еще четырех 3-примитивных плоскостей вне перечня М. Кордеро.

Результаты главы 4 о полуполевых плоскостях, допускающих S_3, опубликованы в совместной работе [138] (соавтор Т. В. Моисеенкова) в нераздельном соавторстве. Результаты о полуполевых плоскостях порядков 16 и 81, допускающих бэровскую инволюцию, опубликованы автором в [129, 131], о полуполевых плоскостях, допускающих Q_8 – в [143]. Результаты о 3-примитивных полуполевых плоскостях опубликованы в совместной работе [140] (соавтор И. В. Шевелева), компьютерные вычисления и доказательства основных результатов проведены автором.

Глава 5 посвящена решению вопросов **(A)**–**(D)** для некоторых конечных полуполей. В § 5.1 перечисляются известные классификационные результаты, обсуждается взаимосвязь автотопизмов полуполевой проективной плоскости с автотопизмами и автоморфизмами конечного полуполя (теорема 5.1.7), матричное представление автотопизмов и автоморфизмов с использованием регулярного множества.

В § 5.2 описан геометрический смысл инволютивного автоморфизма конечного полуполя (теорема 5.2.1) и на основе этого результата определен стабилизатор инволютивного автоморфизма (теоремы 5.2.3, 5.2.4). Изучается понятие внутреннего автоморфизма полуполя, введенное Г. Венэ [120]. Лемма 5.2.6 вводит матричное представление внутреннего автоморфизма, теорема 5.2.7 выделяет элементы полуполя, которые не могут порождать нетривиальный внут-

ренний автоморфизм.

Параграф 5.3 вводит понятие лево- и правоупорядоченного минимальных многочленов конечного полуполя, на основе классического понятия минимального многочлена элемента конечного поля, с использованием лево- и правоупорядоченных степеней элемента лупы. Свойства односторонне упорядоченных минимальных многочленов, в сравнении с классическими, демонстрируют теоремы 5.3.5 и 5.3.6. Теорема 5.3.8 выявляет связь правоупорядоченного минимального многочлена элемента с минимальным многочленом ассоциированной матрицы регулярного множества. Следствие 5.3.12 выделяет в конечном полуполе, используя минимальные многочлены, объединение всех подполей порядка p^2. При помощи техники минимальных многочленов доказывается также теорема 5.3.13 о минимальных собственных полуполях.

В § 5.4 представлено полное решение вопросов **(A)**–**(D)** для полуполей порядка 16; это минимальный возможный порядок конечного полуполя. Автор дополняет теорему 5.4.1, доказанную П. К. Штуккерт и В. М. Левчуком [6], более подробной информацией о строении таких полуполей. Эта информация, в том числе об «аномальных» внутренних автоморфизмах, представлена в теоремах 5.4.5, 5.4.6 и табл. 10–13. Кроме записи умножения с помощью регулярного множества, автором предложен способ умножения элементов полуполя, определенный на парах элементов подходящего конечного поля (теорема 5.4.7).

Параграф 5.5 представляет обсуждение гипотезы лево-(право-)примитивности конечного полуполя, выдвинутой Г. Венэ в 1991 г., ее контрпримеров и обобщений. Автор использует введенную технику минимальных многочленов для доказательства лево-(право-)цикличности некоторых полуполей порядка p^4 (теорема 5.5.8).

В § 5.6 и 5.7 представлено полное решение вопросов **(A)**–**(D)** для исключительных непримитивных полуполей Кнута–Руа порядка 32 и Хентзела–Руа порядка 64, опровергающих гипотезу Венэ, дополненное информацией о внутренних автоморфизмах и минимальных многочленах. Основные результаты этих параграфов изложены в теоремах 5.6.2, 5.6.3, 5.7.1 и табл. 14–15.

Параграф 5.8 содержит решение вопросов **(A)**–**(D)** для некоторых полуполей порядка p^4, $p = 3, 5, 13$, построенных для иллюстрации теоретических результатов главы 3 (подробнее эти примеры описаны в главе 4). Основными результатами параграфа являются теоремы 5.8.1, 5.8.2, 5.8.3, информация обобщена в табл. 16–19.

Теоремы об автотопизмах, автоморфизмах и минимальных многочленах опубликованы автором в [132] и [135]. Результаты о полуполях порядка 16 и исключительных полуполях порядков 32 и 64 получены автором лично и опубликованы в совместной работе [134] (соавтор В. М. Левчук), а также в [133] – о

полуполе Хентзела–Руа. Результаты о полуполях порядка 81 опубликованы в [131], а также, с дополнениями, в совместной работе [140] (соавтор И. В. Шевелева), результаты получены автором лично. Результаты о полуполях порядков 5^4 и 13^4 опубликованы в [143, 184].

Глава 6 содержит решение вопросов **(B)**–**(D)** для конечных почти-полей. Параграф 6.1 напоминает способ построения конечных почти-полей на основе 2-транзитивных групп, а также конструкцию Диксона–Цассенхауза. Теорема 6.1.6 устанавливает связь между центром, ядром и простым подполем, она демонстрирует, в качестве исключений, точно четыре почти-поля Цассенхауза, в которых простое подполе не лежит в центре.

Параграф 6.2 представляет спектр групповых порядков мультипликативной группы (теорема 6.2.4) и известные результаты Цассенхауза об автоморфизмах почти-полей. Параграф 6.3 предлагает необходимый признак регулярного множества почти-поля порядка q^2 с ядром порядка q (теорема 6.3.2). В § 6.4 кратко представлена взаимосвязь бесконечных точно дважды транзитивных групп с почти-областями и почти-полями. С учетом новых результатов К. Тент и других авторов [109, 108], не каждая почти-область является почти-полем.

Выполнение ассоциативного закона умножения при определенном порядке записи элементов конечной лупы приводит к переносу некоторых важных групповых свойств на такие лупы Муфанг. Параграф 6.5 представляет отрицательное решение вопроса А.В. Заварницина (Мальцевские чтения, 2020, устная постановка) о существовании нетривиальных конечных квазиполей с мультипликативной лупой Муфанг. Теорема 6.5.1 использует метод регулярного множества и дает отрицательный ответ для квазиполей порядка 25.

Глава 7 решает, в-основном, вопрос **(A)** о максимальных подполях в конечных почти-полях (§ 7.1, теоремы 7.1.3 и 7.1.4). Решение существенно использует соответствие С. Данкс под-почти-полей и делителей степени расширения почти-поля над простым подполем [40].

В § 7.2 обсуждаются минимальные собственные почти-поля, т.е. нетривиальные почти-поля Q, в которых каждое под-почти-поле $H \neq Q$ является подполем. Теорема 7.2.3 демонстрирует существование минимальных собственных почти-полей в классе почти-полей Диксона $DF(q, n)$ для любого простого $n > 2$.

Теорема 7.2.3. *Для любого простого числа $n > 2$ существует бесконечно много конечных почти-полей степени расширения n над своим центром, в каждом из которых все под-почти-поля являются подполями.*

Для минимальной степени расширения $n = 2$ этот результат, в общем случае, неверен, что показывает теорема 7.2.2. Теорема 7.2.4 представляет отрицательное решение вопроса об ограниченности числа максимальных подполей даже для минимальных собственных почти-полей Диксона.

Теорема 7.2.4. *Для любого натурального числа s существует минимальное собственное почти-поле Диксона, имеющее более чем s максимальных подполей.*

Основные теоремы параграфов 6.2, 7.1 опубликованы в совместной работе [139] (соавтор В. М. Левчук); автору принадлежат, в основном, идеи доказательства, В. М. Левчуку – уточнение и совершенствование формулировок. Все теоремы § 7.2 опубликованы автором в [141]. Результаты параграфов 6.3 и 6.5 представлены в совместной работе [146] (соавтор Д. С. Скок, магистрант); автору принадлежат основные теоремы, Д. С. Скок – построение примеров.

Все основные результаты диссертации являются новыми.

Все основные результаты диссертации опубликованы, в том числе в рецензируемых журналах [123]–[147]. Диссертация носит теоретический характер. Полученные результаты могут быть использованы в исследованиях полуполевых проективных плоскостей (в том числе проблемы разрешимости группы коллинеаций), в классификации конечных полуполей, а также при чтении спецкурсов. Результаты диссертации также могут быть использованы при составлении программ специальных курсов для бакалавров, магистрантов и аспирантов университетских математических кафедр.

Результаты диссертации апробировались на алгебраических семинарах в МГУ (2019), ИМ СФУ (2015–2022), Институте математики СО РАН (Новосибирск, 2019-2020). Они были представлены на Международных алгебраических конференциях (Москва, 1998, 2018, 2019), Международных конференциях «Алгебра и ее приложения» (Красноярск, 2002, 2007), Международных конференциях «Алгебра и логика: теория и приложения» (Красноярск, 2010, 2013, 2016), Международной конференции «Алгебра и математическая логика: теория и приложения» (Казань, 2014), Международной конференции по алгебре, анализу и геометрии (Казань, 2016, 2021), Международных конференциях «Группы и графы» (G2A2, Екатеринбург, 2015; G2S2, Новосибирск, 2016), Международной конференции «Математика в современном мире» (Новосибирск, 2017), Международной конференции «Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения» (Тула, 2018), Международной конференции «Алгебра, теория чисел, дискретная геометрия и многомасштабное моделирование: современные проблемы, приложения и проблемы истории» (Тула, 2021, 2022), Всесибирских Конгрессах женщин-математиков (Красноярск, 2004, 2006, 2012), Всероссийской конференции «Алгебра и теория алгоритмов» (Иваново, 2018), Всероссийской конференции по математике и механике (Томск, 2018), Международной конференции «Group theory in Ankara» (Анкара, 2019), Международной конференции «Мальцевские чтения» (Новосибирск, 2020, 2021), XIII школе-конференции по теории групп (Екатеринбург, 2020), Международ-

ной алгебраической конференции (Екатеринбург, 2021).

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проекты 12-01-00968 А, 15-01-04897 А, 16-01-00707 А, 19-01-00566 А) и Красноярского математического центра.

В заключение автор выражает благодарность своему научному консультанту Николаю Дмитриевичу Подуфалову за помощь и консультации. Автор благодарит Владимира Михайловича Левчука, научного консультанта докторантуры, за предложенное расширение тематики исследования, за постоянную активную поддержку. Автор выражает искреннюю признательность Борису Константиновичу Дуракову, учителю и руководителю, за всестороннюю помощь, поддержку и постоянное внимание к работе, а также Виктору Даниловичу Мазурову и Анатолию Ильичу Созутову за неизменные интерес и поддержку исследований.

Глава 1. Недезарговы полуполевые плоскости и их координатизирующие квазиполя

В этой главе приводится наиболее употребляемая терминология, в соответствии, в основном, с монографией Д. Хьюза и Ф. Пайпера [68], а также основные технические результаты, необходимые для дальнейшей работы.

В § 1.1 вводятся определения квазиполя, полуполя, почти-поля, лево- и правоупорядоченных степеней элементов мультипликативной лупы, левых и правых порядков, левых и правых спектров.

В § 1.2 вводятся основные понятия проективной геометрии, кратко описывается схема координатизации конечной проективной плоскости. Введение координат для точек и прямых проективной плоскости устанавливает тесную связь между геометрическими свойствами плоскости и алгебраическими свойствами координатизирующего множества. Эта взаимосвязь предопределяет необходимость проведения совместных исследований проективных плоскостей и квазиполей.

В § 1.3 перечисляются основные задачи, решаемые в работе: о строении группы коллинеаций полуполевых проективных плоскостей и о строении конечных квазиполей.

1.1. Квазиполя и полуполя

Приведем необходимые определения изучаемых алгебраических систем, в соответствии с [68].

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

Определение 1.1.1. *Алгебраическая система $Q = (Q, +, \cdot)$ с бинарными операциями $+$ и $\cdot$ называется левым квазиполем, если*

1) $(Q, +)$ — абелева группа;

2) $Q^* = (Q \setminus \{0\}, \cdot)$ — лупа;

3) выполнен левый дистрибутивный закон $c(a + b) = ca + cb$ $(a, b, c \in Q)$;

4) $0 \cdot a = 0$ для всех $a \in Q$;

5) уравнение $ax = bx + c$ однозначно разрешимо для всех $a, b, c \in Q$, $a \neq b$.

Правое квазиполе определяют аналогично. Ясно, что все тела представляют тривиальные примеры квазиполей. Квазиполе, не являющееся телом, будем называть нетривиальным или собственным.

Изучение квазиполей началось с работ Л. Диксона 1906 г. [47], О. Веблена и Д. Маклагана–Веддерберна 1907 г. [113]. В литературе до 1975 г. квазиполя, как правило, назывались «системами Веблена–Веддерберна» (см., например, обзор Ч. Вейбела [118]).

В любом квазиполе подкольцо составляют целочисленные кратные единицы:

$$ke := \underbrace{e + e + \ldots + e}_{k \text{ раз}} = ek, \quad (-k)e := -(ke) = e(-k) \quad (k > 0), \quad 0e = 0 = e0.$$

Лемма 1.1.2. *Пусть Q — правое квазиполе с единицей e. Тогда*

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

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

В силу леммы 1.1.2 (прямое доказательство в [134] и [20]) понятие характеристики поля переносится на квазиполя. Если характеристика $p = char\, Q$ квазиполя Q положительна, то $\pi(\mathbb{Z})$ является единственным минимальным в Q (и простым) подполем и $\pi(\mathbb{Z}) \simeq \mathbb{Z}_p$.

Определение 1.1.3. *Ядром левого квазиполя Q называется множество элементов $k \in Q$, удовлетворяющих условиям:*

1) $(a + b)k = ak + bk$;

2) $(ab)k = a(bk)$ для всех $a, b \in Q$.

Ядро правого квазиполя определяют аналогично. Ядро квазиполя всегда является телом, поэтому обязательно содержит простое подполе. Квазиполе можно рассматривать как векторное пространство над своим ядром ([68, Теорема 7.2], см. также И. Андрэ [25]). Таким образом, конечное квазиполе имеет порядок p^m, где p – простое число. Ясно, что квазиполе простого порядка p является полем; хорошо известно, что квазиполе порядка 4 либо 8 также поле. Минимальный порядок нетривиального квазиполя равен 9, квазиполей такого порядка точно четыре.

Если в квазиполе выполняются оба дистрибутивных закона, то оно называется *полуполем*.

Определение 1.1.4. *Алгебраическая система $(S, +, \cdot)$ называется полуполем, если*

1) $(S, +)$ — абелева группа;

2) $S^* = (S \setminus \{0\}, \cdot)$ — лупа;

3) $c(a + b) = ca + cb$ и $(a + b)c = ac + bc$ $(a, b, c \in S)$.

Первые примеры нетривиальных конечных полуполей указаны Л. Диксоном в 1906 г. В ранней литературе термин «полуполе» не использовался. Алгебраическая структура, удовлетворяющая определению 1.1.4, называлась «неассоциативным кольцом с делением», «дистрибутивным квазиполем». Это «квазитело», в терминологии А. Г. Куроша [2]. Современный термин «semifield» используется с 1965 г., он был предложен Д. Кнутом [82] для упрощения терминологии.

Отметим, что термины «полуполе» и «полутело» используются некоторыми авторами также в смысле «алгебраическая структура, являющаяся одновременно мультипликативной группой и аддитивной коммутативной полугруппой, причём умножение дистрибутивно относительно сложения с обеих сторон» [114, 115]. Мы будем всюду далее использовать только определение 1.1.4.

Полуполе S обладает *правым обратным свойством* (RIP), если для любого $x \in S$ найдется такой элемент $x^{-1} \in S$, что для всех $y \in S$ верно $(yx)x^{-1} = y$.

Полуполе S называется *альтернативным*, если оно удовлетворяет обоим альтернативным законам:

$$x(xy) = x^2y, \quad (xy)y = xy^2 \qquad \forall x, y \in S.$$

Нам потребуются следующие хорошо известные теоремы: Скорнякова–Сан Суси 1.1.5, Артина–Цорна 1.1.6 (доказательство в монографии [68]) и теорема 1.1.7 Альберта [21] .

Теорема 1.1.5. *Полуполе S с правым обратным свойством альтернативно.*

Теорема 1.1.6. *Конечное альтернативное полуполе является полем.*

Теорема 1.1.7. *Конечное полуполе с ассоциативными степенями характеристики $p \neq 2$, центр которого состоит более чем из пяти элементов, является конечным полем.*

Если в (левом) квазиполе умножение ассоциативно, то такое квазиполе называют (левым) *почти-полем*. Первые примеры почти-полей были построены Л. Диксоном в 1905 г. [46], все конечные почти-поля полностью классифицировал Х. Цассенхауз в 1936 г. [121, 18], подробнее в главе 6.

Первые примеры конечных квазиполей, не являющихся ни полуполями, ни почти-полями, построил М. Холл [59] в 1943 г. (см. также [18]), это *квазиполя Холла*.

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

Рассмотрим произвольную мультипликативную лупу $(L, \cdot)$ с единицей e. Будем называть *n-й степенью* элемента $v \in L$ любое произведение n множителей, каждый из которых равен v. Например, четвертыми степенями являются

$$((vv)v)v, \quad v((vv)v), \quad (v(vv))v, \quad v(v(vv)), \quad (vv)(vv).$$

Порядок $|v|$ элемента v лупы обобщает соответствующее теоретико-групповое понятие: это наименьшее число $n \in \mathbb{N}$ такое, что хотя бы одна n-я степень элемента v при всевозможных расстановках скобок равна e; порядок бесконечен, если такое n не существует.

Левоупорядоченная n-я степень элемента $v \in L$ определяется индуктивно:

$$v^{(1} = v, \ v^{(i+1} = v \cdot v^{(i}, \ i = 1, 2, \ldots .$$

Левым порядком $|v|_l$ элемента v называется наименьшее число $n \in \mathbb{N}$ с условием $v^{(n} = e$; левый порядок бесконечен, если такое n не существует. Множество всех левых порядков называется *левым спектром* лупы. Правоупорядоченная степень, правый порядок и правый спектр определяются аналогично.

Порядки элементов любой конечной лупы также конечны. Действительно, справедлива лемма (В. М. Левчук, [134]).

Лемма 1.1.8. *Порядок конечной лупы не меньше порядка любого ее элемента.*

Следующее определение связано с ситуацией, когда все элементы конечного квазиполя можно записать с использованием одного фиксированного элемента.

Определение 1.1.9. *Пусть $(Q,+,\cdot)$ – конечное квазиполе. Элемент $a \in Q^*$ называется правопримитивным, если мультипликативная лупа Q^* исчерпывается правоупорядоченными степенями этого элемента:*

$$Q^* = \{e, a, a^{2)}, a^{3)}, \dots\}.$$

Квазиполе Q, содержащее правопримитивный элемент, также называется правопримитивным.

Левопримитивный элемент и левопримитивное квазиполе определяются аналогично.

Наряду с классическим определением изоморфизма, важным для квазиполей является понятие изотопизма.

Определение 1.1.10. *Тройка биективных отображений α, β, γ группоида $(S,\circ)$ на $(V,\cdot)$ называется изотопизмом, если*

$$x^\alpha \cdot y^\beta = (x \circ y)^\gamma \qquad \forall x, y \in S.$$

Изотопизмом квазиполей Q и W (*автотопизмом*, если $Q = W$) называется тройка изоморфизмов α, β, γ аддитивной группы $(Q,+)$ на $(W,+)$, если их ограничение на лупу Q^* является изотопизмом на W^*.

1.2. Недезарговы проективные плоскости и проблема Хьюза

Нам потребуются некоторые определения и известные факты из теории проективных плоскостей. Используются обозначения и термины, принятые в [68].

Определение 1.2.1. *Проективной плоскостью π называется тройка $\langle \mathcal{P}, \mathcal{L}, I\rangle$, где $\mathcal{P}$ – множество точек, $\mathcal{L}$ – множество прямых, I – отношение инцидентности между точками и прямыми, причем выполнены условия:*

1) любые две различные точки инцидентны с единственной прямой;

2) любые две различные прямые инцидентны с единственной точкой;

3) существует невырожденный четырехугольник, то есть четыре различные точки такие, что никакие три из них не инцидентны с одной прямой.

Отношение инцидентности обозначается символами I или $\in$. При $P \in l$ говорят обычно «точка лежит на прямой», «прямая проходит через точку».

Определение 1.2.2. *Аффинной плоскостью $\mathcal{A}$ называется тройка $\langle \mathcal{P}, \mathcal{L}, I\rangle$, где $\mathcal{P}$ – множество точек, $\mathcal{L}$ – множество прямых, I – отношение инцидентности между точками и прямыми, причем выполнены условия:*

1) любые две различные точки инцидентны с единственной прямой;

2) для любой прямой l и любой точки P, не инцидентной с l, существует единственная прямая m, содержащая P, которая не имеет с прямой l ни одной общей точки;

3) существуют три точки, не лежащие на одной прямой.

Определение 1.2.3. *Изоморфизмом φ проективных плоскостей π и π' называется взаимно однозначное отображение множества элементов плоскости π на множество элементов плоскости π', переводящее точки в точки, прямые в прямые и сохраняющее отношение инцидентности, то есть для любой точки A и любой прямой l плоскости π условие $A \in l$ выполняется тогда и только тогда, когда $A^\varphi \in l^\varphi$.*

Если π – проективная плоскость и $l \in \mathcal{L}$ – некоторая прямая, то π^l обозначим множество точек и прямых из π, полученное удалением прямой l и всех точек, инцидентных l. Тогда π^l – аффинная плоскость. Обратно, если $\mathcal{A}$ – аффинная плоскость, то существует единственная, с точностью до изоморфизма, проективная плоскость π с условием $\pi^l = \mathcal{A}$ для некоторой прямой l.

Если одна из прямых проективной плоскости содержит лишь конечное число точек, то все прямые этой плоскости содержат конечное число точек, более того, число это одинаково. В этом случае проективная плоскость называется *конечной*. Справедлива теорема [68].

Теорема 1.2.4. *Пусть π – конечная проективная плоскость. Тогда существует такое натуральное число $n \geq 2$, что:*

1) каждая прямая содержит ровно $n+1$ точек;

2) каждая точка лежит ровно на $n+1$ прямых;

3) π содержит ровно n^2+n+1 точку и n^2+n+1 прямую.

Такое число n называется *порядком* проективной плоскости, $|\pi| = n$. Проективная плоскость наименьшего возможного порядка $n = 2$ называется *плоскостью Фано*, в ней 7 точек и 7 прямых. Для каждого числа p^m, где p – простое, $m \in \mathbb{N}$, существует проективная плоскость порядка p^m. Более того, порядок любой известной проективной плоскости равен степени простого числа. Существует предположение: проективная плоскость порядка n существует тогда и только тогда, когда n является степенью простого числа.

Определение 1.2.5. *Пусть π – проективная плоскость. Обозначим через π^d множество точек и прямых с отношением инцидентности между ними, такое, что точки (прямые) π^d являются прямыми (точками) плоскости π и два элемента инцидентны в π^d тогда и только тогда, когда они инцидентны в плоскости π. π^d – проективная плоскость, называемая дуальной π.*

Изоморфизм проективной плоскости π на себя называется *коллинеацией*. Все коллинеации плоскости образуют группу $Aut\,\pi$, которая называется *полной группой коллинеаций* этой плоскости (дальше говорим *группа коллинеаций* для сокращения записи).

Определение 1.2.6. *Подмножество S точек и прямых проективной плоскости π называется бэровским подмножеством, если каждый элемент π инцидентен с некоторым элементом из S. Если подмножество S является подплоскостью, то оно называется бэровской подплоскостью.*

В [68] доказано: если π – конечная проективная плоскость порядка n и S – ее подплоскость порядка m, то S является бэровской подплоскостью только в случае $n = m^2$.

Определение 1.2.7. *Коллинеация проективной плоскости, поточечно стабилизирующая бэровскую подплоскость, называется бэровской коллинеацией.*

Среди всех коллинеаций проективной плоскости выделяется класс коллинеаций, называемых *перспективностями*, или *центральными коллинеациями*.

Определение 1.2.8. *Центральной называется коллинеация проективной плоскости, которая фиксирует поточечно некоторую прямую (ось), оставляет на месте некоторую точку (центр) и все прямые, проходящие через эту точку. Центральная коллинеация с центром V и осью l называется элацией, если $V \in l$, и называется гомологией, если $V \notin l$.*

Центральная коллинеация с центром V и осью l называется (V, l)-перспективностью. Известно [68], что перспективность порядка k проективной плоскости порядка n является элацией, если k делит n, или гомологией, если k делит $n - 1$. Кроме того, справедлив следующий важный результат.

Теорема 1.2.9. *Всякая коллинеация порядка 2 является либо перспективностью, либо бэровской коллинеацией.*

Пусть α — (V, l)-перспективность, β — произвольная коллинеация проективной плоскости. Тогда коллинеация $\beta^{-1}\alpha\beta$ является (V^β, l^β)-перспективностью [68].

Определение 1.2.10. *Пусть V – точка, l – прямая проективной плоскости π. Плоскость π называется (V, l)-транзитивной, если для любой пары точек A и B, лежащих на одной прямой с V и не принадлежащих l, существует центральная коллинеация α с центром V и осью l такая, что $A^\alpha = B$.*

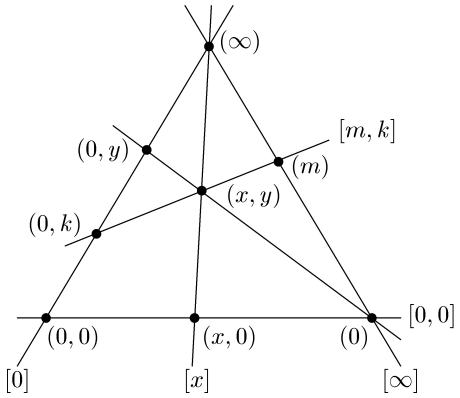

Рис. 1: Схема координатизации проективной плоскости

Определение 1.2.11. *Если проективная плоскость π (V,l)-транзитивна для любой точки $V \in l$ (то есть (l,l)-транзитивна), то π называется плоскостью трансляций относительно прямой l. Прямая l называется трансляционной прямой, элации с осью l образуют элементарную абелеву группу T, которая называется группой трансляций.*

Определение 1.2.12. *Если проективная плоскость π (V,l)-транзитивна для любой прямой l, проходящей через точку V (то есть (V,V)- транзитивна), то плоскость π называется дуальной трансляционной плоскостью с трансляционной точкой V.*

На любой конечной проективной плоскости можно ввести координаты с использованием элементов некоторого множества. Опишем кратко схему координатизации и установим взаимосвязь между коллинеациями проективной плоскости и алгебраическими свойствами координатизирующего множества.

Пусть π — проективная плоскость порядка n, Q — множество, состоящее из n символов, среди которых есть 0 и 1. Добавим к множеству Q также символ ∞. Существуют различные методы координатизации, с помощью которых устанавливается взаимно однозначное соответствие между точками и прямыми плоскости π и элементами либо парами элементов множества $Q \cup \{\infty\}$ (подробнее см. [68, 18]).

Одна из прямых плоскости обозначается символом $[\infty]$ и называется бесконечно удаленной, она состоит из точек с координатами (m), $m \in Q$, и точки (∞). Точка (m) является точкой пересечения всех прямых с координатами $[m,k]$ $(k \in Q)$, точка (∞) — точкой пересечения всех прямых $[b]$ $(b \in Q)$. Все точки плоскости, не лежащие на прямой $[\infty]$, имеют координаты (x,y) $(x,y \in Q)$. Произвольная прямая вида $[b]$ образована точками с координатами (b,y), $y \in Q$ (см. рис. 1).

На множестве Q вводят тернарную операцию T правилом: если $m,x,y \in Q$,

то $T(m,x,y)=k$ тогда и только тогда, когда точка (x,y) принадлежит прямой $[m,k]$. Эта тернарная операция определяет проективную плоскость порядка n системой из $n-1$ латинских квадратов порядка $n\times n$ (т.е. матриц с элементами из Q, в каждой строке и в каждом столбце которой любой элемент из Q встречается ровно один раз, подробнее см. [68]). Далее, на множестве Q задают бинарные операции $+$ и $\cdot$, полагая

$$a+b=T(1,a,b),\qquad a\cdot b=T(a,b,0)\quad (a,b\in Q).$$

Свойства планарного тернарного кольца и алгебраической системы $(Q,+,\cdot)$ тесно связаны с геометрическими свойствами плоскости. В частности, дезаргова плоскость (или классическая проективная плоскость) координатизируется телом (конечная дезаргова плоскость – полем). Если координаты плоскости трансляций выбраны так, что прямая $[\infty]$ является осью трансляций, координатизирующее множество плоскости — квазиполе.

Таблица 1. Взаимосвязь свойств проективной плоскости и координатизирующего множества

Название плоскости	**Геометрические свойства**	**Координатизирующее множество**
Паппова плоскость	(V,l)-транзитивность для всех точек V и всех прямых l, выполнена теорема Паппа	Поле
Дезаргова плоскость	(V,l)-транзитивность для всех точек V и всех прямых l	Тело
Муфангова плоскость	(V,l)-транзитивность для всех инцидентных пар (V,l)	Альтернативное полуполе
Полуполевая плоскость	(l,l)-транзитивность и (V,V)-транзитивность для одной инцидентной пары (V,l)	Полуполе
Плоскость почти-поля	(l,l)-транзитивность и (V,m)-транзитивность для всех $V\in l$, $V\notin m$	Почти-поле
Дуальная плоскость почти-поля	(V,V)-транзитивность и (W,l)-транзитивность для всех $V\in l$, $W\notin l$	Правое почти-поле
Плоскость трансляций	(l,l)-транзитивность для одной прямой l	Квазиполе
Дуальная плоскость трансляций	(V,V)-транзитивность для одной точки V	Правое квазиполе

Связь геометрических свойств конечной проективной плоскости и алгебраических свойств ее координатизирующего множества отражена в монографии [68, глава VI]. Эти результаты кратко представлены в табл. 1. Как видно из таблицы, полуполевая плоскость является одновременно плоскостью трансляций и дуальной плоскостью трансляций. Взаимосвязь свойств полуполей и полуполевых плоскостей иллюстрирует критерий Альберта изоморфизма полуполевых плоскостей [24].

Теорема 1.2.13. *Полуполевые плоскости изоморфны тогда и только тогда, когда их координатизирующие полуполя изотопны.*

Приведенные в табл. 1 результаты справедливы для метода координатизации Хьюза [68]. В этом случае точка (x, y) принадлежит прямой $[m, k]$ при условии $m \cdot x + k = y$. Далее нам будет удобнее использовать координатизацию Холла [18], тогда условие инцидентности меняется на $x \cdot m + k = y$. Это изменение приведет к необходимости замены левого дистрибутивного закона на правый, т.е. координатизации плоскости трансляций правым квазиполем.

Диаграмма (рис. 2), составленная М. Лаврау [83] (учитывая координатизацию Холла), отражает связь типов плоскостей трансляций и координатизирующих квазиполей. Любая конечная дезаргова плоскость является также муфанговой и папповой, согласно теоремам Диксона–Веддерберна и Артина–Цорна.

Если π – дезаргова проективная плоскость, то она может быть определена с помощью трехмерного линейного пространства V над телом K при помощи однородных координат (подробно см. [68]). Группа коллинеаций плоскости $\pi = \mathcal{P}(V)$ описана **основной теоремой проективной геометрии** для случая геометрической размерности два [68, следствие из теоремы 2.8]:

Группа всех автоморфизмов проективной плоскости $\mathcal{P}(V)$ индуцируется группой всех невырожденных полулинейных преобразований пространства V.

Таким образом, $Aut(\pi) \simeq P\Gamma L(V)$ и, в случае $K \simeq GF(q)$, $Aut(\pi) \simeq P\Gamma L_3(q)$. Для $q = p^r$, в соответствии с [18, теорема 20.9.4], имеем

$$|Aut(\pi)| = r(q^2 + q + 1)(q^2 + q)q^2(q - 1)^2.$$

Известны обобщения основной теоремы проективной геометрии на случай однородных координат из произвольного кольца (см., например, М. Оянгурен и Р. Шридхаран [94]. См. также В. М. Левчук, О. А. Старикова [5]).

Группа коллинеаций в случае конечной дезарговой плоскости, таким образом, неразрешима. Существует также значительное число примеров конечных плоскостей трансляций с неразрешимой группой коллинеаций, некоторые примеры будут перечислены в работе далее.

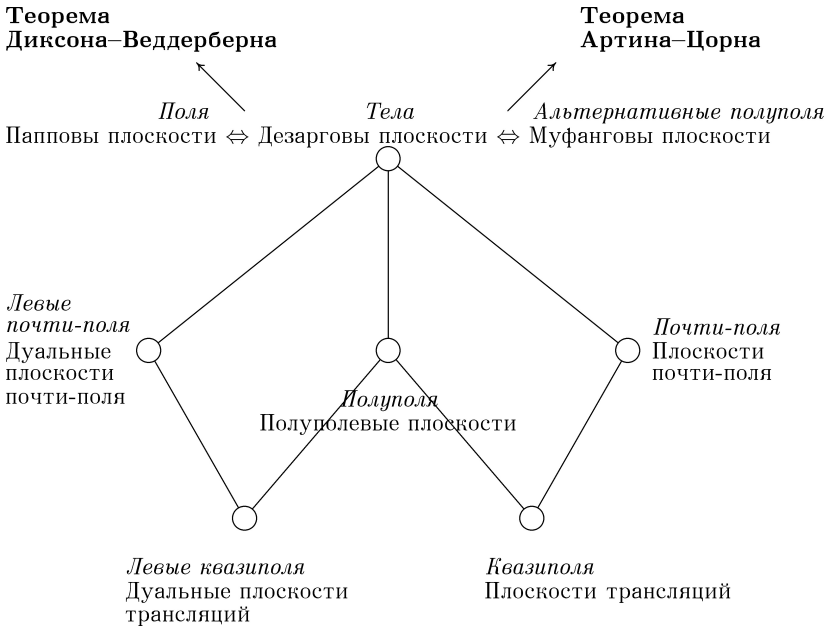

Рис. 2: Типы плоскостей трансляций и ассоциированных алгебраических систем (Д. Хьюз, Ф. Пайпер, М. Лаврау)

Ситуация меняется, если мы рассматриваем конечную недезаргову полулевую плоскость. Все такие плоскости, известные на текущий момент, имеют разрешимую группу коллинеаций, и задача доказательства разрешимости полной группы коллинеаций для произвольной проективной плоскости, координатизируемой конечным неассоциативным полуполем, известна с 1959 г. как *проблема Хъюза.*

1.3. Основные задачи

Исследования зависимости геометрических свойств плоскости трансляций от свойств и строения ее координатизирующего квазиполя, разумеется, вызывают интерес. С другой стороны, естественный интерес вызывают вопросы строения конечных квазиполей Q. В различных ситуациях они исследовались уже давно. Прежде всего, это вопрос

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

Для конечных почти-полей, взаимосвязанно с **(A)**, возникает вопрос:

(A1) *Существует ли такое натуральное число N, что количество максимальных подполей в произвольном конечном почти-поле меньше, чем N?*

Г. Венэ ввел [119] понятия право- и левопримитивного элементов квазиполя (определение 1.1.9) и выдвинул в 1991 г. предположение:

Всякое конечное полуполе является левопримитивным либо правопримитивным.

Это предположение опровергнуто в 2004 г. И. Руа [100], представившим контрпример порядка 32. Это коммутативное *полуполе Кнута–Руа* не является ни право-, ни левопримитивным. Второй контрпример представляет *полуполе Хентзела–Руа* [61] порядка 64, построенное в 2007 г. К настоящему времени исследования проблемы примитивности полностью завершены для всех полуполей до порядка 125 включительно. Кроме двух указанных непримитивных полуполей, не обнаружено новых примеров. Контрпримеры нечетного порядка до сих пор не найдены. Естественным образом обобщают предположение Венэ следующие вопрос и гипотеза.

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

Гипотеза: *лупа Q^* всякого конечного полуполя Q однопорождена.*

С учетом неассоциативности умножения, для квазиполя выделяют три множества, аналогичные теоретико-групповому понятию спектра. Это левый и правый спектры как множества левых (соответственно, правых) порядков элементов и спектр как множество порядков (см. § 1.1). Изучается вопрос

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

Безусловный интерес вызывает строение группы автоморфизмов конечного квазиполя и вопрос

(D) *Найти порядок группы автоморфизмов.*

Вопросы **(A), (B), (C)** формулировал В. М. Левчук в 2013 г. в своем докладе на научно-исследовательском семинаре кафедры высшей алгебры ММФ МГУ, также см. [6, 85], полностью вопросы записывались в [134]. Вопрос **(A1)** В. М. Левчук поставил в 2019 г. (семинар кафедры высшей алгебры ММФ МГУ), записан в [141].

Эти вопросы привлекали внимание исследователей и ранее. Так, работы С. Данкс [40, 41] и У. Фелгнера [49] посвящены изучению под-почти-полей и подполей в конечных почти-полях Диксона. М. Лаврау и О. Полверино в обзоре [84] перечислили вопросы строения конечных полуполей ранга два над ядрами (специальные подполя). В. Джа и Н. Джонсон показали [70], что центр конечного полуполя является его геометрическим инвариантом, сохраняясь при изотопизме. Исследованию гипотезы Венэ посвящены работы М. Кордеро и В. Джа

[38, 39], И. Руа и других [100, 104, 105]. Вопросы **(A)**–**(C)** для полуполей и квазиполей малых четных порядков решала П. К. Штуккерт [4, 6, 19, 86].

К изучаемым в диссертационной работе задачам относится также исследование известной **проблемы Хьюза**: *является ли разрешимой группа коллинеаций конечной недезарговой полуполевой проективной плоскости?*

Все примеры конечных недезарговых полуполевых плоскостей, построенных к середине 1950-х гг., имели разрешимую группу коллинеаций. В 1959 г. А. Альберт указал бесконечную серию полуполевых плоскостей, выбрав в качестве координатизирующего множества скрученное поле (twisted field). Такое полуполе можно построить на множестве элементов конечного поля F, выбрав автоморфизм $\sigma \in Aut(F)$, ненулевой элемент $c \in F$ с условием $c \neq x^\sigma x^{-1}\ \forall x \in F \setminus \{0\}$, и определив новую операцию $x * y := xy^\sigma - cyx^\sigma$. А. Альберт доказал, что конечная проективная плоскость, координатизируемая скрученным полем, имеет разрешимую группу коллинеаций [23, теоремы 6, 7].

В том же 1959 году Д. Хьюз в докладе [65] перечислил некоторые известные классы конечных проективных плоскостей и отметил существование плоскостей трансляций с неразрешимой группой коллинеаций – плоскостей Холла. Он выделил также три класса полуполевых плоскостей, группа коллинеаций которых разрешима. Это плоскости, координатизируемые скрученными полями (А. Альберт, [21, 22, 23]), полуядерными полуполями (semi-nuclear division rings, Д. Хьюз, Э. Клейнфелд, [67]), коммутативными полуполями Диксона (А. Альберт, [21]). Подчеркнув «фрагментарность знаний» о некоторых других конечных полуполях и полуполевых плоскостях, Д. Хьюз отметил, тем не менее, разрешимость группы коллинеаций и предположил, что это свойство может быть присуще всем недезарговым полуполевым плоскостям. Учитывая перечисленные результаты, он выдвинул *гипотезу о разрешимости группы автотопизмов конечного (неассоциативного) полуполя* (эквивалентно, группы коллинеаций недезарговой полуполевой проективной плоскости).

Гипотеза разрешимости в 1973 г. записана в монографии Д. Хьюза и Ф. Пайпера [68], в 1990 г. – Н. Д. Подуфаловым в Коуровской тетради [10, вопрос 11.76].

Подробнее известные результаты и программа решения обсуждаются в главе 2. Параграф 2.1 представляет основной метод исследования, связанный с использованием регулярного множества полуполевой плоскости (полуполя) над простым подполем. Параграф 2.2 перечисляет специальные коллинеации полуполевой плоскости и обосновывает редукцию проблемы к разрешимости группы автотопизмов. Параграф 2.3 представляет, наряду с известными результатами, программу решения проблемы с учетом классификации конечных простых групп и теоремы Д. Г. Томпсона о минимальных простых группах.

Глава 3 представляет последовательные шаги применения представленной программы. Она описывает применение метода регулярного множества для построения конечных полуполевых плоскостей с ограничениями на группу автотопизмов. Доказанные результаты выделяют бесконечные серии полуполевых плоскостей, которые не могут допускать фиксированные минимальные простые подгруппы автотопизмов.

Глава 5 посвящена решению вопросов **(A)**–**(D)** для некоторых конечных полуполей. В параграфах 5.1-5.3 представлена употребляемая специальная терминология и введены новые методы исследования полуполей, основанные на использовании регулярного множества и минимальных многочленов. Параграф 5.4 завершает решение вопросов для всех полуполей минимального порядка 16, начатое П. К. Штуккерт, с учетом новых методов исследования и дополнительной информации о минимальных многочленах и внутренних автоморфизмах. Параграфы 5.5-5.7 посвящены обсуждению гипотезы Г. Венэ и исследованию исключительных непримитивных полуполей Кнута–Руа порядка 32 и Хентзела–Руа порядка 64. Параграф 5.8 представляет решение вопросов для некоторых полуполей порядка p^4 ($p > 2$ – простое), построенных при наличии дополнительных ограничений на автотопизмы.

Главы 6–7 решают, в основном, вопросы **(A)**–**(D)** для всех конечных почтиполей. Методы исследования тесно связаны с результатами Х. Цассенхауза [121] и в значительной мере опираются на работы С. Данкс [40, 41].

Глава 2. Метод регулярного множества построения плоскостей трансляций и их координатизирующих квазиполей

Глава посвящена обсуждению подходов к решению известной проблемы разрешимости группы коллинеаций недезарговой полуполевой проективной плоскости конечного порядка.

Основным используемым далее методом является применение регулярного множества плоскости трансляций и, соответственно, координатизирующего квазиполя. В § 2.1 установлена естественная взаимосвязь между свойствами регулярного множества и свойствами квазиполя. Приводится обоснование представления регулярного множества над простым подполем квазиполя (так называемым «гиперкубом», в случае полуполя).

Особенности строения группы коллинеаций полуполевой проективной плоскости кратко описаны в § 2.2, введены понятия ядер полуполя, группы автотопизмов. Выделены подгруппы центральных коллинеаций, записано их матричное представление.

В § 2.3 обоснована редукция проблемы разрешимости к группе автотопизмов полуполевой плоскости и, далее, к случаю существования бэровской инволюции в группе автотопизмов. Перечислены некоторые известные результаты, связанные с решением проблемы. Обозначены подходы и программа исследований.

2.1. Основы метода регулярного множества

Построение плоскостей трансляций и их координатизирующих квазиполей мы основываем на развитии метода *регулярного множества*. Изложим вначале суть этого подхода.

Пусть $\langle V, + \rangle$ — элементарная абелева группа с согласованным расщеплением $\mathcal{S} = \{V_i \mid i \in I\}$. Это семейство нетривиальных подгрупп с условиями:

$$1)\ V = \bigcup_{i \in I} V_i; \qquad 2)\ V = V_i \oplus V_j \quad \forall i, j \in I,\ i \neq j.$$

Назовем элементы V точками, смежные классы по подгруппам V_i — прямыми и зададим инцидентность естественным образом. Полученная конфигурация $\mathcal{A}(V, \mathcal{S})$ — аффинная плоскость. Действительно, через любые две различные точки проходит единственная прямая, любые две различные прямые либо пересекаются в одной точке, либо не пересекаются (параллельны). Естественно, в качестве параллельных прямых выступают смежные классы по одной компоненте расщепления, в качестве пересекающихся прямых — смежные классы по разным компонентам расщепления.

Аффинную плоскость $\mathcal{A}(V, \mathcal{S})$ можно достроить до проективной плоскости. Множество смежных классов по одной компоненте расщепления назовем точкой. Такие точки образуют прямую, которую обычно называют *бесконечно удаленной*. Легко проверить, что действительно построена проективная плоскость, являющаяся плоскостью трансляций относительно бесконечно удаленной прямой. Трансляциями являются преобразования вида $t_a : x \to x + a$, для $a \in V$.

Пусть π — плоскость трансляций с группой трансляций T, $\mathcal{S}$ — согласованное расщепление группы T. Тогда проективная плоскость, достроенная из конфигурации $\mathcal{A}(T, \mathcal{S})$, изоморфна плоскости π [68].

Обычно при построении плоскостей трансляций в качестве группы V выбирается векторное пространство четной размерности над ядром K координатизирующего квазиполя.

Пусть $V = W \oplus W$, где W — векторное пространство размерности d над полем $K \simeq GF(q)$, θ – инъективное отображение из W в кольцо $d \times d$-матриц над K с условиями:

1) образом нулевого вектора $0 \in W$ является нулевая матрица;

2) единичная матрица E имеет прообраз $e \in W$;

3) для любых различных векторов $u, v \in W$ матрица $\theta(u) - \theta(v)$ невырожденная.

Множество всех образов

$$R = \{\theta(v) \mid v \in W\} \subset GL_d(q) \cup \{0\} \tag{2.1.1}$$

далее называем *регулярным множеством* (spread set, см. также [11]). Выберем в качестве компонент расщепления группы V подпространства

$$\begin{aligned} V_\infty =&\{(0,y) \mid y \in W\},\\ V_u =&\{(x, x\theta(u)) \mid x \in W\}, \qquad u \in W. \end{aligned}$$

Тогда аффинные точки плоскости π – это элементы $(x,y) \in V$ $(x,y \in W)$, каждая аффинная прямая $[m,k]$ – это смежный класс по подгруппе V_m с представителем $(0,k)$ $(m,k \in W)$. Множество всех смежных классов по этой подгруппе будем называть точкой (m). Смежный класс по подгруппе V_∞ с представителем $(b,0)$ $(b \in W)$ назовем прямой $[b]$. Множество всех смежных классов по этой подгруппе — точка (∞). Точка (∞) и все точки вида (m), $m \in W$, образуют прямую $[\infty]$.

В качестве нуля координатизирующего множества берется нулевой вектор $0 \in W$, в качестве единицы — прообраз $e \in W$ единичной матрицы, $\theta(e) = E$. Сложение элементов x и y из W определим как сложение векторов, умножение $*$ зададим правилом

$$x * y = x \cdot \theta(y), \quad x,y \in W \tag{2.1.2}$$

(здесь и всюду далее векторы линейного пространства W рассматриваются как строки). Из условия $\det(\theta(u)-\theta(v)) \neq 0$ для $u \neq v$ следует, что матрица $\theta(u)$ однозначно определяется выбором любой своей строки или столбца. Поэтому без ограничения общности можно считать, что, например, первая строка матрицы $\theta(u)$ совпадает с вектором $u \in W$. В некоторых случаях далее будет удобнее отождествлять вектор-аргумент с последней строкой матрицы, это будет указано дополнительно.

Нетрудно показать, что полученная описанным образом алгебраическая система является правым квазиполем. Заметим, что при записи элементов векторного пространства столбцами, а не строками аналогичное построение приводит к левому квазиполю. Напомним, что всюду далее «квазиполе» обозначает «правое квазиполе», если не оговорено противное.

Лемма 2.1.1. *Пусть R (2.1.1) – регулярное множество. Тогда $\langle W, +, * \rangle$ – правое квазиполе.*

Доказательство. Очевидно, $\langle W, + \rangle$ – абелева группа и для всех $x,y,z \in W$

$$(x+y) * z = (x+y)\theta(z) = x\theta(z) + y\theta(z) = x * z + y * z.$$

Далее, если $a,b \in W$, $a \neq 0$, то матрица $\theta(a)$ невырожденная и существует единственное решение уравнения $x * a = b$:

$$x\theta(a) = b \Rightarrow x = b(\theta(a))^{-1}.$$

Рассмотрим уравнение $a * x = b$ при $a \neq 0$ и два его решения $x_1, x_2 \in W$:

$$a * x_1 = b,\ a * x_2 = b \Rightarrow a\theta(x_1) = a\theta(x_2) \Rightarrow$$

$$a(\theta(x_1) - \theta(x_2)) = 0 \Rightarrow \det(\theta(x_1) - \theta(x_2)) = 0 \Rightarrow \theta(x_1) = \theta(x_2) \Rightarrow x_1 = x_2.$$

Учитывая конечность множества W, заключаем, что всякое уравнение

$$a * x = b, \quad a, b \in W,\ a \neq 0,$$

имеет решение в W, причем единственное.

Далее, очевидно, что e является нейтральным по умножению элементом W:

$$x * e = x\theta(e) = xE = x, \quad e * x = e\theta(x) = x$$

(первая строка матрицы $\theta(x)$). Нулевой вектор $0 \in W$ удовлетворяет условию $0 * x = 0$ для любого $x \in W$.

Рассмотрим уравнение $x * a = x * b + c$ для произвольных $a, b, c \in W$, $a \neq b$. Переписав его в виде

$$x \cdot (\theta(a) - \theta(b)) = c,$$

из невырожденности матрицы $\theta(a) - \theta(b) \neq 0$ делаем вывод о существовании единственного решения такого уравнения. □

Свойства отображения θ и регулярного множества R определяют геометрические свойства плоскости трансляций. Далее перечислены известные результаты о регулярном множестве для полуполя, почти-поля, поля (см., например, [43]).

Лемма 2.1.2. *Пусть R (2.1.1) – регулярное множество. Квазиполе $\langle W, +, * \rangle$ является полуполем тогда и только тогда, когда R замкнуто по сложению.*

Доказательство. Пусть $\langle W, +, * \rangle$ – полуполе, тогда для всех $x, y, z \in W$

$$x * (y + z) = x * y + x * z \Rightarrow x\theta(y + z) = x\theta(y) + x\theta(z) = x(\theta(y) + \theta(z)),$$

ввиду произвольности $x \in W$ имеем

$$\theta(y) + \theta(z) = \theta(y + z) \in R. \tag{2.1.3}$$

Обратно, пусть R замкнуто по сложению, $\theta(y) + \theta(z) = \theta(w) \in R$. Тогда, очевидно, w – первая строка матрицы $\theta(y)+\theta(z)$, т.е. $w = y+z$. Из условия (2.1.3) для произвольных $y, z \in W$ следует дистрибутивность

$$x * (y + z) = x * y + x * z \quad \forall x, y, z \in W.$$

□

Лемма 2.1.3. *Пусть R (2.1.1) – регулярное множество. Квазиполе $\langle W, +, * \rangle$ является почти-полем тогда и только тогда, когда R замкнуто по умножению; при этом $R^* \simeq W^*$.*

Доказательство. Пусть $\langle W, +, * \rangle$ – почти-поле, тогда для всех $x, y, z \in W$

$$(x * y) * z = x * (y * z) \Rightarrow x\theta(y)\theta(z) = x\theta((y\theta(z)),$$

ввиду произвольности $x \in W$ имеем

$$\theta(y)\theta(z) = \theta(y\theta(z)) \in R. \tag{2.1.4}$$

Обратно, пусть R замкнуто по умножению, $\theta(y)\theta(z) = \theta(w) \in R$. Тогда, очевидно, w – первая строка матрицы $\theta(y)\theta(z)$, т.е. $w = y\theta(z)$. Из условия (2.1.4) для произвольных $y, z \in W$ следует ассоциативность

$$(x * y) * z = x * (y * z) \quad \forall x, y, z \in W.$$

□

Лемма 2.1.4. *Пусть R (2.1.1) – регулярное множество. Квазиполе $\langle W, +, * \rangle$ является полем тогда и только тогда, когда R – поле.*

Доказательство. Пусть $\langle W, +, * \rangle$ – поле, тогда по лемме 2.1.2 R замкнуто по сложению и по лемме 2.1.3 замкнуто по умножению.

Так как R конечно и содержит единичную матрицу, то каждая ненулевая матрица из R обратима.

Далее, из коммутативности умножения в W ($\forall y, z \in W$):

$$y * z = z * y \Rightarrow y\theta(z) = z\theta(y) \Rightarrow \theta(y\theta(z)) = \theta(z\theta(y)) \Rightarrow \theta(y)\theta(z) = \theta(z)\theta(y),$$

т.е. умножение в R коммутативно, R – поле.

Обратно, пусть R – поле, тогда по леммам 2.1.2 и 2.1.3 в квазиполе W выполнены оба дистрибутивных закона и ассоциативность умножения. Докажем коммутативность умножения:

$$\theta(y)\theta(z) = \theta(z)\theta(y) \Rightarrow \theta(y\theta(z)) = \theta(z\theta(y)) \Rightarrow y\theta(z) = z\theta(y) \Rightarrow y * z = z * y.$$

Далее, пусть $y \in W$, $y \neq 0$, тогда существует такой $z \in W$, что $\theta(z) = (\theta(y))^{-1}$. Получим

$$\theta(z)\theta(y) = \theta(y)\theta(z) = E \Rightarrow \theta(z\theta(y)) = \theta(y\theta(z)) = \theta(e) \Rightarrow$$

$$z\theta(y) = y\theta(z) = e \Rightarrow z * y = y * z = e,$$

т.е. всякий ненулевой элемент $y \in W$ обратим. W – поле, лемма доказана. □

Отметим, что для построения конечного квазиполя в качестве основного поля $GF(q)$ часто используется ядро K. Размерность квазиполя как линейного пространства над ядром часто называют *рангом* квазиполя и ассоциированной плоскости трансляций. Однако более удобно в некоторых случаях рассматривать линейное пространство W и регулярное множество R над простым подполем $\mathbb{Z}_p$. Тогда отображение θ может быть записано [132] с использованием только линейных функций, что существенно упрощает рассуждения и вычисления.

Лемма 2.1.5. *Пусть $\langle Q, +, \cdot\rangle$ – квазиполе порядка p^n, W – n-мерное линейное пространство над $\mathbb{Z}_p$. Тогда существует регулярное множество*

$$R = \{\theta(v) \mid v \in W\} \subset GL_n(p) \cup \{0\}$$

такое, что квазиполе $\langle Q, +, \cdot\rangle$ изоморфно $\langle W, +, *\rangle$, где умножение $*$ задано правилом (2.1.2).

Доказательство. Квазиполе Q является n-мерным линейным пространством над полем $\mathbb{Z}_p$; пусть $e_1, \ldots, e_n$ – его базис. Рассмотрим произвольный базис $\varepsilon_1, \ldots, \varepsilon_n$ пространства W и установим соответствие $\varphi : e_i \to \varepsilon_i$ $(i = 1, \ldots, n)$, которое продолжим до изоморфизма линейных пространств Q и W.

Для любого фиксированного элемента $q \in Q$ умножение справа

$$\beta_q : x \to x \cdot q, \quad x \in Q,$$

является линейным преобразованием пространства Q над $\mathbb{Z}_p$ (по определению правого квазиполя). Пусть

$$\overline{\beta_q} : \varphi(x) \to \varphi(\beta_q(x))$$

– соответствующее линейное преобразование пространства W и $\theta(\varphi(q))$ – его матрица в базисе $\varepsilon_1, \ldots, \varepsilon_n$. Очевидно, $R = \{\theta(v) \mid v \in W\}$ – подмножество в $GL_n(p) \cup \{0\}$, $\theta(0) = 0$ – нулевая матрица, $\theta(\varphi(1)) = E$ – единичная матрица (где 1 – единица квазиполя Q). Если мы определим умножение $*$ на W правилом (2.1.2), то $\langle Q, +, \cdot\rangle$ изоморфно $\langle W, +, *\rangle$. Докажем, что $\theta(x) - \theta(y) \in GL_n(p)$ для $x \neq y$. Действительно, если $\det(\theta(x) - \theta(y)) = 0$, то для некоторого элемента $z \in W \setminus \{0\}$

$$z(\theta(x) - \theta(y)) = 0 \Rightarrow z\theta(x) = z\theta(y) \Rightarrow z * x = z * y$$

и для прообразов $z_0, x_0, y_0 \in Q$ имеем $z_0 \cdot x_0 = z_0 \cdot y_0$, что противоречит определению квазиполя. □

Другие способы представления конечных полуполей и квазиполей перечислены в монографии [72] и обзорах [78, 83], см. также представление Т. Оямы [96].

2.2. Центральные коллинеации полуполевой плоскости

Конечная проективная плоскость, координатизируемая полуполем, является одновременно плоскостью трансляций относительно прямой $[\infty]$ и дуальной к плоскости трансляций с трансляционной точкой (∞). Конечное полуполе является алгебраической системой, близкой к конечному поля, отличаясь лишь отсутствием ассоциативности умножения. В связи с этим значительный интерес представляет изучение различий группы коллинеаций полуполевой плоскости и группы коллинеаций дезарговой плоскости Π, которая, как известно, индуцируется всеми невырожденными полулинейными преобразованиями 3-мерного векторного пространства над основным полем K, $|K| = |\Pi|$: $Aut\,\Pi \simeq P\Gamma L_3(K)$ [68, 18].

Далее мы рассматриваем недезаргову полуполевую плоскость, ее координатизирующее множество – нетривиальное полуполе. Выделим, следуя [68], в произвольном полуполе W подмножества элементов, для которых умножение обладает свойствами ассоциативности и коммутативности.

Определение 2.2.1. *Правым, средним и левым ядрами полуполя* $\langle W, +, * \rangle$ *называются множества*

$$\begin{aligned} N_r &= \{d \in W \mid (x * y) * d = x * (y * d)\ \forall x, y \in W\}, \\ N_m &= \{d \in W \mid (x * d) * y = x * (d * y)\ \forall x, y \in W\}, \\ N_l &= \{d \in W \mid (d * x) * y = d * (x * y)\ \forall x, y \in W\} \end{aligned}$$

соответственно.

Пересечение $N_0 = N_l \cap N_m \cap N_r$ называется *ядром* полуполя W. Множество

$$Z = \{z \in N_0 \mid z * x = x * z\ \forall x \in W\}$$

называется *центром* полуполя. Учитывая определение (1.1.3), видим, что левое ядро N_l полуполя W является в точности его ядром как квазиполя. Все ядра и центр конечного полуполя являются подполями [68], полуполе W можно рассматривать как левое векторное пространство над Z, N_0, N_l, N_m и как правое векторное пространство над Z, N_0, N_m, N_r. Как правило, в качестве основного поля используют центр полуполя, но мы всюду далее будем рассматривать полуполе W порядка p^n как линейное пространство над простым подполем $\mathbb{Z}_p$. Пусть

$$R = \{\theta(v) \mid v \in W\} \subset GL_n(p) \cup \{0\} \tag{2.2.1}$$

– регулярное множество полуполя W. Как показано в лемме 2.1.2, R замкнуто по сложению. Определим множества, которые будем называть правым, средним

и левым ядрами полуполевой плоскости π, координатизируемой полуполем W:

$$\begin{aligned} R_r &= \{\theta(d) \in R \mid \theta(x)\theta(d) \in R \ \forall x \in W\}, \\ R_m &= \{\theta(d) \in R \mid \theta(d)\theta(x) \in R \ \forall x \in W\}, \\ R_l &= C_{GL_n(p)}(R) = \{D \in GL_n(p) \mid D\theta(x) = \theta(x)D \ \forall x \in W\}. \end{aligned}$$

Нетрудно доказать, что

Лемма 2.2.2. *Справедливо* $N_r \simeq R_r$, $N_m \simeq R_m$, $N_l \simeq R_l$.

Доказательство. 1. Пусть $d \in N_r$, тогда $x\theta(y)\theta(d) = x\theta(y\theta(d))$ для всех $x, y \in W$, поэтому $\theta(d) \in R_r$.

Обратно, пусть $\theta(d) \in R_r$, тогда для любого элемента $y \in W$ найдется элемент $z \in W$ такой, что $\theta(y)\theta(d) = \theta(z)$. Если e — единица множества Q, то

$$e\theta(y)\theta(d) = y\theta(d) = y * d = e\theta(z) = z,$$

$z = y * d$ и для всех $x \in W$ верно равенство $(x * y) * d = x * z = x * (y * d)$, поэтому $d \in N_r$.

2. Изоморфизм $N_m \simeq R_m$ доказывается аналогично.

3. Пусть $d \in N_l$, тогда $\varphi : x \to d * x$ — линейное преобразование пространства W. Следовательно, существует матрица D такая, что $d * x = xD$ $(x \in W)$. Так как $d * (x * y) = (d * x) * y$ для всех $x, y \in W$, верно равенство $(x * y)D = (xD) * y$, поэтому $\theta(y)D = D\theta(y)$ и $D \in R_l$.

Обратно, пусть $D \in R_l$ и $d = eD$, тогда $d * x = xD$ для всех $x \in W$ и

$$(d * x) * y = xD\theta(y) = x\theta(y)D = (x * y)D = d * (x * y)$$

для всех $y \in W$, то есть $d \in N_l$. □

Рассмотрим строение группы коллинеаций конечной полуполевой плоскости π порядка p^n с координатизирующим полуполем W и регулярным множеством R (2.2.1). Так как π является плоскостью трансляций с трансляционной прямой $[\infty]$, то группа коллинеаций полуполевой плоскости может быть записана в виде $Aut\,\pi = T \leftthreetimes G$, где $T = \{t_{(a,b)} \mid a, b \in W\}$ — группа всех трансляций,

$$t_{(a,b)} : (x, y) \to (x + a, y + b) \qquad (x, y \in W),$$

а G — стабилизатор точки $(0, 0)$ [68]. Множество G называется *трансляционным дополнением* плоскости и содержится в $GL_{2n}(p)$, любая коллинеация $\gamma \in G$ определяется как

$$\gamma : (x, y) \to (x, y)\begin{pmatrix} A & B \\ C & D \end{pmatrix} \qquad (x, y \in W),$$

где A, B, C, D – $n \times n$- матрицы над $\mathbb{Z}_p$. Заметим, что если выбрать в качестве основного поля не простое подполе $\mathbb{Z}_p$, а центр полуполя Z или одно из ядер, то в общем случае коллинеации из G определяются полулинейными преобразованиями:

$$\gamma : (x, y) \to (x^\sigma, y^\sigma) \begin{pmatrix} A & B \\ C & D \end{pmatrix} \qquad (x, y \in W),$$

здесь σ – автоморфизм основного поля, действующий на каждую координату вектора из W. Тогда, кроме трансляционного дополнения G, рассматривают *линейное трансляционное дополнение* $G_0 < G$, образованное линейными преобразованиями векторного пространства $W \oplus W$.

Далее, так как (∞) – трансляционная точка в полуполевой плоскости π, то она фиксируется любой коллинеацией γ из трансляционного дополнения. Поэтому γ фиксирует прямую $[0]$ с точками вида $(0, y)$, отсюда $C = 0$,

$$\gamma : (x, y) \to (x, y) \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \qquad (x, y \in W). \tag{2.2.2}$$

Выясним, при каких условиях матрицы A, B, D действительно задают коллинеацию (2.2.2). Так как γ сохраняет инцидентность, то образом произвольной точки $(x, x\theta(m)) \in [m, 0]$ должна быть точка на прямой $[k, 0]$, тоже проходящей через $(0, 0)$:

$$(x, x\theta(m)) \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = (y, yA^{-1}(B + \theta(m)D) = (y, y\theta(k))$$

для $y = xA$. Тогда произведение $A^{-1}(B + \theta(m)D)$ должно принадлежать регулярному множеству R при всех $m \in W$, отсюда $B = A\theta(u)$ и

$$A^{-1}\theta(m)D \in R \quad \forall m \in W. \tag{2.2.3}$$

Очевидно,

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \begin{pmatrix} E & \theta(u) \\ 0 & E \end{pmatrix},$$

поэтому трансляционное дополнение имеет структуру $G = \Omega \leftthreetimes \Lambda$, где

$$\Omega = \left\{ \begin{pmatrix} E & \theta(u) \\ 0 & E \end{pmatrix} \;\middle|\; u \in W \right\} \tag{2.2.4}$$

– группа всех элаций с осью $[0]$ и центром (∞) (для них используется термин «shears»), а

$$\Lambda = \left\{ \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \;\middle|\; A, D \in GL_n(p),\ A^{-1}\theta(m)D \in R\ \forall m \in W \right\} \tag{2.2.5}$$

– группа автотопизмов.

Определение 2.2.3. *Пусть Δ — треугольник в полуполевой плоскости π, одной стороной которого является трансляционная прямая $[\infty]$, одной вершиной — трансляционная точка (∞). Коллинеации, стабилизирующие треугольник Δ, называются автотопизмами, и образуют группу автотопизмов, соответствующую автотопному треугольнику Δ.*

В силу $([\infty],[\infty])$-транзитивности и $((\infty),(\infty))$-транзитивности полуполевой плоскости без потери общности можно считать, что группа автотопизмов соответствует треугольнику

$$\{[\infty],[0],[0,0],(\infty),(0),(0,0)\}$$

и совпадает с Λ (2.2.5). Если основным полем является не $\mathbb{Z}_p$, то в группе автотопизмов $\Lambda < G$ естественным образом выделяется подгруппа линейных автотопизмов $\Lambda_0 < G_0$, тогда $G_0 = \Omega \leftthreetimes \Lambda_0$.

Окончательно имеем факторизацию группы коллинеаций конечной недезарговой полуполевой плоскости:

$$Aut\,\pi = T \leftthreetimes (\Omega \leftthreetimes \Lambda).$$

Здесь группа трансляций T и группа элаций Ω – элементарные абелевы, $|T| = |\pi|^2 = p^{2n}$, $|\Omega| = |\pi| = p^n$. Таким образом, для выяснения строения группы коллинеаций недезарговой полуполевой плоскости достаточно описать ее группу автотопизмов.

Заметим, что подгруппа $T \leftthreetimes \Omega$ представляет частное решение вопроса 10.1 Коуровской тетради, решенного в 1999 г. (В. А. Антонов, Препринт, Челябинск, 1999):

Пусть p – простое число. Описать группы порядка p^9 и ступени нильпотентности 2, содержащие такие подгруппы X и Y, что $|X| = |Y| = p^3$ и любые неединичные элементы $x \in X$, $y \in Y$ неперестановочны. Ответ на этот вопрос позволит описать полуполя порядка p^3. С. Н. Адамов, А. Н. Фомин, 1986 г.

Рассмотрим центральные коллинеации, содержащиеся в группе автотопизмов Λ. Поскольку любой автотопизм оставляет на месте точки $(0),(0,0),(\infty)$, то эти центральные коллинеации не могут быть элациями. Это могут быть только гомологии, у которых центр – одна из перечисленных точек, а две другие лежат на оси.

Лемма 2.2.4. *Пусть π – полуполевая плоскость с регулярным множеством R (2.2.1). Тогда любая центральная коллинеация в группе автотопизмов Λ (2.2.5) принадлежит одной из трех подгрупп гомологий:*

$$H_r = \left\{ \begin{pmatrix} E & 0 \\ 0 & \theta(d) \end{pmatrix} \;\middle|\; \theta(d) \in R_r^* \right\}, \qquad H_m = \left\{ \begin{pmatrix} \theta(d) & 0 \\ 0 & E \end{pmatrix} \;\middle|\; \theta(d) \in R_m^* \right\},$$

$$H_l = \left\{ \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix} \;\middle|\; D \in R_l^* \right\}. \tag{2.2.6}$$

При этом всякая гомология из H_r имеет ось $[0,0]$ и центр (∞), из H_m – ось $[0]$ и центр (0), из H_l – ось $[\infty]$ и цент $(0,0)$.

Доказательство. Доказательство представлено, например, в [76]. Действительно, если

$$\gamma = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \in \Lambda$$

– гомология с осью $[0,0]$, то она оставляет на месте любую точку этой прямой:

$$(x,0)\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} = (xA,0) = (x,0) \Rightarrow A = E,$$

и из условия (2.2.3) следует $D \in R_r^*$. Если γ – гомология с осью $[0]$, то

$$(0,y)\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} = (0,yD) = (0,y) \Rightarrow D = E,\ A \in R_m^*.$$

Гомология с осью $[\infty]$ фиксирует (не поточечно) любую прямую $[m,0]$, тогда

$$(x, x\theta(m))\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} = (xA, x\theta(m)D) = (y, y\theta(m))$$

для $y = xA$, отсюда $A = D \in R_l^*$. □

Следствие 2.2.5. *Подгруппы гомологий H_r, H_m, H_l циклические, их порядки равны соответственно $p^r - 1$, $p^m - 1$, $p^l - 1$, где $p^r = |N_r|$, $p^m = |N_m|$, $p^l = |N_l|$.*

Следующая лемма, уточняющая роль центральных коллинеаций, доказана в [125].

Лемма 2.2.6. *Все центральные коллинеации полуполевой плоскости π в трансляционном дополнении G порождают группу*

$$\Omega \times (H_{ll} \times (H_r \times H_m)),$$

где $H_{ll} \simeq H_l/(H_l \cap (H_r \times H_m))$. Подгруппа $(H_{ll} \times (H_r \times H_m))$ содержит все центральные коллинеации, лежащие в группе автотопизмов Λ плоскости π. Подгруппы гомологий H_l, H_r и H_m нормальны в группе Λ.

Доказательство. Несложно проверить, что все гомологии из подгрупп H_l, H_m, H_r перестановочны. Если подгруппы H_r и H_m нетривиальны, то их произведение может содержать некоторые гомологии из подгруппы H_l. Подгруппы H_l, H_r и H_m нормальны в группе автотопизмов, поскольку произвольный автотопизм оставляет на месте их ось и центр. □

2.3. Редукция проблемы Хьюза к группе автотопизмов

Первыми результатами, связанными с гипотезой разрешимости группы коллинеаций конечной недезарговой полуполевой плоскости, по-видимому, следует считать работы 1952–1959 гг. А. Альберта [21, 22, 23], Д. Хьюза и Э. Клейнфелда [67]. Опираясь на эти результаты о разрешимости для плоскостей, координатизируемых коммутативными полуполями Диксона, скрученными полями, полуядерными полуполями, Д. Хьюз в 1959 г. выдвинул [65] гипотезу разрешимости для случая произвольного нетривиального полуполя. Гипотеза записана в монографии Д. Хьюза и Ф. Пайпера [68] в 1973 г., этот вопрос также поставлен Н.Д. Подуфаловым в Коуровской тетради [10, вопрос 11.76] в 1990 г.

Для некоторых известных полуполевых плоскостей гипотеза о разрешимости группы коллинеаций подтверждена, опровергающих примеров не обнаружено. Ряд результатов получен Д. Кнутом [82], Д. Хьюзом и М. Каллахером [69], Т. Остромом [95], М. Ганли [51], М. Ганли и В. Джа [53], М. Билиотти, Н. Джонсоном, В. Джа и Д. Меничетти [29], Х. Хуангом и Н. Джонсоном [64], М. Кордеро [35] и другими. Например, доказана разрешимость группы автотопизмов для конечных коммутативных полуполей Диксона [106, 107], для обобщенных плоскостей Холла нечетного порядка [73], для p-примитивных полуполевых плоскостей порядка p^4 [35], восьми полуполевых плоскостей Хуанга–Джонсона порядка 8^2 [64], и некоторых других. Эти результаты подтверждают гипотезу разрешимости для отдельных классов недезарговых полуполевых плоскостей, например, в случае фиксированного порядка либо при определенных ограничениях на коллинеации, однако общий подход к решению проблемы не найден.

Значительное количество результатов получено с использованием вычислительной техники при перечислении всех полуполевых плоскостей фиксированного малого порядка. К результатам такого рода следует отнести работы И. Руа и других о полуполях и полуполевых плоскостях порядков 64, 81, 243 [102, 101, 103]. Приведем пример типичного результата, полученного компьютерными вычислениям в [103]: выделено девять классов полуполевых плоскостей, найдены их ядра, определено строение группы автотопизмов или вычислен ее порядок, см. табл. 2 ниже. Строка **I** таблицы соответствует дезарговой плоскости.

Таблица 2. Информация о полуполевых плоскостях порядка 243

Plane	$\|At\|$	ZN
I	292820	(243,243,243,243,243)
II, III	2420, solvable	(3,3,3,3,3)
IV, V, VI	20, $\mathbb{Z}_2 \times \mathbb{Z}_{10}$	(3,3,3,3,3)
VII	220, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times (\mathbb{Z}_5 \leftthreetimes \mathbb{Z}_{11})$	(3,3,3,3,3)
VIII, IX	4, $\mathbb{Z}_2 \times \mathbb{Z}_2$	(3,3,3,3,3)

Примером общих результатов о разрешимости группы коллинеаций являются теоремы 5.1.8, 5.1.9 о полуполях ранга два над своими ядрами, доказанные М. Ганли [51], Д. Хьюзом и М. Каллахером [69], а также следующая теорема, доказанная в [53] М. Ганли и В. Джа.

Теорема 2.3.1. *Пусть π – конечная плоскость трансляций, которая допускает группу коллинеаций, фиксирующую точку (∞) и действующую дважды транзитивно на оставшихся точках прямой $[\infty]$. Тогда π – полуполевая плоскость и ее группа коллинеаций разрешима.*

Перечислим также кратко основные результаты, полученные Н. Д. Подуфаловым, Б. К. Дураковым, Е. Б. Дураковым, И. В. Бусаркиной и автором (1990–2000 гг., см. обзор [125]).

Теорема 2.3.2. *При выполнении одного из следующих условий группа коллинеаций недезарговой полуполевой плоскости π разрешима:*

1) π имеет ранг 2 или 4 над полем $GF(q)$ четного порядка $q = 2^n$;

2) π имеет четный порядок q^2 и правое ядро порядка q, где $q = 2^n$;

3) π является p-примитивной полуполевой плоскостью ($p > 2$ – простое) и удовлетворяет определенным условиям на регулярное множество.

Заметим, что предположение о разрешимости группы коллинеаций не является справедливым ни для дезарговой плоскости, ни для произвольной плоскости трансляций. Опубликован ряд работ о конечных плоскостях трансляций, допускающих подгруппы коллинеаций, изоморфные $SL(2,q)$ [28, 50, 71, 98], $PSL(2,q)$ [93], $PSL(3,q)$ [30], $PSU(3,q)$ [63], $Sz(2^r)$ [33]. Отметим также интересный результат Т. Острома о неразрешимых подгруппах коллинеаций конечных плоскостей трансляций [95].

Теорема 2.3.3. *Пусть π – плоскость трансляций порядка q^d с ядром $GF(q)$, где q и d нечетны, и G – подгруппа в линейном трансляционном дополнении. Предположим, что G неразрешима, G_0 – ее минимальная нормальная неразрешимая подгруппа, d – произведение различных простых чисел. Тогда либо $G_0 \simeq SL(2,u)$ для некоторого нечетного u, либо $\overline{G_0} \simeq A_6$ или A_7. Здесь $\overline{G_0} = G_0/Z(G_0)$.*

Подводя итог обсуждению особенностей строения группы коллинеаций полуполевой плоскости (см. предыдущий параграф) и опираясь на монографию Д. Хьюза и Ф. Пайпера [68] (раздел VIII.3, леммы 8.4–8.5, теорема 8.6), сформулируем теорему:

Теорема 2.3.4. *Группа коллинеаций конечной недезарговой полуполевой плоскости разрешима тогда и только тогда, когда разрешима группа автотопизмов.*

Таким образом, проблема разрешимости редуцируется к исследованию разрешимости группы автотопизмов Λ. Возможность дальнейшей редукции предоставляет особая роль бэровских инволюций. На это указывает следующая теорема ([68, теорема 8.18], см. также [43]).

Теорема 2.3.5. *Пусть D – конечное полуполе. Если координатизируемая им полуполевая плоскость $\mathcal{P}(D)$ имеет четный порядок и не содержит бэровских подплоскостей, или если имеет нечетный порядок и размерность D над хотя бы одним из его ядер нечетна, то группа автотопизмов D разрешима.*

Действительно, в силу теоремы Фейта–Томпсона о разрешимости всех групп нечетного порядка, для решения проблемы следует рассматривать лишь полуполевые плоскости, допускающие автотопизмы порядка два, они могут быть только центральными либо бэровскими (теорема 1.2.9). Подгруппа автотопизмов, порожденная центральными коллинеациями, нормальна в Λ и абелева по лемме 2.2.6. Более того, для плоскости четного порядка в этой подгруппе нет инволюций. Таким образом, с точки зрения проблемы разрешимости интерес представляют полуполевые плоскости, в группе автотопизмов которых содержатся бэровские инволюции.

Обращая внимание снова на теорему Т. Острома 2.3.3 и учитывая теорему 2.3.5, заключаем, что плоскость трансляций π в теореме 2.3.3 не может быть полуполевой: координатизирующее полуполе имеет нечетный порядок и нечетную размерность над ядром. Тем не менее, теорема 2.3.3 упомянута по причине непосредственной связи с предлагаемой ниже программой исследования проблемы разрешимости.

Ясно, что в предположении неразрешимости группы коллинеаций конечной недезарговой полуполевой плоскости композиционные факторы группы автотопизмов должны быть изоморфны известным простым группам.

Ответ на вопрос о возможных минимальных неразрешимых подгруппах группы автотопизмов пока затруднителен. Принципиально важным представляется сначала исключение случаев, когда группа автотопизмов имеет простую

подгруппу. Полное описание минимальных конечных простых групп получено Д. Г. Томпсоном в 1968 г. [110, следствие 1]:

Теорема 2.3.6. *Каждая минимальная простая группа изоморфна одной из следующих минимальных простых групп:*

(a) $PSL(2, 2^p)$, *p любое простое;*

(b) $PSL(2, 3^p)$, *p любое нечетное простое;*

(c) $PSL(2, p)$, *p любое простое более 3,* $p^2 + 1 \equiv 0 (\mathrm{mod}\ 5)$*;*

(d) $Sz(2^p)$, *p любое нечетное простое;*

(e) $PSL(3, 3)$.

С учетом классификации минимальных конечных простых групп, интерес привлекает к себе, прежде всего, ситуация, когда группа автотопизмов имеет подгруппу или сечение, изоморфное знакопеременной группе A_5 или диэдральной группе D_8 порядка 8, подгруппам значительного количества простых неабелевых групп.

Первоочередная задача поэтому состоит в исключении случаев, когда группа автотопизмов содержит подгруппу, изоморфную A_5, D_8 либо $SL(2, 5)$ (как накрывающей A_5).

В следующей главе автор изучает возможность существования некоторых подгрупп четного порядка в группе автотопизмов конечной недезарговой полуполевой плоскости. При этом будут выделены бесконечные серии полуполевых плоскостей, группа автотопизмов которых не может содержать перечисленные выше подгруппы. Результаты, полученные автором, могут обеспечить продвижение в решении проблемы Хьюза.

Глава 3. Специальные подгруппы автотопизмов конечной недезарговой полуполевой плоскости

Основным результатом главы 3 является доказательство для любой недезарговой полуполевой плоскости нечетного порядка отсутствия в группе автотопизмов подгруппы, изоморфной A_5, и диэдральной подгруппы D_8 при ограничении на характеристику поля.

Знакопеременная группа A_5 вызывает естественный интерес в исследовании проблемы разрешимости группы коллинеаций недезарговой полуполевой проективной плоскости конечного порядка, так как является подгруппой значительного числа известных простых групп. Ее отсутствие в группе автотопизмов влечет исключение из числа подгрупп также всех симметрических и знакопеременных групп S_n и A_n при $n \geq 5$, а также некоторых линейных, симплектических и ортогональных групп.

Результаты получены путем построения матричного представления регулярного множества полуполевой плоскости при условии существования в группе автотопизмов бэровской инволюции, далее A_4 и A_5. Кроме того, изучен случай существования в группе автотопизмов подгруппы, изоморфной группе кватернионов Q_8. Эта ситуация представляет интерес в силу изоморфизма A_5 факторгруппе группы $SL_2(5)$ по центру.

Теорема о группе диэдра порядка 8 была получена путем выявления естественных ограничений на порядок элементарной абелевой 2-подгруппы и порядок 2-элемента в группе автотопизмов, определенных рангом полуполевой плоскости. Уточнение геометрического смысла 2-элементов позволяет записать матричное представление регулярного множества.

Отсутствие диэдральной группы порядка 8 в группе автотопизмов недезарговой полуполевой плоскости нечетного порядка при условии, что характеристика поля сравнима с 1 по модулю 4, значительно уменьшает список возможных контрпримеров к гипотезе Хьюза, оставляя в нем по существу лишь простые группы Судзуки, группы Ри и линейные группы размерности 2 и 3.

3.1. Бэровская инволюция в группе автотопизмов

В этом параграфе найдено матричное представление бэровской инволюции в трансляционном дополнении, наиболее удобное для дальнейших рассуждений. Без ограничения общности можно считать, что бэровская инволюция принадлежит группе автотопизмов и определяется поэтому блочно-диагональной матрицей. Вид блоков-подматриц устанавливается в теореме 3.1.2 с использованием жордановой нормальной формы и выбора соответствующего базиса линейного пространства. Выбранный вид матрицы бэровской инволюции позволяет далее записать матричное представление регулярного множества полуполевой плоскости и установить ограничения на отображение θ. Поскольку речь пойдет только о полуполевых плоскостях, то мы всюду считаем, для сокращения формулировок, что регулярное множество замкнуто по сложению, см. лемму 2.1.2.

В 1989 году Н. Л. Джонсоном и другими [29] построено матричное представление регулярного множества полуполевой плоскости порядка q^2 над полем четного порядка $q = 2^k$, допускающей бэровскую инволюцию в линейном трансляционном дополнении:

Теорема 3.1.1. *Пусть π – полуполевая плоскость порядка q^2, $q = 2^k$, с левым ядром, содержащим $GF(q)$, которая допускает бэровскую инволюцию τ в линейном трансляционном дополнении. Тогда регулярное множество π состоит из матриц вида*

$$\theta(v,u) = \begin{pmatrix} u+v+m(v) & f(v)+m(u) \\ v & u \end{pmatrix}, \qquad u,v \in GF(q), \tag{3.1.1}$$

где $m(x)$, $f(x)$ – аддитивные функции, f взаимно однозначна, $m(1) = 0$. Бэровская инволюция τ задается матрицей

$$\tau = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{3.1.2}$$

Рассмотрим более общий случай: если нет информации о порядке (левого) ядра или центра, то естественно считать множество аффинных точек полуполевой плоскости линейным пространством над полем простого порядка. Тогда размерность матриц, определяющих регулярное множество и инволюцию, будет зависеть от порядка плоскости.

Теорема 3.1.2. *Пусть π – полуполевая плоскость π порядка p^N (p – простое), допускающая бэровскую инволюцию τ в трансляционном дополнении.*

Тогда $N = 2n$ и базис $4n$-мерного векторного пространства над $\mathbb{Z}_p$ может быть выбран так, что

$$\tau = \begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix}. \tag{3.1.3}$$

Здесь

$$L = \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix} \quad \textit{при } p > 2, \quad L = \begin{pmatrix} E & E \\ 0 & E \end{pmatrix} \quad \textit{при } p = 2. \tag{3.1.4}$$

Доказательство. Так как бэровская инволюция τ фиксирует поточечно подплоскость π_τ максимального порядка $|\pi_\tau| = \sqrt{|\pi|}$, то $N = 2n$ – четное число.

Рассмотрим множество аффинных точек плоскости π как линейное пространство $W \oplus W$ размерности $4n$ над полем $\mathbb{Z}_p$, где

$$W = \{x = (x_1, x_2, \ldots, x_{2n}) \mid x_i \in \mathbb{Z}_p,\ i = 1, 2, \ldots, 2n\}.$$

Тогда τ – линейное преобразование пространства $W \oplus W$, фиксирующее ровно $2n$ одномерных подпространств. Таким образом, жорданова нормальная форма матрицы τ образована $2n$ жордановыми клетками вида $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ при $p = 2$ или $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ при $p > 2$. Осталось показать, что при $p = 2$ матрица (3.1.3) имеет такую же жорданову нормальную форму. Действительно,

$$\begin{pmatrix} E & E \\ 0 & E \end{pmatrix} - \lambda \begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix} = \begin{pmatrix} (1-\lambda)E & E \\ 0 & (1-\lambda)E \end{pmatrix} \sim \begin{pmatrix} 0 & E \\ (1-\lambda)^2 E & (1-\lambda)E \end{pmatrix} \sim$$
$$\sim \begin{pmatrix} 0 & E \\ (1-\lambda)^2 E & 0 \end{pmatrix} \sim \begin{pmatrix} E & 0 \\ 0 & (1-\lambda)^2 E \end{pmatrix},$$

поэтому жорданова нормальная форма блока $\begin{pmatrix} E & E \\ 0 & E \end{pmatrix}$ образована n жордановыми клетками размерности 2×2. Теорема доказана. □

Таким образом, в теореме 3.1.2 получено единообразное матричное представление бэровской инволюции в группе автотопизмов. Следующие две теоремы выявляют матричное представление регулярного множества полуполевой плоскости π, допускающей такую бэровскую инволюцию τ. Рассуждения проведены отдельно для четного и для нечетного порядка плоскости.

Теорема 3.1.3. *В условиях теоремы 3.1.2 полуполевая плоскость π четного порядка 2^{2n} имеет регулярное множество $R \subset GL_{2n}(2) \cup \{0\}$, образованное*

матрицами вида

$$\theta(V,U)=\begin{pmatrix} U+V+m(V)+w(V) & f(V)+m(U) \\ V & U+w(V) \end{pmatrix}, \tag{3.1.5}$$

где $U,V\in K$, $K\subset GL_n(2)\cup\{0\}$ *– регулярное множество бэровской подплоскости* π_τ, *фиксируемой инволюцией* τ, m, w, f *– линейные отображения из* K *в кольцо* $n\times n$*-матриц над* $\mathbb{Z}_2$, *причем* $m(E)=0$ *и для всех* $V\in K$ *нижняя строка матрицы* $w(V)$ *состоит только из нулей.*

Доказательство. Матрица регулярного множества полуполевой плоскости π однозначно определяется любой своей строкой, допустим, последней. Остальные строки матрицы являются линейными функциями элементов этой строки:

$$\theta(u_{2n,1},\dots,u_{2n,2n})=\begin{pmatrix} u_{11} & \dots & u_{1,2n} \\ u_{21} & \dots & u_{2,2n} \\ \dots & \dots & \dots \\ u_{2n,1} & \dots & u_{2n,2n} \end{pmatrix},$$

где $u_{ij}=q_{ij1}u_{2n,1}+q_{ij2}u_{2n,2}+\dots+q_{ij,2n}u_{2n,2n}$ для $i=1,2,\dots,2n-1$, $j=1,2,\dots,2n$.

Перепишем матрицу в виде

$$\theta(V,U)=\begin{pmatrix} d(U)+h(V) & m(U)+f(V) \\ V+s(U) & U+w(V), \end{pmatrix}$$

разбивая на блоки порядка n. Здесь слагаемые V, $h(V)$, $f(V)$, $w(V)$ содержат линейные функции, зависящие только от $u_{2n,1},\dots,u_{2n,n}$. Остальные слагаемые определяются выбором элементов $u_{2n,2n+1},\dots,u_{2n,2n}$. Тогда, очевидно, последняя строка матриц $s(U)$ и $w(V)$ состоит только из нулей.

Выясним, при каких условиях на указанные функции плоскость с регулярным множеством R допускает бэровскую инволюцию τ вида (3.1.3).

Так как τ – коллинеация, то для любой матрицы $\theta(V,U)\in R$ произведение $L^{-1}\theta(V,U)L$ также принадлежит R по условию (2.2.3), для матрицы L вида (3.1.4). Далее, в силу замкнутости множества R по сложению, матрица $L^{-1}\theta(V,U)L+\theta(V,U)$ принадлежит R. Выполняя действия, получим матрицу:

$$\begin{pmatrix} V+s(U) & d(U)+s(U)+U+h(V)+w(V)+V \\ 0 & V+s(U) \end{pmatrix}=\theta(0,V).$$

Отсюда следует, что матрица V для каждой $\theta(V,U)\in R$ – либо нулевая, либо невырожденная, множество всех таких матриц замкнуто по сложению, содержит нулевую и единичную матрицы, поэтому является регулярным множеством полуполевой плоскости порядка 2^n. Легко проверить, что это бэровская подплоскость π_τ, фиксируемая инволюцией τ:

$$L^{-1}\theta(0,V)L=\theta(0,V).$$

Обозначим регулярное множество подплоскости π_τ через K. Для всех матриц $U, V \in K$ имеем:

$$s(U) = 0, \quad d(U) = U, \quad h(V) = V + m(V) + w(V),$$

причем $m(E) = 0$, так как $\theta(0, E) = \begin{pmatrix} E & m(E) \\ 0 & E \end{pmatrix}$ – единичная матрица. Теорема доказана. □

Замечание 3.1.4. *Теорема 3.1.3 естественным образом обобщает результаты теоремы 3.1.1 на случай многомерного пространства.*

Теорема 3.1.5. *В условиях теоремы 3.1.2 полуполевая плоскость π нечетного порядка p^{2n} ($p > 2$ – простое) имеет регулярное множество $R \subset GL_{2n}(p) \cup \{0\}$, образованное матрицами вида*

$$\theta(V, U) = \begin{pmatrix} m(U) & f(V) \\ V & U \end{pmatrix}, \tag{3.1.6}$$

где $V \in Q$, $U \in K$, $Q, K \subset GL_n(p) \cup \{0\}$ – регулярные множества, K соответствует бэровской подплоскости π_τ, фиксируемой инволюцией τ, m, f – инъективные линейные отображения из Q и K соответственно в $GL_n(p) \cup \{0\}$, причем $m(E) = E$, $f(E) \neq E$.

Доказательство. Рассуждая аналогично случаю $|\pi| = 2^{2n}$, запишем произвольную матрицу регулярного множества R в виде

$$\theta(V, U) = \begin{pmatrix} m(U) + h(V) & d(U) + f(V) \\ V + s(U) & U + w(V), \end{pmatrix}$$

разбивая на блоки порядка n. Так как τ – коллинеация, то для любой матрицы $\theta(V, U) \in R$ произведение $L^{-1}\theta(V, U)L$ также принадлежит R, для матрицы L вида (3.1.4). Имеем:

$$L^{-1}\theta(V, U)L = \begin{pmatrix} m(U) + h(V) & -d(U) - f(V) \\ -V - s(U) & U + w(V) \end{pmatrix} = \theta(-V, U).$$

Отсюда следует, что $s(U) \equiv 0$, $d(U) \equiv 0$, $h(V) \equiv 0$ и $w(V) \equiv 0$,

$$\theta(V, U) = \begin{pmatrix} m(U) & f(V) \\ V & U \end{pmatrix}.$$

Так как R – регулярное множество полуполевой плоскости, то из определения следует, что множества Q и K, образованные всевозможными блоками V и

U соответственно, замкнуты по сложению, содержат нулевую матрицу, все ненулевые матрицы невырожденные. Кроме того, очевидно, что $E \in K$, $m(E) = E$. более того, можно считать, что множество Q также содержит единичную матрицу. Действительно, пусть $V_0 \in K$, $V_0 \neq 0$. Выберем новый базис линейного пространства W, задав матрицу перехода $A = \begin{pmatrix} V_0 & 0 \\ 0 & E \end{pmatrix}$, тогда

$$A\theta(V_0, 0)A^{-1} = \begin{pmatrix} V_0 & 0 \\ 0 & E \end{pmatrix} \begin{pmatrix} 0 & f(V_0) \\ V_0 & 0 \end{pmatrix} \begin{pmatrix} V_0^{-1} & 0 \\ 0 & E \end{pmatrix} = \begin{pmatrix} 0 & V_0 f(V_0) \\ E & 0 \end{pmatrix},$$

причем $ALA^{-1} = L$ и $A\theta(0, E)A^{-1} = \theta(0, E)$.

Условия $m(U) \in GL_n(p)$ для всех $0 \neq U \in K$ и $f(V) \in GL_n(p)$ для всех $0 \neq V \in Q$ вытекают из невырожденности матрицы $\theta(V, U) \neq 0$, так как

$$\det \theta(0, U) = \det m(U) \cdot \det U \quad \text{и} \quad \det \theta(V, 0) = \det f(V) \cdot \det V.$$

Рассматривая множество всех аффинных точек плоскости π вида $(0, x, 0, y)$ для $x = (x_{n+1}, \ldots, x_{2n})$, $y = (y_{n+1}, \ldots, y_{2n})$ $(x_i, y_i \in \mathbb{Z}_p)$, видим, что $(0, x, 0, y)^\tau = (0, x, 0, y)$, поэтому точки такого вида образуют бэровскую подплоскость π_τ, фиксируемую инволюцией τ. Так как $(0, x)\theta(0, U) = (0, xU)$, то K является регулярным множеством плоскости π_τ. Теорема доказана. □

Лемма 3.1.6. *Пусть, в условиях теоремы 3.1.5, множества Q и K – поля порядка p^n в $GL_n(p) \cup \{0\}$. Тогда, без ограничения общности, можно считать, что $Q = K$.*

Доказательство. Пусть матрица D – порождающий элемент мультипликативной группы K^*. Так как поля Q и K сопряжены в $GL_n(p)$, то существует такая матрица $P \in GL_n(p)$, что матрица $C = PDP^{-1}$ является порождающим элементом мультипликативной группы Q^*. Рассмотрим матрицы регулярного множества

$$\theta(C, 0) = \begin{pmatrix} 0 & f(C) \\ C & 0 \end{pmatrix} \quad \text{и} \quad \theta(0, D) = \begin{pmatrix} m(D) & 0 \\ 0 & D \end{pmatrix}$$

и выполним замену базиса линейного пространства W с матрицей перехода

$$M = \begin{pmatrix} D^{-1}PDP^{-1} & 0 \\ 0 & E \end{pmatrix},$$

не меняющей вида бэровской инволюции τ. Тогда

$$M\theta(0, D)M^{-1} = \begin{pmatrix} D^{-1}PDP^{-1}m(D)PD^{-1}P^{-1}D & 0 \\ 0 & D \end{pmatrix} = \begin{pmatrix} \overline{m}(D) & 0 \\ 0 & D \end{pmatrix},$$

$$M\theta(C,0)M^{-1} = \begin{pmatrix} 0 & D^{-1}PDP^{-1}f(C) \\ C & 0 \end{pmatrix} = \begin{pmatrix} 0 & \overline{f}(D) \\ D & 0 \end{pmatrix},$$

где $\overline{m}$, $\overline{f}$ – новые линейные функции, определяющие регулярное множество (в другом базисе). Таким образом, с точностью до изоморфизма плоскостей, можем считать $Q^* = \langle D \rangle$ и $Q = K$. □

Замечание 3.1.7. *Очевидно, что регулярное множество K определяется с точностью до изоморфизма соответствующей подплоскости π_τ. Для доказательства достаточно рассмотреть замену базиса $4n$-мерного линейного пространства с блочно-диагональной матрицей перехода.*

3.2. Элементарные абелевы 2-подгруппы автотопизмов

Для элементарной абелевой 2-подгруппы автотопизмов, порожденной бэровскими инволюциями, найдено матричное представление, единообразное для случаев четного и нечетного порядков полуполевой плоскости. Указана связь порядка плоскости с 2-рангом группы автотопизмов. Основной результат представляет теорема.

Теорема 3.2.1. *Пусть π – недезаргова полуполевая плоскость порядка p^N (p – простое число), группа автотопизмов которой содержит элементарную абелеву 2-подгруппу H порядка 2^m, все неединичные элементы которой являются бэровскими инволюциями,*

$$H = \langle \tau_1 \rangle \times \langle \tau_2 \rangle \times \cdots \times \langle \tau_m \rangle,$$

где τ_i – бэровские инволюции, фиксирующие поточечно различные бэровские подплоскости π_i ($i = 1, 2, \ldots, m$). Тогда N делится на 2^m и базис $2N$-мерного линейного пространства над $\mathbb{Z}_p$ можно выбрать так, что τ_i определяется блочно-диагональной матрицей, образованной 2^i блоками размерности $(N/2^{i-1}) \times (N/2^{i-1})$ вида (3.1.4).

При дополнительных ограничениях получены также результаты о подгруппе автотопизмов $H \simeq Sz(2^{2n+1})$ при $p > 2$ и $H \simeq A_4$ при $p = 2$ (теорема 3.2.4 и лемма 3.2.8).

Естественным образом следует разделять случаи полуполевых плоскостей нечетного и четного порядка, учитывая геометрический смысл инволюций. Пусть π – полуполевая плоскость нечетного порядка, тогда ее группа автотопизмов Λ всегда содержит нормальную элементарную абелеву подгруппу H_0 порядка 4, порожденную гомологиями,

$$H_0 = \left\{ \varepsilon, h_1 = \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix}, h_2 = \begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix}, h_3 = \begin{pmatrix} -E & 0 \\ 0 & -E \end{pmatrix} \right\}. \qquad (3.2.1)$$

Каждая из этих гомологий является единственным элементом порядка 2 в циклической группе, изоморфной мультипликативной группе одного из ядер координатизирующего полуполя. Очевидно, эти гомологии не сопряжены в Λ.

Случай, когда фактор-группа Λ/H_0 имеет нечетный порядок, не представляет интереса с точки зрения проблемы разрешимости Λ, поэтому предполагаем, что Λ содержит бэровскую инволюцию τ. При $|\pi| = 2^N$ группа автотопизмов Λ не содержит центральных коллинеаций, поэтому для $p = 2$ также считаем $\tau \in \Lambda$. Будем использовать результаты о матричном представлении бэровской инволюции τ и регулярного множества плоскости π, полученные в предыдущем параграфе.

Пусть π – недезаргова полуполевая плоскость нечетного порядка и τ – бэровская инволюция в группе автотопизмов Λ. Изучим вопрос об инволюциях в Λ, перестановочных с τ, это могут быть бэровские инволюции либо гомологии h_i (3.2.1).

Лемма 3.2.2. *Пусть π – недезаргова полуполевая плоскость порядка p^N ($p > 2$ – простое), $\tau \in \Lambda$ – бэровская инволюция (3.1.3). Если $\sigma \neq \tau$ – бэровская инволюция в $C_\Lambda(\tau)$, то ограничение σ на бэровскую подплоскость π_τ является либо гомологией, либо бэровской инволюцией. В первом случае $\sigma = h_i\tau$ ($i = 1, 2, 3$), во втором случае N делится на 4 и при подходящем выборе базиса*

$$\sigma = \begin{pmatrix} L & 0 & 0 & 0 \\ 0 & L & 0 & 0 \\ 0 & 0 & L & 0 \\ 0 & 0 & 0 & L \end{pmatrix}. \tag{3.2.2}$$

Доказательство. Так как σ перестановочна с τ, то

$$\sigma = \begin{pmatrix} A_1 & 0 & 0 & 0 \\ 0 & A_2 & 0 & 0 \\ 0 & 0 & B_1 & 0 \\ 0 & 0 & 0 & B_2 \end{pmatrix},$$

где $A_i, B_i \in GL_{N/2}(p)$, $A_i^2 = B_i^2 = E$ $(i = 1, 2)$. Тогда $\sigma_\tau = \begin{pmatrix} A_2 & 0 \\ 0 & B_2 \end{pmatrix}$ – автотопизм бэровской подплоскости π_τ, либо тождественный, либо гомология порядка 2, либо бэровская инволюция.

Пусть σ_τ – тождественное преобразование π_τ, $A_2 = B_2 = E$. Тогда для любой матрицы $\theta(V, U)$ из регулярного множества R (3.1.6) верно условие (2.2.3):

$$\begin{pmatrix} A_1 & 0 \\ 0 & E \end{pmatrix} \theta(V, U) \begin{pmatrix} B_1 & 0 \\ 0 & E \end{pmatrix} \in R.$$

В частности, для $E \in R$ получим $B_1 = A_1$. Далее, можно выбрать новый базис линейного пространства, не меняя τ, так, что матрица A_1 примет жорданову нормальную форму. По условию, σ – бэровская инволюция, поэтому среди ее характеристических корней только -1 и 1, причем в равном количестве. Кроме того, поскольку $\lambda^2 - 1$ – ее минимальный многочлен, то жорданова нормальная форма A_1 – это обязательно $-E$, т.е. $\sigma = \tau$, противоречие условию леммы.

Пусть σ_τ – гомология порядка 2 с осью $[0]$. Тогда $A_2 = -E$, $B_2 = E$ и $B_1 = -A_1$ из условия (2.2.3). Приводя A_1 к жордановой нормальной форме, получим диагональную матрицу с ± 1 на главной диагонали. Покажем, что возможно только $A_1 = \pm E$. Действительно, для $\theta(0, U)$ по (2.2.3) имеем

$$\begin{pmatrix} A_1 & 0 \\ 0 & -E \end{pmatrix} \begin{pmatrix} m(U) & 0 \\ 0 & U \end{pmatrix} \begin{pmatrix} -A_1 & 0 \\ 0 & E \end{pmatrix} = \begin{pmatrix} -A_1 m(U) A_1 & 0 \\ 0 & -U \end{pmatrix} \in R,$$

поэтому $m(-U) = -A_1 m(U) A_1$, $A_1 m(U) = m(U) A_1$ для всех $U \in K$. Предположим, что A_1 содержит и -1, и 1, тогда

$$A_1 = \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix} \begin{matrix} k \\ N/2 - k \end{matrix}$$

(здесь справа указано число строк). Разобьем матрицу $m(U)$ на клетки соответствующей размерности и выполним умножение:

$$m(U) = \begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix} \begin{matrix} k \\ N/2 - k \end{matrix}$$

$$A_1 m(U) = \begin{pmatrix} -M_1 & -M_2 \\ M_3 & M_4 \end{pmatrix} = \begin{pmatrix} -M_1 & M_2 \\ -M_3 & M_4 \end{pmatrix} = m(U) A_1 \Rightarrow M_2 = M_3 = 0,$$

т.е. матрицы $m(U)$ – блочно-диагональные для всех $U \in K$. Это невозможно: множество $\{m(U) \mid U \in K\}$ является регулярным множеством в $GL_{N/2}(p) \cup \{0\}$ и состоит из $p^{N/2}$ матриц, однозначно определяемых, например, нижней строкой. Таких вариантов при $0 < k < N/2$ будет меньше. Итак, матрица A_1 имеет на главной диагонали либо только -1, либо только 1. Получаем варианты $\sigma = h_1$ или $\sigma = h_1 \tau$.

Если σ_τ – гомология с осью $[0, 0]$, то, рассуждая аналогично, получаем $\sigma = h_2$ или $\sigma = h_2 \tau$. Если σ_τ – гомология с осью $[\infty]$, то $\sigma = h_3$ или $\sigma = h_3 \tau$.

Рассмотрим случай, когда σ_τ является бэровской инволюцией. Тогда N делится на 4, при подходящей замене базиса получим $A_2 = B_2 = L$. Приводя A_1 и B_1 к жордановой нормальной форме, приходим к выводу, что соответствующие матрицы диагональны с диагональными элементами ± 1. Кроме того, из условия (2.2.3) при $\theta(0, E) = E$ имеем $A_1 = B_1$. Так как количество элементов, равных -1, равно числу единичных элементов, то без ограничения общности можно полагать $A_1 = B_1 = L$. Лемма доказана. $\square$

Пусть π – полуполевая плоскость нечетного порядка p^N, $H < \Lambda$ – элементарная абелева 2-группа порядка 2^m, не содержащая гомологий. Тогда все инволюции в H только бэровские, и базис линейного пространства можно выбрать так, что все инволюции задаются диагональными матрицами. Занумеруем базисные инволюции в H: $\tau_1, \tau_2, \ldots, \tau_m$. Тогда матрица τ_1 образована двумя диагональными матрицами L размерности $(N/2 \times N/2)$, матрица τ_2 – четырьмя матрицами L размерности $(N/4 \times N/4)$, и так далее. Матрица τ_m образована 2^m матрицами L размерности $(N/2^{m-1} \times N/2^{m-1})$, при этом, конечно, $N/2^m \geq 1$. Эти рассуждения доказывают теорему 3.2.1 в случае $p > 2$.

Следствие 3.2.3. *Пусть π – недезаргова полуполевая плоскость порядка p^N ($p > 2$ – простое), где $N = 2^m \cdot s$, s нечетно, F – подгруппа в группе автотопизмов Λ, порожденная гомологиями. Тогда 2-ранг фактор-группы Λ/F не превышает m.*

Важным следствием теоремы 3.2.1 является также следующий результат.

Теорема 3.2.4. *Пусть π – недезаргова полуполевая плоскость порядка p^N ($p > 2$ – простое). Если N не делится на 2^{2m+1}, то группа автотопизмов плоскости π не содержит подгрупп, изоморфных $Sz(2^{2n+1})$ для всех $n \geq m$.*

Доказательство. Силовская 2-подгруппа в группе Судзуки $Sz(2^{2n+1})$ содержит элементарную абелеву подгруппу порядка 2^{2n+1}, инволюции в которой сопряжены (см., например, [15]). Если H – подгруппа с таким условием в группе автотопизмов, то H не может содержать гомологий. Тогда число 2^{2n+1} должно быть делителем N. □

Если $|\pi| = 2^N$, то каждая гомология имеет нечетный порядок, и элементарная абелева 2-подгруппа в группе автотопизмов Λ содержит только бэровские инволюции.

Лемма 3.2.5. *Пусть π – недезаргова полуполевая плоскость порядка 2^N, $\tau \in \Lambda$ – бэровская инволюция (3.1.3), где $L = \begin{pmatrix} E & E \\ 0 & E \end{pmatrix}$. Если σ – бэровская инволюция в $C_\Lambda(\tau)$ и бэровские подплоскости π_τ и π_σ различны, то ограничение σ на π_τ является бэровской инволюцией, N делится на 4, при подходящем выборе базиса σ имеет вид (3.2.2).*

Доказательство. Если $\sigma \in C_\Lambda(\tau)$ – бэровская инволюция, то

$$\sigma = \begin{pmatrix} A_1 & A_2 & 0 & 0 \\ 0 & A_1 & 0 & 0 \\ 0 & 0 & B_1 & B_2 \\ 0 & 0 & 0 & B_1 \end{pmatrix},$$

где $A_1^2 = B_1^2 = E$, $A_1A_2 = A_2A_1$, $B_1B_2 = B_2B_1$, причем ограничение σ на бэровскую подплоскость π_τ $\sigma_\tau = \begin{pmatrix} A_1 & 0 \\ 0 & B_1 \end{pmatrix}$ является бэровской инволюцией или тождественным преобразованием. Так как по условию σ_τ – бэровская инволюция, то базис в подпространствах $\{(0, x_2, 0, 0)\}$ и $\{(0, 0, 0, y_2)\}$ можно выбрать так, что $A_1 = B_1 = L$, $A_2 = B_2$, $A_2L = LA_2$, поэтому $A_2 = \begin{pmatrix} D_1 & D_2 \\ 0 & D_1 \end{pmatrix}$. Перейдем к новому базису $2N$-мерного пространства, используя матрицу перехода

$$T = \begin{pmatrix} E & C & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & E & C \\ 0 & 0 & 0 & E \end{pmatrix},$$

где $C = \begin{pmatrix} 0 & D_1 \\ D_1 & D_2 \end{pmatrix}$. Непосредственные вычисления показывают, что в новом базисе инволюция τ сохраняет свое матричное представление, а матрица $T\sigma T^{-1}$ становится блочно-диагональной вида (3.2.2).

Эти рассуждения завершают доказательство леммы 3.2.5 и, очевидно, доказывают теорему 3.2.1 для случая $p = 2$. □

Замечание 3.2.6. *Без потери общности можно считать, что в теореме 3.2.1 полуполевая плоскость π порядка q^N задана линейным пространством над ядром $N_0 \supseteq GF(q)$ ($q = p^s$, p – простое число), а Λ – подгруппа линейных над $GF(q)$ автотопизмов.*

Рассмотрим далее случай, когда бэровская инволюция σ (в обозначениях леммы 3.2.5) действует на бэровской подплоскости π_τ тождественно.

Лемма 3.2.7. *Пусть π – недезаргова полуполевая плоскость порядка 2^N, $\tau, \sigma \in \Lambda$ – перестановочные бэровские инволюции, фиксирующие поточечно одну бэровскую подплоскость $\pi_\tau = \pi_\sigma$. Тогда ядро K_0 этой подплоскости содержит подполе порядка 4 и при подходящем выборе базиса τ имеет вид (3.1.3),*

$$\sigma = \begin{pmatrix} E & A & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & E & A \\ 0 & 0 & 0 & E \end{pmatrix}, \qquad A \in K_0^*. \tag{3.2.3}$$

Доказательство. Достаточно показать, что $A \in K_0^*$. Действительно, рассмотрим условие (2.2.3) для σ и регулярного множества (3.1.5):

$$\begin{pmatrix} E & A \\ 0 & E \end{pmatrix} \theta(V, U) \begin{pmatrix} E & A \\ 0 & E \end{pmatrix} \in R \quad \forall U, V \in K. \tag{3.2.4}$$

При $V = 0$ и произвольном $U \in K$ из (3.2.4) имеем

$$\begin{pmatrix} U & m(U) + AU + UA \\ 0 & U \end{pmatrix} = \begin{pmatrix} U & m(U) \\ 0 & U \end{pmatrix},$$

$UA = AU$, то есть $A \in K_l^* = C_{GL_{n(2)}}(K)$, матрица A принадлежит левому ядру подплоскости π_τ. При $U = 0$ и произвольном $V \in K$:

$$\begin{pmatrix} E & A \\ 0 & E \end{pmatrix} \begin{pmatrix} V + m(V) + w(V) & f(V) \\ V & w(V) \end{pmatrix} \begin{pmatrix} E & A \\ 0 & E \end{pmatrix} =$$

$$= \theta(V, 0) + \begin{pmatrix} AV & VA + m(V)A + w(V)A + AVA + Aw(V) \\ 0 & VA \end{pmatrix} = \theta(V, VA),$$

при выполнении условий $AV = VA \in K$ и

$$m(VA) = V(A + A^2) + m(V)A + w(V)A + Aw(V), \qquad \forall V \in K. \tag{3.2.5}$$

Поэтому матрица A принадлежит пересечению правого, среднего и левого ядер подплоскости π_τ, т.е. ядру $K_0 = K_l \cap K_m \cap K_r$. □

Если ядро K_0 подплоскости π_τ изоморфно вкладывается в ядро R_0 плоскости π, то можно рассматривать K_0 в качестве основного поля и подгруппу Λ_0 линейных над K_0 автотопизмов. В этом случае $A = aE \in K_0^*$ – скалярная матрица, и справедлива теорема.

Теорема 3.2.8. *Пусть ядро R_0 плоскости π четного порядка 2^N содержит ядро K_0 бэровской подплоскости π_τ. Тогда подгруппа Λ_0 линейных над K_0 автотопизмов плоскости π не содержит подгруппы H, изоморфной знакопеременной группе A_4, инволюции которой поточечно фиксируют π_τ.*

Доказательство. Будем рассматривать $H \simeq A_4$ как $\langle \tau, \sigma, \gamma \rangle$, где τ и σ – перестановочные инволюции, коллинеация γ имеет порядок 3 и $\gamma^{-1}\tau\gamma = \sigma$. По лемме 3.2.7 бэровская инволюция τ имеет вид (3.1.3), σ имеет вид (3.2.3), условие (3.2.4) для скалярной матрицы $A = aE \in K_0$ принимает вид

$$m(aV) + am(V) = V, \qquad \forall V \in K. \tag{3.2.6}$$

Так как $\tau\gamma = \gamma\sigma$, то

$$\gamma = \begin{pmatrix} B_1 & B_2 & 0 & 0 \\ 0 & aB_1 & 0 & 0 \\ 0 & 0 & C_1 & C_2 \\ 0 & 0 & 0 & aC_1 \end{pmatrix},$$

и так как $\sigma\gamma = \gamma\tau\sigma$, то $a^2 = a+1$. Напомним, что $m(E) = 0$. Тогда условие (3.2.6) при $V = E$ дает $m(aE) = E$, а при $V = aE$

$$m(a^2E) + am(aE) = aE, \qquad m(aE) + m(E) + aE = aE, \qquad m(aE) = 0.$$

Получили противоречие, доказывающее лемму. □

Заметим, что вопрос о существовании подгруппы, изоморфной A_4, в группе коллинеаций конечной полуполевой плоскости, возникал уже давно. Этот вопрос неоднократно рассматривался на научном семинаре в Красноярском государственном университете под руководством Н. Д. Подуфалова. В частности, существенное продвижение в исследовании плоскостей нечетного порядка, допускающих большую группу бэровских коллинеаций, было достигнуто И. В. Бусаркиной (Шевелевой) [13, 12], показавшей, что такие плоскости не допускают A_4.

Для случая четного порядка автором в [154] указаны примеры полуполевых плоскостей, допускающих A_4 в трансляционном дополнении.

Предложение 3.2.9. *Пусть π – недезаргова полуполевая плоскость порядка 2^m, правое ядро R_r которой имеет порядок 4^k, $k \geqslant 1$. Тогда π допускает подгруппу коллинеаций, изоморфную знакопеременной группе A_4.*

Доказательство. Пусть правое ядро R_r плоскости π содержит подполе порядка 4, и $M \in R_r^*$ – примитивный элемент этого подполя, $M^3 = E$. Рассмотрим две элации $\omega_1, \omega_2 \in \Omega$ с осью $[0]$ и центром (∞) и гомологию $\gamma \in H_r$ с осью $[0,0]$ и центром (∞),

$$\omega_1 = \begin{pmatrix} E & E \\ 0 & E \end{pmatrix}, \qquad \omega_2 = \begin{pmatrix} E & M \\ 0 & E \end{pmatrix}, \qquad \gamma = \begin{pmatrix} E & 0 \\ 0 & M \end{pmatrix}.$$

Тогда нетрудно проверить непосредственными расчетами, что $|\omega_1| = |\omega_2| = 2$, $|\gamma| = 3$, $\gamma^{-1}\omega_1\gamma = \omega_2$, т.е. $\langle \omega_1, \omega_2 \rangle \leftthreetimes \langle \gamma \rangle \simeq A_4$. □

Рассмотрим еще три примера, иллюстрирующие результаты этого параграфа.

Пример 3.1. Существуют точно две, с точностью до изоморфизма, недезарговых полуполевых плоскости порядка $16 = 2^4$ (подробно в § 5.5, также [129]). Группа автотопизмов Λ имеет порядок 18 или 108, централизатор бэровской инволюции в Λ равен $\mathbb{Z}_2$ или $\mathbb{Z}_2 \leftthreetimes S_3$ соответственно, что согласуется с леммами 3.2.5 и 3.2.7.

Пример 3.2. Как указано в [123], существуют точно 124 неизоморфных полуполевых плоскости порядка 256 с левым ядром $R_l \simeq GF(16)$, допускающие бэровскую инволюцию τ в трансляционном дополнении G_0. Эти плоскости определяются регулярными множествами из (2×2)-матриц над $GF(16)$, и $G/G_0 \simeq Aut\, R_l$. Поскольку $|\pi| = 256 = 2^8$, элементарная абелева 2-подгруппа в группе автотопизмов Λ имеет порядок не более 8. По теореме 3.2.1, подгруппа линейных автотопизмов Λ_0 не содержит инволюций, перестановочных с τ.

Полученные результаты подтверждаются компьютерными расчетами, представленными в [130]. Централизатор бэровской инволюции τ в группе линейных автотопизмов Λ_0 равен

$$C_{\Lambda_0}(\tau) = H_l \times H_{rd} \times \langle\tau\rangle,$$

где $H_{rd} \simeq R_r^* \cap R_l^*$. Все бэровские инволюции в Λ_0 сопряжены, порядок Λ_0 равен $2 \cdot 5^s \cdot 3^m$ $(s, m = 1, 2, 3)$ или $2 \cdot 5 \cdot 3^2 \cdot 17$, группа Λ_0 разрешима.

Пример 3.3. Существуют точно восемь, с точностью до изоморфизма, полуполевых плоскостей порядка $81 = 3^4$, допускающих бэровскую инволюцию (§ 4.3 и [140]). Для каждой из них 2-ранг группы автотопизмов Λ равен трем, группа Λ имеет порядок 2^m $(m = 8, \ldots, 11)$, разрешима и содержит четыре или 100 (в одном случае) бэровских инволюций. Учитывая наличие инволютивных гомологий, отмечаем согласование результатов с доказанными выше.

3.3. 2-элементы группы автотопизмов

Используем метод регулярного множества для установления естественного ограничения на порядок 2-элементов в группе автотопизмов, а также для записи матричного представления автотопизмов порядка 4. Основной результат представлен в теореме 3.3.3. Следствие 3.3.8 выделяет группы $PSL(2, q)$, которые не могут быть подгруппами автотопизмов полуполевой плоскости данного порядка. Особый случай $p \equiv -1 \pmod 4$ требует иного подхода, что демонстрируют приведенные примеры полуполевых плоскостей порядка 81. Сочетание с результатами предыдущего параграфа выявляет еще один класс полуполевых плоскостей с разрешимой группой коллинеаций (следствие 3.3.7).

Начнем со вспомогательных результатов.

Лемма 3.3.1. *Пусть π – полуполевая плоскость порядка p^N, p – простое, $p \not\equiv -1 \pmod 4$, α – автотопизм порядка 4, $\tau = \alpha^2$ – бэровская инволюция. Тогда ограничение α на бэровскую подплоскость π_τ является бэровской инволюцией π_τ.*

Доказательство. Мы будем рассматривать два случая: $p \equiv 1 \pmod 4$ и $p = 2$. Выберем базис линейного пространства так, чтобы бэровская инволюция имела вид (3.1.3), матрицы регулярного множества – вид (3.1.6) или (3.1.5) соответственно.

Пусть $p \equiv 1 \pmod 4$. Предположим, что автотопизм α действует тождественно на подплоскости

$$\pi_\tau = \{(0, \dots, 0, x_1, \dots, x_n, 0, \dots, 0, y_1, \dots, y_n) \mid x_i, y_i \in \mathbb{Z}_p\}, \tag{3.3.1}$$

тогда из $\alpha\tau = \tau\alpha$ получим

$$\alpha = \begin{pmatrix} A & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & A & 0 \\ 0 & 0 & 0 & E \end{pmatrix}, \qquad A^2 = -E.$$

Так как α является коллинеацией, то выполнено условие (2.2.3) для $\theta(V, 0)$, отсюда

$$\begin{pmatrix} A^{-1} & 0 \\ 0 & E \end{pmatrix} \begin{pmatrix} 0 & f(V) \\ V & 0 \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & E \end{pmatrix} = \begin{pmatrix} 0 & A^{-1}f(V) \\ VA & 0 \end{pmatrix} = \theta(VA, 0), \quad \forall V \in Q,$$

поэтому $A \in Q_r$, это правое ядро полуполевой плоскости с регулярным множеством Q. Циклическая группа Q_r^* содержит все скалярные матрицы zE, $z \in \mathbb{Z}_p^*$, и из условия $p \equiv 1 \pmod 4$ имеем $A = iE$, $i^2 = -1$, $i \in \mathbb{Z}_p^*$. Тогда $f(iV) = -if(V)$, что противоречит $f(iV) = if(V)$ (из линейности функции). Следовательно, α не может действовать на подплоскости π_τ тождественно. Если предположить, что ограничение α на π_τ есть гомология, то следует применить доказанное к произведению α на соответствующую гомологию h_1, h_2 или h_3 (3.2.1).

Пусть $p = 2$. Из условия $\alpha\tau = \tau\alpha$ имеем

$$\alpha = \begin{pmatrix} A_1 & A_2 & 0 & 0 \\ 0 & A_1 & 0 & 0 \\ 0 & 0 & B_1 & B_2 \\ 0 & 0 & 0 & B_1 \end{pmatrix}, \qquad A_1^2 = B_1^2 = E.$$

Если α действует на бэровской подплоскости π_τ тождественно, то $A_1 = B_1 = E$ и α имеет порядок 2. Полученное противоречие полностью доказывает лемму. □

Лемма 3.3.2. *Пусть π – полуполевая плоскость порядка p^N, p – простое, $p \not\equiv -1 \pmod 4$, α – автотопизм порядка 2^n, $n \geq 2$, $\tau = \alpha^{2^{n-1}}$ – бэровская инволюция. Тогда ограничение α на бэровскую подплоскость π_τ является автотопизмом π_τ порядка 2^{n-1}.*

Доказательство. Запишем общее доказательство для $p \equiv 1 \pmod 4$ и $p = 2$. Из условия $\alpha\tau = \tau\alpha$ следует, что

$$\alpha = \begin{pmatrix} A_1 & A_2 & 0 & 0 \\ 0 & A_3 & 0 & 0 \\ 0 & 0 & B_1 & B_2 \\ 0 & 0 & 0 & B_3 \end{pmatrix}, \qquad A_3^{2^{n-1}} = B_3^{2^{n-1}} = E$$

(ограничения на остальные клетки пропустим). Действие α на бэровской подплоскости π_τ определяется матрицей

$$\beta = \begin{pmatrix} A_3 & 0 \\ 0 & B_3 \end{pmatrix}.$$

Если $|\beta| < 2^{n-1}$, то $A_3^{2^{n-2}} = B_3^{2^{n-2}} = E$, тогда автотопизм $\alpha^{2^{n-2}}$ порядка 4 действует тождественно на π_τ, что противоречит лемме 3.3.1. □

Теорема 3.3.3. *Пусть π – полуполевая плоскость порядка p^N, p – простое, $p \not\equiv -1 \pmod 4$. Если α – автотопизм порядка 2^n плоскости π и группа $\langle\alpha\rangle$ не содержит гомологий, то N делится на 2^n.*

Доказательство. Докажем утверждение по индукции. При $n = 1$ автотопизм α является бэровской инволюцией, поэтому порядок плоскости π является квадратом, N делится на 2.

Пусть утверждение доказано для $n-1$ ($n > 1$), и α – автотопизм порядка 2^n. Тогда $\tau = \alpha^{2^{n-1}}$ – бэровская инволюция, фиксирующая поточечно бэровскую подплоскость порядка $p^{N/2}$. По лемме 3.3.2, ограничение α на π_τ есть автотопизм порядка 2^{n-1}. Тогда, по индуктивному предположению, $N/2$ делится на 2^{n-1}, N делится на 2^n. Утверждение полностью доказано. □

Замечание 3.3.4. *Условие «группа $\langle\alpha\rangle$ не содержит гомологий» теоремы 3.3.3 и условие «τ – бэровская инволюция» лемм 3.3.1 и 3.3.2, безусловно, являются избыточными при $p = 2$, так как группа автотопизмов полуполевой плоскости четного порядка не содержит инволютивных гомологий либо элаций, и любая инволюция обязательно является бэровской. Указанные условия записаны для единообразия формулировки утверждений.*

Замечание 3.3.5. *Условие $p \not\equiv -1 \pmod 4$ в утверждениях существенно. Поясняющие примеры полуполевых плоскостей порядка 81 ($p = 3$) будут приведены позже.*

Так как группа автоморфизмов конечного полуполя изоморфна подгруппе автотопизмов соответствующей полуполевой плоскости (теорема 5.1.7 и [132]), то очевидно следствие.

Следствие 3.3.6. *Пусть W – полуполе порядка p^N, $p \not\equiv -1 \pmod 4$, p – простое. Если его группа автоморфизмов содержит элемент порядка 2^n, то N делится на 2^n.*

Следствие 3.3.7. *Пусть π – полуполевая плоскость порядка 4^n, где $n > 1$ нечетно. Тогда силовская 2-подгруппа в ее группе автотопизмов элементарная абелева. Если при этом n простое и все бэровские подплоскости плоскости π недезарговы, то группа коллинеаций $Aut\,\pi$ разрешима.*

Доказательство. Первая часть утверждения очевидна. Для доказательства второй части следует обратиться к § 3.2: если бэровские подплоскости двух перестановочных бэровских инволюций различны, то порядок плоскости равен 2^N, где N делится на 4 (лемма 3.2.5) – это противоречит условию. Значит, любые две различные бэровские инволюции силовской 2-подгруппы фиксируют одну и ту же бэровскую подплоскость порядка 2^n. Эта подплоскость недезаргова по условию, поэтому ее ядро имеет порядок $4 \le 2^k < 2^n$, $k|n$ по определению ядра. Полученное противоречие показывает, что силовская 2-подгруппа в группе автотопизмов Λ имеет порядок 2, Λ разрешима, $Aut\,\pi$ разрешима. □

Укажем пример использования теоремы 3.3.3 к изучению условий существования в группе автотопизмов полуполевой плоскости подгрупп из списка Д.Г. Томпсона. Приведенное ниже следствие уточняет теорему Г. Мурхауза [93, теорема 1.1]: если проективная плоскость Π порядка $n < q$ допускает группу коллинеаций $G \simeq PSL(2,q)$, то Π дезаргова. Из этой теоремы следует, что группа автотопизмов недезарговой полуполевой плоскости порядка p^N не может содержать подгруппы $G \simeq PSL(2,q)$ для $q > p^N$. Теорема 3.3.3 добавляет ограничение на порядок q основного поля.

Следствие 3.3.8. *Пусть π – недезаргова полуполевая плоскость порядка p^N, где $p = 2$ или $p \equiv 1 \pmod 4$, $N = 2^m \cdot s$, s нечетно. Группа автотопизмов Λ плоскости π не содержит подгрупп, изоморфных $PSL(2,q)$, где $q-1$ делится на 2^{m+2}.*

Доказательство. Вытекает из рассмотрения порядка диагональной (циклической) подгруппы в $SL(2,q)$. □

Лемма 3.3.1 позволяет получить унифицированное матричное представление для автотопизмов порядка 4, квадрат которых является бэровской инволюцией. Такое матричное представление полезно для дальнейшего изучения полуполевых плоскостей, допускающих определенные подгруппы автотопизмов, а также для построения примеров.

Теорема 3.3.9. *Пусть π – полуполевая плоскость порядка p^N, p – простое, $p \equiv 1 \pmod 4$, α – автотопизм порядка 4, $\tau = \alpha^2$ – бэровская инволюция. Тогда N делится на 4 и базис линейного пространства может быть выбран так, что, с точностью умножения на инволютивные гомологии h_i, автотопизм τ имеет вид (3.1.3),*

$$\alpha = \begin{pmatrix} iL & 0 & 0 & 0 \\ 0 & L & 0 & 0 \\ 0 & 0 & iL & 0 \\ 0 & 0 & 0 & L \end{pmatrix}, \tag{3.3.2}$$

где $i \in \mathbb{Z}_p$, $i^2 = -1$. Регулярное множество R плоскости π состоит из матриц вида

$$\theta(V_1, U_1, V_2, U_2) = \begin{pmatrix} m_1(U_2) & m_2(V_2) & f_1(V_1) & f_2(U_1) \\ m_3(V_2) & m_4(U_2) & f_3(U_1) & f_4(V_1) \\ \nu(U_1) & \psi(V_1) & \mu(U_2) & \varphi(V_2) \\ V_1 & U_1 & V_2 & U_2 \end{pmatrix}, \tag{3.3.3}$$

где все блоки-подматрицы имеют размерность $(N/4 \times N/4)$, $V_1 \in Q_1$, $U_1 \in K_1$, $V_2 \in Q_2$, $U_2 \in K_2$, множества матриц Q_1, K_1, Q_2, K_2 являются регулярными множествами полуполевых плоскостей порядка $p^{N/4}$, все функции аддитивны.

Доказательство. По лемме 3.3.1, ограничение α на бэровскую подплоскость π_τ является бэровской инволюцией, поэтому $|\pi_\tau|$ является квадратом, N кратно 4, базис можно выбрать так, что

$$\alpha = \begin{pmatrix} A & 0 & 0 & 0 \\ 0 & L & 0 & 0 \\ 0 & 0 & A & 0 \\ 0 & 0 & 0 & L \end{pmatrix}, \qquad A^2 = -E.$$

Из условия (2.2.3) имеем

$$\begin{pmatrix} A^{-1}m(U)A & A^{-1}f(V)L \\ LVA & LUL \end{pmatrix} = \theta(LVA, LUL) \in R \qquad \forall V \in Q\ , U \in K,$$

поэтому

$$LVA \in Q, \quad LUL \in K \qquad \forall V \in Q,\ U \in K.$$

Минимальный многочлен матрицы A делит $\lambda^2 + 1$, поэтому либо матрица скалярная, $A = \pm iE$, либо A диагональная с элементами i и $-i$ на диагонали. При $V = E$ получим $LA \in Q$; рассмотрим матрицу $\pm iE + LA \in Q$. Если A отличается от $\pm iL$, то мы получим ненулевую вырожденную матрицу в регулярном множестве Q, что невозможно. Для определенности, таким образом, можем считать, что $A = iL$.

Снова обращаясь к условию (2.2.3), получим:

$$\begin{pmatrix} -iL & 0 \\ 0 & L \end{pmatrix} \begin{pmatrix} m(U) & f(V) \\ V & U \end{pmatrix} \begin{pmatrix} iL & 0 \\ 0 & L \end{pmatrix} = \begin{pmatrix} Lm(U)L & -iLf(V)L \\ iLVL & LUL \end{pmatrix},$$

отсюда

$$m(LUL) = Lm(U)L, \quad f(LVL) = -Lf(V)L, \qquad \forall V \in Q,\ \forall U \in K.$$

Таким образом, полуполевые плоскости порядка $p^{N/2}$ с регулярными множествами Q и K допускают бэровскую инволюцию (3.1.3), поэтому матрицы $V \in Q$, $U \in K$ имеют форму сходную с (3.1.6):

$$V = \begin{pmatrix} \nu(U_1) & \psi(V_1) \\ V_1 & U_1 \end{pmatrix}, \qquad U = \begin{pmatrix} \mu(U_2) & \varphi(V_2) \\ V_2 & U_2 \end{pmatrix}.$$

Полагая

$$m(U) = m(V_2, U_2) = \begin{pmatrix} m_1(V_2, U_2) & m_2(V_2, U_2) \\ m_3(V_2, U_2) & m_4(V_2, U_2) \end{pmatrix},$$

из условия $m(-V_2, U_2) = Lm(V_2, U_2)L$ и аддитивности m заключаем, что функции m_1, m_4 зависят только от блока U_2, а m_2, m_3 – только от V_2. Аналогичное рассмотрение условия $f(-V_1, U_1) = -Lf(V_1, U_1)L$ завершает доказательство. □

Теорема 3.3.10. *Пусть π – полуполевая плоскость порядка 2^N, α – автотопизм порядка 4, $\tau = \alpha^2$ – бэровская инволюция. Тогда N делится на 4 и базис линейного пространства может быть выбран так, что τ имеет вид (3.1.3),*

$$\alpha = \begin{pmatrix} L & J & 0 & 0 \\ 0 & L & 0 & 0 \\ 0 & 0 & L & J \\ 0 & 0 & 0 & L \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & 0 \\ E & 0 \end{pmatrix}.$$

Доказательство. По лемме 3.3.1, ограничение α на бэровскую подплоскость π_τ является бэровской инволюцией, поэтому $|\pi_\tau|$ – квадрат, N кратно 4, и базис можно выбрать так, что

$$\alpha = \begin{pmatrix} A_1 & A_2 & 0 & 0 \\ 0 & A_1 & 0 & 0 \\ 0 & 0 & B_1 & B_2 \\ 0 & 0 & 0 & B_1 \end{pmatrix}, \qquad \begin{aligned} &A_1^2 = B_1^2 = E, \\ &A_1A_2 + A_2A_1 = E, \\ &B_1B_2 + B_2B_1 = E. \end{aligned}$$

Ограничение α на бэровскую подплоскость π_τ определяется матрицей $\begin{pmatrix} A_1 & 0 \\ 0 & B_1 \end{pmatrix}$, и выбор базиса соответствующего линейного пространства позволяет считать

далее, что $A_1 = B_1 = L$. Так как α является коллинеацией, то из условия (2.2.3) при $\theta(V,U) = E$ получим

$$\begin{pmatrix} L & LA_2L \\ 0 & L \end{pmatrix} \begin{pmatrix} L & B_2 \\ 0 & L \end{pmatrix} = \begin{pmatrix} E & LB_2 + LA_2 \\ 0 & E \end{pmatrix} \in R \Rightarrow B_2 = A_2.$$

Из условия $A_1A_2 + A_2A_1 = E$ при $A_1 = L$ уточним вид клетки A_2:

$$A_2 = \begin{pmatrix} A_{21} & A_{22} \\ E & A_{21} \end{pmatrix}.$$

Выполним теперь замену базиса линейного пространства размерности $2N$ так, чтобы сохранить матрицу τ и, по возможности, упростить матрицу α (следовательно, A_2). Для этого используем матрицу перехода

$$T = \begin{pmatrix} E & T_2 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & E & T_2 \\ 0 & 0 & 0 & E \end{pmatrix}, \qquad \text{где} \quad T_2 = \begin{pmatrix} 0 & 0 \\ A_{21} & A_{22} \end{pmatrix}.$$

Вычисляя $T\alpha T^{-1}$, получим (для одного блока):

$$\begin{pmatrix} E & T_2 \\ 0 & E \end{pmatrix} \begin{pmatrix} L & A_2 \\ 0 & L \end{pmatrix} \begin{pmatrix} E & T_2 \\ 0 & E \end{pmatrix} = \begin{pmatrix} L & LT_2 + A_2 + T_2L \\ 0 & L \end{pmatrix} = \begin{pmatrix} L & J \\ 0 & L \end{pmatrix}.$$

Теорема доказана. □

Мы не будем записывать матричное представление регулярного множества полуполевой плоскости четного порядка, допускающей автотопизм порядка 4, ввиду очень громоздкой записи и долгого вывода. Как и в теореме 3.3.9, блоки-четверти матрицы $\theta(V,U)$ примут вид, отчасти аналогичный (3.1.5).

Отметим особый случай $p \equiv -1 \pmod 4$, исключенный в условии теоремы 3.3.3 и вспомогательных лемм. Обратим внимание, что такая характеристика основного поля выделялась как особенная и в других исследованиях. В частности, Г. Мурхауз [93, лемма 2.5] указывает, что для проективной плоскости Π порядка n^2, где $n \equiv 3 \pmod 4$, и циклической группы коллинеаций G порядка 4 инволюция в G обязательно является перспективностью.

Другая особенность при «плохой» характеристике была замечена автором в ходе изучения 3-примитивных полуполевых плоскостей: множитель 2^m числа N не ограничивает порядок 2-элементов в группе автотопизмов.

Пример 3.4. Существуют ровно восемь, с точностью до изоморфизма, полуполевых плоскостей порядка $81 = 3^4$, допускающих бэровскую инволюцию (подробно в § 4.3). Для каждой из них группа автотопизмов Λ имеет порядок

2^m ($m = 8, \ldots, 11$), разрешима и содержит четыре или 100 (в одном случае) бэровских инволюций. Мы предлагаем обратить внимание на последние два столбца Табл. 8 из § 4.3. Для построенных плоскостей в этих столбцах указано количество n_8 автотопизмов порядка 8: 32, 160, 192 и 576, и количество n_{16} автотопизмов порядка 16: 128 и 768. Таким образом, полуполевые плоскости порядка 3^4 допускают 2-элементы порядка более 4 в группе автотопизмов.

Рассмотрим теперь лемму 3.3.1 и укажем при $p \equiv -1 \pmod 4$ пример автотопизма порядка 4, действующего тождественно на бэровской подплоскости.

Пример 3.5. Поставим задачу: в обозначениях леммы 3.3.1 построить полуполевую плоскость порядка 81, допускающую одновременно автотопизм α порядка 4, действующий тождественно на бэровской подплоскости π_τ, и автотопизм γ порядка 4, индуцирующий на π_τ бэровскую инволюцию. Здесь $\tau = \alpha^2 = \gamma^2$ – бэровская инволюция. Ввиду неприводимости многочлена $\lambda^2 + 1$ над полем $\mathbb{Z}_p$ мы не можем записать α или γ в жордановой нормальной форме. Будем считать, что

$$\alpha = \begin{pmatrix} S & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & S & 0 \\ 0 & 0 & 0 & E \end{pmatrix}, \quad \gamma = \begin{pmatrix} P & 0 & 0 & 0 \\ 0 & L & 0 & 0 \\ 0 & 0 & P & 0 \\ 0 & 0 & 0 & L \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$S^2 = P^2 = -E$, $P \neq S$. Уточняя при условии (2.2.3) для α и γ вид регулярного множества (3.1.6), мы получим:

$$Q = K = \{-xS + yE \mid x, y \in \mathbb{Z}_p\},$$

$$m(-xS + yE) = xM + yE, \qquad f(-xS + yE) = xF - ySF,$$

$$M = \begin{pmatrix} 0 & m_1 \\ -m_1 & 0 \end{pmatrix}, \quad F = \begin{pmatrix} f_1 & 0 \\ 0 & f_2 \end{pmatrix}, \quad P = \begin{pmatrix} p_1 & p_2 \\ p_2 & -p_1 \end{pmatrix}, \quad p_1^2 + p_2^2 = -1.$$

Расчеты, приводящие к этим результатам, весьма несложные, и мы их не приводим. Выбрав в качестве основного поля минимальный вариант $\mathbb{Z}_3$, мы должны теперь подобрать коэффициенты m_1, f_1, f_2 так, чтобы все ненулевые матрицы регулярного множества были невырожденными. Как показывают компьютерные расчеты, это условие выполняется при $M = S$ и $F = \pm E$. Таким образом, регулярное множество из матриц вида

$$\begin{pmatrix} xS + yE & \pm(zE - tS) \\ -zS + tE & -xS + yE \end{pmatrix}, \qquad x, y, z, t \in \mathbb{Z}_3,$$

представляет пример, поясняющий необходимость условия на характеристику поля во всех результатах этого параграфа.

3.4. Подгруппа автотопизмов, изоморфная A_4

Как следует из леммы 3.2.9, несложно указать достаточное количество примеров полуполевых плоскостей четного порядка, допускающих A_4. Тем больший интерес вызывают плоскости нечетного порядка. Первые результаты автора в этом направлении были получены совместно со студенткой В. О. Прамзиной в [127]. Для полуполевой плоскости ранга 2 над конечным полем нечетного порядка доказано отсутствие подгруппы, изоморфной A_4, в группе автотопизмов и в линейном трансляционном дополнении вообще.

Лемма 3.4.1. *Пусть π – полуполевая плоскость ранга нечетного порядка p^{2k} с ядром $N_0 \supseteq GF(p^k)$ ($p > 2$ – простое). Тогда линейное трансляционное дополнение G_0 плоскости π не содержит подгруппы, изоморфной знакопеременной группе A_4.*

Доказательство. Регулярное множество плоскости π зададим 2×2-матрицами над $GF(p^k)$, коллинеации – матрицами размерности 4×4. Так как гомологии порядка два не сопряжены в G_0, то подгруппа $H \simeq A_4$ содержит бэровские инволюции τ, σ, $\tau\sigma = \sigma\tau$ и коллинеацию γ порядка три с условием $\gamma^{-1}\tau\gamma = \sigma$. Без ограничения общности можно считать, что τ имеет вид (3.1.3) при $L = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Если $\gamma = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$ и $\gamma^3 = \varepsilon$, то $A^3 = D^3 = E$, $AB + BD = -A^{-1}BD^{-1}$. Из условия перестановочности τ с $\sigma = \gamma^{-1}\tau\gamma$ имеем

$$LA^2LA = A^2LAL, \quad LD^2LD = D^2LDL$$

$$LA^2LB + L(AB + BD)LD = A^2LBL + (AB + BD)LDL.$$

Пусть $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. Тогда из первого условия $A = \begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix}$ либо $A = \begin{pmatrix} 0 & a_{12} \\ a_{21} & 0 \end{pmatrix}$. Второй случай невозможен, так как $A^3 = E$. Таким образом, A и D – диагональные матрицы, поэтому $LA = AL$, $LD = DL$. Далее, из третьего условия $B = LBL$ и окончательно

$$\sigma = \begin{pmatrix} A^2LA & A^2LB - A^2BD^2LD \\ 0 & D^2LD \end{pmatrix} = \begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix} = \tau,$$

лемма доказана. □

Доказано также, что трансляционное дополнение G плоскости нечетного порядка ранга два тоже не содержит подгруппы, изоморфной A_4. При доказательстве были рассмотрены не только линейные, но и полулинейные отображения в

качестве коллинеаций τ и γ. Мы не будем останавливаться на этом результате: он не является существенным при изучении проблемы разрешимости $Aut\,\pi$.

Отказываясь от условия на порядок ядра полуполевой плоскости, приходим к необходимости записи регулярного множества матрицами размерности $N \times N$ над полем простого порядка $\mathbb{Z}_p$. В работе [131] автором получено матричное представление такого регулярного множества для полуполевой плоскости, допускающей группу автотопизмов $H \simeq A_4$.

Теорема 3.4.2. *Пусть π – полуполевая плоскость нечетного порядка p^N ($p > 2$ – простое), группа автотопизмов Λ которой содержит подгруппу $H \simeq A_4$. Тогда $N = 4n$ и плоскость π может быть задана $8n$-мерным векторным пространством над $\mathbb{Z}_$ так, что регулярное множество плоскости $R \subset GL_{4n}(p) \cup \{0\}$ образовано $(4n \times 4n)$-матрицами вида*

$$\theta(V_1,U_1,V_2,U_2) = \begin{pmatrix} \mu(J^{-1}U_2J) & \nu(J^{-1}V_2) & \psi(J^{-1}U_1) & \varphi(J^{-1}V_1)J^{-1} \\ \psi(JV_2) & \mu(JU_2J^{-1}) & \nu(JV_1) & \varphi(JU_1)J^{-1} \\ \nu(U_1) & \psi(V_1) & \mu(U_2) & \varphi(V_2) \\ V_1 & U_1 & V_2 & U_2 \end{pmatrix}, \quad (3.4.1)$$

где $J^3 = E$; $V_1 \in Q_1$, $U_1 \in K_1$, $V_2 \in Q_2$, $U_2 \in K_2$; Q_1, K_1, Q_2, K_2 – регулярные множества в $GL_n(p) \cup \{0\}$;

$$J^{-1}K_2J = K_2, \quad JK_1 = Q_2, \quad JQ_1 = K_1, \quad JQ_2 = Q_1;$$

ν, ψ, μ, φ – инъективные линейные отображения из K_1, Q_1, K_2, Q_2 соответственно в $GL_n(p) \cup \{0\}$, причем

$$\mu(E) = E, \quad \nu(E) = E, \quad \varphi(E) \neq E, \quad \psi(E) \neq E. \quad (3.4.2)$$

Для доказательства этой теоремы найдем предварительно матричное представление элементов τ, σ, γ, порождающих подгруппу:

$$H = \langle \tau, \sigma \rangle \leftthreetimes \langle \gamma \rangle \simeq A_4, \quad |\tau| = |\sigma| = 2, \quad |\gamma| = 3, \quad \sigma\tau = \tau\sigma, \quad \gamma^{-1}\tau\gamma = \sigma. \quad (3.4.3)$$

Так как инволюции $\tau, \sigma, \tau\sigma$ сопряжены в H, то по лемме (3.2.2) это бэровские инволюции, и можно считать, что τ имеет вид (3.1.3), а σ – вид (3.2.2). При этом матрица τ имеет два диагональных блока L размерности $4n \times 4n$, а матрица σ – четыре диагональных блока L размерности $2n \times 2n$.

Лемма 3.4.3. *Пусть π – полуполевая плоскость нечетного порядка p^N ($p > 2$ – простое), группа автотопизмов Λ которой содержит подгруппу H (3.4.3). Тогда порядок плоскости π равен p^{4n} и, без ограничения общности, можно*

записать автотопизмы τ и σ матрицами размерности $8n \times 8n$ вида (3.1.3) и (3.2.2) соответственно,

$$\gamma = \begin{pmatrix} 0 & 0 & E & 0 & 0 & 0 & 0 & 0 \\ E & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & E & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & J & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & E & 0 \\ 0 & 0 & 0 & 0 & E & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & E & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & J \end{pmatrix}, \qquad J^3 = E. \tag{3.4.4}$$

Доказательство. Учитывая рассуждения выше, найдем только вид матрицы γ. Пусть

$$\gamma = \begin{pmatrix} S & 0 \\ 0 & Z \end{pmatrix}, \quad S = \begin{pmatrix} S_1 & S_2 \\ S_3 & S_4 \end{pmatrix}, \quad Z = \begin{pmatrix} Z_1 & Z_2 \\ Z_3 & Z_4 \end{pmatrix}.$$

Так как $\tau^\gamma = \sigma$, $\sigma^\gamma = \tau\sigma$, то

$$S^{-1} \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix} S = \begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix}, \quad S^{-1} \begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix} S = \begin{pmatrix} -L & 0 \\ 0 & L \end{pmatrix},$$

аналогичные равенства выполняются для матрицы Z. Рассмотрим далее только соотношения, связанные с матрицей S:

$$\begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix} \begin{pmatrix} S_1 & S_2 \\ S_3 & S_4 \end{pmatrix} = \begin{pmatrix} S_1 & S_2 \\ S_3 & S_4 \end{pmatrix} \begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix},$$
$$\begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix} \begin{pmatrix} S_1 & S_2 \\ S_3 & S_4 \end{pmatrix} = \begin{pmatrix} S_1 & S_2 \\ S_3 & S_4 \end{pmatrix} \begin{pmatrix} -L & 0 \\ 0 & L \end{pmatrix},$$

$$-S_1 = S_1L,\ -S_2 = S_2L,\ S_3 = S_3L,\ S_4 = S_4L,$$
$$LS_1 = -S_1L,\ LS_2 = S_2L,\ LS_3 = -S_3L,\ LS_4 = S_4L.$$

Записывая каждую из матриц S_i в виде $S_i = \begin{pmatrix} S_{i1} & S_{i2} \\ S_{i3} & S_{i4} \end{pmatrix}$, получим:

$$S_{12} = S_{14} = S_{11} = 0, \quad S_{22} = S_{24} = S_{23} = 0,$$
$$S_{31} = S_{33} = S_{34} = 0, \quad S_{41} = S_{43} = S_{42} = 0,$$

тогда

$$S = \begin{pmatrix} 0 & 0 & S_{21} & 0 \\ S_{13} & 0 & 0 & 0 \\ 0 & S_{32} & 0 & 0 \\ 0 & 0 & 0 & S_{44} \end{pmatrix},$$

где все записанные блоки S_{ij} являются невырожденными матрицами. Вычисляя $S^3 = E$, получим далее равенства

$$S_{21}S_{32}S_{13} = E, \quad S_{13}S_{21}S_{32} = E, \quad S_{32}S_{13}S_{21} = E, \quad S_{44}^3 = E.$$

Выполним замену базиса, не меняющую вида матриц τ и σ, используя матрицу перехода

$$M = \begin{pmatrix} S_{21}^{-1} & 0 & 0 & 0 \\ 0 & S_{21}^{-1}S_{13}^{-1} & 0 & 0 \\ 0 & 0 & E & 0 \\ 0 & 0 & 0 & E \end{pmatrix},$$

тогда

$$M \begin{pmatrix} 0 & 0 & S_{21} & 0 \\ S_{13} & 0 & 0 & 0 \\ 0 & S_{32} & 0 & 0 \\ 0 & 0 & 0 & S_{44} \end{pmatrix} M^{-1} = \begin{pmatrix} 0 & E & 0 & 0 \\ E & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & 0 & S_{44} \end{pmatrix}.$$

Таким образом, учитывая возможность изменения базиса, считаем, что

$$S = \begin{pmatrix} 0 & E & 0 & 0 \\ E & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & 0 & I \end{pmatrix}, \quad Z = \begin{pmatrix} 0 & E & 0 & 0 \\ E & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & 0 & J \end{pmatrix},$$

где $I^3 = J^3 = E$. Заметим, что рассматривая в качестве матрицы перехода произвольную блочно-диагональную матрицу M с диагональными блоками размерностью $n \times n$, мы не сможем в общем случае привести блок S_{44} к виду E. Однако, если многочлен $\lambda^3 - 1$ разлагается над $\mathbb{Z}_n$ на линейные множители, можно привести S_{44} к жордановой нормальной форме.

Далее, поскольку γ – коллинеация, то из условия (2.2.3) имеем $S^{-1}Z \in R$, тогда

$$S^2Z = \begin{pmatrix} E & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & E & 0 \\ 0 & 0 & 0 & I^2J \end{pmatrix} = E,$$

отсюда $I = J$, $\gamma = \begin{pmatrix} S & 0 \\ 0 & S \end{pmatrix}$, лемма доказана. □

Лемма 3.4.4. *Пусть π – полуполевая плоскость нечетного порядка p^{4n} ($p > 2$ – простое), группа автотопизмов Λ которой содержит бэровские инволюции τ (3.1.3) и σ (3.2.2). Тогда произвольная матрица регулярного мно-*

жества плоскости π *записывается в виде*

$$\theta(V,U)=\begin{pmatrix} m(U) & f(V) \\ V & U \end{pmatrix}=\begin{pmatrix} m_1(U_2) & m_2(V_2) & f_1(U_1) & f_2(V_1) \\ m_3(V_2) & m_4(U_2) & f_3(V_1) & f_4(U_1) \\ \nu(U_1) & \psi(V_1) & \mu(U_2) & \varphi(V_2) \\ V_1 & U_1 & V_2 & U_2 \end{pmatrix},$$

где $V_1\in Q_1$, $U_1\in K_1$, $V_2\in Q_2$, $U_2\in K_2$, *функции* ν, ψ, μ, φ, m_i, f_i $(i=1,\dots,4)$ – *линейные отображения из множества* $n\times n$*-матриц в* $GL_n(p)\cup\{0\}$, *причем* $m_1(E)=m_4(E)=\mu(E)=E$.

Доказательство. По лемме 3.1.5, матрицы регулярного множества $R\subset GL_{4n}(p)\cup\{0\}$ имеют вид (3.1.6). Разобьем матрицы $V\in Q$, $U\in K$ размерности $2n\times 2n$ на $n\times n$-блоки, пусть V_1,U_1 – нижние блоки в V, V_2,U_2 – нижние блоки в U. Тогда (снова по лемме 3.1.5) регулярное множество $K\subset GL_{2n}(p)\cup\{0\}$ бэровской подплоскости π_τ имеет вид

$$K=\left\{U=\begin{pmatrix} \mu(U_2) & \varphi(V_2) \\ V_2 & U_2 \end{pmatrix}\;\middle|\; U_2\in K_2,\ V_2\in Q_2\right\},$$

где K_2,Q_2 – регулярные множества в $GL_n(p)\cup\{0\}$, μ и φ – инъективные линейные отображения из K_2 и Q_2 соответственно в $GL_n(p)\cup\{0\}$, $\mu(E)=E$, $\varphi(E)\neq E$.

Рассмотрим коллинеацию σ и проверим выполнение условия (2.2.3)

$$\begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix}\theta(V,U)\begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix}\in R\quad\forall U\in K,\ \forall V\in Q.$$

Положим $V=0$, тогда для произвольного $U\in K$ имеем

$$\begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix}\begin{pmatrix} m(U) & 0 \\ 0 & U \end{pmatrix}\begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix}=\begin{pmatrix} Lm(U)L & 0 \\ 0 & LUL \end{pmatrix}=\theta(0,LUL),$$

поэтому $LUL\in K$ и $m(LUL)=Lm(U)L$. Положим

$$m(U)=\begin{pmatrix} m_1(V_2,U_2) & m_2(V_2,U_2) \\ m_3(V_2,U_2) & m_4(V_2,U_2) \end{pmatrix},$$

где $V_2\in Q_2$, $U_2\in K_2$, тогда

$$Lm(U)L=\begin{pmatrix} m_1(V_2,U_2) & -m_2(V_2,U_2) \\ -m_3(V_2,U_2) & m_4(V_2,U_2) \end{pmatrix}.$$

Учитывая, что $LUL = \begin{pmatrix} \mu(U_2) & -\varphi(V_2) \\ -V_2 & U_2 \end{pmatrix}$, для произвольных элементов $U_2 \in K_2$ и $V_2 \in Q_2$ получим равенства

$$m_1(V_2, U_2) = m_1(-V_2, U_2), \quad -m_2(V_2, U_2) = m_2(-V_2, U_2),$$
$$-m_3(V_2, U_2) = m_3(-V_2, U_2), \quad m_4(V_2, U_2) = m_4(-V_2, U_2).$$

В силу аддитивности функций m_i делаем очевидные выводы: m_1 и m_4 не зависят от V_2, m_2 и m_3 не зависят от U_2. Таким образом, можно записать функцию $m(U)$ в виде

$$m(U) = \begin{pmatrix} m_1(U_2) & m_2(V_2) \\ m_3(V_2) & m_4(U_2) \end{pmatrix}.$$

Пусть, далее, $U = 0$, тогда для произвольного $V \in Q$ верно

$$\begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix} \begin{pmatrix} 0 & f(V) \\ V & 0 \end{pmatrix} \begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix} = \begin{pmatrix} 0 & Lf(V)L \\ LVL & 0 \end{pmatrix} = \theta(LVL, 0).$$

Из этого условия следует, что регулярное множество Q также определяет полуполевую плоскость, допускающую бэровскую инволюцию $\begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix}$, и поэтому каждая матрица V может быть записана в виде (3.1.6)

$$V = \begin{pmatrix} \nu(U_1) & \psi(V_1) \\ V_1 & U_1 \end{pmatrix},$$

где $V_1 \in Q_1$ и $U_1 \in K_1$. Множества Q_1, K_1 при этом являются регулярными множествами в $GL_n(p) \cup \{0\}$, $\nu(E) = E$, $\psi(E) \neq E$. Вычисляя $Lf(V)L = f(LVL)$, получим соотношения для функций f_i, аналогичные приведенным выше, откуда

$$f(V) = \begin{pmatrix} f_1(U_1) & f_2(V_1) \\ f_3(V_1) & f_4(U_1) \end{pmatrix},$$

лемма доказана. □

Лемма 3.4.5. *В условиях леммы 3.4.3 пусть σ_0 – сужение σ на π_τ, π_1 – бэровская подплоскость в π_τ, фиксируемая инволюцией σ_0, тогда $\begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix}$ – автотопизм плоскости π_1.*

Доказательство. Запишем коллинеацию $\gamma = \begin{pmatrix} S & 0 \\ 0 & S \end{pmatrix}$ в виде (3.4.4), введя обозначения для отдельных блоков:

$$E_1 = \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & E \\ 0 & 0 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 0 & 0 \\ E & 0 \end{pmatrix}, \quad E_J = \begin{pmatrix} 0 & 0 \\ 0 & J \end{pmatrix},$$

тогда $S = \begin{pmatrix} E_3 & E_1 \\ E_2 & E_J \end{pmatrix}$. Так как γ – коллинеация, то для каждой матрицы $\theta(V,U)$ из регулярного множества R плоскости π произведение $S^{-1}\theta(V,U)S$ также принадлежит R. Рассматривая $V = 0$ и произвольное $U \in K$, получим

$$S^{-1}\theta(0,U)S = \begin{pmatrix} E_2 & E_3 \\ E_1 & E_J^2 \end{pmatrix} \begin{pmatrix} m(U) & 0 \\ 0 & U \end{pmatrix} \begin{pmatrix} E_3 & E_1 \\ E_2 & E_J \end{pmatrix} =$$
$$= \begin{pmatrix} E_2 m(U) E_3 + E_3 U E_2 & E_2 m(U) E_1 + E_3 U E_J \\ E_1 m(U) E_3 + E_J^2 U E_2 & E_1 m(U) E_1 + E_J^2 U E_J \end{pmatrix} = \theta(\overline{V}, \overline{U})$$

для некоторых $\overline{V} \in Q$, $\overline{U} \in K$. Запишем матрицы $U \in K$ и $m(U)$ с учетом леммы 3.4.4:

$$U = \begin{pmatrix} \mu(U_2) & \varphi(V_2) \\ V_2 & U_2 \end{pmatrix}, \qquad m(U) = \begin{pmatrix} m_1(U_2) & m_2(V_2) \\ m_3(V_2) & m_4(U_2) \end{pmatrix}.$$

Тогда

$$\overline{U} = E_1 m(U) E_1 + E_J^2 U E_J =$$
$$= \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} m_1(U_2) & m_2(V_2) \\ m_3(V_2) & m_4(U_2) \end{pmatrix} \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & J^2 \end{pmatrix} \begin{pmatrix} \mu(U_2) & \varphi(V_2) \\ V_2 & U_2 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & J \end{pmatrix} =$$
$$= \begin{pmatrix} m_1(U_2) & 0 \\ 0 & J^2 U_2 J \end{pmatrix} \in K.$$

Отсюда $J^{-1}U_2J \in K_2$ для любого $U_2 \in K_2$, т. е. выполнено условие (2.2.3), поэтому матрица $\begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix}$ задает автотопизм полуполевой плоскости π_1 с регулярным множеством K_2. Лемма доказана. □

Лемма 3.4.6. *В условиях леммы 3.4.3 верно* $m_1(U_2) = \mu(J^{-1}U_2J)$, $m_4(U_2) = \mu(JU_2J^{-1})$ *для всех* $U_2 \in K_2$, $f_1(U_1) = m_3(JU_1)$, $f_4(U_1) = \varphi(JU_1)J$ *для всех* $U_1 \in K_1$, *причем* $K_1 = J^{-1}Q_2$.

Доказательство. Опираясь на доказательство леммы 3.4.5, рассмотрим $\theta(\overline{V}, \overline{U}) = S^{-1}\theta(0,U)S$. Так как

$$\overline{U} = \begin{pmatrix} \mu(J^{-1}U_2J) & 0 \\ 0 & J^{-1}U_2J \end{pmatrix},$$

то $m_1(U_2) = \mu(J^{-1}U_2J)$. Вычислим далее

$$m(\overline{U}) = E_2 m(U) E_3 + E_3 U E_2 = \begin{pmatrix} m_4(U_2) & 0 \\ 0 & \mu(U_2) \end{pmatrix} = \begin{pmatrix} m_1(J^{-1}U_2J) & m_2(0) \\ m_3(0) & m_4(J^{-1}U_2J) \end{pmatrix}.$$

Приравнивая блоки, получим для всех $U_2 \in K_2$ и $V_2 \in Q_2$

$$m_1(J^{-1}U_2J) = m_4(U_2), \qquad m_4(J^{-1}U_2J) = \mu(U_2).$$

Заключаем, что

$$m_4(U_2) = m_1(J^{-1}U_2J) = \mu(J^{-2}U_2J^2) = \mu(JU_2J^{-1}).$$

Запишем далее

$$\overline{V} = E_1 m(U) E_3 + E_J^2 U E_2 = \begin{pmatrix} m_2(V_2) & 0 \\ 0 & J^2V_2 \end{pmatrix},$$
$$f(\overline{V}) = E_2 m(U) E_1 + E_3 U E_J = \begin{pmatrix} m_3(V_2) & 0 \\ 0 & \varphi(V_2)J \end{pmatrix} = \begin{pmatrix} f_1(J^2V_2) & f_2(0) \\ f_3(0) & f_4(J^2V_2) \end{pmatrix}.$$

Так как $\overline{V} \in Q$, то $J^2V_2 \in K_1$ для всех $V_2 \in Q_2$, т.е. $K_1 = J^{-1}Q_2$. Так как Q содержит единичную матрицу, то множество Q_2 содержит матрицу J. Выполняя сравнение матриц V и $\overline{V}$, получим

$$\begin{pmatrix} \nu(J^{-1}V_2) & \psi(0) \\ 0 & J^{-1}V_2 \end{pmatrix} = \begin{pmatrix} m_2(V_2) & 0 \\ 0 & J^{-1}V_2 \end{pmatrix},$$

отсюда $m_2(V_2) = \nu(J^{-1}V_2)\ \forall V_2 \in Q_2$.

Записывая $f(\overline{V})$, имеем:

$$\begin{pmatrix} f_1(J^{-1}V_2) & f_2(0) \\ f_3(0) & f_4(J^{-1}V_2) \end{pmatrix} = \begin{pmatrix} m_3(V_2) & 0 \\ 0 & \varphi(V_2)J \end{pmatrix},$$

откуда делаем выводы: $f_1(U_1) = m_3(JU_1)$, $f_4(U_1) = \varphi(JU_1)J$ $(U_1 \in K_1)$. Лемма доказана. □

Учитывая полученный результат, заменим блоки $m_i(U_2)$ и $f_i(V_1)$ $(i = 1, 2, 3, 4)$ в формулировке леммы 3.4.4 и получим уточненный вид матрицы регулярного множества плоскости π:

$$\theta(V, U) = \begin{pmatrix} \mu(J^{-1}U_2J) & \nu(J^{-1}V_2) & m_3(JU_1) & f_2(V_1) \\ m_3(V_2) & \mu(JU_2J^{-1}) & f_3(V_1) & \varphi(JU_1)J \\ \nu(U_1) & \psi(V_1) & \mu(U_2) & \varphi(V_2) \\ V_1 & U_1 & V_2 & U_2 \end{pmatrix}.$$

Доказательство теоремы 3.4.2 завершает следующая лемма.

Лемма 3.4.7. *В условиях леммы 3.4.3 верны равенства* $Q_2 = J^{-1}Q_1$, $K_1 = JQ_1$, *причем для всех* $V_1 \in Q_1$, $U_1 \in K_1$ *и* $V_2 \in Q_2$

$$\begin{aligned} f_1(U_1) &= \psi(J^{-1}U_1), \\ f_2(V_1) &= \varphi(J^{-1}V_1)J^{-1}, \\ f_3(V_1) &= \nu(JV_1), \\ m_3(V_2) &= \psi(JV_2). \end{aligned}$$

Доказательство. Рассмотрим произвольный элемент $V \in Q$,

$$V = \begin{pmatrix} \nu(U_1) & \psi(V_1) \\ V_1 & U_1 \end{pmatrix},$$

и вычислим произведение $S^{-1}\theta(V,0)S$:

$$S^{-1}\theta(V,0)S = \begin{pmatrix} E_3VE_3 + E_2f(V)E_2 & E_3VE_1 + E_2f(V)E_J \\ E_J^2VE_3 + E_1f(V)E_2 & E_J^2VE_1 + E_1f(V)E_J \end{pmatrix} = \theta(\overline{V}, \overline{U}).$$

Здесь

$$\overline{U} = E_J^2VE_1 + E_1f(V)E_J = \begin{pmatrix} 0 & f_2(V_1)J \\ J^2V_1 & 0 \end{pmatrix} \in Q,$$

тогда $J^2V_1 \in Q_2$ и $\varphi(J^2V_1) = f_2(V_1)J$. В силу произвольности $V_1 \in Q_1$ имеем $Q_2 = J^{-1}Q_1$, $J \in Q_1$, $f_2(V_1) = \varphi(J^{-1}V_1)J^{-1}$.

Далее, $m(\overline{U}) = E_3VE_3 + E_2f(V)E_2$, отсюда

$$\begin{pmatrix} m_1(0) & m_2(J^2V_1) \\ m_3(J^2V_1) & m_4(0) \end{pmatrix} = \begin{pmatrix} 0 & f_3(V_1) \\ \psi(V_1) & 0 \end{pmatrix},$$

тогда $m_2(J^2V_1) = f_3(V_1)$ и $m_3(J^2V_1) = \psi(V_1)$, т.е. $m_3(V_2) = \psi(JV_2)$ для произвольного $V_2 \in Q_2$.

Рассмотрим $\overline{V} = E_J^2VE_3 + E_1f(V)E_2 \in Q$, получим равенство

$$\begin{pmatrix} 0 & f_1(U_1) \\ J^2U_1 & 0 \end{pmatrix} = \begin{pmatrix} \nu(0) & \psi(J^2U_1) \\ J^2U_1 & 0 \end{pmatrix},$$

тогда $J^2U_1 \in Q_1$, $J^{-1}K_1 = Q_1$, $f_1(U_1) = \psi(J^2U_1)$.

Для $f(\overline{V}) = E_3VE_1 + E_2f(V)E_J$ получаем

$$\begin{pmatrix} 0 & f_4(U_1)J \\ \nu(U_1) & 0 \end{pmatrix} = \begin{pmatrix} f_1(0) & f_2(J^2U_1) \\ f_3(J^2U_1) & f_4(0) \end{pmatrix}.$$

Приравнивая соответствующие элементы и используя ранее полученные равенства, получаем требуемый результат. □

Теорема 3.4.2 полностью доказана.

3.5. Подгруппа автотопизмов, изоморфная A_5

В предположении неразрешимости группы коллинеаций недезарговой полуполевой плоскости конечного порядка композиционные факторы должны быть изоморфны известным простым группам. Непосредственный перебор всех вариантов из списка простых неабелевых групп приводит к очень большому количеству исследований. Предлагается проверить существование подгруппы группы коллинеаций, изоморфной знакопеременной группе A_5 (подгруппе значительного количества простых неабелевых групп). Будем использовать матричное представление подгруппы автотопизмов, изоморфной A_4, и регулярного множества полуполевой плоскости нечетного порядка p^N.

В этом параграфе получено матричное представление регулярного множества полуполевой плоскости произвольного нечетного порядка p^N, допускающей группу автотопизмов, изоморфную знакопеременной группе A_5. На основе полученного матричного представления показано, что такая ситуация невозможна: группа автотопизмов недезарговой полуполевой плоскости нечетного порядка не может содержать подгруппы, изоморфной A_5.

Теорема 3.5.1. *Пусть π – полуполевая плоскость нечетного порядка p^N ($p > 2$, $p \neq 5$ – простое), группа автотопизмов Λ которой содержит подгруппу $H_0 \simeq A_5$. Тогда $N = 4n$ и плоскость π может быть задана $8n$-мерным векторным пространством над $\mathbb{Z}_p$ так, что регулярное множество плоскости $R \subset GL_{4n}(p) \cup \{0\}$ образовано $(4n \times 4n)$-матрицами вида*

$$\theta(V_1, U_1, V_2, U_2) = \begin{pmatrix} \mu(U_2) & -\psi(V_2) & \psi(U_1) & \varphi(V_1) \\ \psi(V_2) & \mu(U_2) & -\psi(V_1) & \varphi(U_1) \\ -\psi(U_1) & \psi(V_1) & \mu(U_2) & \varphi(V_2) \\ V_1 & U_1 & V_2 & U_2 \end{pmatrix}, \tag{3.5.1}$$

где $V_1, U_1, V_2 \in Q_1$, $U_2 \in Q_2$, Q_1, Q_2 – регулярные множества в $GL_n(p) \cup \{0\}$; ψ, μ, φ – инъективные линейные отображения из Q_1, Q_2 соответственно в $GL_n(p) \cup \{0\}$, причем $\mu(E) = E$, $\varphi(E) \neq E$, $\psi(E) = -E$.

Теорема 3.5.2. *Пусть π – недезаргова полуполевая плоскость нечетного порядка p^N ($p > 2$ – простое). Тогда ее группа автотопизмов Λ не может содержать подгруппу, изоморфную знакопеременной группе A_5.*

Для доказательства используем обозначения и результаты предыдущего параграфа. Считаем, что $H < \Lambda$ – подгруппа группы автотопизмов, изоморфная A_4 (3.4.3). Используя подстановочное представление подгруппы H и полагая

$$\tau \leftrightarrow (12)(34)(5), \quad \sigma \leftrightarrow (13)(24)(5), \quad \gamma \leftrightarrow (132)(4)(5),$$

рассмотрим подстановку $(125)(3)(4)$ и обозначим α соответствующий автотопизм. Тогда

$$|\alpha| = 3, \quad (\tau\alpha)^2 = \varepsilon, \quad \alpha\gamma^2 = \gamma\alpha^2, \quad |\alpha\sigma| = 5,$$

$H_0 = \langle \tau, \gamma, \alpha \rangle \simeq A_5$. Найдем матричное представление автотопизма α, основываясь на перечисленных условиях. Обозначим $\alpha = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}$ и выпишем сначала условия, которым удовлетворяет блок-матрица $D = \begin{pmatrix} D_1 & D_2 \\ D_3 & D_4 \end{pmatrix}$. Далее, для сокращения записи, будем использовать обозначения блоков матрицы γ:

$$\begin{pmatrix} 0 & 0 & E & 0 \\ E & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & 0 & J \end{pmatrix} = \begin{pmatrix} E_3 & E_1 \\ E_2 & J_4 \end{pmatrix}.$$

1. Рассмотрим равенства $(\tau\alpha)^2 = \varepsilon$ и $\alpha^3 = \varepsilon$, получим

$$\left(\begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix} \begin{pmatrix} D_1 & D_2 \\ D_3 & D_4 \end{pmatrix} \right)^2 = \begin{pmatrix} -D_1 & -D_2 \\ D_3 & D_4 \end{pmatrix}^2 = \begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix},$$

$$\begin{pmatrix} -D_1 & -D_2 \\ D_3 & D_4 \end{pmatrix} \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix} = \begin{pmatrix} D_1 & D_2 \\ D_3 & D_4 \end{pmatrix}^2.$$

Выполняя действия с матрицами, получаем систему уравнений

$$\begin{cases} D_1^2 + D_2D_3 = D_1, \\ D_1^2 - D_2D_3 = E, \\ D_1D_2 + D_2D_4 = -D_2, \\ D_1D_2 - D_2D_4 = 0, \\ D_3D_1 + D_4D_3 = -D_3, \\ -D_3D_1 + D_4D_3 = 0, \\ D_4^2 + D_3D_2 = D_4, \\ D_4^2 - D_3D_2 = E. \end{cases}$$

Перепишем систему, складывая и вычитая уравнения попарно:

$$\begin{cases} 2D_1^2 - D_1 - E = 0, \\ 2D_4^2 - D_4 - E = 0, \\ 2D_2D_3 = D_1 - E, \\ 2D_3D_2 = D_4 - E, \\ (2D_1 + E)D_2 = 0, \\ D_2(2D_4 + E) = 0, \\ (2D_4 + E)D_3 = 0, \\ D_3(2D_1 + E) = 0. \end{cases} \tag{3.5.2}$$

Очевидно, характеристические корни матриц D_1 и D_4 могут быть равны только 1 или $-\frac{1}{2}$, поэтому матрицы D_1 и D_4 – невырожденные.

Если матрица D_2 или матрица D_3 является невырожденной, то $D_1 = D_4 = -\frac{1}{2}E$. В этом случае $2D_2D_3 = -\frac{3}{2}E$ и $D_3 = -\frac{3}{4}D_2^{-1}$.

Пусть $|D_2| \neq 0$, $|D_3| \neq 0$, тогда

$$D = \begin{pmatrix} -\frac{1}{2}E & D_2 \\ -\frac{3}{4}D_2^{-1} & -\frac{1}{2}E \end{pmatrix}, \quad D^2 = D^{-1} = \begin{pmatrix} -\frac{1}{2}E & -D_2 \\ \frac{3}{4}D_2^{-1} & -\frac{1}{2}E \end{pmatrix}.$$

Рассмотрим условие $\alpha\gamma^2 = \gamma\alpha^2$, имеем для матрицы D равенство

$$\begin{pmatrix} -\frac{1}{2}E_2 + D_2E_1 & -\frac{1}{2}E_3 + D_2J_4^2 \\ -\frac{3}{4}D_2^{-1}E_2 - \frac{1}{2}E_1 & -\frac{3}{4}D_2^{-1}E_3 - \frac{1}{2}J_4^2 \end{pmatrix} = \begin{pmatrix} -\frac{1}{2}E_3 + \frac{3}{4}E_1D_2^{-1} & -E_3D_2 - \frac{1}{2}E_1 \\ -\frac{1}{2}E_2 + \frac{3}{4}J_4D_2^{-1} & -E_2D_2 - \frac{1}{2}J_4 \end{pmatrix},$$

приравняем элементы на месте 21: $-\frac{1}{2}E_3 + D_2J_4^2 = -E_3D_2 - \frac{1}{2}E_1$. В это равенство подставим $D_2 = \begin{pmatrix} D_{21} & D_{22} \\ D_{23} & D_{24} \end{pmatrix}$, тогда

$$\begin{pmatrix} 0 & D_{22}J^2 \\ -\frac{1}{2}E & D_{24}J^2 \end{pmatrix} = \begin{pmatrix} -\frac{1}{2}E & 0 \\ -D_{21} & -D_{22} \end{pmatrix},$$

что невозможно. Следовательно, $|D_2| = |D_3| = 0$.

Пусть $D_2 = 0$, тогда $D_1 = D_4 = E$ и $D_3 = 0$, тогда матрица D единичная и условие $\alpha\gamma^2 = \gamma\alpha^2$ не выполняется. При $D_3 = 0$ получаем аналогичный результат. Пусть $D_1 = -\frac{1}{2}E$ или $D_4 = -\frac{1}{2}E$, тогда $2D_2D_3 = -\frac{3}{2}E$ и матрицы D_2, D_3 невырожденные. Заметим, что тот же результат получается в случае произвольных скалярных матриц D_1, D_4; оформим рассуждения леммой.

Лемма 3.5.3. *D_1 и D_4 являются невырожденными нескалярными матрицами, D_2 и D_3 – вырожденными ненулевыми матрицами.*

2. Рассмотрим равенство $\alpha\gamma^2 = \gamma\alpha^2$:

$$\begin{pmatrix} D_1 & D_2 \\ D_3 & D_4 \end{pmatrix} \begin{pmatrix} E_2 & E_3 \\ E_1 & J_4^2 \end{pmatrix} = \begin{pmatrix} E_3 & E_1 \\ E_2 & J_4 \end{pmatrix} \begin{pmatrix} D_1 & -D_2 \\ -D_3 & D_4 \end{pmatrix},$$

$$\begin{cases} D_1E_2 + D_2E_1 = E_3D_1 - E_1D_3, \\ D_1E_3 + D_2J_4^2 = -E_3D_2 + E_1D_4, \\ D_3E_2 + D_1E_1 = E_2D_1 - J_4D_3, \\ D_3E_3 + D_4J_4^2 = -E_2D_2 + J_4D_4. \end{cases} \tag{3.5.3}$$

Каждый из блоков D_i $(i = 1, 2, 3, 4)$ заменим на $\begin{pmatrix} D_{i1} & D_{i2} \\ D_{i3} & D_{i4} \end{pmatrix}$, тогда система (3.5.3) преобразуется в 16 равенств

$$\begin{cases} D_{21} = -D_{31}, \\ D_{11} = -D_{32}, \\ D_{23} = D_{11}, \\ D_{13} = D_{12}; \end{cases} \quad \begin{cases} D_{12} = D_{41}, \\ D_{22}J^2 = D_{42}, \\ D_{14} = -D_{21}, \\ D_{24}J^2 = -D_{22}; \end{cases} \quad \begin{cases} D_{41} = D_{13}, \\ D_{31} = D_{14}, \\ D_{43} = -JD_{33}, \\ D_{33} = -JD_{34}; \end{cases} \quad \begin{cases} D_{32} = -D_{23}, \\ D_{42}J^2 = -D_{24}, \\ D_{34} = JD_{43}, \\ D_{44}J^2 = JD_{44}. \end{cases}$$

Учитывая эти равенства, запишем матрицу D в виде

$$D = \begin{pmatrix} D_{11} & D_{12} & -D_{14} & D_{22} \\ D_{12} & D_{14} & D_{11} & -D_{22}J \\ D_{14} & -D_{11} & D_{12} & D_{22}J^2 \\ D_{33} & -J^2D_{33} & -JD_{33} & D_{44} \end{pmatrix}, \tag{3.5.4}$$

при условии

$$JD_{44}J = D_{44}. \tag{3.5.5}$$

Лемма 3.5.4. *Матрица D (эквивалентно, A), определяющая автотопизм α, имеет вид (3.5.4), причем выполнены условия (3.5.2) и (3.5.5).*

Далее подставим блоки D_i $(i = 1, 2, 3, 4)$ в условия (3.5.2), получим при этом 32 новых матричных равенства, которые запишем в порядке, более удобном для дальнейших расчетов:

$$\begin{cases} 2D_{11}^2 + 2D_{12}^2 - D_{11} - E = 0, \\ 2D_{12}^2 + 2D_{14}^2 - D_{14} - E = 0, \\ 2D_{14}^2 + 2D_{11}^2 + D_{12} - E = 0, \\ 2D_{11}^2 - 2D_{22}D_{33} + D_{14} - E = 0, \\ 2D_{12}^2 - 2D_{22}D_{33} - D_{12} - E = 0, \\ 2D_{14}^2 - 2D_{22}D_{33} + D_{11} - E = 0; \end{cases} \tag{3.5.6}$$

$$\begin{cases} 2D_{11}D_{12} + 2D_{12}D_{14} - D_{12} = 0, \\ 2D_{12}D_{14} - 2D_{14}D_{11} - D_{11} = 0, \\ 2D_{14}D_{11} - 2D_{11}D_{12} + D_{14} = 0, \\ 2D_{11}D_{12} + 2D_{22}J^2D_{33} + D_{11} = 0, \\ 2D_{12}D_{14} + 2D_{22}J^2D_{33} + D_{14} = 0, \\ 2D_{14}D_{11} - 2D_{22}J^2D_{33} - D_{12} = 0; \end{cases} \tag{3.5.7}$$

$$\begin{cases} 2D_{12}D_{11} + 2D_{14}D_{12} - D_{12} = 0, \\ 2D_{14}D_{12} - 2D_{11}D_{14} - D_{11} = 0, \\ 2D_{11}D_{14} - 2D_{12}D_{11} + D_{14} = 0, \\ 2D_{12}D_{11} + 2D_{22}JD_{33} + D_{11} = 0, \\ 2D_{14}D_{12} + 2D_{22}JD_{33} + D_{14} = 0, \\ 2D_{11}D_{14} - 2D_{22}JD_{33} - D_{12} = 0; \end{cases} \tag{3.5.8}$$

$$\begin{cases} 2D_{33}D_{11} - 2D_{44}D_{33} - JD_{33} = 0, \\ 2D_{33}D_{12} + 2JD_{44}D_{33} - D_{33} = 0, \\ 2D_{33}D_{14} - 2J^2D_{44}D_{33} - J^2D_{33} = 0, \\ 2D_{33}D_{11} - 2J^2D_{33}D_{12} + D_{33} = 0, \\ 2D_{33}D_{12} - 2J^2D_{33}D_{14} - J^2D_{33} = 0, \\ 2D_{33}D_{14} + 2J^2D_{33}D_{11} - JD_{33} = 0; \end{cases} \tag{3.5.9}$$

$$\begin{cases} 2D_{11}D_{22} - 2D_{22}D_{44} - D_{22}J^2 = 0, \\ 2D_{12}D_{22} + 2D_{22}JD_{44} - D_{22} = 0, \\ 2D_{14}D_{22} - 2D_{22}D_{44}J - D_{22}J = 0, \\ 2D_{11}D_{22} - 2D_{12}D_{22}J + D_{22} = 0, \\ 2D_{12}D_{22} - 2D_{14}D_{22}J - D_{22}J = 0, \\ 2D_{14}D_{22} + 2D_{11}D_{22}J - D_{22}J^2 = 0; \end{cases} \tag{3.5.10}$$

$$\begin{cases} 2JD_{33}D_{22}J^2 - 2D_{44}^2 + D_{44} + E = 0, \\ 2D_{33}D_{22} + 2J^2D_{33}D_{22}J - D_{44} + E = 0. \end{cases} \tag{3.5.11}$$

Решив все системы поочередно относительно произведений и квадратов матриц D_{ij}, выпишем полученные соотношения.

$$\begin{cases} D_{11}^2 = \frac{1}{4}(D_{11} - D_{12} - D_{14} + E), \\ D_{12}^2 = \frac{1}{4}(D_{11} + D_{12} + D_{14} + E), \\ D_{14}^2 = \frac{1}{4}(-D_{11} - D_{12} + D_{14} + E), \\ D_{44}^2 = \frac{1}{4}D_{44}(E + J + J^2) + \frac{1}{4}E, \\ D_{22}D_{33} = \frac{1}{4}(D_{11} - D_{12} + D_{14} - E), \\ D_{33}D_{22} = \frac{1}{4}D_{44}(E + J - J^2) - \frac{1}{4}E, \\ D_{11}D_{12} = D_{12}D_{14} = \frac{1}{4}(-D_{11} + D_{12} + D_{14}), \\ D_{12}D_{14} = D_{14}D_{12} = \frac{1}{4}(D_{11} + D_{12} - D_{14}), \\ D_{14}D_{11} = D_{11}D_{14} = \frac{1}{4}(-D_{11} + D_{12} - D_{14}), \\ D_{22}JD_{33} = D_{22}J^2D_{33} = \frac{1}{4}(-D_{11} - D_{12} - D_{14}), \\ D_{33}D_{11} = D_{33}D_{14} = \frac{1}{4}(-E + J + J^2)D_{33}, \\ D_{33}D_{12} = \frac{1}{4}(E + J + J^2)D_{33}, \\ D_{44}D_{33} = \frac{1}{4}(-E - J + J^2)D_{33}, \\ D_{11}D_{22} = D_{14}D_{22} = \frac{1}{4}D_{22}(-E + J + J^2), \\ D_{12}D_{22} = \frac{1}{4}D_{22}(E + J + J^2), \\ D_{22}D_{44} = \frac{1}{4}D_{22}(-E + J - J^2). \end{cases} \tag{3.5.12}$$

3. Рассмотрим далее условие $|\alpha\sigma| = 5$ и возведем в пятую степень матрицу

$$\overline{D} = \begin{pmatrix} -D_{11} & D_{12} & D_{14} & D_{22} \\ -D_{12} & D_{14} & -D_{11} & -D_{22}J \\ -D_{14} & -D_{11} & -D_{12} & D_{22}J^2 \\ -D_{33} & -J^2D_{33} & JD_{33} & D_{44} \end{pmatrix}.$$

Получаемые при умножении матриц попарные произведения блоков D_{ij} заменяем при помощи равенств (7.2.3). Запишем

$$\overline{D}^2 = \begin{pmatrix} -D_{14} & D_{11} & -D_{12} & -D_{22}J^2 \\ -D_{11} & -D_{12} & D_{14} & -D_{22} \\ D_{12} & D_{14} & D_{11} & -D_{22}J \\ JD_{33} & -D_{33} & -J^2D_{33} & D_{44}J^2 \end{pmatrix}, \quad \overline{D}^3 = \begin{pmatrix} -D_{14} & -D_{11} & D_{12} & -D_{22}J^2 \\ D_{11} & -D_{12} & D_{14} & D_{22} \\ -D_{12} & D_{14} & D_{11} & D_{22}J \\ JD_{33} & D_{33} & J^2D_{33} & D_{44}J^2 \end{pmatrix},$$

$$\overline{D}^5 = \begin{pmatrix} E & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & E & 0 \\ 0 & 0 & 0 & D_{44} \end{pmatrix}.$$

Из $D_{44} = E$ и (3.5.5) имеем $J^2 = E = J^3$ и, следовательно, $J = E$. Преобразуем систему (7.2.3):

$$\begin{cases} D_{11}^2 = \frac{1}{4}(D_{11} - D_{12} - D_{14} + E), \\ D_{12}^2 = \frac{1}{4}(D_{11} + D_{12} + D_{14} + E), \\ D_{14}^2 = \frac{1}{4}(-D_{11} - D_{12} + D_{14} + E), \\ D_{22}D_{33} = \frac{1}{4}(D_{11} - D_{12} + D_{14} - E), \\ D_{33}D_{22} = 0, \\ D_{11}D_{12} = D_{12}D_{14} = \frac{1}{4}(-D_{11} + D_{12} + D_{14}), \\ D_{12}D_{14} = D_{14}D_{12} = \frac{1}{4}(D_{11} + D_{12} - D_{14}), \\ D_{14}D_{11} = D_{11}D_{14} = \frac{1}{4}(-D_{11} + D_{12} - D_{14}), \\ D_{22}D_{33} = \frac{1}{4}(-D_{11} - D_{12} - D_{14}), \\ D_{33}D_{11} = D_{33}D_{14} = \frac{1}{4}D_{33}, \\ D_{33}D_{12} = \frac{3}{4}D_{33}, \\ D_{33} = -\frac{1}{4}D_{33}, \\ D_{11}D_{22} = D_{14}D_{22} = \frac{1}{4}D_{22}, \\ D_{12}D_{22} = \frac{3}{4}D_{22}, \\ D_{22} = -\frac{1}{4}D_{22}. \end{cases} \tag{3.5.13}$$

Если характеристика поля $p \neq 5$, то $D_{22} = D_{33} = 0$. Тогда $D_{12} = -\frac{1}{2}E$, $D_{14} = -D_{11} + \frac{1}{2}E$, $D_{11}^2 - \frac{1}{2}D_{11} - \frac{1}{4}E = 0$. Таким образом, доказана

Лемма 3.5.5. *Если $p \neq 5$, то матрица D (эквивалентно, A), определяющая автотопизм α, имеет вид*

$$D = \begin{pmatrix} D_{11} & -\frac{1}{2}E & -D_{11} - \frac{1}{2}E & 0 \\ -\frac{1}{2}E & -D_{11} + \frac{1}{2}E & D_{11} & 0 \\ -D_{11} + \frac{1}{2}E & -D_{11} & -\frac{1}{2}E & 0 \\ 0 & 0 & 0 & E \end{pmatrix}, \tag{3.5.14}$$

при условии

$$D_{11}^2 - \frac{1}{2}D_{11} - \frac{1}{4}E = 0. \tag{3.5.15}$$

Случай $p = 5$ будет далее рассмотрен особо.

Выясним, какой вид имеют матрицы регулярного множества полуполевой плоскости при $p \neq 5$, допускающей подгруппу автотопизмов, изоморфную A_5. Используем полученный в теореме 3.4.2 вид (3.4.1) и добавим ограничения, следующие из того, что α является коллинеацией. Для любой матрицы $\theta(x)$ из регулярного множества произведение $A^{-1}\theta(x)D$ также должно принадлежать регулярному множеству. В частности, при $\theta(x) = E$ получим $A^{-1}D \in R$, где A

и D – матрицы вида (3.5.14). При умножении имеем

$$A^{-1}D = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ 0 & 0 & 0 & E \end{pmatrix} = E,$$

поэтому $A = D$. Далее, для сокращения обозначений, полагаем $D_{11} = Y$, $4Y^2 - 2Y - E = 0$, $\alpha = \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix}$,

$$D = \begin{pmatrix} Y & -\frac{1}{2}E & -Y - \frac{1}{2}E & 0 \\ -\frac{1}{2}E & -Y + \frac{1}{2}E & Y & 0 \\ -Y + \frac{1}{2}E & -Y & -\frac{1}{2}E & 0 \\ 0 & 0 & 0 & E \end{pmatrix}. \tag{3.5.16}$$

По теореме 3.4.2 при $J = E$ получим:

$$\theta(V_1, U_1, V_2, U_2) = \begin{pmatrix} \mu(U_2) & \nu(V_2) & \psi(U_1) & \varphi(V_1) \\ \psi(V_2) & \mu(U_2) & \nu(V_1) & \varphi(U_1) \\ \nu(U_1) & \psi(V_1) & \mu(U_2) & \varphi(V_2) \\ V_1 & U_1 & V_2 & U_2 \end{pmatrix}, \tag{3.5.17}$$

матрицы V_1, U_1, V_2 принадлежат одному множеству Q_1, $U_2 \in Q_2$,

$$\mu(E) = \nu(E) = E, \quad \varphi(E) \neq E, \quad \psi(E) \neq E.$$

Далее требуем выполнения условия $D^{-1}\theta(V_1, U_1, V_2, U_2)D \in R$ для всех $V_1, U_1, V_2 \in Q_1$, $U_2 \in Q_2$ и уточняем вид регулярного множества.

1. Пусть $V_1 = U_1 = V_2 = 0$, тогда

$$D^{-1}\theta(0,0,0,U_2)D = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ 0 & 0 & 0 & E \end{pmatrix} \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ 0 & 0 & 0 & U_2 \end{pmatrix} \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ 0 & 0 & 0 & E \end{pmatrix} =$$

$$= \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ 0 & 0 & 0 & U_2 \end{pmatrix} = \theta(0,0,0,U_2),$$

из $\theta(0,0,0,U_2)D = D\theta(0,0,0,U_2)$, следует

$$\mu(U_2)Y = Y\mu(U_2) \qquad \forall U_2 \in Q_2. \tag{3.5.18}$$

2. Пусть $V_1 = U_1 = U_2 = 0$, обозначим M матрицу $D^{-1}\theta(0,0,V_1,0)D = \theta(\overline{V_1}, \overline{U_2}, \overline{V_2}, \overline{U_2})$, где

$$\overline{V_1} = m_{41} = V_2\left(-Y + \tfrac{1}{2}E\right), \quad \overline{U_1} = m_{42} = -V_2Y,$$
$$\overline{V_2} = m_{43} = -\tfrac{1}{2}V_2, \qquad \overline{U_2} = m_{44} = 0.$$

Из условия $-V_2Y \in Q_1$ для произвольного $V_2 \in Q_1$ следует, что матрица $Y \in Q_1$ принадлежит правому ядру полуполя с регулярным множеством Q_1.

Далее, сравнивая элементы матрицы M с элементами матрицы регулярного множества R, получаем:

$$m_{11} = \mu(\overline{U_2}) \Rightarrow -\frac{1}{2}\psi(V_2)Y - \frac{1}{2}Y\nu(V_2) = 0 \Rightarrow \nu(V_2) = -Y^{-1}\psi(V_2)Y;$$

$$m_{13} = \psi(\overline{U_1}) \Rightarrow -\frac{1}{2}\psi(V_2)\left(Y - \frac{1}{2}E\right) + Y\nu(V_2)Y = \psi(-V_2Y) \Rightarrow \psi(V_2Y) = \psi(V_2)Y;$$

$$m_{14} = \varphi(\overline{V_1}) \Rightarrow \left(-Y + \frac{1}{2}E\right)\varphi(V_2) = \varphi\left(V_2\left(-Y + \frac{1}{2}E\right)\right) \Rightarrow \varphi(V_2Y) = Y\varphi(V_2);$$

$$m_{33} = \mu(\overline{U_2}) \Rightarrow Y\psi(V_2)\left(Y - \frac{1}{2}E\right) + \left(Y - \frac{1}{2}E\right)\nu(V_2)Y = 0 \Rightarrow$$
$$\psi(V_2)Y = Y\psi(V_2),\ \nu(V_2) = -\psi(V_2);$$

Рассматривая далее случаи $\theta(0, U_1, 0, 0)$ и $\theta(V_1, 0, 0, 0)$, мы не получим новых ограничений на функции μ, ν, φ, ψ и матрицу Y. Окончательно записываем матрицу $\theta(V_1, U_1, V_2, U_2)$ в виде (3.5.1) и, в дополнение к теореме 3.5.1 для случая $p \neq 5$, формулируем леммы о свойствах функций.

Лемма 3.5.6. *В условиях теоремы 3.5.1 матрица Y принадлежит правому ядру Q_1,*

$$\mu(U_2)Y = Y\mu(U_2) \quad \forall U_2 \in Q_2,$$
$$\psi(V_2)Y = Y\psi(V_2) = \psi(V_2Y) \quad \forall V_2 \in Q_1,$$
$$\varphi(V_2Y) = Y\varphi(V_2) \quad \forall V_2 \in Q_1.$$

Лемма 3.5.7. *Если регулярное множество полуполевой плоскости состоит из матриц вида (3.5.1), то $p-1$ не делится на 4 и $\varphi(E) \neq k^2E$ ($k \in \mathbb{Z}_p$).*

Доказательство. Действительно, рассмотрим матрицу вида (3.5.1) при $V_1 = U_1 = 0$, $V_2 = E$, $U_2 = kE$ ($k \in \mathbb{Z}_p$):

$$\theta(0,0,E,kE) = \begin{pmatrix} k\mu(E) & -\psi(E) & 0 & 0 \\ \psi(E) & k\mu(E) & 0 & 0 \\ 0 & 0 & k\mu(E) & \varphi(E) \\ 0 & 0 & E & kE \end{pmatrix} = \begin{pmatrix} kE & E & 0 & 0 \\ -E & kE & 0 & 0 \\ 0 & 0 & kE & \varphi(E) \\ 0 & 0 & E & kE \end{pmatrix}.$$

Определитель этой матрицы равен $\pm|(k^2+1)E| \cdot |\varphi(E) - k^2E|$, следовательно, -1 не является квадратом и $\varphi(E)$ не является квадратом скалярной матрицы. Далее, если $p-1$ делится на 4, то мультипликативная группа поля $\mathbb{Z}_p$ содержит элемент порядка 4, квадрат которого равен -1. Лемма доказана. $\square$

Теперь подробно рассмотрим случай $p = 5$. Вернемся к условиям (3.5.13) и перепишем их:

$$\begin{cases} D_{11}^2 = -D_{11} + D_{12} + D_{14} - E, \\ D_{12}^2 = -D_{11} - D_{12} - D_{14} - E, \\ D_{14}^2 = D_{11} + D_{12} - D_{14} - E, \\ D_{22}D_{33} = -D_{11} + D_{12} - D_{14} + E, \\ D_{33}D_{22} = 0, \\ D_{11}D_{12} = D_{12}D_{14} = D_{11} - D_{12} - D_{14}, \\ D_{12}D_{14} = D_{14}D_{12} = -D_{11} - D_{12} + D_{14}, \\ D_{14}D_{11} = D_{11}D_{14} = D_{11} - D_{12} + D_{14}, \\ D_{22}D_{33} = D_{11} + D_{12} + D_{14}, \\ D_{33}D_{11} = D_{33}D_{14} = -D_{33}, \\ D_{33}D_{12} = 2D_{33}, \\ D_{11}D_{22} = D_{14}D_{22} = -D_{22}, \\ D_{12}D_{22} = 2D_{22}. \end{cases} \tag{3.5.19}$$

Из 4-го и 9-го равенств получим $D_{14} = -D_{11} - 2E$. Подставляя это выражение в остальные равенства, имеем:

$$\begin{cases} (D_{11} + E)^2 = D_{12} - E, \\ (D_{12} - 2E)^2 = 0, \\ D_{22}D_{33} = D_{12} - 2E, \\ D_{33}D_{22} = 0, \\ (D_{11} + E)(D_{12} - 2E) = (D_{12} - 2E)(D_{11} + E) = 0, \\ D_{33}(D_{11} + E) = 0, \\ D_{33}(D_{12} - 2E) = 0, \\ (D_{11} + E)D_{22} = 0, \\ (D_{12} - 2E)D_{22} = 0. \end{cases} \tag{3.5.20}$$

Для упрощения записи в дальнейшем обозначим $D_{11}+E = X$, $D_{12}-2E = Y$, $D_{22} = Z$, $D_{33} = T$.

Лемма 3.5.8. *Если $p = 5$, то матрица D (эквивалентно, A), определяющая*

автотопизм α, *имеет вид*

$$D = \begin{pmatrix} X-E & Y+2E & X+E & Z \\ Y+2E & -X-E & X-E & -Z \\ -X-E & -X+E & Y+2E & Z \\ T & -T & -T & E \end{pmatrix}, \tag{3.5.21}$$

где выполнены условия на блоки:

$$\begin{cases} X^2 = Y, \\ Y^2 = 0, \\ ZT = Y, \\ TZ = 0, \\ XY = YX = 0, \\ TX = TY = 0, \\ XZ = YZ = 0. \end{cases} \tag{3.5.22}$$

Заметим, что в общем случае матрицы A и D различны, что усложняет расчеты. Для дальнейшего уточнения вида матриц докажем вспомогательную лемму.

Лемма 3.5.9. *Пусть* R *– регулярное множество в* $GL_n(p) \cup \{0\}$, T *и* Z *–* $(n \times n)$*-матрицы над* $\mathbb{Z}_p$. *Если для всех матриц* $U \in R$ *верно* $TUZ = 0$, *то* $T = 0$ *либо* $Z = 0$.

Доказательство. Предположим, что $T \neq 0$ и $Z \neq 0$. Пусть T содержит ненулевую строку $t = (t_{i1}, \ldots, t_{in})$, Z содержит ненулевой столбец $z = \begin{pmatrix} z_{1j} \\ \vdots \\ z_{nj} \end{pmatrix}$. Тогда все элементы множества $M = \{tU \mid U \in R\}$ различны. Действительно, пусть $tU_1 = tU_2$ для некоторых $U_1, U_2 \in R$, $U_1 \neq U_2$. Тогда $t(U_1 - U_2) = 0$, $\det(U_1 - U_2) \neq 0$ и $t = 0$, что противоречит предположению.

Рассмотрим линейное уравнение $z_{1j}x_1 + z_{2j}x_2 + \cdots + z_{nj}x_n = 0$. Его решения образуют $(n-1)$-мерное линейное подпространство в $\mathbb{Z}_p^n$, но из условия $TUZ = 0$ следует, что все p^n элементов множества M являются решениями этого уравнения. Полученное противоречие доказывает лемму. □

Лемма 3.5.10. *Пусть полуполевая плоскость порядка* 5^{4n} *допускает автотопизм* $\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}$ *с* A *и* D *вида (3.5.21). Тогда* $X_A = Y_A = X_D = Y_D = 0$.

Доказательство. Запишем матрицы A и D:

$$A = \begin{pmatrix} X_A - E & Y_A + 2E & X_A + E & Z_A \\ Y_A + 2E & -X_A - E & X_A - E & -Z_A \\ -X_A - E & -X_A + E & Y_A + 2E & Z_A \\ T_A & -T_A & -T_A & E \end{pmatrix},$$

$$D = \begin{pmatrix} X_D - E & Y_D + 2E & X_D + E & Z_D \\ Y_D + 2E & -X_D - E & X_D - E & -Z_D \\ -X_D - E & -X_D + E & Y_D + 2E & Z_D \\ T_D & -T_D & -T_D & E \end{pmatrix},$$

предполагая, что матрицы $X_A, Y_A, Z_A, T_A, X_D, Y_D, Z_D, T_D$ удовлетворяют условиям (3.5.22).

Так как α – автотопизм, то для всех матриц $\theta(V_1, U_1, V_2, U_2)$ регулярного множества произведение $A^{-1}\theta(V_1, U_1, V_2, U_2)D$ также принадлежит регулярному множеству. Рассмотрим матрицу $C = A^{-1}\theta(0, 0, 0, U_2)D$ и выпишем ее элементы:

$$\begin{cases} C_{11} = (X_A - E)\mu(U_2)(X_D - E) + (Y_A + 2E)\mu(U_2)(Y_D + 2E) + \\ \qquad + (-X_A - E)\mu(U_2)(-X_D - E) - Z_A U_2 T_D, \\ C_{12} = (X_A - E)\mu(U_2)(Y_D + 2E) + (Y_A + 2E)\mu(U_2)(-X_D - E) + \\ \qquad + (-X_A - E)\mu(U_2)(-X_D + E) - Z_A U_2 T_D, \\ C_{13} = (X_A - E)\mu(U_2)(X_D + E) + (Y_A + 2E)\mu(U_2)(X_D - E) + \\ \qquad + (-X_A - E)\mu(U_2)(Y_D + 2E) + Z_A U_2 T_D, \\ C_{14} = (X_A - E)\mu(U_2)Z_D - (Y_A + 2E)\mu(U_2)Z_D + (-X_A - E)\mu(U_2)Z_D - Z_A U_2; \end{cases}$$

$$\begin{cases} C_{21} = (Y_A + 2E)\mu(U_2)(X_D - E) + (-X_A - E)\mu(U_2)(Y_D + 2E) + \\ \qquad + (-X_A + E)\mu(U_2)(-X_D - E) + Z_A U_2 T_D, \\ C_{22} = (Y_A + 2E)\mu(U_2)(Y_D + 2E) + (-X_A - E)\mu(U_2)(-X_D - E) + \\ \qquad + (-X_A + E)\mu(U_2)(-X_D + E) - Z_A U_2 T_D, \\ C_{23} = (Y_A + 2E)\mu(U_2)(X_D + E) + (-X_A - E)\mu(U_2)(X_D - E) + \\ \qquad + (-X_A + E)\mu(U_2)(Y_D + 2E) - Z_A U_2 T_D, \\ C_{24} = (Y_A + 2E)\mu(U_2)Z_D - (-X_A - E)\mu(U_2)Z_D + (-X_A + E)\mu(U_2)Z_D + Z_A U_2; \end{cases}$$

$$\begin{cases} C_{31} = (X_A + E)\mu(U_2)(X_D - E) + (X_A - E)\mu(U_2)(Y_D + 2E) + \\ \qquad + (Y_A + 2E)\mu(U_2)(-X_D - E) + Z_A U_2 T_D, \\ C_{32} = (X_A + E)\mu(U_2)(Y_D + 2E) + (X_A - E)\mu(U_2)(-X_D - E) + \\ \qquad + (Y_A + 2E)\mu(U_2)(-X_D + E) - Z_A U_2 T_D, \\ C_{33} = (X_A + E)\mu(U_2)(X_D + E) + (X_A - E)\mu(U_2)(X_D - E) + \\ \qquad + (Y_A + 2E)\mu(U_2)(Y_D + 2E) - Z_A U_2 T_D, \\ C_{34} = (X_A + E)\mu(U_2)Z_D - (X_A - E)\mu(U_2)Z_D + (Y_A + 2E)\mu(U_2)Z_D + Z_A U_2; \end{cases}$$

$$\begin{cases} C_{41} = -T_A\mu(U_2)(X_D - E) + T_A\mu(U_2)(Y_D + 2E) + T_A\mu(U_2)(X_D + E) + U_2 T_D, \\ C_{42} = -T_A\mu(U_2)(Y_D + 2E) - T_A\mu(U_2)(X_D + E) - T_A\mu(U_2)(-X_D + E) - U_2 T_D, \\ C_{43} = -T_A\mu(U_2)(X_D + E) + T_A\mu(U_2)(X_D - E) - T_A\mu(U_2)(Y_D + 2E) - U_2 T_D, \\ C_{44} = -3T_A\mu(U_2)Z_D + U_2. \end{cases}$$

Здесь $C_{44} \in Q_2$, поэтому $C_{44} - U_2 \in Q_2$ и $T_A\mu(U_2)Z_D \in Q_2$ для всех $U_2 \in Q_2$.

Если $|T_A| \neq 0$, то из условий (3.5.22) имеем $X_A = Y_A = Z_A = 0$. Если $|Z_D| \neq 0$, то из условий (3.5.22) имеем $X_D = Y_D = T_D = 0$.

Пусть $|T_A| = |Z_D| = 0$, тогда $T_A\mu(U_2)Z_D = 0$ для всех $U_2 \in Q_2$. Так как $\{\mu(U_2) \mid U_2 \in Q_2\}$ – регулярное множество, то по лемме 3.5.9 $T_A = 0$ или $Z_D = 0$.

Пусть $T_A = 0$, тогда $C_{41} = U_2 T_D$. Если $|T_D| \neq 0$, то $X_D = Y_D = 0$. При $|T_D| = 0$ получаем $U_2 T_D = 0$, $T_D = 0$. Тогда $A^{-1}\theta(0,0,0,U_2)D = \theta(0,0,0,U_2)$ для всех $U_2 \in Q_2$. При $U_2 = E$ получим $A = D$, $X_A = X_D$, тогда для всех $U_2 \in Q_2$ верно $\mu(U_2)X_A = X_A\mu(U_2)$. Умножим это равенство слева на X_A:

$$X_A\mu(U_2)X_A = X_A^2\mu(U_2).$$

Если $X_A^2 = 0$, то по лемме 3.5.9 имеем $X_A = 0$. Если $X_A^2 \neq 0$, то при повторном умножении получим

$$X_A^2\mu(U_2)X_A = X_A^3\mu(U_2) = 0$$

и $X_A^2 = 0$ либо $X_A = 0$, противоречие. Итак, при $T_A = 0$ получили $X_A = X_D = 0$.

Пусть $Z_D = 0$, тогда $C_{14} = -Z_A U_2 = \varphi(C_{41})$. Если $|Z_A| \neq 0$, то $X_A = Y_A = 0$. При $|Z_A| = 0$ получаем $Z_A U_2 = 0$ и, следовательно, $Z_A = 0$, $C_{41} = 0$. Аналогично $C_{42} = C_{43} = 0$, тогда $A^{-1}\theta(0,0,0,U_2)D = \theta(0,0,0,U_2)$ и, как в предыдущем случае, $X_A = X_D = 0$.

Таким образом, более подробного рассмотрения требуют случаи:

1) $|T_A| \neq 0$, $X_A = Y_A = Z_A = 0$;
2) $|Z_A| \neq 0$, $X_A = Y_A = Z_A = 0$;
3) $|T_D| \neq 0$, $X_D = Y_D = Z_D = 0$;
4) $|Z_D| \neq 0$, $X_D = Y_D = Z_D = 0$.

Рассуждения во всех четырех случаях аналогичные. Например, в первом случае вычислим произведение $A^{-1}D = C$ и получим $C_{11} = 2Y_D + E$. Так как $Y_D^2 = 0$ и $Y_D = \mu(U)$ для некоторого $U \in Q_2$, то $Y_D = 0$. Тогда $C_{12} = -X_D$ и, в силу вырожденности, $X_D = 0$. Проводя вычисления для случаев 2-4, приходим к окончательному выводу $X_A = X_D = 0$, что доказывает лемму. □

Лемма 3.5.11. *Пусть полуполевая плоскость порядка 5^{4n} допускает автотопизм $\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}$, где A и D имеют вид (3.5.21). Тогда матрица регулярного множества плоскости имеет вид (3.5.1).*

Доказательство. Вычислим произведение $A^{-1}D$ при $X_A = Y_A = X_D = Y_D = 0$, Тогда произведение $A^{-1}D = A^2D$ является элементом регулярного множества,

$$A^{-1}D = \begin{pmatrix} E - Z_AT_D & Z_AT_D & Z_AT_D & Z_D - Z_A \\ Z_AT_D & E - Z_AT_D & -Z_AT_D & -Z_D + Z_A \\ Z_AT_D & -Z_AT_D & E - Z_AT_D & -Z_D + Z_A \\ -T_A + T_D & T_A - T_D & T_A - T_D & -3T_AZ_D + E \end{pmatrix}.$$

Так как $A^{-1}D$ и E принадлежат регулярному множеству, то из вырожденности матриц Z_AT_D и T_AZ_D вытекает равенство их нулю, тогда

$$A^{-1}D - E = \begin{pmatrix} 0 & 0 & 0 & Z_D - Z_A \\ 0 & 0 & 0 & -Z_D + Z_A \\ 0 & 0 & 0 & -Z_D + Z_A \\ -T_A + T_D & T_A - T_D & T_A - T_D & 0 \end{pmatrix}$$

– нулевая матрица и $Z_A = Z_D$, $T_A = T_D$, $A = D$.

Продолжим рассмотрение этого случая и получим ограничения на матрицы регулярного множества, используя условие $D^2\theta(V_1, U_1, V_2, U_2)D \in R$ для всех возможных V_1, U_1, V_2, U_2. В частности, для $V_1 = U_1 = U_2 = 0$ обозначим произведение $D^2\theta(0, 0, V_2, 0)D = C$ и выпишем блоки-подматрицы C_{ij}:

$$\begin{cases} C_{11} = -2\psi(V_2) - 2\nu(V_2) + ZV_2 - \varphi(V_2)T, \\ C_{21} = \psi(V_2) - \nu(V_2) - ZV_2 + \varphi(V_2)T, \\ C_{31} = \psi(V_2) + 2\nu(V_2) - ZV_2 + 2\varphi(V_2)T, \\ C_{41} = -T\psi(V_2) - 2T\nu(V_2) - V_2 - T\varphi(V_2)T; \end{cases}$$

$$\begin{cases} C_{12} = -\psi(V_2) + \nu(V_2) - ZV_2 + \varphi(V_2)T, \\ C_{22} = -2\psi(V_2) - 2\nu(V_2) + ZV_2 - \varphi(V_2)T, \\ C_{32} = -2\psi(V_2) - \nu(V_2) + ZV_2 - 2\varphi(V_2)T, \\ C_{42} = 2T\psi(V_2) + T\nu(V_2) + V_2 + T\varphi(V_2)T; \end{cases}$$

$$\begin{cases} C_{13} = 2\psi(V_2) + \nu(V_2) - 2ZV_2 + \varphi(V_2)T, \\ C_{23} = -\psi(V_2) - 2\nu(V_2) + 2ZV_2 - \varphi(V_2)T, \\ C_{33} = -\psi(V_2) - \nu(V_2) + 2ZV_2 - 2\varphi(V_2)T, \\ C_{43} = T\psi(V_2) + T\nu(V_2) + 2V_2 + T\varphi(V_2)T; \end{cases}$$

$$\begin{cases} C_{14} = 2\psi(V_2)Z + \nu(V_2)Z - ZV_2Z - \varphi(V_2), \\ C_{24} = -\psi(V_2)Z - 2\nu(V_2)Z + ZV_2Z + \varphi(V_2), \\ C_{34} = -\psi(V_2)Z - \nu(V_2)Z + ZV_2Z + 2\varphi(V_2), \\ C_{44} = T\varphi(V_2)Z + T\nu(V_2)Z + V_2Z - T\varphi(V_2). \end{cases}$$

Вычтем из полученной матрицы $\theta(-V_2, V_2, 2V_2, 0)$ и увидим в 4-ой строке вырожденные матрицы, которые, следовательно, являются нулевыми:

$$\begin{cases} C_{41} + V_2 = -T\psi(V_2) - 2T\nu(V_2) - T\varphi(V_2)T = 0, \\ C_{42} - V_2 = 2T\psi(V_2) + T\nu(V_2) + T\varphi(V_2)T = 0, \\ C_{43} - 2V_2 = T\psi(V_2) + T\nu(V_2) + T\varphi(V_2)T = 0. \end{cases}$$

Из полученной системы $T\nu(V_2) = T\psi(V_2) = 0$ для всех V_2, поэтому $T = 0$. Тогда $C_{44} = V_2Z$ – вырожденная матрица, $Z = 0$. Подставляя $T = Z = 0$ в матрицу C, получим

$$\begin{pmatrix} -2\psi(V_2) - 2\nu(V_2) & -\psi(V_2) + \nu(V_2) & 2\psi(V_2) + \nu(V_2) & -\varphi(V_2) \\ \psi(V_2) - \nu(V_2) & -2\psi(V_2) - 2\nu(V_2) & -\psi(V_2) - 2\nu(V_2) & \varphi(V_2) \\ \psi(V_2) + 2\nu(V_2) & -2\psi(V_2) - \nu(V_2) & -\psi(V_2) - \nu(V_2) & 2\varphi(V_2) \\ -V_2 & V_2 & 2V_2 & 0 \end{pmatrix}.$$

В силу равенства C матрице $\theta(-V_2, V_2, 2V_2, 0)$ получаем $\nu(V_2) = -\psi(V_2)$, что приводит к регулярному множеству вида (3.5.1). Лемма доказана. □

Так как в поле $\mathbb{Z}_5$ элемент -1 является квадратом, делаем заключение о невозможности рассмотренного случая: не существует полуполевых плоскостей порядка 5^{4n}, допускающих подгруппу автотопизмов, изоморфную знакопеременной группе A_5. Теорема 3.5.1 полностью доказана. Прежде чем завершить доказательство теоремы 3.5.2, укажем, что в докладе [182] представлен результат: если недезаргова полуполевая плоскость имеет порядок p^4 или p^8, то регулярное множество (3.5.1) также содержит ненулевую вырожденную матрицу, поэтому плоскость такого порядка не может допускать A_5 в группе автотопизмов. Этот результат упоминается здесь без доказательства как частный случай теоремы 3.5.2.

Доказательство теоремы 3.5.2. В обозначениях теоремы 3.5.1, пусть $\varphi(E) = P$. В силу линейности отображений μ, φ, ψ, для любого $t \in \mathbb{Z}_p$ имеем $\mu(tE) = tE$,

$\psi(tE) = -tE$, $\varphi(tE) = tP$. Рассмотрим матрицу $\theta(xE, yE, E, 0)$ $(x, y \in \mathbb{Z}_p)$:

$$\begin{pmatrix} 0 & E & -yE & xP \\ -E & 0 & xE & yP \\ yE & -xE & 0 & P \\ xE & yE & E & 0 \end{pmatrix},$$

прибавим к ее третьей «строке» вторую «строку», умноженную на y:

$$\begin{pmatrix} 0 & E & -yE & xP \\ -E & 0 & xE & yP \\ 0 & -xE & xyE & (1+y^2)P \\ xE & yE & E & 0 \end{pmatrix},$$

теперь прибавим к третьей «строке» первую «строку», умноженную на x:

$$\begin{pmatrix} 0 & E & -yE & xP \\ -E & 0 & xE & yP \\ 0 & 0 & 0 & (1+x^2+y^2)P \\ xE & yE & E & 0 \end{pmatrix}.$$

Известно [68], что каждый элемент конечного поля представим в виде суммы двух квадратов, поэтому найдутся такие $x, y \in \mathbb{Z}_p$, что $x^2 + y^2 = -1$, тогда матрица $\theta(xE, yE, E, 0)$ вырожденная. Теорема 3.5.2 доказана.

Подводя итог, обратим внимание, что вместе со знакопеременной группой A_5 в группе автотопизмов полуполевой плоскости произвольного нечетного порядка исключаются и все другие конечные группы, содержащие A_5 в качестве подгруппы.

Следствие 3.5.12. *Недезаргова полуполевая плоскость нечетного порядка не может содержать в группе автотопизмов подгруппы, изоморфной A_n или S_n для $n \geq 5$.*

Кроме того, учитывая строение трансляционного дополнения недезарговой полуполевой плоскости и ее группы коллинеаций, укажем другое очевидное следствие.

Следствие 3.5.13. *Группа коллинеаций недезарговой полуполевой плоскости нечетного порядка не может содержать подгруппы, изоморфной A_n или S_n для $n \geq 5$.*

Перечислим некоторые известные группы, которые содержат A_5 в качестве подгруппы и поэтому также не могут быть подгруппами группы автотопизмов полуполевой плоскости нечетного порядка (ATLAS, [27]):

1) линейные группы $L_2(p)$ при $p \equiv \pm 1 (\mathrm{mod}\, 10)$, $L_3(4)$, $L_3(5)$, ...;

2) симплектические группы $S_4(4)$, $S_4(5)$, $S_6(2)$, $S_6(3)$, ...;

3) унитарные группы $U_3(4)$, $U_3(4):2$, $U_3(4):4$, $U_3(5)$, $U_3(5):2$, $U_3(5):3$, $U_3(5):S_3$, $U_5(2)$, $U_5(2):2$, $U_6(2)$, $U_6(2):2$, $U_6(2):3$, $U_6(2):S_3$, $U_7(2)$, ...;

4) ортогональные группы $O_8^-(2)$, $O_8^-(2):2$, $O_{10}^-(2)$, $O_{10}^-(2):2$, ...;

5) исключительные группы лиева типа $G_2(4)$, $G_2(4):2$, ...

3.6. Подгруппа автотопизмов, изоморфная D_8

Применяя результаты параграфов 3.2 и 3.3 к полуполевым плоскостям нечетного порядка, получим следующий основной результат.

Теорема 3.6.1. *Недезаргова полуполевая плоскость π порядка p^N, где $p > 2$ – простое, $p \equiv 1 \pmod 4$, не допускает подгруппы автотопизмов, изоморфной диэдральной группе порядка 8 и не содержащей гомологий.*

Доказательство. Пусть Λ – группа автотопизмов плоскости π, $H \simeq D_8$ – ее подгруппа, $H = \langle\alpha\rangle \leftthreetimes \langle\sigma\rangle$, $|\alpha| = 4$, $|\sigma| = 2$, $\sigma\alpha\sigma = \alpha^{-1}$. Так как $\alpha^2 = \tau$ – бэровская инволюция, то, по теореме 3.3.9, базис $2N$-мерного пространства можно выбрать так, что τ имеет вид (3.1.3), α определяется матрицей (3.3.2), регулярное множество R состоит из матриц вида (3.3.3). Отметим, что α определяется с точностью до умножения на инволютивные гомологии, лежащие в центре группы автотопизмов, мы их можем не учитывать.

Далее, σ – бэровская инволюция, коммутирующая с τ, поэтому

$$\sigma = \begin{pmatrix} A_1 & 0 & 0 & 0 \\ 0 & A_2 & 0 & 0 \\ 0 & 0 & B_1 & 0 \\ 0 & 0 & 0 & B_2 \end{pmatrix}, \quad A_1^2 = A_2^2 = B_1^2 = B_2^2 = E.$$

По лемме 3.2.2, σ действует на бэровской подплоскости π_τ как бэровская инволюция, поэтому $A_2 \neq \pm E$, $B_2 \neq \pm E$. Рассмотрим условие $\sigma\alpha\sigma = \alpha^{-1}$, из него получим

$$A_1 L A_1 = B_1 L B_1 = -L, \qquad A_2 L A_2 = B_2 L B_2 = L,$$

$$A_1 = \begin{pmatrix} 0 & A_{11} \\ A_{12} & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} A_{21} & 0 \\ 0 & A_{22} \end{pmatrix}, \quad B_1 = \begin{pmatrix} 0 & B_{11} \\ B_{12} & 0 \end{pmatrix}, \quad B_2 = \begin{pmatrix} B_{21} & 0 \\ 0 & B_{22} \end{pmatrix}.$$

Так как ограничения α и σ на бэровскую подплоскость π_τ – это коммутирующие бэровские инволюции, то, с учетом леммы 3.2.2, базис π_τ можно выбрать так,

что $A_{21} = A_{22} = B_{21} = B_{22} = L$, тогда

$$\sigma = \begin{pmatrix} 0 & S & 0 & 0 & 0 & 0 & 0 & 0 \\ S^{-1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & L & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & L & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & S & 0 & 0 \\ 0 & 0 & 0 & 0 & S^{-1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & L & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & L \end{pmatrix}.$$

Здесь, для сокращения записи, $S = A_{11}$, тогда из $A_1^2 = E$ имеем $A_{12} = S^{-1}$. Равенство $B_1 = A_1$ получается из условия (2.2.3) для σ и $\theta(V, U) = E \in R$:

$$\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix} = \begin{pmatrix} A_1 B_1 & 0 \\ 0 & E \end{pmatrix} \in R \Rightarrow A_1 B_1 = E.$$

Применим замену базиса с блочно-диагональной матрицей перехода

$$T = \operatorname{diag}(E, S, E, E, E, S, E, E).$$

Эта замена сохраняет вид матриц τ и α, приводя σ к более удобному виду:

$$\sigma = \begin{pmatrix} 0 & E & 0 & 0 & 0 & 0 & 0 & 0 \\ E & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & L & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & L & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & E & 0 & 0 \\ 0 & 0 & 0 & 0 & E & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & L & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & L \end{pmatrix}.$$

Рассмотрим условие (2.2.3) для бэровской инволюции σ при $V_2 = U_2 = 0$:

$$\begin{pmatrix} 0 & E & 0 & 0 \\ E & 0 & 0 & 0 \\ 0 & 0 & L & 0 \\ 0 & 0 & 0 & L \end{pmatrix} \begin{pmatrix} 0 & 0 & f_1(V_1) & f_2(U_1) \\ 0 & 0 & f_3(U_1) & f_4(V_1) \\ \nu(U_1) & \psi(V_1) & 0 & 0 \\ V_1 & U_1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & E & 0 & 0 \\ E & 0 & 0 & 0 \\ 0 & 0 & L & 0 \\ 0 & 0 & 0 & L \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 & f_3(U_1)L & f_4(V_1)L \\ 0 & 0 & f_1(V_1)L & f_2(U_1)L \\ L\psi(V_1) & L\nu(U_1) & 0 & 0 \\ LU_1 & LV_1 & 0 & 0 \end{pmatrix} \in R.$$

Таким образом, матрицы LU_1 и LV_1 должны принадлежать регулярным множествам Q_1 и K_1 для всех $V_1 \in Q_1$, $U_1 \in K_1$. В частности, при $V_1 = E$ получаем $L \in K_1$. В силу замкнутости K_1 по сложению вырожденная ненулевая матрица $L + E$ также принадлежит K_1, что невозможно. Полученное противоречие показывает невозможность существования в группе автотопизмов подгруппы без гомологий, изоморфной диэдральной группе порядка 8. Теорема доказана. □

Замечание 3.6.2. *Так как мы изучаем вопрос существования в группе автотопизмов недезарговой полуполевой плоскости простых неабелевых групп (в том числе минимальных, по списку Томпсона), то условие отсутствия в подгруппе гомологий является естественным. Действительно, гомологии образуют нормальные подгруппы в группе автотопизмов, а инволютивные гомологии, более того, лежат в центре.*

Пусть G – подгруппа в группе автотопизмов Λ и S – силовская 2-подгруппа в G. Если две инволюции в S не коммутируют, то они порождают в S диэдральную подгруппу. Далее, используя результаты Д. Голдшмидта [54] о сильно замкнутых подгруппах (см. также Д. Горенстейн [55, th. 4.128]), заключаем, что D_8 содержится почти по всех конечных простых неабелевых группах и перечисляем исключения.

Теорема 3.6.3. *Пусть π – недезаргова полуполевая плоскость порядка p^N, где $p > 2$ – простое, $p \equiv 1 \pmod 4$ Тогда ее группа автотопизмов Λ не содержит простых неабелевых подгрупп, за исключением, возможно, следующих: $PSL(2, 2^n)$, $n \geq 2$, $PSU(3, 2^n)$, $n \geq 2$, $Sz(2^n)$, n нечетно, $n > 1$, $PSL(2, q)$, $q \equiv \pm 3 \pmod 8$, J_1 или ${}^2G_2(3^n)$, n нечетно, $n > 1$.*

Обращаясь к списку Д.Г. Томпсона минимальных простых неабелевых групп, уточняем также, что группа автотопизмов Λ при указанном условии на порядок плоскости не содержит $PSL(2, 3^n)$, n нечетное простое, $PSL(2, n)$, $n \equiv \pm 1 \pmod 8$ – простое, $PSL(3, 3)$.

3.7. Подгруппа автотопизмов, изоморфная Q_8

По основной теореме 3.5.2 предыдущего параграфа, недезаргова полуполевая плоскость нечетного порядка не может допускать подгруппы автотопизмов, изоморфной знакопеременной группе A_5. Рассмотрим ситуацию, когда группа автотопизмов Λ содержит подгруппу, фактор-группа по которой изоморфна A_5. Учитывая $PSL(2, 5) \simeq A_5$, будем изучать возможность вложения $SL(2, 5) < \Lambda$. Силовская 2-подгруппа в $SL(2, 5)$ изоморфна группе кватернионов Q_8.

Поставим задачу: для недезарговой полуполевой плоскости нечетного порядка p^N найти матричное представление регулярного множества $R \subset GL_N(p) \cup \{0\}$, предполагая, что группа автотопизмов Λ содержит подгруппу $H \simeq Q_8$. Задача решена при условии $4|p-1$.

Отметим, что для плоскостей трансляций, в отличие от полуполевых, опубликован ряд результатов ([93, 28, 50, 71, 98] и др.) о существовании $SL(2,q)$ в группе коллинеаций. Они связаны, главным образом, с плоскостями ограниченного порядка n (например, $n \leq q$, $n = q^2$, $n = q^3$) и неприменимы в изучаемой нами ситуации.

Основным результатом параграфа является следующая теорема.

Теорема 3.7.1. *Пусть π – недезаргова полуполевая плоскость π порядка p^N, допускающая подгруппу автотопизмов H, изоморфную группе кватернионов Q_8, $p > 2$ – простое, $p \equiv 1 \pmod 4$. Тогда $N = 2n \geq 4$, элемент порядка 2 в H является гомологией с осью $[\infty]$ и центром $(0,0)$. Базис линейного пространства над $\mathbb{Z}_p$ может быть выбран так, что регулярное множество $R \subset GL_{2n}(p) \cup \{0\}$ плоскости π состоит из матриц вида (3.1.6)*

$$\theta(V,U) = \begin{pmatrix} m(U) & f(V) \\ V & U \end{pmatrix},$$

где $V \in Q$, $U \in K$, множества $Q, K \subset GL_n(p) \cup \{0\}$ замкнуты по сложению, содержат нулевую и единичную матрицы. Аддитивные взаимно однозначные отображения $m : K \to K$ и $f : Q \to Q$ не тождественны, инволютивны и удовлетворяют условиям $m(E) = E$, $f(E) \neq \pm E$. Два элемента порядка 4, порождающих H, в том же базисе определяются матрицами

$$\alpha = \begin{pmatrix} -iE & 0 & 0 & 0 \\ 0 & iE & 0 & 0 \\ 0 & 0 & -iE & 0 \\ 0 & 0 & 0 & iE \end{pmatrix}, \quad \beta = \begin{pmatrix} 0 & E & 0 & 0 \\ -E & 0 & 0 & 0 \\ 0 & 0 & 0 & E \\ 0 & 0 & -E & 0 \end{pmatrix}, \tag{3.7.1}$$

где $i \in \mathbb{Z}_p$, $i^2 = -1$. Плоскость π допускает бэровскую инволюцию (3.1.3).

Дополнительное изучение возможности существования элементов порядка 3 в нормализаторе $H \simeq Q_8$ доказывает следующую теорему.

Теорема 3.7.2. *Пусть π – недезаргова полуполевая плоскость нечетного порядка p^N, $p > 2$ – простое, $p \equiv 1 \pmod 4$. Если $N = 4$ или N не делится на 4, то ее группа автотопизмов Λ не может содержать подгруппу, изоморфную $SL(2,5)$.*

Рассмотрим подгруппу $H \simeq Q_8$:

$$H = \langle \alpha, \beta \mid \alpha^4 = 1,\ \beta^4 = 1,\ \alpha^2 = \beta^2,\ \alpha\beta\alpha = \beta \rangle. \tag{3.7.2}$$

Для доказательства теоремы 3.7.1 обозначим $\tau = \alpha^2 = \beta^2$, тогда автотопизм τ может быть либо бэровской инволюцией, либо гомологией порядка 2. Рассмотрим все возможные случаи.

Случай 1: H содержит бэровскую инволюцию.

Лемма 3.7.3. *Пусть полуполевая плоскость π порядка p^N ($p > 2$ – простое, $p \equiv 1 \pmod 4$) допускает подгруппу автотопизмов H, изоморфную группе кватернионов Q_8. Тогда инволюция в H не может быть бэровской.*

Доказательство. Если τ – бэровская инволюция, то, как показано в § 2.1, N делится на 2 и в некотором подходящем базисе $2N$-мерного линейного пространства над полем $\mathbb{Z}_p$ инволюция задается матрицей вида (3.1.3) $\tau = \begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix}$, где $L = \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix}$. Обозначим $\alpha = \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix}$, $\beta = \begin{pmatrix} B & 0 \\ 0 & B' \end{pmatrix}$, или, подробнее,

$$\alpha = \begin{pmatrix} A_1 & A_2 & 0 & 0 \\ A_3 & A_4 & 0 & 0 \\ 0 & 0 & A_5 & A_6 \\ 0 & 0 & A_7 & A_8 \end{pmatrix}, \qquad \beta = \begin{pmatrix} B_1 & B_2 & 0 & 0 \\ B_3 & B_4 & 0 & 0 \\ 0 & 0 & B_5 & B_6 \\ 0 & 0 & B_7 & B_8 \end{pmatrix},$$

тогда $A^2 = A'^2 = B^2 = B'^2 = L$, $ABA = B$, $A'B'A' = B'$, $AL = LA$, $A'L = LA'$, $BL = LB$, $B'L = LB'$, поэтому

$$A_2 = A_3 = A_6 = A_7 = 0, \qquad B_2 = B_3 = B_6 = B_7 = 0,$$
$$A_1^2 = A_5^2 = B_1^2 = B_5^2 = -E, \quad A_4^2 = A_8^2 = B_4^2 = B_8^2 = E.$$

По лемме 3.1.5, матрицы регулярного множества полуполевой плоскости, допускающей бэровскую инволюцию, могут быть записаны в виде (3.1.6), где $V \in Q$, $U \in K$, $Q, K \subset GL_{N/2}(p) \cup \{0\}$. Множества Q и K замкнуты по сложению, $0, E \in Q, K$, т.е. Q и K являются регулярными множествами подходящих полуполевых плоскостей порядка $p^{N/2}$. Отображения m и f из Q и K соответственно в $GL_{N/2}(p) \cup \{0\}$ аддитивны (линейны), $m(E) = E$, $f(E) \neq E$. Более того, из условия $4|p-1$ следует $f(E) \neq -E$, иначе регулярное множество содержит вырожденную матрицу $\theta(iE, E) = \begin{pmatrix} E & -iE \\ iE & E \end{pmatrix}$, где $i \in \mathbb{Z}_p^*$, $i^2 = -1$.

Выясним, какой вид могут иметь матрицы A_1, A_5, B_1, B_5. Ясно, что матрицы A_1 и B_1 не могут одновременно являться скалярными. Пусть матрица A_1 не скалярна и $A_1^2 = -E$, тогда λ^2+1 – минимальный многочлен этой матрицы. Жорданова нормальная форма матрицы A_1 – диагональная матрица с диагональными

элементами $\pm i$. Докажем, что их равное количество. Если это не так, то в жордановом базисе матрица A_1 примет вид (для определенности) $A_1' = \begin{pmatrix} D & 0 \\ 0 & iE \end{pmatrix}$, где $D \neq \pm iE$ диагональна с диагональными элементами $\pm i$. Тогда из равенства $A_1 B_1 A_1 = B_1$ в жордановом базисе для матрицы $B_1' = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$ имеем

$$\begin{pmatrix} D & 0 \\ 0 & iE \end{pmatrix} \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix} \begin{pmatrix} D & 0 \\ 0 & iE \end{pmatrix} = \begin{pmatrix} DX_1D & iDX_2 \\ iX_3D & i^2X_4 \end{pmatrix} = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix},$$

тогда $-X_4 = X_4$, $X_4 = 0$, поэтому матрица X_2, например, невырожденная. Имеем $iDX_2 = X_2$, $iD = E$, что противоречит предположению. Таким образом, для матрицы A_1 жорданова нормальная форма $\begin{pmatrix} -iE & 0 \\ 0 & iE \end{pmatrix} = iL$.

Определим теперь вид матриц B_1 и B_5. Из условий $A_1 B_1 A_1 = B_1$ и $B_1^2 = -E$ получим $B_1 = \begin{pmatrix} 0 & X \\ -X^{-1} & 0 \end{pmatrix}$. Упростим B_1 за счет выбора базиса: для матрицы перехода $T = \begin{pmatrix} E & 0 \\ 0 & X \end{pmatrix}$ имеем $TA_1T^{-1} = A_1$, $TB_1T^{-1} = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} = S$. Таким образом, без ограничения общности можно считать, что $A_1 = iL$, $B_1 = S$. Рассуждая для A_5, B_5 аналогично, получим

$$\alpha = \begin{pmatrix} iL & 0 & 0 & 0 \\ 0 & A_4 & 0 & 0 \\ 0 & 0 & iL & 0 \\ 0 & 0 & 0 & A_8 \end{pmatrix}, \quad \beta = \begin{pmatrix} S & 0 & 0 & 0 \\ 0 & B_4 & 0 & 0 \\ 0 & 0 & S & 0 \\ 0 & 0 & 0 & B_8 \end{pmatrix}.$$

Рассмотрим действие коллинеаций α и β на бэровской подплоскости $\pi_\tau = \{(0, x, 0, y) \mid x, y \in W\}$, поточечно фиксируемой инволюцией τ. Так как

$$(0, x, 0, y)^\alpha = (0, xA_4, 0, yA_8) \in \pi_\tau, \quad (0, x, 0, y)^\beta = (0, xB_4, 0, yB_8) \in \pi_\tau,$$

то матрицы $\alpha_0 = \begin{pmatrix} A_4 & 0 \\ 0 & A_8 \end{pmatrix}$, $\beta_0 = \begin{pmatrix} B_4 & 0 \\ 0 & B_8 \end{pmatrix}$ задают автотопизмы порядка 2 подплоскости π_τ либо действуют на π_τ тождественно.

Если α_0 действует тождественно на π_τ либо является гомологией, то $A_4, A_8 \in \{E, -E\}$. В этом случае, поскольку

$$\alpha = \begin{pmatrix} iL & 0 & 0 & 0 \\ 0 & (-1)^k E & 0 & 0 \\ 0 & 0 & iL & 0 \\ 0 & 0 & 0 & (-1)^m E \end{pmatrix}$$

является коллинеацией, то произведение

$$\begin{pmatrix} -iL & 0 \\ 0 & (-1)^k E \end{pmatrix} \begin{pmatrix} m(U) & f(V) \\ V & U \end{pmatrix} \begin{pmatrix} iL & 0 \\ 0 & (-1)^m E \end{pmatrix}$$

принадлежит регулярному множеству для всех $V \in Q$, $U \in K$. Тогда при $V = (-1)^{k+1} iE$ имеем $L \in Q$, что невозможно, поскольку $L + E$ – вырожденная ненулевая матрица в Q.

Итак, коллинеации α и β порядка 4 действуют на бэровской подплоскости π_τ как бэровские инволюции, и число N делится на 4. Следовательно, приводя матрицы A_4 и A_8 к жордановой нормальной форме, мы можем считать, что $A = A' = \begin{pmatrix} iL & 0 \\ 0 & L \end{pmatrix}$, тогда

$$\begin{pmatrix} -iL & 0 \\ 0 & L \end{pmatrix} \begin{pmatrix} m(U) & f(V) \\ V & U \end{pmatrix} \begin{pmatrix} iL & 0 \\ 0 & L \end{pmatrix} = \begin{pmatrix} Lm(U)L & -iLf(V)L \\ iLVL & LUL \end{pmatrix} \in R$$

для всех $V \in Q$, $U \in K$. Поэтому Q и K также представляют собой регулярные множества полуполевых плоскостей, допускающих бэровскую инволюцию, и состоят из матриц вида

$$V = \begin{pmatrix} \psi(U_1) & \nu(V_1) \\ V_1 & U_1 \end{pmatrix} \in Q, \quad U = \begin{pmatrix} \mu(U_2) & \varphi(V_2) \\ V_2 & U_2 \end{pmatrix} \in K,$$

здесь $V_1 \in Q_1, U_1 \in K_1, V_2 \in Q_2, U_2 \in K_2$, множества Q_1, K_1, Q_2, K_2 замкнуты по сложению, содержат нулевую и единичную матрицы. Далее, $\psi(E) = E$, $\mu(E) = E$, $\nu(E) \neq \pm E$, $\varphi(E) \neq \pm E$.

Приводя матрицы B_1 и B_4 к жордановой нормальной форме, с учетом условий $B_4^2 = E$, $B_8^2 = E$, $B_4 \neq \pm E$, $B_8 \neq \pm E$, $LB_4L = B_4$, $LB_8L = B_8$, считаем далее, что B_4 и B_8 – диагональные матрицы с ± 1 на главной диагонали. Поскольку β является коллинеацией, то

$$\begin{pmatrix} -S & 0 \\ 0 & B_4 \end{pmatrix} \begin{pmatrix} m(U) & f(V) \\ V & U \end{pmatrix} \begin{pmatrix} S & 0 \\ 0 & B_8 \end{pmatrix} = \begin{pmatrix} -Sm(U)S & -Sf(V)B_8 \\ B_4VS & B_4UB_8 \end{pmatrix} \in R,$$

$B_4VS \in Q$, $B_4UB_8 \in K$ для всех $V \in Q$, $U \in K$. При $U = E$ имеем $B_4B_8 \in K$, поэтому возможно только $B_8 = \pm B_4$. Рассмотрим произведение B_4VS, где $B_4 = \begin{pmatrix} X_1 & 0 \\ 0 & X_4 \end{pmatrix}$:

$$\begin{pmatrix} X_1 & 0 \\ 0 & X_4 \end{pmatrix} \begin{pmatrix} \psi(U_1) & \nu(V_1) \\ V_1 & U_1 \end{pmatrix} \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} = \begin{pmatrix} -X_1\nu(V_1) & X_1\psi(U_1) \\ -X_4U_1 & X_4V_1 \end{pmatrix} \in Q,$$

отсюда при $V_1 = E$ имеем $X_4 \in K_1$. Тогда диагональная матрица X_4 не может содержать одновременно элементы -1 и 1, т.е. $X_4 = \pm E$. Пусть, например, $X_4 = E$, тогда при $V_1 = U_1 = E$ получим:

$$B_4 V S = \begin{pmatrix} -X_1\nu(E) & -X_1 \\ E & E \end{pmatrix} = \begin{pmatrix} E & -X_1 \\ E & E \end{pmatrix},$$

эта матрица является вырожденной для всех диагональных матриц X_1 с диагональными элементами ± 1. Для случая $X_4 = -E$ рассуждения аналогичны. Полученное противоречие завершает доказательство леммы 3.7.3. □

Отметим, что похожий результат доказан Г. Мурхаузом в 1989 г. для произвольных проективных плоскостей при другом ограничении на их порядок [93]:

Лемма 3.7.4. *Пусть* Π *– проективная плоскость порядка* n^2*, где* $n \equiv 2$ *или* $3 \pmod 4$*, и пусть* G *– группа коллинеаций.*

(i) Если $Fix(G) \neq \varnothing$*, то каждая инволюция в производной подгруппе* G' *является перспективностью.*

(ii) Если G *– циклическая порядка 4, то инволюция в* G *является перспективностью.*

Случай 2: H содержит гомологию порядка 2.

Лемма 3.7.5. *Пусть полуполевая плоскость* π *порядка* p^N *(*$p > 2$ *– простое,* $p-1$ *делится на 4) допускает подгруппу автотопизмов* H*, изоморфную группе кватернионов* Q_8*. Тогда инволюция в* H *не может быть гомологией с осью* $[0]$ *и центром* (0) *или гомологией с осью* $[0,0]$ *и центром* (∞)*.*

Доказательство. Рассуждения, в основном, будут аналогичны приведенным выше, поэтому записаны со значительными сокращениями.

Пусть τ – гомология порядка 2 с осью $[0]$ и центром (0), т.е. $\tau = \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix}$. Повторяя рассуждения из доказательства леммы 3.7.3, имеем $A = iL$ и $B = S$. Приводя матрицу A' к жордановой нормальной форме, получим $\alpha = \begin{pmatrix} iL & 0 \\ 0 & L \end{pmatrix}$. Из условия $A'B'A' = B'$ получим $B' = \begin{pmatrix} B_5 & 0 \\ 0 & B_8 \end{pmatrix}$, где $B_5^2 = B_8^2 = E$. Переходя к жордановой нормальной форме (замена базиса не меняет α), можем считать далее, что B_5 и B_8 – диагональные матрицы с диагональными элементами ± 1.

Поскольку α – коллинеация, то матрица $\begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix}$ задает бэровскую инволюцию. В соответствии с леммой 3.1.5, получаем вид матриц регулярного множества (3.1.6). Далее, поскольку β – коллинеация, то $S^{-1}\theta(V,U)B' \in R$ для всех

$V \in Q$, $U \in K$. В частности, при $U = 0$ и $V = E$ имеем $\begin{pmatrix} -B_5 & 0 \\ 0 & f(E)B_8 \end{pmatrix} \in R$. Складывая с $\pm E$, делаем вывод: матрица B_5 может быть только скалярной, $B_5 = \pm E$, иначе результат сложения является ненулевой вырожденной матрицей. Кроме того, $f(E)B_8 = -B_5 = \mp E$, $f(E) = \mp B_8$. Тогда матрица $\theta(E, E) = \begin{pmatrix} E & \mp B_8 \\ E & E \end{pmatrix}$ содержит одинаковые строки и является вырожденной.

Пусть теперь τ – гомология порядка 2 с осью $[0, 0]$ и центром (∞), $\tau = \begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix}$. Повторяя предыдущие рассуждения, приводим коллинеации α и β к виду $\alpha = \begin{pmatrix} L & 0 \\ 0 & iL \end{pmatrix}$, $\beta = \begin{pmatrix} B & 0 \\ 0 & S \end{pmatrix}$, где B – диагональная матрица с ± 1 на главной диагонали, регулярное множество R состоит из матриц (3.1.6). Отображение β – коллинеация, поэтому $B^{-1}\theta(V, U)S \in R$ для всех $V \in Q$, $U \in K$. Это условие не выполняется, в частности, для $B^{-1}S$. Лемма доказана. □

Осталось рассмотреть случай, когда $\tau = \begin{pmatrix} -E & 0 \\ 0 & -E \end{pmatrix}$ – гомология с осью $[\infty]$ и центром $(0, 0)$. В этом случае можем записать элементы α и β в виде (3.7.1), и так как плоскость допускает бэровскую инволюцию $\begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix} = -i\alpha$, то она имеет регулярное множество из матриц вида (3.1.6). Поскольку β – коллинеация, получим условие $S^{-1}\theta(V, U)S = \begin{pmatrix} U & -V \\ -f(V) & m(U) \end{pmatrix} \in R$ для всех $V \in Q$, $U \in K$, тогда $m : K \to K$, $f : Q \to Q$, $m(m(U)) = U$, $f(f(V)) = V$, т.е. отображения m и f инволютивны, причем отображение f не тождественно, так как $f(E) \neq E$.

Рассмотрим собственные подпространства

$$K_+ = \{U \in K \mid m(U) = U\}, \qquad K_- = \{U \in K \mid m(U) = -U\}, \tag{3.7.3}$$

$$Q_+ = \{V \in Q \mid f(V) = V\}, \qquad Q_- = \{V \in Q \mid f(V) = -V\}, \tag{3.7.4}$$

линейных преобразований m и f соответственно. Покажем, что m не тождественно. Действительно, если $m(U) = U$ для всех $U \in K$, выберем ненулевой элемент $V_0 \in Q_+$ и матрицу $U_0 \in K$ с такой же нижней строкой, что и V_0 (такой выбор возможен, т.к. Q и K – регулярные множества). Тогда в ненулевой матрице $\theta(V_0, U_0) = \begin{pmatrix} U_0 & V_0 \\ V_0 & U_0 \end{pmatrix}$ строки с номерами n и $2n$ одинаковы, матрица вырожденная.

Заметим, что при $N = 2$ из линейности и инволютивности функции $f(x)$ имеем $f(x) = \pm x$ ($x \in \mathbb{Z}_p$), противоречие условию. Теорема 3.7.1 полностью доказана. □

Решая задачу о существовании в группе автотопизмов Λ подгруппы, изоморфной $SL(2,5)$, мы должны далее, опираясь на полученные результаты, предположить существование автотопизма порядка 3, переставляющего циклические подгруппы $\langle\alpha\rangle$, $\langle\beta\rangle$, $\langle\alpha\beta\rangle$ в группе H. Если $\sigma \in N_\Lambda(H)$ – такой автотопизм порядка 3, что $\sigma^{-1}\alpha\sigma = \beta$, то возможны варианты:

1) $\sigma^{-1}\beta\sigma = \alpha\beta$, $\sigma^{-1}\alpha\beta\sigma = \alpha$;

2) $\sigma^{-1}\beta\sigma = \beta\alpha$, $\sigma^{-1}\beta\alpha\sigma = \alpha$.

Очевидно, если коллинеация σ удовлетворяет условиям 1, то $\alpha\sigma$ удовлетворяет 2, и наоборот. Поэтому далее, без ограничения общности, рассмотрим матрицу $\sigma = \begin{pmatrix} C & 0 \\ 0 & D \end{pmatrix}$ при условии 1. Из этого условия получим $C = \begin{pmatrix} C_1 & iC_1 \\ C_1 & -iC_1 \end{pmatrix}$ и $D = \begin{pmatrix} D_1 & iD_1 \\ D_1 & -iD_1 \end{pmatrix}$, где $C_1^3 = D_1^3 = \frac{1-i}{4}E$. Поскольку σ – коллинеация, то для всех $\theta(V,U) \in R$ верно $C^{-1}\theta(V,U)D \in R$. Рассмотрим сначала $V = 0$:

$$C^2\theta(0,U)D = m_1 \begin{pmatrix} C_1^{-1}(m(U)+U)D_1 & 0 \\ 0 & C_1^{-1}(m(U)+U)D_1 \end{pmatrix} +$$

$$+m_2 \begin{pmatrix} 0 & -C_1^{-1}(m(U)-U)D_1 \\ C_1^{-1}(m(U)-U)D_1 & 0 \end{pmatrix} = m_1T_1 + m_2T_2 \in R,$$

значения скаляров $m_1, m_2 \in \mathbb{Z}_p$ не уточняем. Далее в качестве $U \in K$ достаточно рассматривать элементы собственных подпространств K_+ и K_-. Пусть $U \in K_+$, тогда $m(U) = U$, $T_2 = 0$, отсюда $C_1^{-1}UD_1 \in K_+$ для всех $U \in K_+$. Пусть $U \in K_-$, тогда $m(U) = -U$, $T_1 = 0$, поэтому $C_1^{-1}UD_1 \in Q_-$ для всех $U \in K_-$. Поскольку отображение $U \to C_1^{-1}UD_1$ является инъективным, то подпространства Q_- и K_- имеют одинаковую размерность над $\mathbb{Z}_p$, также $\dim Q_+ = \dim K_+$.

Пусть теперь $U = 0$, тогда, рассуждая аналогично, имеем $C_1^{-1}VD_1 \in K_-$ для всех $V \in Q_+$, $C_1^{-1}VD_1 \in Q_+$ для всех $V \in Q_-$. Проведенные вычисления доказывают лемму.

Лемма 3.7.6. *Пусть полуполевая плоскость π порядка p^N ($p > 2$ – простое, $p-1$ делится на 4) допускает подгруппу автотопизмов $H \simeq Q_8$, причем нормализатор H в группе автотопизмов Λ содержит элемент σ порядка 3, $\sigma^{-1}\alpha\sigma = \beta$. Тогда N делится на 4, подпространства K_+, K_- (3.7.3), Q_+, Q_- (3.7.4) имеют одинаковую размерность $N/4$.*

Лемма 3.7.7. *Пусть полуполевая плоскость π порядка p^4 ($p > 2$ – простое, $p-1$ делится на 4) допускает подгруппу автотопизмов $H \simeq Q_8$. Тогда $N_\Lambda(H) \setminus C_\Lambda(H)$ не содержит элементов порядка 3.*

Доказательство. Так как $N = 4$, то $|K| = |Q| = p^2$, K и Q – поля в $GL_2(p) \cup \{0\}$, подпространства K_+, K_-, Q_+, Q_- одномерны и $K_+ = \{kE \mid k \in \mathbb{Z}_p\}$ – множество скалярных матриц.

Рассмотрим равенство $C_1^3 = D_1^3 = \frac{1-i}{4}E$ и перепишем $C_1 = \frac{-1-i}{2}C_0$, $D_1 = \frac{-1-i}{2}D_0$, тогда $C_0^3 = D_0^3 = E$. Из условия $C_0^{-1}K_+D_0 = K_+$ получим $C_0^{-1}ED_0 = kE$, т.е. $D_0 = kC_0$, далее можно рассматривать условия

$$C_0^{-1}K_+C_0 = K_+, \quad C_0^{-1}K_-C_0 = Q_-, \quad C_0^{-1}Q_-C_0 = Q_+, \quad C_0^{-1}Q_+C_0 = K_-$$

и отображение $\varphi : U \to C_0^{-1}UC_0$. Очевидно, $K_+ \oplus Q_- = Q$, поэтому $K^\varphi = Q$. Далее, $Q^\varphi = Q$, отсюда $Q = K$, $\varphi \in Aut\, K$. Так как $|Aut\ K| = 2$ и $\varphi^3 = \varepsilon$, то φ тождественно, что противоречит условию $Q_-^\varphi = Q_+$, лемма доказана. □

В качестве следствия получаем теорему 3.7.2.

3.8. Подгруппа автотопизмов, изоморфная S_3

В этом параграфе проводятся исследования полуполевых плоскостей, имеющих ранг 2 над ядром, регулярное множество таких плоскостей образовано 2×2-матрицами. Отметим, что исследованиям таких плоскостей трансляций было посвящено в 1990-2000 гг. значительное число работ (см., например, [29] и др.). Решается задача построения матричного построения регулярного множества в предположении, что полуполевая плоскость π имеет порядок p^{2n}, обладает ядром порядка p^n (p – простое), подгруппа линейных над $GF(p^n)$ автотопизмов содержит подгруппу H, изоморфную симметрической группе S_3.

Симметрическая группа S_3 является некоммутативной группой минимального порядка, ее наличие в группе коллинеаций проективной плоскости и в группе автоморфизмов координатизирующего множества может указывать на наличие особенных свойств. Так, среди всех 23 неизоморфных полуполей порядка 16 ровно одно имеет группу автоморфизмов, изоморфную S_3. Таким же свойством обладает исключительное полуполе Хентзела–Руа порядка 64, не являющееся ни лево-, ни правопримитивным [134]. Кроме того, поскольку S_3 содержится в значительном числе известных групп, условие существования S_3 в группе автотопизмов приводит к получению важных технических результатов для дальнейших исследований. Отметим также особую роль группы S_3 в исследовании полуполевых плоскостей в связи с классификацией полуполей не только с точностью до изотопизма, но и с точностью до S_3 (так называемые орбиты Кнута, см., например, [102]).

Мы рассматриваем полуполевые плоскости ранга 2 над полем $F \simeq GF(p^n)$, считая, что ядро полуполя либо совпадает с F, либо содержит F (в этом случае

плоскость дезаргова, R — поле). Группа линейных автотопизмов состоит из матриц размерности 4×4 с элементами из F, регулярное множество R содержится в $GL_2(p^n)\cup\{0\}$. Пусть $H<\Lambda_0$, $H=\langle\tau,\sigma\rangle\simeq S_3$, где τ и σ — неперестановочные инволюции, коллинеация $\gamma=\tau\sigma$ имеет порядок 3. Обсудим прежде всего геометрический смысл элементов H. При $p=2$ инволюции τ и σ могут быть только бэровскими, при $p>2$ — бэровскими коллинеациями либо гомологиями, произведение $\tau\sigma$ может быть гомологией при $p\neq 3$. Таким образом, случаи $p=2$, $p=3$, $p>3$ требуют отдельного изучения.

Случай $p=2$**.**

Теорема 3.8.1. *Пусть π — полуполевая плоскость порядка 2^{2n} с ядром, содержащим $F\simeq GF(2^n)$, группа линейных автотопизмов которой содержит подгруппу H, изоморфную симметрической группе S_3. Тогда базис 4-мерного линейного пространства над F может быть выбран так, что регулярное множество плоскости $R\subset GL_2(F)\cup\{0\}$ состоит из матриц вида (3.1.1)*

$$\theta(v,u)=\begin{pmatrix} u+v+m(v) & f(v)+m(u)\\ v & u\end{pmatrix},\qquad u,v\in F,$$

где m,f — аддитивные функции на F, причем f взаимно однозначна и $m(1)=0$. Далее,

1) если H содержит гомологию с осью $[0,0]$ и центром (∞), то $f(x)=x$ $\forall x\in F$;

2) если H содержит гомологию с осью $[0]$ и центром (0), то $f(x)=m(m(x))+m(x)+x$ $\forall x\in F$;

3) если H содержит гомологию с осью $[\infty]$ и центром $(0,0)$, то $f(x)=x$, $m(x)=0$ $\forall x\in F$, плоскость дезаргова;

4) если H не содержит гомологий, то функции m и f удовлетворяют условиям ($\forall x\in F$)

$$\begin{aligned} m(m(x))&=m(x), & f(m(x))&=m(x),\\ m(f(x))&=m(x)+f(x)+x, & f(f(x))&=x.\end{aligned}$$

Доказательство. Так как $|\pi|=2^{2n}$, элементы τ и σ являются бэровскими инволюциями. Воспользуемся результатами [29], приведенными выше в теореме 3.1.1: если полуполевая плоскость порядка 2^{2n} с ядром порядка $\geq 2^n$ допускает бэровскую инволюцию τ в линейном трансляционном дополнении, то τ может быть задана матрицей (3.1.2), регулярное множество состоит из матриц вида (3.1.1). Обозначим

$$L=\begin{pmatrix}1&1\\0&1\end{pmatrix},\quad \tau=\begin{pmatrix}L&0\\0&L\end{pmatrix},\quad \sigma=\begin{pmatrix}A&0\\0&B\end{pmatrix},$$

$A, B \in GL_2(p^n)$, тогда для инволюции σ должны быть выполнены условия:

1) $A^2 = B^2 = E$,

2) $AL \neq LA$ или $BL \neq LB$,

3) $(LA)^3 = (LB)^3 = E$.

Тогда матрицы A и B могут быть равны либо L (не одновременно), либо матрице

$$\begin{pmatrix} a & a^2+1 \\ 1 & a \end{pmatrix}, \quad a \in F.$$

Заметим, что верно равенство

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & a^2+1 \\ 1 & a \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = M,$$

поэтому базис линейного пространства можно выбрать так (не меняя τ), что

$$\sigma \in \left\{ \begin{pmatrix} L & 0 \\ 0 & M \end{pmatrix}, \begin{pmatrix} M & 0 \\ 0 & L \end{pmatrix}, \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix} \right\}.$$

Рассмотрим подробно все три возможных случая. В первом случае коллинеация $\gamma = \tau\sigma$ определяется матрицей

$$\gamma = \begin{pmatrix} E & 0 \\ 0 & LM \end{pmatrix}$$

и является гомологией порядка 3 с осью $[0, 0]$ и центром (∞), при этом матрица LM удовлетворяет условию $\theta(v, u)LM \in R$ для всех v, u. При $v = 0$ имеем

$$\theta(0, u)LM = \begin{pmatrix} u & m(u) \\ 0 & u \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} u + m(u) & u \\ u & 0 \end{pmatrix} = \theta(u, 0),$$

отсюда $f(u) = u$. Рассмотрение $u = 0$ не дает новых ограничений на функции f и m.

Во втором случае

$$\gamma = \begin{pmatrix} LM & 0 \\ 0 & E \end{pmatrix}$$

является гомологией порядка 3 с осью $[0]$ и центром (0), при этом $LM\theta(v, u) \in R$ для всех v, u. При $v = 0$

$$LM\theta(0, u) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u & m(u) \\ 0 & u \end{pmatrix} = \begin{pmatrix} u & m(u) + u \\ u & m(u) \end{pmatrix} = \theta(0, m(u)),$$

отсюда $f(u) = m(m(u)) + m(u) + u$. При $u = 0$ получим то же условие.

В третьем случае для $A = B = M$ должно выполняться условие (2.2.3). При $v = 0$

$$M^{-1}\theta(0,u)M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u & m(u) \\ 0 & u \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} u & 0 \\ m(u) & u \end{pmatrix} = \theta(m(u),u),$$

тогда $m(m(x)) = m(x)$, $f(m(x)) = m(x)$. При $u = 0$

$$M^{-1}\theta(v,0)M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} v + m(v) & f(v) \\ v & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & v \\ f(v) & v + m(v) \end{pmatrix} = \theta(f(v), v + m(v)),$$

тогда $m(f(x)) = m(x) + f(x) + x$, $f(f(x)) = x$. Поскольку отображение $m(x)$ в общем случае не является биективным, полученные условия трудно преобразовать к более удобному виду.

Заметим, что если в третьем случае коллинеация γ является гомологией, то ее ось — особая прямая $[\infty]$, центр — точка $(0,0)$, при этом матрица LM должна быть перестановочна со всеми матрицами регулярного множества. Из этого условия $LM\theta(v,u) = \theta(v,u)LM$ получим $f(v) = v$, $m(v) = 0$ для всех v, поэтому, в силу линейности m и f, регулярное множество является полем, т.е. плоскость π дезаргова. Теорема 3.8.1 полностью доказана. □

Случай $p > 2$**.**

Лемма 3.8.2. *Пусть π — полуполевая плоскость порядка p^{2n} с ядром, содержащим $F \simeq GF(p^n)$ ($p > 2$ — простое), группа линейных автотопизмов которой содержит подгруппу H, изоморфную симметрической группе S_3. Тогда инволюции $\tau, \sigma \in H$ являются бэровскими, базис 4-мерного линейного пространства над F может быть выбран так, что $\tau = \begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix}$, регулярное множество плоскости $R \subset GL_2(F) \cup \{0\}$ состоит из матриц вида (3.1.6)*

$$\theta(v,u) = \begin{pmatrix} m(u) & f(v) \\ v & u \end{pmatrix}, \qquad u, v \in F,$$

где m, f — аддитивные взаимно однозначные функции на F, причем $m(1) = 1$. При этом $\sigma = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$, где $A, B \in \{L, M\}$ при $p > 3$, $A, B \in \{L, A_1, A_2\}$ при $p = 3$, $(A,B) \neq (L,L)$,

$$L = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad M = \begin{pmatrix} 1/2 & 1/2 \\ 3/2 & -1/2 \end{pmatrix}, \quad A_1 = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Доказательство. В случае нечетного порядка плоскости π центральные коллинеации порядка 2 в группе автотопизмов Λ являются гомологиями h_1, h_2, h_3 (3.2.1), они не сопряжены в Λ. Поэтому инволюции τ, σ, как и для $p = 2$, являются бэровскими коллинеациями. Воспользуемся теоремой 3.1.2 для ранга 2: в подходящем базисе линейного пространства бэровская инволюция определяется матрицей (3.1.3), регулярное множество состоит из матриц (3.1.6).

Инволюция σ должна удовлетворять условиям 1–3 из доказательства теоремы 3.8.1. При этом для матрицы A (для B аналогично) возможны четыре ситуации ($a \in F$, $a \neq 0$):

1) $A = L$,

2) $p = 3$ и $A = \begin{pmatrix} -1 & 0 \\ a & 1 \end{pmatrix}$,

3) $p = 3$ и $A = \begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix}$,

4) $p \neq 3$ и $A = \begin{pmatrix} \frac{1}{2} & a \\ \\ \frac{3}{4a} & -\frac{1}{2} \end{pmatrix}$.

Для случаев 2–4 можно выбрать замену базиса линейного пространства, упрощающую вид матрицы A и сохраняющую вид L. Действительно,

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ a & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix} = A_1,$$

$$\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} = A_2,$$

$$\begin{pmatrix} 1 & 0 \\ \\ 0 & 2a \end{pmatrix} \begin{pmatrix} \frac{1}{2} & a \\ \\ \frac{3}{4a} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \\ 0 & \frac{1}{2a} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix} = M.$$

Лемма доказана. □

Теорема 3.8.3. *Если π — полуполевая плоскость порядка 3^{2n} с ядром, содержащим $F \simeq GF(3^n)$, то группа линейных над F автотопизмов не содержит подгруппы, изоморфной симметрической группе S_3.*

Доказательство. Если $A = L$ или $B = L$, то $\gamma = \tau\sigma$ является гомологией порядка 3, что невозможно, так как $|\pi| - 1$ не делится на 3.

Для остальных выделенных в лемме 3.8.2 случаев при $p = 3$ проверим выполнение условия (2.2.3). Непосредственные расчеты показывают:

$$A_1^{-1}\theta(v, 0)A_1 = \begin{pmatrix} -f(v) & -f(v) \\ -v + f(v) & f(v) \end{pmatrix} = \theta(-v + f(v), f(v)) \Rightarrow f(f(v)) = 0 \ \forall v;$$

$$A_2^{-1}\theta(v,0)A_2 = \begin{pmatrix} -v & v-f(v) \\ -v & v \end{pmatrix} = \theta(-v,v) \Rightarrow f(-v) = v - f(v)\ \forall v;$$

$$A_1^{-1}\theta(0,u)A_2 = \begin{pmatrix} m(u) & -m(u) \\ -m(u) & m(u)+u \end{pmatrix} = \theta(-m(u), m(u)+u) \Rightarrow m(m(u)) = 0\ \forall u;$$

$$A_2^{-1}\theta(0,u)A_1 = \begin{pmatrix} m(u)+u & u \\ u & u \end{pmatrix} = \theta(u,u) \Rightarrow m(u) = m(u) + u\ \forall u.$$

Учитывая инъективность отображений m и f, заключаем, что все перечисленные случаи невозможны. Теорема 3.8.3 доказана. □

Отметим, что частный случай $|\pi| = 81$ представлен в докладе [168] на Международной конференции G2A2 (Екатеринбург, 2015 г.): если полуполевая плоскость порядка 81 допускает бэровскую инволюцию в группе автотопизмов, то порядок группы автотопизмов равен 2^k, $8 \le k \le 11$.

Теорема 3.8.4. *Пусть π — полуполевая плоскость порядка p^{2n}, с ядром, содержащим $F \simeq GF(p^n)$ ($p > 3$ — простое), группа линейных автотопизмов которой содержит подгруппу H, изоморфную симметрической группе S_3. Тогда базис 4-мерного линейного пространства над F может быть выбран так, что регулярное множество плоскости в $GL_2(F) \cup \{0\}$ имеет вид* (3.1.6). *Далее:*

1) если H содержит гомологию с осью $[0,0]$ и центром (∞), то $f(x) = -m(x)/3\ \forall x \in F$;

2) если H содержит гомологию с осью $[0]$ и центром (0), то $f(m(x)) = m(f(x)) = -x/3\ \forall x \in F$;

3) если H содержит гомологию с осью $[\infty]$ и центром $(0,0)$, то $p-3$ не является квадратом, $f(x) = -x/3$, $m(x) = x\ \forall x \in F$, плоскость дезаргова;

4) если H не содержит гомологий, то функции m и f удовлетворяют условиям ($\forall x \in F$)

$$m(m(x)) = x, \qquad f(f(x)) = \frac{1}{9}x,$$

$$m(f(x)) = -\frac{1}{3}m(x) - f(x) - \frac{1}{3}x, \qquad f(m(x)) = \frac{1}{3}m(x) + f(x) - \frac{1}{3}x.$$

Доказательство. Аналогично доказательству теоремы 3.8.3, рассмотрим случаи для $p > 3$, выделенные в лемме 3.8.2.

При $(A,B) = (L,M)$ коллинеация $\gamma = \tau\sigma$ является гомологией с осью $[0,0]$ и центром (∞), тогда матрица

$$LM = \begin{pmatrix} -1/2 & -1/2 \\ 3/2 & -1/2 \end{pmatrix}$$

должна удовлетворять условию $\theta(v,u)LM \in R$ для всех $v,u \in F$. В силу замкнутости R по сложению вместо LM достаточно рассмотреть матрицу $N = 2LM + E$. Тогда при $v = 0$ получим

$$\theta(0,u)N = \begin{pmatrix} 0 & -m(u) \\ 3u & 0 \end{pmatrix} = \theta(3u,0),$$

отсюда $f(x) = -m(x)/3$ для всех x. Случай $u = 0$ дает то же условие.

При $(A,B) = (M,L)$, аналогично, γ является гомологией в осью $[0]$ и центром (0), матрица N удовлетворяет условию $N\theta(v,u) \in R$ для всех v,u. Рассматривая отдельно $v = 0$ и $u = 0$, получим условие $f(m(x)) = m(f(x)) = -x/3$ для всех x.

При $A = B = M$ проверяем выполнение условия (2.2.3). При $v = 0$ получим

$$M^{-1}\theta(0,u)M = \frac{1}{4}\begin{pmatrix} m(u)+3u & m(u)-u \\ 3m(u)-3u & 3m(u)+u \end{pmatrix} \in R,$$

из замкнутости регулярного множества по сложению следуют равенства

$$m(3m(u)+u) = m(u)+3u, \quad f(3m(u)-3u) = m(u)-u.$$

Аналогично, при $v = 0$ условие (2.2.3) приводит к равенствам

$$m(-v-3f(v)) = v+3f(v), \quad f(-v+9f(v)) = v-f(v).$$

Преобразуя, получаем условия теоремы 3.8.4.

Дополнительно рассмотрим ситуацию, когда коллинеация γ является гомологией с осью $[\infty]$ и центром $(0,0)$. Тогда матрица LM централизует R, поэтому матрица $N = 2LM + E$ также удовлетворяет условию $N\theta(v,u) = \theta(v,u)N$ для всех v,u, $f(v) = -v/3$, $m(u) = u$,

$$|\theta(v,u)| = \begin{vmatrix} u & -\frac{1}{3}v \\ v & u \end{vmatrix} = \frac{u^2}{3}\left(3 + \left(\frac{v}{u}\right)^2\right).$$

Если $p-3$ не является квадратом, то $|\theta(v,u)| \neq 0$ для всякой ненулевой матрицы, и плоскость π дезаргова. Теорема 3.8.4 доказана. □

Рассматривая произведение гомологий $\begin{pmatrix} E & 0 \\ 0 & LM \end{pmatrix}$ и $\begin{pmatrix} LM & 0 \\ 0 & E \end{pmatrix}$, приходим к очевидному следствию.

Следствие 3.8.5. *Пусть π — полуполевая плоскость порядка p^{2n} ($p = 2$ или $p > 3$ — простое) с ядром $\supseteq GF(p^n)$, группа линейных автотопизмов содержит подгруппы*

$$H_1 = \langle \tau, \gamma_1 \rangle \simeq S_3, \quad H_2\langle \tau, \gamma_2 \rangle \simeq S_3,$$

где τ — бэровская инволюция, γ_1 — гомология порядка 3 с осью $[0,0]$ и центром (∞), γ_2 — гомология порядка 3 с осью $[0]$ и центром (0). Тогда подгруппа $H_3 = \langle \tau, \gamma_1\gamma_2 \rangle$ также изоморфна S_3 и не содержит гомологий.

Глава 4. Алгоритмы построения полуполевых плоскостей

В этой главе рассматриваются примеры полуполевых плоскостей, иллюстрирующие теоретические результаты главы 3. Запись матричного представления регулярного множества полуполевой плоскости при фиксированных ограничениях на коллинеации не является достаточным условием существования таких плоскостей. Поэтому важно выяснить, является ли множество изучаемых объектов непустым.

В § 4.1 перечислены минимальные примеры полуполевых плоскостей ранга 2 над ядром, допускающие S_3 в группе автотопизмов. Представлены примеры к теореме 3.1.2 для $p = 2$ полуполевых плоскостей четного порядка, допускающих бэровскую инволюцию. Приложениями к теореме 3.7.1 являются примеры полуполевых плоскостей порядков 5^4 и 13^4, допускающих подгруппу автотопизмов, изоморфную группе кватернионов Q_8. Кратко описан алгоритм построения полуполевых плоскостей на основе матричного представления их регулярного множества с применением вычислительной техники. В § 4.2 также обсуждаются возможности использования методов компьютерной алгебры для доказательства изоморфиза двух полуполевых плоскостей.

§ 4.3 посвящен построению примеров полуполевых плоскостей порядка 81, допускающих бэровскую инволюцию (к теореме 3.1.2). Основной результат показывает, что все построенные примеры являются 3-примитивными плоскостями и расширяют список примеров М. Кордеро [37].

4.1. Построение полуполевых плоскостей малых рангов

Особенностью ряда результатов о полуполевых проективных плоскостях и их координатизирующих полуполях (как и результатов о других алгебраических системах) является отсутствие достаточных условий существования этих объектов при изучаемых дополнительных ограничениях. Указание матричного представления регулярного множества с достаточно общими ограничениями не является достаточным условием существования плоскости трансляций с таким регулярным множеством. Так, например, существование недезарговых полуполевых плоскостей ранга 2 с регулярным множеством (3.1.1), допускающих бэровскую инволюцию [29], было подтверждено [64] только в 1990 г. Х. Хуангом и Н. Джонсоном, построившими примеры восьми полуполевых плоскостей порядка 64.

Другим примером этой проблемы служит сравнение теорем 3.5.1 и 3.5.2: первая из них указывает матричное представление регулярного множества плоскости, если она существует, вторая – выявляет отсутствие плоскостей при поставленном условии. Итак, перечисление любых условий на группу автотопизмов приводит к естественному вопросу: существуют ли проективные плоскости при таких условиях?

Целью этого параграфа является указание полуполевых плоскостей порядка p^4, удовлетворяющих:

(1) теореме 3.1.2 для $p = 2$ (для $p > 2$ см. § 4.3),

(2) теореме 3.7.1,

(3) теоремам 3.8.1 и 3.8.4.

В случае (3) полуполевая плоскость, допускающая подгруппу автотопизмов $H \simeq S_3$, имеет порядок q^2 и левое ядро порядка q. Поэтому регулярное множество такой плоскости имеет представление в кольце 2×2-матриц над полем $GF(q)$. Рассмотрим (подробнее см. [138]) такие полуполевые плоскости, выбирая минимальный возможный порядок $p^4 = 16$ и $p^4 = 625$ (по теореме 3.8.3, при $p = 3$ полуполевая плоскость не допускает S_3 в группе линейных автотопизмов).

Мы используем результат Т. Воан [112] о представлении аддитивной функции $g(x)$ на $GF(p^n)$ линейной комбинацией автоморфизмов поля:

$$g(x) = c_0 x + c_1 x^p + c_1 x^{p^2} + \cdots + c_{n-1} x^{p^{n-1}}, \qquad c_0, c_1, c_2, \ldots, c_{n-1} \in GF(p^n).$$

Пример 4.1. Пусть $p = 2$, $p^{2n} = 16$, $F = \{0, 1, \alpha, \alpha + 1\} \simeq GF(4)$, $\alpha^2 = \alpha + 1$. Как указано в § 5.6, существуют ровно два неизотопных полуполя порядка 16, т.е. две неизоморфных недезарговых полуполевых плоскости порядка 16. Покажем, что одна из них обеспечивает необходимый пример. Рассмотрим условия

в теореме 3.8.1, полагая

$$m(x) = m_0(x + x^2), \qquad f(x) = f_0x + f_1x^2 \quad (x \in F),$$

здесь $m_0, f_0, f_1 \in F$. Достаточным условием существования полуполевой плоскости, удовлетворяющей теореме 3.8.1, является требование

$$\begin{vmatrix} u + v + m_0(v + v^2) & f_0v + f_1v^2 + m_0(u + u^2) \\ v & u \end{vmatrix} \neq 0 \quad \forall u, v \in F,\ (u, v) \neq (0, 0). \tag{4.1.1}$$

Перебор коэффициентов m_0, f_0, f_1, удовлетворяющих условиям теоремы 3.8.1 и (4.1.1), приводит к результатам, перечисленным в табл. 3.

Таблица 3. Коэффициенты функций $m(x)$, $f(x)$ при $p = 2$

Регулярное множество	m_0	f_0	f_1	Случай теоремы 3.8.1
R_1	1	1	0	1
R_2	1	0	1	2
R_3	α	1	0	1,2,4
R_4	$\alpha + 1$	1	0	1,2,4

Таким образом, найдены четыре полуполевых плоскости порядка 16 с регулярными множествами R_1, R_2, R_3, R_4, группа линейных автотопизмов которых содержит подгруппу, изоморфную S_3. Отметим, что эти плоскости изоморфны. Действительно, автоморфизм $x \to x^2$ поля F переводит R_3 в R_4, и непосредственная проверка показывает, что выполнено

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} R_1 \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} = R_2, \qquad \begin{pmatrix} 0 & \alpha^2 \\ \alpha^2 & 1 \end{pmatrix} R_1 = R_3.$$

Пример 4.2. Построим примеры плоскостей порядка 625, используя результаты теоремы 3.8.4. Рассмотрим поле $GF(25) = GF(5^2)$ как фактор-кольцо кольца $\mathbb{Z}_5[x]$ по идеалу, порожденному неприводимым в $\mathbb{Z}_5[x]$ многочленом $x^2 - 2$,

$$GF(25) \simeq \mathbb{Z}_5[x]/(x^2 - 2) = \{0, 1, 2, 3, 4, \alpha, \alpha + 1, \ldots, 4\alpha + 4\},$$

где $\alpha^2 = 2$. В условиях теоремы 3.8.4 полагаем

$$m(x) = m_0x + m_1x^5, \qquad f(x) = f_0x + f_1x^5 \quad (x \in F),$$

здесь $m_0, m_1, f_0, f_1 \in F$. Достаточным условием существования полуполевой плоскости, удовлетворяющей теореме 3.8.4, является требование

$$\begin{vmatrix} m_0u + m_1u^5 & f_0v + f_1v^5 \\ v & u \end{vmatrix} \neq 0 \quad \forall u, v \in F,\ (u, v) \neq (0, 0). \tag{4.1.2}$$

Компьютерный перебор коэффициентов m_0, m_1, f_0, f_1, удовлетворяющих условиям теоремы 3.8.4 и (4.1.2), приводит к результатам, перечисленным в табл. 4. В таблице исключены изоморфные копии, полученные автоморфизмом $x \to x^5$ поля F.

Таблица 4. Коэффициенты функций $m(x)$, $f(x)$ при $p = 5$

№	m_0	m_1	f_0	f_1	Случай теоремы 3.8.4
1	2	4	1	2	1
2	4	2	2	1	1
3	$\alpha+4$	$4\alpha+2$	$3\alpha+2$	$2\alpha+1$	1
4	$2\alpha+1$	3α	$\alpha+3$	4α	1
5	$2\alpha+2$	$3\alpha+4$	$\alpha+1$	$4\alpha+2$	1
6	2	4	2	1	2
7	4	2	1	2	2
8	$\alpha+4$	$4\alpha+2$	$\alpha+1$	$4\alpha+2$	2
9	$2\alpha+1$	3α	$4\alpha+3$	α	2
10	$2\alpha+2$	$3\alpha+4$	$3\alpha+2$	$2\alpha+1$	2
11	α	$4\alpha+1$	2α	4	4
12	2α	$3\alpha+1$	4α	3α	4
13	α	$4\alpha+1$	3α	$2\alpha+3$	1,2,4
14	$\alpha+4$	$4\alpha+2$	$3\alpha+2$	$2\alpha+1$	1,2,4

Дальнейшее выделение в приведенном списке попарно изоморфных полуполевых плоскостей не проводилось, поскольку значительно более трудоемко в сравнении со случаем $|\pi| = 16$. Существование полуполевых плоскостей порядка 625 с подгруппой линейных автотопизмов, изоморфной S_3, подтверждено.

Возвращаясь к обсуждению случая $p^4 = 16$, заметим, что полуполя V_i в § 5.6 не могут быть заданы регулярным множеством в кольце 2×2-матриц над $GF(4)$, так как имеют ядра $N_l = N_m = N_r = \mathbb{Z}_2$. Для их построения используется (подробнее см. [129]) регулярное множество в $GL_4(2)\cup\{0\}$, заданное линейными функциями.

Пример 4.3. Пусть π – полуполевая плоскость порядка 16, допускающая бэровскую инволюцию. Тогда, по теореме 3.1.3, ее регулярное множество в $GL_4(2) \cup \{0\}$ может быть представлено матрицами вида (3.1.5)

$$\theta(V,U) = \begin{pmatrix} U+V+m(V)+w(V) & f(V)+m(U) \\ V & U+w(V) \end{pmatrix},$$

где $U, V \in K$, $K \subset GL_2(2)\cup\{0\}$ – регулярное множество бэровской подплоскости π_τ, фиксируемой инволюцией τ, m, w, f – линейные отображения из K в кольцо

2×2-матриц над $\mathbb{Z}_2$, причем $m(E)=0$ и для всех $V\in K$ нижняя строка матрицы $w(V)$ состоит только из нулей.

Так как регулярное множество K замкнуто относительно сложения, то оно соответствует полуполю порядка 4, т.е. полю $GF(4)$, и мы можем считать

$$K=\left\{\begin{pmatrix}a+b & a\\ a & b\end{pmatrix}\;\middle|\;a,b\in\mathbb{Z}_2\right\}.$$

Это двумерное линейное пространство над $\mathbb{Z}_2$ с базой $D=\begin{pmatrix}1&1\\1&0\end{pmatrix}, E=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, т.е. $K=\{aD+bE\mid a,b\in\mathbb{Z}_2\}$.

Регулярное множество R плоскости π является 4-мерным линейным пространством над $\mathbb{Z}_2$, его база состоит из четырех матриц:

$$A_1=\begin{pmatrix}D+M+W_1 & F_1\\ D & W_1\end{pmatrix},\qquad A_2=\begin{pmatrix}E+W_2 & F_2\\ E & W_2\end{pmatrix},$$

$$A_3=\begin{pmatrix}D & M\\ 0 & D\end{pmatrix},\qquad A_4=\begin{pmatrix}E & 0\\ 0 & E\end{pmatrix},$$

где $W_1=w(D)$, $W_2=w(E)$, $M=m(D)$, $F_1=f(D)$, $F_2=f(E)$ и для любой матрицы $U=aD+bE\in K$, в силу линейности отображений,

$$w(U)=aW_1+bW_2,\qquad m(U)=aM,\qquad f(U)=aF_1+bF_2,$$

тогда $R=\{x_1A_1+x_2A_2+x_3A_3+x_4A_4\mid x_i\in\mathbb{Z}_2,\ i=1,2,3,4\}$.

Исходя из требования невырожденности всех матриц регулярного множества R, кроме нулевой, получим (с использованием компьютера) список возможных вариантов матриц M,F_1,F_2,W_1,W_2, содержащий 224 набора. Таким образом, построено 224 регулярных множества вида (3.1.5) и, следовательно, 224 полуполевых плоскости порядка 16, допускающих бэровскую инволюцию.

Для дальнейшего исследования и классификации построенных плоскостей найдено левое ядро R_l как централизатор регулярного множества R, для этого достаточно выбрать матрицы, перестановочные с A_1, A_2, A_3. Непосредственные вычисления показывают, что 8 плоскостей из построенных 224 имеют левое ядро порядка 16, поэтому R является полем, соответствующие плоскости – дезарговы. 72 плоскости имеют левое ядро порядка 4, поэтому изоморфны плоскостям ранга 2 над полем $GF(4)$. Оставшиеся 144 плоскости имеют левое ядро порядка 2, поэтому не могут быть заданы линейным пространством размерности менее 4.

В соответствии с классификацией полуполей порядка 16 (теорема 5.4.1), существует ровно одна недезаргова полуполевая плоскость ранга 2 над $GF(4)$,

поэтому 72 плоскости с ядром $\mathbb{Z}_2$ должны быть попарно изоморфны. Как показано, например, в [126, 128], изоморфизм таких плоскостей задается линейным преобразованием 8-мерного линейного пространства:

$$\varphi : (x, y) \to (x, y) \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

где x, y – векторы 4-мерного пространства, клетки A и B имеют размерность 4×4. Если преобразование φ задает изоморфизм плоскостей с регулярными множествами R и R', то матрицы A и B удовлетворяют условию:

$$\forall \theta \in R \quad A^{-1}\theta B \in R'.$$

Так как обе плоскости допускают бэровскую инволюцию τ вида (3.1.3), поставим условие $\varphi\tau\varphi^{-1} = \tau$ и зададим преобразование φ матрицей вида

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \begin{pmatrix} A_1 & A_2 & 0 & 0 \\ 0 & A_1 & 0 & 0 \\ 0 & 0 & B_1 & B_2 \\ 0 & 0 & 0 & B_1 \end{pmatrix}. \tag{4.1.3}$$

Отображения (4.1.3) образуют группу порядка 288, действующую на классе полуполевых плоскостей с регулярным множеством вида (3.1.5). При этом класс построенных плоскостей разбивается на пять непересекающихся орбит:

1) 8 дезарговых плоскостей попарно изоморфны;

2) 144 плоскости с ядром порядка 2 попарно изоморфны;

3) множество из 72 плоскостей с ядром порядка 4 разбивается на 3 класса по 24 попарно изоморфных плоскости.

Для подтверждения изоморфности плоскостей с ядром порядка 4 потребовалось рассмотреть линейные преобразования φ, не перестановочные с бэровской инволюцией τ, отказавшись от условия (4.1.3). Компьютерный перебор произвольных невырожденных 4×4-матриц A и B показал, что все плоскости с ядром порядка 4 изоморфны между собой.

Проведенные вычисления, очевидно, показывают, что любая полуполевая плоскость порядка 16 допускает бэровскую инволюцию.

Теорема 4.1.1. *Существуют ровно три, с точностью до изоморфизма, полуполевые плоскости порядка 16, допускающие бэровскую инволюцию в трансляционном дополнении: π_1, π_2, π_3. Регулярное множество этих плоскостей имеет вид (3.1.5) и определяется матрицами M, F_1, F_2, W_1, W_2, см. табл. 5. Плоскость π_3 дезаргова, плоскость π_1 имеет ядро порядка 4, плоскость π_2 – ядро порядка 2.*

Таблица 5. Коэффициенты регулярного множества полуполевых плоскостей порядка 16

Плоскость	M	F_1	F_2	W_1	W_2
π_1	$\begin{pmatrix}0&0\\0&0\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1&0\\1&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&0\end{pmatrix}$	$\begin{pmatrix}1&1\\0&0\end{pmatrix}$
π_2	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&0\end{pmatrix}$	$\begin{pmatrix}1&0\\0&0\end{pmatrix}$
π_3	$\begin{pmatrix}0&0\\0&0\end{pmatrix}$	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}0&0\\0&0\end{pmatrix}$	$\begin{pmatrix}0&0\\0&0\end{pmatrix}$

С использованием того же программного аппарата, что и для построения изоморфизмов, найдены группа автотопизмов Λ, централизатор бэровской инволюции τ и общее количество инволюций в Λ, см. табл. 6. В этой таблице P – подгруппа в Λ, порожденная перспективностями, $P = H_l(H_m \times H_r)$.

Таблица 6. Автотопизмы полуполевых плоскостей порядка 16

Плоскость	$\lvert R_l\rvert$	$\lvert C_\Lambda(\tau)\rvert$	$\lvert P\rvert$	$\lvert\Lambda\rvert$	Число инволюций в Λ
π_1	4	12	27	108	27
π_2	2	2	1	18	9
π_3	16	36	225	900	25

Из полученных результатов непосредственно следует разрешимость группы автотопизмов Λ и поэтому группы коллинеаций для плоскостей π_1 и π_2.

Пример 4.4. Для полуполевой плоскости нечетного порядка, допускающей бэровскую инволюцию, матричное представление (3.1.6) регулярного множества определено в теореме 3.1.5. Случай $|\pi| = 3^4$ будет рассмотрен подробно в параграфе 5.3. Следующие примеры представляют полуполевые плоскости порядка p^4, допускающие подгруппу автотопизмов $H \simeq Q_8$, для $p = 5$ и $p = 13$. Так как $p-1$ делится на 4, то матричное представление регулярного множества такой плоскости также состоит из матриц (3.1.6),

$$\theta(V,U) = \begin{pmatrix} m(U) & f(V) \\ V & U \end{pmatrix},$$

где $V \in Q$, $U \in K$, множества $Q, K \subset GL_2(p) \cup \{0\}$ замкнуты по сложению, содержат нулевую и единичную матрицы. Аддитивные взаимно однозначные отображения $m : K \to K$ и $f : Q \to Q$ не тождественны, инволютивны и удовлетворяют условиям $m(E) = E$, $f(E) \neq \pm E$.

Так как $|\pi| = p^4$, то Q и K – поля порядка p^2 в $GL_2(p) \cup \{0\}$. Тогда

$$K = \{xD + yE \mid x, y \in \mathbb{Z}_p\}, \quad Q = \{xC + yE \mid x, y \in \mathbb{Z}_p\}, \quad D, C \in GL_2(p),$$

причем все ненулевые матрицы этих множеств невырожденные. Линейные отображения m и f с условиями выше записываются как

$$\begin{aligned} &m(xD + yE) = xM + yE, && M \in K; \\ &f(xC + yE) = xF_1 + yF_2, && F_1, F_2 \in Q,\ F_2 \neq \pm E,\ M \neq D. \end{aligned}$$

Для случаев $p = 5$ и $p = 13$ можно считать, что $D = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$, т.к. 2 не является квадратом в $\mathbb{Z}_5$ и $\mathbb{Z}_{13}$. Матрица $C = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}$ будет подбираться с условием: $a^2 + 4b$ не является квадратом. Матрицы $M \in K$, $F_1, F_2 \in Q$ запишем в виде

$$M = \begin{pmatrix} m_2 & 2m_1 \\ m_1 & m_2 \end{pmatrix}, \quad F_1 = \begin{pmatrix} af_1 + f_2 & bf_1 \\ f_1 & f_2 \end{pmatrix}, \quad F_1 = \begin{pmatrix} af_3 + f_4 & bf_3 \\ f_3 & f_4 \end{pmatrix}.$$

Из условий $m(m(U)) \equiv U$ и $f(f(V)) \equiv V$ следует:

$$\begin{aligned} &m_1^2 = 1, && f_1^2 + f_2 f_3 = 1, \\ &m_1 m_2 + m_2 + 1 = 0; && f_3(f_1 + f_4) = 0, \\ & && f_2(f_1 + f_4) = 0, \\ & && f_4^2 + f_2 f_3 = 1. \end{aligned} \tag{4.1.4}$$

Выбрав все матрицы $M, F_1, F_2 \in GL_2(p)$, удовлетворяющие условиям (4.1.4), поставим требование невырожденности ненулевой матрицы регулярного множества:

$$\begin{vmatrix} zM + tE & xF_1 + yF_2 \\ xC + yE & zD + tE \end{vmatrix} \neq 0, \quad \forall x, y, z, t \in \mathbb{Z}_p, \tag{4.1.5}$$

кроме случая $(x, y, z, t) = (0, 0, 0, 0)$.

Компьютерные расчеты приводят к следующему результату: существует 36 наборов коэффициентов $(a, b, m_1, m_2, f_1, f_2, f_3, f_4)$, удовлетворяющих условию (4.1.5) для $\mathbb{Z}_5$, и 396 наборов – для $\mathbb{Z}_{13}$. Таким образом, построено 36 полуполевых плоскостей порядка 5^4, допускающих подгруппу автотопизмов $H \simeq Q_8$ (возможно, изоморфных), и 396 плоскостей порядка 13^4 с этим свойством. Отметим, что в обоих случаях наблюдается $Q = K$, т.е. $a = 0$ и $b = 2$.

Решая вопрос о разбиении множества построенных плоскостей на классы изоморфизма, определим вид матриц перехода $\delta = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ к новому базису 8-мерного линейного пространства, сохраняющих подгруппу H. Возможны

случаи:

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & k_1 A_1 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & A_1 \\ k_2 A_1 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} A_1 & k_1 A_1 \\ k_2 A_1 & -k_1 k_2 A_1 \end{pmatrix},$$

где $k_1, k_2 \in \{1, -1, i, -i\}$, $A_1 \in N_{GL_2(p)}(K^*)$, для матрицы B аналогично. Здесь $i \in \mathbb{Z}_p$ и $i^2 = -1$, как указано в теореме 3.7.1. Окончательный список неизоморфных плоскостей порядка 13^4 приведен в табл. 7, где строка коэффициентов $(m_1, m_2, f_1, f_2, f_3, f_4)$ обозначена (m, f). Для порядка 5^4 получено три набора коэффициентов:

$$(4, 0, 2, 1, 2, 3), \quad (4, 0, 2, 2, 1, 3) \quad (4, 1, 2, 3, 4, 3),$$

задающих все попарно неизоморфные плоскости. В случае, когда матрица δ задает переход к исходной плоскости, в качестве дополнительного результата компьютерных вычислений мы получаем нормализатор и централизатор подгруппы H в группе автотопизмов Λ. Итогом всех расчетов служит теорема.

Теорема 4.1.2. *1. Существуют ровно три, с точностью до изоморфизма, полуполевых плоскости порядка 5^4, группа автотопизмов Λ которых содержит подгруппу H, изоморфную группе кватернионов Q_8. При этом $C_\Lambda(H) = \mathbb{Z}_{24} \times \mathbb{Z}_4$, $|N_\Lambda(H)| = 384$.*

2. Существуют ровно 33, с точностью до изоморфизма, полуполевых плоскости порядка 13^4, группа автотопизмов Λ которых содержит подгруппу H, изоморфную группе кватернионов Q_8. При этом $C_\Lambda(H) = \mathbb{Z}_{168} \times \mathbb{Z}_{12}$, $|N_\Lambda(H)| = 8064$.

Таблица 7. Наборы коэффициентов при $p = 13$

№	(m, f)	№	(m, f)	№	(m, f)
1	(12,0,3, 1, 5,10)	**2**	(12,0,3, 2, 9,10)	**3**	(12,0,3, 3, 6,10)
4	(12,0,3, 4,11,10)	**5**	(12,0,3, 5, 1,10)	**6**	(12,0,3, 6, 3,10)
7	(12,0,4, 1,11, 9)	**8**	(12,0,4, 2,12, 9)	**9**	(12,0,4, 3, 8, 9)
10	(12,0,4, 4, 6, 9)	**11**	(12,0,4, 5,10, 9)	**12**	(12,0,4, 6, 4, 9)
13	(12,0,5, 1, 2, 8)	**14**	(12,0,5, 2, 1, 8)	**15**	(12,0,5, 3, 5, 8)
16	(12,0,5, 4, 7, 8)	**17**	(12,0,5, 5, 3, 8)	**18**	(12,0,5, 6, 9, 8)
19	(12,1,2, 9, 4,11)	**20**	(12,1,3, 4,11,10)	**21**	(12,1,4, 1,11, 9)
22	(12,1,4, 6, 4, 9)	**23**	(12,1,4,11, 1, 9)	**24**	(12,1,5, 2, 1, 8)
25	(12,1,6, 6, 5, 7)	**26**	(12,2,3, 4,11,10)	**27**	(12,2,3, 5, 1,10)
28	(12,2,4, 2,12, 9)	**29**	(12,2,4,11, 1, 9)	**30**	(12,2,5, 1, 2, 8)
31	(12,2,5, 5, 3, 8)	**32**	(12,3,2, 9, 4,11)	**33**	(12,3,3, 6, 3,10)

Исследования полуполей порядка 5^4 и 13^4, координатизирующих описанные полуполевые плоскости, представлены в § 5.9, их результатом является теорема 5.8.3 и табл. 19,20.

4.2. Оптимизация выделения классов изоморфизма

Обсудим подробнее вопрос: *являются ли две полуполевые плоскости* π *и* π'*, заданные регулярными множествами* $R = \{\theta(x) \mid x \in W\}$ *и* $R' = \{\sigma(x) \mid x \in W\}$ *в* $GL_n(p) \cup \{0\}$*, изоморфными?* Здесь W – n-мерное линейное пространство над полем $\mathbb{Z}_p$, и изоморфизм плоскостей эквивалентен изотопизму полуполей $W_1 = W(n, p, \theta)$ и $W_2 = W(n, p, \sigma)$. Учитывая матричный критерий изоморфизма (см. [126, 128, 91]), перепишем вопрос в виде: *существуют ли такие матрицы* $P_1, P_2 \in GL_n(p)$*, что для каждой матрицы* $\theta(x) \in R$ *произведение* $P_1^{-1}\theta(x)P_2$ *принадлежит регулярному множеству* R'*?*

Оценим возможности прямого перебора вариантов и обсудим пути сокращения их необходимого количества. Например, пусть $|\pi| = |\pi'| = 3^4$, поэтому $P_1, P_2 \in GL_4(3)$. Тогда число возможных вариантов выбора двух матриц равно

$$|GL_4(3)|^2 = ((81-1)(81-3)(81-9)(81-27))^2 = 24261120^2 \approx 5,88 \cdot 10^{14}.$$

Далее, для $\theta(x) = E \in R$ имеем $P_1^{-1}P_2 = S_0 = \sigma(x_0) \in R'$, тогда $P_2 = P_1S_0$, т.е. достаточно рассматривать все возможные матрицы $P_1 \in GL_4(3)$ и все ненулевые матрицы S_0 из регулярного множества второй плоскости. Число вариантов при этом сокращается до

$$|GL_4(3)| \cdot (|R'| - 1) = 24261120 \cdot 80 \approx 1,94 \cdot 10^9,$$

хотя и остается неприемлемым для «быстрого» решения проблемы изоморфизма. Нам может помочь информация о порядках ядер координатизирующих полуполей, или, что эквивалентно (лемма 2.2.2), порядках ядер плоскостей π и π'. Рассмотрим, например, алгоритм отыскания среднего ядра и его последующее использование, в случае порядка более p.

Пусть, например, матрицы $A_1, \ldots, A_n \in GL_n(p)$ образуют базис регулярного множества R, и R_m – среднее ядро плоскости π. Тогда (см. § 1.4), матрица $M \in GL_n(p)$ принадлежит R_m в том и только в том случае, когда произведение $M\theta(x)$ также является элементом регулярного множества. Ясно, что это условие достаточно проверять только для произведений MA_i на базисные элементы (за исключением единичной матрицы) и строить разложение этого произведения по базису $A_1, \ldots, A_n$, если это возможно.

Построив ядра R_l, R_m, R_r плоскости π и ядра R'_l, R'_m, R'_r плоскости π', мы будем далее обсуждать возможный изоморфизм $\pi \simeq \pi'$ только в случае равенства порядков всех соответствующих ядер. Пусть $|R_l| = |R'_l|$, $|R_m| = |R'_m|$, $|R_r| = |R'_r|$ и хотя бы одно из ядер не изоморфно простому подполю $\mathbb{Z}_p$ полуполя W. Пусть, для определенности, $|R_m| > p$.

Замена базиса $2n$-мерного линейного пространства над $\mathbb{Z}_p$ с матрицей перехода $T = \begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}$ переводит группу автотопизмов Λ плоскости π в изо-

морфную ей группу автотопизмов $\Lambda' = T^{-1}\Lambda T$ плоскости π'. Рассмотрим, как при этом меняется матричное представление гомологий из подгрупп H_l, H_m, H_r (лемма 2.2.4). Если $h_r \in H_r$, то

$$T^{-1}h_rT = \begin{pmatrix} P_1^{-1} & 0 \\ 0 & P_2^{-1} \end{pmatrix} \begin{pmatrix} E & 0 \\ 0 & \theta(d) \end{pmatrix} \begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix} = \begin{pmatrix} E & 0 \\ 0 & P_2^{-1}\theta(d)P_2 \end{pmatrix} \in H'_r,$$

здесь $\theta(d) \in R_r$, поэтому имеем $P_2^{-1}R_rP_2 = R'_r$. Аналогично, рассматривая гомологии $h_m \in H_m$ и $h_l \in H_l$, получаем $P_1^{-1}R_mP_1 = R'_m$ и $P_1^{-1}R_lP_1 = P_2^{-1}R_lP_2 = R'_l$, или, эквивалентно,

$$P_1^{-1}MP_1 \in R'_m \quad \forall M \in R^*_m;$$

$$P_2^{-1}MP_2 \in R'_r \quad \forall M \in R^*_r;$$

$$P_1^{-1}MP_1 = P_2^{-1}MP_2 \in R'_l \quad \forall M \in R^*_l.$$

Эти условия окажутся бесполезными, если все ядра изоморфны $\mathbb{Z}_p$ – это самый сложный для проверки случай. Пусть, например, плоскости π и π' порядка 3^4 имеют среднее ядро порядка 9. Выберем матрицы M и M', порождающие мультипликативные группы R^*_m и R'^*_m соответственно, и перепишем условие $P_1^{-1}MP_1 \in R'_m$ как равенство $XM = M'X$, где $X = P_1^{-1}$ – искомая матрица. Это равенство представляет систему из 16 линейных однородных уравнений на 16 неизвестных. Если, например, ранг основной матрицы равен 8, то множество решений состоит из 5760 матриц $X = P_1^{-1}$. Вычисляя для каждого варианта матрицы P_1 все матрицы $P_2 = P_1S_0$, получаем очень значительное уменьшение количества вариантов: с $24261120 \cdot 80$ до $5760 \cdot 80 = 460800$, т.е. в 4212 раз. Для каждого варианта матриц P_1 и P_2, проверяя основное условие изоморфизма для базисных элементов регулярного множества R:

$$P_1^{-1}A_iP_2 \in R', \quad i = 1, \ldots, n,$$

находим изоморфизмы из π на π' или доказываем, что $\pi \ncong \pi'$.

Для случаев большого правого либо большого левого ядра рассуждения аналогичные. Отметим дополнительно, что если обе полуполевые плоскости π и π' допускают фиксированную группу автотопизмов H, то прежде всего следует рассматривать матрицы T, нормализующие H.

4.3. 3-примитивные полуполевые плоскости

В этом параграфе изучены 3-примитивные полуполевые плоскости порядка 81 и построены новые примеры таких плоскостей, подробнее см. [140]. Результаты кратко представляет

Теорема 4.3.1. *Существуют ровно восемь, с точностью до изоморфизма, полуполевых плоскостей порядка 81, допускающих бэровскую инволюцию. Все они являются 3-примитивными и имеют разрешимую группу коллинеаций.*

Пусть π — полуполевая плоскость порядка p^{2n} с (левым) ядром $K \simeq GF(p^s)$, где p – простое число. Коллинеация β плоскости π называется *p-примитивной бэровской коллинеацией*, если она фиксирует бэровскую подплоскость поточечно и ее порядок есть p-примитивный делитель $p^n - 1$ (то есть $|\beta| \mid (p^n - 1)$, но $|\beta| \nmid (p^i - 1)$, $i < n$). Полуполевая плоскость порядка p^{2n} называется *p-примитивной полуполевой плоскостью*, если она допускает p-примитивную бэровскую коллинеацию.

Первая работа, посвященная изучению p-примитивных полуполевых плоскостей, была опубликована в 1987 году. В этой работе Й. Хирамин, М. Мацумото и Т. Ояма начали изучение плоскостей ранга 2. Они предложили идею построения регулярного множества и получили некоторые свойства группы коллинеаций таких плоскостей [62]. Изучение p-примитивных полуполевых плоскостей было продолжено Н. Джонсоном в статьях [74, 75]. В частности, в [75] он доказал, что порядок p-примитивной полуполевой плоскости π ранга 2 равен q^4 ($q = p^r$) и записал матричное представление регулярного множества плоскости. В работах [35, 36] М. Кордеро нашла матричное представление всех автотопизмов и доказала разрешимость группы автотопизмов в частном случае при $q = p$. М. Кордеро построила [37] матричное представление регулярного множества p-примитивной полуполевой плоскости порядка p^{2n} с ядром порядка p^n и привела примеры четырех попарно неизоморфных 3-примитивных полуполевых плоскостей порядка 81 с ядром $GF(9)$. Если π – p-примитивная полуполевая плоскость порядка $q^4 = p^{2n}$ с ядром $GF(q^2)$, то базис 4-мерного линейного пространства над $GF(q^2)$ может быть выбран так, что регулярное множество плоскости π в $GL_2(q^2) \cup \{0\}$ имеет вид

$$\Sigma_0 = \left\{ \begin{pmatrix} u^q & f(v) \\ v & u \end{pmatrix} \;\middle|\; u, v \in GF(q^2) \right\}. \tag{4.3.1}$$

Здесь и далее при ссылках на разные источники выбраны единообразные обозначения.

И. В. Шевелевой (Бусаркиной) описан [12] общий случай p-примитивной полуполевой плоскости с ядром произвольного порядка p^s: построено матричное представление регулярного множества, доказана разрешимость группы коллинеаций, описано ее строение. Перечислим некоторые из результатов.

Лемма 4.3.2. *Пусть π – полуполевая плоскость порядка q^4 с ядром $K \simeq GF(p^s)$ ($q = p^r$, $q^4 = (p^s)^{2n}$, $p > 2$ – простое число), допускающая линейную*

бэровскую коллинеацию σ порядка $q+1$. Тогда π может быть представлена $4n$-мерным векторным пространством над K так, что ее регулярное множество $\Sigma \subset GL_{2n}(K) \cup \{0\}$ имеет вид

$$\Sigma = \left\{ \begin{pmatrix} U^q & f(V) \\ V & U \end{pmatrix} \;\middle|\; U, V \in F \right\}, \tag{4.3.2}$$

где $F \subset GL_n(K) \cup \{0\}$, $F \simeq GF(q^2)$, f – аддитивная взаимно однозначная функция из F в $GL_n(K) \cup \{0\}$. Подгруппа бэровских коллинеаций $\langle\sigma\rangle$ в этом случае записывается как

$$Q = \langle\sigma\rangle = \left\{ \begin{pmatrix} E & 0 & 0 & 0 \\ 0 & C^m & 0 & 0 \\ 0 & 0 & C^m & 0 \\ 0 & 0 & 0 & E \end{pmatrix} \;\middle|\; C \in F,\ |C| = q+1,\ m = 1, 2, \ldots, q+1 \right\}. \tag{4.3.3}$$

Элементы матриц здесь и всюду далее представляют собой квадратные блоки-подматрицы одинаковой размерности, E – единичная матрица.

Далее, в [13] рассмотрен следующий частный случай.

Пусть π – полуполевая плоскость порядка q^4 с ядром $K \simeq GF(p^s)$ ($q = p^r$, $q^4 = (p^s)^{2n}$, $p > 2$ – простое число), регулярное множество которой в $GL_{2n}(K) \cup \{0\}$ имеет вид

$$\Sigma_1 = \left\{ \begin{pmatrix} U^q & \tau\varphi(V) \\ V & U \end{pmatrix} \;\middle|\; U, V \in F \right\}, \tag{4.3.4}$$

где φ – аддитивная взаимно однозначная функция из F в F, $\tau \notin F$ нормализует F.

Лемма 4.3.3. *2-ранг группы линейных автотопизмов Λ_0 плоскости π с регулярным множеством Σ_1 равен трем или четырем.*

Лемма 4.3.4. *Нормализатор подгруппы Q (4.3.3) в группе линейных автотопизмов Λ_0 содержит ровно 7 инволюций:*

$$h_1 = \begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix}, \quad h_2 = \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix}, \quad h_3 = \begin{pmatrix} -E & 0 \\ 0 & -E \end{pmatrix},$$

$$h_4 = \begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix}, \quad h_5 = \begin{pmatrix} L & 0 \\ 0 & -L \end{pmatrix}, \quad h_6 = \begin{pmatrix} -L & 0 \\ 0 & L \end{pmatrix}, \quad h_7 = \begin{pmatrix} -L & 0 \\ 0 & -L \end{pmatrix},$$

где $L = \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix} \in GL_{2n}(K)$, причем h_1, h_2, h_3 – гомологии, h_4, h_5, h_6, h_7 – бэровские инволюции.

Теорема 4.3.5. *Пусть π – полуполевая плоскость порядка q^4 с регулярным множеством Σ_1. Тогда группа коллинеаций плоскости π разрешима.*

Заметим, что при $p > 2$ некоторая степень p-примитивной бэровской коллинеации является бэровской инволюцией, и применим теорему 3.1.2 о матричном представлении бэровской инволюции и теорему 3.1.5 о матричном представлении регулярного множества.

Найдем, с точностью до изоморфизма, все полуполевые плоскости порядка 81, допускающие бэровскую инволюцию [131]. Обозначим регулярное множество такой плоскости π в $GL_4(3) \cup \{0\}$ через

$$\Sigma_2 = \left\{ \theta(V,U) = \begin{pmatrix} m(U) & f(V) \\ V & U \end{pmatrix} \;\middle|\; U \in K_1,\ V \in K_2 \right\}, \tag{4.3.5}$$

здесь K_1 и K_2 – регулярные множества в $GL_2(3) \cup \{0\}$, m, f – инъективные линейные отображения из K_1 и K_2 соответственно в $GL_2(3) \cup \{0\}$, причем $m(E) = E$, $f(E) \neq E$. Так как плоскость имеет ранг 4, то $K_1 = K_2 = F \simeq GF(9)$ (лемма 3.1.6). Без потери общности полагаем далее $D = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$,

$$F = \{U = u_1 D + u_2 E \mid u_1, u_2 \in \mathbb{Z}_3\}, \tag{4.3.6}$$

D, E – базис F. Линейные функции m и f представимы в виде

$$m(u_1 D + u_2 E) = u_1 M + u_2 E, \qquad f(u_1 D + u_2 E) = u_1 F_1 + u_2 F_2$$

для каждого $U = u_1 D + u_2 E \in F$. Здесь $M, F_1, F_2 \in GL_2(3)$, $m(E) = E$, $F_2 = f(E) \neq E$. Регулярное множество Σ_2 является 4-мерным линейным пространством над $\mathbb{Z}_3$ с базисом, например,

$$\theta(D,0) = \begin{pmatrix} 0 & F_1 \\ D & 0 \end{pmatrix}, \quad \theta(E,0) = \begin{pmatrix} 0 & F_2 \\ E & 0 \end{pmatrix},$$

$$\theta(0,D) = \begin{pmatrix} M & 0 \\ 0 & D \end{pmatrix}, \quad \theta(0,E) = \begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix}.$$

Если матрицы M, F_1, F_2 выбраны так, что для всех $x, y, z, t \in \mathbb{Z}_3$ матрица

$$\theta(xD + yE, zD + tE) = \begin{pmatrix} zM + tE & xF_1 + yF_2 \\ xD + yE & zD + tE \end{pmatrix} =$$

$$= x \begin{pmatrix} 0 & F_1 \\ D & 0 \end{pmatrix} + y \begin{pmatrix} 0 & F_2 \\ E & 0 \end{pmatrix} + z \begin{pmatrix} M & 0 \\ 0 & D \end{pmatrix} + t \begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix}$$

является либо нулевой (при $x = y = z = t = 0$), либо невырожденной, то тройка матриц M, F_1, F_2 задает полуполевую плоскость π, удовлетворяющую указанным условиям.

С использованием компьютера получено 106 наборов матриц M, F_1, F_2, т.е. построено 106 полуполевых плоскостей порядка 81, допускающих бэровскую инволюцию в трансляционном дополнении. Для каждой из построенных плоскостей были найдены левое, правое и среднее ядра координатизирующих полуполей. Выделены следующие случаи:

$$
\begin{aligned}
&1)\ |N_l| = |N_m| = 3,\ |N_r| = 9;\\
&2)\ |N_l| = |N_r| = 3,\ |N_m| = 9;\\
&3)\ |N_m| = |N_r| = 3,\ |N_l| = 9;\\
&4)\ |N_l| = |N_m| = |N_r| = 9;\\
&5)\ |N_l| = |N_m| = |N_r| = 81.
\end{aligned}
$$

В случае 5, очевидно, построенная плоскость является дезарговой.

Разобьем построенные плоскости на классы изоморфизма, используя замену базиса 8-мерного линейного пространства, сохраняющую бэровскую инволюцию τ (3.1.3). При этом матрица перехода $\begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}$ состоит из блочно-диагональных подматриц P_1 и P_2. Использование такой матрицы перехода выделяет 16 классов попарно изоморфных плоскостей порядка 81, считая дезаргову.

Следующий этап расчетов должен устанавливает наличие изоморфизма между плоскостями из разных выделенных классов, без требования сохранения бэровской инволюции τ. С помощью компьютерных программ в каждом из случаев найдены все матрицы, задающие изоморфизмы построенных плоскостей, и, для $R' = R$ – автотопизмы каждой плоскости. Окончательно имеем восемь попарно неизоморфных недезарговых плоскостей порядка 81, т.е. восемь классов изоморфизма.

Эти расчеты показали, что группа автотопизмов Λ в каждом случае является 2-группой порядка 2^m, $8 \leqslant m \leqslant 11$, откуда немедленно следует ее разрешимость и, следовательно, разрешимость группы коллинеаций.

Матрицы, задающие регулярные множества неизоморфных плоскостей, приведены ниже в табл. 9. Перечислять элементы групп автотопизмов не представляется целесообразным.

Вычисление порядков автотопизмов для каждой из восьми неизоморфных плоскостей показывает, что каждая плоскость допускает 7 автотопизмов порядка 2, в соответствии со списком леммы 4.3.4. Кроме того, порядок любого

автотопизма не превышает 16. Из общего списка выделены бэровские коллинеации, информация об элементах группы Λ представлена в табл. 8.

Таблица 8. Автотопизмы 3-примитивных полуполевых плоскостей

Плоскость	$\lvert N_l\rvert$, $\lvert N_m\rvert$, $\lvert N_r\rvert$	$\lvert\Lambda\rvert$	n_2	B_2	n_4	B_4	n_8	n_{16}
A1	3,3,9	256	7	4	88	4	32	128
A2	3,3,9	512	7	4	216	4	160	128
B1	3,9,3	256	7	4	88	4	32	128
B2	3,9,3	512	7	4	216	4	160	128
C1	9,3,3	256	7	4	88	4	32	128
C2	9,3,3	512	7	4	216	4	160	128
D1	9,9,9	1024	7	4	56	8	192	768
D2	9,9,9	2048	103	100	600	8	576	768

Здесь n_k – число автотопизмов порядка k; B_k – число бэровских коллинеаций порядка k, причем $B_k = 0$ для $k > 4$, $n_k = 0$ для $k > 16$. Так как $B_4 \neq 0$ для каждой из восьми плоскостей, то все они являются 3-примитивными, причем случай $N_l \simeq \mathbb{Z}_3$ представляет четыре новых примера, в сравнении с работой [37] М. Кордеро.

Так как плоскости 3-примитивны, перепишем их регулярное множество в виде Σ (4.3.2). Для этого должно выполняться условие $m(U) = U^3$ для всех $U \in F$, поэтому отберем в каждом классе изоморфизма плоскость с $M = D^3 = \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}$. табл. 9 представляет матрицы F_1 и F_2, задающие функцию $f(V)$ для выбранных плоскостей.

Выделим далее в общем списке полуполевые плоскости с регулярным множеством вида Σ_1 (4.3.4). Для этого перепишем аддитивную функцию $f(V)$ в другом виде.

Лемма 4.3.6. *Пусть p – простое число, $F \simeq GF(p^n)$, $\mathcal{R}$ – ассоциативное кольцо с единицей, содержащее подполе F. Произвольную аддитивную функцию $f : F \to \mathcal{R}$ можно представить, причем однозначно, в виде*

$$f(x) = A_0 x + A_1 x^p + A_2 x^{p^2} + \cdots + A_{n-1} x^{p^{n-1}}, \quad x \in F, \tag{4.3.7}$$

где $A_0, A_1, \ldots, A_{n-1} \in \mathcal{R}$.

Доказательство. Пусть u – порождающий элемент мультипликативной группы поля F, тогда минимальный многочлен u над $\mathbb{Z}_p$ является неприводимым многочленом степени n. Поэтому $1, u, u^2, \ldots, u^{n-1}$ линейно независимы как элементы n-мерного линейного пространства F над $\mathbb{Z}_p$.

Так как функция f аддитивна, то она является линейным отображением из линейного пространства F над $\mathbb{Z}_p$ в $\mathcal{R}$. Следовательно, f однозначно определяется образами базисных элементов $1, u, u^2, \ldots, u^{n-1}$. Используя (4.3.7), составим систему линейных уравнений относительно неизвестных A_i:

$$\begin{cases} A_0 + A_1 + A_2 + \cdots + A_{n-1} = f(1), \\ A_0 u + A_1 u^p + A_2 u^{p^2} + \cdots + A_{n-1} u^{p^{n-1}} = f(u), \\ A_0 u^2 + A_1 u^{2p} + A_2 u^{2p^2} + \cdots + A_{n-1} u^{2p^{n-1}} = f(u^2), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ A_0 u^{n-1} + A_1 u^{(n-1)p} + A_2 u^{(n-1)p^2} + \cdots + A_{n-1} u^{(n-1)p^{n-1}} = f(u^{n-1}). \end{cases} \tag{4.3.8}$$

Основной определитель этой системы

$$\Delta = \begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ u & u^p & u^{p^2} & \ldots & u^{p^{n-1}} \\ u^2 & u^{2p} & u^{2p^2} & \ldots & u^{2p^{n-1}} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ u^{n-1} & u^{(n-1)p} & u^{(n-1)p^2} & \ldots & u^{(n-1)p^{n-1}} \end{vmatrix}$$

является определителем Вандермонда и равен $\Delta = \prod\limits_{0 \leqslant j < i \leqslant n-1} (u^{p^i} - u^{p^j})$. По выбору u, определитель отличен от нуля, поэтому система имеет единственное решение в $\mathcal{R}$. Лемма доказана. □

В частности, это утверждение справедливо для кольца $(n \times n)$-матриц над $\mathbb{Z}_p$ и его подполя $F \subset GL_n(p) \cup \{0\}$.

Запишем для построенных полуполевых плоскостей функцию $f(V)$ в виде (4.3.7). Для наших построений

$$f(V) = f(xD + yE) = xF_1 + yF_2 = A_0 V + A_1 V^3.$$

Система (4.3.8) в этом случае имеет вид

$$\begin{cases} A_0 + A_1 = F_2, \\ A_0 D + A_1 D^3 = F_1, \end{cases}$$

откуда имеем $A_0 = F_1 \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} - F_2 \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}$, $A_1 = F_2 - A_0$. Вычисления по этим формулам приводят к результатам, перечисленным в табл. 9.

Таблица 9. Функция $f(V)$ для 3-примитивных плоскостей порядка 81

Плоскость	F_1	F_2	$f(V)$	Тип
A1	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}2&2\\1&2\end{pmatrix}$	$\begin{pmatrix}2&2\\1&2\end{pmatrix} V^3$	Σ
A2	$\begin{pmatrix}1&0\\2&2\end{pmatrix}$	$\begin{pmatrix}2&2\\2&1\end{pmatrix}$	$\begin{pmatrix}2&2\\2&1\end{pmatrix} V^3$	Σ_1
B1	$\begin{pmatrix}1&0\\1&1\end{pmatrix}$	$\begin{pmatrix}1&2\\2&0\end{pmatrix}$	$\begin{pmatrix}2&2\\2&1\end{pmatrix} V+2V^3$	Σ
B2	$\begin{pmatrix}1&0\\2&2\end{pmatrix}$	$\begin{pmatrix}0&1\\2&0\end{pmatrix}$	$\begin{pmatrix}0&1\\2&0\end{pmatrix} V$	Σ_1
C1	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&2\\2&2\end{pmatrix}$	$\begin{pmatrix}2&2\\2&0\end{pmatrix} V+2V^3$	Σ_0
C2	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&2\end{pmatrix}$	$\begin{pmatrix}0&1\\1&2\end{pmatrix} V$	Σ_0
D1	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}2&2\\2&0\end{pmatrix}$	$\begin{pmatrix}2&2\\2&0\end{pmatrix} V^3$	Σ_0
D2	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1&2\\2&2\end{pmatrix}$	$\begin{pmatrix}1&2\\2&2\end{pmatrix} V^3$	Σ_0

Если коэффициенты A_0, A_1 принадлежат полю F (плоскости C1, C2, D1, D2), то плоскость имеет регулярное множество вида Σ_0 (4.3.1), т.е. относится к типу Кордеро. Для плоскостей A2 и B2 ненулевой коэффициент функции $f(V)$ нормализует поле F (4.3.6), поэтому плоскости имеют регулярное множество вида Σ_1 (4.3.4). Плоскости A1 и B1 не допускают представления регулярного множества в виде Σ_1, они относятся к существенно новому типу.

Обозначим $C = D + E$ и выпишем подгруппы бэровских коллинеаций, порожденные 3-примитивными элементами. Каждая из плоскостей A1–D2 допускает подгруппу

$$Q = \left\langle \begin{pmatrix} E & 0 & 0 & 0 \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & E \end{pmatrix} \right\rangle$$

порядка 4 вида (4.3.3). Кроме Q, плоскости A1 и A2 допускают подгруппу

$$Q_1 = \left\langle \begin{pmatrix} E & 0 & 0 & 0 \\ 0 & C & 0 & 0 \\ 0 & 0 & E & 0 \\ 0 & 0 & 0 & C \end{pmatrix} \right\rangle,$$

плоскости B1 и B2 – подгруппу

$$Q_2 = \left\langle \begin{pmatrix} C & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & E \end{pmatrix} \right\rangle,$$

плоскости C1 и C2 – подгруппу

$$Q_3 = \left\langle \begin{pmatrix} C & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & E & 0 \\ 0 & 0 & 0 & C \end{pmatrix} \right\rangle,$$

плоскости D1 и D2 – подгруппы Q_1, Q_2, Q_3.

Таким образом, заключаем, что построены все попарно неизоморфные собственно полуполевые плоскости порядка 81, допускающие бэровскую инволюцию. Все они являются 3-примитивными, только четыре из построенных восьми плоскостей имеют левое ядро порядка 9 и изоморфны примерам М. Кордеро. Из оставшихся четырех новых плоскостей две плоскости обладают регулярным множеством вида Σ_1, две другие демонстрируют существование p-примитивных полуполевых плоскостей другого типа. Отметим, что особенности строения группы автотопизмов согласуются с доказанными в [12, 13, 131, 132] теоретическими результатами. Программное обеспечение, разработанное для построения представленных примеров, несложно адаптировать для другого основного поля $\mathbb{Z}_p$ или другой размерности пространства.

Полуполя $\mathcal{A}_1$–$\mathcal{D}_2$, координатизирующие полуполевые плоскости A1–D2, подробно исследованы в § 5.9.

Глава 5. Структурные вопросы для конечных полуполей

Глава 5 посвящена решению для некоторых конечных полуполей вопросов **(A)**–**(D)**. Вопросы полностью решены для полуполей порядка 16 — наименьший порядок нетривиальных полуполей, полуполей Кнута–Руа и Хентзела–Руа — контрпримеры порядков 32 и 64 к гипотезе Венэ [119], для некоторых полуполей порядков p^4 (p – простое).

В параграфах 5.1–5.3 представлена употребляемая специальная терминология и введены новые методы исследования полуполей, основанные на использовании регулярного множества и минимальных многочленов. Параграф 5.4 завершает решение вопросов для всех полуполей минимального порядка 16, начатое П. К. Штуккерт, с учетом новых методов исследования и дополнительной информации о минимальных многочленах и внутренних автоморфизмах. Параграфы 5.5–5.8 посвящены обсуждению гипотезы Г. Венэ и исследованию исключительных непримитивных полуполей Кнута–Руа порядка 32 и Хентзела–Руа порядка 64. Параграф 5.9 представляет решение вопросов для некоторых полуполей порядка p^4 ($p > 2$ – простое), построенных при наличии дополнительных ограничений на автотопизмы.

5.1. Автоморфизмы и автотопизмы конечных полуполей

В этом параграфе применяется подход с использованием регулярного множества, чтобы установить связь между преобразованиями конечных полуполей и коллинеациями ассоциированных полуполевых проективных плоскостей. Мы обсуждаем также проблему классификации конечных полуполей.

Напомним, что полуполе, в соответствии с определением 1.1.4, есть квазиполе, в котором выполнены оба дистрибутивных закона, т.е. это алгебраическая система, удовлетворяющая всем аксиомам тела, за исключением (возможно) ассоциативности умножения. Ясно, что конечное ассоциативное полуполе, в соответствии с теоремой Веддерберна, является конечным полем, поэтому далее мы говорим о нетривиальных (т.е. неассоциативных) полуполях.

Первые примеры нетривиальных полуполей предложил Л. Диксон [47] еще в 1906 г., эти коммутативные полуполя будут рассмотрены подробнее в следующем параграфе.

Минимальный возможный порядок нетривиального полуполя указал Д. Кнут [81].

Теорема 5.1.1. *Собственное полуполе порядка p^n для простого p существует в том и только в том случае, когда $n \geq 3$ и $p^n \geq 16$.*

В 2003 г. У. Кантор [77] записал: «Исследование конечных коммутативных полуполей было начато Диксоном почти столетие назад ... Удивительно, что до сих пор о них так мало известно». Полная классификация конечных полуполей пока отсутствует. В обзоре М. Лаврау и О. Полверино [84] перечислены некоторые классификационные результаты, в том числе следующая теорема 5.1.2. Первое из ее утверждений доказано Л. Диксоном, второе и третье – Д. Меничетти [89, 90] .

Теорема 5.1.2. *1. Конечное полуполе размерности 2 над своим центром есть конечное поле.*

2. Полуполе порядка q^3 с центром, содержащим $GF(q)$, является полем либо изотопно обобщенному скрученному полю.

3. Пусть S – полуполе простой размерности над своим центром $GF(q)$. Если q достаточно велико, то S является полем либо изотопно обобщенному скрученному полю.

К настоящему моменту перечислены [84] 28 классов известных конечных полуполей. Полуполя малых порядков 2^4, 2^5, 2^6, 3^4 и 3^5 полностью классифицированы с использованием компьютерной техники (Э. Клейнфелд, Р. Уолкер,

И. Руа и др., [102, 101, 103, 44, 80]). У. Кантор [78] предположил, что количество попарно неизоморфных полуполей порядка N не ограничено никаким многочленом от N.

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

Определение 5.1.3. *Полуполя* $(S,+,*)$ *и* $(W,+,\circ)$ *называются изотопными, если существует тройка* $\langle\alpha,\beta,\gamma\rangle$ *изоморфизмов аддитивной группы* $(S,+)$ *на аддитивную группу* $(W,+)$*, удовлетворяющая условию*

$$x^\alpha \circ y^\beta = (x*y)^\gamma \qquad \forall x,y \in S.$$

Такая тройка называется изотопизмом.

При $S=W$ изотопизм называют *автотопизмом* полуполя S. Если $\alpha=\beta=\gamma$, то изотопизм есть изоморфизм.

Обозначим $[S]$ класс всех полуполей, изотопных полуполю S. А. Альбертом [24] показана эквивалентность класса изоморфизма полуполевых проективных плоскостей и класса изотопизма полуполей (теорема 1.2.13).

М. Ганли и В. Джа [52] подтверждено предположение М. Каллахера и Р. Либлера [76] о возможной мощности любого класса изотопизма: для конечной полуполевой плоскости π число неизоморфных полуполей, координатизирующих π, не менее пяти. Заметим, что принято также группировать конечные полуполя в более крупные семейства – так называемые *орбиты Кнута*.

Пусть $(S,+,*)$ – полуполе порядка p^n, его можно представить n-мерным линейным пространством над $\mathbb{Z}_p$ с базисом $e_1,\dots,e_n$. Тогда умножение $*$ достаточно определить на базисных элементах: если $x = x_1e_1+\dots+x_ne_n$ и $y = y_1e_1+\dots+y_ne_n$ $(x_i,y_i\in\mathbb{Z}_p,\ i=1,\dots,n)$, то

$$x*y = \sum_{i,j=1}^{n} x_iy_j(e_i*e_j) = \sum_{i,j=1}^{n} x_iy_j\left(\sum_{k=1}^{n} a_{ijk}e_k\right),$$

где $a_{ijk}\in\mathbb{Z}_p$ – структурные константы S относительно базиса $e_1,\dots,e_n$ (см. также лемму 2.1.5). Эти коэффициенты образуют так называемый *кубический массив, или гиперкуб*. Д. Кнут [82] показал, что действие симметрической группы S_3 на индексах i, j, k элементов гиперкуба позволяет перейти к полуполю, в общем случае отличному от S, и возможно, даже не изотопному. Это действие распространяется на классы изотопизма, шесть таких классов образуют орбиту Кнута

$$\mathcal{K}(S) = \{[S],[S]^{(12)},[S]^{(13)},[S]^{(23)},[S]^{(123)},[S]^{(132)}\}.$$

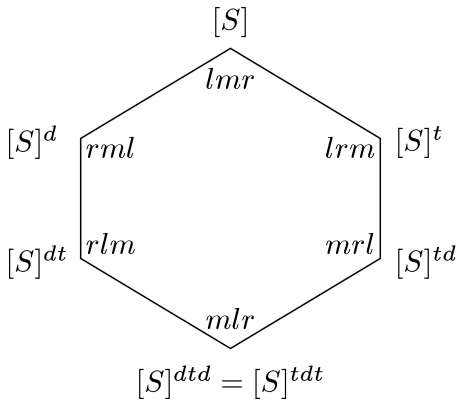

Рис. 3: Орбита Кнута полуполя S с ядрами lmr

Если полуполе S координатизирует полуполевую плоскость π, то дуальная плоскость π^d координатизируется полуполем $S^d = S^{(12)} = S^{op}$, противоположным к S.

Напомним, что биективное отображение φ из полуполя $(S, +, *)$ на полуполе $(W, +, \circ)$ называется *антиизоморфизмом*, если

$$(x + y)^\varphi = x^\varphi + x^\varphi, \quad (x * y)^\varphi = y^\varphi \circ x^\varphi \quad \forall x, y \in S.$$

Для любого полуполя $S = (S, +, *)$ *противоположное* полуполе $S^{op} = (S, +, \circ)$ определяется правилом $a \circ b = b * a$ $(a, b \in R)$. Ясно, что полуполя S^{op} и S антиизоморфны.

Далее, полуполе $S^{(23)}$ может быть получено транспонированием матриц, соответствующих отображениям $L_{e_i} : x \to e_i * x$ $(x \in S)$. Это полуполе S^t также называют *транспонированным* к S. Описание действия S_3 на орбите Кнута завершает [84] следующая диаграмма (см. рис. 3).

Левое, правое и среднее ядра N_l, N_r, N_m полуполя S не сохраняются произвольным изотопизмом, инвариантны лишь их порядки. Действие S_3, как показывает диаграмма, переставляет ядра. Следует заметить, что свойства полуполей, изучаемые в вопросах **(A)**–**(D)**, в общем случае не сохраняются при изотопизмах и тем более при действии S_3.

Мы будем рассматривать полуполе $W = (W, +, *)$ порядка p^n как линейное пространство над простым подполем $\mathbb{Z}_p$ (см. лемму 2.1.5). В этом случае регулярное множество

$$R = \{\theta(x) \mid x \in W\} \subset GL_n(p) \cup \{0\}, \tag{5.1.1}$$

в силу замкнутости по сложению (лемма 2.1.2), также является n-мерным линейным пространством над $\mathbb{Z}_p$. Закон умножения $x * y = x\theta(y)$ достаточно определить только для базисных элементов $e_1, \ldots, e_n$ полуполя W:

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

Все коэффициенты a_{ijk} $(i,j,k=1,\ldots,n)$ образуют кубический массив (гиперкуб Кнута), который представляет совокупность $n\times n$-матриц $A_1,\ldots,A_n$, образующих базис R. Далее для обозначения полуполя W порядка p^n с регулярным множеством (5.1.1) часто будем использовать $W=W(n,p,\theta)$.

Пример 5.1. Рассмотрим *коммутативное полуполе Диксона* порядка 81 и составим его регулярное множество в $GL_4(3)\cup\{0\}$.

Пусть $F=GF(p^2)$, σ – автоморфизм поля F и a – элемент F, не являющийся квадратом. Тогда множество $S=\{x+\lambda y \mid x,y\in F\}$ со сложением

$$(x+\lambda y)+(z+\lambda t)=(x+z)+\lambda(y+t)$$

и умножением

$$(x+\lambda y)(z+\lambda t)=(xz+ay^\sigma t^\sigma)+\lambda(yz+xt)$$

есть коммутативное полуполе (теорема 9.12, [68]).

Полагаем $F\simeq\mathbb{Z}_3[x]/(x^2-x-1)$,

$$F=\{0,1,-1,\alpha,\alpha+1,\alpha-1,-\alpha,-\alpha+1,-\alpha-1\},\qquad \alpha^2=\alpha+1,$$

и выбираем $a=\alpha$, $x^\sigma=x^3$, тогда закон умножения определен как

$$(x+\lambda y)(z+\lambda t)=(xz+\alpha y^3t^3)+\lambda(yz+xt).$$

Далее, выберем базис $1,\alpha,\lambda,\lambda\alpha$ в S и вычислим все произведения на базисные элементы:

$$\begin{array}{cccc}
1\cdot 1=1 & 1\cdot\alpha=\alpha & 1\cdot\lambda=\lambda & 1\cdot\lambda\alpha=\lambda\alpha\\
\alpha\cdot 1=\alpha & \alpha\cdot\alpha=\alpha+1 & \alpha\cdot\lambda=\lambda\alpha & \alpha\cdot\lambda\alpha=\lambda\alpha+\lambda\\
\lambda\cdot 1=\lambda & \lambda\cdot\alpha=\lambda\alpha & \lambda\cdot\lambda=\alpha & \lambda\cdot\lambda\alpha=-1\\
\lambda\alpha\cdot 1=\lambda\alpha & \lambda\alpha\cdot\alpha=\lambda\alpha+\lambda & \lambda\alpha\cdot\lambda=-1 & \lambda\alpha\cdot\lambda\alpha=\alpha-1
\end{array}$$

Пусть W – 4-мерное линейное пространство над $\mathbb{Z}_3$ и

$$f_1=(1,0,0,0),\ f_2=(0,1,0,0),\ f_3=(0,0,1,0),\ f_4=(0,0,0,1)$$

– канонический базис. Используя соответствие

$$1\to f_1,\ \alpha\to f_2,\ \lambda\to f_3,\ \lambda\alpha\to f_4,$$

найдем матрицы $\theta(f_2)$, $\theta(f_3)$, $\theta(f_4)$ ($\theta(f_1) = E$):

$$\begin{aligned}
&f_1 \circ f_2 = f_1\theta(f_2) = f_2,\\
&f_2 \circ f_2 = f_2\theta(f_2) = f_2 + f_1,\\
&f_3 \circ f_2 = f_3\theta(f_2) = f_4,\\
&f_4 \circ f_2 = f_4\theta(f_2) = f_3 + f_4,
\end{aligned} \qquad \theta(f_2) = \begin{pmatrix} 0 & 1 & 0 & 0\\ 1 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 1 \end{pmatrix};$$

$$\begin{aligned}
&f_1 \circ f_3 = f_1\theta(f_3) = f_3,\\
&f_2 \circ f_3 = f_2\theta(f_3) = f_4,\\
&f_3 \circ f_3 = f_3\theta(f_3) = f_2,\\
&f_4 \circ f_3 = f_4\theta(f_3) = -f_1,
\end{aligned} \qquad \theta(f_3) = \begin{pmatrix} 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0 \end{pmatrix};$$

$$\begin{aligned}
&f_1 \circ f_4 = f_1\theta(f_4) = f_4,\\
&f_2 \circ f_4 = f_2\theta(f_4) = f_3 + f_4,\\
&f_3 \circ f_4 = f_3\theta(f_4) = -f_1,\\
&f_4 \circ f_4 = f_4\theta(f_4) = -f_1 + f_2,
\end{aligned} \qquad \theta(f_4) = \begin{pmatrix} 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 1\\ -1 & 0 & 0 & 0\\ -1 & 1 & 0 & 0 \end{pmatrix}.$$

Таким образом, регулярное множество $R \subset GL_4(3) \cup \{0\}$ состоит из всех матриц

$$\theta(y_1, y_2, y_3, y_4) = y_1 \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 \end{pmatrix} + y_2 \begin{pmatrix} 0 & 1 & 0 & 0\\ 1 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 1 \end{pmatrix} +$$
$$+ y_3 \begin{pmatrix} 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0 \end{pmatrix} + y_4 \begin{pmatrix} 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 1\\ -1 & 0 & 0 & 0\\ -1 & 1 & 0 & 0 \end{pmatrix}.$$

Непосредственно проверяется, что для любого ненулевого вектора y матрица $\theta(y)$ невырожденная. Таким образом, построено представление коммутативного полуполя Диксона порядка 81 над $\mathbb{Z}_3$.

В предыдущих рассуждениях мы использовали первую строку для определения матрицы из регулярного множества. Очевидно, любая другая строка или любой столбец задают другой закон умножения и, следовательно, другое полуполе, не обязательно изоморфное первому.

Пример 5.2. Например, в списке У. Демпволфа [44] полуполей порядка 81 выберем первое из 12 представленных регулярных множеств. Его базисные

элементы следующие:

$$E, \quad B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 2 & 0 & 0 & 2 \\ 2 & 2 & 2 & 2 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 2 & 2 \\ 1 & 1 & 2 & 2 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 2 & 2 & 2 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}.$$

Зададим отображение θ правилом

$$\theta(y_1, y_2, y_3, y_4) = y_1E + y_2B + y_3C + y_4D,$$

т.е. определим матрицу ее первой строкой. Получим полуполе $\langle W, +, * \rangle$, которое содержит подполе $\{(y_1, y_2, 0, 0) \mid y_1, y_2 \in \mathbb{Z}_3\}$ порядка 9.

Далее рассмотрим другой базис для того же регулярного множества R:

$$B' = \begin{pmatrix} 1 & 2 & 0 & 2 \\ 2 & 0 & 1 & 0 \\ 2 & 1 & 2 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad C' = \begin{pmatrix} 2 & 2 & 2 & 1 \\ 2 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad D' = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 2 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad E;$$

где, очевидно, $B' = 1 \cdot E + 2 \cdot B + 0 \cdot C + 2 \cdot D$ и т.д. При этом мы сопоставляем матрицу регулярного множества ее четвертой строке и получаем другое отображение $\sigma : W \to R$,

$$\sigma(y_1, y_2, y_3, y_4) = y_1B' + y_2C' + y_3D' + y_4E,$$

и другую операцию:

$$x \circ y = x \cdot \sigma(y), \quad \forall x, y \in W.$$

Тогда полуполе $\langle W, +, \circ \rangle$ не содержит собственных подполей, кроме простого подполя $\mathbb{Z}_3$, что проверяется непосредственными вычислениями.

Полуполя, определенные разными базами одного регулярного множества R, изотопны, что следует из теоремы Альберта 1.2.13. Для полноты изложения приведем этот результат в своих обозначениях.

Лемма 5.1.4. *Пусть W – n-мерное линейное пространство над $\mathbb{Z}_p$, $R \subset GL_n(p) \cup \{0\}$ – регулярное множество, замкнутое по сложению, и*

$$R = \{\theta(x) \mid x \in W\} = \{\sigma(x) \mid x \in W\},$$

где θ и σ – две аддитивные биекции из W на R,

$$x * y = x\theta(y), \qquad x \circ y = x\sigma(y), \quad x, y \in W.$$

Тогда полуполе $\langle W, +, * \rangle$ изотопно полуполю $\langle W, +, \circ \rangle$.

Доказательство. Для любого $y \in W$ матрица $\theta(y) \in R$ совпадает с некоторой, однозначно определенной матрицей $\sigma(y')$, $y' \in W$, тогда

$$x * y = x\theta(y) = x\sigma(y') = x \circ y' = x \circ \sigma^{-1}(\theta(y)), \quad x, y \in W.$$

Биективное отображение $y \to \sigma^{-1}(\theta(y))$, очевидно, является аддитивным и удовлетворяет определению. □

Обращаем внимание, что пример выше показывает: изотопизм в общем случае не сохраняет порядки подполей. Однако соответствующие ядра N_l, N_m, N_r изотопных полуполей изоморфны.

Пусть полуполе W порядка p^n координатизирует полуполевую проективную плоскость π, и Λ – группа автотопизмов плоскости π. Каждая коллинеация $\lambda \in \Lambda$ фиксирует треугольник с вершинами $(0,0)$, (0), (∞) и сторонами $[0,0]$, $[0]$, $[\infty]$ (см. [68]) и определяется блочно-диагональной матрицей:

$$(x, y)^\lambda = (x, y) \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}. \tag{5.1.2}$$

При этом блоки A и D должны удовлетворять условию (2.2.3): $A^{-1}\theta(x)D \in R$ для всех $x \in W$. Это условие обобщается и на случай основного поля непростого порядка, а также для произвольных плоскостей трансляций (см., например, теорему Д. Мадурам [91] и теорему Н.Д. Подуфалова [97]).

Далее рассмотрим автотопизм $\langle \alpha, \beta, \gamma \rangle$ полуполя W (как изотопизм из W на W):

$$x^\alpha * y^\beta = (x * y)^\gamma, \quad x, y \in W.$$

Поскольку отображения α, β, γ аддитивны, то это линейные преобразования пространства W, пусть

$$x^\alpha = xA, \quad x^\beta = xB, \quad x^\gamma = xD, \quad x \in W, \tag{5.1.3}$$

для подходящих матриц $A, B, D \in GL_n(p)$.

Лемма 5.1.5. *Если тройка матриц (A, B, D) из $GL_n(p)$ определяет автотопизм* (5.1.3) *полуполя W, то матрица*

$$\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \tag{5.1.4}$$

задает автотопизм полуполевой плоскости π, координатизируемой полуполем W. И обратно, если матрица (5.1.4) *– автотопизм плоскости π, то существует такая матрица $B \in GL_n(p)$, что (A, B, D) – автотопизм полуполя W.*

Доказательство. В соответствии с определением автотопизма,

$$(xA) * (yB) = (x * y)D, \quad xA\theta(yB) = x\theta(y)D \quad \forall x, y \in W.$$

Тогда $\theta(yB) = A^{-1}\theta(y)D$, выполнено условие (2.2.3), поэтому матрица (5.1.4) определяет автотопизм плоскости π. Обратно, для произвольного автотопизма $\lambda \in \Lambda$ (5.1.2) отображение

$$y \to A^{-1}\theta(y)D$$

из W в $GL_n(p)$ линейно. Тогда $A^{-1}\theta(y)D = \theta(yB)$ для некоторой матрицы B. $\square$

Пусть φ – автоморфизм полуполя W; тогда $x^\varphi * y^\varphi = (x * y)^\varphi$ $(x, y \in W)$. Аналогичные рассуждения с заменой $x^\varphi = xA$ доказывают следующий результат.

Лемма 5.1.6. *Если матрица $A \in GL_n(p)$ определяет автоморфизм полуполя W, то матрица*

$$\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} \tag{5.1.5}$$

задает автотопизм полуполевой плоскости π, координатизируемой W (такой автотопизм фиксирует прямую $y = x$, не обязательно поточечно). Обратно, если матрица (5.1.5) *задает автотопизм плоскости π и удовлетворяет условию*

$$A^{-1}\theta(y)A = \theta(yA) \qquad \forall y \in W, \tag{5.1.6}$$

то матрица A определяет автоморфизм полуполя W.

Определяя на автотопизмах полуполя W операцию покомпонентной суперпозиции,

$$\langle \alpha_1, \beta_1, \gamma_1 \rangle \cdot \langle \alpha_2, \beta_2, \gamma_2 \rangle = \langle \alpha_1\alpha_2, \beta_1\beta_2, \gamma_1\gamma_2 \rangle,$$

заключаем, что все автотопизмы W образуют группу $At\,W$ и справедливо следствие лемм 5.1.5 и 5.1.6 (см. также [68, лемма 8.8]):

Теорема 5.1.7. *Пусть W – полуполе порядка p^n с регулярным множеством (5.1.1) и π – координатизируемая W полуполевая проективная плоскость. Тогда группа автотопизмов $At\,W$ полуполя W изоморфна группе автотопизмов Λ плоскости π, группа автоморфизмов $Aut\,W$ изоморфна ее подгруппе*

$$\left\{ \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} \;\middle|\; A \in GL_n(p),\ A^{-1}\theta(y)A = \theta(yA)\ \forall y \in W \right\}.$$

Из этой теоремы следует, очевидно, эквивалентность *гипотезы разрешимости группы коллинеаций конечной недезарговой полуполевой плоскости* и вопроса о разрешимости группы автотопизмов произвольного нетривиального конечного полуполя. В связи с этим пополним перечень известных результатов о разрешимости из § 2.3 следующими теоремами М. Ганли [51], Д. Хьюза и М. Каллахера [69].

Теорема 5.1.8. *Пусть S – полуполе порядка 2^s. Если S имеет размерность 2 над одним из своих ядер, то его группа автотопизмов разрешима.*

Теорема 5.1.9. *Пусть S – полуполе порядка p^s (p – простое). Если S имеет размерность 2 над двумя из своих ядер, то группа его автотопизмов разрешима.*

Подчеркнем, что результаты автора в теореме 2.3.2 доказаны независимо иными методами.

5.2. Инволютивные и внутренние автоморфизмы

Рассмотрим автоморфизмы порядка 2 конечного полуполя W и инволютивные коллинеации полуполевой плоскости π, координатизируемой W. Их взаимосвязь устанавливает следующая теорема.

Теорема 5.2.1. *Пусть φ – автоморфизм порядка 2 полуполя $W = W(n, p, \theta)$, $x^\varphi = xA$, $A \in GL_n(p)$. Тогда $\overline{\varphi} = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$ – бэровская инволюция полуполевой плоскости π порядка p^n, координатизируемой W. И обратно, пусть π – конечная полуполевая плоскость, которая допускает бэровскую инволюцию в трансляционном дополнении. Тогда, по крайней мере, одной из координатизирующих полуполей допускает автоморфизм порядка 2.*

Доказательство. Для доказательства будем использовать теоремы 3.1.2, 3.1.3, 3.1.5 о матричном представлении бэровской инволюции и регулярного множества.

Пусть φ – автоморфизм полуполя W. Тогда, по лемме 5.1.6, $\overline{\varphi}$ – автотопизм плоскости π. Так как $|\varphi| = 2$, то $|\overline{\varphi}| = 2$ и $\overline{\varphi}$ либо центральная, либо бэровская инволюция.

Если $p = 2$, то центральные коллинеации порядка 2 – это элации (2.2.4), они не являются автотопизмами.

Если $p > 2$, то центральная коллинеация $\overline{\varphi}$ порядка 2 – это гомология с осью $[\infty]$ и центром $(0,0)$ из подгруппы H_l (лемма 2.2.4). Единственный элемент порядка 2 в H_l определяется матрицей $\begin{pmatrix} -E & 0 \\ 0 & -E \end{pmatrix}$, но условие (5.1.6) не выполняется:

$$(-E)^{-1}\theta(y)(-E) = \theta(y) \neq \theta(y(-E)).$$

Таким образом, $\overline{\varphi}$ – бэровская инволюция плоскости π.

Обратно, пусть τ – бэровская инволюция в трансляционном дополнении. Тогда, с точностью до изоморфизма плоскостей, можно считать τ автотопизмом вида (3.1.3) $\begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix}$, где L – матрица (3.1.4):

$$L = \begin{pmatrix} E & E \\ 0 & E \end{pmatrix}, \quad p = 2, \text{ или } L = \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix}, \quad p > 2,$$

Пусть $(v,u) = (v_1, \ldots, v_n, u_1, \ldots, u_n)$ – нижняя строка матрицы $\theta(V,U)$ вида (3.1.5), (3.1.6). Для упрощения обозначений пишем далее $\theta(v,u)$. Для проверки условия (5.1.6) вычислим произведение $L^{-1}\theta(v,u)L$.

Если $p = 2$, то $(v,u)L = (v, v+u)$,

$$L^{-1}\theta(v,u)L = \begin{pmatrix} E & E \\ 0 & E \end{pmatrix} \begin{pmatrix} U+V+m(V)+w(V) & f(V)+m(U) \\ V & U+w(V) \end{pmatrix} \begin{pmatrix} E & E \\ 0 & E \end{pmatrix} =$$

$$= \begin{pmatrix} U+m(V)+w(V) & f(V)+m(U+V) \\ V & U+V+w(V) \end{pmatrix} = \theta(v, v+u) = \theta((v,u)L),$$

условие (5.1.6) выполнено.

Если $p > 2$, то $(v,u)L = (-v,u)$,

$$L^{-1}\theta(v,u)L = \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix} \begin{pmatrix} m(U) & f(V) \\ V & U \end{pmatrix} \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix} =$$

$$= \begin{pmatrix} m(U) & -f(V) \\ -V & U \end{pmatrix} = \theta(-v,u) = \theta((v,u)L),$$

условие (5.1.6) также выполнено. Теорема доказана. □

Эта теорема устанавливает существование инволютивного автоморфизма только с точностью до изотопизма полуполей, так как в общем случае бэровская инволюция, возможно, не фиксирует прямую $y = x$. Необходимая замена базиса линейного пространства в этом случае приведет к другому, изотопному полуполю. Рассматривая пять неизоморфных (изотопных) полуполей порядка 16 с ядром порядка 4 (см. параграф 5.5), координатизирующих одну и ту

же полуполевую плоскость, заметим, что полуполя T_{24}, T_{25} и T_{50} допускают единственный нетривиальный автоморфизм – порядка 2, полуполе T_{35} имеет группу автоморфизмов порядка 3, полуполе T_{45} – порядка 4. Кроме того, инволютивный автоморфизм полуполя не обязательно единственный. Например, исключительное полуполе Хентзела–Руа допускает три автоморфизма порядка 2 (см. параграф 5.8). Теорема 5.2.1 приводит к очевидному следствию.

Следствие 5.2.2. *Если конечное полуполе W допускает инволютивный автоморфизм, то порядок полуполя является квадратом, $|W| = p^{2n}$.*

Используя описанную взаимосвязь, докажем результаты о некоторых подмножествах полуполя.

Теорема 5.2.3. *Пусть W – полуполе порядка p^{2n} (p – простое), допускающее автоморфизм φ порядка 2. Тогда стабилизатор φ*

$$U = \{x \in W \mid x^{\varphi} = x\} \tag{5.2.1}$$

является подполуполем порядка p^n. Если $n = 2$, то U – подполе W, и любое максимальное подполе W имеет порядок p^2.

Доказательство. Очевидно, U содержит оба нейтральных элемента W и замкнуто по сложению и умножению. Поэтому U есть подполуполе W. Чтобы найти его порядок, рассмотрим множество точек

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

полуполевой плоскости π, координатизируемой W. Тогда

$$\{(x, y) \mid x, y \in U\}$$

– множество точек бэровской подплоскости π_0, которая фиксируется бэровской инволюцией

$$\overline{\varphi} : (x, y) \to (x^{\varphi}, y^{\varphi}), \quad (x, y) \in W.$$

Поэтому $|\pi| = |W| = p^{2n}$, $|U| = |\pi_0| = \sqrt{|\pi|}$, $|U| = p^n$.

Пусть $n = 2$, тогда $|U| = p^2$ и $U \simeq GF(p^2)$ по теореме 5.1.2. Предположим, что H – подполе порядка p^3 в W.

1. Если $H^{\varphi} = H$, то φ – инволютивный автоморфизм H. Это невозможно, $|Aut(H)| = 3$.

2. Если $H^{\varphi} \neq H$, то H^{φ} – другое подполе порядка p^3. Рассмотрим подполя H и H^{φ} как линейные подпространства и используем тождество Грассмана:

$$\dim H + \dim H^{\varphi} = \dim(H \cap H^{\varphi}) + \dim(H + H^{\varphi}),$$

$3 + 3 = \dim(H \cap H^{\varphi}) + 4$ и $\dim(H \cap H^{\varphi}) = 2$, т.е. пересечение $H \cap H^{\varphi}$ – подполе порядка p^2 в поле порядка p^3, что невозможно. Таким образом, любое максимальное подполе в W имеет порядок p^2. $\square$

Заметим, что последнее утверждение теоремы будет доказано далее другим способом.

Теорема 5.2.4. *Если полуполе W нечетного порядка p^{2n} ($p > 2$ – простое) допускает автоморфизм порядка 2, то его мультипликативная лупа W^* содержит подлупу порядка $2(p^n - 1)$.*

Доказательство. Пусть φ – инволютивный автоморфизм полуполя W, U (5.2.1) – стабилизатор φ (подполуполе порядка p^n). Рассмотрим подпространство

$$U' = \{x \in W \mid x^\varphi = -x\}$$

и жорданову нормальную форму L (3.1.4) матрицы φ. Заключаем, что $|U'| = p^n$. Объединение $U \cup U'$ замкнуто относительно умножения. Действительно, если $x, y \in U'$, то

$$(x * y)^\varphi = x^\varphi * y^\varphi = (-x) * (-y) = x * y, \qquad x * y \in U;$$

если $x \in U$, $y \in U'$ (или наоборот), то

$$(x * y)^\varphi = x^\varphi * y^\varphi = x * (-y) = -(x * y), \qquad x * y \in U'.$$

Более того, подполуполе U содержит единицу e полуполя W. Таким образом, объединение $(U \setminus \{0\}) \cup (U' \setminus \{0\})$ является подлупой W^* порядка $2(p^n - 1)$. Заметим, что это множество не замкнуто по сложению. □

Г. Венэ [120] обобщил традиционное понятие внутреннего автоморфизма группы $x \to g^{-1}xg$ для случая конечного полуполя. Он называет *внутренним автоморфизмом* полуполя W отображение

$$\lambda_m : x \to (m_l^{-1} * x) * m, \quad x \in W, \tag{5.2.2}$$

где $m \in W^*$ и m_l^{-1} – левый обратный к m (т.е. $m_l^{-1} * m = e$) при условии

$$(x * y)^{\lambda_m} = x^{\lambda_m} * y^{\lambda_m}, \quad x, y \in W$$

(λ_m сохраняет операцию сложения ввиду дистрибутивности). Ясно, что поле не может обладать нетривиальными внутренними автоморфизмами. Отсутствие в полуполе ассоциативности умножения приводит к существованию нетривиальных внутренних автоморфизмов даже для некоторых коммутативных полуполей. В частности, Г. Венэ [120] указывает внутренние автоморфизмы полуполей Хьюза–Клейнфелда и комутативных полуполей Диксона. Он рассматривает только внутренние автоморфизмы, порожденные элементами m из ядра полуполя $N_0 = N_l \cap N_m \cap N_r$. Для таких автоморфизмов результаты Г. Венэ обобщает следующая теорема.

Теорема 5.2.5. *Пусть W – конечное полуполе, $m \in W^*$ и отображение λ_m определено правилом (5.2.2). Тогда:*

1) если m принадлежит ядру N_0, то отображение λ_m является автоморфизмом полуполя W;

2) если m принадлежит центру Z, то λ_m – тождественный автоморфизм;

3) ненулевые элементы $a, b \in N_0$ задают один и тот же внутренний автоморфизм тогда и только тогда, когда $a^{-1}b \in Z$;

4) $\{\lambda_m \mid m \in N_0^*\}$ является группой, ее порядок равен $(|N_0| - 1)/(|Z| - 1)$.

Внутренние автоморфизмы полуполей, введенные Г. Венэ, предоставляют весьма востребованную технику для описания автоморфизмов полуполей из различных классов. Например, К. Браун, С. Пумплюн и Э. Стил [32] в 2017 г. указали, используя результаты Г. Венэ, автоморфизмы полуполей Джа–Джонсона, Сандлера и некоторых полуполей Кнута.

Введем обозначения для множества всех внутренних автоморфизмов

$$In\, W = \{\lambda_m \mid \lambda_m \in Aut\, W,\ m \in W^*\}$$

и множества порождающих их элементов

$$\mathcal{M} = \{m \in W \mid \lambda_m \in In\, W\}.$$

Подчеркнем, что мы не требуем выполнения условия $m \in N_0$. Оказывается, тогда непосредственные вычисления приводят к некоторым аномальным результатам. Для отыскания внутренних автоморфизмов полуполей малых порядков будем применять их матричное представление, найденное с помощью регулярного множества.

Лемма 5.2.6. *Пусть $W = W(n, p, \theta)$ – полуполе порядка p^n с единицей e и регулярным множеством R (5.1.1), элементы $e_1, e_2, \ldots, e_n$ образуют базис W над $\mathbb{Z}_p$. Если $0 \neq m \in W$ и $\lambda_m : x \to xM$ – внутренний автоморфизм полуполя W, где $M \in GL(n, p)$, то i-я строка матрицы M равна*

$$e[\theta(m)]^{-1}\theta(e_i)\theta(m).$$

Доказательство. По определению левого обратного элемента, $m_l^{-1} * m = m_l^{-1}\theta(m) = e$, отсюда $m_l^{-1} = e[\theta(m)]^{-1}$. Найдем образ базисного вектора e_i:

$$(m_l^{-1} * e_i) * m = m_l^{-1}\theta(e_i)\theta(m) = e[\theta(m)]^{-1}\theta(e_i)\theta(m).$$

□

С использованием этого технического результата построено [176] матричное представление внутренних автоморфизмов всех полуполей порядка 16, исключительных полуполей Кнута–Руа порядка 32 и Хентзела–Руа порядка 64, некоторых полуполей порядка 81. Результаты будут перечислены в соответствующих параграфах далее. Кратко укажем факты, демонстрирующие, что условия теоремы 5.2.5 не являются достаточными. Найдены:

1) полуполе с внутренним автоморфизмом λ_m при $m \notin N_0$;

2) полуполе с тождественным внутренним автоморфизмом λ_m при $m \notin Z$;

3) полуполе, в котором множество $In\,W$ внутренних автоморфизмов не является группой;

4) полуполе, в котором множество $\mathcal{M}$ не замкнуто по сложению и умножению.

Следующая теорема предоставляет примеры элементов, которые не могут порождать нетривиальный внутренний автоморфизм (определение 5.5.6 правоциклического элемента приведено в § 5.6).

Теорема 5.2.7. *Если λ_m – нетривиальный внутренний автоморфизм конечного полуполя W, то элемент $m \in W^*$ не является лево- и правопримитивным, лево- и правоциклическим, лупа W^* не порождается элементом m.*

Доказательство. Пусть $\mathcal{F}$ – множество элементов полуполя W, фиксируемых автоморфизмом λ_m. Тогда, очевидно, $m \in \mathcal{F}$ и это множество замкнуто относительно сложения и умножения. Поэтому $\mathcal{F}$ содержит все степени элемента m и значения любого многочлена $f(x) \in Z[x]$ при $x = m$ (при любом вычислении степени). Если m порождает W^* (тем более является примитивным или циклическим элементом), то $W \subset \mathcal{F}$, поэтому автоморфизм λ_m тождественный. □

5.3. Минимальные многочлены в конечных полуполях

В этом параграфе мы применяем [135] классическое понятие минимального многочлена к изучению конечных полуполей. Напомним определение минимального многочлена элемента конечного поля и основные свойства минимальных многочленов, в соответствии с [7] (в этом параграфе мы используем обозначение $\mathbb{F}_q$ для $GF(q)$).

Определение 5.3.1. *Пусть $\mathbb{F}_{q^n}$ – поле порядка q^n и $a \in \mathbb{F}_{q^n}$. Минимальным многочленом элемента a над $\mathbb{F}_q$ называется такой нормированный многочлен $M(x) \in \mathbb{F}_q[x]$ минимальной степени, что $M(a) = 0$.*

Теорема 5.3.2. *Пусть $a \in \mathbb{F}_{q^n}$, a имеет степень d над $\mathbb{F}_q$ и $M(x)$ – минимальный многочлен элемента a над $\mathbb{F}_q$.*

1. $M(x)$ неприводим над $\mathbb{F}_q$ и степень $\deg M = d$ делит n.

2. Для любого многочлена $f \in \mathbb{F}_q[x]$ равенство $f(a) = 0$ выполняется тогда и только тогда, когда M делит f.

3. Если a – примитивный элемент, то $\deg M = n$.

4. Корни $M(x)$ – это в точности a, $a^q, \ldots, a^{q^{d-1}}$, и $M(x)$ является минимальным многочленом для каждого из них.

5. Если $f(x)$ – нормированный неприводимый многочлен из $\mathbb{F}_q[x]$ и $f(a) = 0$, то $f = M$.

6. $M(x)$ делит $x^{q^d} - x$ и $x^{q^n} - x$.

Пусть $W = W(n, p, \theta)$ – полуполе порядка p^n (p – простое), заданное инъективным отображением θ. Рассмотрим многочлен $f(x) \in \mathbb{Z}_p[x]$,

$$f(x) = c_m x^m + c_{m-1} x^{m-1} + \cdots + c_2 x^2 + c_1 x + c_0, \quad c_i \in \mathbb{Z}_p,\ i = 0, 1, \ldots, m.$$

Для элемента $a \in W$ определим *право-* и *левоупорядоченное значение* многочлена $f(x)$:

$$f(a)) = c_m a^{m)} + c_{m-1} a^{m-1)} + \cdots + c_2 a^2 + c_1 a + c_0 e,$$
$$f((a) = c_m a^{(m} + c_{m-1} a^{(m-1} + \cdots + c_2 a^2 + c_1 a + c_0 e.$$

Здесь $a^{s)}$ и $a^{(s}$ – право- и левоупорядоченные степени элемента a. Произведение коэффициента $c \in \mathbb{Z}_p$ на элемент $a \in W$ равно сумме c слагаемых, равных a, для $c \neq 0$, и равно нулю для $c = 0$.

Пример 5.3. Пусть $f(x) = x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$, $a \in W(n, 2, \theta)$, тогда

$$f(a)) = a^{3)} + a^2 + a + e = a^2 * a + a^2 + a + e = a\theta(a)\theta(a) + a\theta(a) + a + e,$$
$$f((a) = a^{(3} + a^2 + a + e = a * a^2 + a^2 + a + e = a\theta(a\theta(a)) + a\theta(a) + a + e.$$

Очевидно, в случае степени ≤ 2 право- и левоупорядоченное значения $f(a))$ и $f((a)$ равны. Отметим, что $(fg)(a))$ в общем случае не равно $f(a)) * g(a))$. Если $f(a)) = 0$, то для любого многочлена $g(x)$ выполнено $(fg)(a)) = 0$, однако обратное не верно: из равенства $(fg)(a)) = 0$ не следует $f(a)) = 0$ или $g(a)) = 0$ (аналогично для левоупорядоченных значений).

Определение 5.3.3. *Правоупорядоченным минимальным многочленом элемента $a \in W$ называется такой нормированный многочлен $\mu_a^r(x) \in \mathbb{Z}_p[x]$ минимальной степени, что $\mu_a^r(a)) = 0$. Левоупорядоченный минимальный многочлен $\mu_a^l(x)$ определяется аналогично.*

Мы рассматриваем многочлены над простым подполем $\mathbb{Z}_p$, но результаты могут быть обобщены для центра Z полуполя. Некоторые свойства односторонне-упорядоченных минимальных многочленов в конечных полуполях подобны аналогичным результатам для конечных полей.

Лемма 5.3.4. *Если $a \neq 0$, то $\mu_a^r(0)) \neq 0$, $\mu_a^l((0) \neq 0$, т.е. x не делит $\mu_a^r(x)$ и $\mu_a^l(x)$.*

Доказательство. Если $\mu_a^r(x) = c_0x^m + \cdots + c_{m-1}x = (c_0x^{m-1} + \cdots + c_{m-1}) \cdot x$, то

$$\mu_a^r(a)) = (c_0a^{m-1)} + \cdots + c_{m-1}) * a = 0, \qquad c_0a^{m-1)} + \cdots + c_{m-1} = 0,$$

что противоречит определению (для $\mu_a^l(x)$ аналогично). □

Теорема 5.3.5. *Пусть $a \in W = W(n, p, \theta)$, $a \neq 0$, $\mu_a^r(x), \mu_a^l(x) \in \mathbb{Z}_p[x]$ – право- и левоупорядоченный минимальные многочлены элемента a соответственно.*

1. Для любого многочлена $f(x) \in \mathbb{Z}_p[x]$ равенство $f(a)) = 0$ выполняется тогда и только тогда, когда $\mu_a^r(x)$ делит $f(x)$, равенство $f((a) = 0$ – тогда и только тогда, когда $\mu_a^l(x)$ делит $f(x)$.

2. Право-(лево-)упорядоченный минимальный многочлен элемента a делит многочлен $x^k - 1$, где k есть правый (левый) порядок a, $k = |a|_r$ ($k = |a|_l$).

3. Если $K \simeq \mathbb{F}_{p^m}$ – подполе полуполя W, то для $a \in K$ правоупорядоченный многочлен элемента a совпадает с левоупорядоченным, $\mu_a^r(x) = \mu_a^l(x)$, и является неприводимым многочленом степени $s|m$.

Доказательство. Первое утверждение достаточно доказать, например, только для правоупорядоченного многочлена. Если $g(x) = \mu_a^r(x) \cdot x$, то $g(a)) = \mu_a^r(a)) * a = 0 * a = 0$, поэтому для

$$f(x) = \mu_a^r(x) \cdot (d_0x^k + \cdots + d_k) \in \mathbb{Z}_p[x]$$

верно $f(a)) = 0$. И обратно, пусть $f(a)) = 0$. Выполним деление с остатком:

$$f(x) = \mu_a^r(x)q(x) + r(x),$$

где многочлен $r(x)$ нулевой или $\deg r < \deg \mu_a^r$. Тогда

$$f(a)) = (\mu_a^r \cdot q)(a)) + r(a)) = 0 + r(a)) = 0,$$

и минимальность $\mu_a^r(x)$ влечет $r(x) = 0$. Второе утверждение очевидно следует из первого. Третье утверждение следует из теоремы 5.3.2. □

В отличие от случая конечного поля, право-(лево-)упорядоченный минимальный многочлен элемента в полуполе не обязательно неприводим. Это верно для элементов подполей (по третьему утверждению теоремы), но не только, как будет показано далее. Если право-(лево-)упорядоченный минимальный многочлен неприводим, то элемент не обязательно принадлежит подполю.

Теорема 5.3.6. *1. Если φ – автоморфизм полуполя $W(n,p,\theta)$, то любой элемент $a \in W$ и его образ a^φ имеют одинаковые право-(лево-)упорядоченные минимальные многочлены,*

$$\mu^r_{a^\varphi}(x) = \mu^r_a(x), \qquad \mu^l_{a^\varphi}(x) = \mu^l_a(x).$$

2. Если φ – антиизоморфизм из $W(n,p,\theta)$ на $V(n,p,\tau)$, то для любого элемента $a \in W$

$$\mu^r_{a^\varphi}(x) = \mu^l_a(x), \qquad \mu^l_{a^\varphi}(x) = \mu^r_a(x).$$

3. Если полуполе W антиизоморфно себе, то для любого элемента $a \in W$ правоупорядоченный минимальный многочлен совпадает с левоупорядоченным.

4. Если $a \in W^*$ и λ_a – нетривиальный внутренний автоморфизм полуполя W, то право- и левоупорядоченный минимальные многочлены элемента a имеют степень меньше n.

Доказательство. Утверждения 1–3 очевидны. Для доказательства четвертого утверждения укажем: если, например, правоупорядоченный минимальный многочлен элемента a имеет степень n, то a – правоциклический элемент и по теореме 5.2.7 внутренний автоморфизм λ_a тривиален. □

Несмотря на простоту результата, отметим, что группа автоморфизмов конечного поля $\mathbb{F}_{p^n}$ циклическая, порожденная автоморфизмом $x \to x^p$. В случае полуполя порядка p^n такое преобразование в общем случае не является автоморфизмом (см., например, полуполе Хентзела–Руа) и минимальные многочлены элементов a и a^p (при любой расстановке скобок) могут быть различны.

Сравним односторонне-упорядоченный многочлен элемента $a \in W$ с минимальным многочленом (в классическом смысле) соответствующей матрицы из регулярного множества, $A = \theta(a)$.

Лемма 5.3.7. *Для любого многочлена $f(x) \in \mathbb{Z}_p[x]$, $f(0) \neq 0$, любого ненулевого элемента $a \in W(n,p,\theta)$ и соответствующей матрицы $A = \theta(a)$ равенство $f(A) = 0$ влечет $f(a)) = 0$.*

Доказательство. Пусть $f(A) = 0$. Так как $f(0) \neq 0$, то мы можем, без ограничения общности, полагать $c_0 = -1$, тогда

$$c_m A^m + c_{m-1}A^{m-1} + \cdots + c_2 A^2 + c_1 A = E,$$

$$A(c_m A^{m-1} + c_{m-1}A^{m-2} + \cdots + c_2 A + c_1 E) = E.$$

Умножим левую и правую части равенства на единицу полуполя W:

$$eA(c_m A^{m-1} + c_{m-1}A^{m-2} + \cdots + c_2 A + c_1 E) = eE,$$

$$a(c_m A^{m-1} + c_{m-1}A^{m-2} + \cdots + c_2 A + c_1 E) = eE,$$
$$c_m a^{m)} + c_{m-1}a^{m-1)} + \cdots + c_2 a^2 + c_1 a = e$$

отсюда $f(a)) = 0$. □

Отметим, что обратное в общем случае неверно, т.е. из равенства $f(a)) = 0$ не следует $f(A) = 0$. Действительно, перепишем равенство

$$a(c_m A^{m-1} + c_{m-1}A^{m-2} + \cdots + c_2 A + c_1 E) = eE$$

в виде $aB = e$, тогда $a = eB^{-1}$. Так как $a = eA = e\theta(a)$, то $e(B^{-1} - A) = 0$ и отсюда следует только, что первая строка A равна первой строке B^{-1}, но не следует равенство матриц $A = B^{-1}$. Кроме того, аналогичный результат для левоупорядоченных многочленов в общем случае неверен (контрпример см. далее).

Условие $f(0) \neq 0$ в тексте леммы не является существенным по причине отсутствия делителей нуля в полуполе.

Из доказанной леммы непосредственно следует

Теорема 5.3.8. *Если $a \in W(n, p, \theta)$ и $A = \theta(a)$, то правоупорядоченный минимальный многочлен элемента a делит минимальный многочлен матрицы A.*

Следствие 5.3.9. *Если φ – антиизоморфизм из $W(n, p, \theta)$ на $V(n, p, \tau)$, то для любого $a \in W^*$ левоупорядоченный минимальный многочлен $m_a^l(x)$ делит минимальный многочлен матрицы $\tau(a^\varphi)$.*

Пример 5.4. Проиллюстрируем результаты на примере полуполя порядка 16. Пусть W – 4-мерное линейное пространство над $\mathbb{Z}_2$,

$$W = \{x = (x_1, x_2, x_3, x_4) \mid x_i \in \mathbb{Z}_2,\ i = 1, \ldots, 4\}.$$

Определим отображение $\theta : W \to GL_4(2) \cup \{0\}$ как

$$\theta(x_1, x_2, x_3, x_4) = x_1 E + x_2 \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} + x_3 \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} + x_4 \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Тогда $R = \{\theta(x) \mid x \in W\}$ – регулярное множество и $(W, +, *)$ полуполе порядка 16 с умножением $x * y = x \cdot \theta(y)$. Вектор $e = (1, 0, 0, 0)$ является мультипликативной единицей. Построенное полуполе изоморфно полуполю V_8 из списка Клейнфелда (см. параграф 5.5).

Кроме прямого перебора вариантов, мы можем использовать следующий метод отыскания односторонне-упорядоченного минимального многочлена элемента. Пусть e_1, $e_2, \ldots,$ e_n – базис линейного пространства $W = W(n, p, \theta)$ над $\mathbb{Z}_p$. Запишем правоупорядоченные степени e, a, a^2, $a^{3)}, \ldots,$ $a^{n)}$ как линейные комбинации базисных векторов:

$$a^{i)} = \sum_{j=1}^{n} \alpha_{ij} e_j,$$

где $\alpha_{ij} \in \mathbb{Z}_p$, $i = 0, 1, \ldots, n$, $j = 1, \ldots, n$. Составим матрицу (α_{ij}) и приведем ее к ступенчатому виду. Нулевая строка соответствует линейной комбинации правоупорядоченных степеней a, равной нулю. Из полученных нулевых строк выбираем соответствующую многочлену наименьшей степени, он и является $\mu_a^r(x)$.

Например, рассмотрим $e = (1, 0, 0, 0)$, $b = (0, 0, 1, 1)$, $b^2 = (1, 1, 0, 1)$, $b^{3)} = (0, 0, 1, 0)$, $b^{4)} = (0, 1, 0, 1)$ в полуполе $W = W(4, 2, \theta)$, тогда

$$\begin{pmatrix} 1 & 0 & 0 & 0 & e \\ 0 & 0 & 1 & 1 & b \\ 1 & 1 & 0 & 1 & b^2 \\ 0 & 0 & 1 & 0 & b^{3)} \\ 0 & 1 & 0 & 1 & b^{4)} \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 & e \\ 0 & 1 & 0 & 1 & b^2 + e \\ 0 & 0 & 1 & 1 & b \\ 0 & 0 & 0 & 1 & b^{3)} + b \\ 0 & 0 & 0 & 0 & b^{4)} + b^2 + e \end{pmatrix}.$$

Таким образом, правоупорядоченный минимальный многочлен элемента b есть $\mu_b^r(x) = x^4 + x^2 + 1 = (x^2 + x + 1)^2$. Отметим, что он не является неприводимым. Все односторонне-упорядоченные минимальные многочлены и все односторонние порядки для $a \in W \setminus \{0, e\}$ представлены в табл. 10. В последнем столбце перечислены минимальные многочлены матриц $A = \theta(a)$.

Элементы порядка 3, вместе с 0 и e, образуют два подполя порядка 4. Право- и левоупорядоченные минимальные многочлены этих элементов равны неприводимому многочлену $x^2 + x + 1$. Отметим, что это многочлен степени 2, имеющий в W четыре различных корня. Также, многочлен $x^4 + x + 1$ имеет 6 «правых» корней в W. Во всех случаях правоупорядоченный минимальный многочлен элемента делит минимальный многочлен соответствующей матрицы. В то же время левоупорядоченный минимальный многочлен делит минимальный многочлен матрицы только для элементов из подполей.

В полуполе $W(4, 2, \theta)$ видим 6 правопримитивных элементов (т.е. с правым порядком 15) и 4 левопримитивных элемента. Минимальный многочлен каждой из соответствующих матриц есть неприводимый примитивный многочлен степени 4. Правоупорядоченный минимальный многочлен шести правопримитивных элементов совпадает с минимальным многочленом матрицы, левоупорядочен-

ный минимальный многочлен левопримитивных элементов таким свойством не обладает.

Таблица 10. Минимальные многочлены элементов полуполя $W(4,2,\theta)$

a	$\lvert a\rvert_l$	$\lvert a\rvert_r$	$\lvert a\rvert$	$\mu_a^l(x)$	$\mu_a^r(x)$	$\mu_A(x)$
$(0,0,1,0)$	3	3	3	x^2+x+1	x^2+x+1	$(x^2+x+1)^2$
$(1,0,1,0)$	3	3	3	x^2+x+1	x^2+x+1	$(x^2+x+1)^2$
$(0,1,0,1)$	3	3	3	x^2+x+1	x^2+x+1	x^2+x+1
$(1,1,0,1)$	3	3	3	x^2+x+1	x^2+x+1	x^2+x+1
$(0,0,0,1)$	5	6	4	$x^4+x^3+x^2+x+1$	$(x^2+x+1)^2$	$(x^2+x+1)^2$
$(1,0,1,1)$	5	6	4	$x^4+x^3+x^2+x+1$	$(x^2+x+1)^2$	$(x^2+x+1)^2$
$(0,1,0,0)$	5	15	5	$x^4+x^3+x^2+x+1$	x^4+x+1	x^4+x+1
$(0,1,1,0)$	5	15	5	$x^4+x^3+x^2+x+1$	x^4+x+1	x^4+x+1
$(0,1,1,1)$	6	15	6	$(x^2+x+1)^2$	x^4+x+1	x^4+x+1
$(1,1,1,1)$	6	15	6	$(x^2+x+1)^2$	x^4+x+1	x^4+x+1
$(0,0,1,1)$	15	6	5	x^4+x^3+1	$(x^2+x+1)^2$	$(x^2+x+1)^2$
$(1,0,0,1)$	15	6	5	x^4+x^3+1	$(x^2+x+1)^2$	$(x^2+x+1)^2$
$(1,1,0,0)$	15	15	5	x^4+x^3+1	x^4+x+1	x^4+x+1
$(1,1,1,0)$	15	15	5	x^4+x^3+1	x^4+x+1	x^4+x+1

Полуполе $W(4,2,\theta)$ допускает единственный нетривиальный автоморфизм φ порядка 2,

$$\varphi : (x_1,x_2,x_3,x_4) \to (x_1,x_2,x_3,x_4)\begin{pmatrix}1&0&0&0\\0&1&1&0\\0&0&1&0\\1&0&1&1\end{pmatrix}.$$

Можно проверить, что для любого элемента $a \in W$ право- и левоупорядоченный минимальные многочлены его образа a^φ совпадают с $\mu_a^r(x)$ и $\mu_a^l(x)$ соответственно. Например, $(0,0,0,1)^\varphi = (1,0,1,1)$ (см. табл. 10).

Отображение $x \to x^2$ не инъективно на W (сравнить со случаем поля $\mathbb{F}_{16}$). Действительно, $(0,0,0,1)^2 = (0,1,0,1)^2 = (1,1,0,1)$ и односторонне-упорядоченные минимальные многочлены элементов $(0,0,0,1)$, $(0,1,0,1)$ и $(1,1,0,1)$ не совпадают.

Рассмотрим противоположное полуполе $V = V(4,2,\tau) = W^{op}$, оно изоморфно V_9 (см. табл. 11, § 5.5). Матрицы $\tau(e_i)$ его регулярного множества получим из условия $e_i\theta(e_j) = e_j\tau(e_i)$, $i,j = 1,\dots,4$. Тогда

$$\tau(x_1,x_2,x_3,x_4) = x_1E + x_2\begin{pmatrix}0&1&0&0\\0&0&0&1\\0&0&1&1\\1&0&1&0\end{pmatrix} + x_3\begin{pmatrix}0&0&1&0\\0&0&1&1\\1&0&1&0\\1&1&1&1\end{pmatrix} + x_4\begin{pmatrix}0&0&0&1\\1&0&1&1\\0&1&0&1\\1&1&0&1\end{pmatrix}.$$

Непосредственное вычисление минимальных многочленов для всех элементов $a \in V = W^{op}$ иллюстрирует третье утверждение теоремы 5.3.6: левоупорядоченный минимальный многочлен $a \in W^{op}$ совпадает с правоупорядоченным минимальным многочленом $a \in W$, и наоборот. Далее, если $A = \theta(a)$ и $A^{op} = \tau(a)$, то левоупорядоченный минимальный многочлен $a \in W$ делит $m_{A^{op}}(x)$. Например, левоупорядоченный минимальный многочлен элемента $\tau(1,1,1,0)$ равен $x^4 + x^3 + 1$ (см. табл. 10, сравнить с последним столбцом).

Используем минимальные многочлены элементов конечного полуполя для описания некоторых подполей. Прежде всего, докажем вспомогательные результаты. В том числе, приведем с доказательством хорошо известный результат о регулярном множестве.

Лемма 5.3.10. *Пусть W – полуполе порядка p^n, $R \subset GL_n(p) \cup \{0\}$ – его регулярное множество. Тогда для любой нескалярной матрицы $A \in R$ характеристический многочлен $\chi_A(x) \in \mathbb{Z}_p[x]$ не имеет линейных делителей.*

Доказательство. Действительно, пусть $A = \theta(a)$, $a \in W$, и $\chi_A(x)$ делится на $x - \lambda$. Если $b \in W$ – соответствующий собственный вектор, то

$$b\theta(a) = \lambda b, \quad b\theta(a - \lambda e) = 0, \quad b * (a - \lambda e) = 0.$$

Отсюда, в силу отсутствия делителей нуля, имеем $a = \lambda e$ и $\theta(a) = \lambda E$, что противоречит условию. □

Лемма 5.3.11. *Пусть W – полуполе порядка p^n с единицей e, ненулевой элемент $a \in W$ имеет правоупорядоченный минимальный многочлен $\mu_a^r(x) \in \mathbb{Z}_p[x]$. Тогда $deg(\mu_a^r) = 1$ тогда и только тогда, когда a принадлежит простому подполю $P \simeq \mathbb{Z}_p$; $deg(\mu_a^r) = 2$ тогда и только тогда, когда*

$$K = \{\alpha_1 e + \alpha_2 a \mid \alpha_1, \alpha_2 \in \mathbb{Z}_p\}$$

– подполе в W порядка p^2.

Доказательство. Первое утверждение очевидно. Пусть $deg(\mu_a^r) = 2$. Тогда система векторов e, a линейно независима над $\mathbb{Z}_p$, $a^2 \in K$, поэтому $|K| = p^2$, K замкнуто по умножению, в K выполнен ассоциативный закон. Обратно, если K – подполе порядка p^2, то $a \notin P$ и $a^2 \in K$. □

Следствие 5.3.12. *Подмножество элементов полуполя W порядка p^n, минимальный многочлен которых имеет степень 1 или 2 (вместе с 0), является объединением всех подполей порядка p^2 в W.*

Следует отметить, что для подполуполя (или подполя) U порядка p^m в полуполе W порядка p^n не обязательно выполнено условие $m|n$. Этот факт связан с отсутствем ассоциативности умножения: полуполе W не обязательно является линейным пространством над U. Кроме того, конечное полуполе может содержать несколько подполуполей (подполей) одного и того же порядка. Например, известно полуполе порядка 32, содержащее подполе порядка 4, а также полуполя порядка 81, содержащие три подполя порядка 9 (подробнее см. [19] и [134]).

Очевидные примеры подполей в конечных полуполях – это левое, среднее и правое ядра N_l, N_m, N_r, ядро N_0 и центр Z. Другой пример полуполей порядка p^4, содержащих подполя порядка p^2, предоставляет теорема 5.2.3 – это стабилизатор инволютивного автоморфизма.

Естественно предположить, что в полуполе порядка p^n всякое подполуполе должно иметь порядок p^m, где $m \leq n/2$. Покажем, что это верно, по крайней мере, для полуполей порядков p^3 и p^4 [141].

Теорема 5.3.13. *В полуполе W порядка p^n, где $n = 3$ или $n = 4$, всякое подполуполе является подполем порядка p^m, $m \leq n/2$.*

Доказательство. Пусть $|W| = p^3$ и U – подполе порядка p^2, элемент $a \in U$ не принадлежит простому подполю P. Тогда минимальный многочлен $\mu_a(x) \in \mathbb{Z}_p[x]$ элемента a имеет степень два и делит минимальный многочлен $\mu_A(x)$ соответствующей матрицы регулярного множества $A = \theta(a) \in GL_3(p)$. Тогда характеристический многочлен $\chi_A(x)$ матрицы A имеет линейный делитель, что невозможно.

Пусть $|W| = p^4$ и U – подполуполе порядка p^3. Оно не содержит подполей порядка p^2, поэтому каждый его элемент $a \in U$, не принадлежащий простому подполю P, имеет правоупорядоченный минимальный многочлен $\mu_a^r(x) \in \mathbb{Z}_p[x]$ степени 3. Следовательно, характеристический многочлен $\chi_A(x)$ соответствующей матрицы регулярного множества $A = \theta(a) \in GL_4(p)$ имеет линейный делитель. □

Таким образом, нетривиальные полуполя W порядка p^3 и p^4 следует считать *минимальными собственными полуполями*: каждое их подполуполе $U \neq W$ является полем.

Полученный выше результат обобщается для правоциклического подполуполя (см. определение 5.5.6).

Следствие 5.3.14. *Полуполе W порядка p^n не содержит правоциклических над $\mathbb{Z}_p$ подполуполей порядка p^{n-1}.*

Доказательство. Достаточно рассмотреть правоупорядоченный минимальный многочлен правоциклического элемента a в подполуполе порядка p^{n-1}, характеристический многочлен соответствующей матрицы регулярного множества $A = \theta(a)$ имеет линейный делитель. □

5.4. Структурное описание полуполей порядка 16

В этом параграфе мы изучаем вопросы **(A)**–**(D)** для полуполей наименьшего возможного порядка 16.

В соответствии с перечислением Э. Клейнфелда [80], число собственных полуполей порядка 16, с точностью до изоморфизма, равно 23. Эти полуполя образуют два класса изотопизма из 18 (V_i, $1 \leq i \leq 18$) и 5 (T_{24}, T_{25}, T_{35}, T_{45} и T_{50}) попарно неизоморфных полуполей с ядрами N_l, N_m, N_r порядков 2 и 4 соответственно.

П. К. Штуккерт и В. М. Левчук сокращают [6] этот список, с точностью до изоморфизмов и антиизоморфизмов, до 16 полуполей.

Теорема 5.4.1. *Любое собственное полуполе порядка 16, с точностью до изоморфизма, есть либо одно из 7 полуполей* $V_1, V_3, V_4, V_8, V_{11}, V_{15}, T_{25}$ *или одно из противоположных к ним* $V_6, V_7, V_5, V_9, V_{14}, V_6, T_{50}$*, соответственно, или одно из 9 полуполей* $V_2, V_{10}, V_{12}, V_{13}, V_{17}, V_{18}, T_{21}, T_{35}, T_{45}$.

Э. Клейнфелд получает таблицу Кэли лупы W^* для любого полуполя $W = V_i$ или T_j с помощью специальной порождающей последовательности и выстраивает таблицу как латинский квадрат. Законы умножения для всех 16 полуполей представлены в [6]. Все вопросы строения для полуполей порядка 16 полностью решены [6, 126, 134] П. К. Штуккерт, В. М. Левчуком и автором.

Пусть $\mathcal{S}$ – множество всех подполей порядка 4 в данном полуполе. Следующая таблица обобщает результаты.

Таблица 11. Строение неизоморфных полуполей порядка 16

Полуполе W	$\lvert\mathcal{S}\rvert$	**Спектр**	**Правый спектр**	**Левый спектр**	$\lvert Aut\, W\rvert$	$\lvert At\, W\rvert$
$V_1 \simeq V_6^{op}$	0	$\{1,4,5\}$	$\{1,5,6,15\}$	$\{1,6,15\}$	1	18
V_2	1	$\{1,3,4,5,6\}$	$\{1,3,6,15\}$	$\{1,3,6,15\}$	2	18
$V_3 \simeq V_7^{op}$	0	$\{1,4,5,6\}$	$\{1,5,6,15\}$	$\{1,5,6,15\}$	1	18
$V_4 \simeq V_5^{op}$	1	$\{1,3,4,5,6\}$	$\{1,3,6,15\}$	$\{1,3,5,6,15\}$	1	18
$V_8 \simeq V_9^{op}$	2	$\{1,3,4,5,6\}$	$\{1,3,6,15\}$	$\{1,3,5,6,15\}$	2	18
V_{10}	1	$\{1,3,5,6\}$	$\{1,3,6,15\}$	$\{1,3,6,15\}$	3	18
$V_{11} \simeq V_{14}^{op}$	1	$\{1,3,4,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,6,15\}$	2	18
V_{12}	0	$\{1,4,5,6\}$	$\{1,5,6,15\}$	$\{1,5,6,15\}$	1	18
V_{13}	4	$\{1,3,5\}$	$\{1,3,15\}$	$\{1,3,15\}$	6	18
$V_{15} \simeq V_{16}^{op}$	2	$\{1,3,4,5\}$	$\{1,3,6,15\}$	$\{1,3,6,15\}$	2	18
V_{17}	1	$\{1,3,4,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,5,6,15\}$	1	18
V_{18}	2	$\{1,3,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,5,6,15\}$	2	18
T_{24}	2	$\{1,3,4,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,5,6,15\}$	2	108
$T_{25} \simeq T_{50}^{op}$	2	$\{1,3,4,5,6\}$	$\{1,3,5,6,15\}$	$\{1,3,6,15\}$	2	108
T_{35}	1	$\{1,3,4,5,6\}$	$\{1,3,6,15\}$	$\{1,3,6,15\}$	3	108
T_{45}	3	$\{1,3,5\}$	$\{1,3,5,15\}$	$\{1,3,5,15\}$	4	108

Метод Клейнфелда не подходит для полуполей порядка более 16. Общим методом является использование регулярного множества. Автором независимо построены все регулярные множества в $GL_4(2)$, их количество 19936:

$$R = \{\, \theta(x_1,x_2,x_3,x_4) = x_1E + x_2A_2 + x_3A_3 + x_4A_4 \mid\ x_i \in \mathbb{Z}_2,\ i = 1,2,3,4\}\,,$$

$A_2, A_3, A_4 \in GL_4(2)$. Здесь первая строка матрицы $\theta(x)$ совпадает с x. Для разбиения этой совокупности на классы изоморфизма рассмотрим линейное преобразование φ 4-мерного линейного пространства W над полем $\mathbb{Z}_2$, заданное матрицей $B \in GL_4(2)$. Преобразование φ задает изоморфизм полуполя с регулярным множеством $R = \{\theta(x) \mid x \in W\}$ на полуполе с регулярным множеством $S = \{\tau(x) \mid x \in W\}$ тогда и только тогда, когда выполнено условие

$$B^{-1}\theta(x)B = \tau(xB) \qquad \forall x \in W \tag{5.4.1}$$

(аналогично получено условие (5.1.6)). Ясно, что это условие достаточно проверять для только базисных векторов

$$e_1 = (1,0,0,0), \quad e_2 = (0,1,0,0), \quad e_3 = (0,0,1,0), \quad e_4 = (0,0,0,1). \tag{5.4.2}$$

Более того, из условия для e_1 получим равенство первой строки матрицы B вектору e_1. Непосредственный компьютерный перебор всех невырожденных 4×4-матриц над $\mathbb{Z}_2$ показывает, что все построенные полуполя разбиваются на 24 непересекающихся класса изоморфизма (считая 336 полей). Для каждого класса найдено 1344 матрицы B с условием (5.4.1), причем для каждого класса некоторые такие матрицы задают отображение полуполя на себя. Количество таких матриц – 1, 2, 3, 4 или 6, это порядок группы автоморфизмов. Учитывая это значение, находим мощность каждого класса изоморфизма. В следующей табл. 12 использованы обозначения Э. Клейнфелда.

Таблица 12. Классы изоморфизма полуполей порядка 16

Полуполе W	V_1, V_3, V_4, V_5, V_6, V_7, V_{12}, V_{17}	V_2, V_8, V_9, V_{11}, V_{14}, V_{15}, V_{16}, V_{18}, T_{24}, T_{25}, T_{50}	V_{10}, T_{35}	T_{45}	V_{13}	$GF(16)$
$\lvert Aut\, W\rvert$	1	2	3	4	6	4
Мощность класса изоморфизма	1344	672	448	336	224	336

18 классов полуполей V_i с ядрами порядка 2 (16800 регулярных множеств) координатизируют одну и ту же полуполевую плоскость порядка 16, так как все эти полуполя попарно изотопны. Для любой пары таких полуполей с регулярными множествами R и S существует 18 пар матриц (A, D) из $GL_4(2)$, удовлетворяющих условию

$$A^{-1}\theta(x)D \in S \qquad \forall\theta(x) \in R. \tag{5.4.3}$$

Таким образом, группа автотопизмов Λ каждого полуполя V_i имеет порядок 18.

5 классов полуполей T_i с ядрами порядка 4 (2800 регулярных множеств) образуют второй класс изотопизма и соответствуют второй полуполевой плоскости порядка 16. Группа автотопизмов Λ каждого полуполя T_i имеет порядок 108, это число пар матриц (A, D) с условием (5.4.3).

Полученные результаты иллюстрируют теорему, доказанную в [128].

Теорема 5.4.2. *Пусть π – полуполевая плоскость порядка p^n, p – простое число, $R \subset GL_n(p)\cup\{0\}$ – ее регулярное множество, Λ – группа автотопизмов плоскости π,*

$$\Psi = \left\{ \psi = \begin{pmatrix} \theta_1 D & 0 \\ 0 & D \end{pmatrix} \;\middle|\; \theta_1 \in R\setminus\{0\},\ D \in GL_n(p) \right\}.$$

Тогда количество регулярных множеств в $GL_n(p) \cup \{0\}$*, соответствующих полуполевым плоскостям, изоморфным* π*, равно*

$$\frac{|\Psi|}{|\Lambda|} = \frac{(p^n-1)|GL_n(p)|}{|\Lambda|}.$$

Действительно, имеем $GL_4(2) = 15{\cdot}14{\cdot}12{\cdot}8 = 20160$, тогда для первого класса изотопизма $\frac{15\cdot 20160}{18} = 16800$ и для второго класса $\frac{15\cdot 20160}{108} = 2800$, совпадает с компьютерными расчетами и результатами, например, таблицы выше:

$$16800 = 8\cdot 1344 + 8\cdot 672 + 1\cdot 448 + 1\cdot 224, \quad 2800 = 3\cdot 672 + 1\cdot 448 + 1\cdot 336.$$

Напомним также теорему Д. Кнута [82] о числе изотопных, но не изоморфных полуполей.

Теорема 5.4.3. *Пусть* D *– конечное полуполе,* $\mathcal{D}$ *– множество всех неизоморфных полуполей, изотопных* D*. Тогда*

$$(|D|-1)^2 = |At\, D| \sum_{E\in\mathcal{D}} \frac{1}{|Aut\, E|}.$$

Здесь $At\, D$ – группа автотопизмов полуполя D. В нашем случае для класса V_i имеем

$$15^2 = 18\cdot\left(8\cdot 1 + 8\cdot\frac{1}{2} + \frac{1}{3} + \frac{1}{6}\right),$$

для класса T_i:

$$15^2 = 108\cdot\left(3\cdot\frac{1}{2} + \frac{1}{3} + \frac{1}{4}\right).$$

Оба равенства, очевидно, верны.

Дополнительная информация о спектрах полуполей V_i и T_i, полученная автором, представлена в табл. 13. В ее позициях указано число элементов полуполя, имеющих указанный (левый, правый) порядок. Как и следует из определения противоположного кольца, в данной таблице совокупность данных о правом спектре каждого полуполя W совпадает с данными о левом спектре противоположного полуполя W^{op}, а информация о спектре для W и W^{op} одинакова. Сравним, допустим, строки V_1 и V_6: число элементов с левым порядком 3, 5, 6, 15 в V_1 равно 0, 0, 8, 6 соответственно. Это количества элементов с таким правым порядком в V_6.

Таблица 13. Порядки элементов неизоморфных полуполей порядка 16

Полуполе	Левый порядок				Правый порядок				Порядок			
	3	**5**	**6**	**15**	**3**	**5**	**6**	**15**	**3**	**4**	**5**	**6**
$V_1 \simeq V_6^{op}$			8	6		4	6	4		5	9	
V_6		4	6	4			8	6		5	9	
V_2	2		6	6	2		6	6	2	4	4	4
$V_3 \simeq V_7^{op}$		4	6	4		4	6	4		2	8	4
V_7		4	6	4		4	6	4		2	8	4
$V_4 \simeq V_5^{op}$	2	4	4	4	2		6	6	2	4	6	2
V_5	2		6	6	2	4	4	4	2	4	6	2
$V_8 \simeq V_9^{op}$	4	4	2	4	4		4	6	4	2	6	2
V_9	4		4	6	4	4	2	4	4	2	6	2
V_{10}	2		6	6	2		6	6	2		6	6
$V_{11} \simeq V_{14}^{op}$	2		6	6	2	4	4	4	2	2	10	
V_{14}	2	4	4	4	2		6	6	2	2	10	
V_{12}		4	6	4		4	6	4		4	9	1
V_{13}	8			6	8			6	8		6	
$V_{15} \simeq V_{16}^{op}$	4		4	6	4		4	6	4	2	8	
V_{16}	4		4	6	4		4	6	4	2	8	
V_{17}	2	4	4	4	2	4	4	4	2	3	7	2
V_{18}	4	4	2	4	4	4	2	4	4	0	6	4
T_{24}	4	4	2	4	4	4	2	4	4	4	2	4
$T_{25} \simeq T_{50}^{op}$	4		4	6	4	4	2	4	4	4	2	4
T_{50}	4	4	2	4	4		4	6	4	4	2	4
T_{35}	2		6	6	2		6	6	2	3	3	6
T_{45}	6	4		4	6	4		4	6		8	

Следует отметить, что левый и правый спектры полуполя не отражают полностью информацию о его строении: два элемента полуполя a и b с равными левыми и правыми порядками $|a|_l = |b|_l$, $|a|_r = |b|_r$ и даже равными лево-(право-)упорядоченными минимальными многочленами могут иметь разные порядки $|a| \neq |b|$. Например, в полуполе V_{17} четыре элемента имеют левый и правый порядок 6, лево- и правоупорядоченные минимальные многочлены $\mu_a^l(x) = \mu_a^r(x) = x^4 + x^2 + 1$, такой же минимальный многочлен имеет и соответствующая матрица регулярного множества. Однако из этих четырех элементов один имеет порядок 4, один – порядок 5 и два – порядок 6. Кроме того,

в этом же полуполе два элемента с $|a|_l = 15$, $|a|_r = 5$, $\mu_a^l(x) = x^4 + x^3 + 1$, $\mu_a^r(x) = \mu_A(x) = x^4 + x^3 + x^2 + x + 1$ имеют разные порядки 4 и 5.

Как мы видим, даже строение полуполей минимального возможного порядка пока не объясняется полностью известными методами. В связи с этим укажем один из девяти вопросов строения конечных полуполей, перечисленных М. Лаврау и О. Полверино в [84]: *найти новые инварианты классов изотопизма конечных полуполей.*

Отметим, что изотопные, но не изоморфные полуполя T_i имеют левое, среднее и правое ядра порядка 4. Порядки ядер N_l, N_m, N_r являются геометрическими инвариантами, т. е. сохраняются при иной координатизации полуполевой плоскости, так как мультипликативные группы ядер биективно соответствуют группам гомологий H_l, H_m, H_r (см. лемму 2.2.2). Известно также, что центр Z полуполя также является геометрическим инвариантом [70]:

Теорема 5.4.4. *Все полуполя, координатизирующие данную конечную полуполевую плоскость, имеют изоморфные центры.*

Тем не менее, этот результат не переносится на ядро полуполя, т.е. на пересечение $N_0 = N_l \cap N_m \cap N_r$. В частности, у полуполя T_{35} все три ядра совпадают: $N_l = N_m = N_r$. У полуполя T_{45} это три различных подполя порядка 4. У трех оставшихся полуполей T_i число подполей порядка 4 равно двум, либо $N_l = N_m \neq N_r$, либо $N_l = N_r \neq N_m$, либо $N_r = N_m \neq N_l$. Одно из полуполей V_i имеет ядра порядка 2, но содержит четыре различных подполя порядка 4. Таким образом, заключаем, что изотопизм полуполей, в отличие от изоморфизма, не сохраняет многие важные особенности строения.

Уточняя ответ на вопрос **(D)** о группе автоморфизмов полуполей порядка 16, докажем следующий результат.

Теорема 5.4.5. *Ровно пять неизоморфных полуполей W порядка 16 допускают нетривиальные внутренние автоморфизмы, т. е. заданные сопряжением $\varphi : x \to (a_l^{-1}x)a$ $(x \in W)$, где $a_l^{-1}a = e$. Это полуполя T_{25} и T_{50} с одним инволютивным внутренним автоморфизмом и полуполя T_{35}, V_{10}, V_{13} с двумя внутренними автоморфизмами порядка три.*

Доказательство. Пусть $a \in W$ – произвольный ненулевой элемент полуполя, a_l^{-1} – его левый обратный, $a_l^{-1}a = e$. Очевидно, отображение φ есть линейное преобразование пространства W. Его матрицу можем получить, рассматривая образы базисных элементов e_i (5.4.2). Сравнивая полученную матрицу с уже найденными автоморфизмами всех 23 полуполей V_i и T_i, получим:

1) для T_{25}

$$i = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ i^2 = \varepsilon, \quad Aut\, T_{25} = In\, T_{25} \simeq \mathbb{Z}_2;$$

2) для T_{50}

$$i = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix},\ i^2 = \varepsilon, \quad Aut\, T_{50} = In\, T_{50} \simeq \mathbb{Z}_2;$$

3) для T_{35}

$$j = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix},\ j^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix},\ j^3 = \varepsilon, \quad Aut\, T_{35} = In\, T_{35} \simeq \mathbb{Z}_3;$$

4) для V_{10}

$$j = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},\ j^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix},\ j^3 = \varepsilon, \quad Aut\, V_{10} = In\, V_{10} \simeq \mathbb{Z}_3;$$

5) для V_{13}

$$j = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ j^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ j^3 = \varepsilon, \quad Aut\, V_{13} \simeq S_3,\ In\, V_{13} \simeq \mathbb{Z}_3.$$

Для всех остальных полуполей единственный внутренний автоморфизм – это тождественное преобразование ε. □

Следующая теорема представляет аномальные свойства внутренних автоморфизмов полуполей порядка 16 (см. теорему 5.2.5 Г. Венэ).

Теорема 5.4.6. *1. Существуют 4 полуполя порядка 16, которые допускают внутренние автоморфизмы λ_m, порожденные элементами $m \notin N_0$, не принадлежащими ядру полуполя.*

2. Существуют 4 полуполя порядка 16, в которых множество элементов

$$\mathcal{M} = \{m \in W \mid \lambda_m \in In\, W\}$$

не замкнуто относительно сложения и умножения.

3. Существуют 2 полуполя порядка 16, для которых тождественный внутренний автоморфизм $\lambda_m = \varepsilon$ порождается элементами не из центра $m \notin Z$.

Эта теорема обобщает результаты расчетов, приведенные в табл. 14 (здесь $e = (1, 0, 0, 0)$ – единица полуполя).

Таблица 14. Особенности внутренних автоморфизмов полуполей порядка 16

Полуполе	$\lvert N_r\rvert = \lvert N_m\rvert = \lvert N_l\rvert$	$\lvert Aut\, W\rvert$	$\lvert In\, W\rvert$	$\lambda_m,\ m \notin N_0$ (не из ядра)	$\lambda_m = \varepsilon,\ m \notin Z$ (не из центра)
T_{25}	4	2	2	$m \in N_r \setminus (N_m \cup N_l)$	-
T_{50}	4	2	2	$m \in N_l \setminus (N_m \cup N_r)$	-
V_{13}	2	6	3	$\{0, e, m, m+e\}$ – подполе $\neq N_0$	-
V_{10}	2	3	3	$\{0, e, m, m+e\}$ – подполе $\neq N_0$	-
T_{35}	4	3	3	$m, m+e \in N$	-
V_1	2	1	1	$m = (0, 0, 1, 0)$	$m \neq e$
V_6	2	1	1	$m = (0, 0, 0, 1)$	$m \neq e$

Обсудим далее различные способы задания полуполей. Примеры двух полуполей порядка 16 построены Д. Кнутом [82] на основе двумерного векторного пространства над полем $GF(4) = \{0, 1, \omega, \omega + 1\}$ $(\omega^2 = \omega + 1)$ с поэлементным сложением пар и законом умножения

$$(u, v) \circ (x, y) = (ux + \omega v^2 y, vx + u^2 y) \quad \text{или}$$

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

В обозначениях Э. Клейнфелда эти полуполя изоморфны T_{35} и V_{13} соответственно.

Для конечного полуполя порядка p^n матричное представление регулярного множества над простым подполем $\mathbb{Z}_p$ является универсальным способом определения операции умножения. Тем не менее, в некоторых случаях оказывается удобнее задавать элементы полуполя не n-мерными векторами, а элементами или парами элементов подходящего конечного поля. Рассмотрим возможность задания всякого полуполя порядка p^4 парами элементов поля $GF(p^2)$.

Следующая теорема, доказанная автором, была успешно применена студенткой А. В. Поповой для всех 23 неизоморфных полуполей порядка 16 [14]. Были получены законы умножения для всех V_i и T_j, в том числе два закона Д. Кнута, указанные выше.

Теорема 5.4.7. *Пусть $(W, +, *)$ – полуполе порядка p^4 (p – простое), $\overline{W}$ – двумерное линейное пространство над полем $GF(p^2)$. Определим операцию $\circ$ правилом*

$$(u, v) \circ (x, y) = (\overline{u}\, Z\, \overline{x}^T, \overline{u}\, T\, \overline{x}^T) \quad (u, v, x, y \in GF(p^2)), \tag{5.4.4}$$

где Z, T – 4×4-матрицы над $GF(p^2)$, $\overline{u} = (u, v, u^p, v^p)$, $\overline{x} = (x, y, x^p, y^p)$. Тогда матрицы Z, T можно выбрать так, что полуполе $(W, +, *)$ изоморфно $(\overline{W}, +, \circ)$ (сложение стандартное).

Доказательство. Зададим полуполе W элементами 4-мерного векторного пространства над $\mathbb{Z}_p$, пусть $w_1, \ldots, w_4$ – его базис, $R \subset GL_4(p) \cup \{0\}$ – регулярное множество с базисом $A_1, \ldots, A_4$. По лемме 2.1.5, строки матриц A_j образованы координатами произведений $w_i * w_j$ векторов базиса.

Далее, пусть ω – примитивный элемент поля $GF(p^2)$ и

$$e_1 = (1, 0),\ e_2 = (\omega, 0),\ e_3 = (0, 1),\ e_4 = (0, \omega)$$

– базис пространства $\overline{W}$ над $\mathbb{Z}_p$. Зададим изоморфизм линейных пространств W и $\overline{W}$ правилом $w_i \to e_i$ $(i = 1, \ldots, 4)$. Для доказательства теоремы достаточно рассмотреть произведения базисных элементов $e_i \circ e_j$ и показать, что для произвольных матриц A_j система линейных уравнений относительно неизвестных элементов z_{ij}, t_{ij} матриц Z, T имеет единственное решение.

Согласно условию теоремы, пусть

$$\overline{e_1} = (1, 0, 1, 0), \quad \overline{e_2} = (\omega, 0, \omega^p, 0), \quad \overline{e_3} = (0, 1, 0, 1), \quad \overline{e_4} = (0, \omega, 0, \omega^p).$$

Вычислим, например, произведения $\overline{e_i}\, Z\, \overline{e_j}^T$ для $i, j = 1, 2$:

$$\begin{aligned}
\overline{e_1}\, Z\, \overline{e_1}^T &= z_{11} + z_{31} + z_{13} + z_{33},\\
\overline{e_2}\, Z\, \overline{e_1}^T &= z_{11}\omega + z_{31}\omega^p + z_{13}\omega + z_{33}\omega^p,\\
\overline{e_1}\, Z\, \overline{e_2}^T &= (z_{11} + z_{31})\omega + (z_{13} + z_{33})\omega^p,\\
\overline{e_2}\, Z\, \overline{e_2}^T &= (z_{11}\omega + z_{31}\omega^p)\omega + (z_{13}\omega + z_{33}\omega^p)\omega^p.
\end{aligned}$$

Основной определитель системы линейных уравнений для неизвестных z_{11}, z_{13}, z_{31}, z_{33} равен

$$\Delta = \begin{vmatrix} 1 & 1 & 1 & 1 \\ \omega & \omega^p & \omega & \omega^p \\ \omega & \omega & \omega^p & \omega^p \\ \omega^2 & \omega^{p+1} & \omega^{p+1} & \omega^{2p} \end{vmatrix}.$$

Это кронекеровский квадрат определителя $\begin{vmatrix} 1 & 1 \\ \omega & \omega^p \end{vmatrix}$, он равен $(\omega^p - \omega)^4$ (см., например, [17, 122]). Так как ω – примитивный элемент поля $GF(p^2)$, то $\omega^p \neq \omega$ и $\Delta \neq 0$. Проводя вычисления остальных произведений аналогично, видим, что все элементы матриц Z и T определяются однозначно выбором регулярного множества R. Таким образом, изоморфизм $W \simeq \overline{W}$ доказан. □

Пример 5.5. Далее представлены законы умножения в двух полуполях порядка 16, V_6 и T_{24}. Остальные законы перечислены А. В. Поповой в [14].

$$V_6: \quad (u,v)\circ(x,y) = (ux + v^2y, vx + vy + u^2y);$$

$$Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

$$\begin{aligned} T_{24}: \quad & (u,v)\circ(x,y) = (\omega^2ux + uy + \omega^2vx + \\ & + \omega u^2x + u^2y + \omega^2v^2y + \omega ux^2 + \omega^2vx^2 + \omega vy^2 + \omega u^2x^2 + \omega v^2y^2, \\ & \omega^2ux + \omega^2uy + \omega vx + \omega^2u^2x + \omega u^2y + v^2x + \omega^2v^2y + \omega^2ux^2 + \\ & + uy^2 + \omega^2vx^2 + vy^2 + \omega^2u^2x^2 + u^2y^2 + v^2x^2 + v^2y^2); \end{aligned}$$

$$Z = \begin{pmatrix} \omega^2 & 1 & \omega & 0 \\ \omega^2 & 0 & \omega^2 & \omega \\ \omega & 1 & \omega & 0 \\ 0 & \omega^2 & 0 & \omega \end{pmatrix}, \quad T = \begin{pmatrix} \omega^2 & \omega^2 & \omega^2 & 1 \\ \omega & 0 & \omega^2 & 1 \\ \omega^2 & \omega & \omega^2 & 1 \\ 1 & \omega^2 & 1 & 1 \end{pmatrix}.$$

Используя тот же алгоритм, поле порядка 16 тоже можем задать парами элементов из $GF(4)$ с умножением, например,

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

5.5. Гипотеза Венэ примитивности конечного полуполя

В 1991 году Г. Венэ [119] выдвинул гипотезу: *всякое конечное полуполе W право- или левопримитивно*, т. е. лупа W^* есть множество право- или левоупорядоченных степеней некоторого элемента полуполя W. Венэ показал также, что все полуполя до порядка 27 включительно право- и левопримитивны. В 2004 г. И. Руа [100] указал контрпример к предположению Венэ, используя бинарное полуполе Кнута порядка 32. Это коммутативное *полуполе Кнута–Руа* не является ни право-, ни левопримитивным. Второй контрпример представляет *полуполе Хентзела–Руа* [61] порядка 64, построенное в 2007 г. К настоящему

времени исследования проблемы примтивности полностью завершены для всех полуполей до порядка 125 включительно. Кроме двух указанных непримитивных полуполей, не обнаружено новых примеров. Заметим, что контрпримеры нечетного порядка до сих пор не найдены.

Исследования проблемы примитивности основаны на свойствах регулярного множества. Известно, что для любого конечного полуполя W с центром $Z \simeq GF(q)$ и регулярным множеством Σ характеристический многочлен любой матрицы из $\Sigma \setminus \{\lambda E \mid \lambda \in GF(q)\}$ не имеет линейных делителей (см. также лемму 5.3.10). Следующая теорема, доказанная в [61], используется в качестве основного инструмента для исследования.

Теорема 5.5.1. *Если W – конечное полуполе размерности n над своим центром $Z \simeq GF(q)$, то $w \in W$ является левопримитивным элементом W тогда и только тогда, когда характеристический многочлен линейного преобразования $L_w : W \to W$, заданного как $L_w(x) = w * x$, есть неприводимый примитивный многочлен степени n над Z.*

Некоторые условия примитивности полуполей, полученные И. Руа [100], Р. Гау и Д. Шики [56], представляет теорема.

Теорема 5.5.2. *Пусть W – полуполе, n-мерное над своим центром $GF(q)$. Тогда W и лево- и правопримитивно, если $n = 3$ либо если n простое и q достаточно велико.*

М. Кордеро и В. Джа [38, 39] изучали проблему примитивности для квазиполей и некоторые геометрические условия примитивности полуполей.

Теорема 5.5.3. *Непримитивное квазиполе порядка q^2 существует тогда и только тогда, когда $q > 4$.*

Теорема 5.5.4. *Для достаточно большого простого числа p полуполя, координатизирующие полуполевую плоскость Π порядка p^5, все являются примитивными (и право-, и лево-), если Π не содержит собственных подплоскостей порядка $> p$.*

Примеры непримитивных полуполей позволяют предположить связь примитивности с размерностью полуполя как линейного пространства над своим центром. Все трехмерные над центром полуполя обладают свойствами право- и левопримитивности, непримитивные примеры имеют размерность 5 и 6. Для полуполей размерности 4 над центром $GF(q)$ в 2015 г. И. Руа [104] доказал право- и левопримитивность при достаточно большом q:

Теорема 5.5.5. *Если $q > 25944$ и нечетно, то полуполе размерности 4 над центром $GF(q)$ является право- и левопримитивным.*

Для 4-мерных полуполей достаточно большого четного порядка 2^{4e} право- и левопримитивность доказана И. Руа в 2017 г. [105].

Заметим, что Г. Венэ и некоторые его последователи называли правопримитивный элемент полуполя или квазиполя также «правоциклическим элементом». Исследование гипотезы Венэ и примеры И. Руа показали целесообразность использования этого термина в другом смысле.

Определение 5.5.6. *Пусть W – конечное полуполе, рассматриваемое как n-мерное линейное пространство над своим центром Z. Элемент $a \in W$ называется правоциклическим (над Z), если элементы*

$$e,\ a,\ a^{2)}, \ldots,\ a^{n-1)}$$

образуют базис W. Полуполе W, содержащее правоциклический элемент, также называется правоциклическим (над Z).

Левоциклический элемент и левоциклическое полуполе определяются аналогично. Заметим, что иногда более удобно рассматривать полуполе как линейное пространство над простым подполем $\mathbb{Z}_p$ и, соответственно, право- и левоцикличность над $\mathbb{Z}_p$. Все известные к настоящему моменту конечные полуполя являются право- и левоциклическими, в том числе и контрпримеры к гипотезе Венэ. Следующий результат вытекает из теоремы 5.5.1, но докажем его для полноты изложения.

Теорема 5.5.7. *Всякое правопримитивное полуполе также является правоциклическим над своим центром.*

Доказательство. Пусть полуполе W n-мерно над своим центром Z и W имеет правопримитивный элемент a, тогда минимальный многочлен матрицы $\theta(a)$ является неприводимым многочленом степени. Поскольку правоупорядоченный минимальный многочлен (над Z) элемента a делит минимальный многочлен матрицы, по теореме 5.3.8, то $\mu_a^r(x)$ также имеет степень n. Тогда элементы e, a, $a^2, a^{3)}, \ldots,\ a^{n-1)}$ линейно независимы и поэтому образуют базис n-мерного линейного пространства. □

Обратное утверждение неверно: даже известные непримитивные полуполя порядков 32 и 64 левоциклические и правоциклические. Эти полуполя содержат элементы с односторонне-упорядоченными минимальными многочленами степеней 5 и 6 соответственно (см. далее). Таким образом, понятие правоцикличности (левоцикличности) позволяет ослабить предположение Г. Венэ:

Гипотеза 1. *Всякое конечное полуполе является право- или левоциклическим над своим центром.*

Эта гипотеза легко подтверждается [187] для некоторых полуполей порядка p^4.

Теорема 5.5.8. *Если полуполе порядка p^4 имеет левое или правое ядро порядка p^2, то полуполе является лево- и правоциклическим над $\mathbb{Z}_p$.*

Доказательство. Пусть $(W, +, \cdot)$ – полуполе порядка p^4 и его левое ядро N_l имеет порядок p^2. Тогда W можно рассматривать как левое векторное пространство размерности 2 над N_l:

$$W = \{te + za \mid t, z \in N_l\},$$

где e – единица полуполя и $a \notin N_l$. Предположим, что полуполе W не является левоциклическим или не является правоциклическим. Тогда любой его элемент имеет левоупорядоченный (правоупорядоченный) минимальный многочлен степени не выше 2 (см. теоремы 5.3.10 и 5.3.13). Значит, W есть объединение подполей порядка p^2. Из этого следует, что любой ненулевой элемент обратим и, например, $a^{-1} = ke + ma$, где $k, m \in \mathbb{Z}_p$.

Докажем, что W обладает правым обратным свойством (RIP): для любого $x \in W$ найдется такой элемент $x^{-1} \in W$, что для всех $y \in W$ верно $(yx)x^{-1} = y$. Ясно, что без ограничения общности достаточно полагать $x = a$ и $y = te + az$. Из $a^{-1} = ke + ma$ следует $a^2 = \frac{1}{m}\, e - \frac{k}{m}\, a$, имеем:

$$(yx)x^{-1} = ((te + za)a)a^{-1} = (ta + (za)a)a^{-1} = (ta)a^{-1} + ((za)a)a^{-1} =$$

$$= t(aa^{-1}) + (z(a^2))a^{-1} = te + \left(z\left(\frac{1}{m}\, e - \frac{k}{m}\, a\right)\right)a^{-1} = te + \left(\frac{1}{m}\, z - \frac{k}{m}\, (za)\right)a^{-1} =$$

$$= te + \frac{1}{m}\, za^{-1} - \frac{k}{m}\, (za)a^{-1} = te + \frac{1}{m}\, z(ke + ma) - \frac{k}{m}\, z(aa^{-1}) = te + za = y.$$

Тогда, по теореме 1.1.5, полуполе W альтернативно и, по теореме Артина–Цорна 1.1.6, является полем. Так как поле порядка p^4 не может быть объединением своих подполей порядка p^2, получили противоречие с предположением нецикличности. Таким образом, в случае $|N_l| = p^2$ теорема доказана. Результат для $|N_r| = p^2$ получается переходом к противоположному полуполю W^{op}. $\square$

Следствие 5.5.9. *Если полуполе порядка p^4 имеет левое или правое ядро порядка p^2, то полуполе не может быть объединением своих подполей порядка p^2.*

Обратим внимание на это следствие и сравним его с примером П. К. Штуккерт [86] *квазиполей* порядка 16. Три квазиполя Q_j из списка У. Демпволфа [45] являются теоретико-множественными объединениями семи максимальных подполей порядка 4, все их спектры равны $\{1, 3\}$.

Гипотеза В. М. Левчука об однопорожденности (см. вопросы **(A)**–**(D)**) также ослабляет предположение Г. Венэ:

Гипотеза 2. *Мультипликативная лупа W^* любого конечного полуполя порождается одним элементом.*

Эта гипотеза также справедлива для изученных на текущий момент конечных полуполей, даже исключительные непримитивные полуполя Кнута–Руа и Хентзела–Руа имеют однопорожденную лупу (см. § 5.7, 5.8).

5.6. Полуполе Кнута–Руа порядка 32

Полуполе Кнута–Руа порядка 32 представляет первый контрпример к гипотезе Венэ примитивности конечных полуполей. Это коммутативное полуполе с тождеством $x^{(22} = x$, заданное, например, регулярным множеством

$$R = \{\theta(x_1, \ldots, x_5) = x_1A_1 + \cdots + x_5A_5 \mid x_i \in \mathbb{Z}_2,\ i = 1, \ldots, 5\},$$

где $A_1 = E$,

$$A_2 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}, \quad A_5 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Вопросы **(A)**–**(C)** для полуполя $\mathcal{R}$ решены П. К. Штуккерт в [19, 6].

Теорема 5.6.1. *Лупа $\mathcal{R}^*$ полуполя Кнута–Руа $\mathcal{R}$ порядка 32 порождается любым неединичным элементом. Ее спектр равен $\{1, 5, 6, 7, 8, 10\}$, правый и левый спектры совпадают с $\{1, 21\}$. Единственным подполем в $\mathcal{R}$ является простое подполе $\mathbb{Z}_2$.*

Обозначим $K(m)$ множество элементов, имеющих порядок m, при этом запишем $K(7)$ в виде объединения $K(7) = K_a(7) \cup K_b(7)$. Здесь $K_a(7)$ есть множество элементов порядка 7 с минимальным многочленом $x^5 + x^4 + 1$, а $K_b(7)$ – с минимальным многочленом $x^5 + x + 1$.

Вопрос **(D)** решен автором в следующей теореме.

Теорема 5.6.2. *1. Группа автоморфизмов $Aut\,\mathcal{R}$ полуполя Кнута–Руа $\mathcal{R}$ – циклическая группа порядка 5, и множество $\mathcal{R}\setminus\{0,e\}$ есть объединение шести орбит под действием $Aut\,\mathcal{R}$: $K(5)\cup K(6)\cup K_a(7)\cup K_b(7)\cup K(8)\cup K(10)$.*

2. Преобразование $\varphi: x\to x^2$ полуполя $\mathcal{R}$ является линейным преобразованием порядка 15, но не является автоморфизмом,

$$K(5)\xrightarrow{\varphi}K(8)\xrightarrow{\varphi}K_a(7)\xrightarrow{\varphi}K(5),\quad K(10)\xrightarrow{\varphi}K(6)\xrightarrow{\varphi}K_b(7)\xrightarrow{\varphi}K(10).$$

Доказательство. Пусть τ – автоморфизм полуполя $\mathcal{R}$. Тогда τ является линейным преобразованием векторного пространства $\mathcal{R}$ и задается некоторой 5×5-матрицей T над $\mathbb{Z}_2$. Выберем базис $\mathcal{R}$:

$$e_1=(1,0,0,0,0)=e,\quad e_2=(0,1,0,0,0),\quad \ldots,\quad e_5=(0,0,0,0,1)$$

и выясним, при каком условии верно

$$\tau(e_i*e_j)=\tau(e_i)*\tau(e_j),\quad i,j=1,2,\ldots,5.$$

Так как $e_i*e_j=e_i\theta(e_j)=e_iA_j$, то $\tau(e_i*e_j)=e_iA_jT$; далее

$$\tau(e_i)*\tau(e_j)=e_iT\theta(e_jT)=e_iT\theta(t_{j1},t_{j2},\ldots,t_{j5})=e_iT\sum_{k=1}^{5}t_{jk}A_k.$$

В силу произвольности $i=1,\ldots,5$ получим условие

$$T\sum_{k=1}^{6}t_{jk}A_k=A_jT,\quad j=1,\ldots,5. \tag{5.6.1}$$

При $j=1$ имеем, в частности, $t_{11}=1$, $t_{12}=t_{13}=\cdots=t_{15}=0$. Каждая матрица $T\in GL_5(2)$, удовлетворяющая условию (5.6.1), задает автоморфизм полуполя $\mathcal{R}$. Этому условию удовлетворяют ровно 5 матриц:

$$T_1=\begin{pmatrix}1&0&0&0&0\\0&0&0&1&1\\0&1&1&0&0\\1&0&1&0&0\\0&1&1&1&0\end{pmatrix},\quad T_2=\begin{pmatrix}1&0&0&0&0\\0&0&1&1&1\\1&0&1&0&1\\1&1&1&1&1\\0&1&0&0&1\end{pmatrix},$$

$$T_3=\begin{pmatrix}1&0&0&0&0\\1&0&1&1&0\\1&0&0&1&0\\0&0&1&0&1\\0&1&1&0&1\end{pmatrix},\quad T_4=\begin{pmatrix}1&0&0&0&0\\1&1&0&1&0\\0&1&1&1&1\\1&1&1&0&0\\1&1&0&1&1\end{pmatrix},\quad T_5=E.$$

Непосредственная проверка показывает, что $Aut\,\mathcal{R} = \{T_1, T_2, T_3, T_4, T_5\} \simeq \mathbb{Z}_5$ и $\mathcal{R}$ является объединением шести орбит, каждая из которых может включать только элементы одного порядка.

Так как полуполе $\mathcal{R}$ коммутативно, то $(x+y)^2 = x^2+x*y+y*x+y^2 = x^2+y^2$, но при этом $(x*y)*(x*y) \neq (x*x)*(y*y)$ $(x, y \in \mathcal{R})$. Вычисляя образы базисных элементов, получаем матрицу линейного преобразования φ:

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

и находим образы всех элементов полуполя $\mathcal{R}$. □

Информация о минимальных многочленах элементов полуполя $\mathcal{R}$ представлена в табл. 15. Действительно, полуполе Кнута–Руа не является ни лево-, ни правопримитивным, так как среди минимальных многочленов нет неприводимых многочленов 5-й степени. Анализ результатов приводит к выводам, подтверждающим для $\mathcal{R}$ гипотезы 1 и 2 (см. § 5.6).

Теорема 5.6.3. *Полуполе Кнута–Руа $\mathcal{R}$ порядка 32 является лево- и правоциклическим. Мультипликативная лупа $\mathcal{R}^*$ порождается любым элементом $a \neq 0, e$, она совпадает со множеством всех n-х степеней a при $n \geq 11$, если $|a| = 6, 8, 10$, при $n \geq 12$, если $|a| = 5, 7$. Полуполе $\mathcal{R}$ не допускает нетривиальных внутренних автоморфизмов.*

Доказательство. Лево- и правоцикличность полуполя следует из существования в $\mathcal{R}$ элементов с минимальным многочленом степени 5. Так как любой элемент a, отличный от нуля и единицы, является лево- и правоциклическим и порождает лупу $\mathcal{R}^*$, то по теореме 5.2.7 отображение $\lambda_a : x \to (a_l^{-1}x)a$ не может быть нетривиальным внутренним автоморфизмом. □

Таблица 15. Информация о полуполе Кнута–Руа порядка 32

$\|a\|$	Число элементов порядка $\|a\|$	Минимальные многочлены $\mu_a^l(x) = \mu_a^r(x) = \mu_A(x)$	Минимальная степень n, исчерпывающая $\mathcal{R}^*$
6	5	$x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$	11
10	5	$x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$	11
8	5	$x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$	11
5	5	$x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$	12
7	10	$x^5 + x^4 + 1$ или $x^5 + x + 1$	12

Еще раз обратим внимание на аномальные свойства конечных полуполей, в сравнении с конечными полями: на их мультипликативную лупу в общем случае не переносится теорема Лагранжа. Как указано в теореме 5.6.1, порядок (левый, правый) элемента в $\mathcal{R}$ не является делителем порядка лупы 31. Кроме того, преобразование $x \to x^2$ не является автоморфизмом.

5.7. Полуполе Хентзела–Руа порядка 64

В 2007 г. И. Руа и И. Хентзел указали [61] второй контрпример к гипотезе Г. Венэ. Полуполе Хентзела–Руа – единственное среди всех 87714 полуполей порядка 64, которое не является ни лево-, ни правопримитивным. Существует также 35 полуполей порядка 64, которые правопримитивны, но не являются левопримитивными (см. также классификацию полуполей порядка 64 в [102]).

Изучим строение полуполя Хентзела–Руа (подробнее см. [134, 133]), используя базис регулярного множества $R \subset GL_6(2) \cup \{0\}$, найденный в [61]. Пусть W – 6-мерное линейное пространство над $\mathbb{Z}_2$,

$$W = \{x = (x_1, \ldots, x_6) \mid x_i \in \mathbb{Z}_2,\ i = 1, \ldots, 6\}.$$

Определим инъективное отображение $\theta : W \to GL_6(2) \cup \{0\}$ правилом

$$\theta(x) = x_1 A_1 + \cdots + x_6 A_6, \quad (x \in W)$$

где базисные матрицы равны, согласно [61],

$$A_1 = E, \quad A_2 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_5 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix},$$

$$A_6 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Тогда $R = \{\theta(x) \mid x \in W\}$ – регулярное множество и $\langle W, +, * \rangle$ порядка 64 с умножением

$$x * y = x \cdot \theta(y) = x \sum_{i=1}^{6} y_i A_i.$$

Далее обозначаем это полуполе $\mathcal{H}$ и называем *полуполем Хентзела–Руа*. Вектор $e = (1, 0, \ldots, 0)$ является мультипликативной единицей этого полуполя.

Вопросы **(A)**–**(D)** для полуполя $\mathcal{H}$ решает следующая теорема.

Теорема 5.7.1. *Пусть $\mathcal{H}$ – исключительное непримитивное полуполе Хентзела–Руа порядка 64.*
1. Группа автоморфизмов полуполя $\mathcal{H}$ изоморфна симметрической группе S_3; полуполе не допускает нетривиальных внутренних автоморфизмов.
2. Полуполе $\mathcal{H}$ содержит точно шесть максимальных подполей: 5 подполей порядка 8, три из которых стабилизируются различными инволютивными автоморфизмами, и единственное подполе порядка 4, которое стабилизируется автоморфизмом порядка 3.
3. Спектр мультипликативной лупы $\mathcal{H}^*$ равен $\{1, 3, 5, 6, 7\}$, левый и правый спектры совпадают с $\{1, 3, 6, 7, 12, 15\}$.
4. Полуполе $\mathcal{H}$ является лево- и правоциклическим, его лупа $\mathcal{H}^*$ порождается любым своим элементом a, не принадлежащим объединению подполей; она совпадает со множеством всех n-х степеней a при $n \geq 10$.
5. Все ядра полуполя $\mathcal{H}$ совпадают с его простым подполем $\mathbb{Z}_2$, все элементы удовлетворяют тождествам $x^{(4} = x^{4)}$, $x^{(8} = x^{8)}$.

Доказательство. 1. Пусть τ – автоморфизм полуполя $\mathcal{H}$, заданный 6×6-матрицей T над $\mathbb{Z}_2$. Перепишем для нее условие (5.6.1):

$$T \sum_{k=1}^{6} t_{jk} A_k = A_j T, \quad j = 1, \ldots, 6. \tag{5.7.1}$$

Каждая матрица $T \in GL_6(2)$, удовлетворяющая условию (5.7.1), задает авто-

морфизм полуполя $\mathcal{H}$. Этому условию удовлетворяют ровно 6 матриц:

$$T_1 = \begin{pmatrix} 1&0&0&0&0&0\\ 0&0&0&1&1&1\\ 1&1&1&0&1&0\\ 1&0&1&1&1&0\\ 0&0&1&1&1&1\\ 0&1&0&1&1&0 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 1&0&0&0&0&0\\ 1&1&0&1&1&1\\ 0&1&0&0&1&0\\ 1&1&1&0&1&1\\ 0&0&1&1&0&1\\ 1&0&0&1&1&0 \end{pmatrix},$$

$$T_3 = \begin{pmatrix} 1&0&0&0&0&0\\ 0&0&0&1&1&1\\ 1&1&1&0&1&0\\ 1&1&0&0&1&1\\ 0&1&0&1&0&1\\ 1&1&0&1&1&0 \end{pmatrix}, \quad T_4 = \begin{pmatrix} 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 1&1&1&1&0&0\\ 1&0&1&0&1&0\\ 1&0&0&0&0&1 \end{pmatrix},$$

$$T_5 = \begin{pmatrix} 1&0&0&0&0&0\\ 1&1&0&1&1&1\\ 0&1&0&0&1&0\\ 1&1&1&1&1&0\\ 1&1&1&1&1&1\\ 0&0&0&1&1&0 \end{pmatrix}, \quad T_6 = E.$$

Так как $T_2 = T_1^2$, $T_1 = T_2^2$, $T_3^2 = T_4^2 = T_5^2 = E$, то $Aut\,\mathcal{H} = \{T_1, T_2, T_3, T_4, T_5, T_6\} \simeq S_3$. Непосредственные расчеты показывают, что все перечисленные автоморфизмы не являются внутренними. Первое утверждение теоремы доказано.

2. Рассмотрим множество $F = \{0, e, a = (0,1,0,0,0,1), a+e\}$ и вычислим произведение

$$a * a = a \cdot \theta(a) = a(A_2 + A_6) = (1,1,0,0,0,1) = a + e;$$

поэтому $F \simeq GF(4)$ – подполе порядка 4. Обозначим $h_1 = (0,0,0,0,1,0)$ и вычислим h_1^2 и h_1^3:

$$h_1^2 = h_1\theta(h_1) = h_1 A_5 = (0,0,1,1,0,1), \quad h_1^{(3} = h_1^{3)} = (1,0,0,0,1,0) = e + h_1.$$

Тогда h_1 – корень многочлена x^3+x+1, неприводимого над $\mathbb{Z}_2$, и в силу $h_1^{(3} = h_1^{3)}$ множество $H_1 = \{0, e, h_1, h_1^2, \ldots, h_1^6\}$ есть подполе порядка 8 в W. Аналогично, имеем:

$$h_2 = (0,0,0,1,0,1), \quad h_2^2 = (0,1,0,1,1,1), \quad h_2^{(3} = h_2^{3)} = (1,1,0,1,1,1) = e + h_2^2,$$

$$H_2 = \{0, e, h_2, h_2^2, \ldots, h_2^6\};$$

$$h_3 = (0,0,0,1,1,1), \quad h_3^2 = (1,1,1,0,1,0), \quad h_3^{(3} = h_3^{3)} = (1,0,0,1,1,1) = e + h_3,$$
$$H_3 = \{0, e, h_3, h_3^2, \ldots, h_3^6\};$$
$$h_4 = (0,0,1,0,0,0), \quad h_4^2 = (0,1,1,0,0,0), \quad h_4^{(3} = h_4^{3)} = (1,0,1,0,0,0) = e + h_4,$$
$$H_4 = \{0, e, h_4, h_4^2, \ldots, h_4^6\};$$
$$h_5 = (0,0,1,0,1,0), \quad h_5^2 = (1,1,0,1,0,1), \quad h_5^{(3} = h_5^{3)} = (0,1,0,1,0,1) = e + h_5^2,$$
$$H_5 = \{0, e, h_5, h_5^2, \ldots, h_5^6\}.$$

Поскольку элементы h_1, h_3, h_4 – корни многочлена x^3+x+1, h_2, h_5 – многочлена $x^3 + x^2 + 1$ (неприводимых над $\mathbb{Z}_2$), множества H_1, H_2, H_3, H_4, H_5 являются подполями порядка 8 в полуполе W. Рассмотрим

$$U = \mathcal{H} \setminus (F \cup H_1 \cup H_2 \cup H_3 \cup H_4 \cup H_5). \tag{5.7.2}$$

Для каждого элемента $x \in U$ левая и правая третьи степени не совпадают: $x^{(3} \neq x^{3)}$. Следовательно, полуполе $\mathcal{H}$ не содержит подполей, кроме простого подполя, F и H_i, $i = 1, \ldots, 5$. Обозначим $\mathcal{F}(\tau)$ множество элементов полуполя W, фиксируемых преобразованием τ. Несложно вычислить, что

$$\mathcal{F}(T_1) = \mathcal{F}(T_2) = F, \quad \mathcal{F}(T_3) = H_2, \quad \mathcal{F}(T_4) = H_4, \quad \mathcal{F}(T_5) = H_3.$$

Второе утверждение теоремы доказано.

3. Для описания спектров введем следующие обозначения:

$$K(m,n,k) = \{x \in \mathcal{H} \mid |x|_l = m,\ |x|_r = n,\ |x| = k\}, \quad m,n,k \in \mathbb{N}.$$

Тогда, очевидно,

$$K(3,3,3) = \{x \in \mathcal{H} \mid |x|_l = |x|_r = |x| = 3\} = \{a, e+a\} = F \setminus \{0, e\};$$

$$K(7,7,7) = \{x \in \mathcal{H} \mid |x|_l = |x|_r = |x| = 7\} = (H_1 \cup H_2 \cup H_3 \cup H_4 \cup H_5) \setminus \{0, e\},$$

$|K(7,7,7)| = 30$, $K(3,3,3) \cup K(7,7,7) \cup \{0, e\}$ – объединение всех подполей. Далее,

$$K(6,6,6) = \{x \in \mathcal{H} \mid |x|_l = |x|_r = |x| = 6\} =$$
$$= \{a_1 = (0,0,0,1,0,0), a_2 = (0,0,1,1,1,0), a_3 = (0,1,0,0,1,1), a_4 = (0,1,1,0,1,1),$$
$$a_5 = (0,1,1,1,0,0), a_6 = (0,1,1,1,1,0), e+a_1, e+a_2, e+a_3, e+a_4, e+a_5, e+a_6\},$$

$$|K(6,6,6)| = 12;$$

$$K(7,7,6) = \{x \in \mathcal{H} \mid |x|_l = |x|_r = 7, |x| = 6\} = \{b_1 = (0,0,0,0,0,1),$$
$$b_2 = (0,0,0,1,1,0), b_3 = (0,1,0,1,1,0), e+b_1, e+b_2, e+b_3\},$$

$$|K(7,7,6)| = 6;$$

$$K(12,12,7) = \{x \in \mathcal{H} \mid |x|_l = |x|_r = 12, |x| = 7\} = \{c_1 = (0,0,1,0,0,1),$$
$$c_2 = (0,0,1,1,0,0), c_3 = (0,1,0,1,0,0), e + c_1, e + c_2, e + c_3\},$$
$$|K(12,12,7)| = 6;$$
$$K(15,15,5) = \{x \in \mathcal{H} \mid |x|_l = |x|_r = 15, |x| = 5\} = \{d_1 = (0,0,0,0,1,1),$$
$$d_2 = (0,0,1,0,1,1), d_3 = (0,1,1,0,0,1), e + d_1, e + d_2, e + d_3\},$$
$$|K(15,15,5)| = 6;$$
$$\mathcal{H}^* = \{e\} \cup K(3,3,3) \cup K(7,7,7) \cup K(6,6,6) \cup K(7,7,6) \cup K(12,12,7) \cup K(15,15,5).$$

Из этого перечисления следует третье утверждение теоремы. Левый и правый спектры лупы не содержат числа $63 = |\mathcal{H}^*| - 1$, поэтому полуполе $\mathcal{H}$ не является ни лево-, ни правопримитивным.

Заметим также, что полуполе $\mathcal{H}$ не коммутативно (например, $x^{3)} \neq x^{(3}$ для $x \in U$), но для любого элемента $x \in \mathcal{H}^*$ левый и правый порядки равны, $|x|_l = |x|_r$. Кроме того, для любого элемента $x \in \mathcal{H}^*$, $x \neq e$, (левый, правый) порядок элемента $e + x$ равен (левому, правому) порядку элемента x,

$$|e + x| = |x|, \ |e + x|_l = |x|_l, \ |e + x|_r = |x|_r.$$

4. Вычислим последовательно третьи, четвертые, пятые и следующие степени каждого элемента $x \in U$ (5.7.2), получим при этом все элементы $\mathcal{H}^*$. Для каждого $x \in U$ выберем наименьшее число $n = n(x)$ такое, что все n-е степени элемента x образуют $\mathcal{H}^*$, тогда $n(x) = 8$ для $x \in K(7,7,6)$, $n(x) = 9$ для $x \in K(6,6,6) \cup K(15,15,5)$, $n(x) = 10$ для $x \in K(12,12,7)$. Таким образом, каждый элемент $x \in U$ порождает лупу $\mathcal{H}^*$, причем для любого $n \geq 10$ все n-е степени элемента x исчерпывают $\mathcal{H}^*$.

Лево- и правоцикличность полуполя $\mathcal{H}$ следуют из информации в табл. 16: все элементы множеств $K(7,7,6)$ и $K(12,12,7)$ обладают лево- и правоупорядоченными минимальными многочленами степени 6, являясь одновременно лево- и правоциклическими элементами. Отметим, что среди многочленов степени 6 в табл. 16 действительно нет неприводимых.

Пятое утверждение проверяется непосредственными вычислениями. □

Вычисление спектров показывает, что на лупу $\mathcal{H}^*$ не переносится теорема Лагранжа. Действительно, $63 = |\mathcal{H}^*|$ не делится на 5, 6, 12 и 15. Однако заметим, что для произвольного элемента $x \in \mathcal{H}^*$, $x \neq e$, его левый и правый порядки имеют общий делитель с 63.

Свойства полуполя Хентзела–Руа $\mathcal{H}$ описывает также следующая лемма. Ее результаты использовались для упрощения вычислений, необходимых для доказательства теоремы 5.7.1.

Лемма 5.7.2. *Преобразование $\varphi : x \to x^2$ полуполя $\mathcal{H}$ биективно, но не является линейным преобразованием, причем $\varphi^6 = \varepsilon$,*

$$K(3,3,3) \xrightarrow{\varphi} K(3,3,3), \quad K(7,7,7) \xrightarrow{\varphi} K(7,7,7), \quad K(6,6,6) \xrightarrow{\varphi} K(6,6,6),$$

$$K(7,7,6) \xrightarrow{\varphi} K(12,12,7) \xrightarrow{\varphi} K(15,15,5) \xrightarrow{\varphi} K(7,7,6).$$

Доказательство. Вычисляя для каждого $x \in \mathcal{H}$ значение

$$\varphi(x) = x * x = x\theta(x) = x(x_1A_1 + x_2A_2 + x_3A_3 + x_4A_4 + x_5A_5 + x_6A_6),$$

отмечаем, что $\{x^\varphi \mid x \in \mathcal{H}\} = \mathcal{H}$. Укажем орбиты элементов $\mathcal{H}$ под действием φ. Для упрощения записи обозначим элемент $x = (x_1, x_2, x_3, x_4, x_5, x_6)$ числом

$$32x_1 + 16x_2 + 8x_3 + 4x_4 + 2x_5 + x_6,$$

тогда $(0,0,0,0,0,0) \leftrightarrow 0$, $e = (1,0,0,0,0,0) \leftrightarrow 32$,

$$K(3,3,3) = \{17, 19\}, \quad K(6,6,6) = \{4, 14, 19, 27, 28, 30, 36, 46, 51, 59, 60, 62\},$$

$$K(7,6,6) = \{1, 6, 22, 33, 38, 54\}, \quad K(12,12,7) = \{9, 12, 20, 40, 44, 52\},$$

$$K(15,15,5) = \{3, 11, 25, 35, 43, 57\}.$$

Остальные элементы принадлежат $K(7,7,7)$ и образуют 10 орбит длины 3:

$$(2,13,15), \quad (5,23,50), \quad (7,58,61), \quad (8,24,16), \quad (10,53,31),$$
$$(18,37,55), \quad (21,63,42), \quad (26,29,39), \quad (34,45,47), \quad (40,56,48).$$

Элементы каждой орбиты записаны в порядке $(x, x^\varphi, x^{\varphi^2}, \dots)$. Множество $K(6,6,6)$ является объединением двух орбит длины 6:

$$(4,27,46,36,59,14), \quad (19,62,28,51,30,60).$$

Множество $K(7,7,6) \cup K(12,12,7) \cup K(15,15,5)$ есть объединение трех 6-элементных орбит:

$$(1,9,57,33,41,25), \quad (3,38,52,35,6,20), \quad (11,54,12,43,22,44),$$

причем для каждого $x \in K(7,7,6)$

$$x^\varphi \in K(12,12,7), \quad x^{\varphi^2} \in K(15,15,5), \quad x^{\varphi^3} \in K(7,7,6).$$

Отметим, что φ не является не только автоморфизмом полуполя $\mathcal{H}$, но даже линейным преобразованием, так как полуполе не коммутативно. Непосредственно проверяется, что φ^6 – тождественное преобразование $\mathcal{H}$. $\square$

Таблица 16. Минимальные многочлены элементов полуполя Хентзела–Руа и ассоциированных матриц

$\lvert a\rvert_l = \lvert a\rvert_r$	$\lvert a\rvert$	$\mu_a^l(x) = \mu_a^r(x)$	$\mu_A(x)$
7	6	$x^6+x^5+x^4+x^3+x^2+x+1 =$ $= (x^3+x+1)(x^3+x^2+1)$	$x^6+x^5+x^4+x^3+x^2+x+1 =$ $= (x^3+x+1)(x^3+x^2+1)$
12	7	$x^6+x^5+x^3+x+1 =$ $= (x^2+x+1)^3$	$x^6+x^5+x^3+x+1 =$ $= (x^2+x+1)^3$
15	5	x^4+x+1	$x^6+x^5+x^4+x^3+1 =$ $= (x^4+x+1)(x^2+x+1)$
6	6	$x^4+x^2+1 =$ $= (x^2+x+1)^2$	$x^6+x^5+x^3+x+1 =$ $= (x^2+x+1)^3$
7	7	x^3+x+1 или x^3+x^2+1	$x^6+x^2+1 = (x^3+x+1)^2$ или $x^6+x^4+1 = (x^3+x^2+1)^2$
3	3	x^2+x+1	x^2+x+1

Итак, несмотря на непримитивность полуполя Хентзела–Руа $\mathcal{H}$ и другие его аномальные свойства, для него подтверждаются гипотезы лево-(право-)цикличности и однопорожденности лупы $\mathcal{H}^*$.

5.8. Полуполя порядка p^4 с условиями на автотопизмы

В этом параграфе представлено решение вопросов **(A)**–**(D)** для некоторых полуполей нечетных порядков 3^4, 5^4, 13^4. При изучении этих полуполей целью автора было построение примеров полуполевых плоскостей с определенными ограничениями на группу автотопизмов. А именно, были построены полуполевые плоскости порядка 3^4, которые удовлетворяют теоремам 3.1.2 и 3.1.5, то есть допускают бэровскую инволюцию (3.1.3) и имеют регулярное множество вида (3.1.6). Построенные полуполевые плоскости порядков 5^4 и 13^4 удовлетворяют теореме 3.7.1, то есть допускают подгруппу автотопизмов, изоморфную группе кватернионов Q_8. О построении примеров плоскостей было рассказано в главе 4.

Пусть π – полуполевая плоскость порядка 3^4, группа автотопизмов которой содержит бэровскую инволюцию τ (3.1.3). Тогда хотя бы одно из координатизирующих полуполей $W = W(4,3,\theta)$ допускает автоморфизм

$$\varphi : (x_1, x_2, x_3, x_4) \to (-x_1, -x_2, x_3, x_4), \tag{5.8.1}$$

где $x_i \in \mathbb{Z}_3$, $i = 1, \ldots, 4$. Из теорем 5.2.1, 5.2.3, 5.2.4 и изучения построенных в § 4.3 примеров следует результат.

Теорема 5.8.1. *Существуют ровно 8 попарно неизотопных нетривиальных полуполей порядка* 3^4*, допускающих автоморфизм* φ *(5.8.1). Каждое из них содержит подполе порядка 9*

$$U = \{(0, 0, x, y) \mid x, y \in \mathbb{Z}_3\}$$

(стабилизатор φ*), имеет ранг 2 над хотя бы одним из своих ядер, мультипликативная лупа содержит подлупу порядка 16*

$$L_0 = U^* \cup \{(x, y, 0, 0) \mid x, y \in \mathbb{Z}_3,\ (x, y) \neq (0, 0)\}.$$

Группа автотопизмов имеет порядок 2^m*, где* $8 \leq m \leq 11$.

В этой теореме перечислены только свойства, инвариантные относительно изотопизмов полуполей. Более подробно изучены свойства восьми представителей классов изотопизма, обозначим их

$$\mathcal{A}_1,\ \mathcal{A}_2,\ \mathcal{B}_1,\ \mathcal{B}_2,\ \mathcal{C}_1,\ \mathcal{C}_2,\ \mathcal{D}_1,\ \mathcal{D}_2. \tag{5.8.2}$$

Теорема 5.8.2. *Полуполя (5.8.2) лево- и правопримитивны, не коммутативны, но для всякого ненулевого элемента левый порядок равен правому порядку.*

Табл. 17 содержит информацию о ядрах, спектре, левом (правом) спектре, группе автоморфизмов и группе автотопизмов полуполей $\mathcal{A}_1$–$\mathcal{D}_2$. Здесь $|\mathcal{S}|$ обозначает число подполей порядка 9. Отметим, что левый спектр содержит число 80, что говорит о левопримитивности полуполя.

Таблица 17. Информация о полуполях порядка 3^4

Полуполе W	$\lvert\mathcal{S}\rvert$	$\lvert N_l\rvert$, $\lvert N_m\rvert$, $\lvert N_r\rvert$	Левый спектр	Спектр	$Aut\,W$	$\lvert At\,W\rvert$
$\mathcal{A}_1$	1	3, 3, 9	{1,2,4,8,16,40,80}	{1,2,4,5,6,7,8}	$\mathbb{Z}_2$	256
$\mathcal{A}_2$	1	3, 3, 9	{1,2,4,8,16,40,80}	{1,2,4,6,7,8}	$\mathbb{Z}_4$	512
$\mathcal{B}_1$	1	3, 9, 3	{1,2,4,8,16,40,80}	{1,2,4,6,7,8}	$\mathbb{Z}_4$	256
$\mathcal{B}_2$	1	3, 9, 3	{1,2,4,8,16,80}	{1,2,4,5,6,7,8}	$\mathbb{Z}_4$	512
$\mathcal{C}_1$	1	9, 3, 3	{1,2,4,8,16,40,80}	{1,2,4,5,6,7,8}	$\mathbb{Z}_2$	256
$\mathcal{C}_2$	1	9, 3, 3	{1,2,4,8,16,80}	{1,2,4,6,7,8}	$\mathbb{Z}_4$	512
$\mathcal{D}_1$	1	9, 9, 9	{1,2,4,8,16,40,80}	{1,2,4,6,8,9,13}	$\mathbb{Z}_4$	1024
$\mathcal{D}_2$	3	9, 9, 9	{1,2,4,8,16,40,80}	{1,2,4,6,7,8}	Q_8	2048

Для описания внутренних автоморфизмов (5.2.2) полуполей (5.8.2) введем обозначения для элементов $e = (0,0,0,1)$, $a = (0,0,1,1)$, $b = (0,0,1,0)$, множества $K = \{e, -e, a, -a\}$ и преобразования

$$\psi : (x_1, x_2, x_3, x_4) \to (-x_1 + x_2, x_1 + x_2, x_3, x_4), \qquad x_i \in \mathbb{Z}_3,\ i = 1, \ldots, 4.$$

Тогда $(K, *)$ – циклическая подгруппа, $\lambda_a = \lambda_{-a} = \varphi$ – внутренний автоморфизм (5.8.1). Табл. 18 представляет информацию о внутренних автоморфизмах полуполей $\mathcal{A}_1$–$\mathcal{D}_2$. Множества $\mathcal{M}$ и $\mathcal{E}$ замкнуты по умножению, причем $\mathcal{M}$ не совпадает с ядром полуполя, для четырех из полуполей верно:

$$\psi = \lambda_b = \lambda_{-b}, \qquad \varphi\psi = \lambda_{a+b} = \lambda_{-a-b},$$

в полуполе $\mathcal{B}_2$ восемь элементов порождают тождественный внутренний автоморфизм.

Таблица 18. Внутренние автоморфизмы полуполей порядка 3^4

Полуполе W	$In\, W$	$\mathcal{M} = \{m \mid \lambda_m \in In\, W\}$	$\mathcal{E} = \{m \mid \lambda_m = \varepsilon\}$
$\mathcal{A}_1$	$\{\varepsilon, \varphi\}$	K	Z^*
$\mathcal{A}_2$	$\{\varepsilon, \varphi\}$	K	Z^*
$\mathcal{B}_1$	$\{\varepsilon, \varphi, \psi, \varphi\psi\}$	U^*	Z^*
$\mathcal{B}_2$	$\{\varepsilon, \varphi, \psi, \varphi\psi\}$	L_0	$L_0 \setminus U^*$
$\mathcal{C}_1$	$\{\varepsilon, \varphi\}$	K	Z^*
$\mathcal{C}_2$	$\{\varepsilon, \varphi\}$	K	Z^*
$\mathcal{D}_1$	$\{\varepsilon, \varphi, \psi, \varphi\psi\}$	U^*	Z^*
$\mathcal{D}_2$	$\{\varepsilon, \varphi, \psi, \varphi\psi\}$	U^*	Z^*

Пусть π – полуполевая плоскость порядка p^4, где $p-1$ делится на 4, группа автотопизмов которой содержит подгруппу H, изоморфную группе кватернионов Q_8. Тогда, по теореме 3.7.1, регулярное множество плоскости может быть записано в виде (3.1.6), автотопизмы порядка 4, порождающие H, в подходящем базисе имеют матричное представление (3.7.1). Рассмотрим соответствующие (см. лемму 5.1.5) автотопизмы координатизирующего полуполя $W = W(4, p, \theta)$: $\sigma_1 = \langle \gamma_1, \gamma_1, \beta_1 \rangle$, $\sigma_2 = \langle \gamma_2, \gamma_2, \beta_2 \rangle$, где

$$\begin{aligned} &\gamma_1 : (x_1, x_2, x_3, x_4) \to (-ix_1, -ix_2, ix_3, ix_4), \\ &\gamma_2 : (x_1, x_2, x_3, x_4) \to (-x_3, -x_4, x_1, x_2), \end{aligned} \qquad x_j \in \mathbb{Z}_p,\ j = 1, \ldots, 4,$$

$i \in \mathbb{Z}_p$, $i^2 = -1$. Линейные преобразования β_1 и β_2 однозначно определяются условием $x^{\gamma_k} * y^{\beta_k} = (x * y)^{\gamma_k}$. В частности, $\beta_1 = \varphi$ (5.8.1). Кроме того, как показано в доказательстве теоремы 3.7.1, φ является автоморфизмом полуполя W. Результатом построений в § 4.1 и теорем 5.2.1, 5.2.3, 5.2.4 является

Теорема 5.8.3. *Существуют ровно три попарно неизотопных нетривиальных полуполя порядка* 5^4*, допускающих подгруппу автотопизмов* $\langle \sigma_1, \sigma_2 \rangle \simeq Q_8$*, и 33 попарно неизотопных полуполя порядка* 13^4 *с тем же условием. Каждое из таких полуполей* $W = W(4, p, \theta)$ *не коммутативно, лево- и правопримитивно, имеет центр порядка* p*, левое ядро* N_l *порядка* p^2*, мультипликативная лупа содержит подлупу порядка* $(p^2-1)^2$*. Число максимальных подполей порядка* p^2 *равно 1, 2 или* $p+2$*. Группа автоморфизмов* $Aut\, W$ *есть* $\mathbb{Z}_2$ *или* $\mathbb{Z}_{p+1}$*.*

Более подробно решение вопросов **(A)**–**(D)** представлено в табл. 19 для $p = 5$ и в табл. 19 для $p = 13$. Отметим, что каждый изученный класс изотопизма состоит из трех попарно неизоморфных полуполей, обладающих различными свойствами.

Для спектров в табл. 18 использованы следующие обозначения: S – множество всех делителей числа 624,

$$
\begin{aligned}
L_1 &= S \setminus \{13, 26, 52, 104\},\\
L_2 &= S \setminus \{48\},\\
L_3 &= S \cup \{15, 30, 40, 60, 120\},\\
L_4 &= S \setminus \{48\} \cup \{15, 30, 40, 60, 120\}.
\end{aligned}
$$

В номере полуполя первое число означает номер класса изотопизма.

Таблица 19. Информация о неизоморфных полуполях порядка 5^4

№	$\lvert N_m\rvert = \lvert N_r\rvert$	$Aut\ W$	Левый спектр	Правый спектр	Число подполей порядка 25
1.1	$25, = N_l$	$\mathbb{Z}_6$	L_1	L_1	1
1.2	$25, \neq N_l$	$\mathbb{Z}_2$	L_2	L_1	2
1.3	$25, \neq N_l$	$\mathbb{Z}_2$	L_3	L_1	2
2.1	5	$\mathbb{Z}_2$	L_1	L_1	1
2.2	5	$\mathbb{Z}_2$	L_2	L_1	2
2.3	5	$\mathbb{Z}_2$	L_3	L_1	2
3.1	5	$\mathbb{Z}_6$	L_1	L_1	7
3.2	5	$\mathbb{Z}_2$	L_3	L_1	7
3.3	5	$\mathbb{Z}_2$	L_4	L_1	7

В табл. 20 используются обозначения L_i для левого спектра и R_i для правого спектра полуполя.

Пусть теперь S – множество всех делителей числа $28560 = 13^4 - 1$,

$$S_0 = S \setminus \{5, 10, 15, 17, 21, 30, 34, 40, 51, 60, 68, 80, 85, 102, 120, 136, 170, 204, 240, 255, 280, 340, 408, 510, 680, 840, 1020, 2040\},$$
$$S_1 = S \cup \{91, 104, 182, 273, 312, 364, 546, 728, 1092, 2184\}.$$

Тогда

$$R_1 = S_0,$$
$$R_2 = S_0 \setminus \{35, 70, 105, 140, 210, 420\},$$
$$R_3 = S_0 \setminus \{119, 238, 272, 357, 476, 714, 816, 1428\},$$
$$L_1 = S_0 \cup \{21\} \setminus \{20\},$$
$$L_2 = S_1 \setminus \{80, 240\},$$
$$L_3 = S \setminus \{5, 10, 15, 20, 30, 40, 60, 80, 120, 240\},$$
$$L_4 = S_0 \cup \{21\} \setminus \{20, 35, 70, 105, 140, 210, 420\},$$
$$L_5 = S_1 \setminus \{5, 10, 15, 20, 30, 40, 60, 120\},$$
$$L_6 = S \setminus \{5, 10, 15, 20, 30, 40, 60, 120, 136, 408\},$$
$$L_7 = S_0 \cup \{21\} \setminus \{20, 119, 238, 272, 357, 476, 714, 816, 1428\},$$
$$L_8 = S_1 \setminus \{5, 10, 15, 17, 20, 30, 34, 40, 51, 60, 68, 102, 120, 204\},$$
$$L_9 = S \setminus \{136, 408\},$$
$$L_{10} = S_1 \setminus \{5, 10, 15, 20, 30, 40, 60, 80, 120, 240\},$$
$$L_{11} = S_1 \setminus \{5, 10, 15, 20, 30, 40, 60, 120, 136, 408\},$$
$$L_{12} = S_1 \setminus \{136, 408\}.$$

Таблица 20. Информация о неизоморфных полуполях порядка 13^4

№	*Aut W*	$\lvert N_m\rvert = \lvert N_r\rvert$	Левый спектр	Правый спектр	Число подполей порядка 169
1.1	$\mathbb{Z}_{14}$	169, N_l	L_1	R_1	1
1.2	$\mathbb{Z}_2$	169, $\neq N_l$	L_2	R_1	2
1.3	$\mathbb{Z}_2$	169, $\neq N_l$	L_3	R_1	2
2.1	$\mathbb{Z}_{14}$	169, N_l	L_4	R_2	1
2.2	$\mathbb{Z}_2$	169, $\neq N_l$	L_5	R_2	2
2.3	$\mathbb{Z}_2$	169, $\neq N_l$	L_6	R_2	2
3.1	$\mathbb{Z}_{14}$	169, N_l	L_7	R_3	1
3.2	$\mathbb{Z}_2$	169, $\neq N_l$	L_8	R_3	2
3.3	$\mathbb{Z}_2$	169, $\neq N_l$	L_9	R_3	2
4.1, 5.1, 6.1, 7.1, 8.1	$\mathbb{Z}_2$	13	L_1	R_1	1
4.2, 5.2, 6.2, 7.2, 8.2	$\mathbb{Z}_2$	13	L_2	R_1	2
4.3, 5.3, 6.3, 7.3, 8.3	$\mathbb{Z}_2$	13	L_3	R_1	2
9.1, 10.1, 11.1, 12.1, 13.1	$\mathbb{Z}_2$	13	L_4	R_1	1
9.2, 10.2, 11.2, 12.2, 13.2	$\mathbb{Z}_2$	13	L_5	R_1	2
9.3, 10.3, 11.3, 12.3, 13.3	$\mathbb{Z}_2$	13	L_6	R_1	2
14.1, 15.1, 16.1, 17.1, 18.1	$\mathbb{Z}_2$	13	L_7	R_1	1
14.2, 15.2, 16.2, 17.2, 18.2	$\mathbb{Z}_2$	13	L_8	R_1	2
14.3, 15.3, 16.3, 17.3, 18.3	$\mathbb{Z}_2$	13	L_9	R_1	2
19.1	$\mathbb{Z}_{14}$	13	L_1	R_1	15
19.2	$\mathbb{Z}_2$	13	L_2	R_1	15
19.3	$\mathbb{Z}_2$	13	L_{10}	R_1	15

Продолжение табл. 20. Информация о неизоморфных полуполях порядка 13^4

№	*Aut W*	$\lvert N_m\rvert = \lvert N_r\rvert$	Левый спектр	Правый спектр	Число подполей порядка 169
20.1	$\mathbb{Z}_{14}$	13	L_4	R_2	15
20.2	$\mathbb{Z}_2$	13	L_5	R_2	15
20.3	$\mathbb{Z}_2$	13	L_{11}	R_2	15
21.1	$\mathbb{Z}_{14}$	13	L_7	R_3	15
21.2	$\mathbb{Z}_2$	13	L_8	R_3	15
21.3	$\mathbb{Z}_2$	13	L_{12}	R_3	15
22.1, 23.1	$\mathbb{Z}_{14}$	13	L_1	R_2	15
22.2, 23.2	$\mathbb{Z}_2$	13	L_2	R_2	15
22.3, 23.3	$\mathbb{Z}_2$	13	L_{10}	R_2	15
24.1, 25.1	$\mathbb{Z}_{14}$	13	L_1	R_3	15
24.2, 25.2	$\mathbb{Z}_2$	13	L_2	R_3	15
24.3, 25.3	$\mathbb{Z}_2$	13	L_{10}	R_3	15
26.1, 27.1	$\mathbb{Z}_{14}$	13	L_4	R_1	15
26.2, 27.2	$\mathbb{Z}_2$	13	L_5	R_1	15
26.3, 27.3	$\mathbb{Z}_2$	13	L_{11}	R_1	15
28.1, 29.1	$\mathbb{Z}_{14}$	13	L_4	R_3	15
28.2, 29.2	$\mathbb{Z}_2$	13	L_5	R_3	15
28.3, 29.3	$\mathbb{Z}_2$	13	L_{11}	R_3	15
30.1, 31.1	$\mathbb{Z}_{14}$	13	L_7	R_1	15
30.2, 31.2	$\mathbb{Z}_2$	13	L_8	R_1	15
30.3, 31.3	$\mathbb{Z}_2$	13	L_{12}	R_1	15
32.1, 33.1	$\mathbb{Z}_{14}$	13	L_7	R_2	15
32.2, 33.2	$\mathbb{Z}_2$	13	L_8	R_2	15
32.3, 33.3	$\mathbb{Z}_2$	13	L_{12}	R_2	15

Вопрос о количестве максимальных подполей порядка p^2 решен построением минимальных многочленов элементов (см. следствие 5.3.12). Спектр и внутренние автоморфизмы не рассматривались ввиду обширности массива данных.

Глава 6. Вопросы строения конечных почти-полей

В этой главе изложено решение вопросов **(B)**–**(D)** для конечных почти-полей (§ 6.2). Параграф 6.1 представляет известное соответствие между конечными почти-полями и точно дважды транзитивными группами, перечисляя конечные почти-поля, у которых простое подполе не лежит в центре. Параграф 6.3 выявляет характеристическое свойство регулярного множества почти-поля размерности два над ядром, в том числе для исключительных почти-полей. Параграф 6.4 отмечает существенные особенности случая бесконечных точно дважды транзитивных групп. В параграфе 6.5 методом регулярного множества доказано, что не существует квазиполей порядка 25, мультипликативная лупа которых является лупой Муфанг.

6.1. Почти-поля и точно 2-транзитивные группы

Определение 6.1.1. *Алгебраическая система* $\langle Q, +, \cdot \rangle$ *называется почти-полем, если*

1) $(Q, +)$ *— абелева группа с нейтральным элементом* 0*,*

2) $(Q^*, \cdot)$ *— группа* $(Q^* = Q \setminus \{0\})$*;*

3) выполнен левый дистрибутивный закон $c \cdot (a+b) = c \cdot a + c \cdot b$ $(a, b, c \in Q)$*;*

4) $0 \cdot a = 0$ *для всех* $a \in Q$*,*

5) уравнение $ax = bx + c$ *однозначно разрешимо для всех* $a, b, c \in Q$*,* $a \neq b$*.*

Таким образом, это (левое) квазиполе, в котором умножение ассоциативно. Все конечные почти-поля описал в 1936 г. Х. Цассенхауз [121], связывая с каждым из них определенную точно 2-транзитивную группу (см. также [18, гл. 20]).

Определение 6.1.2. *Группа* G *перестановок множества* F $(|F| \geq k)$ *называется точно* k*-транзитивной на* F*, если для любых двух упорядоченных множеств* $(\alpha_1, ..., \alpha_k)$ *и* $(\beta_1, ..., \beta_k)$ *элементов из* F *таких, что* $\alpha_i \neq \alpha_j$ *и* $\beta_i \neq \beta_j$ *для* $i \neq j$*, существует точно один элемент группы* G*, переводящий* α_i *в* β_i $(i = 1, ..., k)$*.*

Каждая конечная точно 2-транзитивная группа представима в качестве группы аффинных преобразований конечного почти-поля, и группа аффинных преобразований каждого конечного почти-поля точно 2-транзитивна. Рассмотрим кратко эту взаимосвязь.

Пусть G – конечная дважды транзитивная группа подстановок множества $\Omega = \{c_0, c_1, \ldots, c_{n-1}\}$, причем только единица ε оставляет неподвижными два символа. Построим алгебраическую систему $Q = (Q, +, \cdot)$ на множестве Ω. Один символ этой системы назовем нулем, считая $c_0 = 0$, а другой – единицей $c_1 = 1$.

Подстановки в G, переставляющие все символы, образуют вместе с единичной подстановкой нормальную абелеву подгруппу A, транзитивную на Ω. Если $b, x \in Q$, то в подгруппе A существует и единственна подстановка

$$A_b = \begin{pmatrix} 0 & \ldots & x & \ldots \\ b & \ldots & y & \ldots \end{pmatrix} \in A.$$

Таким образом, в Q однозначно определена сумма $y = x + b$. Обозначая через M стабилизатор символа 0, считаем

$$y = xm \quad (x, m \in Q^* = Q \setminus \{0\})$$

тогда и только тогда, когда в группе G содержится подстановка

$$M_m = \begin{pmatrix} 0 & 1 & \dots & x & \dots \\ 0 & m & \dots & y & \dots \end{pmatrix} \in M.$$

Согласно [18], полагая дополнительно $0x = x0 = 0$, мы получаем на Q корректно определенные сложение и умножение, причем $(Q, +, \cdot)$ является почти-полем, а группа G изоморфна группе преобразований $y = xm + b$, $m \neq 0$. Кроме того,

$$A_a A_b = A_{a+b}, \quad M_m M_t = M_{mt},$$

$$M_m^{-1} A_1 M_m = A_m, \quad M_t^{-1} A_m M_t = A_{mt} \qquad (a, b \in Q,\ m, t \in Q^*).$$

Обратно, указанные преобразования любого конечного почти-поля K образуют точно 2-транзитивную группу.

Известный способ построения конечного почти-поля как специального расширения его центра $GF(q)$ (поле Галуа), впервые начал применять еще Диксон. Эта *конструкция Диксона–Цассенхауза* описана М. Холлом в [18, теорема 20.7.2].

Теорема 6.1.3. *Пусть $q = p^l$, где p – простое число, и пусть n – такое целое число, что все его простые делители делят число $q - 1$ и $n \not\equiv 0 \pmod 4$, если $q \equiv 3 \pmod 4$. Тогда для $r = ln$ мы можем следующим образом построить почти-поле K, состоящее из p^r элементов, исходя из поля Галуа $GF(p^r)$.*

1) Элементами почти-поля K являются элементы поля $GF(p^r)$.

2) Сложение в K производится по тому же правилу, что и в поле $GF(p^r)$.

3) Произведение $w \circ u$ в почти-поле K определяется в терминах произведения $x \cdot y$ поля $GF(p^r)$ следующим образом:

пусть z – фиксированный первообразный корень поля $GF(p^r)$; если $u = z^{kn+j}$, то сравнением

$$q^i \equiv 1 + j(q-1) \pmod{n(q-1)}$$

однозначно определяется натуральное число i по модулю n. Тогда произведение $w \circ u$ определяем так:

$$w \circ u = u \cdot w^{q^i}.$$

4) Центром почти-поля K является его подполе $GF(q)$. Любое почти-поле K из p^r элементов можно построить описанным выше способом из поля $GF(p^r)$, если почти-поле K обладает тем свойством, что его мультипликативная группа M содержит такую инвариантную циклическую подгруппу C, что фактор-группа M/C также циклична.

Построенные конструкцией Диксона–Цассенхауза почти-поля порядка q^n с центром $GF(q)$ называют *почти-полями Диксона*, указанная пара чисел (q, n) называется *парой Диксона*. Класс всех почти-полей Диксона порядка q^n с центром $GF(q)$, $q = p^l$, обозначают через $DF(q, n)$.

Х. Люнебург [87] показал:

Теорема 6.1.4. *Если (q, n) – пара Диксона, $q = p^l$ (p – простое), то класс $DF(q, n)$ всех почти-полей Диксона порядка q^n с центром $GF(q)$ не пуст и содержит $\varphi(n)/g$ типов изоморфных почти-полей, где φ – функция Эйлера и g – порядок p по модулю n.*

Следствие 6.1.5. *Число $|DF(p, r)|$ (r – простое и делит $p-1$) почти-полей Диксона порядка p^r равно $r - 1$.*

По теореме Цассенхауза [121], *все конечные почти-поля Q исчерпываются почти-полями Диксона и, кроме того, семью исключительными почти-полями порядка p^2 для простых чисел $p = 5, 7, 11$ (два почти-поля), $23, 29, 59$.*

Для решения вопросов **(A)**–**(D)** для конечных почти-полей изучим прежде всего взаимосвязь центра, ядра и простого подполя.

Центр почти-поля Q определяет равенство

$$Z(Q) = \{x \in Q \mid xy = yx \ \ \forall y \in Q\},$$

очевидно, $Z(Q) = Z(Q^*) \cup \{0\}$. *Ядро почти-поля Q* определяется так же, как и для квазиполя (см. определение 1.1.3), с учетом ассоциативности умножения:

$$K(Q) = \{x \in Q \mid (y + z)x = yx + zx,\ x(y + z) = xy + xz \ \ \forall y, z \in Q\}.$$

Простое подполе каждого конечного квазиполя состоит из всех целочисленных кратных единицы, $\pi(\mathbb{Z}) \simeq \mathbb{Z}_p$ (см. лемму 1.1.2). Известно, что в случае полуполя простое подполе всегда лежит в центре. Оказывается, это не всегда верно в произвольном квазиполе и даже в почти-поле. Следующая теорема [139] перечисляет исключения.

Теорема 6.1.6. *В конечном почти-поле центр и ядро совпадают, являются подполями и содержат простое подполе. Исключения составляют точно четыре почти-поля Q, для которых порядки $|Q|$ равны 5^2, 7^2, 11^2 и 29^2, порядки центров $Z(Q^*)$ группы Q^* равны $2, 2, 2$ и 14 соответственно, а ядро $K(Q)$ есть простое подполе.*

Доказательство. Известно [68, теорема 7.2], что ядро любого квазиполя есть тело. Следовательно, в конечном почти-поле Q ядро является подполем и содержит простое подполе. Непосредственно из определений ядра и центра получаем также включение $Z(Q) \subseteq K(Q)$.

Для почти-полей Диксона, по построению, центр является подполем и содержит простое подполе, а согласно [121] и [49, § 2], ядро и центр совпадают.

Исключительным почти-полям Q порядка p^2 (почти-поля Цассенхауза) присваиваем один из типов I–VII соответственно нумерации после теоремы 20.7.2 в [18]. В каждом из них ядро, очевидно, совпадает с простым подполем $P = \pi(\mathbb{Z}) \simeq \mathbb{Z}_p$. Силовская 2-подгруппа S_2 мультипликативной группы Q^* является обобщенной кватернионной порядка 16 или 8, имеет единственную инволюцию и центр $Z(S_2)$ порядка 2. При $|Q| = 7^2$ группа Q^* порядка 48 представляется бинарной октаэдральной группой [1, § 6.5], обозначаемой через $2O$.

Отраженное в [18], [117, § 5,6] строение группы Q^* и ее центра резюмирует Табл. 21.

Таблица 21. Исключительные почти-поля Q

Тип	$\|Q\|$	Q^*	$\|Z(Q^*)\|$	$\|S_2\|$
I	5^2	$SL(2,3)$	2	8
II	11^2	$SL(2,3) \times \mathbb{Z}_5^+$	10	8
III	7^2	$2O$	2	16
IV	23^2	$2O \times \mathbb{Z}_{11}^+$	22	16
V	11^2	$SL(2,5)$	2	8
VI	29^2	$SL(2,5) \times \mathbb{Z}_7^+$	14	8
VII	59^2	$SL(2,5) \times \mathbb{Z}_{29}^+$	58	8

Для почти-полей Q типа II, IV и VII порядок центра $Z(Q^*)$ мультипликативной группы Q^* совпадает с $|P^*| = p-1$. Поэтому $P^* = Z(Q^*)$ и P — центр $Z(Q)$ почти-поля Q. В остальных четырех случаях имеем $|Z(Q^*)| < p-1$, и поэтому центр $Z(Q)$ почти-поля Q лежит в простом подполе P, но не совпадает с ним. В частности, вопрос о равенстве простого подполя и центра решается по-разному для двух почти-полей порядка 11^2 — типа II и V. □

6.2. Автоморфизмы и спектры конечных почти-полей

Для решения вопроса **(B)** достаточно заметить, что если лупа Q^* почти-поля Q однопорождена, то она является циклической группой и поэтому почти-поле Q коммутативно. Отсюда сразу вытекает

Лемма 6.2.1. *Почти-поле Q является полем, если его лупа $(Q^*, \cdot)$ однопорождена.*

Для определения строения группы Q^* конечного почти-поля Цассенхауз [121] существенно использовал выявленное свойство (см. [18, лемма 20.7.K3]): *Если числа q и s простые, то подгруппы порядков q^2 и qs группы Q^* циклические.*

Лемма 6.2.2. *[18, Лемма 20.7.K4] Силовская r-подгруппа S_r группы M является циклической, или при $r = 2$ и подходящем $n \geq 3$ обобщенной кватернионной*

$$\langle a, b \mid a^{2^{n-1}} = 1,\ b^2 = a^{2^{n-2}},\ ba = ab^{-1} \rangle.$$

Строение мультипликативных групп Q^* семи исключительных почти-полей Цассенхауза отражено в табл. 21. Для почти-полей Диксона в [121] (см. также [48, предложения 1,2] и [117, теорема IV.1.5]), наряду с цикличностью центра $Z(Q^*)$ и фактор-группы $Q^*/Z(Q^*)$ (метацикличность группы Q^*), установлена

Лемма 6.2.3. *Мультипликативная группа Q^* конечного почти-поля Диксона $Q \in DF(q, n)$ есть метациклическая двупорожденная группа*

$$Q^* = \langle a, b \mid a^m = 1, \quad b^n = a^t, \quad bab^{-1} = a^q \rangle, \qquad m = \frac{q^n - 1}{n}, \quad t = \frac{m}{q-1}. \tag{6.2.1}$$

Кроме того, $Z(Q^*) = \langle a^t \rangle$ и НОД $(n, t) =$ НОД $(q - 1, t) \leq 2$.

Как показано в [48, предложение 3], условие НОД$(q - 1, t) = 1$ равносильно цикличности силовской 2-подгруппы в Q^*.

Пример 6.1. Если $Q \in DF(7, 2)$, то силовская 2-подгруппа Q^* есть обобщенная кватернионная группа порядка 16, а для $Q \in DF(5, 2)$ — циклическая группа порядка 8.

Вопрос **(C)** о спектре порядков элементов группы Q^*, в обозначениях (6.2.1), решает [139]

Теорема 6.2.4. *Пусть $Q \in DF(q, n)$ — почти-поле Диксона, Q^* — его мультипликативная группа. Тогда спектр Q^* состоит из всех делителей числа m и всех делителей z числа $q^n - 1$, минимальных с условием*

$$\left(k\,\frac{q^{zs} - 1}{q^s - 1} + \frac{zst}{n} \right) \vdots\ m, \qquad k = 0, 1, \ldots, m - 1,\ s = 1, 2, \ldots, n - 1. \tag{6.2.2}$$

Доказательство. Найдем порядки элементов в мультипликативной группе Q^* почти-поля Диксона $Q \in DF(q, n)$. Используя ее определяющие соотношения (6.2.1) и факторизацию $Q^* = \langle a \rangle \langle b \rangle$, получаем

$$ba^k b^{-1} = a^{kq}, \quad b^2 ab^{-2} = a^{q^2}, \ldots, \quad b^s ab^{-s} = a^{q^s}, \quad b^s a^k b^{-s} = a^{kq^s},$$

$$(a^k b^s)(a^k b^s) = a^k (b^s a^k b^{-s}) b^{2s} = a^{k(1+q^s)} b^{2s}.$$

Поэтому для произвольных k и s из (6.2.2) имеем

$$(a^k b^s)^z = a^{k(1+q^s+q^{2s}+\cdots+q^{(z-1)s})} b^{zs}.$$

Если $(a^k b^s)^z = 1$, то $a^{k(1+q^s+q^{2s}+\cdots+q^{(z-1)s})} b^{zs} = 1$. Деление zs на n с остатком дает $zs = nu + r$, $0 \le r < n$, так что

$$a^{k(1+q^s+q^{2s}+\cdots+q^{(z-1)s})} b^{nu+r} = 1 \Rightarrow a^{k(1+q^s+q^{2s}+\cdots+q^{(z-1)s})+tu} = b^{-r}.$$

Учитывая соотношения $b^n = a^t$ и $r < n$, получаем $r = 0$ и, следовательно,

$$u = \frac{zs}{n} \quad \text{и} \quad a^{k(1+q^s+q^{2s}+\cdots+q^{(z-1)s})+tu} = 1.$$

Таким образом, порядок элемента $a^k b^s \ne 1$ – это наименьшее натуральное число z, удовлетворяющее условию (6.2.2) и делящее $q^n - 1$.

Теорема доказана. □

Пример 6.2. Проиллюстрируем теорему на примере почти-поля $Q \in DF(5, 2)$, где

$$Q^* = \{a^k b^s \mid k = 0, 1, \ldots, 11,\ s = 0, 1\},$$

$$m = 12, \quad t = 3, \quad a^{12} = 1, \quad b^2 = a^3, \quad bab^{-1} = a^5.$$

Для произвольного элемента $a^k b \in \langle a \rangle b$ условие (6.2.2) принимает вид

$$\left(\frac{k(5^z - 1)}{4} + \frac{3z}{2} \right) \vdots\ 12,$$

получаем $z = |a^k b| = 8$. Поэтому спектр группы Q^* получается присоединением числа 8 к спектру циклической группы $\langle a \rangle$ порядка 12, то есть равен $\{1, 2, 3, 4, 6, 8, 12\}$. Отметим для сравнения, что спектр мультипликативной группы почти-поля Цассенхауза H порядка 25 совпадает со спектром группы $SL(2, 3)$, то есть равен $\{1, 2, 3, 4, 6\}$. Подробнее см. табл. 22.

Таблица 22. Число элементов порядка z группы K^* почти-полей K порядка 25

Порядок z элемента	**1**	**2**	**3**	**4**	**6**	**8**	**12**
Случай $K = Q$	1	1	2	2	2	12	4
Случай $K = H$	1	1	8	6	8	0	0

В связи с вопросом **(D)** отметим, что группу автоморфизмов конечного почти-поля Q описал Х. Цассенхауз. В случае $Q \in DF(3,2)$ имеем $Aut\, Q \simeq S_3$; для других почти-полей Диксона $Q \in DF(p^l, n)$ группа автоморфизмов $Aut\, Q$ — циклическая группа порядка ln/g, где g — порядок p по модулю n [121, предложение 18]. Т. Бойкетт и К. Хауэлл [31] описали группу автоморфизмов $Aut\ Q^*$. Группы автоморфизмов для семи почти-полей Цассенхауза отражает табл. 23.

Таблица 23. Автоморфизмы исключительных почти-полей Q

Тип	$\lvert Q\rvert$	Q^*	$Aut(Q^*)$	$\lvert Aut(Q)\rvert$
I	5^2	$SL(2,3)$	S_4	4
II	11^2	$SL(2,3) \times \mathbb{Z}_5^+$	$S_4 \times \mathbb{Z}_4^+$	2
III	7^2	$2O$	$S_4 \times \mathbb{Z}_2^+$	3
IV	23^2	$2O \times \mathbb{Z}_{11}^+$	$S_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{10}^+$	1
V	11^2	$SL(2,5)$	S_5	5
VI	29^2	$SL(2,5) \times \mathbb{Z}_7^+$	$S_5 \times \mathbb{Z}_6^+$	2
VII	59^2	$SL(2,5) \times \mathbb{Z}_{29}^+$	$S_5 \times \mathbb{Z}_{28}^+$	1

Завершая параграф, отметим, что проективные плоскости, координатизируемые конечными почти-полями, изучал И. Андрэ ([26], см. также [65]). За исключением плоскости порядка 9 (являющейся также плоскостью Холла), группа коллинеаций этих плоскостей, по модулю группы трансляций, есть произведение мультипликативной группы почти-поля на группу автоморфизмов почти-поля. Группа коллинеаций, следовательно, разрешима, исключая плоскость Холла порядка 9 и три плоскости, координатизируемые исключительными почти-полями Цассенхауза порядков 11^2, 29^2 и 59^2 (мультипликативная группа содержит $SL(2,5)$).

6.3. Регулярное множество двумерного почти-поля

Рассмотрим почти-поле порядка q^2 с центром $GF(q)$, где $q = p^l$, $p > 2$ — простое. Это либо регулярное почти-поле Диксона, способ построения которого приведен в теореме 6.1.3, либо одно из семи исключительных почти-полей Цассенхауза. Найдем матричное представление регулярного множества R конечного двумерного почти-поля Q. Следующее техническое предложение поэлементно перечисляет матрицы R для $Q \in DF(q,2)$, где новая операция $\circ$ на множестве элементов

$$Q = \{0, 1, \beta, \beta^2, \ldots, \beta^{q^2-2}\}$$

(β – фиксированный первообразный корень поля $GF(q^2)$) введена теоремой 6.1.3.

Предложение 6.3.1. *Регулярное множество $R \subset GL_2(q) \cup \{0\}$ почти-поля Диксона $Q \in DF(q,2)$ в базисе $e_1 = 1$, $e_2 = \beta$ состоит из матриц вида:*

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

где $[\beta^j]$ обозначает строку координат элемента β^j в выбранном базисе.

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

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

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

Предложение доказано. □

Более удобной является общая (функциональная) запись матриц регулярного множества:

$$\theta(x,y) = \begin{pmatrix} x & y \\ f(x,y) & g(x,y) \end{pmatrix}. \tag{6.3.1}$$

Она выявляет закономерности во всех матрицах регулярного множества данного почти-поля и поэтому позволяет выделить это почти-поле в классе, например, всех построенных квазиполей данного порядка. Отметим, что при такой записи матриц базис линейного пространства выбирается так: $e_1 = 1$, $e_2 \notin K$. Запишем многочлены f и g с коэффициентами из $GF(q)$ как

$$f(x,y) = \sum_{i=0}^{q-1} \sum_{j=0}^{q-1} f_{ij} x^i y^j, \qquad g(x,y) = \sum_{i=0}^{q-1} \sum_{j=0}^{q-1} g_{ij} x^i y^j, \tag{6.3.2}$$

причем из невырожденности всех ненулевых матриц вытекает $f_{00} \neq 0$, $g_{00} \neq 0$. Напомним, что только четыре исключительных почти-поля Цассенхауза имеют центр, отличный от ядра. В зависимости от порядка центра почти-поля уточним вид функций f и g.

Теорема 6.3.2. *Пусть Q — почти-поле порядка q^2 с ядром $K \simeq GF(q)$ ($q = p^l$) и центром Z, матрицы $\theta(x,y)$ вида* (6.3.1) *образуют его регулярное множество.*

1. Если $Z = K$, то

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

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

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

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

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

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

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

то для любых $u, v \in GF(q)$ имеем

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

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

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

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

Кроме того, из условия

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

имеем $g_{01}\varphi(f_{01}, g_{01}) = g_{01}\psi(f_{01}, g_{01}) = 0$. Остальные произведения матриц регулярного множества мы не рассматриваем, так как они предоставляют более сложные в использовании условия на коэффициенты однородных многочленов φ и ψ. Переобозначая, для краткости записи, коэффициенты, получаем первое утверждение теоремы.

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

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

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

$$f(x,0)y + g(x,0)f(y,0) = f(xy,0) \tag{6.3.3}$$

имеем $f(x,0) = 0$, тогда $Z = K$. Поэтому $m > 1$ и условие (6.3.3) дает $f(x,0) = f_{10}(x - x^m)$. Умножим теперь $\theta(x,0)$ на $\theta(0,y)$ и получим пару условий

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

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

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

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

рассмотрим произведение $\theta(x,0)\theta(u,v)$ и из условия замкнутости получим:

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

что приведет к равенствам

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

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

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

Здесь φ и ψ — однородные многочлены степени $m-2$. Для упрощения записи изменим обозначения коэффициентов и получим второе утверждение теоремы. Теорема полностью доказана. □

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

Пример 6.3. Рассмотрим регулярные множества всех правых квазиполей порядка 9. Для этого выберем $q = 3$ и найдем все многочлены $f, g \in \mathbb{Z}_3[x,y]$ вида (6.3.2), $f_{ij}, g_{ij} \in \mathbb{Z}_3$, с условием $\det(\theta(x,y) - \theta(u,v)) \neq 0$ для матриц вида (6.3.1) и всех пар $(x,y) \neq (u,v)$. Непосредственный компьютерный перебор предоставляет 12 вариантов подходящих многочленов f и g, список приведен в Табл. 24.

Таблица 24. Ассоциированные функции правых квазиполей порядка 9

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

Существует точно пять неизоморфных квазиполей порядка 9; одно из них — поле GF(9) (линейные функции № 1,2 и 5). Другое — почти-поле Диксона № 6, в соответствии с теоремой 6.3.2. Еще два — квазиполя Холла № 3,4 [146]. Пятое — «странное» квазиполе с центром $\{0,1\}$ [59, приложение II]. Этому квазиполю соответствуют в Табл. 24 варианты № 7–12, отличающиеся выбором второго базисного элемента.

Пример 6.4. Применим теорему 6.3.2 для записи матричного представления почти-полей порядка 25: это единственное почти-поле Диксона $Q \in DF(5,2)$ с центром $\mathbb{Z}_5$ и исключительное почти-поле Цассенхауза W с центром порядка 3.

Выберем многочлен $\varphi(x) = x^2 + 3x + 3$, неприводимый над $\mathbb{Z}_5$, и его корень β. Произведение $w \circ u$ определяем так: $w \circ \beta^{2k} = \beta^{2k} \cdot w$, $w \circ \beta^{2k+1} = \beta^{2k+1} \cdot w^5$. Используя предложение 6.3.1, найдем все матрицы регулярного множества. Например,

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

так как $\beta^6 = (2\beta+2)^3 = 3$. Тогда по первому утверждению теоремы 6.3.2 имеем $a = 3$ и $b = 0$,

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

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

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

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

Исключительное почти-поле Цассенхауза W порядка 25 построим, учитывая предложение 2.1.3: мультипликативная группа почти-поля изоморфна мультипликативной группе его регулярного множества. Известно [18, 20.7], что $W^* \simeq SL(2,3)$; используем это множество матриц для отыскания коэффициентов функций f и g.

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

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

По второму утверждению теоремы 6.3.2, $(m, p-1) = (m,4) = 1$, $m \neq 1$ и $a(x - x^m) = 0$, тогда $m = 3$ и $a = 0$. Сравнение матрицы $\theta(0,y)$ с

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

дает $c = 0$ и $b = 4$, откуда

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

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

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

6.4. Замечания о бесконечных точно 2-транзитивных группах, почти-полях и почти-областях

Точно дважды и трижды транзитивные группы тесно связаны с почти-полями, почти-областями, проективными плоскостями и KT-полями ([18, 117], см. также [137]).

Определение 6.4.1. *Алгебраическая система $(F, +, \cdot)$ называется почти-областью, если:*

1) $(F, +)$ – лупа с нейтральным элементом 0;

2) $(F^*, \cdot)$ – группа с нейтральным элементом 1 ($F^* = F \setminus \{0\}$);

3) $a + b = 0 \Rightarrow b + a = 0$;

4) $0 \cdot a = 0 \Rightarrow a \cdot 0 = 0$;

5) $a \cdot (b + c) = a \cdot b + a \cdot c$;

6) существует однозначно определенный элемент $d_{a,b} \in F^*$ такой, что

$$a + (b + x) = (a + b) + d_{a,b} \cdot x$$

для всех $x \in F$ (здесь a, b, c – любые элементы из F).

Почти-область $(F, +, \cdot)$ является почти-полем, если $(F, +)$ – абелева группа. Почти-поле $(F, +, \cdot)$ называется *планарным*, если для любых $a, b \in F$ и $b \neq 1$ уравнение $a + bx = x$ разрешимо в F.

Каждая точно дважды транзитивная группа представима в качестве группы $T_2(F)$ аффинных преобразований

$$t_{a,b} : x \to a + bx \qquad (a, b, x \in F, b \neq 0)$$

почти-области $(F, +, \cdot)$, и группа аффинных преобразований каждой почти-области точно дважды транзитивна. Г. Цассенхауз [121] дал полную классификацию конечных точно дважды и трижды транзитивных групп и почти-полей [18, 117]. Описание локально конечных почти-полей, точно дважды и трижды транзитивных групп можно найти в [117, гл. IV]. Локально конечные точно трижды транзитивные группы классифицировал О. Кегель [79]. Точно дважды и трижды транзитивные группы с дополнительными условиями изучались в [8, 16] и др. Следующая теорема кратко перечисляет результаты, которые доказывали Г. Карцель, Г. Гретцер, Г. Вефельшайд, Ж. Титс, В. Керби, М. Холл, В.Д. Мазуров и другие авторы [117, 8, 9].

Теорема 6.4.2. *1. Если $(F, +, \cdot)$ – почти-область, то $T_2(F)$ – точно дважды транзитивная группа подстановок множества F.*

2. *Если T – точно дважды транзитивная группа подстановок множества F, то можно ввести на F такие две операции $+$, $\cdot$, согласованные с действием группы T, что $(F,+,\cdot)$ будет почти-областью, а T – ее группой $T_2(F)$ аффинных преобразований.*

3. *Почти-область $(F,+,\cdot)$ тогда и только тогда является почти-полем, когда $d_{a,b}=1$ для всех $a,b\in F$.*

4. *Почти-область $(F,+,\cdot)$ тогда и только тогда является почти-полем, когда группа $T_2(F)$ обладает нетривиальной абелевой нормальной подгруппой.*

5. *Группа $T_2(F)$ почти-поля $(F,+,\cdot)$ тогда и только тогда является группой Фробениуса, когда $(F,+,\cdot)$ – планарное почти-поле.*

6. *Если $(F,+,\cdot)$ – почти-область и F^* – группа с конечными классами сопряженных элементов, то F – либо поле, либо конечное почти-поле.*

Пара (F,ε) называется *KT-полем* [117], если $(F,+,\cdot)$ – почти область, ε – автоморфизм группы $(F^*,\cdot)$ и для всех $x\in F^*\setminus\{1\}$ выполняется равенство

$$(1-x^{\varepsilon})^{\varepsilon}=1-(1-x)^{\varepsilon}.$$

В последнее время в работах К. Тент и других [99, 108] были построены примеры точно дважды транзитивных групп без регулярных абелевых нормальных подгрупп, а в работе [109], на основе групп из [99, 108], – примеры точно трижды транзитивных групп. Значит, существуют почти-области, не являющиеся почти-полями, и KT-поля (F,ε), в которых почти-области $(F,+,\cdot)$ – не почти-поля. Эти результаты дают еще одно основание для изучения указанных структур при дополнительных ограничениях. Бесконечные KT-поля (F,ε) при некоторых условиях, наложенных на инволюцию ε, изучаются в [137].

Заметим, что теорема 6.3.2 предоставляет возможность строить примеры нетривиальных бесконечных почти-полей. Перечитаем первое утверждение теоремы, учитывая равенство $y^{q-i}=y\cdot y^{-i}$ для любого ненулевого элемента $y\in GF(q)$. Мы можем переписать тогда функции f и g в виде

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

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

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

Если найдутся такие многочлены $\Phi(x)$ и $\Psi(x)$, что для любых пар $(x, y) \neq (u, v)$ элементов из K матрица $\theta(x, y) - \theta(u, v)$ является невырожденной, то при некоторых дополнительных условиях матрицы $\theta(x, y)$ образуют регулярное множество почти-поля размерности 2 над своим центром K. Требование изучения дополнительных условий вызвано тем, что теорема 6.3.2 дает лишь необходимое условие для регулярного множества почти-поля. Задача представляется нетривиальной и заслуживающей исследования.

6.5. Квазиполя с ослабленной ассоциативностью

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

$$(xy)(zx) = (x(yz))x, \qquad ((xy)z)y = x(y(zy)), \qquad x(y(xz)) = ((xy)x)z. \quad (6.5.1)$$

Лупа Муфанг удовлетворяет также тождествам

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

в силу которых она *диассоциативна*, любые два ее элемента порождают группу. На лупы Муфанг удается переносить теоретико-групповые результаты — теоремы Лагранжа, Силова и другие важные результаты [57, 58].

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

Существуют ли конечные квазиполя Муфанг?

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

Теорема 6.5.1. *Не существует квазиполей Муфанг порядка 25.*

Используем описание луп Муфанг порядка 24, полученное О. Чейном [34].

Лемма 6.5.2. *Если Q — квазиполе Муфанг порядка 25, то его мультипликативная лупа Q^* содержит циклическую подгруппу порядка 6, остальные элементы имеют порядок 4.*

Доказательство. О.Чейн перечислил все лупы Муфанг порядков менее 31, среди них пять луп порядка 24. Нам понадобится часть таблицы 3 статьи [34].

Таблица 25. Порядки элементов луп Муфанг порядка 24

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

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

Таким образом, если Q — квазиполе Муфанг порядка 25, то $Q^* \simeq M_{24}(G_{12}, Q)$. Информация из Табл. 25 о порядках элементов доказывает лемму 6.5.2. □

Лемма 6.5.3. *Пусть Q — квазиполе Муфанг порядка 25. Тогда при некотором выборе базиса e_1, e_2 его регулярное множество состоит из матриц вида*

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

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

Доказательство. В качестве первого базисного элемента выберем единицу квазиполя: $e_1 = e$, в качестве второго — элемент порядка 4. По лемме 6.5.2, такой выбор возможен, так как ядро $K = \langle e_1 \rangle$ содержит только два элемента порядка 4 из 18. Итак, далее $e_2^2 = -e$. Для $\theta(x, y)$ вида (6.3.1) имеем:

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

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

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

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

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

Получим условия $f(x,0)(x+g(x,0)=f(x^2,0)$, $g^2(x,0)=g(x^2,0)$, из которых при $x=-1$ имеем $f(-1,0)=0$, $g(-1,0)=-1$. В обозначения (6.3.2) для коэффициентов многочленов f и g верно $f_{00}=g_{00}=0$,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Таким образом, возможен только случай (2), лемма 6.5.3 доказана. □

Доказательство теоремы 6.5.1. По лемме 6.5.3,

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

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

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

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

Таким образом, уравнение $(1, 2)x = (2, 4)$ имеет в лупе Q^* два решения, что невозможно. Полученное противоречие доказывает теорему 6.5.1.

Применяемый метод позволил избежать компьютерного перебора всех квазиполей порядка 25 с проверкой выполнения условий (6.5.1). Для доказательства существенно использованы структурные результаты О.Чейна для луп Муфанг порядка 24, поэтому метод не переносится на другие порядки непосредственно. Тем не менее, метод регулярного множества представляется перспективным для решения вопроса существования квазиполей Муфанг — положительного либо отрицательного.

Глава 7. Максимальные подполя и под-почти-поля в конечных почти-полях

Основные теоремы этой главы представляют, в основном, решение вопроса **(A)** для конечных почти-полей. Решение существенно использует результаты Х. Цассенхауза [121] и С. Данкс [40].

В § 7.2 обсуждаются минимальные собственные почти-поля, т.е. нетривиальные почти-поля, в которых каждое собственное под-почти-поле является подполем. Теорема 7.2.3 демонстрирует существование минимальных собственных почти-полей в классе почти-полей Диксона $DF(q, n)$ для любого простого $n > 2$. Теорема 7.2.4 представляет способ построения минимального собственного конечного почти-поля, в котором количество максимальных подполей превосходит произвольное выбранное число.

7.1. Подполя в конечных почти-полях

Исследуем вопрос **(A)** для конечных почти-полей.

Простое подполе является единственным максимальным подполем в почти-поле характеристики p и порядка p^r для любого простого числа r, в силу [20, теорема 3] (при $r = 2$ – по теореме 6.1.6). Поэтому вопрос **(A)** редуцируется к почти-полям Диксона.

Отметим, что на под-почти-поля почти-поля Диксона $Q \in DF(q, n)$ переносится известное соответствие между подполями конечного поля и делителями степени его расширения над простым подполем. В силу основной теоремы С. Данкс в [40] и леммы 1.2 в [42], обобщенное соответствие можно представить следующей леммой.

Лемма 7.1.1. *Для любого под-почти-поля H почти-поля $Q \in DF(p^l, n)$ существуют числа $h \,|\, (ln)$ и $0 < j \leq n$ такие, что $|H| = p^h$, $H \in DF(p^z, h/z)$, $z = \text{НОД}(jl, h)$, причем*

$$j \equiv \frac{p^{ln} - 1}{p^h - 1} \,(\bmod\, n). \tag{7.1.1}$$

Обратно: если h делит ln, то Q имеет единственное под-почти-поле H порядка p^h.

Выделим случай коммутативных под-почти-полей или, равносильно, подполей.

Следствие 7.1.2. *Под-почти-поле H порядка p^h почти-поля $Q \in DF(p^l, n)$ есть подполе тогда и только тогда, когда h делит произведение $l \cdot \text{НОД}(j, n)$.*

Известно (У. Фелгнер, [49, теорема 2.1]), что в Q максимальное подполе $M(Q) \supseteq Z(Q)$ единственно. В следующей теореме мы выявляем изменения пары Диксона (q, n) при переходе к максимальному под-почти-полю и, вместе с тем, находим явно порядок максимального подполя $M(Q)$. Запишем каноническое разложение числа n и выделим число λ:

$$n = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}, \qquad \lambda = p_1^{[n_1/2]} p_2^{[n_2/2]} \dots p_r^{[n_r/2]}. \tag{7.1.2}$$

Теорема 7.1.3. *Пусть H — под-почти-поле порядка p^h почти-поля $Q \in DF(q, n)$, $q = p^l$ и $h = ln/p_i$ для некоторого p_i из (7.1.2). Тогда $H \in DF(q, n/p_i)$ при $n_i = 1$ и $H \in DF(q^{p_i}, n/p_i^2)$ при $n_i > 1$. Кроме того, под-почти-поле порядка q^λ в Q является единственным максимальным подполем, содержащим центр $Z(Q)$.*

Доказательство. В силу [41, лемма 2.3], для любой пары Диксона (q, n) имеем

$$\frac{q^n-1}{q^m-1} \equiv \frac{n}{m} \pmod{n} \quad \forall m \mid n.$$

Когда $n_i = 1$, для числа $n' = n/p_i$ получаем $h = ln'$ и НОД$(p_i, n') = 1$. Учитывая соответствие из леммы 7.1.1, находим

$$\frac{p^{ln}-1}{p^{ln'}-1} \equiv \frac{n}{n'} \pmod{n} = p_i,$$

$$z = \text{НОД}(lp_i, ln') = l \cdot \text{НОД}(p_i, n') = l, \qquad \frac{h}{z} = n', \qquad H \in DF(p^l, n/p_i).$$

При $n_i > 1$ полагаем $n' = n/p_i^2$. Тогда $h = lp_in'$ и с помощью леммы 7.1.1 находим

$$\frac{p^{ln}-1}{p^{lp_in'}-1} \pmod{n} = \frac{n}{p_in'} = p_i,$$

$$z = \text{НОД}(lp_i, lp_in') = lp_i, \qquad \frac{h}{z} = n', \qquad H \in DF(p^{lp_i}, n/p_i^2).$$

Построим сейчас убывающую последовательность под-почти-полей

$$H_0 \supset H_1 \supset H_2 \supset \ldots, \quad |H_i| = p^{h_i}, \quad h_0 = ln, \quad \frac{h_i}{h_{i+1}} \text{ — простые числа,} \quad (7.1.3)$$

начинающуюся с $H_0 = Q$. Вначале выполним $k_1 = [(n_1+1)/2]$ шагов ($[m]$ — целая часть числа m), переходя от H_i к H_{i+1} с простым числом $h_i/h_{i+1} = p_1$ из (7.1.2). Применяя альтернативу доказанного первого утверждения теоремы, получаем под-почти-поле

$$H_{k_1} \in DF(q^{p_1^{[n_1/2]}}, n/(p_1^{n_1})).$$

Затем выполним $k_2 = [(n_2+1)/2]$ переходов от H_i к H_{i+1} с простым числом $h_i/h_{i+1} = p_2$. Аналогично получим

$$H_{k_1+k_2} \in DF(q^{p_1^{[n_1/2]}p_2^{[n_2/2]}}, n/(p_1^{n_1}p_2^{n_2})).$$

Итак, степень под-почти-поля $H_{k_1+k_2}$ над его центром получаем из степени n в разложении (7.1.2), отбрасывая все простые сомножители p_1 и p_2. Ясно, что $Z(Q) \subseteq Z(H_{k_1}) \subseteq Z(H_{k_1+k_2})$.

Продолжая процесс, через $k = k_1 + k_2 + \cdots + k_r$ шагов приходим к под-почти-полю H_k, соответствующему паре Диксона $(q^\lambda, 1)$. Поэтому H_k совпадает со своим центром $Z(H_k)$ и, в частности, является подполем. Утверждение единственности в лемме 7.1.1 показывает, что подполе H_k не зависит от последовательности переходов в нашем построении. С другой стороны, $Z(H_i) \neq H_i$ при $i < k$ для любой последовательности (7.1.3) от $H_0 = Q$ до H_k. Следовательно, H_k — единственное максимальное подполе в Q, содержащее центр $Z(Q)$.

Теорема доказана. □

Через $\pi(m)$ обозначим множество простых делителей числа m. В связи с вопросом **(A)**, нас интересует каждое под-почти-поле H_i в (7.1.3), являющееся подполем, с наименьшим номером i для данной последовательности. В силу теоремы 7.1.3, изучения требует случай, когда $h_i/h_{i+1} \notin \pi(n)$.

Теорема 7.1.4. *Пусть H — под-почти-поле порядка $p^{l'n}$ почти-поля $Q \in DF(p^l, n)$. Тогда*

1) если $\text{НОД}(l/l', n) = 1$ *и* $n|(p^{l'n} - 1)$, *то* $H \in DF(p^{l'}, n)$;

2) если n простое и не делит $p^{l'n} - 1$, то H есть подполе.

Кроме того, если пересечение $\pi(n) \cap \pi(p-1)$ пусто, l — простое число и не делит n, то Q имеет точно два максимальных подполя — $M(Q)$ и подполе порядка p^n.

Доказательство. Полагая $k = l/l'$, находим

$$\frac{p^{ln} - 1}{p^{l'n} - 1} = p^{l'n(k-1)} + p^{l'n(k-2)} + \cdots + 1.$$

Если $p^{l'n} \equiv 1(\bmod n)$, то сравнение (7.1.1) дает $j \equiv k(\bmod n)$ и, в силу леммы 7.1.1,

$$z = \text{НОД}(jl, l'n) = \text{НОД}(k^2 l', l'n) = l', \qquad H \in DF(p^{l'}, n).$$

Таким образом, первое утверждение доказано. Если n не делит $p^{l'n} - 1$, то для простого n получим $j = n$ и $z = l'n$. Отсюда $H \in DF(p^{l'n}, 1)$, т. е. H — подполе, что доказывает второе утверждение.

Докажем последнее утверждение теоремы. Пусть l — простое число, не делящее n. Если под-почти-поле H порядка p^n не коммутативно, то $H \in DF(p^{n/k}, k)$ для некоторого делителя k числа n. Тогда каждый простой делитель p_i числа k делит числа $p^{n/k} - 1$ и $p^l - 1$, в силу определения пары Диксона. Следовательно, p_i делит и число $p^d - 1$, где $d = \text{НОД}(l, n/k) = 1$; это противоречит условию $p_i \notin \pi(p-1)$. Поэтому под-почти-поле H коммутативно и является подполем. Его максимальность следует из простоты l.

Пусть теперь P — любое другое максимальное подполе в Q. Его порядок равен p^{lk} для некоторого делителя k числа n. Тогда, по следствию на с. 254 в [41], P содержит центр почти-поля Q и, по теореме 7.1.3, совпадает с $M(Q)$.

Теорема доказана. □

Пример 7.1. Условие $\pi(n) \cap \pi(p-1) = \varnothing$ в теореме существенно. Например, в почти-поле $Q \in DF(5^3, 2)$ центр $Z(Q)$ является единственным максимальным подполем. Действительно, Q имеет под-почти-поле H порядка 5^2 по лемме 7.1.1. Однако H не является подполем, поскольку

$$\frac{5^6 - 1}{5^2 - 1} = 5^4 + 5^2 + 1 \equiv 1(\bmod 2), \quad j = 1, \quad z = \text{НОД}(3, 2) = 1, \quad H \in DF(5^1, 2).$$

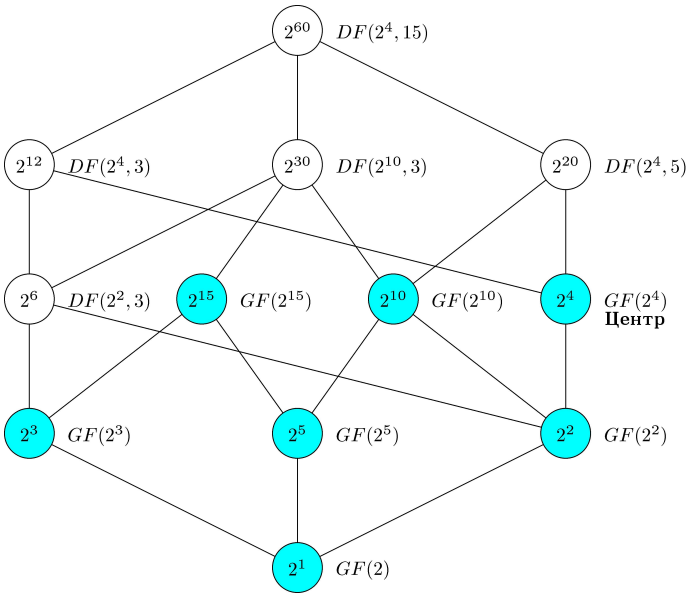

Рис. 4: Решетка под-почти-полей в почти-поле Диксона порядка 2^{60}

Отметим, что для другого почти-поля $P \in DF(5^2, 3)$ того же порядка 5^6 условие теоремы 7.1.4 выполнено, и поэтому P содержит точно два максимальных подполя — порядков 5^3 и 5^2.

Пример 7.2. Решетку под-почти-полей произвольного почти-поля порядка 2^{60} из класса $DF(2^4, 15)$ находим, используя теоремы 7.1.3 и 7.1.4, см. рис. 4; это почти-поле имеет три максимальных подполя — порядков 2^{15}, 2^{10} и 2^4. С другой стороны, почти-поле $Q \in DF(2^4, 45)$ порядка 2^{180} имеет три максимальные под-почти-поля

$$H \in DF(2^{10}, 9), \quad P \in DF(2^4, 9), \quad S \in DF(2^{12}, 5).$$

Их попарные пересечения дают три предмаксимальных под-почти-поля, из которых два — $H \cap S = M(H)$ и $P \cap S = M(P) = M(S)$ — являются максимальными в Q подполями порядков 2^{30} и 2^{12} соответственно. Из двух оставшихся предмаксимальных под-почти-полей одно (максимальное в H) порядка 2^{45} дает последнее максимальное в Q подполе.

Пример 7.3. Более симметричной решеткой под-почти-полей обладает почти-поле Q порядка 2^{180} из класса $DF(2^4, 45)$ (рис. 5). Это почти-поле имеет три максимальных подполя — порядков 2^{45}, 2^{30} и $2^{12} = |M(Q)|$. Максимальные под-почти-поля порядков 2^{90}, 2^{36}, 2^{60} не являются подполями.

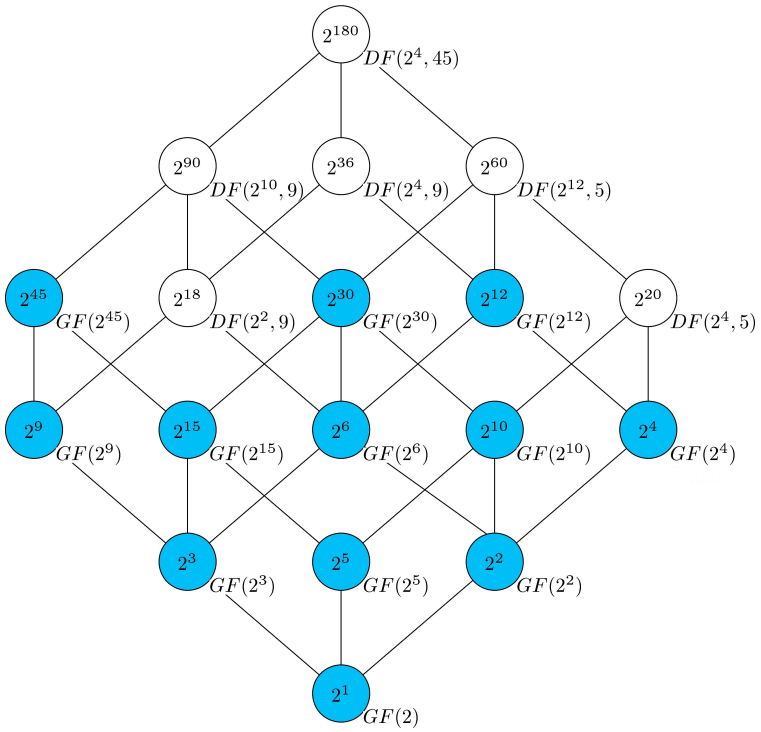

Рис. 5: Решетка под-почти-полей в почти-поле Диксона порядка 2^{180}

7.2. О неограниченности в совокупности числа максимальных подполей в конечных почти-полях

Квазиполе Q, не являющееся телом, часто называют *собственным* квазиполем. Будем называть Q *минимальным собственным квазиполем*, если всякое его подквазиполе $H \neq Q$ есть подполе. Теоремы 5.3.13, 5.6.1, 5.7.1 указывают примеры минимальных собственных полуполей.

В этом параграфе предложен [141] метод (теорема 7.2.3) построения некоторых *минимальных собственных почти-полей* Диксона. Кроме того, изучение решетки под-почти-полей в конечном почти-поле вызывает естественный вопрос (В.М. Левчук):

Существует ли такое натуральное число N, что количество максимальных подполей в произвольном конечном почти-поле меньше, чем N?

У. Фелгнером [49] показано, что максимальное подполе $M(Q)$, содержащее центр почти-поля Диксона Q, единственно (см. также квазиполя Холла). Почти-поле $Q \in DF(5^2, 3)$ имеет два максимальных подполя (пример 7.1), примеры 7.2 и 7.3 представляют почти-поля с тремя максимальными подполями. Далее показано, что вопрос выше решается отрицательно, и указан алгоритм (теорема 7.2.4) построения минимального собственного почти-поля, в котором коли-

чество максимальных подполей больше любого заданного натурального числа.

Для доказательства основных теорем нам потребуется следующий технический результат.

Лемма 7.2.1. *Пусть H — под-почти-поле порядка p^h почти-поля $Q \in DF(p^l, n)$ и $H \in DF(p^z, h/z)$. Тогда $(h/z)|n$.*

Доказательство. Достаточно рассмотреть случай, когда $k = (ln)/h$ — простое число. Пусть k делит n. Тогда $n = kn'$, $h = ln'$,

$$z = \text{НОД}\,(jl, h) = \text{НОД}\,(jl, ln') = l \cdot \text{НОД}\,(j, n') = ln'',$$

где n'' – делитель n. Получим

$$\frac{h}{z} = \frac{ln'}{ln''} = \frac{n'}{n''}|n.$$

Пусть k делит l. Тогда $l = kl'$. $h = l'n$,

$$z = \text{НОД}\,(jl, h) = \text{НОД}\,(jkl', l'n) = l' \cdot \text{НОД}\,(jk, n) = l'n',$$

где n' – делитель n. Получим

$$\frac{h}{z} = \frac{l'n}{l'n'} = \frac{n}{n'},$$

это число делит n. □

Выделим прежде всего случай минимальной степени расширения $n = 2$.

Теорема 7.2.2. *Всякое конечное почти-поле Диксона $Q \in DF(p^l, 2)$ имеет точно одно максимальное подполе – центр $Z(Q) \simeq GF(p^l)$.*

Доказательство. Очевидно, $p > 2$ и $Z(Q)$ является максимальным подполем в почти-поле Q. Пусть H – другое максимальное подполе в Q. Тогда $H \not\subset Z(Q)$ и $|H| = p^{2l'}$, где l' делит l. Рассмотрим убывающую цепочку под-почти-полей

$$Q = H_0 \supset H_1 \supset \cdots \supset H_{k-1} \supset H_k = H,$$

где $|H_i| = p^{h_i}$ и h_{i-1}/h_i – простые числа. Тогда, в силу максимальности подполя H, имеем $H_k \in DF(p^{2l'}, 1)$ и $H_{k-1} \in DF(p^{l''}, 2)$, где $l'|l''$, $l''|l$ и $l''/l' = m$ – простое число. Вычисляя параметр j (7.1.1) для под-почти-поля H_k в H_{k-1}, получим

$$j = \frac{p^{2l''} - 1}{p^{2l'} - 1} = \frac{p^{2ml'} - 1}{p^{2l'} - 1} = p^{2l'(m-1)} + p^{2l'(m-2)} + \cdots + p^{2l'} + 1 \equiv m (\bmod 2),$$

то есть $j = 1$ при $m > 2$ и $j = 2$ при $m = 2$.

Если $m > 2$, то $z = \text{НОД}(jl'', h) = \text{НОД}(l'm, 2l') = l'$, поэтому $H_k \in DF(p^{l'}, 2)$ и H_k не является подполем, противоречие.

Если $m = 2$, то $z = \text{НОД}(jl'', h) = \text{НОД}(2l'', 2l') = 2l'$. Получим $H_k \in DF(p^{2l'}, 1)$, $H_{k-1} \in DF(p^{2l'}, 2)$, где $2l'$ делит l, поэтому H_k содержится в центре $Z(Q)$ и не является максимальным подполем, противоречие. □

Если простая степень расширения n больше двух, то число p может быть выбрано так, что почти-поле Диксона $Q \in DF(q,n)$ является минимальным собственным почти-полем.

Теорема 7.2.3. *Для любого простого числа $n > 2$ существует бесконечно много конечных почти-полей степени расширения n над своим центром, в каждом из которых все под-почти-поля являются подполями.*

Доказательство. Пусть $n > 2$ – простое число. Выберем в поле $\mathbb{Z}_n$ примитивный элемент p_0, $p_0^{n-1} \equiv 1(\bmod n)$ и $p_0^m \not\equiv 1(\bmod n)$ для любого $0 < m < n-1$. Арифметическая прогрессия $\{p_0 + nt\}_{t=0}^{\infty}$ содержит бесконечно много простых чисел. Пусть $p = p_0 + nt$ – любое из них. Тогда (p^{n-1}, n) – пара Диксона. Действительно,

$$p^{n-1} = (p_0 + nt)^{n-1} \equiv p_0^{n-1} \equiv 1(\bmod n),$$

то есть n делит $q - 1 = p^{n-1} - 1$. Пусть теперь Q – произвольное почти-поле из класса $DF(p^{n-1}, n)$. Рассмотрим все его максимальные под-почти-поля. Ясно, в силу простоты n, что центр $Z(Q) \simeq GF(p^{n-1})$ является максимальным под-почти-полем в Q. Пусть $H \neq Z(Q)$ – любое другое максимальное под-почти-поле в Q. Тогда $|H| = p^h$, где $h = nl'$ и $k = (n-1)/l'$ – простое число. Вычислим для под-почти-поля H параметры j и z (7.1.1). Получим

$$j \equiv \frac{p^{(n-1)n} - 1}{p^{l'n} - 1}(\bmod n),$$

$$p^{(n-1)n} - 1 \equiv 0(\bmod n), \qquad p^n \equiv p(\bmod n),$$

$$p^{l'n} - 1 = (p^n)^{l'} - 1 \equiv p^{l'} - 1(\bmod n) \not\equiv 0(\bmod n),$$

отсюда $j = n$. Далее, $z = \text{НОД}(jl, h) = \text{НОД}(n(n-1), nl') = nl' = h$, поэтому $H \in DF(p^h, 1)$, то есть H есть подполе в Q. Таким образом, все максимальные под-почти-поля в Q являются подполями, их количество равно $|\pi(n-1)|+1$. $\square$

Следующая теорема предлагает способ построения минимального собственного почти-поля, в котором число максимальных подполей больше, чем любое заданное натуральное число.

Теорема 7.2.4. *Для любого натурального числа s существует минимальное собственное почти-поле Диксона, имеющее более чем s максимальных подполей.*

Доказательство. Пусть s – произвольное натуральное число. Рассмотрим произведение s различных простых чисел $N = r_1 \cdot r_2 \cdot \cdots \cdot r_s$. Тогда арифметическая прогрессия $\{1 + Nt\}_{t=1}^{\infty}$ содержит бесконечно много простых чисел.

Пусть $n = 1 + Nt_0$ – одно из них. По теореме 7.2.3, при некотором простом p класс почти-полей Диксона $DF(p^{n-1}, n)$ содержит почти-поле, в котором все под-почти-поля являются подполями. Число максимальных подполей в таком почти-поле равно $1 + |\pi(n-1)| \geq 1 + s$. □

Пример 7.4. Используя доказанные результаты, укажем пример почти-поля, в котором пять максимальных подполей, причем каждое под-почти-поле является подполем. Вычислим $n = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$, это простое число. Среди примитивных элементов поля $\mathbb{Z}_{211}$ выберем, например, простое число 3: $3^{210} \equiv 1 (\mathrm{mod}\, 211)$ и $3^m \not\equiv 1 (\mathrm{mod}\, 211)$ для всех $0 < m < 210$. Тогда почти-поле $Q \in DF(3^{210}, 211)$ имеет пять подполей H_i порядков 3^{h_i}, $i = 1, \ldots, 5$, где

$$h_1 = \frac{210 \cdot 211}{2},\ h_2 = \frac{210 \cdot 211}{3},\ h_3 = \frac{210 \cdot 211}{5},\ h_4 = \frac{210 \cdot 211}{7},\ h_5 = \frac{210 \cdot 211}{211}.$$

Действительно, непосредственные вычисления значений j и z (7.1.1) показывают, что $j = n$ и $z = h_i$, поэтому $h_i/z = 1$ и $H_i \simeq GF(3^{h_i})$. В силу простоты чисел n/h_i каждое такое подполе является также максимальным под-почти-полем в почти-поле Q.

Рассмотрим дополнительно минимальные собственные почти-поля Диксона, в которых максимальное подполе единственно.

Предложение 7.2.5. *Почти-поле Диксона Q является минимальным собственным почти-полем с единственным максимальным подполем тогда и только тогда, когда Q принадлежит одному из классов $DF(p, r)$, $DF(p, r^2)$, $DF(p^r, r)$, где p и r – допустимые простые числа.*

Доказательство. По результату [20], в почти-поле $Q \in DF(p, r)$ центр $\mathbb{Z}_p$ является единственным максимальным подполем, и других под-почти-полей в нем нет по лемме Данкс 7.1.1. Для почти-поля $Q \in DF(p, r^2)$ или $Q \in DF(p^r, r)$ порядка p^{r^2} единственное максимальное под-почти-поле является подполем $M(Q)$, так как $\lambda = r$. Обратно, пусть $Q \in DF(p^l, n)$ удовлетворяет условию леммы. В силу единственности максимального под-почти-поля в нем ясно, что произведение ln есть степень одного простого числа, $ln = r^t$. Максимальное подполе $M(Q)$, содержащее центр $GF(p^l)$, имеет порядок p^λ, где $\lambda = r^{[t/2]}$. Если $H \neq Q$ – максимальное под-почти-поле в Q порядка $p^{r^{t-1}}$, то $H = M(Q)$, Поэтому $t = 1$ или $t = 2$. Случай $DF(p^r, 1)$, очевидно, исключается ввиду коммутативности. □

Обращает на себя внимание возможность взаимосвязи минимальных собственных почти-полей Диксона и групп Миллера–Морено – конечных неабелевых групп, в которых всякая собственная подгруппа абелева [92]. Каждая такая

группа G разрешима, ее порядок может делиться не более чем на два различных простых числа. Если порядок G равен $p^\alpha q^\beta$ ($p \neq q$ – простые, $\alpha, \beta > 0$), то G содержит точно q^β циклических подгрупп порядка p^α и одну (нормальную) подгруппу порядка q^β типа $(1, 1, 1, \dots)$. Заметим, что если G – мультипликативная группа почти-поля Диксона, то такая подгруппа также должна быть циклической и поэтому $\beta = 1$. Если порядок группы Миллера–Морено равен p^α, то в ней точно $p + 1$ подгруппа порядка $p^{\alpha-1}$.

Легко привести примеры минимальных почти-полей Диксона Q, в которых мультипликативная группа Q^* является группой Миллера–Морено. Например, указанное на рис. 5 почти-поле из класса $DF(2^2, 3)$ – минимальное собственное, в нем точно два максимальных подполя порядков 2^2 и 2^3. Его мультипликативная группа имеет порядок 63 и является группой Миллера–Морено. С другой стороны, рассмотренное выше минимальное почти-поле Диксона из класса $DF(3^{210}, 211)$ имеет мультипликативную группу порядка $3^{210 \cdot 211} - 1$, это число делится, по крайней мере, на три простых числа 2, 11, 13, поэтому группа не является группой Миллера–Морено. Более простые примеры представляют минимальные почти-поля Диксона порядков 5^2 и 11^2.

Список литературы

[1] Коксетер Г. С. М., Мозер У. О. Дж. Порождающие элементы и определяющие соотношения дискретных групп. – М.: Наука, 1980, 240 с.

[2] Курош А. Г. Лекции по общей алгебре. – М.: Физматгиз, 1962, 396 с.

[3] Курош А. Г. Теория групп. – М.: Наука, 1967, 648 с.

[4] Левчук В. М., Панов С. В., Штуккерт П. К. Вопросы перечисления проективных плоскостей и латинских прямоугольников // В сборнике "Механика и моделирование". — Красноярск: СибГАУ, 2012, с. 56–70.

[5] Левчук В. М., Старикова О. А. Квадратичные формы проективных пространств над кольцами // Матем. сб., т. 197 (2006), № 6, с. 97-–110.

[6] Левчук В. М., Штуккерт П. К. Строение квазиполей малых четных порядков // Тр. ИММ УрО РАН, т. 21 (2015), № 3, с. 197–212.

[7] Лидл Р., Пильц Г. Прикладная абстрактная алгебра. – Екатеринбург: Изд-во Урал. ун-та, 1996, 744 с.

[8] Мазуров В. Д. О точно дважды транзитивных группах // Новосибирск: Издательство ИМ СО РАН. Вопросы алгебры и логики, 1996, с. 233–236.

[9] Мазуров В. Д. О бесконечных группах с абелевыми централизаторами инволюций // Алгебра и логика, т. 39 (2000), № 1, с. 74–86.

[10] Нерешенные вопросы теории групп. Коуровская тетрадь / Сост. Мазуров В. Д., Хухро Е. И. – 16 изд., доп. – Ин-т матем. им. С. Л. Соболева СО РАН, Новосибирск, 2006, 193 с.

[11] Подуфалов Н. Д. О функциях на линейных пространствах, связанных с конечными проективными плоскостями // Алгебра и логика, т. 41 (2002), № 1, с. 83–103.

[12] Подуфалов Н. Д., Бусаркина И. В. Группа автотопизмов полуполевой p-примитивной плоскости порядка q^4 // Алгебра и логика, т. 35 (1996), № 3, с. 334–344.

[13] Подуфалов Н. Д., Бусаркина И. В., Дураков Б. К. О группе автотопизмов полуполевой p-примитивной плоскости // В сб. материалов межрегиональной научной конференции «Исследования по анализу и алгебре». – Томск, ТГУ, 1998, с. 190–195.

[14] Попова А. В. О законе умножения в полуполях порядка 16 // В сб. материалов Международной конференции студентов, аспирантов и молодых ученых «Проспект Свободный-2015». – Красноярск, СФУ, 2015, с. 18–19.

[15] Созутов А. И., Сучков Н. М., Сучкова Н. Г. Бесконечные группы с инволюциями. – Красноярск: Сибирский федеральный ун-т, 2011, 149 с.

[16] Созутов А. И., Дураков Е. Б., О локальной конечности периодических точно трижды транзитивных групп // Алгебра и логика, т. 54 (2015), № 1, с. 70–84.

[17] Супруненко Д. А. Группы матриц. – М.: Наука, 1972, 352 с.

[18] Холл М. Теория групп. – М.: Госиноиздат, 1962, 468 с.

[19] Штуккерт П. К. Квазиполя и проективные плоскости трансляций малых четных порядков // Известия Иркутского государственного университета. Серия Математика, т. 7 (2014), с. 141–159.

[20] Яковлева Т. Н. Вопросы строения квазиполей с ассоциативными степенями // Известия Иркутского государственного университета. Серия «Математика», т. 29 (2019), с. 107–119.

[21] Albert A. A. On nonassociative division algebras // Trans. Amer. Math. Soc., vol. 72 (1952), p. 296–309.

[22] Albert A. A. Finite noncommutative division algebras // Proc. Amer. Math. Soc., vol. 9 (1958), p. 928–932.

[23] Albert A. A. On the collineation groups of certain non-desarguesian planes // Port. Math., vol. 18 (1959), p. 207–224.

[24] Albert A. A. Finite division algebras and finite planes // Proc. Sympos. Appl. Math., AMS, Provid. R.I, vol. 10 (1960), p. 53–70.

[25] André J. Über nicht-Desarguessche Ebenen mit Transitiver Translationsgruppe // Mathematische Zeitschrift, vol. 60 (1954), p. 156—186.

[26] André J. Projektive Ebenen Über Fastkörpern // Mathematische Zeitschrift, vol. 62 (1955), p. 137-160.

[27] ATLAS of Finite Group Representations – Version 3, http://brauer.maths.qmul.ac.uk/Atlas/v3/

[28] Bartolone C., Ostrom T. G. Translation planes of order q^3 which admit $SL(2,q)$ // Journal of Algebra, vol. 99 (1986), p. 50–57.

[29] Biliotti M., Jha V., Johnson N. L., Menichetti G. A structure theory for two-dimensional translation planes of order q^2 that admit collineation group of order q^2 // Geom. Dedicata, vol. 29 (1989), p. 7–43.

[30] Biliotti M., Montinaro A. On the finite projective planes of order up to q^4, q odd, admitting $PSL(3,q)$ as a collineation group // Innovations in Incidence Geometry: Algebraic, Topological and Combinatorial, vol. 6 (2008), no. 1, p. 73–94.

[31] Boykett T., Howell K.-T. The multiplicative automorphisms of a finite nearfield, with an application // Commun. Algebra, vol. 44 (2016), is. 6, p. 2336–2350.

[32] Brown C., Pumplün S., Steele A. Automorphisms and isomorphisms of Jha-Johnson semifields obtained from skew polynomial rings // Communications in Algebra, vol. 46 (2018), no. 10, p. 4561–4576.

[33] Büttner W. On 4-Dimensional Translation Planes Admitting a Suzuki Group as Group of Automorphisms // J. Comb. Theory, Ser. A, vol. 37 (1984), no. 1, p. 76–79.

[34] Chein O. Moufang loops of small order. I // Trans. of the Amer. Math. Soc., vol. 188 (1974), is. 2, p. 31–51.

[35] Cordero M. Semifield plans of order p^4 that admit a p-primitive Baer collineation // Osaka J. Math., vol. 28 (1991), p. 305–321.

[36] Cordero-Vourtsanis M. The autotopizm group of p-primitive semifield plans of order p^4 // ARS Combinatoria, vol. 32 (1991), p. 57–64.

[37] Cordero M. Matrix spread sets of p-primitive semifeld planes // Internat. J. Math. and Math. Sci., vol. 20 (1997), no. 2, p. 293–298.

[38] Cordero M., Jha V. On the multiplicative structure of quasifields and semifields: cyclic and acyclic loops // Note di Matematica, vol. 29 (2009), no. 1, p. 45–59.

[39] Cordero M., Jha V. Primitive semifields and fractional planes of order q^5 // Rendiconti di Matematica, Serie VII, Roma, vol. 30 (2010), p. 1–21.

[40] Dancs S. The sub-near-field structure of finite near-fields // Bull. Austral. Math. Soc., vol. 5 (1971), p. 275–280.

[41] Dancs S. On finite Dickson near-fields // Abh. Math. Sem. Univ. Hamburg, vol. 37 (1972), p. 254–257.

[42] Dancs Groves S. Locally finite near-fields // Abh. Math. Sem. Univ. Hamburg, vol. 48 (1979), p. 89–107.

[43] Dembowski P. Finite geometries: Reprint of the 1968 edition. – Springer-Verlag Berlin Heidelberg, 1997, 317 p.

[44] Dempwolff U. Semifield planes of order 81 // J. Geom., vol. 89 (2008), no. 1–2, p. 1–16.

[45] Dempwolff U. File of Translation Planes of Small Order, ($http : //www.mathematik.uni - kl.de/ \sim dempw/dempw\_Plane.html$).

[46] Dickson L. E. On finite algebras // Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. II (1905), p. 358–393.

[47] Dickson L. E. Linear algebras in which division is always uniquely possible // Trans. Amer. Math. Soc., vol. 7 (1906), no.3, p. 370–390.

[48] Ellers E., Karzel H. Endliche Inzidenzgruppen // Abh. Math. Sem. Hamburg, vol. 27 (1964), p. 250–264.

[49] Felgner U. Pseudo-finite near-fields. – In «Near-rings and near-fields». Elsevier Science Publisher B. V. North-Holland, 1987, p. 15–29.

[50] Foulser D. A., Johnson N. L., Ostrom T. G. A characterization of the Desarguesian planes of order q^2 by $SL(2, q)$ // Internat. J. Math. & Math. Sci., vol. 6 (1983), no. 3, p. 605–608.

[51] Ganley M. J. Baer involutions in semi-field planes of even order // Geom. Dedi., vol. 2 (1974), p. 499–508.

[52] Ganley M. J., Jha V. On a conjecture of Kallaher and Liebler // Geom Dedicata, vol. 21 (1986), p. 277–289.

[53] Ganley M. J., Jha V. On translation planes with a 2-transitive orbit on the line at infinity // Arch. Math., vol. 47 (1986), p. 379–384.

[54] Goldschmidth D. M. 2-fusion in finite groups // Ann. Math., vol. 99 (1974), no 1, p. 70–117.

[55] Gorenstein D. Finite simple groups. An introduction to their classification. Plenum Press, New York, 1982, 352 p.

[56] Gow R., Sheekey J. On primitive elements in finite semifields // Finite Fields and Their Applications, vol. 17 (2011), p. 194–204.

[57] Grishkov A.N., Zavarnitsyn A.V. Lagrange's theorem for Moufang loops // Math. Proc. Phil. Soc., vol. 139 (2005), p. 41–57.

[58] Grishkov A.N., Zavarnitsyn A.V. Sylow's theorems for Moufang loops // J. Algebra, vol. 321 (2009), no. 7, p. 1813–1825.

[59] Hall M., Jr. Projective planes // Transactions of the American Mathematical Society, vol. 54 (1943), p. 229–277.

[60] Hall M. On a theorem of Jordan // Pacific J. Math., vol. 4 (1954), p. 219–226.

[61] Hentzel I. R., Rúa I. F. Primitivity of finite semifields with 64 and 81 elements // International Journal of Algebra and Computation, vol. 17 (2007), no. 7, p. 1411–1429.

[62] Hiramine Y., Matsumoto M., Oyama T. On some extension of 1-sread sets // Osaka J. Math., vol. 24 (1987), p. 123–137.

[63] Ho C., Goncalves A. On $PSU(3, q)$ as collineation groups // Journal of Algebra, vol. 111 (1987), p. 1–13.

[64] Huang H., Johnson N. L. 8 semifield planes of order 8^2 // Discrete Math., vol. 80 (1990), no. 1, p. 69–79.

[65] Hughes D. R. Review of some results in collineation groups // Proc. Sympos. Pure Math., American Mathematical Society, Providence, R. I., v. 1 (1959), p. 42–55.

[66] Hughes D. R. Collineation groups of non-Desarguesian planes II, Some seminuclear division algebras // Amer. J. Math., vol. 82 (1960), no. 1, p. 113–119.

[67] Hughes D. R., Kleinfeld E. Seminuclear extension of Galois fields // Am. J. Math., vol. 82 (1960), p. 389–392.

[68] Hughes D. R., Piper F. C. Projective planes. – Springer–Verlag New–York Inc., 1973, 292 p.

[69] Hughes D. R., Kallaher M. J. On the Knuth semi-fields // Internat. J. Math. & Math. Sci., vol. 3 (1980), no. 1, p. 29–45.

[70] Jha V., Johnson N. L. The centre of a finite semifield plane is a geometric invariant // Arch. Math., vol. 59 (1988), p. 93–96.

[71] Jha V., Johnson N. L. The translation planes of order 81 admitting $SL(2,5)$ // Note di Matematica, vol. 24 (2005), no. 2, p. 59–73.

[72] Johnson N. L., Jha V., Biliotti M. Handbook of finite translation planes. – Chapman and Hall, Boca Raton, London, New York, 2007, 861 p.

[73] Johnson N. L. On the solvability of the collineation groups of derivable translation planes // Journal of Algebra, vol. 71 (1981), p. 569–575.

[74] Johnson N. L. Sequences of derivable translation plans // Osaka J. Math., vol. 25 (1988), p. 519–530.

[75] Johnson N. L. Semifield plans of characteristic p admiting p-primitive Baer collineation // Osaka J. Math., vol. 26 (1989), p. 281–285.

[76] Kallaher M. J. A conjecture on semi-field planes // Arch. Math., vol. 26 (1975), p. 436–440.

[77] Kantor W. M. Commutative semifields and symplectic spreads // Journal of Algebra, vol. 270 (2003), no. 1, p. 96–114.

[78] Kantor W. M. Finite semifields. – In «Finite geometries, groups, and computation». Walter de Gruyter GmbH & Co. KG, Berlin, 2006, p. 103–114.

[79] Kegel O. H. Zur Structur lokal endlicher Zassenhausgruppen // Arch. Math., vol. 18 (1967), p. 337–348.

[80] Kleinfeld E. Techniques for enumerating Veblen-Wedderburn systems // J. Assoc. Comput. Mach., vol. 7 (1960), p. 330–337.

[81] Knuth D. E. Finite semifields and projective planes (PhD dissertation). – Pasadena: California Inst. of Thechnology, 1963.

[82] Knuth D. E. Finite semifields and projective planes // J. Algebra, vol. 2 (1965), p. 182–217.

[83] Lavrauw M. Finite semifields and nonsingular tensors // Des. Codes Cryptogr., vol. 68 (2013), p. 205–227.

[84] Lavrauw M., Polverino O. Finite semifields. – In «Current research topics in Galois Geometry», L. Storme and J. De Beule, editors, NOVA Academic Publishers, 2011, chapter 6, p. 131–160.

[85] Levchuk V. M., Panov S. V., Shtukkert P. K. The structure of finite quasifields and their projective translation planes // Proc. XII Int. conf. on Algebra and Number Theory, Tula (2014), p. 106–108.

[86] Levchuk V. M., Shtukkert P. K. Problems on structure for quasifields of orders 16 and 32 // J. of Siberian Federal University. Ser. Math. & Physics, vol. 7 (2014), no. 3, p. 362–372.

[87] Lüneburg H. Über die Anzahl der Dickson'schen Fastkörper gegebender Ordnung // Atti del convegno di geometria combinatoria e sue applicazioni, Perugia, 1971, p. 319–322.

[88] Lüneburg H. Translation planes. – Springer-Verlag, New-York, 1980, 270 p.

[89] Menichetti G. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field // Journal of Algebra, vol. 47 (1977), no. 2, p. 400–410.

[90] Menichetti G. n-dimensional algebras over a field with a cyclic extension of degree n // Geometriae Dedicata, vol. 63 (1996), no. 1, p. 69–94.

[91] Maduram D. M. Matrix representation of translation planes // Geom Dedicata 4, 485–492 (1975). https://doi.org/10.1007/BF00148776

[92] Miller G. A., Moreno H. C. Nonabelian groups in which every subgroup is abelian // Trans. Amer. Math. Soc., vol. 4 (1903), p. 398–404.

[93] Moorhouse G. E. $PSL(2, q)$ as a collineation group of projective planes of small orders // Geom. Dedicata, vol. 31 (1989), no. 1, p. 63–88.

[94] Ojanguren M., Sridharan R. A note on the fundamental theorem of projective geometry // Comment Math. Helv., vol. 44 (1969), p.310–315.

[95] Ostrom T. G. Translation planes of odd order and odd dimension // Internat. J. Math.& Math. Sci., vol. 2 (1979), no. 2, p. 187–208.

[96] Oyama T. On quasifields // Osaka J. Math., vol. 22 (1985), p. 35–54.

[97] Podufalov N. D. On spread sets and collineations of projective planes // Contem. Math., vol. 131 (1992), part 1, p. 697–705.

[98] Prince A. R. A class of two-dimensional translationplanes admitting $SL(2, 5)$ // Note di Matematica, vol. 29 (2009), suppl. no. 1, p. 223–230.

[99] Rips E., Segev Y., Tent K. A sharply 2-transitive group without a non-trivial abelian normal subgroup // Journal of the European mathematical society, vol. 19 (2017), is. 10, p. 2895–2910.

[100] Rúa I. F. Primitive and Non-Primitive Finite Semifields // Commun. Algebra, vol. 22 (2004), p. 223–233.

[101] Rúa I. F., Combarro E. F. New Semifield Planes of order 81 // arXiv:0803.0411, 2008.

[102] Rúa I. F., Combarro E. F., Ranilla J. Classification of semifields of order 64 // J. of Algebra, vol. 322 (2009), no. 11, p. 4011–4029.

[103] Rúa I. F., Combarro E. F., Ranilla J. Determination of division algebras with 243 elements // Finite Fields and their Applications, vol. 18 (2012), p. 1148–1155.

[104] Rúa I. F. On the primitivity of four-dimensional finite semifields // Finite Fields and Their Applications, vol. 33 (2015), p. 212–229.

[105] Rúa I. F. Primitive semifields of order 2^{4e} // Designs, Codes and Cryptography, vol. 83 (2017), is. 2, p. 345–356.

[106] Sandler R. The collineation groups of some finite projective planes // Portugal. Math., vol. 21 (1962), p. 189–199.

[107] Hui A. M. W., Tai Y. K., Wong P. P. W. On the autotopism group of the commutative Dickson semifield $\mathcal{K}$ and the stabilizer of the Ganley unital embedded in the semifield plane $\Pi(\mathcal{K})$ // Innovations in Incidence Geometry, vol. 14 (2015), p. 27–42.

[108] Tent K., Ziegler M. Sharply 2-transitive groups // Advances in Geometry, vol. 16 (2016), no. 1, p. 131–134.

[109] Tent K. Sharply 3-tranzitive groups // Advances in Mathematics, vol. 286 (2016), p. 722–728.

[110] Thompson J. G. Nonsolvable finite groups all of whose local subgroups are splvable // Bull. Amer. Math. Soc., vol. 74 (1968), p. 383–437.

[111] Tits J. Groups triplement transitivs et generalizations // Algébre et Théorie des Nombers, Coll. Int. du Centre Nat. de la Rech. Sci., vol. 24 (1950), p. 207–208.

[112] Vaughan T. P. Polynomials and linear transformations over finite fields // J. Reine Angew. Math., vol. 262 (1974), p. 179–206.

[113] Veblen O., Maclagan–Wedderburn J. H. Non-Desarguesian and Non-Pascalian Geometries // Trans. Amer. Math. Soc., vol. 8 (1907), no. 3, p. 379–388.

[114] Vechtomov E. M., Cheraneva A. V. Semifields and their properties // J. Math. Sci., vol. 163 (2009), № 6, p. 625-–661. (Вечтомов Е. М., Черанева А. В. Полутела и их свойства // Фундамент. и прикл. матем., т. 14 (2008), № 5, с. 3–54.)

[115] Vechtomov E. M., Chuprakov D. V. The principal kernels of semifields of continuous positive functions // J. Math. Sci., vol. 163 (2009), № 5, p. 500-–514. (Вечтомов Е. М., Чупраков Д. В. Главные ядра полуполей непрерывных положительных функций // Фундамент. и прикл. матем., т. 14 (2008), № 4, с. 87–107.)

[116] Walker R. J. Determination of division algebras with 32 elements. – In Proc. Sympos. Appl. Math., Amer. Math. Soc., Providence, R.I., 1963, vol. XV, p. 83–85.

[117] Wähling H. Theorie der Fastkörper. Volume 1 of Thales Monographs. – Thales-Verlag, Essen, 1987, 393 p.

[118] Weibel C. Survey of non-Desarguesian planes // Notice of the AMS, v. 54 (2007), no. 10, p. 1294–1303.

[119] Wene G. P. On the multiplicative structure of finite division rings // Aequationes Math., vol. 41 (1991), no. 1, p. 222–233.

[120] Wene G. P. Inner automorphisms of finite semifields // Note Mat., vol. 29 (2009), suppl. no. 1, p. 231–242.

[121] Zassenhaus H. Uber endliche Fastkörper // Abh. Math. Sem. Hamburg, vol. 11 (1936), p. 187–220.

[122] Zehfuss J. G. Ueber eine gewisse Determinante // Zeitschrift für Mathematik und Physik, vol. 3 (1858), p. 298–301.

Работы автора по теме диссертации

[123] Подуфалов Н. Д., Дураков Б. К., Кравцова О. В., Дураков Е. Б. О полуполевых плоскостях порядка 16^2 // Сиб. Мат. Журн., т. 37 (1996), № 3, с. 616–623.

[124] Кравцова О. В. Полуполевая плоскость ранга 2, допускающая нелинейную бэровскую инволюцию // Фундамент. и прикл. матем., т. 6 (2000), № 1, с. 163–170.

[125] Podufalov N. D., Durakov B. K., Busarkina I. V., Kravtsova O. V., Durakov E. B. Some results on finite projective planes // Journal of Mathematical Sciences, vol. 102 (2000), no. 3, p. 4032–4038. (Подуфалов Н. Д., Дураков Б. К., Бусаркина И. В., Кравцова О. В., Дураков Е. Б. Некоторые результаты о конечных полуполевых плоскостях // Итоги науки и техники, Серия «Современная математика и ее приложения. Тематические обзоры», том 63, Алгебра (1999), № 13.)

[126] Кравцова О. В., Куршакова (Штуккерт) П. К. К вопросу об изоморфизме полуполевых плоскостей // Вестник КГТУ. Математические методы и моделирование, Красноярск, вып. 42 (2006), с. 13–19.

[127] Кравцова О. В., Прамзина В. О. О подгруппе коллинеаций полуполевой плоскости, изоморфной A_4 // Журнал Сибирского федерального университета. Математика и физика, т. 4 (2011), № 4, с. 498–504.

[128] Kravtsova O. V., Panov S. V., Shevelyova I. V. Some results on isomorphisms of finite semifield planes // Journal of Siberian Federal University. Mathematics & Physics, vol. 6 (2013), no. 1, p. 33–39.

[129] Кравцова О. В. Полуполевые плоскости, допускающие бэровскую инволюцию // Известия Иркутского государственного университета. Серия «Математика», (2013), № 2, с. 26–38.

[130] Дураков Б. К., Кравцова О. В. Построение и исследование полуполевых плоскостей порядка 256 // Вестник Красноярского государственного педагогического университета им. В. П. Астафьева, т. 23 (2013), № 1, с. 207–210.

[131] Кравцова О. В. Полуполевые плоскости нечетного порядка, допускающие подгруппу автотопизмов, изоморфную A_4 // Изв. вузов. Матем., (2016), № 9, с. 10–25 (Russian Math. (Iz. VUZ), vol. 60 (2016), no. 9, p. 7–22).

[132] Kravtsova O. V. On automorphisms of semifields and semifield planes // Siberian Electronic Mathematical Reports, vol. 13 (2016), p. 1300–1313.

[133] Кравцова О. В. О гипотезе левопримитивности конечного полуполя // Вестник московского университета им. С. Ю. Витте, серия «Образовательные ресурсы и технологии», т. 14 (2016), № 2, с. 330–336

[134] Levchuk V. M., Kravtsova O. V. Problems on structure of finite quasifelds and projective translation planes // Lobachevskii Journal of Mathematics, vol. 38 (2017), no 4, p. 688—698.

[135] Kravtsova O. V. Minimal polynomials in finite semifields // Journal of Siberian Federal University. Mathematics & Phisics, vol. 11 (2018), no. 5, p. 588–596.

[136] Кравцова О. В., Дураков Б. К. Полуполевые плоскости нечетного порядка, допускающие подгруппу автотопизмов, изоморфную A_5 // Сиб. матем. журн., т. 59 (2018), № 2, с. 396–411 (Siberian Math. J., vol. 59 (2018), no. 2, p. 309–322).

[137] Созутов А. И., Кравцова О. В. О KT-полях и точно трижды транзитивных группах // Алгебра и логика, т. 57 (2018), № 2, с. 232–242 (Algebra and Logic, vol. 57 (2018), no. 2, 153–160).

[138] Кравцова О. В., Моисеенкова Т. В. Полуполевые плоскости ранга 2, допускающие группу S_3 // Тр. ИММ УрО РАН, т. 25 (2019), № 4, с. 118–128.

[139] Кравцова О. В., Левчук В. М. Вопросы строения конечных почти-полей // Тр. ИММ УрО РАН, т. 25 (2019), № 4, с. 107–117.

[140] Кравцова О. В., Шевелева И. В. О некоторых 3-примитивных полуполевых плоскостях // Чебышевский сборник, т. 20, (2019), вып. 3, с. 316–332.

[141] Kravtsova O. V. Minimal proper quasifields with additional conditions // Journal of Siberian Federal University. Mathematics & Physics, vol. 13 (2020), no. 1, p. 104–113.

[142] Kravtsova O. V. On alternating subgroup A_5 in autotopism group of finite semifield plane // Сибирские электронные математические известия, т. 17 (2020), с. 47–50.

[143] Кравцова О. В. Полуполевые плоскости, допускающие группу кватернионов Q_8 // Алгебра и логика, т. 59 (2020), № 1, с. 101–115.

[144] Kravtsova O. V. Elementary abelian 2-subgroups in an autotopism group of a semifield projective plane // Известия Иркутского государственного университета. Серия «Математика», т. 32 (2020), с. 49–63.

[145] Кравцова О. В. 2-элементы в группе автотопизмов полуполевой проективной плоскости // Известия Иркутского государственного университета. Серия «Математика», т. 39 (2022), с. 96—110.

[146] Кравцова О. В., Скок Д. С. Метод регулярного множества построения конечных квазиполей // Тр. ИММ УрО РАН, т. 28 (2022), № 1, с. 164–181.

[147] Kravtsova O. V. Dihedral group of order 8 in an autotopism group of a semifield projective plane of odd order // Journal of Siberian Federal University. Mathematics & Physics, vol. 15 (2022), no. 3, p. 21–27.

[148] Кравцова О. В. Полуполевая плоскость ранга 2, допускающая нелинейную бэровскую инволюцию // Тезисы докладов на Международной алгебраической конференции памяти А. Г. Куроша. – Москва: изд-во механико-математического факультета МГУ, 1998, с .184.

[149] Кравцова О. В. О построении дуальных полуполевых плоскостей // Материалы XVI Межвузовской научно-технической конференции, посвященной 370-летию Красноярска. – Красноярск, КрасГАСА, 1998, с. 8.

[150] Подуфалов Н. Д., Дураков Б. К., Бусаркина И. В., Кравцова О. В., Дураков Е. Б. Некоторые результаты о конечных полуполевых плоскостях // Материалы XVI Межвузовской научно-технической конференции, посвященной 370-летию Красноярска. – Красноярск, КрасГАСА, 1998, с. 13.

[151] Кравцова О. В. Полуполевая плоскость ранга 2, допускающая нелинейную бэровскую инволюцию // Материалы межрегиональной научной конференции «Исследования по анализу и алгебре», Томск, ТГУ, 1998.

[152] Дураков Е. Б., Кравцова О. В. Исследование полуполевых плоскостей с использованием вычислительной техники // Материалы международной научной конференции «Компьютерные и вычислительные методы в математике», Омск, 1998.

[153] Дураков Б. К., Дураков Е. Б., Кравцова О. В., Никитина О. А., Завьялов М. Н. О функциях, построенных на основе регулярных множеств полуполевых плоскостей // Международная конференция «Алгебра и ее приложения» (тезисы докл.), Красноярск: КГУ, 2002.

[154] Кравцова О. В. О некоторых трансляционных плоскостях, допускающих A_4 // «Тезисы докладов III Всесибирского Конгресса женщин-математиков», Красноярск, 2004, с. 38–39.

[155] Кравцова О. В., Куршакова О. В. Изоморфизм полуполевых плоскостей // Материалы конференции «IV Всесибирский конгресс женщин-математиков», Красноярск, 2006, с. 87–88.

[156] Кравцова О. В. Полярности некоторых полуполевых плоскостей // Международная конференция «Алгебра и ее приложения», Красноярск, 2007, с. 79–80.

[157] Кравцова О. В., Панов С. В. Полуполевые плоскости, заданные линейными функциями // Тезисы докладов международной конференции «Алгебра, логика и приложения», Красноярск, 2010, с. 56–57.

[158] Созутов А. И., Дураков Е. Б., Кравцова О. В. О некоторых точно трижды транзитивных группах // Тезисы докладов международной конференции «Алгебра, логика и приложения», Красноярск, 2010, с. 86–89.

[159] Кравцова О. В., Панов С. В., Шевелева И. В. Некоторые результаты об изоморфизмах конечных полуполевых плоскостей // Материалы Всероссийской научной конференции «VII Всесибирский конгресс женщин-математиков», Красноярск: СибГТУ, 2012, с. 101–103.

[160] Дураков Б. К., Кравцова О. В. Построение и исследование полуполевых плоскостей порядка 256 // Научно-методическая конференция «Информационные технологии в математике и математическом образовании», Красноярск, 2012.

[161] Кравцова О. В. Полуполевые плоскости, допускающие бэровскую инволюцию // Международная конференция "Алгебра и комбинаторика посвященная 60-летию А. А. Махнева, Екатеринбург, 2013.

[162] Кравцова О. В. Некоторые подгруппы автоморфизмов полуполевых плоскостей // «Алгебра и логика: теория и приложения. Международная конференция, посвященная памяти В.П. Шункова», Красноярск, 2013, с. 78–80.

[163] Кравцова О. В. Подгруппа автотопизмов полуполевой плоскости нечетного порядка, изоморфная знакопеременной группе A_4 // «Материалы конференции «Алгебра и математическая логика: теория и приложения», Казань: Изд-во Казан. ун-та, 2014, с. 89.

[164] Кравцова О. В. Об изоморфизме полуполевых плоскостей // XII Международная конференция «Алгебра и теория чисел: современные проблемы и приложения», посвященная 80-летию В. Н. Латышева, Тула, 2014, с. 167–168.

[165] Кравцова О. В. Подгруппа автотопизмов полуполевой плоскости нечетного порядка, изоморфная группе кватернионов Q_8 // «Алгебра и при-

ложения»: Труды Международной конференции по алгебре, посвященной 100-летию со дня рождения Л.А. Калужнина, Нальчик, 2014, с. 71-72.

[166] Кравцова О. В. Об автоморфизме порядка 2 конечного полуполя // Международная конференция «Мальцевские чтения», посвященная 75-летию Ю. Л. Ершова, Новосибирск, 2015, с. 161.

[167] Кравцова О. В. О некоторых полуполевых плоскостях нечетного порядка // «Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения»: Материалы XIII Международной конференции, посвященной 85-летию со дня рождения профессора С. С. Рышкова, Тула, 2015, с. 162–163.

[168] Kravtsova O. V. The automorphism group of finite semifield // Groups and Graphs, Algoritms and Automata, 2015: Abstracts of the International Conference and PhD Summer School in honor of the 80th Birthday of Professor V.A. Belonogov and of the 70th Birthday of Professor V.A. Baransky. Yekaterinburg: UrFU Publishing house, 2015, p. 64–65.

[169] Levchuk V. M., Kravtsova O. V. Problems on structure of finite quasifields and projective translation planes // Groups and Graphs, Algoritms and Automata, 2015: Abstracts of the International Conference and PhD Summer School in honor of the 80th Birthday of Professor V.A. Belonogov and of the 70th Birthday of Professor V.A. Baransky. Yekaterinburg: UrFU Publishing house, 2015, p. 24.

[170] Кравцова О. В. О некоторых полуполях порядка 64 // Материалы международной конференции по алгебре, анализу и геометрии и молодежной школы-конференции по алгебре, анализу, геометрии, Казань: Казанский университет, изд-во Академии наук РТ, 2016, с. 221.

[171] Sozutov A. I., Kravtsova O. V. On KT-fields and sharply 3-transitive groups // Материалы международной конференции по алгебре, анализу и геометрии и молодежной школы-конференции по алгебре, анализу, геометрии, Казань: Казанский университет, изд-во Академии наук РТ, 2016, с. 70.

[172] Levchuk V. M., Kravtsova O. V. Problems on structure of finite quasifields and projective translation planes // Материалы международной конференции по алгебре, анализу и геометрии и молодежной школы-конференции по алгебре, анализу, геометрии, Казань: Казанский университет, изд-во Академии наук РТ, 2016, с. 32.

[173] Levchuk V. M., Kravtsova O. V. Problems on structure of finite quasifields and projective translation planes // «Алгебра и логика: теория и приложения»: тезисы докладов Международной конференции, посвященной 70-летию В. М. Левчука, Красноярск, Сибирский федеральный университет, 2016, с. 103.

[174] Durakov B. K., Kravtsova O. V. Automorphism group of finite semifield plane // XI Школа-конференция по теории групп: тезисы докладов Международной конференции, посвященной 70-летию А. Ю. Ольшанского, Красноярск, Сибирский федеральный университет, 2016, с. 67–68.

[175] Kravtsova O. V. The structure of Hentzel-Rua semifield of order 64 // Graphs and Groups, Spectra and Symmetries, 2016: Abstracts of the International Conference and PhD-Master School on Graphs and Groups, Spectra and Symmetries, Novosibirsk: Sobolev Institute of Mathematics, 2016, p. 75.

[176] Кравцова О. В. О внутренних автоморфизмах конечных полуполей // Математика в современном мире. Международная конференция, посвященная 60-летию института математики им. С. Л. Соболева: Тез. докладов, Новосибирск, 2017, с. 84.

[177] Дураков Б. К., Кравцова О. В. Подгруппа автотопизмов полуполевой плоскости, изоморфная A_5 // Алгебра и теория алгоритмов [Электронный ресурс]: Всероссийская конференция, посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета: сборник материалов, Иваново: Иван. гос. ун-т, 2018, с. 58.

[178] Кравцова О. В., Моисеенкова Т. В. Конечные полуполевые плоскости, допускающие подгруппу автотопизмов, изоморфную S_3 // Международная алгебраическая конференция, посвященная 110-летию со дня рождения профессора А. Г. Куроша. Тезисы докладов. М.: Издательство МГУ, 2018, с. 116–117.

[179] Кравцова О. В., Шевелева И. В. О некоторых 3-примитивных проективных плоскостях // «Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения»: Материалы XV Междунар. конф., посвященной 100-летию со дня рождения профессора Н. М. Коробова, Тула: ТГПУ, 2018, с. 283–284.

[180] Кравцова О. В. О проблеме разрешимости полной группы коллинеаций конечной полуполевой плоскости // Всерос. конференция по математике

и механике, посвященная 140-летию Томского государственного университета и 70-летию механико-матем. факультета: сборник тезисов (Томск, 2-4 октября 2018 г.) – Томск, 2018, с. 25.

[181] Kravtsova O. V., Levchuk V. M. Problems on structure of finite quasifields and projective planes // International Conference «Group theory in Ankara», Middle East Technical University, 2019, p. 11–12.

[182] Podufalov N. D., Kravtsova O. V. On collineation groups of finite semifield projective planes // International Conference dedicated to the 90th anniversary of the Higher Algebra Department of the Faculty of Mechanics and Mathematics of Moscow State University: Abstracts of talks, 2019, p. 54.

[183] Кравцова О. В. Полуполевые плоскости, допускающие подгруппу автотопизмов, изоморфную Q_8 // Материалы конференции «Алгебра и математическая логика: теория и приложения», Казань: КФУ, 2019, с. 130.

[184] Кравцова О. В. О некоторых полуполях порядка 5^4 и 13^4 // Тезисы Международной конференции «Алгебра, теория чисел и математическое моделирование динамических систем», посвященной 70-летию А. Х. Журтова, Нальчик: Издательство КБГУ, 2019, с. 63.

[185] Кравцова О. В., Моисеенкова Т. В. Полуполевые проективные плоскости, допускающие подгруппу коллинеаций, изоморфную S_3 // «Алгебра, теория чисел и дискретная геометрия»: современные проблемы, приложения и проблемы истории: Материалы XVI Междунар. конф., посвященной 80-летию со дня рождения профессора Мишеля Деза.– Тула: ТГПУ, 2019, с. 260.

[186] Кравцова О.В. Силовская 2-подгруппа в группе автотопизмов полуполевой проективной плоскости четного порядка // XIII школа-конференция по теории групп, посвященная 85-летию В.А. Белоногова «Теория групп и ее приложения», 3–7 августа 2020 г. Тезисы докладов. – Екатеринбург, 2020, с. 61.

[187] Кравцова О. В. О примитивности и цикличности конечных полуполей // Конференция «Алгебра и ее приложения», посвященная 70-летию пермской алгебраической школы С. Н. Черникова, 12-16 октября 2020 г. Тезисы докладов. – Пермь, 2020, с. 32–33.

[188] Кравцова О. В., Левчук В. М., Подуфалов Н. Д. Problems on structure of finite quasifields and collineation groups of semifield projective translation

planes // Международная конференция «Мальцевские чтения», 16–20 ноября 2020 г. Тезисы докладов. – Новосибирск, 2020, с. 178.

[189] Кравцова О. В. 2-элементы в группе автотопизмов конечной полуполевой проективной плоскости. // Труды Математического центра имени Н.И. Лобачевского. Т. 60. Материалы Международной конференции по алгебре, анализу и геометрии 2021 – Казань: Изд-во Академии наук РТ, 2021. – Т. 60. – с. 85.

[190] Кравцова О. В. Метод регулярного множества построения конечных квазиполей // Алгебра, теория чисел, дискретная геометрия и многомасштабное моделирование: Современные проблемы, приложения и проблемы истории: Материалы XIX Международной конференции, посвященной 200-летию со дня рождения академика П. Л. Чебышева. – Тула: ТГПУ, 2021, с. 85.

[191] Кравцова О. В. Подгруппы Судзуки в группе автотопизмов полуполевой проективной плоскости // Международная конференция «Мальцевские чтения». 20–24 сентября 2021 г. Тезисы докладов. – Новосибирск, 2021, с. 98.

[192] Кравцова О. В., Моисеенкова Т. В., Шевелева И. В. Группы автотопизмов малых четных порядков полуполевых проективных плоскостей // Международная алгебраическая конференция, посвященная 90-летию со дня рождения А. И. Старостина, 4–9 октября 2021 г. Тезисы докладов. – Екатеринбург, 2021, с. 46.

[193] Кравцова О. В. Группа диэдра порядка 8 в группе автотопизмов полуполевой проективной плоскости нечетного порядка // Алгебра, теория чисел, дискретная геометрия и многомасштабное моделирование: современные проблемы, приложения и проблемы истории: Материалы XXI Международной конференции, посвященной году математики. – Тула: ТГПУ, 2022.