Федеральное государственное бюджетное учреждение науки

Институт математики им. С. Л. Соболева

Сибирского отделения Российской академии наук

На правах рукописи

Чуриков Дмитрий Владимирович

О ЗАМЫКАНИЯХ КОНЕЧНЫХ ГРУПП ПОДСТАНОВОК

01.01.06 — математическая логика, алгебра и теория чисел

Диссертация на соискание ученой степени кандидата физико-математических наук

Научный руководитель

доктор физико-математических наук, профессор

Васильев Андрей Викторович

Новосибирск – 2022

Оглавление

Введение

Постановка задачи и цели исследования. Теория групп подстановок — один из старейших разделов абстрактной алгебры, восходящий к классическим работам Э. Галуа и К. Жордана. Современный интерес к этой теории связан во многом с комбинаторикой и теорией сложности, поскольку группы подстановок естественно возникают как группы автоморфизмов комбинаторных структур, а вопрос об изоморфизме последних зачастую сводится к вопросу о поиске их полных групп автоморфизмов. Если P — k-арная комбинаторная структура множества Ω (можно считать, что P — разбиение множества Ω^k), то группа $\mathrm{Aut}(P)$ ее автоморфизмов, состоит из тех подстановок множества Ω, которые сохраняют классы разбиения P:

$$\mathrm{Aut}(P) = \{g \in \mathrm{Sym}(\Omega) : O^g = O, O \in P\}.$$

В настоящей диссертации, следуя Х. Виланду [49], мы рассматриваем комбинаторные структуры, инвариантные относительно заданных групп подстановок. Здесь естественно возникают понятия k-орбиты и k-замыкания группы подстановок, введенные Х. Виландом в 1969 году [49]. Если G — группа подстановок множества Ω, и k — натуральное число, то G покомпонетно действует на декартову степень Ω^k множества Ω:

$$(\alpha_1, \ldots, \alpha_k)^g = (\alpha_1^g, \ldots, \alpha_k^g) \text{ для всех } g \in G, (\alpha_1, \ldots, \alpha_k) \in \Omega^k.$$

Множество орбит этого действия, элементы которого называются *k-орбитами* группы G, обозначим через $\mathrm{Orb}_k(G)$. Легко понять, что k-орбиты группы G — это G-инвариантные отношения на множестве Ω^k.

Как показано выше, любой k-арной комбинаторной структуре соответствует некоторая группа подстановок, и наоборот, любая группа подстановок соответствует некоторой k-арной комбинаторной структуре. Это соответствие является соответствием Галуа и выражается следующими включениями

$$G \leq \mathrm{Aut}(\mathrm{Orb}_k(G)), \text{ и } P \leq \mathrm{Orb}_k(\mathrm{Aut}(P)). \tag{1}$$

Группа $G^{(k)} = \mathrm{Aut}(\mathrm{Orb}_k(G))$ называется *k-замыканием* группы G. Эквивалентно, k-замыкание группы G — это наибольшая по включению подгруппа в симметрической группе $\mathrm{Sym}(\Omega)$ с такими же k-орбитами, что и у G. Общая проблема, которая изучается в диссертации формулируется следующим образом.

Проблема k-замыкания. Для группы G подстановок конечного множества и целого положительного числа k найти k-замыкание $G^{(k)}$ группы G.

С теоретической точки зрения, k-замыкания группы подстановок можно рассматривать как ее последовательные аппроксимации, поскольку они связаны следующими включениями [49, теорема 5.8]:

$$G^{(1)} \geq G^{(2)} \geq G^{(3)} \geq \dots G^{(n)} = G^{(n+1)} = \dots = G,$$

где ряд очевидно стабилизируется не позднее шага $n = |\Omega|$.

Несложно понять, что k-замыкание k-транзитивной группы подстановок множества Ω — это вся симметрическая группа $\mathrm{Sym}(\Omega)$. Поэтому 1-замыкание есть прямое произведение симметрических групп, действующих на орбитах исходной группы, и в этом смысле имеет прозрачную структуру, но может оказаться очень далеким от исходной группы. Следующий вопрос, поднятый Х. Виландом в [49], гораздо нетривиальнее: какие классы групп замкнуты относительно k-замыкания при $k \geq 2$? Сам Х. Виланд показал, что классы конечных абелевых групп, p-групп и групп нечетного порядка замкнуты относительно k-замыкания при $k \geq 2$. Хотя 2-замыкание разрешимой группы не обязано быть разрешимым (достаточно взять разрешимую 2-транзитивную группу степени не меньше 5), совсем недавно в [34] было доказано, что класс разрешимых групп замкнут относительно k-замыкания при $k \geq 3$. В диссертации рассматривается вопрос о замкнутости класса нильпотентных групп относительно k-замыкания при $k \geq 2$.

Поскольку k-замыкание является оператором алгебраического замыкания, то естественно взглянуть на *k-замкнутые* группы, т. е. группы, совпадающие со своим k-замыканием. В диссертации мы изучаем условия k-замкнутости абелевых групп. В особенности нас интересует вопрос о критерии 2-замкнутости абелевых групп подстановок, который бы допускал эффективную алгоритмическую проверку.

Отметим, что недавно Д. Холт предложил подход, при котором понятие k-замкнутости переносится на абстрактные группы. В соответствии с ним абстрактная группа называется вполне k-замкнутой, если все ее точные подстановочные представления k-замкнуты [18]. В диссертации рассматриваются необходимые и достаточные условия вполне k-замкнутости конечных абелевых групп.

С точки зрения теории вычислительной сложности, наиболее важной является проблема 2-замыкания, которая эквивалентна проблеме нахождения группы автоморфизмов некоторого графа исходной группы. Действительно, пару $\Gamma = (\Omega, \mathrm{Orb}_2(G))$ можно рассматривать как цветной полный граф на множестве вершин Ω, где каждой 2-орбите группы G соответствует

свой цвет. Тогда группа $G^{(2)}$ является полной группой автоморфизмов этого графа. Граф Γ называется *цветной шуровой когерентной конфигурацией*, ассоциированной с G. Для краткости мы назовем эту конфигурацию *схемой* группы G и обозначим через $\mathrm{Inv}(G)$. В этих обозначениях соответствие Галуа из (1) записывается следующим образом

$$G \leq \mathrm{Aut}(\mathrm{Inv}(G)) \text{ и } \Gamma \leq \mathrm{Inv}(\mathrm{Aut}(\Gamma))$$

(в случае $k = 2$). Замкнутые относительно этого соответствия объекты — это в точности 2-замкнутые группы подстановок, и *шуровы когерентные конфигурации* — когерентные конфигурации множества Ω, удовлетворяющие условию $\Gamma = \Gamma^{(2)}$, где $\Gamma^{(2)} = \mathrm{Inv}(\mathrm{Aut}(\Gamma))$.

Указанное соответствие Галуа приводит к двум естественным задачам: задаче нахождения 2-орбит группы автоморфизмов произвольной цветной когерентной конфигурации, т.е. по Γ найти $\Gamma^{(2)}$, и проблеме 2-замыкания, т.е. по G найти $G^{(2)}$. Хорошо известно, что первая из этих задач полиномиально эквивалентна общей проблеме изоморфизма графов, а вторая, очевидно, полиномиально к ней сводится. В частности, по модулю недавнего прорывного результата Л. Бабаи [10] это означает, что обе проблемы могут быть решены за квазиполиномиальное от размера множества Ω время. В то же время семейство групп, для которых известны полиномиальные алгоритмы нахождения 2-замыкания, достаточно ограничено. В диссертации изучается алгоритмическая сложность вычисления 2-замыкания $\frac{3}{2}$-транзитивной группы подстановок и проверки изоморфизма цветных шуровых $\frac{3}{2}$-однородных когерентных конфигураций (точные определения см. ниже).

Среди шуровых $\frac{3}{2}$-однородных когерентных конфигураций отдельный интерес представляют так называемые циклотомические схемы над конечными почти-полями. Если $\mathbb{K}$ — конечное почти-поле, и K — собственная подгруппа мультипликативной группы $\mathbb{K}^\times$, то группа $G = \mathbb{K}^+ \rtimes K$ — $\frac{3}{2}$-транзитивная группа Фробениуса, и когерентная конфигурация $\mathrm{Inv}(G)$ называется циклотомической схемой над почти-полем $\mathbb{K}$ с базисной группой K. Впервые такие схемы изучались в работе Дж. Багеряна, И. Н. Пономаренко и А. Рахнама Барги [12]. В диссертации изучается высказанная в этой статье гипотеза о том, что за конечным числом исключений группы автоморфизмов циклотомических схем над почти-полями, т.е. 2-замыкания соответствующих групп Фробениуса, содержатся в одномерных полулинейных аффинных группах.

Степень разработанности и актуальность темы исследования. Основы теории k-замыканий были заложены Х. Виландом в 1969 году [49]. К теоретическим результатам про k-замыкания относятся теорема Л. А. Калужнина и М. Х. Клина 1976 года про k-замыкания импримитивных сплетений групп подстановок [4], результаты М. Либека, Ш. Прегер и Я. Са-

ксла про цоколи k-замыканий примитивных групп [31,40] и недавний результат Э. А. О'Брайена, А. В. Васильева, Е. П. Вдовина и И. Н. Пономаренко о разрешимости 3-замыкания конечной разрешимой группы [34]. Алгоритмическая постановка проблемы 2-замыкания возникла впервые в работе [42] И. Н. Пономаренко 1994 года, в которой было доказано существование полиномиального от степени группы алгоритма, решающего эту проблему в классе нильпотентных групп. Позднее аналогичные результаты были получены им для групп нечетного порядка [22] в соавторстве с С. А. Евдокимовым и для сверхразрешимых групп [43] в соавторстве с А. В. Васильевым.

Х. Виланд заметил, что класс конечных абелевых групп замкнут относительно k-замыкания при $k \geq 2$. А. З. Зеликовский изучал проблему графичности группы подстановок и в своей статье 1989 года предложил, как оказалось, ошибочный критерий 2-замкнутости абелевых групп [3]. Ошибку недавно отметили М. Грех и А. Киселевич [25], которые тоже изучали проблему графичности и в результате серии работ [25–27] установили критерий 2-замкнутости конечных абелевых групп в терминах теории графов, который, к сожалению, сложно проверить алгоритмически.

Понятие вполне k-замкнутости было недавно предложено Д. Холтом в [18]. Первый результат по этой тематике получен А. Абдоллахи и М. Арезумандом. Они описали все вполне 2-замкнутые конечные нильпотентные группы [7]. Позже эти авторы вместе с Г. Трэйси получили аналогичный результат для конечных разрешимых групп [8]. Вполне 2-замкнутые конечные группы с тривиальной подгруппой Фиттинга были недавно классифицированы М. Арезумандом, М. Иранманешем, Ш. Э. Прегер и Г. Трэйси [9].

$\frac{3}{2}$-Транзитивные группы были введены Х. Виландом в монографии 1964 года [48]. Напомним, что группа G называется $\frac{3}{2}$-*транзитивной*, если она транзитивна и орбиты стабилизатора G_α точки α на множестве $\Omega \setminus \{\alpha\}$ имеют одинаковую неединичную длину. $\frac{3}{2}$-Транзитивные группы естественно возникают как нормальные подгруппы дважды транзитивных групп. Примерами таких групп являются группы Фробениуса и группы автоморфизмов циклотомических схем над конечными полями [15, 19] и почти-полями [12, 51]. Основы теории $\frac{3}{2}$-транзитивных групп были заложены Х. Виландом [48], который показал, что каждая $\frac{3}{2}$-транзитивная группа примитивна или является группой Фробениуса. Далее Пассман классифицировал разрешимые группы из этого класса [36, 38, 39]. Почти простые $\frac{3}{2}$-транзитивные группы были описаны в [13], а окончательно классификация $\frac{3}{2}$-транзитивных групп была завершена совсем недавно в [24, 30].

Циклотомические схемы были введены Ф. Дельсартом в связи с проблемами теории кодирования и изначально определены над конечными полями [19]. Из основного результа-

та [33] следует, что группы автоморфизмов таких схем содержатся в одномерных полулинейных аффинных группах. Дж. Багерян, И. Н. Пономаренко и А. Рахнама Барги предложили рассматривать циклотомические схемы над конечными почти-полями и указали некоторое достаточное условие вложения группы автоморфизмов такой схемы в одномерную полулинейную аффинную группу. [12].

Теория когерентных конфигураций, методы которой используются при изучении k-замыканий, идейно восходит к методу колец Шура, предложенному И. Шуром и разработанному Х. Виландом в той же монографии 1964 года [48]. В отечественной науке конструкции, близкие к когерентным конфигурациям, были предложены Б. Ю. Вейсфейлером и А. А. Леманом в статье 1968 года [1]. Современное определение когерентной конфигурации было сформулировано в классической работе Д. Хигмана 1970 года [28]. Текущее состояние теории когерентных конфигураций отражено в монографии Г. Чена и И. Н. Пономаренко [17].

Основные результаты диссертации

1. Показано, что k-замыкание конечной нильпотентной группы подстановок есть прямое произведение k-замыканий ее силовских подгрупп при любом $k \geq 2$ (теорема 1).

2. Найден допускающий эффективную алгоритмическую проверку индуктивный критерий 2-замкнутости конечных абелевых групп с циклическими транзитивными составляющими (теорема 4).

3. Получен критерий вполне замкнутости конечных абелевых групп. Доказано, что нетривиальная конечная абелева группа, раскладывающаяся в произведение n инвариантных множителей, вполне $(n+1)$-замкнута, но не вполне n-замкнута (теорема 6).

4. Найдены полиномиальные алгоритмы поиска 2-замыканий $\frac{3}{2}$-транзитивных групп подстановок и решения проблемы изоморфизма цветных шуровых $\frac{3}{2}$-однородных когерентных конфигураций (теоремы 7 и 8).

Первый результат получен автором лично [54]. Второй результат получен в неразделимом соавторстве с И. Н. Пономаренко [55], третий — с Ш. Э. Прегер [53], четвертый — с А. В. Васильевым [52].

Научная новизна и значимость работы. Работа носит теоретический характер. Все полученные результаты являются новыми. Результаты работы могут быть использованы в дальнейших исследованиях по теории групп, алгебраической комбинаторике и теории сложности, а также могут быть включены в спецкурсы для студентов и аспирантов.

Методы исследования. В диссертации используются классические методы теории групп [5] и особенно теории групп подстановок [6, 20, 48] и их замыканий [49]. Изучение

$\frac{3}{2}$-транзитивных групп базируется на классификации $\frac{3}{2}$-транзитивных групп подстановок и $\frac{1}{2}$-транзитивных линейных групп [30], которая, в свою очередь, опирается на классификацию конечных простых групп.

В диссертации существенно используются методы теории когерентных конфигураций и ассоциативных схем [11, 17, 21], а также теория конечных почти-полей [46, 50] и циклотомических схем над ними [12].

При решении проблем вычислительной сложности используется хорошо известный инструментарий полиномиальных алгоритмов для групп подстановок [45]. Основную роль же играет алгоритм Вейсфейлера-Лемана [1, 47] и различные его модификации [41], в том числе разработанные автором диссертации.

Апробация результатов. Результаты диссертации докладывались на Международной конференции «Мальцевские чтения» (Новосибирск, 2018, 2020), Международной конференции «Symmetry vs. Regularity» (Пльзень, Чехия, 2018), Международной школе-конференции «Алгоритмические вопросы теории групп и смежных областей» (Новосибирск, 2016, 2018), Международной конференции «Graphs and Groups, Spectra and Symmetries» (Новосибирск, 2016), Международной конференции «Workshop on Group Theory and Algebraic Combinatorics» (Новосибирск, 2017), Международной конференции «The 4th Workshop on Algebraic Graph Theory and its Applications» (Новосибирск, 2021), Международной конференции «Graphs and Groups, Geometries and GAP» (Рогла, Словения, 2021), Конференции международных математических центров мирового уровня (Сочи, 2021), а также обсуждались на семинарах «Алгебра и логика» и «Теория групп» Института математики СО РАН и Новосибирского государственного университета.

Публикации. Результаты работы опубликованы в [51–60]. Основные результаты диссертации опубликованы в [52–55] в изданиях, входящих в перечень ВАК рецензируемых научных журналов, в которых должны быть опубликованы основные результаты диссертаций на соискание ученых степеней доктора и кандидата наук.

Структура и объем диссертации. Диссертация состоит из введения, 5 глав, приложения, заключения и списка литературы. Она изложена на 59 страницах и включает 3 таблицы. Главы диссертации подразделяются на параграфы. Результаты диссертации сформулированы в виде теорем и имеют сквозную нумерацию. Вспомогательные леммы имеют тройную нумерацию: номер главы, номер параграфа в главе и номер утверждения в текущем параграфе. Формулы имеют двойную нумерацию: номер главы и номер формулы внутри главы. Список литературы содержит 60 наименований. Работы автора по теме диссертации приведены отдельным списком.

Основное содержание диссертации

Во **введении** приводятся постановка и описание задачи, аргументируется актуальность темы исследования и описывается степень ее проработанности. Представлены основные результаты диссертации и методы, применяемые в исследовании. Также отражается теоретическая значимость и новизна полученных результатов. В конце размещены данные об апробации и публикации полученных результатов, а также краткое содержание диссертации.

В **первой главе** размещены основные определения и вспомогательные утверждения по k-замыканиям групп подстановок, $\frac{3}{2}$-транзитивным группам, когерентным конфигурациям, циклотомическим схемам над конечными почти-полями и алгоритму Вейсфейлера-Лемана. Отдельно отметим следующее полезное утверждение о связи k-замыкания и прямого произведения групп, которое, насколько известно автору, ранее нигде не было доказано явно.

Лемма 1.1.7. *Если $G_i \leq \mathrm{Sym}(\Omega_i)$, $i = 1, 2$, и группа $G_1 \times G_2$ действует на декартовом произведении $\Omega_1 \times \Omega_2$, то для всех целых $k \geq 2$ выполняется равенство $(G_1 \times G_2)^{(k)} = G_1^{(k)} \times G_2^{(k)}$.*

Во **второй главе** изучаются k-замыкания конечных нильпотентных групп подстановок. Известно, что каждая конечная нильпотентная группа имеет вид прямого произведения своих силовских подгрупп [5, Теорема 17.1.4]. После нескольких вспомогательных утверждений в первом параграфе, во втором параграфе устанавливается, что оператор k-замыкания сохраняет это прямое произведение.

Теорема 1. *Если G — конечная нильпотентная группа подстановок и k — целое число, большее 1, то $G^{(k)}$ — прямое произведение k-замыканий силовских подгрупп группы G. В частности, $G^{(k)}$ нильпотентна.*

Результаты главы получены автором лично и опубликованы в [54].

Третья глава посвящена 2-замыканиям конечных абелевых групп. В ней предложен алгоритм CYCLOSURE проверки 2-замкнутости конечных абелевых групп с циклическими транзитивными составляющими. За вспомогательными утверждениями в параграфе 1 следуют доказательства основных для построения алгоритма теорем 2 и 3 в параграфах 2 и 3 соответственно,

Теорема 2. *Пусть G — квазирегулярная группа подстановок и $Z = \mathrm{Zel}(G)$. Тогда G 2-замкнута в том и только в том случае, если $Z \leq G$ и $G^{\mathrm{Orb}(Z)}$ 2-замкнута.*

В теореме 2 через $\mathrm{Zel}(G)$ обозначается группа

$$\mathrm{Zel}(G) = \prod_{\Delta} \bigcap_{\Delta' \neq \Delta} (G_{\Delta'})^{\Delta},$$

где Δ и Δ' пробегают множество орбит группы G, и $(G_{\Delta'})^{\Delta}$ — это ограничение поточечного стабилизатора множества Δ' на множество Δ. Если $\mathrm{Zel}(G) \neq 1$, то теорема 2 является критерием 2-замкнутости квазирегулярных групп. При изучении абелевых групп со свойством $\mathrm{Zel}(G) = 1$ оказалась полезной концепция несущественной орбиты. Орбита Δ группы $G \leq \mathrm{Sym}(\Omega)$ называется несущественной, если группа G 2-замкнута тогда и только тогда, когда группа $G^{\Omega\setminus\Delta}$ 2-замкнута.

Теорема 3. *Пусть p — простое число, G — интранзитивная p-группа с циклическими транзитивными составляющими и $\mathrm{Zel}(G) = 1$. Тогда каждая орбита группы G является несущественной.*

В четвертом параграфе с помощью теорем 1, 2 и 3 доказывается теорема 4.

Теорема 4. *Алгоритм* CYCLOSURE *корректен и осуществляет проверку 2-замкнутости абелевых групп с циклическими транзитивными составляющими.*

В **четвертой главе** рассматриваются вполне k-замкнутые конечные абелевы группы. Известно, что любая конечно порожденная абелева группа изоморфна прямому произведению так называемых инвариантных множителей. В первом параграфе размещены вспомогательные утверждения, с помощью которых во втором параграфе доказывается следующая

Теорема 5. *Пусть A — нетривиальная конечная абелева p-группа и n — количество инвариантных множителей группы A. Тогда группа A вполне $(n+1)$-замкнута, но не вполне n-замкнута.*

В третьем параграфе с помощью теоремы 1 теорема 5 обобщается для всех конечных абелевых групп.

Теорема 6. *Пусть A — нетривиальная конечная абелева группа и n — количество инвариантных множителей группы A. Тогда A вполне $(n+1)$-замкнута, но не вполне n-замкнута.*

В **пятой главе** изучаются $\frac{3}{2}$-транзитивные группы подстановок и возникающие из них когерентные конфигурации. Группа подстановок множества Ω является $\frac{3}{2}$-транзитивной, если она транзитивна и орбиты стабилизатора точки α на множестве $\Omega \setminus \{\alpha\}$ одинаковой неединичной длины. В первом параграфе строится полиномиальный алгоритм нахождения 2-замыкания $\frac{3}{2}$-транзитивной группы подстановок.

Теорема 7. *Проблема 2-замыкания для $\frac{3}{2}$-транзитивной группы подстановок степени n может быть решена за время, полиномиальное от n.*

Напомним, что если G — $\frac{3}{2}$-транзитивная группа множества Ω, то пара $(\Omega, \mathrm{Orb}_2(G))$ называется цветной шуровой $\frac{3}{2}$-однородной когерентной конфигурацией. Теорема 7 позволяет

получить полиномиальное решение проблемы изоморфизма таких конфигураций.

Теорема 8. *Проблема изоморфизма цветных шуровых $\frac{3}{2}$-однородных когерентных конфигураций на n точках может быть решена за время, полиномиальное от n.*

В третьем параграфе классифицируются группы автоморфизмов циклотомических схем над конечными почти-полями. В частности, подтверждается гипотеза Багеряна-Пономаренко-Рахнама Барги о том, что за конечным числом исключений такие группы автоморфизмов содержатся в одномерных аффинных полулинйеных группах. Отметим, что доказательство этого результата использует в том числе и компьютерные вычисления [14, 44].

Теорема 9. *Пусть $\mathbb{K}$ — конечное почти-поле, K — собственная подгруппа группы $\mathbb{K}^\times$ и $\mathcal{C} = \mathrm{Cyc}(\mathbb{K}, K)$ — циклотомическая схема над почти-полем $\mathbb{K}$ с базисной группой K. Тогда выполняется одно из следующих утверждений.*

1. *$\mathbb{K}$ — почти-поле Диксона и $\mathrm{Aut}(\mathcal{C}) \leq \mathrm{A\Gamma L}(1, \mathbb{F})$, где $\mathbb{F}$ — поле, ассоциированное с $\mathbb{K}$.*

2. *$\mathbb{K}$ — почти-поле Диксона порядка 7^2, $K = \langle a, b\rangle \cong 3 \times Q_8$ и $\mathrm{Aut}(\mathcal{C}) = \mathbb{K}^+ \rtimes H$, где $H = \langle K, c\rangle \cong 3 \times \mathrm{SL}(2,3)$ и действие a, b и c на $\mathbb{K}^+$ представлено матрицами*

$$\begin{pmatrix} 2 & 2 \\ 1 & -2 \end{pmatrix}, \quad \begin{pmatrix} 0 & -2 \\ -1 & 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

3. *$\mathbb{K}$ — почти-поле Цассенхауза, K — подгруппа группы M, где M — максимальная разрешимая подгруппа группы $\mathbb{K}^\times$, и $\mathrm{Aut}(\mathcal{C})$ — подгруппа группы $\mathbb{K}^+ \rtimes H$, где $K \leq M \leq H$. Группы $\mathbb{K}^+$, M, H и порождающие групп M и H приведены в таблице 2 в приложении.*

4. *$\mathbb{K}$ — почти-поле Цассенхауза порядка 29^2 или 59^2, $K \cong \mathrm{SL}(2,5)$ и $\mathrm{Aut}(\mathcal{C}) = \mathbb{K}^+ \rtimes H$, где $H = \mathrm{SL}(2,5) \rtimes 2$ или $H = \mathrm{SL}(2,5)$ соответственно. Группы $\mathbb{K}^+$, K, H и порождающие групп K и H приведены в таблице 3 в приложении.*

В частности, если базисная группа K разрешима, то группа $\mathrm{Aut}(\mathcal{C})$ тоже разрешима.

Результаты главы получены автором в неразделимом соавторстве с А. В. Васильевым и опубликованы в [51, 52].

Благодарности

Автор глубоко признателен своему научному руководителю Андрею Викторовичу Васильеву за постановку интересных исследовательских задач и всестороннюю помощь. Автор благодарен Илье Николаевичу Пономаренко и Шерил Элизабет Прегер за научное сотрудничество и консультации. Также автор признателен всем сотрудниками лаборатории алгебры ИМ СО РАН и кафедры алгебры и математической логики НГУ за полученные знания и творческую атмосферу.

1. Предварительные сведения

§ 1.1. k-Замыкания групп подстановок

Пусть G — группа подстановок конечного непустого множества Ω и k — положительное целое число. Обозначим через $\mathrm{Orb}_k(G)$ множество орбит покомпонентного действия группы G на декартовой степени Ω^k (для краткости, $\mathrm{Orb}_1(G) = \mathrm{Orb}(G)$). Элементы множества $\mathrm{Orb}_k(G)$ называются k-орбитами группы G и образуют разбиение множества Ω^k. Две подгруппы G и H из $\mathrm{Sym}(\Omega)$ называются k-эквивалентными, если $\mathrm{Orb}_k(G) = \mathrm{Orb}_k(H)$. Наибольшая из k-эквивалентных G подгрупп группы $\mathrm{Sym}(\Omega)$ называется ее k-замыканием и обозначается через $G^{(k)}$. Эквивалентно, k-замыканием $G^{(k)}$ группы G называется группа автоморфизмов ее k-орбит [49, опр. 5.3], т.е.

$$G^{(k)} = \{g \in \mathrm{Sym}(\Omega) \mid O^g = O \ \forall O \in \mathrm{Orb}_k(G)\}.$$

В частности, $G \leq G^{(k)}$. Группа G называется k-замкнутой, если $G = G^{(k)}$.

Из определения k-замыкания следует простой критерий принадлежности подстановки к k-замыканию.

Лемма 1.1.1. [49, теорема 5.6] *Если $G \leq \mathrm{Sym}(\Omega)$, $k \geq 1$, и $x \in \mathrm{Sym}(\Omega)$, то $x \in G^{(k)}$ тогда и только тогда, когда для любых $\alpha_1, \ldots, \alpha_k \in \Omega$ существует элемент $g \in G$ такой, что $\alpha_i^x = \alpha_i^g$, $i = 1, \ldots, k$.*

Следующая лемма устанавливает связь между $(k+1)$-орбитами транзитивной группы и k-орбитами стабилизатора точки.

Лемма 1.1.2. [49, упр. 2.4] *Пусть $G \leq \mathrm{Sym}(\Omega)$ — транзитивная группа и k — положительное целое число. Тогда существует биекция между $(k+1)$-орбитами группы G и k-орбитами стабилизатора G_α произвольной точки $\alpha \in \Omega$: $(k+1)$-орбите O группы G соответствует орбита $O_\alpha = \{(\alpha_1, \ldots, \alpha_k) \in \Omega^k \mid (\alpha_1, \ldots, \alpha_k, \alpha) \in \Omega^{k+1}\}$ группы G_α. Более того, для любой $(k+1)$-орбиты O и для любого α выполняется равенство $|O| = |\Omega||O_\alpha|$.*

Отметим здесь следующий базисный факт, из которого, в частности, вытекает транзитивность (примитивность) k-замыкания транзитивной (соответственно примитивной) группы.

Лемма 1.1.3. [49, теорема 5.7] *Если $H \leq G$, то $H^{(k)} \leq G^{(k)}$.*

k-Замыкания группы при различных k можно понимать как некоторые приближения исходной группы. Следующая лемма иллюстрирует, что чем больше k, тем «ближе» k-замыкание к исходной группе.

Лемма 1.1.4. [49, теорема 5.8] *Если $G \leq \mathrm{Sym}(\Omega)$, то*

$$\mathrm{Sym}(\Omega) \geq G^{(1)} \geq \ldots \geq G^{(k)} \geq G^{(k+1)} \geq \ldots \geq G.$$

Отметим, что для конечных групп эта последовательность обязательно стабилизируется на группе G. Следующая лемма дает общую оценку на момент этой стабилизации.

Лемма 1.1.5. [49, теорема 5.12] *Пусть $G \leq \mathrm{Sym}(\Omega)$, $k \geq 1$ — целое число и $\alpha_1, \ldots, \alpha_k \in \Omega$ такие что $G_{\alpha_1 \ldots \alpha_k} = 1$. Тогда $G^{(k+1)} = G$.*

Напомним, что прямое произведение $G_1 \times G_2$ групп подстановок $G_i \leq \mathrm{Sym}(\Omega_i), i = 1, 2$ действует как на множестве $\Omega_1 \times \Omega_2$ по правилу $(\alpha_1, \alpha_2)^{(g_1, g_2)} = (\alpha_1^{g_1}, \alpha_2^{g_2})$, так и на множестве $\Omega_1 \sqcup \Omega_2$ по правилу

$$\alpha^{(g_1,g_2)} = \begin{cases} \alpha^{g_1}, \text{ если } \alpha \in \Omega_1, \\ \alpha^{g_2}, \text{ если } \alpha \in \Omega_2. \end{cases}$$

Следующие две леммы показывают согласованность k-замыкания и прямого произведения групп подстановок. Частные случаи этих лемм можно найти в [16, 22].

Лемма 1.1.6. *Если $G_i \leq \mathrm{Sym}(\Omega_i)$, $i = 1, 2$, и группа $G_1 \times G_2$ действует на дизъюнктном объединении $\Omega_1 \cup \Omega_2$, то для всех целых $k \geq 1$ выполняется равенство*

$$(G_1 \times G_2)^{(k)} = G_1^{(k)} \times G_2^{(k)}.$$

Доказательство. $\boxed{\geq}$ Достаточно доказать, что $G_1^{(k)} \times 1$ и $1 \times G_2^{(k)}$ содержатся в $(G_1 \times G_2)^{(k)}$. Зафиксируем набор элементов $\alpha_1, \ldots, \alpha_k \in \Omega_1 \cup \Omega_2$ и его поднабор $\alpha_{j_1}, \ldots, \alpha_{j_l}$, состоящий из элементов, лежащих в Ω_1. Если $(g, 1) \in G_1^{(k)} \times 1$, то из леммы 1.1.4 следует, что $g \in G_1^{(l)}$, и по лемме 1.1.1 существует $h \in G_1$ такой, что $\alpha_{j_i}^g = \alpha_{j_i}^h$ для всех $i = 1, \ldots, l$.

Теперь рассмотрим элемент $(h, 1) \in G_1 \times G_2$. По построению для всех $i = 1, \ldots, k$

$$\alpha_i^{(h,1)} = \begin{cases} \alpha_i^h = \alpha_i^g = \alpha_i^{(g,1)} \text{ если } \alpha_i \in \Omega_1, \\ \alpha_i = \alpha_i^{(g,1)} \text{ если } \alpha_i \in \Omega_2. \end{cases}$$

Тогда из леммы 1.1.1 следует, что $(g, 1) \in (G_1 \times G_2)^{(k)}$. Так что, $G_1^{(k)} \times 1 \leq (G_1 \times G_2)^{(k)}$. Включение $1 \times G_2^{(k)} \leq (G_1 \times G_2)^{(k)}$ доказывается аналогично.

$\boxed{\leq}$ Пусть $x \in (G_1 \times G_2)^{(k)}$, тогда $\Omega_i^x = \Omega_i$. Для $i = 1, 2$ положим $x_i = x^{\Omega_i}$. Тогда подстановка x совпадает с подстановкой $(x_1, x_2) \in \mathrm{Sym}(\Omega_1 \cup \Omega_2)$, действующей на Ω_i как x_i, $i = 1, 2$. Покажем, что $x_i \in G_i^{(k)}$ для $i = 1, 2$. Пусть $\alpha_1, \ldots, \alpha_k \in \Omega_i$. По лемме 1.1.1 существует $(h_1, h_2) \in G_1 \times G_2$ такой, что $\alpha_j^x = \alpha_j^{(h_1,h_2)}$, $j = 1, \ldots, k$. В частности, $\alpha_j^{x_i} = \alpha_j^{h_i}$ ввиду $\alpha_j^{x_i} = \alpha_j^x = \alpha_j^{(h_1,h_2)} = \alpha_j^{h_i}$. Тогда из леммы 1.1.1 следует, что $x_i \in G_i^{(k)}$, и тем самым $x \in G_1^{(k)} \times G_2^{(k)}$. □

Лемма 1.1.7. *Если $G_i \leq \mathrm{Sym}(\Omega_i)$, $i = 1, 2$, и группа $G_1 \times G_2$ действует на декартовом произведении $\Omega_1 \times \Omega_2$, то для всех целых $k \geq 2$ выполняется равенство*

$$(G_1 \times G_2)^{(k)} = G_1^{(k)} \times G_2^{(k)}.$$

Доказательство. $\boxed{\geq}$ Достаточно доказать, что $G_1^{(k)} \times 1$ и $1 \times G_2^{(k)}$ содержатся в $(G_1 \times G_2)^{(k)}$. Пусть $(g, 1) \in G_1^{(k)} \times G_2^{(k)}$ и $(\alpha_1, \beta_1), \ldots, (\alpha_k, \beta_k) \in \Omega_1 \times \Omega_2$. Поскольку $g \in G_1^{(k)}$, по лемме 1.1.1 существует $h \in G_1$ такой, что $\alpha_j^g = \alpha_j^h$, $j = 1, \ldots, k$. Это значит, что для элемента $(h, 1) \in G_1 \times G_2$ имеет место равенство $(\alpha_j, \beta_j)^{(g,1)} = (\alpha_j^g, \beta_j) = (\alpha_j^h, \beta_j) = (\alpha_j, \beta_j)^{(h,1)}$, и из леммы 1.1.1 следует, что $(g, 1) \in (G_1 \times G_2)^{(k)}$. Так что, $G_1^{(k)} \times 1 \leq (G_1 \times G_2)^{(k)}$. Включение $1 \times G_2^{(k)} \leq (G_1 \times G_2)^{(k)}$ доказывается аналогично.

$\boxed{\leq}$ Сначала мы изучим структуру элементов из $(G_1 \times G_2)^{(2)}$. Положим $\Sigma_1 = \{\{\alpha_1\} \times \Omega_2 \mid \alpha_1 \in \Omega_1\}$, $\Sigma_2 = \{\Omega_1 \times \{\alpha_2\} \mid \alpha_2 \in \Omega_2\}$. Очевидно, что группа $G_1 \times G_2$ действует на множествах Σ_1 и Σ_2. Покажем, что группа $(G_1 \times G_2)^{(2)}$ тоже действует на этих множествах, т.е. для всех $x \in (G_1 \times G_2)^{(2)}$ и всех $\Delta \in \Sigma_i$, $i = 1, 2$, либо $\Delta^x = \Delta$, либо $\Delta^x \cap \Delta = \varnothing$.

Если Δ — одноэлементное множество, то утверждение очевидно. Предположим, что существуют два различных элемента $u, v \in \Delta$ таких, что $u^x \in \Delta$, и $v^x \notin \Delta$. По лемме 1.1.1 существует $h \in G_1 \times G_2$ такой, что $(u^x, v^x) = (u^h, v^h)$. Но это означало бы, что $u^h \in \Delta$ и $v^h \notin \Delta$, что невозможно, поскольку группа $G_1 \times G_2$ действует на множестве Σ_i.

Итак, группа $(G_1 \times G_2)^{(2)}$ действует на множествах Σ_1 и Σ_2, а значит и на множестве $\Sigma_1 \times \Sigma_2$. Биекция

$$\rho : \Omega_1 \times \Omega_2 \to \Sigma_1 \times \Sigma_2, \quad (\alpha_1, \alpha_2) \mapsto (\{\alpha_1\} \times \Omega_2, \Omega_1 \times \{\alpha_2\})$$

задает подстановочный изоморфизм между группой $(G_1 \times G_2)^{(2)}$ и некоторой подгруппой группы $\mathrm{Sym}(\Sigma_1 \times \Sigma_2)$. Для $i = 1, 2$ определим действие подстановки x_i на $\alpha \in \Omega_i$ следующим образом:

$$\alpha^{x_1} = \beta \Leftrightarrow (\{\alpha\} \times \Omega_2)^x = \{\beta\} \times \Omega_2,$$
$$\alpha^{x_2} = \beta \Leftrightarrow (\Omega_1 \times \{\alpha\})^x = \Omega_1 \times \{\beta\}.$$

Тогда образ подстановки x при определенном выше подстановочном изоморфизме совпадает с подстановкой $(x_1, x_2) \in \mathrm{Sym}(\Omega_1 \times \Omega_2)$.

Вернемся к доказательству леммы. Пусть $x \in (G_1 \times G_2)^{(k)}$. Из предыдущих наблюдений и леммы 1.1.4 следует, что $x = (x_1, x_2)$, $x_i \in \mathrm{Sym}(\Omega_i)$, $i = 1, 2$. Покажем, что $x_i \in G_i^{(k)}$. Пусть $\alpha_1^i, \ldots, \alpha_k^i \in \Omega_i$. Из леммы 1.1.1 следует, что для $x \in (G_1 \times G_2)^{(k)}$ и $(\alpha_1^1, \alpha_1^2), \ldots, (\alpha_k^1, \alpha_k^2) \in \Omega_1 \times \Omega_2$ существует $(h_1, h_2) \in G_1 \times G_2$ такой, что $(\alpha_j^1, \alpha_j^2)^x = (\alpha_j^1, \alpha_j^2)^{(h_1,h_2)}$, $j = 1, \ldots, k$. В частности, $(\alpha_j^i)^{x_i} = (\alpha_j^i)^{h_i}$, $j = 1, \ldots, k$, поэтому лемма 1.1.1 влечет $x_i \in G_i^{(k)}$, и потому $x \in G_1^{(k)} \times G_2^{(k)}$. □

Транзитивная группа подстановок G называется группой Фробениуса, если стабилизатор одной точки нетривиален, а стабилизатор двух различных точек тривиален.

Лемма 1.1.8. *Пусть $G \leq \mathrm{Sym}(\Omega)$ и $G^{(2)}$ — группа Фробениуса. Тогда G 2-замкнута.*

Доказательство. Пусть $\Theta \in \mathrm{Orb}(G_\alpha)$. Из леммы 1.1.2 следует, что $\Theta \in \mathrm{Orb}((G^{(2)})_\alpha)$, поэтому

$$|\Theta| = |G_\alpha^{(2)} : G_{\alpha\beta}^{(2)}| = |G_\alpha : G_{\alpha\beta}|.$$

Поскольку $G^{(2)}$ — группа Фробениуса, $G_{\alpha\beta}^{(2)} = G_{\alpha\beta} = 1$, и $|G_\alpha^{(2)}| = |G_\alpha|$, поэтому для $O_\alpha \in \mathrm{Orb}(G) = \mathrm{Orb}(G^{(2)})$ выполнено равенство

$$|O_\alpha| = |G^{(2)} : G_\alpha^{(2)}| = |G : G_\alpha|,$$

которое влечет равенство $|G| = |G^{(2)}|$. Учитывая, что $G \leq G^{(2)}$, получаем $G = G^{(2)}$. □

§ 1.2. $\frac{3}{2}$-Транзитивные группы подстановок

Напомним, что группа подстановок G множества Ω называется $\frac{1}{2}$-транзитивной, если все орбиты группы одинаковой длины, и $\frac{3}{2}$-транзитивной, если группа транзитивна и стабилизатор точки $\alpha \in \Omega$ $\frac{1}{2}$-транзитивен на множестве $\Omega \setminus \{\alpha\}$.

Начнем с классического результата Виланда, дающего описание импримитивных $\frac{3}{2}$-транзитивных групп.

Лемма 1.2.1. [48, теорема 10.4] *$\frac{3}{2}$-Транзитивная группа подстановок примитивна или является группой Фробениуса.*

Недавно в [30] была завершена классификация всех $\frac{3}{2}$-транзитивных групп подстановок и $\frac{1}{2}$-транзитивных линейных групп.

Лемма 1.2.2. [30, Следствие 2] *Пусть* $H \leq \mathrm{GL}(V) = \mathrm{GL}(d,p)$ *и* H *—* $\frac{1}{2}$*-транзитивная группа на* $V^\sharp = V \setminus \{\bar{0}\}$*, тогда справедливо одно из следующих утверждений.*

1. H *транзитивна на* $V^\sharp$*.*
2. $H \leq \Gamma\mathrm{L}(1, p^d)$*.*
3. H *— дополнение Фробениуса, действующее полурегулярно на* $V^\sharp$*.*
4. $H = \mathrm{S}_0(p^{d/2})$*, где* p *нечетно.*
5. H *разрешима и* $p^d = 3^2, 5^2, 7^2, 11^2, 17^2$ *или* 3^4*.*
6. $\mathrm{SL}(2,5) \lhd H \leq \Gamma\mathrm{L}(2, p^{d/2})$*, где* $p^{d/2} = 9, 11, 19, 29$ *или* 169*.*

В лемме 1.2.2 через $S_0(p^{d/2})$ обозначена группа мономиальных матриц размерности 2 с определителем ± 1:

$$\mathrm{S}_0(p^{d/2}) = \langle \begin{pmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle,$$

а θ — порождающий элемент мультипликативной группы $\mathbb{F}^\times_{p^{d/2}}$.

Лемма 1.2.3. [30, Следствие 3] *Пусть* G *—* $\frac{3}{2}$*-транзитивная группа подстановок степени* n*. Тогда справедливо одно из следующих утверждений.*

1. G *дважды транзитивна.*
2. G *— группа Фробениуса.*
3. G *— почти простая группа,* $n = \frac{1}{2}q(q-1)$*,* $q = 2^f \geq 8$*,* f *простое, и либо*
   - *а)* $G = \mathrm{PSL}(2,q)$*, и размер нетривиальной орбиты стабилизатора равен* $q+1$*, либо*
   - *б)* $G = \mathrm{P\Gamma L}(2,q)$*, и размер нетривиальной орбиты стабилизатора равен* $f(q+1)$*.*
4. G *— аффинная группа,* $n = p^d$*,* p *простое, и*
   - *а) либо* $G < \mathrm{A\Gamma L}(1, p^d)$*,*
   - *б) либо* $G = \mathrm{AS}_0(p^d)$*, где* p *нечетно, а* d *четно.*

В лемме 1.2.3 фигурирует аффинная группа подстановок $\mathrm{AS}_0(p^d) = \mathbb{F}_{p^{d/2}} \rtimes S_0(p^{d/2})$, которую будем называть группой Пассмана.

Следующие результаты объясняют структуру примитивных $\frac{3}{2}$-транзитивных групп.

Лемма 1.2.4. [13, теорема 1.1] *Примитивная $\frac{3}{2}$-транзитивная группа подстановок либо аффинна, либо почти проста.*

Лемма 1.2.5. *Порядок унипримитивной $\frac{3}{2}$-транзитивной группы G степени n ограничен полиномом от n.*

Доказательство. Если группа G разрешима, то ее порядок полиномиально ограничен в силу [35]. Неразрешимые $\frac{3}{2}$-транзитивные группы степени больше 13^4 либо группы Фробениуса, либо проективные группы размерности 2 по лемме 1.2.3. В обоих случаях порядки групп полиномиально ограничены степенью группы. □

Лемма 1.2.6. *Унипримитивная $\frac{3}{2}$-транзитивная группа G степени, большей 13^4, 2-порождена.*

Доказательство. Обозначим через $d(H)$ минимальное число порождающих группы H. В силу основного результата [32], если N — единственная минимальная нормальная подгруппа группы G, то $d(G) = \max\{2, d(G/N)\}$. Поэтому если группа G почти проста, то требуемое следует из пункта 3 леммы 1.2.3. Таким образом, снова используя лемму 1.2.3, можно считать, что минимальная нормальная подгруппа группы G — регулярная элементарная абелева p-группа. Поэтому $d(G) = \max\{2, d(H)\}$, где H — стабилизатор точки. Если группа G не является группой Фробениуса, то в силу пункта 4 леммы 1.2.3 группа H является подгруппой либо в $\mathrm{\Gamma L}(1, p^d)$, либо в $\mathrm{S}_0(p^{d/2})$, а значит, является подгруппой метациклической группы, т.е. порождается двумя элементами. Наконец, если G — группа Фробениуса, то строение ее стабилизатора точки H, так называемого дополнения Фробениуса, хорошо известно (см., [37, § 18]). Из [37, теоремы 18.2 и 18.6], используя [37, предл. 12.11], несложно вывести, что $d(H) \leq 2$. □

Рассмотрим теперь вопрос о 2-замыкании $\frac{3}{2}$-транзитивных групп. Сначала отметим, что класс $\frac{3}{2}$-транзитивных групп замкнут относительно взятия 2-замыкания.

Лемма 1.2.7. *Если G — $\frac{3}{2}$-транзитивная группа, то ее 2-замыкание $G^{(2)}$ тоже $\frac{3}{2}$-транзитивно.*

Доказательство. Как уже отмечалось, из транзитивности группы G следует транзитивность группы $G^{(2)}$. В силу хорошо известного соответствия между 2-орбитами транзитивной группы и орбитами ее стабилизатора точки совпадение 2-орбит групп G и $G^{(2)}$ влечет совпадение орбит стабилизатора точки. □

Лемма 1.2.8. [23, теорема 2.5.8] *Импримитивная группа Фробениуса 2-замкнута.*

Для удобства построения алгоритмов мы будем ограничивать снизу степень $\frac{3}{2}$-транзитивной группы.

Лемма 1.2.9. *Пусть G — унипримитивная $\frac{3}{2}$-транзитивная почти простая группа подстановок степени, большей 13^4. Тогда $G^{(2)} = G$.*

Доказательство. По доказанному ранее, $G^{(2)}$ тоже унипримитивная $\frac{3}{2}$-транзитивная группа, не являющаяся группой Фробениуса. По лемме 1.2.3 степень n группы G, равная $\frac{1}{2}q(q-1)$, $q = 2^f \geq 8$, f простое, не является степенью простого числа. Поэтому $G^{(2)}$ не может быть аффинной группой. Наконец, группы $\mathrm{P\Gamma L}(2,q)$ и $\mathrm{PSL}(2,q)$ не могут быть 2-эквивалентны из-за различия размеров нетривиальных орбит стабилизатора точки (снова см. лемму 1.2.3). □

Лемма 1.2.10. *Пусть G — $\frac{3}{2}$-транзитивная группа степени, большей 13^4. Если $G \neq G^{(2)}$, то выполняется одно из следующих утверждений:*

а) G дважды транзитивна и $G^{(2)} = \mathrm{Sym}(\Omega)$;

б) G примитивна, $G < \mathrm{AS}_0(p^d)$ и $G^{(2)} = \mathrm{AS}_0(p^d)$;

в) G примитивна, $G < \mathrm{A\Gamma L}(1,q)$ и $G^{(2)} < \mathrm{A\Gamma L}(1,q)$.

Доказательство. Если G — импримитивная группа, то она является группой Фробениуса по лемме 1.2.1 и по лемме 1.2.8 будет 2-замкнутой. Множество $\mathrm{Orb}_2(G)$ любой дважды транзитивной группы состоит из двух элементов, и поэтому $G^{(2)} = \mathrm{Sym}(\Omega)$. Таким образом, мы можем считать, что группа G унипримитивна. Применение лемм 1.1.8 и 1.2.9 показывает, что $G^{(2)}$ удовлетворяет условиям пункта 4 леммы 1.2.3, отсюда следует заключение леммы. □

Лемма 1.2.11. *Пусть k — целое число, большее 1, и G — $\frac{3}{2}$-транзитивная, но не дважды транзитивная группа степени, большей 13^4. Если $G \neq G^{(k)}$, то G примитивна и $G^{(k)} \leq G^{(2)} \leq H$, где $H \in \{\mathrm{AS}_0(p^d), \mathrm{A\Gamma L}(1,q)\}$.*

Доказательство. Если $G \neq G^{(k)}$, то в силу замечания выше $G \neq G^{(2)}$. Из леммы 1.2.10 вытекает примитивность группы G и включения $G^{(k)} \leq G^{(2)} \leq H$. □

Напомним, что цоколь $\mathrm{Soc}(G)$ группы G — это подгруппа, порожденная всеми минимальными нормальными подгруппами группы G. Стоит отметить, что в работах [31, 40] изучался вопрос о совпадении цоколя примитивной группы G и цоколя ее k-замыкания. Далее показывается, что в случае, когда G — $\frac{3}{2}$-транзитивная группа, но не дважды транзитивная группа, из вышеупомянутой классификации несложно вывести, что то же самое равенство имеет место для любого $k \geq 2$.

Лемма 1.2.12. *Пусть k — целое число, большее 1 и G — $\frac{3}{2}$-транзитивная, но не дважды транзитивная группа. Тогда* $\mathrm{Soc}(G) = \mathrm{Soc}(G^{(k)})$.

Доказательство. В силу лемм 1.2.1 и 1.2.8 можно считать, что G примитивна. По лемме 1.2.4 из этого вытекает, что G либо почти проста, либо аффинна. Теперь требуемое следует из [13, теорема 1.2], если G почти проста, и из [12, теорема 3.2], если она аффинна. □

Доказательство. Если G — импримитивная группа, то она является группой Фробениуса по лемме 1.2.1 и по лемме 1.2.8 будет 2-замкнутой. Множество $\mathrm{Orb}_2(G)$ любой дважды транзитивной группы состоит из двух элементов, и поэтому $G^{(2)} = \mathrm{Sym}(\Omega)$. Таким образом, мы можем считать, что группа G унипримитивна. Применение лемм 1.1.8 и 1.2.9 показывает, что $G^{(2)}$ удовлетворяет условиям пункта 4 леммы 1.2.3, отсюда следует заключение леммы. □

§ 1.3. Когерентные конфигурации

В этом параграфе собраны хорошо известные факты о когерентных конфигурациях (см., например, [17] и литературу, там цитируемую).

Пусть S — некоторое разбиение множества $\Omega \times \Omega$ и $S^{\cup}$ — множество всех объединений отношений из S. Пара $\mathcal{X} = (\Omega, S)$ называется *когерентной конфигурацией* на Ω, если выполняются следующие условия:

(K1) $1_\Omega \in S^{\cup}$,

(K2) $s^* \in S$ для любого $s \in S$,

(K3) для любых $r, s, t \in S$, число $c_{rs}^t = |\alpha r \cap \beta s^*|$ не зависит от выбора $(\alpha, \beta) \in t$.

Элементы множеств Ω, S и числа c_{rs}^t называются соответственно *точками*, *базисными отношениями* и *числами пересечений* когерентной конфигурации $\mathcal{X}$. Числа $|\Omega|$ и $|S|$ называются *степенью* и *рангом* конфигурации $\mathcal{X}$.

Подмножество Δ множества Ω называется *фиброй* конфигурации $\mathcal{X}$, если $1_\Delta \in S$. Когерентная конфигурация $\mathcal{X}$ называется *однородной* или *ассоциативной схемой*, если она имеет только одну фибру, т.е. $1_\Omega \in S$. Однородная когерентная конфигурация $\frac{3}{2}$-*однородна*, если для любых $r, s \in S \setminus \{1_\Omega\}$ выполняется $|r| = |s|$. Мы будем рассматривать когерентные конфигурации, возникающие из групп. Если G — группа подстановок множества Ω, то $\mathrm{Inv}(G) = (\Omega, \mathrm{Orb}_2(G))$ называется *шуровой когерентной конфигурацией*, ассоциированной с G. Из леммы 1.1.2 следует, что шуровы когерентные конфигурации, ассоциированные с $\frac{3}{2}$-транзитивными группами являются $\frac{3}{2}$-однородными.

Точка $\alpha \in \Omega$ когерентной конфигурации $\mathcal{X}$ называется *регулярной*, если

$$|\alpha r| \leq 1 \quad \text{для всех } \ r \in S.$$

Если множество регулярных точек конфигурации $\mathcal{X}$ не пусто, то $\mathcal{X}$ называется *1-регулярной*, а если оно совпадает со всем множеством Ω, то — *полурегулярной*.

На множестве когерентных конфигураций, заданных на одном множестве, можно определить естественный частичный порядок, полагая для $\mathcal{X} = (\Omega, S)$ и $\mathcal{X}' = (\Omega, S')$, что

$$\mathcal{X} \leq \mathcal{X}' \ \Leftrightarrow \ S^{\cup} \subseteq (S')^{\cup}.$$

Минимальный и максимальный элементы относительно этого порядка — это *тривиальная* и *полная* когерентные конфигурации: базисные отношения первой из них — это диагональ 1_Ω и ее дополнение (при $n > 1$), а все базисные отношения второй одноэлементны.

Для двух данных когерентных конфигураций $\mathcal{X}_1 = (\Omega, S_1)$ и $\mathcal{X}_2 = (\Omega, S_2)$ единственным образом определяется когерентная конфигурация $\mathcal{Y} = (\Omega, T) = \mathcal{X}_1 \cap \mathcal{X}_2$, для которой $T^{\cup} = (S_1)^{\cup} \cap (S_2)^{\cup}$. Это дает возможность определить *поточечное расширение* $\mathcal{X}_{\alpha,\beta,\dots}$ когерентной конфигурации $\mathcal{X} = (\Omega, S)$ относительно точек $\alpha, \beta, \ldots \in \Omega$ следующим образом:

$$\mathcal{X}_{\alpha,\beta,\dots} = \bigcap_{\mathcal{Y}:\ S \subseteq T^{\cup}, 1_\alpha, 1_\beta, \dots \in T^{\cup}} \mathcal{Y},$$

где $\mathcal{Y} = (\Omega, T)$. Иными словами, $\mathcal{X}_{\alpha,\beta,\dots}$ — это наименьшая когерентная конфигурация на Ω, которая больше или равна $\mathcal{X}$ и содержит одноэлементные множества $\{\alpha\}, \{\beta\}, \ldots$ в качестве фибр.

Множество $\Delta = \{\alpha, \beta, \ldots\} \subseteq \Omega$ называется *базой* когерентной конфигурации $\mathcal{X}$, если поточечное расширение $\mathcal{X}_{(\Delta)} = \mathcal{X}_{\alpha,\beta,\dots}$ относительно точек $\alpha, \beta, \ldots$ из Δ является полной когерентной конфигурацией. Наименьшая возможная мощность базы называется *базисным числом* конфигурации $\mathcal{X}$ и обозначается через $b(\mathcal{X})$ (иногда, допуская некоторую вольность речи, об этом числе говорят, как о *размере базы* конфигурации $\mathcal{X}$). Несложно видеть, что размер базы ограничен следующим образом: $0 \leq b(\mathcal{X}) \leq n - 1$, и граничные значения достигаются для полной и тривиальной конфигураций соответственно.

Следующее утверждение, которое можно рассматривать как комбинаторный аналог леммы 1.2.1, будет играть ключевую роль при построении алгоритмов.

Лемма 1.3.1. *Пусть $\mathcal{X} = \mathrm{Inv}(G)$ — схема импримитивной $\frac{3}{2}$-транзитивной группы G. Тогда $b(\mathcal{X}) = 2$.*

Доказательство. Следует из [2, теорема 5.11]. □

Когерентные конфигурации $\mathcal{X} = (\Omega, S)$ и $\mathcal{X}' = (\Omega', S')$ называются *изоморфными*, если существует биекция $f : \Omega \to \Omega'$, для которой отношение $s^f = \{(\alpha^f, \beta^f) : \ (\alpha, \beta) \in s\}$ лежит в S' для всех $s \in S$. Сама биекция f называется *изоморфизмом* из $\mathcal{X}$ на $\mathcal{X}'$; множество всех таких изоморфизмов обозначается через $\mathrm{Iso}(\mathcal{X}, \mathcal{X}')$. Очевидно, что множество $\mathrm{Iso}(\mathcal{X}, \mathcal{X})$ — группа подстановок множества Ω.

Пусть теперь фиксирована биекция $\psi : S \to S'$. Изоморфизм $f \in \mathrm{Iso}(\mathcal{X}, \mathcal{X}')$, для которого $s^f = s^\psi$ для каждого $s \in S$, назовем изоморфизмом цветных конфигураций (относительно ψ) и обозначим множество всех таких изоморфизмов через $\mathrm{Iso}(\mathcal{X}, \mathcal{X}', \psi)$. Подмножество $\mathrm{Aut}(\mathcal{X}) = \mathrm{Iso}(\mathcal{X}, \mathcal{X}, \mathrm{id}_S)$ элементов группы $\mathrm{Iso}(\mathcal{X}, \mathcal{X})$, где id_S — тождественное отображение на множестве S, является ее нормальной подгруппой и называется *группой автоморфизмов* (цветной) когерентной конфигурации $\mathcal{X}$.

Биекция $\varphi : S \to S', \ r \mapsto r'$ называется *алгебраическим изоморфизмом* из $\mathcal{X}$ на $\mathcal{X}'$, если

$$c_{rs}^t = c_{r's'}^{t'}, \qquad r, s, t \in S. \tag{1.1}$$

В этом случае когерентные конфигурации $\mathcal{X}$ и $\mathcal{X}'$ называются *алгебраически изоморфными*. Каждый изоморфизм f из $\mathcal{X}$ на $\mathcal{X}'$ индуцирует естественным образом алгебраический изоморфизм между ними. Множество всех изоморфизмов, индуцирующих данный алгебраический изоморфизм φ, очевидно, равно $\mathrm{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$. Если это множество не пусто для любого алгебраического изоморфизма $\varphi : \mathcal{X} \to \mathcal{X}'$, то когерентная конфигурация $\mathcal{X}$ называется *отделимой*. В соответствии с формулой (1.1), конфигурация $\mathcal{X}$ отделима тогда и только тогда, когда она с точностью до изоморфизма определяется набором своих чисел пересечения.

Лемма 1.3.2. *Каждая 1-регулярная когерентная конфигурация отделима. Более того, если α и α' — регулярные точки когерентных конфигураций $\mathcal{X}$ и $\mathcal{X}'$, лежащие в фибрах Δ и Δ' соответственно, а φ — алгебраический изоморфизм между этими конфигурациями, для которого $1_\Delta^\varphi = 1_{\Delta'}$, то существует единственный изоморфизм f из $\mathrm{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$, переводящий α в α'.*

Доказательство. Первое утверждение хорошо известно (см., например, [21, теорема 3.3]), а второе сразу вытекает из определения регулярной точки. □

Лемма 1.3.3. *Пусть $\mathcal{X}$ — когерентная конфигурация, удовлетворяющая условию*

$$\Gamma \in F(\mathcal{X}) \ и \ \Gamma \cap \Delta = \varnothing \Rightarrow n_s = 1 \ для \ некоторого \ s \in S(\mathcal{X})_{\Delta,\Gamma},$$

для некоторого $\Delta \in F(\mathcal{X})^\cup$. Тогда отображение ограничения из $\mathrm{Aut}(\mathcal{X})$ в $\mathrm{Aut}(\mathcal{X}_\Delta)$ является изоморфизмом групп.

Доказательство. Это утверждение является частным случаем [17, лемма 3.3.20] □

§ 1.4. Циклотомические схемы над конечными почти-полями

Алгебраическая система $\mathbb{K} = \langle \mathbb{K}, +, \circ \rangle$ называется (правым) *почти-полем*, если $\mathbb{K}^+ = \langle \mathbb{K}, + \rangle$ — аддитивная группа с нейтральным элементом 0, $\mathbb{K}^\times = \langle \mathbb{K} \setminus \{0\}, \circ \rangle$ — мультипликативная группа, $x \circ 0 = 0$ для любого $x \in \mathbb{K}$ и

$$(x + y) \circ z = x \circ z + y \circ z, \quad x, y, z \in \mathbb{K}.$$

В [50] Цассенхауз классифицировал конечные почти-поля, показав, что проблема нахождения конечных почти-полей эквивалентна нахождению дважды транзитивных групп Фробениуса.

Лемма 1.4.1. *Каждое конечное почти-поле лежит в одном из двух классов:*

1) *почти-поля Диксона,*

2) *почти-поля Цассенхауза* (7 *исключительных почти-полей*).

Таблица 1: Почти-поля Цассенхауза

$\mathbb{K}$	порождающие $\mathbb{K}^\times$
5^2	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -2 \\ -1 & -2 \end{pmatrix}$
11^2	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 5 \\ -5 & -2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$
7^2	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix}$
23^2	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -6 \\ 12 & -2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$
11^2	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 4 \\ 1 & -3 \end{pmatrix}$
29^2	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -7 \\ 12 & -2 \end{pmatrix}, \begin{pmatrix} 16 & 0 \\ 0 & 16 \end{pmatrix}$
59^2	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 9 & 15 \\ -10 & -10 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$

Конечное почти-поле $\mathbb{K}$ называется *почти-полем Диксона*, если существует поле $\mathbb{F}_0$ порядка $q_0 = p^l$ и его расширение $\mathbb{F}$ порядка q_0^n такое, что $\mathbb{F}^+ = \mathbb{K}^+$ и умножение элементов в

почти-поле можно задать через умножение элементов в поле $\mathbb{F}$ с использованием автоморфизмов расширения:

$$y \circ x = y^{\sigma_x} \cdot_{\mathbb{F}} x, \quad x, y \in \mathbb{K}, \sigma_x \in \mathrm{Aut}(\mathbb{F}/\mathbb{F}_0).$$

Доказано, что если почти-поле $\mathbb{K}$ порядка $q = q_0^n$ получено из расширения $\mathbb{F}$ степени n поля $\mathbb{F}_0$ порядка q_0, то $\langle q_0, n\rangle$ образуют так называемую *пару Диксона*, т.е. каждый простой делитель числа n является делителем числа $q_0 - 1$ и, если 4 делит n, то 4 делит и $q_0 - 1$. Обратно, для каждой пары Диксона $\langle q_0, n\rangle$ существует $\varphi(n)/k$ попарно неизоморфных почти-полей Диксона, где $\varphi(n)$ — значение функции Эйлера от числа n, и k — порядок числа p по модулю n. Заметим, что почти-поле Диксона является полем тогда и только тогда, когда $n = 1$. Кроме почти-полей Диксона существует 7 исключительных почти-полей Цассенхауза. Для каждого почти-поля Цассенхауза $\mathbb{K}$ в таблице 1 приведены порождающие мультипликативной группы $\mathbb{K}^\times$ как матричные преобразования аддитивной группы $\mathbb{K}^+$. Детальное описание конченых почти-полей можно найти в монографии [46].

Пусть $\mathbb{K}$ — конечное почти-поле порядка q, и K — подгруппа группы $\mathbb{K}^\times$. Положим $\mathcal{R}_K = \{R_K(a) \mid a \in \mathbb{K}\}$, где

$$R_K(a) = \{(x, y) \in \mathbb{K}^2 \mid x - y \in K \circ a\}.$$

Пара $\mathrm{Cyc}(\mathbb{K}, K) = (\mathbb{K}, \mathcal{R}_K)$ является $\frac{3}{2}$-однородной когерентной конфигурацией и называется *циклотомической схемой* над почти-полем $\mathbb{K}$ с базисной группой K. Непосредственно проверяется, что множество отношений $\mathcal{R}_K$ этой циклотомической схемы совпадает с множеством $\mathrm{Orb}_2(G)$ 2-орбит группы

$$G = G(\mathbb{K}, K) = \{x \mapsto x \circ b + c \mid b \in K, c \in \mathbb{K}^+, x \in \mathbb{K}\}$$

подстановок множества $\mathbb{K}$, и потому $\mathrm{Aut}(\mathcal{C}) = G^{(2)}$. В частности, G является подгруппой группы $\mathrm{Aut}(\mathcal{C})$.

Как показано в [50], для конечного почти-поля $\mathbb{K}$ группа $G(\mathbb{K}, \mathbb{K}^\times)$ — дважды транзитивная группа Фробениуса. Поэтому, во-первых, 2-замыкание группы $G(\mathbb{K}, \mathbb{K}^\times)$ совпадает с симметрической группой $\mathrm{Sym}(\mathbb{K})$ и $\mathrm{Aut}(\mathcal{C}) = \mathrm{Sym}(\mathbb{K})$, во-вторых, если K — нетривиальная подгруппа группы $K^\times$, то $G(\mathbb{K}, K)$ — группа Фробениуса как подгруппа группы Фробениуса $G(\mathbb{K}, \mathbb{K}^\times)$. Будем называть циклотомическую схему $\mathrm{Cyc}(\mathbb{K}, K)$ *собственной*, если K — собственная подгруппа группы $\mathbb{K}^\times$.

Лемма 1.4.2. *Пусть $\mathbb{K}$ — почти-поле Диксона порядка q, K — подгруппа группы $\mathbb{K}^\times$, $\mathcal{C} = \mathrm{Cyc}(\mathbb{K}, \mathbb{K}^\times)$ и группа $G = G(\mathbb{K}, K)$ 2-замкнута. Тогда $\mathrm{Aut}(\mathcal{C}) \leq \mathrm{A\Gamma L}(1, q)$.*

Доказательство. $G = G(\mathbb{K}, K) = \{x \mapsto x \circ b + c \mid b \in K, c \in \mathbb{K}^+, x \in \mathbb{K}\}$. Для почти-поля Диксона $\mathbb{K}$ существует поле $\mathbb{F}_0$ и его расширение $\mathbb{F}$, такое что $\mathbb{K}^+ = \mathbb{F}^+$ и $x \circ b = x^{\sigma_b} \cdot_{\mathbb{F}} b$ для некоторого $\sigma_b \in \mathrm{Aut}(\mathbb{F})$. Тогда $G = \{x \mapsto x^{\sigma_b} \cdot_{\mathbb{F}} b + c \mid b \in K, c \in \mathbb{K}^+, x \in \mathbb{K}, \sigma_b \in \mathrm{Aut}(\mathbb{F}/\mathbb{F}_0)\}$, и поэтому $G \leq \mathrm{A\Gamma L}(1, q)$. Так как G 2-замкнута, то $\mathrm{Aut}(\mathcal{C}) = G^{(2)} = G \leq \mathrm{A\Gamma L}(1, q)$. □

Как отмечено в доказательстве леммы 1.4.2, для циклотомической схемы $\mathrm{Cyc}(\mathbb{K}, K)$ над почти-полем Диксона, соответствующая ей группа $G(\mathbb{K}, K)$ — подгруппа группы $\mathrm{A\Gamma L}(1, q)$. В частности, $G(\mathbb{K}, K) = \mathbb{K}^+ \rtimes K$ и $K \leq \Gamma\mathrm{L}(1, q) = \{x \mapsto x^{\sigma} \cdot_{\mathbb{F}} b \mid b \in K, x \in \mathbb{K}, \sigma \in \mathrm{Aut}(\mathbb{F})\}$. Более того, группу $\mathbb{K}^+$ можно рассматривать как аддитивную группу векторного пространства $V_{\mathbb{K}}$, а группа $G(\mathbb{K}, K)$ может быть рассмотрена как подгруппа аффинной линейной группы $\mathrm{AGL}(V_{\mathbb{K}})$, где $K \leq \mathrm{GL}(V_{\mathbb{K}})$.

Следующее утверждение следует из основного результата [33].

Лемма 1.4.3. *Пусть $\mathcal{C} = \mathcal{C}(\mathbb{F}, K)$ — собственная циклотомическая схема над конечным полем $\mathbb{F}$ порядка q с базисной группой K. Тогда* $\mathrm{Aut}(\mathcal{C}) \leq \mathrm{A\Gamma L}(1, q)$.

Циклотомическая схема $\mathrm{Cyc}(\mathbb{K}, K)$ *примитивна*, если группа $G(\mathbb{K}, K)$ примитивна.

Лемма 1.4.4. [42, теорема 2.4] *Каждая примитивная циклотомическая схема над конечным почти-полем с абелевой базисной группой является циклотомической схемой над некоторым конечным полем.*

Лемма 1.4.5. *Пусть $\mathbb{K}$ — почти-поле, $1 \neq K \leq \mathbb{K}^\times$ и $G = G(\mathbb{K}, K)$. Тогда группы G и $G^{(2)}$ $\frac{3}{2}$-транзитивны.*

Доказательство. Транзитивность группы G следует из ее определения. Поскольку $G \leq G^{(2)}$, группа $G^{(2)}$ тоже транзитивна. Покажем $\frac{1}{2}$-транзитивность стабилизаторов G_α, $(G^{(2)})_\alpha$ точки $\alpha \in \mathbb{K}$. Множества 2-орбит групп G и $G^{(2)}$ совпадают с разбиением $\mathcal{R}_K$ циклотомической схемы $\mathrm{Cyc}(\mathbb{K}, K)$, а элементы $R_K(a)$ разбиения $\mathcal{R}_K$ равномощны, потому что, по сути, являются смежными классами. Далее по лемме 1.1.2 равномощны орбиты стабилизатора точки α, соответствующие нетривиальным 2-орбитам. Таким образом, стабилизаторы точки групп G и $G^{(2)}$ $\frac{1}{2}$-транзитивны, и поэтому группы G и $G^{(2)}$ $\frac{3}{2}$-транзитивны. □

§ 1.5. Алгоритм Вейсфейлера–Лемана и его приложения

Ключевую роль в построении алгоритмов будет играть классический алгоритм Вейсфейлера–Лемана, впервые появившийся в [1] и детально описанный в [47, Часть B]. Входом

этого алгоритма является произвольное множество P бинарных отношений на множестве Ω, а выходом — наименьшая когерентная конфигурация

$$\mathrm{WL}(P) = (\Omega, S)$$

такая, что $P \subseteq S^{\cup}$. Мы будем называть ее WL-замыканием множества P. Время работы алгоритма полиномиально от размеров P и Ω. Анализ этого алгоритма в [47, Часть M] дает доказательство следующего утверждения (точная формулировка взята из [41, теорема 2.4]).

Лемма 1.5.1. *Пусть P и P' — два m-элементных множества бинарных отношений на n-элементном множестве и задана биекция $\psi : P \to P'$. Тогда за время $mn^{O(1)}$ можно проверить, существует ли алгебраический изоморфизм $\varphi : \mathrm{WL}(P) \to \mathrm{WL}(P')$, для которого $\varphi|_P = \psi$. Более того, если φ существует, то его можно найти за то же время.*

Используя эту лемму, несложно показать, что существует эффективный алгоритм проверки изоморфизма между двумя алгебраически изоморфными когерентными конфигурациями с ограниченным размером базы. А именно, верно следующее утверждение.

Лемма 1.5.2. [41, теорема 3.5] *Пусть $\mathcal{X}$ и $\mathcal{X}'$ — когерентные конфигурации на n точках и $\varphi : \mathcal{X} \to \mathcal{X}'$ — алгебраический изоморфизм между ними. Тогда все элементы множества $\mathrm{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$ могут быть перечислены за время $(bn)^{O(b)}$, где $b = b(\mathcal{X})$ — размер базы конфигурации $\mathcal{X}$.*

Комбинируя данные две леммы с леммой 1.3.1, получаем решение проблемы изоморфизма цветных шуровых когерентных конфигураций, ассоциированных с импримитивными $\frac{3}{2}$-транзитивными группами.

Лемма 1.5.3. *Пусть G и G' — $\frac{3}{2}$-транзитивные группы подстановок множества Ω и ψ — биекция между множествами их 2-орбит. Если группа G импримитивна, то множество $\mathrm{Iso}(\mathrm{Inv}(G), \mathrm{Inv}(G'), \psi)$ может быть найдено за время $\mathrm{poly}(n)$.*

Следующий хорошо известный «теоретико-групповой» алгоритм может быть реализован с помощью алгоритма Вейсфейлера–Лемана как «комбинаторный».

Алгоритм **IMBED**

Вход: транзитивная группа $G \leq \mathrm{Sym}(\Omega)$ с порождающим d-элементным множеством T, группа $H \leq \mathrm{Sym}(\Omega)$, порядок которой ограничен полиномом от n, d-элементное подмножество T' из H, биекция $\psi : T \to T'$ и пара $(\omega, \omega') \in \Omega \times \Omega$.

Выход: либо подстановка x множества Ω, для которой $G^x \leq H$, $t^x = t^\psi$ по всем $t \in T$ и $\omega^x = \omega'$, либо пустое множество, если такой подстановки нет.

Описание алгоритма

Шаг 1: Пусть $T = \{t_1, \ldots, t_d\}$, $T' = \{t'_1, \ldots, t'_d\}$ и $t_i^\psi = t'_i$ для всех $i = 1, \ldots, d$. Определим два множества $P = \{p_1, \ldots, p_d\}$ и $P' = \{p'_1, \ldots, p'_d\}$ бинарных отношений на Ω следующим образом: для любого $\alpha \in \Omega$ и $i = 1, \ldots, d$ положим $(\alpha, \alpha^{t_i}) \in p_i$ и $(\alpha, \alpha^{t'_i}) \in p'_i$. Зафиксируем биекцию $\psi : P \to P', p_i \mapsto p'_i, i = 1, \ldots, d$, индуцированную биекцией между множествами T и T'.

Шаг 2: С помощью алгоритма Вейсфейлера-Лемана найдем WL-замыкания $\mathrm{WL}(P)$ и $\mathrm{WL}(P')$ множеств P и P'. Заметим, что по построению множеств P и P' обе когерентные конфигурации $\mathrm{WL}(P)$ и $\mathrm{WL}(P')$ полурегулярны.

Шаг 3: С помощью алгоритма из леммы 1.5.2 проверим, существует ли алгебраический изоморфизм φ между $\mathrm{WL}(P)$ и $\mathrm{WL}(P')$, для которого $\varphi|_P = \psi$ и $1_\Delta^\varphi = 1_{\Delta'}$, где Δ и Δ' — фибры когерентных конфигураций $\mathrm{WL}(P)$ и $\mathrm{WL}(P')$, такие что $(\omega, \omega') \in \Delta \times \Delta'$.

Шаг 4: Если указанный на шаге 3 алгебраический изоморфизм φ между $\mathrm{WL}(P)$ и $\mathrm{WL}(P')$ найден, то по лемме 1.3.2 в силу полурегулярности $\mathrm{WL}(P)$ и $\mathrm{WL}(P')$ мы определим единственным образом подстановку $x \in \mathrm{Iso}(\mathrm{WL}(P), \mathrm{WL}(P'), \varphi)$, для которой $\omega' = \omega^x$. Положим $\mathrm{IMBED}((G, T), (H, T'), \psi, (\omega, \omega')) = x$.

Шаг 5: Если алгебраического изоморфизма нет, положим $\mathrm{IMBED}((G, T), (H, T'), \psi, (\omega, \omega')) = \varnothing$.

Лемма 1.5.4. *Алгоритм* IMBED *корректен, и время его работы не превосходит* $\mathrm{poly}(dn)$.

Доказательство. Если подстановка $x \in \mathrm{Sym}(\Omega)$ такова, что $G^x \leq H$, $t^x = t^\psi$ по всем $t \in T$ и $\omega' = \omega^x$, то она по построению лежит в $\mathrm{Iso}(\mathrm{WL}(P), \mathrm{WL}(P'), \varphi)$, где P, P' и алгебраический изоморфизм $\varphi : \mathrm{WL}(P) \to \mathrm{WL}(P')$ определены в алгоритме. Обратно, если $\mathrm{Iso}(\mathrm{WL}(P), \mathrm{WL}(P'), \varphi) \neq \varnothing$ и для фибр Δ и Δ' выполняется $1_\Delta^\varphi = 1_{\Delta'}$, то по лемме 1.3.2 в силу полурегулярности $\mathrm{WL}(P)$ и $\mathrm{WL}(P')$ найдется подстановка $x \in \mathrm{Iso}(\mathrm{WL}(P), \mathrm{WL}(P'), \varphi)$, для которой $\omega' = \omega^x$. Тогда

$$(\omega')^{t'_i} = (\omega^{t_i})^x = (\omega^x)^{x^{-1} t_i x} = (\omega')^{t_i^x}, i = 1, \ldots, d.$$

Поскольку G транзитивна, эти равенства влекут равенства $t'_i = t_i^x$, $i = 1, \ldots, d$. Осталось заметить, что множество T порождает группу G, а T' — подгруппу группы H, изоморфную группе G. Таким образом, алгоритм корректен. Оценка на время алгоритма вытекает из оценки на время алгоритма Вейсфейлера–Лемана. □

2. k-Замыкания нильпотентных групп

Основным результатом этой главы является следующая

Теорема 1. *Если G — конечная нильпотентная группа подстановок и k — целое число, большее 1, то*

$$G^{(k)} = \prod_{P \in \mathrm{Syl}(G)} P^{(k)},$$

т.е. k-замыкание группы G является прямым произведением k-замыканий всех силовских подгрупп группы G. В частности, $G^{(k)}$ нильпотентна.

§ 2.1. Вспомогательные утверждения

Пусть π — множество простых чисел и n — натуральное число. Обозначим через n_π делитель числа n такой, что $(n_\pi, \frac{n}{n_\pi}) = 1$ и множество всех простых делителей числа n_π совпадает с π. Оказывается, что в этих обозначениях выражаются порядки орбит холловой подгруппы транзитивной нильпотентной группы.

Лемма 2.1.1. *Пусть G — транзитивная нильпотентная группа подстановок степени n и H — холлова подгруппа группы G. Тогда*

а) длина каждой H-орбиты равна n_π, где $\pi = \pi(H)$,

б) G действует на множестве $\mathrm{Orb}(H)$*. Более того, H – ядро этого действия.*

Доказательство. Поскольку $H \trianglelefteq G$, орбиты группы H одной длины m и группа G действует на множестве орбит $\Sigma = \mathrm{Orb}(H)$. Обозначим ядро этого действия через K и заметим, что $H \leq K$.

Группа $G^\Sigma \leq \mathrm{Sym}(\Sigma)$ транзитивна, и потому $|\Sigma|$ делит $|G^\Sigma|$ и число $|G^\Sigma|$ имеет вид $|G^\Sigma| = \frac{|G|}{|K|}$. Учитывая включение $H \leq K$, получаем, что $|G^\Sigma|$ делит $n_{\pi'}$, где π' — множество всех простых делителей числа n, которые не содержатся π. В итоге, $|\Sigma|$ делит π'. Учитывая, что m делит $|H| = n_\pi$, получаем цепочку неравенств

$$n = m \cdot |\Sigma| \leq n_\pi \cdot n_{\pi'} = n,$$

из которой следует, что $m = n_\pi$ и $|\Sigma| = n_{\pi'}$.

$$n_{\pi'} = |\Sigma| \leq |G^\Sigma| \leq n_{\pi'},$$

которая влечет равенство $|G^\Sigma| = n_{\pi'}$. Вспоминая, что $|G^\Sigma| = \frac{|G|}{|K|}$, получаем $|K| = n_\pi = |H|$, откуда следует $K = H$. □

Лемма 2.1.2. *Пусть G — конечная нильпотентная группа подстановок, $P \in \mathrm{Syl}(G)$, $\Delta_1, \ldots, \Delta_k \in \mathrm{Orb}(P)$ и $\Delta = \bigcup_{i=1}^k \Delta_i$. Тогда*

$$\left(\bigcap_{i=1}^k G_{\{\Delta_i\}}\right)^\Delta \leq P^\Delta.$$

Доказательство. Пусть $g \in \left(\bigcap_{i=1}^k G_{\{\Delta_i\}}\right)^\Delta$. Поскольку группа G нильпотентна, $G = P \times H$, где H — холлова подгруппа группы G, и тем самым $g = xy$ для некоторых $x \in P$ и $y \in H$. Из выбора g и x следует, что $\Delta_i^g = \Delta_i^x = \Delta_i$ для всех $i = 1, \ldots, k$, что влечет то же самое для y, потому что

$$\Delta_i = \Delta_i^g = \Delta_i^x = \Delta_i^{x^{-1}g} = \Delta_i^y.$$

Покажем, что $y^{\Delta_i} = 1_{\Delta_i}$ для всех $i = 1, \ldots, k$. Действительно, из выбора y следует, что элемент y^{Δ_i} принадлежит централизатору Z_i транзитивной группы $P^{\Delta_i} \leq \mathrm{Sym}(\Delta_i)$, который полурегулярен по [48, упр. 4.5']. Поэтому $|Z_i|$ делит число $|\Delta_i|$, которое в свою очередь является степенью числа p. Так что, Z_i является p-группой. В частности, порядок элемента y^{Δ_i} – степень числа p, и потому $y^{\Delta_i} \in P^{\Delta_i}$. Учитывая, что $P^{\Delta_i} \cap H^{\Delta_i} = 1$, получаем $y^{\Delta_i} = 1_{\Delta_i}$.

Итак, $y^\Delta = 1_\Delta$, а значит

$$g^\Delta = (xy)^\Delta = x^\Delta y^\Delta = x^\Delta \in P^\Delta,$$

что и требовалось доказать. □

Как известно, конечная нильпотентная группа G, которая не является p-группой, имеет вид прямого произведения $G = P \times H$, где P — силовская p-подгруппа группы G, а H — холлова подгруппа группы G. Следующая лемма показывает, что для транзитивных нильпотентных групп это прямое произведение является прямым произведением групп подстановок.

Лемма 2.1.3. [6, 34.3, лемма 2] *Пусть G — транзитивная нильпотентная группа подстановок конечного множества Ω, не являющаяся p-группой, т.е. $G = P \times H$, где P — силовская p-подгруппа, а H — холлова подгруппа группы G. Тогда существуют множества Δ и Γ такие, что группы P и H действуют точно и транзитивно на множествах Δ и Γ соответственно, и группа $P^\Delta \times H^\Gamma \leq \mathrm{Sym}(\Delta \times \Gamma)$ подстановочно изоморфна группе G.*

§ 2.2. Доказательство теоремы 1

Сначала рассмотрим случай, когда группа G транзитивна. Будем использовать индукцию по числу $|\pi(G)|$. Если $|\pi(G)| = 1$, то G — p-группа, и в силу [49, упр. 5.28] 2-замыкание $G^{(2)}$ тоже p-группа, а значит, в силу леммы 1.1.4 p-группой является и $G^{(k)}$ для любого $k \geq 2$.

Пусть теперь $G = P \times H$, где P — силовская p-подгруппа группы G, и H — холлова подгруппа группы G. По лемме 2.1.3 группа G подстановочно изоморфна группе $P' \times H'$, действующей на некотором множестве $\Delta \times \Gamma$. Из леммы 1.1.7 следует, что

$$(P' \times H')^{(k)} = (P')^{(k)} \times (H')^{(k)}.$$

Доказательство завершается применением индукционного предположения к группе H, что возможно в силу равенства $\pi(G) = \pi(P) \cup \pi(H)$.

Теперь пусть G интранзитивна. Каждая транзитивная составляющая H группы G нильпотентна (как гомоморфный образ нильпотентной группы), и $\pi(H) \subseteq \pi(G)$. Из предыдущих рассуждений следует, что группа $H^{(k)}$ тоже нильпотентна, и $\pi(H) = \pi(H^{(k)})$. Применяя лемму 1.1.6, получаем, что

$$G \leq G^{(k)} \leq \big(\prod_H H\big)^{(k)} = \prod_H H^{(k)},$$

что влечет равенство $\pi(G) = \pi(G^{(k)})$.

Теперь рассмотрим силовские подгруппы групп G и $G^{(k)}$.

Лемма 2.2.1. *Если $P \in \mathrm{Syl}_p(G)$, и $Q \in \mathrm{Syl}_p(G^{(k)})$, то $P^{(k)} \leq Q$, и $\mathrm{Orb}(P) = \mathrm{Orb}(Q)$.*

Доказательство. Включение $P^{(k)} \leq Q$ следует из [49, упр. 5.28] и леммы 1.1.4. Поэтому для доказательства равенства $\mathrm{Orb}(P) = \mathrm{Orb}(Q)$ остается показать, что каждая P-орбита является Q-орбитой.

Пусть $\Delta \in \mathrm{Orb}(P)$, и $\Gamma \in \mathrm{Orb}(G)$ такая, что $\Delta \subseteq \Gamma$. k-Замыкание сохраняет 1-орбиты, поэтому Γ также и $G^{(k)}$-орбита. Обозначим через Δ' орбиту группы Q такую, что

$$\Delta \subseteq \Delta' \subseteq \Gamma.$$

Группы G^Γ и $(G^{(k)})^\Gamma$ транзитивны и нильпотентны, поэтому двойное применение леммы 2.1.1 влечет равенство $|\Delta| = |\Gamma|_p = |\Delta'|$, и $\Delta = \Delta'$. □

Лемма 2.2.2. *В обозначениях выше $P^{(k)} = Q$.*

Доказательство. В лемме 2.2.1 было установлено, что $P^{(k)} \leq Q$. Для доказательства обратного включения пусть $(\alpha_1, \ldots, \alpha_k) \in \Omega^k$ и $g \in Q$. По лемме 1.1.1 существует $h \in G$ такой, что

$$(\alpha_1, \ldots, \alpha_k)^g = (\alpha_1, \ldots, \alpha_k)^h.$$

Обозначим через Δ_i орбиту группы Q, содержащую α_i, $i = 1, \ldots, k$. Из леммы 2.2.1 следует, что каждая Δ_i также орбита группы P. Элемент h фиксирует каждую орбиту Δ_i как множество, потому что $\alpha_i^h = \alpha_i^g \in \Delta_i$. Другими словами, $h \in \bigcap_{i=1}^k G_{\{\Delta_i\}}$, и по лемме 2.1.2 существует $u \in P$ такой, что $h^\Delta = u^\Delta$ (здесь $\Delta = \bigcup_{i=1}^k \Delta_i$), и потому

$$(\alpha_1, \ldots, \alpha_k)^g = (\alpha_1, \ldots, \alpha_k)^h = (\alpha_1, \ldots, \alpha_k)^u.$$

Из леммы 1.1.1 получаем, что $g \in P^{(k)}$, и $Q \leq P^{(k)}$. □

Доказательство теоремы завершается применением леммы 2.2.2 в следующей цепочке равенств:

$$G^{(k)} = \prod_{\mathrm{Syl}(G^{(k)})} Q = \prod_{\mathrm{Syl}(G)} P^{(k)}.$$

3. 2-Замыкания абелевых групп

Группа подстановок G называется квазирегулярной, если G^{Δ} — регулярная группа для всех $\Delta \in \mathrm{Orb}(G)$. Для таких групп определим подгруппу Зеликовского $\mathrm{Zel}(G) \leq \mathrm{Sym}(\Omega)$ следующим образом

$$\mathrm{Zel}(G) = \prod_{\Delta} \bigcap_{\Delta' \neq \Delta} (G_{\Delta'})^{\Delta},$$

где Δ и Δ' пробегают множество $\mathrm{Orb}(G)$. В этих обозначениях будет доказана следующая

Теорема 2. *Пусть G — квазирегулярная группа подстановок и $Z = \mathrm{Zel}(G)$. Тогда G 2-замкнута в том и только в том случае, если $Z \leq G$ и $G^{\mathrm{Orb}(Z)}$ 2-замкнута.*

Следующие два примера показывают существенность условий теоремы 2. Рассмотрим группу

$$G = \langle (1\,2\,3\,4)(5\,6\,7\,8)(9\,10\,11\,12)(13\,14\,15\,16), (9\,10\,11\,12)(13\,14\,15\,16)(17\,18\,19\,20)(21\,22\,23\,24),$$
$$(1\,3)(2\,4), (5\,7)(6\,8), (9\,11)(10\,12), (13\,15)(14\,16), (17\,19)(18\,20)\rangle$$

порядка 256, для которой $\mathrm{Zel}(G) \leq G$, где

$$\mathrm{Zel}(G) = \langle (13)(24), (57)(68), (9\ 11)(10\ 12), (13\ 15)(14\ 16), (17\ 19)(18\ 20), (21\ 23)(22\ 24)\rangle.$$

Обозначая орбиты группы $\mathrm{Zel}(A)$ следующим образом:

$$\mathbf{1} = \{1, 3\}, \mathbf{2} = \{2, 4\}, \mathbf{3} = \{5, 7\}, \mathbf{4} = \{6, 8\}, \mathbf{5} = \{9, 11\}, \mathbf{6} = \{10, 12\},$$

$$\mathbf{7} = \{13, 15\}, \mathbf{8} = \{14, 16\}, \mathbf{9} = \{17, 19\}, \mathbf{10} = \{18, 20\}, \mathbf{11} = \{21, 23\}, \mathbf{12} = \{22, 24\},$$

получаем группу порядка 4:

$$G^{\mathrm{Orb}(\mathrm{Zel}(G))} = \langle (\mathbf{1\,2})(\mathbf{3\,4})(\mathbf{5\,6})(\mathbf{7\,8}), (\mathbf{1\,2})(\mathbf{3\,4})(\mathbf{9\,10})(\mathbf{11\,12})\rangle,$$

которая не 2-замкнута:

$$(G^{\mathrm{Orb}(\mathrm{Zel}(G))})^{(2)} = \langle (\mathbf{1\,2})(\mathbf{3\,4}), (\mathbf{5\,6})(\mathbf{7\,8}), (\mathbf{9\,10})(\mathbf{11\,12})\rangle > G^{\mathrm{Orb}(\mathrm{Zel}(G))}.$$

Теперь рассмотрим не 2-замкнутую группу

$$H = \{\varepsilon, (12)(34), (34)(56), (12)(56)\},$$

для которой

$$\mathrm{Zel}(H) = \langle (12), (34), (56) \rangle.$$

Получается, что $H^{(2)} = \mathrm{Zel}(H)$, $H^{\mathrm{Orb}(\mathrm{Zel}(H))} = 1$, и тем самым $\mathrm{Zel}(H) \not\leq H$.

Орбита Δ группы $G \leq \mathrm{Sym}(\Omega)$ называется несущественной, если G 2-замкнута тогда и только тогда, когда группа $G^{\Omega \setminus \Delta}$ 2-замкнута.

Теорема 3. *Пусть p — простое число, G — интранзитивная p-группа с циклическими транзитивными составляющими и $\mathrm{Zel}(G) = 1$. Тогда каждая орбита группы G является несущественной.*

Комбинация теорем 1, 2 и 3 дает явный индуктивный критерий проверки 2-замкнутости (абелевых) групп подстановок с циклическими транзитивными составляющими.

Алгоритм **CYCLOSURE**

Вход: G — абелева группа подстановок множества Ω с циклическими транзитивными составляющими.

Выход: $G = G^{(2)}$ или $G \neq G^{(2)}$

Описание алгоритма

Шаг 1: Если G тривиальна или регулярна, то $G = G^{(2)}$.

Шаг 2: Если G не p-группа и $P = P^{(2)}$ для всех $P \in \mathrm{Syl}(G)$, то $G = G^{(2)}$.

Шаг 3: Если $1 \neq \mathrm{Zel}(G) \leq G$, то $G = G^{(2)}$ тогда и только тогда, когда $G^{\mathrm{Orb}(\mathrm{Zel}(G))}$ 2-замкнута.

Шаг 4: $G = G^{(2)}$ тогда и только тогда, когда $G^{\Omega \setminus \Delta}$ 2-замкнута для некоторой $\Delta \in \mathrm{Orb}(G)$.

Теорема 4. *Алгоритм* CYCLOSURE *корректен и осуществляет проверку 2-замкнутости абелевых групп с циклическими транзитивными составляющими.*

§ 3.1. Вспомогательные утверждения

Далее через $\overline{G}$ будет обозначаться 2-замыкание группы G.

Лемма 3.1.1. *Если G — квазирегулярная группа подстановок множества Ω и $Z = \mathrm{Zel}(G)$, то $Z \leq \overline{G}$ и $Z^{\Delta} \trianglelefteq \overline{G}^{\Delta}$ для всех $\Delta \in \mathrm{Orb}(G)$.*

Доказательство. Для доказательства включения $Z \leq \overline{G}$ нужно показать, что $s^z = s$ для всех $s \in \mathrm{Orb}_2(G)$. Пусть Δ' и Δ'' — орбиты группы G такие, что $s \subseteq \Delta' \times \Delta''$. Группа Z

порождена подстановками z со следующим свойством: существует орбита $\Delta \in \mathrm{Orb}(Z)$ такая, что $z^\Delta \in Z^\Delta$ и $z^{\Omega\setminus\Delta} = \mathrm{id}_{\Omega\setminus\Delta}$. Поэтому если $\Delta' \neq \Delta \neq \Delta''$ или $\Delta' = \Delta = \Delta''$, то $s^z = s$ для всех $s \in \mathrm{Orb}_2(G)$. Осталось рассмотреть случай, когда $\Delta = \Delta'' \neq \Delta'$ (случай $\Delta \neq \Delta'' = \Delta'$ аналогичен). Снова по построению группы Z существует $g \in G_{\Delta'}$ такой, что

$$z^{\Delta\cup\Delta'} = g^{\Delta\cup\Delta'},$$

откуда следует $s^z = s^g = s$.

Докажем, что $Z^\Delta \trianglelefteq \overline{G}^\Delta$. Сначала отметим, что $G_{\Delta'} \trianglelefteq G$ для всех $\Delta' \in \mathrm{Orb}(G)$, откуда сразу следует, что $G^\Delta_{\Delta'} \trianglelefteq G^\Delta$. Тогда и пересечение всех $G^\Delta_{\Delta'}$, где Δ' пробегает множество $\mathrm{Orb}(G)\setminus\{\Delta\}$ тоже нормально в G^Δ. Это пересечение совпадает с Z^Δ, и учитывая, что $G^\Delta = \overline{G}^\Delta$, получаем требуемое включение. □

Лемма 3.1.2. *Если G — квазирегулярная группа подстановок множества Ω и $Z = \mathrm{Zel}(G)$, то $\overline{G}$ действует на множестве $\mathrm{Orb}(Z)$ с ядром Z и образом $\overline{G^{\mathrm{Orb}(Z)}}$.*

Доказательство. Из леммы 3.1.1 следует, что для всех $\Delta \in \mathrm{Orb}(G)$ группа $\overline{G}^\Delta$ действует на множестве $\mathrm{Orb}(Z^\Delta)$. Но это влечет, что группа $\overline{G}$ действует на объединение

$$\bigcup_{\Delta\in\mathrm{Orb}(G)} \mathrm{Orb}(Z^\Delta) = \mathrm{Orb}(Z).$$

Обозначим через $\overline{\rho}$ — гомоморфизм из $\overline{G}$ на $\overline{G}^{\mathrm{Zel}(G)}$, действующий по правилу $\overline{\rho} : g \mapsto g^{\mathrm{Zel}(G)}$.

Докажем, что $\ker(\overline{\rho}) = Z$. Очевидно, что $Z \leq K = \ker(\overline{\rho})$. Если $\Delta \in \mathrm{Orb}(G)$, то $K^\Delta = Z^\Delta$, потому что K^Δ и Z^Δ — это 1-эквивалентные подгруппы регулярной группы $\overline{G}^\Delta$. Поскольку K содержится в прямом произведении Z^Δ (а это произведение совпадает с Z), $K \leq Z$. Таким образом, $K = Z$.

Теперь докажем, что $\mathrm{im}(\overline{\rho}) = \overline{G^{\mathrm{Orb}(Z)}}$. Из леммы [43, Lemma 2.1(1)] следует, что группы $G^{\mathrm{Orb}(Z)}$ и $G^{(2)^{\mathrm{Orb}(Z)}}$ 2-эквивалентны, откуда следует, что

$$\mathrm{im}(\overline{\rho}) = \overline{G}^{\mathrm{Orb}(Z)} \leq \overline{G^{\mathrm{Orb}(Z)}}.$$

Осталось доказать, что для всех $\overline{g} \in \overline{G^{\mathrm{Orb}(Z)}}$, существует $g \in \overline{G}$ такой, что

$$\overline{\rho}(g) = \overline{g}.$$

Пусть $\Delta \in \mathrm{Orb}(G)$. Напомним, что $\overline{G}^\Delta = G^\Delta$ — регулярная группа, и по лемме 3.1.1 $Z^\Delta \trianglelefteq \overline{G}^\Delta$, откуда следует, что группа $(\overline{G}^\Delta)^{\mathrm{Orb}(Z^\Delta)}$ корректно определена, регулярна и потому 2-замкнута. Таким образом, получаем

$$\big(\overline{G^{\mathrm{Orb}(Z)}}\big)^{\overline{\Delta}} \leq \overline{(G^\Delta)^{\mathrm{Orb}(Z^\Delta)}} = \overline{(\overline{G}^\Delta)^{\mathrm{Orb}(Z^\Delta)}} = (\overline{G}^\Delta)^{\mathrm{Orb}(Z^\Delta)},$$

где $\overline{\Delta}$ — это орбита группы $\overline{G^{\mathrm{Orb}(Z)}}$ точки которой являются Z-орбитами на множестве Δ. Таким образом, для всех $\Delta \in \mathrm{Orb}(\overline{G})$, существует $g_\Delta \in \overline{G}^\Delta$ такой, что

$$\overline{\rho}_\Delta(g_\Delta) = \overline{g}^{\overline{\Delta}},$$

где $\overline{\rho}_\Delta$ — гомоморфизм из $\overline{G}^\Delta$ в $(\overline{G}^\Delta)^{\mathrm{Orb}(Z^\Delta)}$, индуцированный $\overline{\rho}$. Если произведение $g = \prod_\Delta g_\Delta$ лежит в G, то

$$\overline{\rho}(g) = \overline{\rho}(\prod_\Delta g_\Delta) = \prod_\Delta \overline{\rho}_\Delta(g_\Delta) = \prod_{\overline{\Delta}} \overline{g}^{\overline{\Delta}} = \overline{g}.$$

Итак, имеется равенство $\overline{\rho}(g) = \overline{g}$, но осталось доказать, что $g \in \overline{G}$. Пусть $s \in \mathrm{Orb}_2(G)$ и $\Delta, \Gamma \in \mathrm{Orb}(G)$ такие, что $s \subseteq \Delta \times \Gamma$. Если $\Delta = \Gamma$, то $s^g = s^{g_\Delta} = s$, потому что $g_\Delta \in \overline{G}^\Delta$. Если же $\Delta \neq \Gamma$, то из леммы 3.1.1 и определения группы Z следует, что $Z^\Delta \times Z^\Gamma \subseteq \overline{G}^{\Delta \cup \Gamma}$, и тем самым

$$(\alpha, \beta) \in s \quad \Leftrightarrow \quad \overline{\alpha} \times \overline{\beta} \subseteq s,$$

где $\overline{\alpha} = \alpha^Z$, и $\overline{\beta} = \beta^Z$. Множество $\overline{s} = \{(\overline{\alpha}, \overline{\beta}) : \ (\alpha, \beta) \in s\}$ является 2-орбитой группы $\overline{G}^{\mathrm{Orb}(Z)}$, поэтому $\overline{s}^{\overline{G}} = \overline{s}$ и

$$s^g = \big(\bigcup_{(\overline{\alpha},\overline{\beta}) \in \overline{s}} \overline{\alpha} \times \overline{\beta} \big)^g = \bigcup_{(\overline{\alpha},\overline{\beta}) \in \overline{s}} \overline{\alpha}^{\overline{g}} \times \overline{\beta}^{\overline{g}} = \bigcup_{(\overline{\alpha},\overline{\beta}) \in \overline{s}^{\,\overline{g}}} \overline{\alpha} \times \overline{\beta} = \bigcup_{(\overline{\alpha},\overline{\beta}) \in \overline{s}} \overline{\alpha} \times \overline{\beta} = s,$$

и тем самым $g \in \overline{G}$. □

§ 3.2. Доказательство теоремы 2

Пусть G — квазирегулярная группа подстановок, $Z = \mathrm{Zel}(G)$ и $\overline{\rho} : \overline{G} \to \overline{G}^{\mathrm{Zel}(G)}$ — гомоморфизм действия из леммы 3.1.2. Этот гомоморфизм индуцирует действие группы G на множестве $\mathrm{Orb}(Z)$. Обозначим гомоморфизм этого действия через ρ.

Пусть группа G 2-замкнута. Тогда из леммы 3.1.1 следует, что $Z \leq \overline{G} = G$, по лемме 3.1.2

$$G^{\mathrm{Orb}(Z)} = \overline{G}^{\mathrm{Orb}(Z)} = \mathrm{im}(\overline{\rho}) = \overline{G^{\mathrm{Orb}(Z)}}.$$

Таким образом, группа $G^{\mathrm{Orb}(Z)}$ 2-замкнута.

Пусть теперь $Z \leq G$ и группа $G^{\mathrm{Orb}(Z)}$ 2-замкнута. Учитывая лемму 3.1.2, получаем, что

$$Z \leq \ker(\rho) \leq \ker(\overline{\rho}) = Z,$$
$$\mathrm{im}(\rho) = G^{\mathrm{Orb}(Z)} = \overline{G^{\mathrm{Orb}(Z)}} = \mathrm{im}(\overline{\rho}).$$

В результате имеем, что $\ker(\rho) = \ker(\overline{\rho})$ и $\mathrm{im}(\rho) = \mathrm{im}(\overline{\rho})$, откуда следует, что

$$|G| = |\ker(\rho)| \cdot |\mathrm{im}(\rho)| = |\ker(\overline{\rho})| \cdot |\mathrm{im}(\overline{\rho})| = |\overline{G}|.$$

Учитывая, что $G \leq G^{(2)}$, получаем $\overline{G} = G$. Теорема доказана.

§ 3.3. Доказательство теоремы 3

Лемма 3.3.1. *Пусть G — квазирегулярная группа подстановок множества Ω, $\Delta \in \mathrm{Orb}(G)$ и $G^{\Delta}_{\Delta'} = 1$ для некоторой G-орбиты $\Delta' \neq \Delta$. Тогда орбита Δ несущественная.*

Доказательство. Из квазирегулярности группы G следует, что $G_{\delta'} = G_{\Delta'}$ для любой $\delta' \in \Delta'$. Это значит, что для любых $\delta, \lambda \in \Delta$ выполнено

$$(\delta', \delta) \in (\delta', \lambda)^G \quad \Rightarrow \quad \delta = \lambda. \tag{3.2}$$

Действительно, если $(\delta', \delta) = (\delta', \lambda)^g$ для некоторого $g \in G$, то $g \in G_{\delta'} = G_{\Delta'}$. Учитывая, что $G^{\Delta}_{\Delta'} = 1$, получаем $\delta = \lambda^g = \lambda$.

Пусть $\mathcal{X} = \mathrm{Inv}(G)$. Тогда из формулы 3.2 следует, что выполняются условия леммы 1.3.3 для конфигурации $\mathcal{X}$ и множества $\Omega' = \Omega \setminus \Delta$. Тогда по лемме 1.3.3 отображение ограничения из $\mathrm{Aut}(\mathcal{X})$ в $\mathrm{Aut}(\mathcal{X}_{\Omega'})$ является изоморфизмом. В частности,

$$\overline{G}^{\Omega'} = \mathrm{Aut}(\mathcal{X})^{\Omega'} = \mathrm{Aut}(\mathcal{X}_{\Omega'}) = \overline{G^{\Omega'}} \tag{3.3}$$

и $|\overline{G}| = |\overline{G^{\Omega'}}|$.

Предположим, что группа G 2-замкнута. Тогда из формулы 3.3 следует, что группа $G^{\Omega'}$ тоже 2-замкнута. Если теперь группа $G^{\Omega'}$ тоже 2-замкнута, то

$$|G| \leq |\overline{G}| = |\overline{G^{\Omega'}}| = |G^{\Omega'}| \leq |G|,$$

и потому $|G| = |\overline{G}|$, что влечет $G = \overline{G}$. □

Теперь докажем саму теорему 3. Если $\mathrm{Zel}(G) = 1$, то для для любой $\Delta \in \mathrm{Orb}(G)$ выполняется равенство

$$\bigcap_{\Delta' \neq \Delta} G^{\Delta}_{\Delta'} = 1.$$

Также по условию теоремы $G^{\Delta}_{\Delta'} \leq G^{\Delta}$ — циклическая p-группа для любой орбиты Δ' группы G, откуда следует, что $G^{\Delta}_{\Delta'} = 1$ хотя бы для одной орбиты Δ', и по лемме 3.3.1 орбита Δ несущественная.

§ 3.4. Доказательство теоремы 4

2-Замкнутость тривиальных и регулярных групп на первом шаге алгоритма легко следует из леммы 1.1.5. Второй шаг алгоритма обеспечивается теоремой 1, которая сводит проблему 2-замкнутости к случаю, когда G является p-группой. Далее, на третьем и четвертом

шаге, в зависимости от тривиальности группы $\mathrm{Zel}(G)$, проблема сводится к группе $G^{\mathrm{Orb}(\mathrm{Zel}(G))}$ (теорема 2), либо к группе $G^{\Omega\setminus\Delta}$ для произвольной орбиты Δ группы G (теорема 3). В обоих случаях уменьшается степень группы и проверка завершается не более чем через $|\Omega|$ редукций, когда на очередном шаге редукции группа G будет либо тривиальной, либо транзитивной.

4. Вполне k-замкнутые абелевы группы

Пусть k — положительное целое число. Группа A называется вполне k-замкнутой, если все ее точные подстановочные представления k-замкнуты.

По теореме о конечно порожденных абелевых группах любая нетривиальная конечная абелева группа A имеет вид

$$A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_{n(A)}}, d_1 > 1, d_i | d_{i+1}, 1 \leq i < n(A),$$

где $n(A)$ — количество инвариантных множителей группы G. Также обозначим $N(A) = \sum_{P \in \mathrm{Syl}(A)} n(P)$.

В данной главе будут доказаны следующие две теоремы.

Теорема 5. *Пусть A — нетривиальная конечная абелева p-группа и $n = n(A)$. Тогда группа A вполне $(n+1)$-замкнута, но не вполне n-замкнута.*

Следствие 1. *Для любого натурального числа k, для любого простого числа p существует бесконечно много вполне k-замкнутых, но не вполне $(k-1)$-замкнутых абелевых p-групп.*

Теорема 6. *Пусть A — нетривиальная конечная абелева группа и $n = n(A)$. Тогда группа A вполне $(n+1)$-замкнута, но не вполне n-замкнута.*

§ 4.1. Вспомогательные утверждения

Если $G \leq \mathrm{Sym}(\Omega)$, то *базовым числом* $b(G)$ группы G называется минимальное число b такое, что существуют $\alpha_1, \ldots, \alpha_b \in \Omega$ такие, что $G_{\alpha_1 \ldots \alpha_b} = 1$. Множество $\{\alpha_1, \ldots, \alpha_b\}$ называется *базой* группы G.

Лемма 4.1.1. *Конечная группа вполне 1-замкнута тогда и только тогда, когда она тривиальна.*

Доказательство. Предположим, что A — конечная вполне 1-замкнутая группа. Рассмотрим $G \leq \mathrm{Sym}(A)$ регулярное представление группы A. Группа G транзитивна, поэтому $G^{(1)} = \mathrm{Sym}(A)$, а значит $G = \mathrm{Sym}(A)$. Симметрическая группа регулярна только при $|A| \leq 2$. Случай $|A| \leq 2$ не подходит, потому что в этом случае $A \cong \mathbb{Z}_2$, а эта группа не вполне 1-замкнута ввиду существования не 1-замкнутого точного подстановочного представления $\mathbb{Z}_2 \cong \langle (1,2)(3,4) \rangle$. Таким образом, $A = 1$. Обратная импликация очевидна. □

Лемма 4.1.2. *Если A — абелева группа, то базовое число любого точного подстановочного представления группы A не превосходит $N(A)$ и эта оценка точна.*

Доказательство. Если группу A представить в виде $A = \prod_{P \in \mathrm{Syl}(A)} P$, а потом каждую силовскую подгруппу в этом разложении разложить по теореме о конечно порожденных абелевых группах, то получится разложение вида $A = B_1 \times \ldots \times B_{N(A)}$, где все множители являются циклическими p-группами.

Пусть группа A действует точно на множестве Ω. Доказательство будет вестись индукцией по числу $N(A)$. Имеем $B_1 = \langle b_1 \rangle \cong \mathbb{Z}_{p^a}$ для некоторого простого число p и целого положительного a, и для любого $\alpha \notin \mathrm{Fix}(b_1^{p^{a-1}})$ будет выполняться $A_\alpha \cap B_1 = 1$. Если $N(A) = 1$, то $A = B_1$ — циклическая p-группа, и $A_\alpha = 1$, откуда следует, что $\{\alpha\}$ — база группы A.

Пусть теперь $N(A) \geq 2$. Поскольку $A_\alpha \cap B_1 = 1$, $A_\alpha \cong (A_\alpha B_1)/B_1 \leq A/B_1 \cong \prod_{i=2}^{N(A)} B_i$, откуда следует, что $N(A_\alpha) \leq n - 1 = N(A) - 1$. По индукции для группы A_α существует база $\{\alpha_1, \ldots, \alpha_s\} \subseteq \Omega \setminus \{\alpha\}$ размера $s \leq N(A) - 1$. Тогда $\{\alpha_1, \ldots, \alpha_s, \alpha\}$ — база группы A размера не более чем $N(A)$.

Покажем точность этой оценки. Пусть для всех $i = 1 \ldots N(A)$ группа B_i действует на себя умножением справа. Такое действие регулярно, и тем самым $b(B_i) = 1$. Тогда A действует точно на множестве $\Omega := \bigcup_{i=1}^{N(A)} B_i$, и в этом действии справедливо равенство $b(A) = \sum_{i=1}^{N(A)} b(B_i) = N(A)$. □

§ 4.2. Доказательство теоремы 5

Пусть A — нетривиальная абелева p-группа и $G \leq \mathrm{Sym}(\Omega)$ — точное подстановочное представление группы A. Из леммы 4.1.2 следует, что $b(G) \leq N(A) = n(A) = n$, и по лемме 1.1.5 группа G $(n+1)$-замкнута. Из произвольности представления G следует, что группа A вполне $(n+1)$-замкнута.

Теперь построим не n-замкнутое точное подстановочное построение группы A. Напомним, что

$$A \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \ldots \times \mathbb{Z}_{d_n}, d_1 > 1, d_i | d_{i+1}, 1 \leq i < n.$$

Пусть Ω — множество из $d_1 + \sum_{i=1}^{n} d_i$ элементов и $\tau_0, \tau_1, \ldots, \tau_n$ — попарно независимые циклы на Ω с длинами $|\tau_0| = d_1$, и $|\tau_i| = d_i$ для всех $i = 1, \ldots, n$. Также положим $G_1 = \langle \tau_0 \tau_1 \rangle$ и $G_i = \langle \tau_0^{-1} \tau_i \rangle$ для $i = 2, \ldots, n$, и

$$G = \langle G_1, \ldots, G_n \rangle.$$

Утверждается, что G — точное подстановочное представление группы A. Действительно,

группы G_i коммутируют, и индукцией по n легко видеть, что

$$G_i \cap \langle G_1, \ldots, G_{i-1}, G_{i+1}, \ldots, G_n \rangle = 1, \text{ for } i = 1, \ldots, n.$$

Таким образом, $G = G_1 \times \ldots \times G_n$, $G_i \cong \mathbb{Z}_{d_i}$ для всех $i = 1, \ldots, n$.

Теперь покажем, что $\tau_0 \in G^{(n)}$. Пусть $(\alpha_1, \ldots, \alpha_n) \in \Omega^n$, и пусть $\Delta_i = \mathrm{supp}(\tau_i)$ для всех $i = 0, \ldots, n$. Более того, $\{\Delta_0, \ldots, \Delta_n\} = \mathrm{Orb}(G)$. Поскольку G имеет $n+1$ орбит, существует $k \in \{0, \ldots, n\}$, такое, что $\Delta_k \cap \{\alpha_1, \ldots, \alpha_n\} = \varnothing$. Определим подстановку τ следующим образом:

$$\tau = \begin{cases} 1, & \text{если } k = 0, \\ \tau_0 \tau_k^{-1}, & \text{если } 1 \leq k \leq n. \end{cases}$$

По построению $\tau \in G$. Если $\tau = 1$, то и $\alpha_i^\tau = \alpha_i^{\tau_0} = \alpha_i$ для всех $i = 0, \ldots, n$. Если $\tau = \tau_0 \tau_k^{-1}$ для некоторого k, то подстановки τ и τ_0 действуют одинаково на множестве $\Omega \setminus \Delta_k$, и $\alpha_i^\tau = \alpha_i^{\tau_0}$. Таким образом, из леммы 1.1.1 следует, что $\tau_0 \in G^{(n)}$. По построению группы G, $\tau_0 \notin G$, и тогда $G \neq G^{(n)}$.

§ 4.3. Доказательство теоремы 6

Пусть A — нетривиальная абелева группа, $n = n(A)$ и $G \leq \mathrm{Sym}(\Omega)$ — точное подстановочное представление группы A. Поскольку $n = \max_{P \in \mathrm{Syl}(G)} n(P)$, каждая силовская подгруппа P группы G является $(n+1)$-замкнутой по теореме 5, и по теореме 1 группа A тоже $(n+1)$-замкнута. Таким образом, группа A вполне $(n+1)$-замкнута.

Покажем, что группа A не вполне n-замкнута. Если $n = 1$, то по лемме 4.1.1 группа A не вполне 1-замкнута. Поэтому далее считаем, что $n \geq 2$. Снова вспомним, что $n = \max_{P \in \mathrm{Syl}(A)} n(P)$, и пусть этот максимум достигается на группе $Q \in \mathrm{Syl}(A)$, т. е. $n(Q) = n$. По теореме 5 группа Q не вполне n-замкнута, т. е. существует множество Ω_Q такое, что Q действует точно на Ω_Q, и в этом действии группа Q не n-замкнутая группа.

Если $A = Q$, то теорема доказана. В противном случае пусть любая группа $P \in \mathrm{Syl}(A) \setminus \{Q\}$ действует на $\Omega_P = P$ регулярно умножением справа. Таким образом, группа A действует точно на множестве $\Omega = \bigcup_{P \in \mathrm{Syl}(A)} \Omega_P$. Из теоремы 1 следует, что в этом действии n-замыкание группы A имеет вид

$$A^{(n)} = \prod_{P \in \mathrm{Syl}(A)} P^{(n)} = Q^{(n)} \times \prod_{P \in \mathrm{Syl}(A) \setminus \{Q\}} P^{(n)},$$

и не совпадает с A, потому что $Q^{(n)} > Q$ по построению и $P^{(n)} = P$ ввиду регулярности группы P. В итоге, группа A не вполне n-замкнута.

5. Замыкания $\frac{3}{2}$-транзитивных групп

В данной главе изучаются k-замыкания $\frac{3}{2}$-транзитивных групп подстановок и связанные с ними конструкции. Сначала мы построим полиномиальный алгоритм, позволяющий находить 2-замыкание произвольной $\frac{3}{2}$-транзитивной группы подстановок.

Теорема 7. *Проблема 2-замыкания для $\frac{3}{2}$-транзитивной группы подстановок степени n может быть решена за время полиномиальное от n.*

Мы используем стандартный набор полиномиальных алгоритмов из [45]. В частности, мы считаем, что группы на входе и выходе нашего алгоритма заданы порождающими множествами размера, полиномиального от их степени. Также применение классификации $\frac{3}{2}$-транзитивных групп [30, следствие 3] позволяет доказать, что каждая такая группа, не являющаяся дважды транзитивной, либо 2-замкнута, либо вкладывается в группу ограниченного полиномом от n порядка, которую можно эффективно построить. Более того, учитывая включения $G \leq G^{(k)} \leq G^{(2)}$ (для $k \geq 2$) из леммы 1.1.4, получаем что в описанной ситуации общая проблема k-замыкания тоже может быть решена за то же время.

Следствие 2. *Для каждого положительного целого числа k проблема k-замыкания для $\frac{3}{2}$-транзитивной группы подстановок, не являющейся дважды транзитивной, может быть решена за время полиномиальное от ее степени.*

Теперь перейдем к когерентным конфигурациям. Напомним, что когерентная конфигурация называется $\frac{3}{2}$-однородной, если она однородна и все ее базисные отношения за исключением диагонального равномощны. Таким образом, схема $\frac{3}{2}$-транзитивной группы G — это в точности шурова $\frac{3}{2}$-однородная когерентная конфигурация $\mathrm{Inv}(G)$, поэтому на комбинаторном языке результат теоремы 7 может быть сформулирован так: группу автоморфизмов цветной шуровой $\frac{3}{2}$-однородной когерентной конфигурации $\mathcal{X}$ можно найти за полиномиальное время (при этом предполагается, что предъявлен сертификат шуровости схемы $\mathcal{X}$, т. е. группа G, для которой $\mathcal{X} = \mathrm{Inv}(G)$). Естественным продолжением здесь выглядит вопрос об изоморфизме таких конфигураций. Более точно, если мы обозначим через ψ некоторую биекцию между $\mathrm{Orb}_2(G)$ и $\mathrm{Orb}_2(G')$, а через $\mathrm{Iso}(\mathrm{Inv}(G), \mathrm{Inv}(G'), \psi)$ — множество всех подстановок f из Ω таких, что $s^f = s^\psi$ для всех $s \in \mathrm{Orb}_2(G)$, то соответствующая проблема формулируется следующим образом.

Проблема изоморфизма цветных шуровых когерентных конфигураций. Для групп G и G' подстановок конечного множества Ω и биекции ψ между $\mathrm{Orb}_2(G)$ и $\mathrm{Orb}_2(G')$ найти множество $\mathrm{Iso}(\mathrm{Inv}(G), \mathrm{Inv}(G'), \psi)$.

Ясно, что если множество $\mathrm{Iso}(\mathrm{Inv}(G), \mathrm{Inv}(G'), \psi)$ не пусто, то оно образует смежный класс в симметрической группе $\mathrm{Sym}(\Omega)$ по подгруппе

$$G^{(2)} = \mathrm{Aut}(\mathrm{Inv}(G)) = \mathrm{Iso}(\mathrm{Inv}(G), \mathrm{Inv}(G), \mathrm{id}),$$

где id — тождественное отображение множества $\mathrm{Orb}_2(G)$ на себя. Поэтому решение данной проблемы по модулю решенной проблемы 2-замыкания сводится к тому, чтобы либо найти подстановку из $\mathrm{Sym}(\Omega)$, сопрягающую $G^{(2)}$ и $(G')^{(2)}$, либо доказать, что ее нет. Оказывается, что в случае схем $\frac{3}{2}$-транзитивных групп это также можно сделать за полиномиальное время, поэтому верна следующая

Теорема 8. *Проблема изоморфизма цветных шуровых $\frac{3}{2}$-однородных когерентных конфигураций на n точках может быть решена за время, полиномиальное от n.*

Последний результат данной главы теоретический и посвящен группам автоморфизмов циклотомических схем над конечными почти-полями. Напомним, что группа автоморфизмов $\mathrm{Aut}(\mathrm{Cyc}(\mathbb{K}, K))$ циклотомической схемы над почти-полем совпадает с 2-замыканием $\frac{3}{2}$-транзитивной группой Фробениуса $G(\mathbb{K}, K)$ (см. § 1.4).

Теорема 9. *Пусть $\mathbb{K}$ — конечное почти-поле, K — собственная подгруппа группы $\mathbb{K}^\times$ и $\mathcal{C} = \mathrm{Cyc}(\mathbb{K}, K)$ — циклотомическая схема над почти-полем $\mathbb{K}$ с базисной группой K. Тогда выполняется одно из следующих утверждений.*

1. *$\mathbb{K}$ — почти-поле Диксона и $\mathrm{Aut}(\mathcal{C}) \leq \mathrm{A\Gamma L}(1, |\mathbb{F}|)$, где $\mathbb{F}$ — поле, ассоциированное с $\mathbb{K}$.*

2. *$\mathbb{K}$ — почти-поле Диксона порядка 7^2, $K = \langle a, b\rangle \cong 3 \times Q_8$ и $\mathrm{Aut}(\mathcal{C}) = \mathbb{K}^+ \rtimes H$, где $H = \langle K, c\rangle \cong 3 \times \mathrm{SL}(2,3)$, и действие a, b и c на $\mathbb{K}^+$ представлено матрицами*

$$\begin{pmatrix} 2 & 2 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} 0 & -2 \\ -1 & 0 \end{pmatrix} \text{ и } \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

3. *$\mathbb{K}$ — почти-поле Цассенхауза, K — подгруппа группы M, где M — максимальная разрешимая подгруппа группы $\mathbb{K}^\times$, и $\mathrm{Aut}(\mathcal{C})$ — подгруппа группы $\mathbb{K}^+ \rtimes H$, где $K \leq M \leq H$. Группы $\mathbb{K}^+$, M, H и порождающие групп M и H приведены в таблице 2 в приложении.*

4. $\mathbb{K}$ — *почти-поле Цассенхауза порядка* 29^2 *или* 59^2, $K \cong \mathrm{SL}(2,5)$ *и* $\mathrm{Aut}(\mathcal{C}) = \mathbb{K}^+ \rtimes H$, *где* $H = \mathrm{SL}(2,5) \rtimes 2$ *или* $H = \mathrm{SL}(2,5)$ *соответственно. Группы* $\mathbb{K}^+$, K, H *и порождающие групп* K *и* H *приведены в таблице* 3 *в приложении.*

В частности, если базисная группа K *разрешима, то группа* $\mathrm{Aut}(\mathcal{C})$ *тоже разрешима.*

§ 5.1. Доказательство теоремы 7

Можно считать, что группа G подстановок множества Ω на входе наших алгоритмов задана порождающим множеством размера, полиномиального от ее степени n. Это означает, что за время $\mathrm{poly}(n)$ можно проверить является ли группа G дважды транзитивной, примитивной (см., например, [45]), а также построить схему $\mathcal{X} = \mathrm{Inv}(G)$ группы G.

Мы можем проверить, является ли мощность n множества Ω степенью p^d простого числа p, и, если является, то построить подгруппу $H \leq \mathrm{Sym}(\Omega)$, изоморфную $\mathrm{A\Gamma L}(1, p^d)$ или $\mathrm{AS}_0(p^d)$, цоколь V которой действуют регулярно на Ω. В данном случае построить означает, что мы можем предъявить все элементы H, так как ее порядок, очевидно, ограничен полиномом от n.

Если H — подмножество в $\mathrm{Sym}(\Omega)$, мощность которого ограничена полиномом от n, то все автоморфизмы когерентной конфигурации $\mathcal{X}$ (все изоморфизмы между конфигурациями $\mathcal{X}$ и $\mathcal{X}'$) на множестве Ω, которые лежат в H, могут быть найдены полным перебором за время $\mathrm{poly}(n)$. Поэтому за полиномиальное от n время можно найти множества $G^{(2)} \cap H$ и $\mathrm{Iso}(\mathrm{Inv}(G), \mathrm{Inv}(G')) \cap H$. Для удобства мы обозначим результаты работы двух последних алгоритмов через $\mathrm{BFC}(G; H)$ и $\mathrm{BFI}(\mathrm{Inv}(G), \mathrm{Inv}(G'); H)$ соответственно.

Следующий алгоритм решает проблему 2-замыкания для $\frac{3}{2}$-транзитивных групп подстановок.

Алгоритм **TWOCLOSURE**

Вход: G — $\frac{3}{2}$-транзитивная группа подстановок множества Ω степени n.

Выход: $G^{(2)}$.

Описание алгоритма

Шаг 1: Если $n \leq 13^4$, то выход $\mathrm{BFC}(G; \mathrm{Sym}(\Omega))$.

Шаг 2: Если G дважды транзитивна, то выход $\mathrm{Sym}(\Omega)$.

Шаг 3: Если G примитивна и $n = p^d$ — степень простого числа, то зафиксируем некоторую точку $\omega \in \Omega$ и найдем все 2-элементные подмножества T, порождающие группу G.

Шаг 4: Построим $H \leq \mathrm{Sym}(\Omega)$, изоморфную группе Пассмана $\mathrm{AS}_0(p^d)$. Для каждого 2-элементного подмножества T, порождающего G, каждого 2-элементного подмножества T' из H, каждой биекции $\psi : T \to T'$ и каждой точки $\omega' \in \Omega$ выполним алгоритм

$$\mathrm{IMBED}((G,T),(H,T'),\psi,(\omega,\omega')).$$

Если найдется подстановка $x = \mathrm{IMBED}((G,T),(H,T'),\psi,(\omega,\omega'))$, то выход

$$\mathrm{BFC}(G^x;H)^{x^{-1}}.$$

Шаг 5: Построим $H \leq \mathrm{Sym}(\Omega)$, изоморфную группе $\mathrm{A\Gamma L}(1,p^d)$. Для каждого 2-элементного подмножества T, порождающего G, каждого 2-элементного подмножества T' из H, каждой биекции $\psi : T \to T'$ и каждой точки $\omega' \in \Omega$ выполним алгоритм

$$\mathrm{IMBED}((G,T),(H,T'),\psi,(\omega,\omega')).$$

Для всех подстановок $x = \mathrm{IMBED}((G,T),(H,T'),\psi,(\omega,\omega'))$, если они существуют, найдем

$$K(x) = \mathrm{BFC}(G^x;H).$$

Выберем ту подстановку, для которой порядок группы $K(x)$ максимален. Обозначим эту подстановку через y, и выход $K(y)^{y^{-1}}$.

Шаг 6: Выход G.

Лемма 5.1.1. *Алгоритм* TWOCLOSURE *корректен и время его работы не превосходит* $\mathrm{poly}(n)$.

Доказательство. Корректность алгоритма вытекает из лемм 1.2.10 и 1.5.4. Действительно, после шага 1 можно считать, что степень группы G, больше 13^4. Предположим, что $G \neq G^{(2)}$.

После шага 2 в силу леммы 1.2.10 можно полагать, что G — унипримитивная группа, степень которой является степенью p^d простого числа. Лемма 1.2.6 влечет 2-порожденность группы G, что гарантирует корректность на шаге 3. Поскольку G не дважды транзитивна, выполняется либо пункт 2 леммы 1.2.10, т. е. $G \leq G^{(2)} \cong \mathrm{AS}_0(p^d)$, либо пункт 3, т. е. $G \leq G^{(2)} \cong K \leq \mathrm{A\Gamma L}(1,p^d)$. Заметим, что если аффинные подгруппы группы $\mathrm{Sym}(\Omega)$, т. е. подгруппы, содержащие нормальную регулярную элементарную абелеву подгруппу, изоморфны, то они сопряжены в $\mathrm{Sym}(\Omega)$. Последний факт вытекает из очевидной сопряженности изоморфных регулярных подгрупп в симметрической группе и эквивалентности естественного действия стабилизатора точки на Ω его действию сопряжениями на нормальной регулярной подгруппе

(см., например, [37, предл. 4.2]). Таким образом, если выполнен пункт 2 леммы 1.2.10, то найдется подстановка $x \in \mathrm{Sym}(\Omega)$, для которой $(G^{(2)})^x = H$, где H — подгруппа, построенная на шаге 4, и эта подстановка будет найдена с помощью алгоритма IMBED, корректность которого обеспечена леммой 1.5.4.

Если выполнен пункт 3 леммы 1.2.10, т. е. среди всех подстановок x из $\mathrm{Sym}(\Omega)$ со свойством $G^x \le H \cong \mathrm{A\Gamma L}(1, p^d)$, где H — подгруппа, изоморфная группе $\mathrm{A\Gamma L}(1, p^d)$ и построенная на шаге 5 (эти подстановки снова ищутся с помощью алгоритма IMBED), можно выбрать такую подстановку y, для которой $K = K(y) = (G^y)^{(2)} = (G^{(2)})^y \le H$. Тогда для остальных x будет выполнено $K(x) = (G^x)^{(2)} \cap H \le K$, а значит, K имеет максимальный порядок среди всех $K(x)$, найденных нами на шаге 5.

Наконец, если подстановок x с указанным свойством не нашлось, то ни один из пунктов леммы 1.2.10 не выполняется, а значит, группа $G = G^{(2)}$ будет найдена на шаге 6 алгоритма.

Оценим время работы алгоритма. Число операций на шаге 1, очевидно, не превосходит некоторой константы. Проверка дважды транзитивности на шаге 2, как и примитивности на шаге 3, полиномиальна от n. Лемма 1.2.5 гарантирует что порядок группы G, а значит и число 2-элементных подмножеств T, порождающих G ограничено полиномом от n. Наконец, на шагах 4 и 5 мы применяем полиномиальный алгоритм IMBED, причем количество применений этого алгоритма ограничено полиномом от порядков групп G и H, которые в свою очередь полиномиальны от n. □

§ 5.2. Доказательство теоремы 8

Любая нетривиальная система импримтивности группы G на Ω задает отношение эквивалентности на $\Omega \times \Omega$, отличное от 1_Ω и Ω^2. Поэтому группы G и $G^{(2)}$ примитивны или импримитивны одновременно. Следовательно, в силу леммы 1.5.3, чтобы доказать теорему 3, достаточно рассмотреть случай, когда группы G и G' примитивны. Как уже говорилось во введении, в случае примитивных групп мы можем сделать даже больше. А именно, с помощью нижеследующего алгоритма **ISO** мы можем найти множество $\mathrm{Iso}(\mathcal{X}, \mathcal{X}')$ всех (не только сохраняющих цвета) изоморфизмов между схемами $\mathcal{X} = (\Omega, S) = \mathrm{Inv}(G)$ и $\mathcal{X}' = (\Omega', S') = \mathrm{Inv}(G')$.

Алгоритм **ISO**

Вход: G и G' — $\frac{3}{2}$-транзитивные примитивные группы подстановок множества Ω степени n.

Выход: множество $\mathrm{Iso}(\mathrm{Inv}(G), \mathrm{Inv}(G'))$.

Описание алгоритма

Шаг 1: Если $n \leq 13^4$, то выход $\mathrm{BFI}(\mathrm{Inv}(G), \mathrm{Inv}(G'); \mathrm{Sym}(\Omega))$.

Шаг 2: Найдем $G^{(2)} = \mathrm{TWOCLOSURE}(G)$ и $(G')^{(2)} = \mathrm{TWOCLOSURE}(G')$.

Шаг 3: Если $G^{(2)} = (G')^{(2)} = \mathrm{Sym}(\Omega)$, то выход $\mathrm{Sym}(\Omega)$.

Шаг 4: Если $|G^{(2)}| = |(G')^{(2)}|$, то зафиксируем $\omega \in \Omega$ и выход

$$\{x \in \mathrm{Sym}(\Omega) \mid x = \mathrm{IMBED}((G^{(2)}, T), ((G')^{(2)}, T'), \tau, (\omega, \omega'))\},$$

где T пробегает все 2-элементные множества, порождающие $G^{(2)}$, T' — все 2-элементные множества, порождающие $(G')^{(2)}$, τ — все биекции из T в T', и ω' — все элементы из Ω.

Шаг 5: Выход $\varnothing$.

Нам осталось доказать следующее

Лемма 5.2.1. *Алгоритм* ISO *корректен и за время, не превосходящее* $\mathrm{poly}(n)$, *находит множество* $\mathrm{Iso}(\mathrm{Inv}(G), \mathrm{Inv}(G'))$.

Доказательство. Как и в предыдущем случае, мы можем считать, что $n > 13^4$. Группы $G^{(2)}$ и $(G')^{(2)}$, в силу леммы 5.1.1 корректно и за полиномиальное время найденные на шаге 2, являются полными группами автоморфизмов схем $\mathcal{X} = \mathrm{Inv}(G)$ и $\mathcal{X}' = \mathrm{Inv}(G')$. Если группа G дважды транзитивна, то схема $\mathcal{X}$ имеет ранг 2, поэтому она изоморфна схеме $\mathcal{X}'$ группы G' тогда и только тогда, когда G' дважды транзитивна. В этом случае любая подстановка из $\mathrm{Sym}(\Omega)$ является требуемым изоморфизмом. Поэтому далее мы считаем, что G и G' унипримитивны, а значит, группы $G^{(2)}$ и $(G')^{(2)}$ являются 2-порожденными и их порядки полиномиальны от n. В частности, несложно проверить, верно ли равенство $|G^{(2)}| = |(G')^{(2)}|$, которое, очевидно, является необходимым условием того, что множество $\mathrm{Iso}(\mathcal{X}, \mathcal{X}')$ не пусто.

Заметим, что подгруппа $\mathrm{Iso}(\mathcal{X}, \mathcal{X})$ — это нормализатор в $\mathrm{Sym}(\Omega)$ группы $\mathrm{Aut}(\mathcal{X}) = G^{(2)}$, то же верно и для схемы $\mathcal{X}'$ группы G'. Поэтому для $x \in \mathrm{Sym}(\Omega)$ из равенства $(G^{(2)})^x = (G')^{(2)}$ следует равенство $\mathrm{Iso}(\mathcal{X}, \mathcal{X})^x = \mathrm{Iso}(\mathcal{X}', \mathcal{X}')$. Как несложно проверить, множество всех подстановок x, сопрягающих $\mathrm{Iso}(\mathcal{X}, \mathcal{X})$ с $\mathrm{Iso}(\mathcal{X}', \mathcal{X}')$, совпадает с искомым множеством $\mathrm{Iso}(\mathcal{X}, \mathcal{X}')$. С другой стороны, подстановка $x \in \mathrm{Iso}(\mathcal{X}, \mathcal{X}')$, переводящая $\mathcal{X}$ в $\mathcal{X}'$, сопрягает группы автоморфизмов этих схем, т. е. сопрягает $G^{(2)}$ с $(G')^{(2)}$ в $\mathrm{Sym}(\Omega)$. Таким образом, искомое множество совпадает с множеством всех подстановок, сопрягающих $G^{(2)}$ с $(G')^{(2)}$, которое стоит в правой части равенства на шаге 4. Оно находится корректно и за полиномиальное время в силу

леммы 1.5.4 и того факта, что размеры множеств всех T, T', τ и ω', определенных на том же шаге, ограничены функцией $\mathrm{poly}(n)$. $\square$

Для завершения доказательства теоремы 8 осталось заметить, что, зная все изоморфизмы между двумя когерентными конфигурациями, несложно проверить, какие из них сохраняют цвета.

§ 5.3. Доказательство теоремы 9

Пусть $\mathbb{K}$ — конечное почти-поле порядка q, $q = p^d$, где p — простое число, K — собственная подгруппа группы $\mathbb{K}^\times$, $G = G(\mathbb{K}, K)$, и $\mathcal{C} = \mathrm{Cyc}(\mathbb{K}, K)$.

Напомним, что $\mathrm{Aut}(\mathcal{C}) = G^{(2)}$. По лемме 1.4.5 и G, и $G^{(2)}$ $\frac{3}{2}$-транзитивны, и они не могут быть 2-транзитивными из-за того, что $K \neq \mathbb{K}^\times$. Далее по лемме 1.2.12 получаем, что $\mathrm{Soc}(G^{(2)}) = \mathrm{Soc}(G) \cong \mathbb{K}^+$, а значит группы $G = \mathbb{K}^+ \rtimes K$ и $G^{(2)} = \mathbb{K}^+ \rtimes H$ аффинны, где $K, H \leq \mathrm{GL}(V_\mathbb{K})$ и группы K и H $\frac{1}{2}$-транзитивны на $\mathbb{K}^+ \setminus \{0\}$. Более того, $K \leq H$ ввиду $G \leq G^{(2)}$.

Из леммы 1.4.1 следует, что $\mathbb{K}$ либо почти-поле Диксона, либо почти-поле Цассенхауза. Рассмотрим отдельно каждую ситуацию.

Пусть $\mathbb{K}$ — почти-поле Диксона, соответствующее паре Диксона (q_0, n), где $q_0 = p^l$, $\mathbb{F}_0$ — центральное подполе почти-поля $\mathbb{K}$ порядка q_0, и $\mathbb{F}$ — поле порядка q, ассоциированное с $\mathbb{K}$. Мы покажем, что почти всегда $\mathrm{Aut}(\mathcal{C}) = G^{(2)} \leq \mathrm{A\Gamma L}(1, q)$. Заметим, что если группа G импримитивна, то $G^{(2)}$ — группа Фробениуса по лемме 1.2.1, которая всегда 2-замкнута ввиду леммы 1.2.8, и из леммы 1.4.2 следует, что $G^{(2)} \leq \mathrm{A\Gamma L}(1, q)$.

Далее считаем группу G примитивной. Мы также можем предполагать, что группа K неабелева, потому что в противном случае включение $G^{(2)} \leq \mathrm{A\Gamma L}(1, q)$ легко следует из лемм 1.4.3 и 1.4.4. В частности, мы также можем считать, что $\mathbb{K}$ не является полем, т.е. $q_0 < q$, и $n > 1$.

Включение $G^{(2)} \leq \mathrm{A\Gamma L}(1, q)$ имеет место тогда и только тогда, когда $H \leq \Gamma\mathrm{L}(1, q)$. Поскольку H действует $\frac{1}{2}$-транзитивно на $\mathbb{K}^+ \setminus \{0\}$, группа H — $\frac{1}{2}$-транзитивная группа из леммы 1.2.2. Рассмотрим имеющиеся возможности.

1. Если H транзитивна на $V^\sharp$, то $G^{(2)}$, а значит и G, дважды транзитивны, но такое возможно только в случае $K = \mathbb{K}^\times$, что противоречит выбору K.

2. Если $H \leq \Gamma\mathrm{L}(1, q)$, то доказывать нечего.

3. Если H — дополнение Фробениуса, действующее полурегулярно на $V^\sharp$, то $G^{(2)}$ — группа Фробениуса, и из лемм 1.1.8 и 1.4.2 следует, что $\mathrm{Aut}(\mathcal{C}) = G^{(2)} = G \leq \mathrm{A\Gamma L}(1, q)$, что

и требовалось.

4. Пусть $H = \mathrm{S}_0(u) \leq \mathrm{GL}(2,u)$, $u = p^c$, $q = u^2$, и p — нечетное число. Разрешимая группа H порядка $4(u-1)$ может быть представлена следующим образом [39] (как подгруппа группы $\mathrm{GL}(2,p^c)$):

$$H = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \pm\alpha^{-1} \end{pmatrix}, \begin{pmatrix} 0 & \alpha \\ \pm\alpha^{-1} & 0 \end{pmatrix} \;\middle|\; \alpha \in \mathbb{F}_u^\times \right\}.$$

Легко видеть, что каждая нетривиальная орбита группы H на $\mathbb{K}^+$ длины $2(u-1)$.

Поскольку K — дополнение Фробениуса, действующее полурегулярно на $\mathbb{K}^+$, группа K оказывается собственной подгруппой группы H порядка $2(u-1)$, которая не содержит элемент

$$t = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Поскольку $t \in H$, векторы $(1,0),(0,1) \in \mathbb{K}^+$ лежат в одной орбите группы H, поэтому группа K содержит элементы

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } -s.$$

Получается, что группа K может быть представлена следующим образом:

$$K = \left\langle \begin{pmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle,$$

где θ — порождающий элемент группы $\mathbb{F}_u^\times$.

Если $u = p = 3$, то $q = 9$ и K — циклическая группа порядка 4, и потому $G^{(2)} \leq \mathrm{A\Gamma L}(1,\mathbb{F})$. Поэтому далее считаем, что $q > 9$, откуда K неабелева с центром порядка 2.

Напомним, что $|\mathbb{F}_0| = q_0$, поэтому $|Z(\mathbb{K}^\times)| = q_0 - 1 = p^l - 1$. Предположим, что r — нечетное простое число, делящее $p^{(l,c)} - 1 = (q_0 - 1, u - 1)$. Тогда $(u-1)_r = (q-1)_r$, и тогда силовская r-подгруппа группы K является силовской и для $\mathbb{K}^\times$. Поскольку $Z(K) \geq K \cap Z(\mathbb{K}^\times)$, получается, что r делит $|Z(K)|$, чего не может быть. Итак, p — число Ферма и $(l,c) = 1$ или $p = 3$ и $(l,c) = 2$.

Если $p > 3$ или $(l,c) = 2$, то 4 делит $u-1$, поэтому $2(u-1)_2 = (q-1)_2$, и силовская 2-подгруппа K является силовской 2-подгруппой $\mathbb{K}^\times$. Из этого следует, что $|Z(K)|$ кратно 4, что есть противоречие. Таким образом, $p = 3$ и $(l,c) = 1$. Вместе с равенствами $3^{ln} = q_0^n = q = u^2 = 3^{2c}$ это оставляет нам две возможности: либо $l = 1$ и $n = 2c$, либо $l = 2$ и $n = c$. Принимая во внимание, что (q_0, n) является парой Диксона, получаем, что $l = 1$ и $n = 2$, а значит и $q = 9$, что есть противоречие.

5. Группа H разрешима, и $q \in \{3^2, 3^4, 5^2, 7^2, 11^2, 17^2\}$.

Проверим включение $\mathrm{Aut}(\mathcal{C}) \leq \mathrm{A\Gamma L}(1,q)$. Как упоминалось выше, это всегда верно, когда K абелева, поэтому мы можем ограничиться случаем неабелевых базисных групп. Более того, если включение справедливо для всех максимальных подгрупп группы $\mathbb{K}^\times$, то оно справедливо для всех собственных подгрупп группы $\mathbb{K}^\times$ с учетом леммы 1.1.3. Поскольку у нас есть только конечное число возможностей для $\mathbb{K}$, мы прибегнем к компьютерным вычислениям.

Используя MAGMA [14], мы построим группу $\mathbb{K}^+ \rtimes \mathbb{K}^\times$. Затем, применяя к полученным группам пакет IRREDSOL для GAP [44], мы получим группу $\mathbb{K}^\times$ как группу линейных преобразований пространства $V_{\mathbb{K}}$. Далее, с помощью GAP мы построим группу $Q \leq \mathrm{GL}(V_{\mathbb{K}})$ такую, что $Q \cong \Gamma\mathrm{L}(1,q)$ и $\mathbb{K}^\times \leq Q$. Затем мы находим все (с точностью до сопряжения) неабелевы максимальные подгруппы M группы $\mathbb{K}^\times$ и для каждого такого M строим группу перестановок $\mathbb{K}^+ \rtimes M$. Наконец, используя пакет COCO для GAP, мы находим 2-замыкание группы $\mathbb{K}^+ \rtimes M$ и проверяем включение этого 2-замыкания в $\mathbb{K}^+ \rtimes Q$.

Пусть $|\mathbb{K}| = 3^2$. Существует только одно почти-поле Диксона такого порядка, и оно соответствует паре Диксона $(3,2)$. В этом случае $\mathbb{K}^\times \cong Q_8$. Все максимальные подгруппы Q_8 являются абелевыми, поэтому для каждой правильной подгруппы $\mathbb{K}^\times$ выполняется включение $\mathrm{Aut}(\mathcal{C}) \leq \mathrm{A\Gamma L}(1,9)$.

Предположим, $|\mathbb{K}| = 3^4$. Поскольку $(3,4)$ не является парой Диксона, опять же, существует только одно поле Диксона $\mathbb{K}$ такого порядка, и оно соответствует паре $(9,2)$. В этом случае $\mathbb{K}^\times \cong 5 \rtimes 16$ и все максимальные подгруппы $\mathbb{K}^\times$ являются абелевыми.

Поскольку $n = 2$ для всех остальных случаев у нас всегда есть единственное ближнее поле Диксона для каждого возможного q.

Если $q = 5^2$, то $\mathbb{K}^\times \cong 3 \times 8$. Опять же, все максимальные подгруппы $\mathbb{K}^\times$ являются абелевыми.

Предположим, что $q = 7^2$. В этом случае $\mathbb{K}^\times \cong 3 \times Q_{16}$. Представителями классов сопряженности максимальных подгрупп $\mathbb{K}^\times$ являются M_1, M_2 и M_3, где $M_1 \cong Q_{16}$, $M_2 \cong M_3 \cong 3 \times Q_8$. Если $G = G(\mathbb{K}, M_1)$, то $G^{(2)} \cong 7^2 \rtimes (Q_{16} \rtimes 2)$ и $G^{(2)} \leq \mathrm{A\Gamma L}(1,49)$. В случае $G = G(\mathbb{K}, M_2)$ (или $G = G(\mathbb{K}, M_3)$), у нас есть $G^{(2)} = 7^2 \rtimes (3 \times \mathrm{SL}(2,3))$, и утверждение (2) теоремы справедливо. Обратите внимание, что $G^{(2)} \not\leq \mathrm{A\Gamma L}(1,49)$, поскольку порядок $G^{(2)}$ не разделяет порядок $\mathrm{A\Gamma L}(1,49)$. Стоит отметить, что это 2-замыкание появляется как подгруппа индекса 2 в исключительной разрешимой 2-транзитивной группе степени 49 (все такие группы были классифицированы в [29]). Если K является собственной подгруппой группы либо M_2, либо M_3, то она сопряжена с подгруппой M_1, поэтому $G^{(2)} \leq \mathrm{A\Gamma L}(1,49)$ для всех таких K.

Пусть $q = 11^2$. В этом случае $\mathbb{K}^\times \cong 5 \times (3 \rtimes Q_8)$. Представители классов сопряженности

неабелевых максимальных подгрупп и соответствующие 2-замыкания выглядят следующим образом:

$M_1 \cong 5 \times (3 \rtimes 4)$, и $G^{(2)} = G$;

$M_2 \cong M_1$, и $G^{(2)} = G$;

$M_3 \cong 3 \rtimes Q_8$, и $G^{(2)} = 11^2 \rtimes (24 \rtimes 2) \leq \mathrm{A\Gamma L}(1, 11^2)$;

$M_4 \cong 5 \times Q_8$, и $G^{(2)} = G$.

Если $q = 17^2$, то $\mathbb{K}^\times \cong 9 \rtimes 32$. Существует только один класс неабелевых максимальных подгрупп группы $\mathbb{K}^\times$ с представителем $M \cong 3 \rtimes 32$, и $G^{(2)} = G$ для него.

6. $\mathrm{SL}(2,5) \lhd H \leq \Gamma\mathrm{L}(2, p^{d/2})$, где $p^{d/2} \in \{9, 11, 19, 29, 169\}$. Аналогично, для всех возможных почти-полей Диксона $\mathbb{K}$ и всех неабелевых максимальных подгрупп M из $\mathbb{K}^\times$ мы построим группу $G = G(\mathbb{K}, M)$ и найдем ее 2-замыкание, тем самым доказывая, что $G^{(2)} = \mathbb{K}^+ \rtimes H$ разрешима, а значит H не содержит $\mathrm{SL}(2,5)$.

Если $q = p^d$ равно 3^4 или 11^2, то требуемое утверждение уже было доказано выше.

Предположим, что $q = 19^2$. В этом случае $\mathbb{K}^\times \cong 9 \times (5 \rtimes Q_8)$. Представители классов сопряженности неабелевых максимальных подгрупп $\mathbb{K}^\times$ и соответствующих 2-замыканий являются следующими:

$M_1 \cong 9 \times (5 \rtimes 4)$, и $G^{(2)} = G$;

$M_2 \cong M_1$, и $G^{(2)} = G$;

$M_3 \cong 3 \times (5 \rtimes Q_8)$, и $G^{(2)} = 19^2 \rtimes (3 \times (40 \rtimes 2))$;

$M_4 \cong 9 \times Q_8$, и $G^{(2)} = G$.

Если $q = 29^2$, то $\mathbb{K}^\times \cong 7 \times (15 \rtimes 8)$. Представителями классов сопряженности неабелевых максимальных подгрупп и соответствующими 2-замыканиями являются:

$M_1 \cong 15 \rtimes 8$, и $G^{(2)} = 29^2 \rtimes (120 \rtimes 2)$;

$M_2 \cong 7 \times (5 \rtimes 8)$, и $G^{(2)} = G$;

$M_3 \cong M_2$, и $G^{(2)} = G$.

Если $q = 13^4$, то существует три неизоморфных почти-поля Диксона порядка q.

Для пары Диксона $(13, 4)$ существует два неизоморфных почти-поля $\mathbb{K}_1$ и $\mathbb{K}_2$. Однако, $\mathbb{K}_1^\times \cong \mathbb{K}_2^\times \cong 3 \times (595 \rtimes 16)$, и $M_i^1 \cong M_i^2$, $i \in \{1..5\}$ для соответствующих представителей классов сопряженности неабелевых максимальных подгрупп.

$M_1^1 \cong M_1^2 \cong 21 \times (85 \rtimes 8)$, и $G^{(2)} = 13^4 \rtimes (3 \times (4760 \rtimes 4))$;

$M_2^1 \cong M_2^2 \cong 595 \rtimes 16$, и $G^{(2)} = 13^4 \rtimes (9520 \rtimes 4)$;

$M_3^1 \cong M_3^2 \cong 3 \times (119 \rtimes 16)$, и $G^{(2)} = G$;

$M_4^1 \cong M_4^2 \cong 3 \times (85 \rtimes 16)$, и $G^{(2)} = 13^2 \rtimes (3 \times ((85 \rtimes 16) \rtimes 2))$;

$M_5^1 \cong M_5^2 \cong 3 \times (35 \rtimes 16)$, и $G^{(2)} = G$.

Для пары Диксона $(169, 2)$, $\mathbb{K}^\times \cong 21 \times (85 \rtimes 16)$. Представители классов сопряженности неабелевых максимальных подгрупп и соответствующие им 2-замыкания следующие:

$M_1 \cong 7 \times (85 \rtimes 16)$, и $G^{(2)} = 13^4 \rtimes (9520 \rtimes 4)$;

$M_2 \cong 3 \times (85 \rtimes 16)$, и $G^{(2)} = 13^4 \rtimes (3 \times (1360 \rtimes 16))$;

$M_3 \cong 21 \times (17 \rtimes 16)$, и $G^{(2)} = G$;

$M_4 \cong 21 \times (5 \rtimes 16)$, и $G^{(2)} = G$.

Все 2-замыкания оказались разрешимыми, поэтому $\mathrm{SL}(2, 5) \not\leq H$, что и требовалось.

В итоге, если $\mathbb{K}$ — почти-поле Диксона и K — собственная подгруппа группы $\mathbb{K}^\times$, то верны утверждения (1) и (2) теоремы 9. В частности, группа автоморфизмов нетривиальной схемы $\mathrm{Cyc}(\mathbb{K}, K)$ разрешима для любого почти-поля Диксона $\mathbb{K}$.

Пусть теперь $\mathbb{K}$ — почти-поле Цассенхауза. Предположим сначала, что K — разрешимая подгруппа группы $\mathbb{K}^\times$. По лемме 1.1.3, достаточно найти 2-замыкания групп $G = G(\mathbb{K}, M)$, где M — максимальная разрешимая подгруппа группы $\mathbb{K}^\times$. Для каждой такой группы M (с точностью до сопряжения), мы строим группу подстановок G, снова используя MAGMA, и находим ее 2-замыкание с помощью пакета COCO для GAP, тем самым доказывая утверждение (3) теоремы 9. Результаты вычислений отображены в таблице 3 в Приложении. В частности, если $\mathbb{K}$ — конечное почти-поле и K — собственная разрешимая подгруппа K группы $\mathbb{K}^\times$, то группа автоморфизмов схемы $\mathcal{C} = \mathrm{Cyc}(\mathbb{K}, K)$ разрешима.

Теперь предположим, что K — неразрешимая подгруппа группы $\mathbb{K}^\times$. Таких возможностей только две.

Если K — почти-поле Цассенхауза порядка 29^2, то $\mathbb{K}^\times \cong 7 \times \mathrm{SL}(2, 5)$.

Если K — почти-поле Цассенхауза порялка 29^2, то $\mathbb{K}^\times \cong 7 \times \mathrm{SL}(2, 5)$. Существует только одна собственная неразрешимая подгруппа $K \cong \mathrm{SL}(2, 5)$ группы $\mathbb{K}^\times$, и в этом случае $G^{(2)} = 29^2 \rtimes (\mathrm{SL}(2, 5) \rtimes 2)$.

Если $\mathbb{K}$ — почти-поле Цассенхауза порядка 59^2, то $\mathbb{K}^\times \cong 29 \times \mathrm{SL}(2, 5)$. В этом случае тоже существует только одна собственная неразрешимая подгруппа K группы $\mathbb{K}^\times$, изоморфная группе $\mathrm{SL}(2, 5)$. В этом случае, $G^{(2)} = G$.

Таким образом, выполнено утверждение (4) теоремы 9, что завершает доказательство этой теоремы.

Приложение

Таблица 2: Группы автоморфизмов циклотомических схем над почти-полями Цассенхауза с максимальной разрешимой базисной группой

$\mathbb{K}^+$	M	H	Порождающие M	Порождающие H
5^2	Q_8	$(4 \times 2) \rtimes 2$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$	$M, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
5^2	6	D_{12}	$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$	$M, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
11^2	$5 \times Q_8$	$5 \times Q_8$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	M
11^2	$\mathrm{SL}(2,3)$	$\mathrm{GL}(2,3)$	$\begin{pmatrix} 5 & -2 \\ -1 & 5 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$M, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
11^2	30	30	$\begin{pmatrix} -5 & 1 \\ 2 & -1 \end{pmatrix}$	M
7^2	$\mathrm{SL}(2,3)$	$3 \times \mathrm{SL}(2,3)$	$\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -2 & -2 \\ -1 & 2 \end{pmatrix}$	$M, \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}$
7^2	Q_{16}	QD_{32}	$\begin{pmatrix} 2 & 2 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}$	$M, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
7^2	$3 \rtimes 4$	$(6 \times 2) \rtimes 2$	$\begin{pmatrix} 3 & 2 \\ 2 & -3 \end{pmatrix}, \begin{pmatrix} -3 & 0 \\ -3 & 2 \end{pmatrix}$	$M, \begin{pmatrix} 1 & 0 \\ -3 & -1 \end{pmatrix}$
23^2	$11 \times \mathrm{SL}(2,3)$	$11 \times \mathrm{SL}(2,3)$	$\begin{pmatrix} -8 & 10 \\ -2 & -4 \end{pmatrix}, \begin{pmatrix} -10 & 9 \\ -1 & 10 \end{pmatrix}$	M
23^2	$2.S_4$	$2.S_4$	$\begin{pmatrix} -7 & -6 \\ 11 & 6 \end{pmatrix}, \begin{pmatrix} 9 & 1 \\ 10 & -9 \end{pmatrix}$	M
23^2	$11 \times Q_{16}$	$11 \times Q_{16}$	$\begin{pmatrix} -10 & 5 \\ 2 & -8 \end{pmatrix}, \begin{pmatrix} -2 & 6 \\ 6 & 2 \end{pmatrix}$	M
23^2	$11 \times (3 \rtimes 4)$	$11 \times (3 \rtimes 4)$	$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 7 & -1 \\ -8 & -7 \end{pmatrix}$	M
продолжение на следующей странице				

Продолжение таблицы 2

$\mathbb{K}^+$	M	H	Порождающие M	Порождающие H
11^2	$\mathrm{SL}(2,3)$	$\mathrm{GL}(2,3)$	$\begin{pmatrix}-1 & -1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}-5 & -2\\ 2 & 5\end{pmatrix}$	$M, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
11^2	$5 \rtimes 4$	$(10 \times 2) \rtimes 2$	$\begin{pmatrix}-1 & -1\\ 2 & 0\end{pmatrix}, \begin{pmatrix}0 & -1\\ 1 & 3\end{pmatrix}$	$M, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
11^2	$3 \rtimes 4$	$3 \rtimes 4$	$\begin{pmatrix}-4 & 1\\ 5 & 4\end{pmatrix}, \begin{pmatrix}-1 & -1\\ 1 & 0\end{pmatrix}$	M
29^2	$7 \times \mathrm{SL}(2,3)$	$7 \times \mathrm{SL}(2,3)$	$\begin{pmatrix}7 & 6\\ 13 & 2\end{pmatrix}, \begin{pmatrix}9 & -6\\ 4 & -9\end{pmatrix}$	M
29^2	$7 \times (5 \rtimes 4)$	$7 \times (5 \rtimes 4)$	$\begin{pmatrix}8 & 0\\ 10 & -8\end{pmatrix}, \begin{pmatrix}-6 & -1\\ 1 & 0\end{pmatrix}$	M
29^2	$7 \times (3 \rtimes 4)$	$7 \times (3 \rtimes 4)$	$\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}, \begin{pmatrix}-3 & -9\\ -6 & 3\end{pmatrix}$	M
59^2	$29 \times \mathrm{SL}(2,3)$	$29 \times \mathrm{SL}(2,3)$	$\begin{pmatrix}-1 & 22\\ -23 & -14\end{pmatrix}, \begin{pmatrix}4 & 29\\ -25 & -4\end{pmatrix}$	M
59^2	$29 \times (5 \rtimes 4)$	$29 \times (5 \rtimes 4)$	$\begin{pmatrix}-18 & 26\\ 22 & 18\end{pmatrix}, \begin{pmatrix}-26 & -1\\ 1 & 0\end{pmatrix}$	M
59^2	$29 \times (3 \rtimes 4)$	$29 \times (3 \rtimes 4)$	$\begin{pmatrix}-24 & 6\\ 16 & 23\end{pmatrix}, \begin{pmatrix}19 & -16\\ -15 & -19\end{pmatrix}$	M

Таблица 3: Группы автоморфизмов циклотомических схем над почти-полями Цассенхауза с неразрешимой базисной группой

$\mathbb{K}^+$	K	H	Порождающие K	Порождающие H
29^2	$\mathrm{SL}(2,5)$	$\mathrm{SL}(2,5) \rtimes 2$	$\begin{pmatrix}2 & -5\\ 1 & -2\end{pmatrix}, \begin{pmatrix}12 & 4\\ 3 & -11\end{pmatrix}$	$K, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
59^2	$\mathrm{SL}(2,5)$	$\mathrm{SL}(2,5)$	$\begin{pmatrix}4 & -1\\ -1 & -29\end{pmatrix}, \begin{pmatrix}-29 & 10\\ -5 & 28\end{pmatrix}$	K

Заключение

В диссертации изучаются теоретические и алгоритмические аспекты проблемы k-замыкания групп подстановок и связанные с ней вопросы. Особое внимание уделено нильпотентным, абелевым и $\frac{3}{2}$-транзитивным группам подстановок. Полученные результаты открывают новые методы и направления изучения k-замыканий. Например, теорема 1 может помочь обобщить результаты о вполне k-замкнутых абелевых группах (теорема 6) на нильпотентные группы. Из теоремы 2 следует, что отдельный интерес представляют квазирегулярные группы со свойством $\mathrm{Zel}(G) = 1$. В теоремах 7 и 8 решены проблемы эффективного нахождения 2-замыкания $\frac{3}{2}$-транзитивной группы и изоморфизма цветных шуровых $\frac{3}{2}$-однородных когерентных конфигураций, тем самым, основной интерес теперь переносится на сложностной аспект проверки шуровости $\frac{3}{2}$-однородных когерентных конфигураций.

Список литературы

[1] Вейсфейлер Б., Леман А. Приведение графа к каноническому виду и возникающая при этом алгебра // Научно-техн. информ. Сб. ВИНИТИ. — 1968. — Т. 2, № 9. — С. 12–16.

[2] Евдокимов С. А., Пономаренко И. Н. О примитивных клеточных алгебрах // Теория представлений, динамические системы, комбинаторные и алгоритмические методы III //Зап. научн. сем. ПОМИ — 1999. — Т. 256. — С. 38–68.

[3] Зеликовский А. З. Задача Кёнига для абелевых групп перестановок // Изв. АН БССР. Сер. Физ.-Мат. Наук. — 1989. — Т. 125. — Н. — С. 34–39.

[4] Калужнин Л. А., Клин М. Х. О некоторых числовых инвариантых групп подстановок // Латв. Мат. Ежегод. — 1976. — Т. 18 — С. 81–99.

[5] Каргаполов М. И., Мерзляков Ю. И. Основы теории групп: Учебное пособие. 5-е изд., стер. // СПб.: Изд. «Лань» — 2009. — 288 с.

[6] Супруненко Д. А. Группы подстановок // Навука і тэхніка, Мінск. — 1996.

[7] Abdollahi A., Arezoomand M. Finite nilpotent groups that coincide with their 2-closures in all of their faithful permutation representations // J. Algebra Appl. — 2018. — Vol. 17, no. 4. — P. 1850065.

[8] Abdollahi A., Arezoomand M., Tracey G. On finite totally 2-closed groups — 2020. — URL: `arxiv.org/abs/2001.09597v2`.

[9] Arezoomand M., Iranmanesh M. A, Praeger C. E., Tracey G. Totally 2-closed finite groups with trivial Fitting subgroup — 2021. — URL: `arxiv.org/abs/2111.02253`.

[10] Babai L. Groups, Graphs, Algorithms: The Graph Isomorphism Problem // Proc. ICM 2018, Rio de Janeiro. — 2015. — Vol. 3. — P. 3303–3320.

[11] Bannai E., Ito T. Algebraic combinatorics. I. Association schemes // The Benjamin/Cummings Publishing Co., Inc. — 1984. — 425 p.

[12] Bagherian J., Ponomarenko I., Rahnamai Barghi A. On cyclotomic schemes over finite near-fields // J. Algebraic Combin. — 2008. — Vol. 27. — P. 173–185.

[13] Bamberg J., Giudici M., Liebeck M. W., Praeger C. E., Saxl J. The classification of almost simple $\frac{3}{2}$-transitive groups // Trans. Amer. Math. Soc. — 2013. — Vol. 365. — P. 4257–4311.

[14] Bosma W., Cannon J., Playoust C. The Magma algebra system I: The user language // J. Symbolic Comput. — 1997. — Vol. 24.

[15] Brouwer A. E., Cohen A. M., Neumaier A. Distance-regular graphs // Ergebnisse der Mathematik und ihrer Grenzgebiete. — 1989.

[16] Cameron P. J., Giudici M., Jones G. A., Kantor W. M., Klin M. H., Marušič D., Nowitz L. A. Transitive Permutation Groups Without Semiregular Subgroups // Journal of the London Mathematical Society. — 2002. — Vol. 66. — P. 325–333.

[17] Chen G., Ponomarenko I. Coherent configurations // Wuhan: Central China Normal University Press. — 2019. — URL: `pdmi.ras.ru/~inp/ccNOTES.pdf`.

[18] 2-closure of a permutation group: Questions / Answers — 2016. — URL: `mathoverflow.net/q/235114`.

[19] Delsarte P. An Algebraic Approach to the Association Schemes of Coding Theory // Philips Research Reports Suppl. — 1973. — Vol. 10.

[20] Dixon J. D., Mortimer B. Permutation Groups. // Berlin: Springer Verlag. — 1996. — 346 p.

[21] Evdokimov S., Ponomarenko I. Permutation group approach to association schemes // European J. Combin. — 2009. — Vol. 30, no. 6. — P. 1456–1476.

[22] Evdokimov S.,Ponomarenko I. Two-closure of odd permutation group in polynomial time // Discrete Math. — 2001. — Vol. 235, no. 1-3. — P. 221–232.

[23] Faradzev I. et al. Investigations in Algebraic Theory of Combinatorial Objects // Kluwer Academic Publishers, Dordrecht. — 1994.— P. 1–152.

[24] Giudici M., Liebeck M. W., Praeger C. E., Saxl J., Tiep P. H. Arithmetic results on orbits of linear groups // Trans. Amer. Math. Soc. — 2016. — Vol. 368. — P. 2415–2467.

[25] Grech M., Kisielewicz A. 2-Closed Abelian Permutation Groups // Electron. Notes Discrete Math. — 2018. — Vol. 68. — P. 83–88.

[26] Grech M., Kisielewicz A. Abelian permutation groups with graphical representations // J. Algebr. Comb. — 2021. — Vol. 277. — P. 172–179.

[27] Grech M., Kisielewicz A. Graphical representations of cyclic permutation groups // J. Algebr. Comb. — 2021. URL: doi.org/10.1007/s10801-021-01060-8.

[28] Higman D. G. Coherent configurations. I. // Rend. Sem. Mat. Univ. Padova. — 1970. — Vol. 44. — 1–25.

[29] Huppert B. Zweifach transitive auflosbare Permutationsgruppen // Math. Z. — 1957. — V. 68. — P. 126–150.

[30] Liebeck M. W., Praeger C. E, Saxl J. The classification of $\frac{3}{2}$-transitive permutation groups and $\frac{1}{2}$-transitive linear groups // Proc. Amer. Math. Soc. — 2019. — Vol. 147. — P. 5023–5037.

[31] Liebeck M. W., Praeger C. E., Saxl J. On the 2-closures of finite permutation groups // J. Lond. Math. Soc. — 1988. — Vol. 37. — P. 241–252.

[32] Lucchini A., Menegazzo F. Generators for finite groups with a unique minimal normal subgroup // Rend. Sem. Mat. Univ. Padova. — 1997. — Vol. 98. — P. 173–191.

[33] McConnel R. Pseuso-ordered polynomials over a finite field // Acta Arith. — 1963. — Vol. 8. — P. 127–151.

[34] O'Brien E. A., Ponomarenko I., Vasil'ev A. V., Vdovin E. The 3-closure of a solvable permutation group is solvable // Journal of Algebra. — 2021. — URL: doi.org/10.1016/j.jalgebra.2021.07.002.

[35] Palfy P. P. A polynomial bound for the orders of primitive solvable groups // J. Algebra. — 1982. — Vol. 77. — P. 127–137.

[36] Passman D. S. Exceptional $\frac{3}{2}$-transitive permutation groups // Pacific J. Math. — 1969. — Vol. 29. — P. 669–713.

[37] Passman D. S. Permutation Groups // W.A. Benjamin, Inc., New York. — 1968.

[38] Passman D. S. Solvable Half-Transitive Automorphism Groups // J. Algebra. — 1967. — Vol. 6. — P. 285–304.

[39] Passman D. S. Solvable $\frac{3}{2}$-transitive groups // J. Algebra. — 1967. — Vol. 7. — P. 192–207.

[40] Praeger C. E., Saxl J. Closures of finite primitive permutation groups // Bull. London Math. Soc. — 1992. — Vol. 24. — P. 251–258.

[41] Ponomarenko I. Bases of schurian antisymmetric coherent configurations and isomorphism test for schurian tournaments // Journal of Mathematical Sciences — 2013. — Vol. 192, no. 3. — P. 316-338.

[42] Ponomarenko I. Graph isomorphism problem and 2-closed permutation groups // Appl. Algebra Eng. Comm. Comput. — 1994. — Vol. 5. — P. 9–22.

[43] Ponomarenko I.,Vasil′ev A. Two-closure of supersolvable permutation group in polynomial time // Computational Complexity — 2020. — Vol. 29: 5.

[44] Schonert M. et al. GAP — Groups, Algorithms, and Programming // Lehrstuhl D fur Mathematik, Rheinisch Westfalische Technische Hochschule, Aachen, Germany. — 1995.

[45] Seress A. Permutation Group Algorithms // Cambridge Tracts in Mathematics. — 2003.

[46] Wahling H. Theorie der Fastkorper // Thales. — 1987.

[47] Weisfeiler B. (editor) On construction and identification of graphs // Springer Lecture Notes. — 1976. — Vol. 558.

[48] Wielandt H. Finite permutation groups // Academic Press, New York – London. — 1964.

[49] Wielandt H. Permutation groups through invariant relations and invariant functions // Lecture Notes Dept. Math., Ohio State Univ., Colombus, Ohio. — 1969.

[50] Zassenhaus H. Uber endliche Fastkorper // Abh. Math. Sem. Hamburg. — 1936. — Vol. 11. — P. 187–220.

Работы автора по теме диссертации

[51] Churikov D. V., Vasil′ev A. V. Automorphism groups of cyclotomic schemes over finite near-fields // Сиб. электрон. матем. изв. — 2016. — Т. 13. — С. 1271–1282.

[52] Васильев А. В., Чуриков Д. В. 2-Замыкание $\frac{3}{2}$-транзитивных групп за полиномиальное время // Сиб. матем. журн. — 2019. — Т. 60, № 2. — С. 360–375.

[53] Churikov D., Praeger C. E. Finite totally k-closed groups // Труды Института Математики и Механики УрО РАН. — 2021. — Т. 27, №. 1. — С. 240–245.

[54] Чуриков Д. В. Структура k-замыканий конечных нильпотентных групп подстановок // Алгебра и Логика. — 2021.— Т. 60, №. 2— С. 231–239.

[55] Churikov D., Ponomarenko I. On 2-closed abelian permutation groups // Comm. Algebra. — 2021. — URL: doi.org/10.1080/00927872.2021.1990307.

[56] Churikov D. V. Automorphism groups of cyclotomic schemes over finite near-fields // Материалы международной конференции «Graphs and Groups, Spectra and Symmetries». — 2016. — Новосибирск: ИМ СО РАН, Новосиб. гос. ун-т. — С. 51.

[57] Churikov D. On 2-closures of abelian groups // Материалы международной конференции «Workshop on Group Theory and Algebraic Combinatorics». — 2017. — Новосибирск: ИМ СО РАН, Новосиб. гос. ун-т. — С. 30.

[58] Churikov D. V. 2-closure of $\frac{3}{2}$-transitive groups in polynomial time // Abstracts of International Conference «Symmetry vs. Regularity». — 2018. — Plzen, Czech Republic: University of West Bohemia. — P. 43.

[59] Churikov D. V., Vasil′ev A. V. Isomorphism problem for coherent configurations associated with $\frac{3}{2}$-transitive permutation groups // Материалы международной конференции «Мальцевские чтения». — 2018. — Новосибирск: ИМ СО РАН, Новосиб. гос. ун-т. — С. 131.

[60] Churikov D. V. On 2-closed quasiregular permutation groups // Материалы международной конференции «Мальцевские чтения». — 2020. — Новосибирск: ИМ СО РАН, Новосиб. гос. ун-т. — С. 50.