Федеральное государственное бюджетное учреждение науки
Институт математики им. С. Л. Соболева
Сибирского отделения Российской академии наук

На правах рукописи

Бутурлакин Александр Александрович

Специальные классы подгрупп и строение локально конечных групп

01.01.06 — математическая логика, алгебра и теория чисел

Диссертация на соискание ученой степени доктора физико-математических наук

Научный консультант
профессор, д.ф.-м.н.
А. В. Васильев

Новосибирск
2021

Оглавление

Введение

Постановка задачи. Основным объектом изучения в диссертации являются локально конечные группы, т. е. группы, в которых любое конечное множество элементов содержится в конечной подгруппе. При этом решаются задачи двух естественных типов: первый — это получение информации о всей группе из информации о подгруппах из некоторого класса, и второй, обратный к первому, — по информации о группе получить информацию о подгруппах данного класса. В работе рассматривается три класса подгрупп: циклические подгруппы, холловы подгруппы и централизаторы.

Уже из определения ясно, что классы конечных и локально конечных групп довольно близки. Однако класс локально конечных групп гораздо менее исследован. Дело в том, что многие существенные результаты о конечных группах не переносятся непосредственным образом на бесконечные. В связи с этим для получения содержательных результатов часто накладываются некоторые дополнительные условия, в том числе различные ограничения на некоторый класс подгрупп: условия минимальности/максимальности, разрешимость, субнормальность подгрупп определенного класса и т. п. Одним из таких условий является ограничение на c-размерность группы, т. е. максимальную длину цепи строго вложенных централизаторов, которое является естественным усилением классического условия минимальности для централизаторов. Современный интерес к группам с этим условием связан с теорией моделей: универсально эквивалентные группы имеют одинаковую c-размерность. В диссертации мы исследуем структуру локально конечных групп конечной c-размерности, решая таким образом задачу первого типа.

Ко второму типу относится задача описания спектров конечных простых групп. Спектр $\omega(G)$ группы G — это множество порядков всех ее циклических подгрупп или, что то же самое, множество порядков ее элементов. В диссертации дается описание спектров конечных простых исключительных групп лиева типа, что завершает решение общей задачи описания спектров конечных простых групп. При изучении конечных групп лиева типа одним из основных методов является погружение конечной группы в соответствующую (локально конечную) группу лиева типа над алгебраически замкнутым полем. При этом конечные подгруппы выделяются в бесконечных группах как группы неподвижных точек специального класса отображений, так называемых эндоморфизмов Стейнберга. Преимущество указанного метода состоит в том, что группы лиева типа над алгебраически замкнутыми полями устроены гораздо более регулярно, чем их конечные аналоги.

Со спектрами связана и следующая проблема, изучаемая в диссертации: для данного множества $\mathcal{M}$ натуральных чисел требуется определить, совпадает ли оно со спектром некоторой конечной группы G, и если совпадает, то найти все конечные группы с таким свойством. В общей постановке эта задача, по-видимому, слишком трудна. Однако спектры простых групп известны, а значит, в случае простой группы G задача имеет очевидное

теоретическое решение, и вопрос (который и исследуется в диссертации) состоит скорее в том, можно ли найти подходящую простую группу G за полиномиальное время. Отметим, что если такая группа нашлась, то в большинстве случаев можно решить исходную задачу, т. е. предъявить список всех конечных групп, чей спектр равен $\mathcal{M}$, причем их цоколи (подгруппы, порожденные всеми минимальными нормальными подгруппами) будут изоморфны G.

Если информация о порядках циклических подгрупп позволяет зачастую «распознать» простую группу, то из существования определенных бипримарных подгрупп можно иногда вывести разрешимость всей группы или некоторых ее подгрупп. Так, хорошо известно, что конечная группа G разрешима, если она содержит $\{p, q\}$-холлову подгруппу для любой пары p и q простых делителей порядка группы G. В диссертации мы усилим этот результат, заменив соответственно множество всех простых делителей порядка группы на произвольное множество простых чисел π, а разрешимость всей группы — на существование разрешимой π-холловой подгруппы.

Актуальность и степень разработанности темы исследования. Понятие c-размерности было введено в 2004 г. в работе А. Г. Мясникова и П. В. Шумяцкого, посвященной дискриминируемым группам [79]. В последней работе c-размерность применяется как инвариант универсальной эквивалентности. Локально конечные группы конечной c-размерности нужно рассматривать скорее как подкласс $\mathfrak{M}_c$-групп, т.е. групп с условием минимальности для централизаторов. Напомним, что группа обладает условием минимальности для некоторого класса подгрупп, если любая убывающая цепочка подгрупп данного класса стабилизируется за конечное число шагов. Локально конечные $\mathfrak{M}_c$-группы возникли как естественное обобщение периодических линейных групп и имеют много общих свойств с последними. Например, локально конечная $\mathfrak{M}_c$-группа удовлетворяет теореме Силова (Р. М. Брайант, 1979 г. [35]), периодические локально разрешимые $\mathfrak{M}_c$-группы разрешимы (Р. М. Брайант и Б. Хартли, 1979 г. [36]). Хотя структура локально конечных $\mathfrak{M}_c$-групп не описана, имеется результат О. Кегеля [70, теорема 4.4] о более широком классе групп, дающий довольно сильные ограничения на их строение. В нем описываются локально конечные группы, удовлетворяющие сильной теореме Силова для некоторого простого числа $p \geqslant 5$. Напомним, что группа удовлетворяет сильной теореме Силова, если в любой ее подгруппе все максимальные p-подгруппы сопряжены (в силу упомянутого выше результата локально конечные $\mathfrak{M}_c$-группы удовлетворяют сильной теореме Силова для любого простого числа). В частности, теорема Кегеля утверждает, что фактор-группа такой группы по p-разрешимому радикалу является группой автоморфизмов прямого произведения конечного числа простых линейных групп.

Естественным подходом при изучении локально конечных групп конечной c-размерности является усиление имеющихся результатов об $\mathfrak{M}_c$-группах. Например, основной результат работы Е. И. Хухро 2009 г. [72] усиливает упоминавшийся выше результат о периодических локально разрешимых $\mathfrak{M}_c$-группах. В частности, в этой работе показано, что ступень разрешимости периодической локально разрешимой группы конечной c-размер-

ности k ограничена в терминах k. Кроме того, было показано, что фактор-группа такой группы по второму радикалу Хирша–Плоткина содержит абелеву подгруппу, чей индекс ограничен в терминах k. По аналогии с последним утверждением А. В. Боровик сформулировал гипотезу, приведенную в [72], о строении произвольных локально конечных групп конечной c-размерности. Изучение справедливости этой гипотезы явилось началом и составляет существенную часть исследования, результаты которого изложены в первой главе. Для формулировки этой гипотезы нам понадобятся некоторые определения и обозначения. Радикалом Хирша–Плоткина $\mathrm{F}(G)$ группы G называется максимальная нормальная локально нильпотентная подгруппа группы G. Компонентой группы называется субнормальная квазипростая подгруппа. Подгруппа, порожденная всеми компонентами данной группы G, называется слоем и обозначается $\mathrm{E}(G)$. Обобщенная подгруппа Фиттинга $\mathrm{F}^*(G)$ группы G — это произведение подгрупп $\mathrm{F}(G)$ и $\mathrm{E}(G)$.

Гипотеза Боровика–Хухро. *Пусть G — это локально конечная группа конечной c-размерности k. Пусть S — это полный прообраз обобщенной подгруппы Фиттинга $\mathrm{F}^*(G/\mathrm{F}(G))$ в G. Тогда*

(1) *число неабелевых композиционных факторов группы G конечно и ограничено в терминах k;*

(2) *G/S содержит абелеву подгруппу конечного индекса, ограниченного в терминах k.*

В диссертации доказывается первое утверждение гипотезы и строится контрпример ко второй части. Однако более важным результатом является полученное описание строения локально конечных групп конечной c-размерности в духе результата Кегеля. В частности, показано, что фактор-группа такой группы по локально разрешимому радикалу является группой автоморфизмов прямого произведения простых линейных групп, совокупный «размер» которых ограничен в терминах c-размерности, а образ этого фактора в группе внешних автоморфизмов почти абелев с индексом абелевой подгруппы, также ограниченным в терминах c-размерности. Кроме того, было показано, что c-размерность фактора по локально разрешимому радикалу ограничена в терминах c-размерности исходной локально конечной группы. Этот факт представляет отдельный интерес, поскольку в общей ситуации при факторизации c-размерность ведет себя непредсказуемо.

Отметим, что наши результаты о локально конечных группах конечной c-размерности обобщают некоторые известные результаты о периодических линейных группах. Известно, что количество неабелевых композиционных факторов конечной линейной группы ограниченно в терминах размерности представления этой группы (М. И. Каргаполов, 1962-63 гг. [17,18]). Обобщение этого результата на случай периодических линейных групп может быть найдено в монографии Б. А. Ф. Верфрица [86, теорема 9.30]. Полученное нами доказательство первого утверждения гипотезы Боровика–Хухро обобщает эти результаты.

Согласно теореме Жордана–Шура периодическая группа, имеющая конечномерное представление степени n над полем характеристики 0, почти абелева с минимальным индексом абелевой подгруппы, ограниченным функцией от n. Существует аналог этого

утверждения для конечных групп над полями положительной характеристики. Для его формулировки нам понадобится следующее обозначение. Для простого числа p обозначим через $\mathrm{E}_p(G)$ подгруппу группы G, порожденную всеми компонентами, чей фактор по центру является группой лиева типа над полем характеристики p. Известно, что если G — это подгруппа общей линейной группы $GL_n(F)$, где F — поле положительной характеристики p, то группа $\overline{G} = G/O_p(G)$ содержит нормальную абелеву подгруппу N такую, что порядок фактор-группы $\overline{G}$ по $N\,\mathrm{E}_p(\overline{G})$ ограничен функцией от n (точное значение этой функции для достаточно больших n найдено в работе М. Дж. Коллинза 2008 г. [42]). Аналогичное утверждение о периодических линейных группах с тривиальным унипотентным радикалом, имеющих конечномерное представление над полем положительной характеристики, можно найти, например, в лекциях о локально конечных группах У. Мейерфранкенфельда [77, теорема 15.12]. Отметим, что прямое произведение линейных групп (имеющих представление над полями разных характеристик) может не быть линейной группой, однако имеет конечную c-размерность. Таким образом, естественно при попытках обобщить эти результаты на группы конечной c-размерности заменять p-радикал на радикал Хирша–Плоткина, а подгруппу $\mathrm{E}_p(G)$ на слой $\mathrm{E}(G)$. Как упоминалось выше, такое обобщение, и даже второе утверждение гипотезы Боровика–Хухро, неверно. Тем не менее, удается показать, что если заменить в гипотезе радикал Хирша–Плоткина на разрешимый радикал, то утверждение становится верным.

Последнее утверждение о линейных группах, которое мы хотим здесь упомянуть — это теорема Д. Дж. Уинтера 1968 г. [88], которая говорит, что периодическая линейная группа содержит нормальную унипотентную подгруппу не более чем счетного индекса. Одним из следствий основных результатов диссертации является утверждение о том, что локально конечная группа конечной c-размерности является не более чем счетным расширение нильпотентной группы, что является прямым обобщением теоремы Уинтера.

Отметим, что описание строения локально конечных групп конечной c-размерности было независимо и почти одновременно с автором диссертации получено А. В. Боровиком и У. Кархумаки в 2019 г. [30]. Эта работа построена на иной идее, чем наше доказательство, — она построена вокруг понятия ограниченной (constrained) группы. По определению группа ограничена, если ступени разрешимости всех ее разрешимых подгрупп ограничены в совокупности. Легко видеть, что любая секция локально конечной группы конечной c-размерности является ограниченной. Основной результат работы А. В. Боровика и У. Кархумаки дает только качественное описание строения, но не дает количественных оценок на параметры группы (за исключением оценки на ступень разрешимости локально разрешимого радикала, взятой из работы Е. И. Хухро [72]).

Важной частью теории конечных групп является изучение свойств и различных параметров конечных простых групп, ставшее особенно актуальным в ходе и после получения их классификации. К числу наиболее естественных изучаемых характеристик конечных простых групп относятся индексы и строение максимальных подгрупп, таблицы характеров, неприводимые представления и многие другие, в том числе и изучаемые в диссертации

спектры.

Обозначим через $\mu(G)$ подмножество спектра, состоящее из максимальных по делимости элементов. Скажем, что спектр конечной группы G описан, если указано множество натуральных чисел $\nu(G)$ такое, что $\mu(G) \subseteq \nu(G) \subseteq \omega(G)$, действительно, как несложно понять, $\omega(G)$ однозначно определяется любым множеством $\nu(G)$, удовлетворяющим этому условию. Согласно классификации конечных простых групп все конечные неабелевы простые группы делятся на три класса: знакопеременные группы, группы лиева типа и спорадические группы. Спектры знакопеременных групп известны и их описание не представляет особого труда. Спектры спорадических групп указаны, например, в атласе конечных групп [43]. Спектры классических групп известны (А. А. Бутурлакин, 2008, 2010 гг. [1, 2]). Спектры групп Ри и Сузуки также известны (см., например, работы М. Сузуки 1962 г. [81], Р. Брандла и В. Дж. Ши 1993 г. [33], Х. В. Дэна и В. Дж. Ши 1999 г. [44]). Описание спектров групп $G_2(q)$, ${}^3D_4(q)$ и $F_4(q)$ может быть получено из работ В. М. Кантора и А. Сереша 2002 г. [68] и Д. И. Деризиотиса 1984 г. [46] и содержится, например, в работах А. В. Васильева и А. М. Старолетова 2013 г. [10] и М. А. Гречкосеевой и М. А. Звездиной 2016 г. [57]. Таким образом, для завершения описания спектров конечных простых групп требуется дать описание спектров групп $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$ и $E_8(q)$, что и сделано в диссертации. Для этих групп некоторую информацию о спектре можно извлечь из ряда известных результатов. Приведем наиболее здесь важные из них.

Если G — конечная группа лиева типа над полем характеристики p, то все элементы группы делятся на три естественных класса: полупростые (порядка взаимно простого с p), унипотентные (p-элементы) и остальные («смешанных» порядков). В работе Д. М. Тестерман 1995 г. [82] содержится формула, позволяющая вычислять максимальный порядок унипотентных элементов в любой конечной группе лиева типа. В работе Д. И. Деризиотиса и А. П. Факиоласа 1991 г. [47] дано описание максимальных торов в универсальных группах типов $E_l(q)$, где $l \in \{6, 7, 8\}$, и ${}^2E_6(q)$, что дает в качестве следствия описание полупростой части спектра этих групп. Для элементов смешанных порядков базовым является тот факт, что любой элемент группы лиева типа может быть помещен специальным образом в централизатор полупростого элемента. Структура последних в группах лиева типа изучалась, например, Д. И. Деризиотисом в работе 1984 г. [46], но имеющиеся описания не позволяют вычислить спектр точно.

Подход, при котором некоторые свойства простых групп определяются по набору порядков элементов, используется во многих задачах. Наиболее близкой к решаемой в диссертации задаче является проблема распознавания групп по спектру. Известно, что все знакопеременные группы достаточно большой степени и все простые группы лиева типа достаточно большого лиева ранга почти распознаваемы по спектру, т.е. для каждой из них существует конечное число конечных групп с тем же спектром (см. работу И. Б. Горшкова 2013 г. о знакопеременных группах [13] и обзор результатов о группах лиева типа в работе А. В. Васильева и М. А. Гречкосеевой 2015 г. [56]). Таким образом, в диссертации получена некоторого рода алгоритмическая версия этого результата.

Кроме того, такой подход используется при построении различных алгоритмов, а также компьютерных вычислениях в конечных группах. Особенно широкое применение он имеет в области так называемых black-box алгоритмов, т. е. алгоритмов, которые не используют особенности конкретного представления группы. Например, Л. Бабаи, В. М. Кантор, П. П. Палфи и А. Сереш в 2002 г. [29] предложили полиномиальный вероятностный алгоритм, который, получая на вход матричную группу, про которую известно, что она является простой группой лиева типа, и характеристику поля определения этой группы, определяет ее стандартное имя, используя информацию о порядках случайной достаточно равномерно распределенной выборки элементов конечной простой группы. М. Либек и Э. О'Брайен в 2007 г. [75] предложили вероятностный алгоритм для нахождения характеристики поля определения конечной простой группы лиева типа, также имеющий полиномиальное время работы. В 2009 г. В. М. Кантор и А. Сереш [69] предложили другой вероятностный алгоритм, определяющий характеристику абсолютно неприводимой квазипростой матричной группы, основанный на том факте, что три наибольших порядка элементов простой группы однозначно определяют характеристику поля определения группы.

Более того, имеющиеся алгоритмы используются в различных компьютерных системах вычислений для практического распознавания конечных простых групп. Таким образом, наш результат имеет теоретическое значение. С точки зрения практических вычислений представляется, что некоторые методы и понятия, разработанные при его доказательстве, могут найти применение при построении новых алгоритмов (понятие AD-графа, его применение для нахождения лиева ранга группы и др.).

Пусть π — некоторое множество простых чисел. Подгруппа H конечной группы G называется π-холловой, если H — это π-подгруппа, а индекс H в G не делится на числа из π (является π'-числом). В работе 1956 г. Ф. Холл [62] выдвинул гипотезу, что группа, содержащая $\{p, q\}$-холлову подгруппу для любой пары простых чисел p и q, является разрешимой. Эта гипотеза была доказана З. Арадом и М. Б. Уордом в 1982 г. [27] с использованием классификации конечных простых групп. В диссертации показано, что если π — некоторое конечное множество простых чисел и G — конечная группа, то G содержит разрешимую π-холлову подгруппу тогда и только тогда, когда G содержит $\{p, q\}$-холлову подгруппу для любой пары простых $p, q \in \pi$. Этот критерий очевидно усиливает результат Арада и Уорда. Кроме того, он дает положительный ответ на вопрос Ф. Гросса из работы 1995 г. [61], в которой он, в частности, доказал этот критерий для некоторых серий классических групп в предположении, что двойка и характеристика не лежат в π [61, теорема 4.9]. Кроме того, аналогичный результат только для нильпотентных холловых подгрупп в конечных простых группах был получен в 2013 г. А. Морето [78, лемма 3.2].

Основные результаты диссертации.

1. Описано строение локально конечных групп конечной c-размерности.

2. Получено описание спектров конечных простых исключительных групп лиева типа, тем самым задача описания спектров решена для всех конечных простых групп.

3. Изучена проблема: по данному множеству натуральных чисел $\mathcal{M}$ эффективно определить, существует ли конечная простая группа G, множество порядков элементов которой совпадает с $\mathcal{M}$. Предложен полиномиальный алгоритм, оставляющий не более одного кандидата для группы G, более того, множество порядков элементов этого кандидата содержит $\mathcal{M}$. В частности, если $\mathcal{M}$ — это множество порядков элементов некоторой конечной простой группы, то алгоритм определяет эту группу однозначно.

4. Доказан критерий существования разрешимой холловой подгруппы в терминах существования бипримарных холловых подгрупп, тем самым, в частности, дан положительный ответ на вопрос Ф. Гросса 1995 г.

Результаты пункта 1 получены совместно с А. В. Васильевым и Д. О. Ревиным [93, 95, 99], при этом вклад автора диссертации является решающим. Результаты пункта 2 получены автором лично [90–92]. Результат пункта 3 получен в неразделимом соавторстве с А. В. Васильевым [94, 100]. Результат пункта 4 получен в неразделимом соавторстве с ученицей автора А. П. Храмовой [97].

Научная новизна и значимость работы. Работа носит теоретический характер. Все полученные результаты являются новыми. Как говорилось выше, описание строения локально конечных групп конечной c-размерности обобщает многие известные результаты. Информация о спектрах конечных простых групп бывает полезна не только при решении задач теории групп, но и других областей математики, а методы, разработанные при его получении, могут использоваться для описания спектров других классов групп близких к простым (например, почти простых или квазипростых групп). Алгоритм распознавания простых групп по спектру имеет в первую очередь теоретическое значение, однако конструкции, полученные при его построении, могут использоваться при построении других алгоритмов распознавания простых групп по наборам порядков элементов. Критерий существования разрешимой холловой подгруппы дает усиленную версию гипотезы Холла, а утверждения, полученные при его доказательстве, могут использоваться для доказательства других утверждений о разрешимых холловых подгруппах конечных групп. Результаты диссертации могут быть включены в спецкурсы для студентов и аспирантов, специализирующихся в области алгебры.

Методы исследования. Все основные результаты диссертации используют классификацию конечных простых групп.

При изучении локально конечных групп конечной c-размерности помимо стандартных фактов теории конечных групп и локально конечных групп используется более специальная информация. Так, при описании строения этих групп используется упоминавшийся ранее результат О. Кегеля о локально конечных группах, удовлетворяющих сильной теореме Силова для p-подгрупп, где p — простое число, большее 5. Несколько раз используется лемма Е. И. Хухро о c-размерности естественного полупрямого произведения p-группы P и элементарной абелевой q-группы, точно действующей на P. При построении контрпримеров ко второй части гипотезы Боровика–Хухро используются глубокие факты из теории чисел, в частности, доказательство ослабленной версии гипотезы Диксона о

простых значениях в наборах целочисленных арифметических прогрессий для некоторого частного случая, полученное в работе К. Аллади, Р. Соломона и А. Тёрела 2000 г. [24]. Однако основную часть доказательств составляют оригинальные результаты. Например, получено новое ограничение на c-размерность конечного расширения группы конечной c-размерности (предыдущая, известная автору оценка, была получена в работе 2006 г. А. Дж. Дункана, И. В. Казачкова и В. Н. Ремесленникова [49], которая также содержит хороший обзор групп конечной c-размерности и их свойств). Важным инструментом при описании строения локально конечных групп конечной c-размерности, имеющий самостоятельный интерес, является доказанное в диссертации утверждение о том, что c-размерность фактора по локально разрешимому радикалу такой группы ограничена в терминах c-размерности исходной группы.

При описании спектров конечных исключительных групп лиева типа используется подход, при котором эти группы рассматриваются как группы неподвижных точек эндоморфизмов Стейнберга соответствующих алгебраических групп. При этом применяется метод описания так называемых связных централизаторов полупростых элементов, разработанный в работе 1978 г. Р. В. Картера [39]. Заметим, что связный централизатор всегда является редуктивной подгруппой максимального ранга и в диссертации изучаются классы сопряженности последних. При этом аккуратный выбор корневых подсистем редуктивных подгрупп максимального ранга во многих случаях позволяет избежать непосредственных вычислений. В остальных случаях используются компьютерные вычисления в системе Magma [31]. При описании порядков полупростых элементов в универсальных группах рассматриваемых типов используются результаты 1991 г. Д. И. Деризиотиса и А. П. Факиоласа [47].

При построении полиномиального алгоритма распознавания конечных простых групп по спектру используется довольно большое количество различных фактов о порядках элементов этих групп. Среди наиболее важных отметим описание графов простых чисел конечных простых групп, полученное А. В. Васильевым и Е. П. Вдовиным в 2005 г. [7]; результат В. М. Кантора и А. Сереша 2009 г. о том, что характеристика конечной простой группы лиева типа, если она нечетна, однозначно определяется тремя наибольшими порядками элементов этой группы [69], а также полученное при его доказательстве описание этих наибольших порядков (для большинства групп описаны два наибольших порядка, поскольку третий порядок необходим только в некоторых случаях); описание спектров конечных простых классических групп, полученное автором в [1, 2]. Кроме того, важным инструментом при построении алгоритма является введенное в диссертации понятия графа атомарных делителей группы.

При изучении холловых подгрупп первым шагом доказательства является сведение вопроса к почти простым группам с помощью доказательства частичного аналога теоремы 3.5 из работы Ф. Гросса 1986 г. [59]. В случае простых групп широко применяется классификация холловых подгрупп в конечных простых группах (см. обзор по этой теме в работе Е.П. Вдовина и Д.О. Ревина [12]).

Апробация результатов. Результаты работы опубликованы в рецензируемых научных изданиях, удовлетворяющих требованиям, предъявляемым Положением о присуждении ученых степеней [90–100].

Результаты диссертации докладывались на следующих конференциях: международная конференция «Мальцевские чтения» (г. Новосибирск, 2012, 2014, 2015, 2017, 2019, 2020 гг.), международная конференция по теории групп, посвященная 70-летию В. Д. Мазурова (г. Новосибирск, 16–20 июля 2013 г.), международная конференция «Группы и графы, алгоритмы и автоматы» (г. Екатеринбург, 09–15 августа 2015 г.), международная конференция «Groups, Rings, and Their Automorphisms» (г. Линкольн, Великобритания, 31 августа–02 сентября 2016 г.), XII школа-конференция по теории групп, посвященная 65-летию А. А. Махнева (г. Геленджик, 13-20 мая 2018 г.), международная алгебраическая конференция, посвящённая 110-летию со дня рождения профессора А. Г. Куроша (г. Москва, 23 - 25 мая 2018 г.).

Результаты первой главы излагались в миникурсе лекций, прочитанным автором на международной конференции «Finite Groups and Their Automorphisms 2017» (г. Болу, Турция, 3-6 мая 2017 г.). Результаты второй и третьей глав послужили материалом для миникурса лекций на 47-ой Всероссийской молодежной школе-конференции «Современные проблемы математики и ее приложений» (г. Екатеринбург, 31 января–06 февраля 2016).

Благодарности. Я глубоко признателен своему научному консультанту Андрею Викторовичу Васильеву за научное сотрудничество и помощь при подготовке текста диссертации. Я благодарен Даниле Олеговичу Ревину, а также своим ученицам Антонине Павловне Храмовой и Ирине Евгеньевне Девятковой за плодотворное сотрудничество. Я признателен Виктору Даниловичу Мазурову, Евгению Ивановичу Хухро, Андрею Витальевичу Заварницину, Евгению Петровичу Вдовину и другим сотрудникам лаборатории за замечательную творческую и профессиональную атмосферу, в которой была выполнена диссертация. Я благодарен своей жене Марии Александровне Гречкосеевой за неизменную поддержку.

1. Локально конечные группы конечной c-размерности

Напомним, что c-размерностью группы называется максимальная длина цепи строго вложенных централизаторов. Радикалом Хирша–Плоткина $\mathrm{F}(G)$ группы G называется максимальная нормальная локально нильпотентная подгруппа группы G. Компонентой группы называется субнормальная квазипростая подгруппа. Подгруппа, порожденная всеми компонентами данной группы G, называется слоем и обозначается $\mathrm{E}(G)$. Обобщенная подгруппа Фиттинга $\mathrm{F}^*(G)$ группы G — это произведение подгрупп $\mathrm{F}(G)$ и $\mathrm{E}(G)$.

В этой главе мы изучим структуру локально конечных групп конечной c-размерности. В частности, мы изучим справедливость следующей гипотезы.

Гипотеза Боровика–Хухро. *Пусть G — локально конечная группа конечной c-размерности k. Пусть S — полный прообраз обобщенной подгруппы Фиттинга $\mathrm{F}^*(G/\mathrm{F}(G))$ в G. Тогда*

(1) *число неабелевых композиционных факторов группы G конечно и ограничено в терминах k;*

(2) *G/S содержит абелеву подгруппу конечного индекса, ограниченного в терминах k.*

В параграфе 1.1 мы докажем первое утверждение гипотезы. В параграфе 1.2 построим серию контрпримеров ко второй части гипотезы. В параграфе 1 дадим описание структуры локально конечных групп конечной c-размерности, из которого, в частности, следует ослабленный вариант утверждения (2) гипотезы. В последнем параграфе главы мы получим усиление результата Брайанта 1979 г. [35] о периодических локально нильпотентных $\mathfrak{M}_c$-группах на случай групп конечной c-размерности.

§ 1.1. Неабелевы композиционные факторы

В этом параграфе мы покажем, что первое утверждение гипотезы Боровика–Хухро справедливо. Более точно, мы докажем, что справедливо следующее утверждение.

Теорема 1. *Пусть G — локально конечная группа c-размерности k. Тогда количество неабелевых композиционных факторов группы G меньше $5k$.*

Поскольку понятие композиционного фактора в бесконечной группе имеет несколько трактовок, следует пояснить, что здесь имеется ввиду. Композиционным рядом группы G мы будем называть неуплотняемый субнормальный ряд группы G такой, что вся группа G есть объединение групп этого ряда (более подробное определение можно найти, например, в [77, определение. 4.2]). Факторы этого ряда называются композиционными факторами группы G.

Прежде, чем перейти к доказательству теоремы, введем некоторые обозначения и

приведем необходимые вспомогательные утверждения.

В следующей лемме сформулированы некоторые элементарные свойства централизаторов.

Лемма 1.1.1. *Пусть G — это группа и X, Y — подмножества в G. Тогда*

(1) $C_G(X) = \bigcap\limits_{x\in X} C_G(x)$;

(2) $C_G(X) = C_G(\langle X\rangle)$;

(3) $C_G(X) \leqslant C_G(Y)$ *тогда и только тогда, когда* $C_G(C_G(X)) \geqslant C_G(C_G(Y))$; *более того,* $C_G(X) = C_G(Y)$ *равносильно* $C_G(C_G(X)) = C_G(C_G(Y))$.

Следующая лемма является важным инструментом при доказательстве многих утверждений этой главы.

Лемма 1.1.2. [72, лемма 3] *Если элементарная абелева p-группа E порядка p^n действует точно на конечной нильпотентной p'-группе Q, то существует ряд подгрупп $E = E_0 > E_1 > E_2 > \cdots > E_n = 1$ такой, что все включения $C_Q(E_0) < C_Q(E_1) < \cdots < C_Q(E_n)$ строгие.*

Как обычно, через $O_p(G)$ обозначается наибольшая нормальная p-подгруппа конечной группы G, а через $O_{p'}(G)$ — наибольшая нормальная p'-подгруппа группы G. Если ряд коммутантов группы G стабилизируется, то $G^{(\infty)}$ обозначает последний член этого ряда. Квазипростая группа — это совершенное центральное расширение неабелевой простой группы. Слой $E(G)$ — это подгруппа группы G, порожденная всеми субнормальными квазипростыми подгруппами группы G, последние называются компонентами группы G. Напомним, что слой является центральным произведением компонент группы G.

Если q — степень некоторого простого числа, то F_q обозначает поле Галуа порядка q.

Для локально конечной группы G обозначим через $\mathrm{ncf}(G)$ количество неабелевых композиционных факторов группы G.

Следующий хорошо известный факт (см., например, [77, следствие 3.5]) позволяет свести доказательство теоремы к случаю конечной группы.

Лемма 1.1.3. *Если G — локально конечная локально разрешимая простая группа, то G циклическая.*

Если H — подгруппа группы G, то группа $\mathrm{Aut}_G(H) = N_G(H)/C_G(H)$ называется группой индуцированных автоморфизмов подгруппы H в группе G.

Пусть G — конечная группа и пусть $\overline{G}$ — ее фактор-группа по разрешимому радикалу. Пусть $\mathrm{Soc}(\overline{G})$ является прямым произведением простых групп $S_1, \ldots, S_n$. Хорошо известно, что группа $\overline{G}$ изоморфна подгруппе полупрямого произведения прямого произведения $\mathrm{Aut}_{\overline{G}}(S_1) \times \cdots \times \mathrm{Aut}_{\overline{G}}(S_n)$ и подгруппы симметрической группы Sym_n, переставляющей подгруппы $S_1, \ldots, S_n$. Из классификации конечных простых групп следует, что группа внешних автоморфизмов конечной простой группы разрешима. Следовательно, каждый неабелев композиционный фактор группы G является либо композиционным фактором

группы $\mathrm{Soc}(G/R)$, либо композиционным фактором соответствующей подгруппы группы Sym_n.

Следующие три леммы дают верхнюю грань для количества неабелевых композиционных факторов произвольной подгруппы группы Sym_n. Обозначим через $\delta(G)$ степень минимального точного подстановочного представления конечной группы G.

Лемма 1.1.4. [66, теорема 2] *Пусть G — конечная группа. Пусть $\mathfrak{L}$ — класс конечных групп, замкнутый относительно взятия подгрупп, гомоморфных образов и расширений. Если N — максимальная нормальная $\mathfrak{L}$-подгруппа группы G, то $\delta(G) \geqslant \delta(G/N)$.*

Лемма 1.1.5. [50, теорема 3.1] *Пусть S_1, S_2, …, S_r — простые конечные группы. Тогда $\delta(S_1 \times S_2 \times \cdots \times S_r) = \delta(S_1) + \delta(S_2) + \cdots + \delta(S_r)$.*

Лемма 1.1.6. *Если G — подгруппа симметрической группы Sym_n, то*

$$\mathrm{ncf}(G) \leqslant (n-1)/4.$$

Доказательство. Будем вести индукцию по n. Если R — разрешимый радикал группы G, то из леммы 1.1.4 следует, что число $\delta(G/R)$ не превосходит $\delta(G)$. Таким образом, можно считать, что разрешимый радикал группы G тривиален. Пусть цоколь $Soc(G)$ группы G — это прямое произведение неабелевых простых групп S_1, S_2, …, S_l. По лемме 1.1.5 имеем $l \leqslant n/5$. Группа G является подгруппой полупрямого произведения $(\mathrm{Aut}(S_1) \times \mathrm{Aut}(S_2) \times \cdots \times \mathrm{Aut}(S_l)) \leftthreetimes H$, где H — это подгруппа в Sym_l. По предположению индукции $\mathrm{ncf}(G) \leqslant n/5 + (n/5-1)/4 = (n-1)/4$. □

Замечание. Группа Sym_n, где $n = 5^k$ для $k \geqslant 1$, содержит подгруппу G, изоморфную подстановочному сплетению $(\ldots((Alt_5 \wr Alt_5) \wr Alt_5)\ldots)$, где сплетение берется $k-1$ раз. Имеем $\mathrm{ncf}(G) = \frac{5^k-1}{5-1} = \frac{n-1}{4}$.

Предложение 1.1.7. *Если G — конечная группа c-размерности k, то* $\mathrm{ncf}(G) < 5k$.

Доказательство. Пусть R — разрешимый радикал группы G. Если P — силовская подгруппа группы R, то $G/R \simeq N_G(P)/(R \cap N_G(P))$, и неабелевы композиционные факторы групп $N_G(P)$ и G совпадают. С другой стороны, c-размерность группы $N_G(P)$ как подгруппы группы G не превосходит k. Следовательно, мы можем считать, что $N_G(P) = G$ для каждой силовской подгруппы P группы G, т. е. что R нильпотентна.

Очевидно, мы можем считать, что $R \neq G$. Положим $\overline{G} = G/R$. Цоколь $\overline{L}$ группы $\overline{G}$ равен прямому произведению неабелевых простых групп S_1, $S_2, \ldots$, S_n. Как отмечено в предыдущем параграфе, группа $\overline{G}/\overline{L}$ — это расширение нормальной разрешимой подгруппы с помощью некоторой подгруппы симметрической группы Sym_n. По лемме 1.1.6 количество неабелевых композиционных факторов произвольной подгруппы группы Sym_n меньше $n/4$. Таким образом, достаточно показать, что $\mathrm{ncf}(\overline{L}) = n \leqslant 4k$. В частности, мы можем предполагать, что группа G совпадает с L, полным прообразом группы $\overline{L}$ в G, и что неабелевы композиционные факторы группы G — это группы S_1, $S_2, \ldots$, S_n.

Пусть $K = C_G(R)$. Нормальная подгруппа $\overline{K} = KR/R$ группы $\overline{G}$ является прямым произведением неабелевых простых групп. Без ограничения общности мы можем считать, что $\overline{K} = S_1 \times S_2 \times \ldots \times S_l$ для некоторого $1 \leqslant l \leqslant n$. Для $i = 1, \ldots, l$ обозначим через K_i полный прообраз группы S_i в K. Тогда подгруппа $H_i = K_i^{(\infty)}$ нормальна в K и является совершенным центральным расширением группы S_i, т. е. является компонентой группы K. Следовательно, если $E(K)$ — это слой группы K, то $KR = E(K)R$ и $E(K)$ — это центральное произведение подгрупп H_1, $H_2, \ldots$, H_l. Отсюда $\mathrm{ncf}(K) = \mathrm{ncf}(E(K)) = l$. Поскольку $[H_i, H_j] = 1$ при $i \neq j$, все включения $C_{E(K)}(H_1) < C_{E(K)}(H_1H_2) < \cdots < C_{E(K)}(H_1H_2 \ldots H_l)$ строгие. Таким образом, $l \leqslant k$.

Пусть P — силовская p-подгруппа группы G и $\overline{P}$ — образ P в группе $\overline{G}$. Поскольку $O_p(R) \leq C_G(O_{p'}(R))$, действие сопряжениями группы P на подгруппе $O_{p'}(R)$ индуцирует действие $\overline{P}$ на $O_{p'}(R)$. Для простого числа p определим множество $\mathcal{F}_p$ следующим образом: подгруппа S_i группы $\overline{G}$ лежит в $\mathcal{F}_p$ тогда и только тогда, когда существует элемент g порядка p в S_i, действующий точно на $O_{p'}(R)$. По лемме 1.1.2 имеем $|\mathcal{F}_p| \leqslant k$ для каждого простого числа p. С другой стороны, если S_i не лежит в $\mathcal{F}_p$, то S_i является подгруппой группы $C_G(O_{p'}(R))R/R$. По теореме Фейта–Томсона [51] и теореме Томсона–Глаубермана [53, глава II, следствие 7.3] порядок произвольной конечной неабелевой простой группы делится на 2 и не взаимно прост с 15. Поскольку $R = O_2(R) \times O_{2'}(R)$, каждая подгруппа S_i либо лежит в объединении $\mathcal{F}_2 \cup \mathcal{F}_3 \cup \mathcal{F}_5$, либо является подгруппой группы $\overline{K} = C_G(R)R/R$. Таким образом, $\mathrm{ncf}(G) \leq |\mathcal{F}_2| + |\mathcal{F}_3| + |\mathcal{F}_5| + \mathrm{ncf}(K) \leq 4k$, что и требовалось показать. □

Доказательство теоремы 1. Теперь G — локально конечная группа. Предположим, что $\mathrm{ncf}(G) \geq 5k$. Пусть $\{G_i\}_{i \in I}$ — композиционный ряд группы G, где I — это некоторое линейно упорядоченное множество и G_i — это собственная подгруппы группы G_j при $i < j$. Пусть S_1, S_2, …, S_{5k} — попарно различные неабелевы композиционные факторы группы G. По лемме 1.1.3 произвольная локально конечная неабелева простая группа содержит конечную неразрешимую группу. Следовательно, мы можем выбрать конечные подмножества X_1, X_2, …, X_{5k} группы G таким образом, чтобы образ множества X_i в S_i порождал неразрешимую подгруппу. Пусть H — конечная подгруппа группы G, порожденная объединением множеств X_1, X_2, …, X_{5k}. Тогда $\{G_i \cap H\}_{i \in I}$ — субнормальный ряд группы H, имеющий не менее чем $5k$ неразрешимых секций. Это противоречит предложению 1.1.7. Теорема доказана. □

§ 1.2. Контрпример ко второй части гипотезы Боровика–Хухро

В этом параграфе мы приведем серию контрпримеров ко второй части гипотезы Боровика–Хухро. Сначала мы докажем некоторые вспомогательные утверждения.

Пусть G — группа, а V — нормальная абелева подгруппа группы G. Пусть $^- : G \to G/V$ — естественный гомоморфизм. Действие сопряжениями группы G на V индуцирует действие группы G/V на V. В следующей лемме централизатор $C_V(\overline{Y})$ для $Y \leqslant G$ определяется относительно этого действия и поэтому совпадает с $C_V(Y)$.

Лемма 1.2.1. *Пусть G — группа, а V — ее нормальная абелева подгруппа. Предположим, что длина каждой цепи строго вложенных подгрупп в G/V не превосходит l. Тогда c-размерность группы G не превосходит $2l$. Если подгруппа V является центральной, то c-размерность G не превосходит l.*

Доказательство. Пусть c-размерность группы G равна k. Пусть[1]

$$Y_0 > \cdots > Y_k \tag{1.1}$$

— цепь подгрупп группы G таких, что

$$C_G(Y_0) < \cdots < C_G(Y_k). \tag{1.2}$$

Как и выше, $^- : G \to G/V$ — естественный гомоморфизм. С учетом (1.1) и (1.2) мы имеем следующие цепочки включений:

$$\overline{Y}_0 \geqslant \cdots \geqslant \overline{Y}_k, \tag{1.3}$$

$$C_V(Y_0) \leqslant \cdots \leqslant C_V(Y_k), \tag{1.4}$$

$$\overline{C_G(Y_0)} \leqslant \cdots \leqslant \overline{C_G(Y_k)}, \tag{1.5}$$

$$C_V(\overline{Y}_0) \leqslant \cdots \leqslant C_V(\overline{Y}_k). \tag{1.6}$$

Поскольку $C_G(Y_i)/C_V(Y_i) \cong \overline{C_G(Y_i)}$ и $C_G(Y_{i-1}) < G_G(Y_i)$ для каждого i, по крайней мере одно из включений

$$C_V(\overline{Y}_{i-1}) = C_V(Y_{i-1}) \leqslant C_V(Y_i) = C_V(\overline{Y}_i) \text{ и } \overline{C_G(Y_{i-1})} \leqslant \overline{C_G(Y_i)}$$

является строгим. Более того, если $C_V(\overline{Y}_{i-1}) < C_V(\overline{Y}_i)$, то $\overline{Y}_{i-1} > \overline{Y}_i$. Таким образом, k не превышает суммы чисел строгих включений в цепях (1.3) и (1.5) подгрупп группы G/V. Следовательно, $k \leqslant 2l$. Наконец, если V центральна, то все включения в (4) являются равенствами, а все включения в (5) строгие. □

Отметим, что оценка, полученная в общей ситуации в лемме 1.2.1, является неулучшаемой. Соответствующий пример построен в [99] в замечании после леммы 1.2.

Обозначим через $\Omega(n)$ число простых делителей положительного целого числа n с учетом кратностей, т.е. если $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ для простых чисел $p_1, \ldots, p_m$, то

$$\Omega(n) = \alpha_1 + \cdots + \alpha_m.$$

Для положительных целых чисел n и M положим

$$\pi_{n,M} = \{r \mid r - \text{ нечетное простое и } \Omega(r^n - 1) \leqslant M\}.$$

Очевидно, что для каждого n справедливы включения

$$\pi_{n,1} \subseteq \pi_{n,2} \subseteq \pi_{n,3} \subseteq \ldots \tag{1.7}$$

[1]Здесь и далее, $H < K$ обозначает строгое включение, то есть $H \leqslant K$ и $H \neq K$.

Большую роль при построении контрпримеров играет следующее теоретико-числовое утверждение.

Предложение 1.2.2 [24, теорема C]. *Для каждого положительного целого числа n существует положительное целое число M такое, что $\pi_{n,M}$ бесконечно.*

Для данного n положим

$$M_n = \min\{M \mid \pi_{n,M} \text{ бесконечно } \} \quad \text{и} \quad \pi_n = \pi_{n,M_n}.$$

Таким образом, π_n — это первое бесконечное множество в ряду (1.7).

Зафиксируем целое положительное число n и нечетное простое число r. Пусть

$$R_{n,r} - \text{ это экстраспециальная группа порядка } r^{2n+1} \text{ и периода } r.$$

Известно, что группа автоморфизмов $\mathrm{Aut}(R_{n,r})$ расщепляется над $\mathrm{Inn}(R_{n,r})$ [58, с. 404] и образ в $\mathrm{Out}(R_{n,r})$ централизатора в $\mathrm{Aut}(R_{n,r})$ подгруппы $Z(R_{n,r})$ изоморфен симплектической группе $Sp_{2n}(r)$ [28, с. 116]. Следовательно, группа $\mathrm{Aut}(R_{n,r})$ содержит подгруппу

$$A_{n,r} \cong Sp_{2n}(r),$$

централизующую $Z(R_{n,r})$. Рассмотрим естественное полупрямое произведение

$$X_{n,r} = R_{n,r}A_{n,r}.$$

Пусть p — простое число такое, что $p \equiv 1 \pmod{r}$. Известно [73, с. 151], что группа $R_{n,r}$ имеет точное неприводимое представление степени r^n над полем $\mathbb{F}_p$ порядка p. Более того, это представление продолжается до точного представления группы $X_{n,r}$ [25, 3A и 3B]. Пусть

$$V_{n,r} - \text{ это точный неприводимый } \mathbb{F}_pX_{n,r}\text{-модуль размерности } r^n,$$

соответствующий этому представлению, и положим

$$G_{n,r} = V_{n,r}X_{n,r}.$$

Следующее утверждение содержит список некоторых свойств группы $G_{n,r}$, которые легко следуют из ее определения.

Предложение 1.2.3.

(1) $F(G_{n,r}) = V_{n,r}$;

(2) $F^*(G_{n,r}/V_{n,r}) = F(G_{n,r}/V_{n,r}) \cong R_{n,r}$;

(3) $G_{n,r}/(R_{n,r}V_{n,r}) \cong A_{n,r} \cong Sp_{2n}(r)$.

Для натурального n положим

$$\overline{n} = 2\,\mathrm{lcm}(1, 2, \ldots, n) \text{ и } \mathscr{G}_n = \{G_{n,r} \mid r \in \pi_{\overline{n}}\}.$$

Заметим, что из определения следует, что множество $\mathscr{G}_n$ бесконечно.

Теорема 2. *Если n — произвольное натуральное число, то c-размерность произвольной группы из $\mathscr{G}_n$ не превосходит*

$$2\left((n+1)^2 + nM_{\overline{n}}\right). \tag{1.8}$$

Доказательство. Пусть $G = G_{n,r} \in \mathscr{G}_n$. По определению $r \in \pi_{\overline{n}}$ и

$$\Omega(r^{\overline{n}} - 1) \leqslant M_{\overline{n}}.$$

По теореме Лагранжа длина любой цепи строго вложенных подгрупп в $X_{n,r}$ не превосходит $l = \Omega(|X_{n,r}|)$. Поскольку

$$|X_{n,r}| = |R_{n,r}||A_{n,r}| = r^{2n+1}|Sp_{2n}(r)| = r^{(n+1)^2}\prod_{i=1}^{n}(r^{2i} - 1)$$

и $r^{2i} - 1$ делит $r^{\overline{n}} - 1$ для любого $i = 1, \ldots, n$, имеем

$$l = (n+1)^2 + \sum_{i=1}^{n}\Omega(r^{2i} - 1) \leqslant (n+1)^2 + n\Omega(r^{\overline{n}} - 1) \leqslant (n+1)^2 + nM_{\overline{n}}.$$

Таким образом, теорема справедлива в силу леммы 1.2.1. □

Теперь мы готовы показать основное утверждение данного параграфа

Теорема 3. *Утверждение* (2) *гипотезы Боровика–Хухро не выполнено.*

Доказательство. Допустим, что утверждение (2) гипотезы Боровика–Хухро справедливо. Зафиксируем натуральное n и рассмотрим множество $\mathscr{G}_n$. Теорема 2 влечет, что c-размерности групп из $\mathscr{G}_n$ ограничены числом, приведенным в (1.8). Тогда каждая группа $G_{n,r}/(R_{n,r}V_{n,r}) \cong Sp_{2n}(r)$ для $r \in \pi_{\overline{n}}$ содержит абелеву, а следовательно, и нормальную абалеву, подгруппу индекса, ограниченного в терминах n. Но группа $Sp_{2n}(r)$ содержит единственную собственную нормальную подгруппу, а именно, центр порядка 2, чей индекс растет вместе с r. Это противоречие завершает доказательство теоремы. □

Интересным представляется вопрос о том, для какого наименьшего значения c-размерности существует контрпример ко второй части гипотезы Боровика–Хухро. Предложение 1.2.2 имеет следующее уточнение [24, следствие 4.2]: существует бесконечного много простых r таких, что $\Omega(r^2 - 1) \leqslant 21$. Отсюда вытекает, что $M_2 \leqslant 21$ и, значит, следующее утверждение напрямую вытекает из теоремы 2.

Следствие 1.2.4. *Если G — это группа из $\mathscr{G}_1$, то* $\mathrm{cdim}(G) \leqslant 50$.

Таким образом, наименьшая c-размерность, для которой может быть построен контрпример, не превосходит 50.

§ 1.3. Строение локально конечных групп конечной c-размерности

В этом параграфе мы дадим описание структуры локально конечных групп конечной c-размерности и докажем ослабленную версию второго утверждения гипотезы Боровика–Хухро.

Сначала введем некоторые обозначение и приведем необходимые предварительные утверждения.

Для группы G обозначим через $l(G)$ точную верхнюю грань длин цепей строго вложенных подгрупп группы G.

Идея доказательства следующего утверждения в основном повторяет идею из [71, лемма 3.20].

Предложение 1.3.1. *Пусть G — группа и N — ее нормальная подгруппа. Предположим, что $l(G/N)$ равно l для некоторого натурального числа l. Если N является $\mathfrak{M}_c$-группой, то G также $\mathfrak{M}_c$-группа. Если N имеет конечную c-размерность k, то c-размерность G также конечна и не превосходит $(l+1)^2(k+1)$.*

Доказательство. Пусть $C_1 < C_2 < \cdots < C_i < \ldots$ — строго возрастающая цепь централизаторов в группе G. Поскольку $l(G/N) = l$, цепь

$$C_1N \leqslant C_2N \leqslant \cdots \leqslant C_iN \leqslant \ldots$$

содержит не более чем $l+1$ различных подгрупп. Таким образом, без ограничения общности можем считать, что $C_iN = C_jN$ для всех подгрупп цепи. Тогда $C_i = C_1(C_i \cap N)$ и $C_G(C_i) = C_G(C_1) \cap C_G(C_i \cap N)$. Следовательно, подгруппы $C_G(C_i \cap N)$ образуют строго убывающую цепь централизаторов. Поскольку фактор-группа $C_G(C_i \cap N)/C_N(C_i \cap N)$ является подгруппой в G/N, длина этой цепи, равно как и исходной цепи, конечна. Это доказывает утверждение об $\mathfrak{M}_c$-группах. Аналогичное рассуждение показывает, что если $\operatorname{cdim}(N) = k$, то $\operatorname{cdim}(G) \leqslant (l+1)^2(k+1)$, что и требуется. □

Лемма 1.3.2. *Пусть G — это центральное произведение конечных групп H и K. Тогда* $\operatorname{cdim}(G) \geqslant \operatorname{cdim}(H) + \operatorname{cdim}(K)$.

Доказательство. Пусть

$$H_0 < H_1 < \cdots < H_m \quad \text{и} \quad K_0 < K_1 < \cdots < K_l$$

— это ряды подгрупп групп H и K таких, что ряды их централизаторов имеют максимальные длины. Мы можем считать, что и H, и K являются подгруппами в G, и, следовательно, все их подгруппы также являются подгруппами в G. Имеем $C_G(H_i) = C_H(H_i) \circ K$ и $C_G(HK_i) = Z(H) \circ C_K(K_i)$. Следовательно, подгруппы H_i и HK_i дают ряд подгрупп с цепью централизаторов требуемой длины. □

В [99] в замечании после леммы 1.4 приведен пример, показывающий, что c-размерность центрального произведения может быть больше суммы c-размерностей сомножителей.

Напомним, что p-рангом конечной группы G для простого числа p называется наибольший ранг ее элементарных абелевых p-подгрупп.

Лемма 1.3.3. *Пусть $r \in \{2, 3, 5\}$. Существует константа $c > 0$ такая, что r-ранг произвольной конечной неабелевой простой группы G, чей порядок делится на r, не меньше, чем $c\lambda(G)$.*

Доказательство. Для спорадических групп утверждение леммы тривиально. В случае знакопеременных групп утверждение очевидно. В случае групп лиева типа оно следует, например, из [54, часть I, 10-6]. □

Лемма 1.3.4. *Пусть G — общая линейная группа размерности n. Тогда* $\mathrm{cdim}(G) \leqslant n^2 - 1$.

Доказательство. Это утверждение напрямую следует из того факта, что общая линейная группа может быть вложена в соответствующую алгебру матриц, в которой централизаторы являются подалгебрами. Этот факт неоднократно отмечался ранее (см., например, [79, предложение 2.1] или [49, пример 3.2, пункт 2]). □

Поскольку симметрическая группа Sym_n имеет точное линейное представление размерности $n - 1$, следующая лемма является прямым следствием предыдущей.

Лемма 1.3.5. $\mathrm{cdim}(\mathrm{Alt}_n) \leqslant (n-1)^2 - 1$.

Лемма 1.3.6. *Если G — группа лиева типа лиева ранга n, то c-размерность группы G ограничена сверху функцией от n.*

Доказательство. Группа лиева типа является группой автоморфизмов конечномерной алгебры Ли. Размерность этой алгебры является функцией от n. Следовательно, произвольная группа лиева типа может быть вложена в группу $GL_l(q)$ для некоторого l, зависящего от n и лиева типа группы G. Поскольку c-размерность подгруппы не превосходит c-размерности объемлющей группы, утверждение следует из леммы 1.3.4. □

Определим класс $\mathfrak{C}$ локально конечных групп следующим образом. Группа G лежит в $\mathfrak{C}$ тогда и только тогда, когда G имеет конечное число неабелевых композиционных факторов и каждый неабелев композиционный фактор группы G является линейной группой. Напомним, что простая неабелева линейная локально конечная группа является группой лиева типа над локально конечным полем [5, 6, 64, 83].

Обозначим через λ функцию, отображающую класс $\mathfrak{C}$ в множество натуральных чисел по следующему правилу. Сначала определим функцию на неабелевых простых группах. Если G — это локально конечная группа лиева типа, то $\lambda(G)$ является минимумом лиевых рангов групп лиева типа, изоморфных G (под лиевым рангом здесь подразумевается ранг соответствующей (B, N)-пары [28, с. 249]). Если G — это знакопеременная группа, то $\lambda(G)$ — это степень группы G (за исключением групп Alt_5, Alt_6 и Alt_8, которые изоморфны группам лиева типа и для которых уже определено значение $\lambda(G)$). Положим $\lambda(G) = 1$ для спорадических групп. Если G — произвольная $\mathfrak{C}$-группа, то $\lambda(G)$ определяется как сумма чисел $\lambda(S)$, где S пробегает множество неабелевых композиционных факторов группы G.

Лемма 1.3.7. *Существует универсальная константа b такая, что*

$$\lambda(\mathrm{E}(G)) \leqslant b \cdot \mathrm{cdim}(G)$$

для произвольной конечной группы G.

Доказательство. Поскольку c-размерность подгруппы не превосходит c-размерности объемлющей группы, можем считать, что $G = E(G)$. По лемме 1.3.2 можно считать, что группа G квазипроста. Обозначим через $^-$ естественный гомоморфизм из G на $G/Z(G)$. Заметим, что если $\overline{G}$ является спорадической, либо группой лиева типа ограниченного лиева ранга, либо знакопеременной группой ограниченной степени, то константа b может быть выбрана достаточно большой, чтобы сделать утверждение леммы тривиальным. Таким образом, можно считать, что $\overline{G}$ является либо знакопеременной группой достаточно большой степени, либо классической группой достаточно большого лиева ранга.

Предположим, что существует простой делитель r порядка группы $\overline{G}$, удовлетворяющий следующим двум условиям. Во-первых, он взаимно прост с порядком центра $Z(G)$. Во-вторых, существует цепь вложенных подмножеств r-элементов такая, что ее длина l ограничена снизу линейной функцией от $\lambda(G)$ (не зависящей от G) и централизаторы различных. Очевидно, что любое множество r-элементов группы $\overline{G}$ может быть представлено как образ $\overline{M}$ некоторого подмножества M группы G, также состоящего из r-элементов. Пусть $M_0 \subset M_1 \subset \cdots \subset M_l \subset G$ — это цепь подмножеств r-элементов таких, что

$$C_{\overline{G}}(\overline{M}_0) > C_{\overline{G}}(\overline{M}_1) > \cdots > C_{\overline{G}}(\overline{M}_l).$$

Поскольку порядки элементов из M_i и порядок группы $Z(G)$ взаимно просты, имеем $C_{\overline{G}}(\overline{M_i}) = \overline{C_G(M_i)}$. Следовательно,

$$C_G(M_0) > C_G(M_1) > \cdots > C_G(M_l).$$

Таким образом, l не превосходит c-размерности группы G. Наконец, требуемое неравенство следует из того, что число l ограниченно снизу линейной функцией от $\lambda(G)$. Осталось показать, что такое простое r существует для произвольной группы G.

Рассмотрим условие, что r не делит порядок центра $Z(G)$. Каждый простой делитель порядка группы $Z(G)$ является простым делителем порядка мультипликатора Шура $M(\overline{G})$ группы $\overline{G}$. Порядки мультипликаторов Шура всех конечных неабелевых простых групп известны (см., например, [55, параграф 6.1]. Согласно этой информации, если $M(\overline{G})$ не $\{2,3\}$-группа, то группа $\overline{G}$ изоморфна $A_n(q)$ или ${}^2A_n(q)$ и все простые делителя порядка группы $M(\overline{G})$ делят $6(q^2-1)$. Таким образом, r следует выбирать с учетом этих ограничений.

Теперь рассмотрим второе ограничение на r, т.е. линейную нижнюю границу на максимальную длину цепи централизаторов r-элементов. Если G — это знакопеременная группа Alt_n, то r положим равным 5. Для $1 \leqslant i \leqslant \frac{n}{5}$ можно выбрать вложенные множества M_i, состоящие из i независимых циклов длины 5. Их централизаторы образуют строго

убывающую цепь длины не менее $\frac{n}{5}-1$. Таким образом, по определению функции λ в качестве нижней оценки для l можно взять $\frac{\lambda(G)}{5}-1$.

Пусть $\overline{G}$ — это классическая группа над полем порядка q. Согласно [40, предложения 7–12] группа $\overline{G}$ содержит центральное произведение квазипростых групп $H_1, \ldots, H_s$, где каждая группа H_i является группой лиева типа A_3 или ${}^2A_3$ над полем порядка q. Более того, число s этих факторов не меньше, чем $\frac{\lambda(G)-6}{4}$. По теореме Жигмонди существует простое число r, делящее порядок каждой H_i, но не $6(q^2-1)$. Для каждого $i=1,\ldots,s$ пусть $h_i \in H_i$ — это элемент порядка r. Тогда h_i не является центральным в H_i. Следовательно,

$$C_{\overline{G}}(h_1) > C_{\overline{G}}(h_1,h_2) > \cdots > C_{\overline{G}}(h_1,h_2,\ldots,h_s),$$

и мы имеем строго убывающую цепь централизаторов множеств r-элементов, чья длина не меньше $\frac{\lambda(G)-6}{4}-1$, что завершает доказательство леммы. □

Лемма 1.3.8. *Существует универсальная константа d такая, что*

$$\lambda(G) \leqslant d \cdot \operatorname{cdim}(G)$$

для произвольной конечной группы G.

Доказательство. Обозначим через R разрешимый радикал группы G. Если P — это силовская подгруппа группы R, то $G/R \cong N_G(P)/(R \cap N_G(P))$. В частности, неабелевы композиционные факторы групп $N_G(P)$ и G совпадают. Кроме того, c-размерность группы $N_G(P)$ как подгруппы группы G не превосходит k. Следовательно, можно считать, что R является подгруппой Фиттинга группы G.

Положим $\overline{G} = G/R$. Обозначим через t число неабелевых композиционных факторов цоколя $\overline{L}$ группы $\overline{G}$ (напомним, что $\overline{L}$ является прямым произведением неабелевых простых групп). Фактор-группа $\overline{G}/\overline{L}$ является расширением разрешимой группы с помощью подгруппы из Sym_l. Из теоремы 1 следует, что число t меньше $5k$. Следовательно, $\lambda(\overline{G}/\overline{L}) < 25k/4$ по лемме 1.1.6. Таким образом, достаточно показать, что $\lambda(\overline{L}) \leqslant d' \cdot k$ для некоторого d'. В частности, можно предполагать, что G совпадает с полным прообразом $\overline{L}$ в G.

Пусть $\mathcal{F}$ — это множество неабелевых композиционных факторов группы $C_G(R)$. Для простого числа p обозначим через $\mathcal{F}_p$ множество тех неабелевых композиционных факторов группы $G/C_G(O_{p'}(R))$, порядок которых делится на p. Как упоминалось выше, порядок произвольной конечной неабелевой простой группы делится на 2 и не взаимно прост с 15. Поскольку $R = O_{p'}(R)O_{q'}(R)$ для различных простых p и q, имеем $C_G(O_{p'}(R)) \cap C_G(O_{q'}(R)) = C_G(R)$. Следовательно, каждый неабелев композиционный фактор группы G содержится в объединении $\mathcal{F} \cup \mathcal{F}_2 \cup \mathcal{F}_3 \cup \mathcal{F}_5$, и для доказательства леммы достаточно ограничить значения функции λ на каждом из четырех множеств линейной функцией от k.

Положим $K = C_G(R)$. Поскольку группа $\overline{K} = KR/R$ нормальна в $\overline{G}$, она является прямым произведением элементов из $\mathcal{F}$. Пусть $\overline{S}$ — это элемент множества $\mathcal{F}$ и пусть S —

это полный прообраз $\overline{S}$ в K. Тогда $S^{(\infty)}$ является совершенным центральным расширением группы $\overline{S}$, которое нормально в K, т.е. компонентой K. Следовательно, все группы из $\mathcal{F}$ являются композиционными факторами слоя $E(K)$. Поскольку $E(K)$ — это подгруппа в $E(G)$, число $\lambda(K)$ ограничено сверху числом $b{\cdot}k$ для некоторой константы b в соответствии с леммой 1.3.7.

Положим $K_p = G/C_G(O_{p'}(R))$ для $p \in \{2,3,5\}$. Очевидно, что K_p — это расширение прямого произведения некоторых композиционных факторов группы G с помощью нильпотентной p'-группы. По определению K_p действует точно на $O_{p'}(R)$, так же как и ее силовская p-подгруппа P. Подгруппа P является прямым произведением силовских p-подгрупп элементов множества $\mathcal{F}_p$. По лемме 1.3.3 группа P содержит элементарную абелеву p-подгруппу, чей ранг ограничен снизу числом $c\sum_{S\in\mathcal{F}_p}\lambda(S)$ для некоторой положительной константы c. Лемма 1.1.2 влечет, что $c\sum_{S\in\mathcal{F}_p}\lambda(S) \leqslant k$.

Наконец, $\lambda(G) \leqslant 3k/c + b\cdot k$, что и требовалось. □

Лемма 1.3.9. *Пусть G — локально конечная группа и Q — компонента группы G. Обозначим через $^-$ естественный гомоморфизм из G на G/R, где R — локально разрешимый радикал группы G. Тогда* $\mathrm{Aut}_G(Q) \simeq \mathrm{Aut}_{\overline{G}}(\overline{Q})$.

Доказательство. По определению $\mathrm{Aut}_{\overline{G}}(\overline{Q}) \simeq N_{\overline{G}}(\overline{Q})/C_{\overline{G}}(\overline{Q})$. Полный прообраз $N_{\overline{G}}(\overline{Q})$ в G равен $N_G(QR)$. Равенство $Q = E(QR)$ влечет, что Q характеристическая подгруппа группы QR и, следовательно, $N_G(QR) = N_G(Q)$. Поскольку $\overline{C_G(Q)} \leqslant C_{\overline{G}}(\overline{Q})$, группа $\mathrm{Aut}_{\overline{G}}(\overline{Q})$ является гомоморфным образом группы $\mathrm{Aut}_G(Q)$. Поскольку обе эти группы почти простые, они изоморфны, что и требовалось показать. □

Лемма 1.3.10. *Если G — локально конечная группа конечной c-размерности k, то G содержит конечную подгруппу H такую, что $cdim(H) = k$.*

Доказательство. Поскольку c-размерность группы G равна k, существуют упорядоченный набор элементов $x_1, \ldots, x_k$ группы G такой, что

$$G = C_G(1) > C_G(x_1) > C_G(x_1, x_2) > \cdots > C_G(x_1, x_2, \ldots, x_k),$$

т.е. дающий цепь централизаторов максимальной длины. Выберем

$$h_i \in C_G(x_1, x_2, \ldots, x_i) \setminus C_G(x_1, x_2, \ldots, x_{i+1})$$

для $0 \leqslant i < k$. Легко видеть, что c-размерность конечной группы, порожденной элементами $x_1, \ldots, x_k$ и $h_1, \ldots, h_{k-1}$, равна k, что завершает доказательство леммы. □

Напомним некоторую информацию о локально конечных полях (подробности и доказательства приведенных фактов можно найти, например, в [34]).

Число Штейница — это формальное произведение

$$\prod_{i=0}^{\infty} p_i^{x_i},$$

где p_i обозначает i-ое простое число, а x_i — элемент расширенного множества натуральных чисел $\{0, 1, \ldots, n, \ldots, \infty\}$. Одно число Штейница N_1 делит другое N_2, если для любого i

степень, с которой p_i входит в N_1, не превосходит соответствующей степени в N_2. Очевидно, что натуральные числа с отношением делимости являются подсистемой в системе чисел Штейница с отношением делимости. Пусть N — число Штейница и q — натуральная степень простого числа. Положим

$$\mathrm{F}_{q^N} = \bigcup_{d|N} \mathrm{F}_{q^d},$$

где объединение берется по всем натуральным делителям d. Любое локально конечное поле изоморфно F_{q^N} для некоторой степени простого числа q и числа Штейница N.

Группа автоморфизмов поля F_{q^N} — это обратный предел групп автоморфизмов его конечных подполей. Каждый гомоморфный образ группы $\mathrm{Aut}(\mathrm{F}_{q^N})$ является циклической группой.

Если S — группа лиева типа над полем F, то обозначим через Φ_S группу полевых автоморфизмов группы S, т.е. автоморфизмов, действующих на корневых подгруппах по правилу $x_r(t) \mapsto x_r(t^\sigma)$ для некоторого автоморфизма σ поля F. Если S не является группой лиева типа, то положим $\Phi_S = 1$.

Лемма 1.3.11. *Пусть G — группа такая, что слой $\mathrm{E}(G)$ — это группа лиева типа S над локально конечным полем F и $G \leqslant S\Phi_S$. Если c-размерность группы G конечна и равна k, то $l(G/S) \leqslant k$.*

Доказательство. Допустим, что $l(G/S) > k$. Тогда существует конечное подполе K поля F такое, что образ A группы G/S в группе автоморфизмов поля K удовлетворяет неравенству $l(A) > k$. Пусть X — подгруппа некоторой корневой подгруппы, состоящая из элементов $x_r(t)$, где $t \in K$. Если B и C — это различные подгруппы группы A, то $C_X(B) \neq C_X(C)$. Следовательно, c-размерность группы G не меньше $l(A)$, что противоречит предположению. □

Напомним, что группа называется p-разрешимой, если она имеет конечный нормальный ряд, в котором каждая секция либо p'-группа, либо разрешимая p-группа. В следующей лемме $S_p(G)$ обозначает локально p-разрешимый радикал группы G. Группа называется p-совершенной, если она совершенна и порождается своими p-элементами. Группа удовлетворяет сильной теореме Силова для простого p, если каждая ее подгруппа удовлетворяет теореме Силова для этого простого числа.

Лемма 1.3.12. [70, теорема 4.3] *Пусть $p > 3$ — простое число. Если локально конечная группа G не является p-разрешимой и удовлетворяет сильной теореме Силова для p, то цоколь $\mathrm{Soc}(X)$ фактор-группы $X \simeq G/S_p(G)$ — это прямое произведение конечного числа линейных простых p-совершенных подгрупп. Более того, централизатор $C_X(\mathrm{Soc}(X))$ тривиален.*

Следующая теорема дает пример нечастой ситуации, когда можно контролировать c-размерность фактор-группы. Кроме того, она является инструментом при описании локально конечных групп конечной c-размерности.

Теорема 4. *Пусть G — локально конечная группа конечной c-размерности k. Пусть $\overline{G}$ — ее фактор-группа по локально разрешимому радикалу. Тогда c-размерности группы $\overline{G}$ ограничена в терминах k.*

Сначала мы докажем эту теорему для конечных групп.

Предложение 1.3.13. *Пусть G — конечная группа конечной c-размерности k. Пусть $\overline{G}$ — ее фактор-группа по разрешимому радикалу. Тогда c-размерности группы $\overline{G}$ ограничена в терминах k.*

Доказательство. Цоколь группы $\overline{G}$ — это прямое произведение конечных неабелевых простых групп. Обозначим через $\mathfrak{S}$ множество композиционных факторов этого цоколя. По лемме 1.3.8 число $\lambda(\mathrm{Soc}(\overline{G}))$ ограничено линейной функцией от k; в частности, количество элементов множества $\mathfrak{S}$ ограничено в терминах k. Из лемм 1.3.5 и 1.3.6 следует, что c-размерность $\mathrm{Soc}(\overline{G})$ также ограничена в терминах k. Из предложения 1.3.1 следует, что c-размерность $\overline{G}$ ограничена в терминах c-размерности $\mathrm{Soc}(\overline{G})$ и числа $l(\overline{G}/\mathrm{Soc}(\overline{G}))$. Группа $G/\mathrm{Soc}(\overline{G})$ является подгруппой в

$$\prod_{S\in\mathfrak{S}} \mathrm{Out}_{\overline{G}}(S) \rtimes H,$$

где $\mathrm{Out}_{\overline{G}}(S)$ обозначает группу внешних индуцированных автоморфизмов подгруппы S в $\overline{G}$, т.е. фактор-группу $\mathrm{Aut}_{\overline{G}}(S)$ по S, и H — некоторая подгруппа в соответствующей симметрической группе. Поскольку порядок группы H ограничен в терминах $|\mathfrak{S}|$, для доказательства предложения достаточно показать, что число $l(\mathrm{Out}_{\overline{G}}(S))$ ограничено функцией от k для любого $S \in \mathfrak{S}$.

Положим $\Phi = \prod_{S\in\mathfrak{S}} \Phi_S$. Пусть $\widehat{\ }$ — естественный гомоморфизм из $\mathrm{Aut}(\mathrm{Soc}(\overline{G}))$ в группу внешних автоморфизмов $\mathrm{Out}(\mathrm{Soc}(\overline{G}))$. Хорошо известно, что если S — конечная неабелева простая группа, не являющаяся группой лиева типа, то порядок группы $\mathrm{Out}(S)$ не превосходит 2, а если S — группа лиева типа, то индекс $\widehat{\Phi_S}$ в $\mathrm{Out}(S)$ ограничен функцией от лиева ранга группы S. Следовательно, индекс $\widehat{\Phi}$ в $\mathrm{Out}(\mathrm{Soc}(\overline{G}))$ ограничен в терминах $\lambda(\mathrm{Soc}(\overline{G}))$. Таким образом, индекс $\widehat{\Phi}\cap\overline{G}/\mathrm{Soc}(\overline{G})$ в $\overline{G}/\mathrm{Soc}(\overline{G})$ ограничен в терминах k. По предложению 1.3.1 можно считать, что фактор-группа $\overline{G}/\mathrm{Soc}(\overline{G})$ является подгруппой в $\widehat{\Phi}$.

Пусть R — разрешимый радикал группы G. Пусть P — силовская подгруппа R. По аргументу Фраттини $G = RN_G(P)$. Следовательно, $\overline{G} \simeq N_G(P)/N_R(P)$, и можно заменить группу G на $N_G(P)$, не теряя общности. Более того, поскольку это можно проделать для всех силовских подгрупп группы R, можно считать, что группа R нильпотентна. Пусть $S \in \mathfrak{S}$ — группа лиева типа над полем порядка p^α, где p — простое число. Если X_r — корневая подгруппа группы S, то центр $\mathrm{Z}(X_r)$ — это элементарная абелева подгруппа, чей ранг не меньше $\alpha/2$. Группа $\mathrm{Z}(X_r)$ действует на $O_{p'}(R)$, и либо это действие точное, либо S является композиционным фактором группы $C_G(O_{p'}(R))$. Если действие точное, то лемма 1.1.2 влечет, что $\alpha/2 \leqslant k$ и, следовательно, порядок группы Φ_S не превосходит $2k$.

Предположим, что S является композиционным фактором группы $C_G(O_{p'}(R))$. Снова

имеем два случая: либо S является композиционным фактором централизатора $C_G(R)$, либо S — композиционный фактор группы $\mathrm{Aut}_G(O_p(R))$.

Если S — это композиционный фактор $C_G(R)$, то S — композиционный фактор слоя $\mathrm{E}(G)$ и существует квазипростая подгруппа T группы G такая, что $T/\mathrm{Z}(T) \simeq S$. По лемме 1.3.9 группа $\mathrm{Aut}_G(T)$ изоморфна группе $\mathrm{Aut}_{\overline{G}}(S)$. Из леммы 1.3.11 следует, что $l(\mathrm{Out}_G(T)) \leqslant k$, что и требовалось.

Пусть S —композиционный фактор $\mathrm{Aut}_G(O_p(R))$. Поскольку группа S — композиционный фактор $C_G(O_{p'}(R))$, она является композиционным фактором слоя группы $G/O_p(R)$. Обозначим через T соответствующую компоненту группы $G/O_p(R)$. За конечным числом исключений (точный список исключений может быть найден, например, в [55, таблица 6.1.3]), группа T также является группой лиева типа. Поскольку целью является ограничение числа $l(\mathrm{Out}_{\overline{G}}(S))$, эти исключения можно не рассматривать. По лемме 1.3.9 группа индуцированных автоморфизмов подгруппы T совпадает с группой $\mathrm{Aut}_{\overline{G}}(S)$.

Обозначим через A полный прообраз группы $G/O_p(R)$ в группе $\mathrm{Out}_{G/O_p(R)}(T)$ (напомним, что по предположению последняя является подгруппой в Φ_T). В частности, A — циклическая группа. Рассмотрим подгруппу Картана C группы T (структура подгрупп Картана описана в [55, теорема 2.4.7]). Если элементы σ_1, $\sigma_2 \in A$ имеют различные порядки, то $C_C(\sigma_1) \neq C_C(\sigma_2)$. Для произвольной подгруппы группы A существует элемент группы C, централизуемый этой подгруппой, но не централизуемый большей подгруппой. Следовательно, существуют элементы c_1, c_2, …, $c_{l(A)}$ группы C такие, что

$$C_{G/O_p(R)}(c_1, c_2, \ldots, c_i) > C_{G/O_p(R)}(c_1, c_2, \ldots, c_{i+1})$$

для $1 \leqslant i < l(A)$. Пусть c'_1, …, $c'_{l(A)}$ — это некоторые прообразы этих элементов в группе G, которые также являются p'-элементами. Поскольку $C_{G/O_p(R)}(c_i) = C_G(c'_i)O_p(G)/O_p(G)$, имеем

$$C_G(c_1, c_2, \ldots, c_i) > C_G(c_1, c_2, \ldots, c_{i+1})$$

для $1 \leqslant i < l(A)$. Таким образом, $l(A) \leqslant \mathrm{cdim}(G)$, что, как замечено выше, завершает доказательство предложения. □

Доказательство теоремы 4. Пусть f — неубывающая функция такая, что для любой конечной группы G имеем

$$\mathrm{cdim}(G/R) \leqslant f(\mathrm{cdim}(G)),$$

где R — разрешимый радикал группы G. Пусть G — локально конечная группа c-размерности k и R — ее локально разрешимый радикал. Предположим, что

$$\mathrm{cdim}(G/R) > f(\mathrm{cdim}(G)).$$

По лемме 1.3.10 существует конечная подгруппа $\overline{H}$ группы G/R такая, что $\mathrm{cdim}(\overline{H}) > f(\mathrm{cdim}(G))$. Пусть H — конечный прообраз группы $\overline{H}$ в G. Обозначим через Σ локальную систему группы G, состоящую из конечных подгрупп (определение локальной системы

может быть найдено в [71, с. 8]). Пусть X — некоторый элемент в Σ, содержащий H. Известно (см. [71, с. 12–15]), что существует $Y \in \Sigma$ такой, что $X \cap R$ совпадает с пересечением подгруппы X с разрешимым радикалом $R(Y)$ подгруппы Y. Следовательно, группа $\overline{H}$ изоморфна подгруппе группы $Y/R(Y)$. Поскольку $\mathrm{cdim}(Y) \leqslant \mathrm{cdim}(G)$, имеем противоречие с предложением 1.3.13. □

Предложение 1.3.14. *Пусть G — локально конечная группа конечной с-размерности k и R — ее локально разрешимый радикал. Тогда цоколь L/R группы $\overline{G} = G/R$ является прямым произведением конечного числа линейных простых групп и $\lambda(L/R)$ ограничено линейной функцией от k. При этом централизатор $C_{\overline{G}}(L/R)$ тривиален.*

Доказательство. По теореме 1 число неабелевых композиционных факторов группы G меньше $5k$. Следовательно, существует конечное множество простых чисел P такое, что каждое число из P больше 3 и каждый неабелев композиционный фактор группы G содержит элемент порядка, лежащего в P, в частности, G не p-разрешима для любого $p \in P$.

Из [35, теорема B] следует, что локально конечная группа с условием минимальности для централизаторов удовлетворяет сильной теореме Силова для любого простого числа p. Лемма 1.3.12 влечет, что группа $\overline{G}$ изоморфна подпрямому произведению групп $X_p = G/S_p(G)$ по всем $p \in P$. Более того, $C_{X_p}(\mathrm{Soc}(X_p)) = 1$ для всех $p \in P$.

Сначала покажем, что $C_{\overline{G}}(L/R) = 1$. Поскольку локально разрешимый радикал группы $\overline{G}$ тривиален, достаточно показать, что каждая нетривиальная нормальная подгруппа N группы $\overline{G}$ содержит минимальную нормальную подгруппу. Пусть φ_p — проекция на X_p. Можно считать, что образ $N\varphi_p$ либо тривиален, либо является минимальной нормальной подгруппой в X_p. Действительно, если $N\varphi_p \neq 1$, то по лемме 1.3.12 группа $N\varphi_p$ содержит минимальную нормальную подгруппу M_p группы X_p и, не уменьшая общности, можно заменить N на полный прообраз M_p в N. Таким образом, группа N является подпрямым произведением конечного числа простых групп и, следовательно, является прямым произведением простых групп. Теперь с необходимостью N содержит минимальную нормальную подгруппу группы G. Аналогичное рассуждение показывает, что любая минимальная нормальная подгруппа группы $\overline{G}$ является прямым произведением конечного числа простых групп, то же верно и для L/R.

Как уже упоминалось, каждая линейная локально конечная простая группа является группой лиева типа над локально конечным полем и, следовательно, содержит конечную подгруппу того же лиева типа. Значит, число $\lambda(L/R)$ ограничено линейной функцией от k по лемме 1.3.8, что завершает доказательство предложения. □

Теперь мы готовы дать описание структуры групп из названия главы.

Теорема 5. *Пусть G — локально конечная группа конечной с-размерности k. Существует нормальный ряд*

$$R \leqslant L \leqslant A \leqslant G,$$

такой, что выполнены следующие утверждения.

(1) R — *(локально) разрешимый радикал, чья ступень разрешимости ограничена в терминах* k.

(2) L/R — *цоколь группы* G/R *и* $C_{G/R}(L/R) = 1$. *Группа* L/R *является прямым произведением линейных простых групп, причем число* $\lambda(L/R)$ *ограничено линейной функцией от* k.

(3) A/L — *абелева группа и число* $l(A/L)$ *ограничено в терминах* k.

(4) *Индекс* A *в* G *ограничен в терминах* k.

Доказательство. Пункт (1) теоремы — это в точности пункт (a) теоремы Хухро [72]. Пункт (2) доказан в предложении 1.3.14. Таким образом, остается доказать пункты (3) и (4). По теореме 4 можно предполагать, что $R = 1$. Следовательно, L совпадает с $\mathrm{Soc}(G)$. Поскольку $C_G(L) = 1$, можно рассматривать G как подгруппу в $\mathrm{Aut}(L)$. Пусть Φ — это произведение групп Φ_S, где S пробегает все композиционные факторы группы L. Положим $F = L\Phi$ и $A = G \cap F$. Поскольку индекс F в $\mathrm{Aut}(L)$ ограничен в терминах $\lambda(L)$, индекс A в G ограничен в терминах k. Кроме того, группа A/L абелева. Остается показать, что число $l(A/L)$ ограничено в терминах k. По лемме 1.3.11 число $l(\mathrm{Out}_A(S))$ ограничено функцией от k для любого композиционного фактора S группы L. Раз число неабелевых композиционных факторов группы L также ограничено в терминах k, доказательство теоремы завершено. □

Из теоремы 5 несложно вывести следующее утверждение, которое близко по формулировке ко второму утверждению гипотезы Боровика–Хухро.

Теорема 6. *Пусть* G — *локально конечная группа с-размерности* k. *Пусть* $\overline{G}$ — *ее фактор-группа по третьему радикалу Хирша–Плоткина* $\mathrm{F}_3(G)$. *Тогда фактор-группа группы* $\overline{G}$ *по слою* $\mathrm{E}(\overline{G})$ *содержит конечную абелеву подгруппу* A, *у которой индекс и* $l(A)$ *ограничены в терминах* k.

Доказательство. По теореме Хухро [72] локально разрешимый радикал R группы $\overline{G}$ конечен и имеет порядок, ограниченный в терминах k.

Покажем, что централизатор $C_{\overline{G}}(\mathrm{F}^*(\overline{G}))$ содержится в $\mathrm{F}^*(\overline{G})$. Положим $C = C_{\overline{G}}(\mathrm{F}^*(\overline{G}))$. Легко видеть, что $\mathrm{F}^*(C) \leqslant \mathrm{F}^*(\overline{G}) \leqslant C_{\overline{G}}(C)$. Следовательно, $\mathrm{F}^*(C) = \mathrm{Z}(C)$. Предположим, что $C \neq \mathrm{F}^*(C)$. Если $C \cap R \neq \mathrm{F}^*(C)$, то группа $C/\mathrm{F}^*(C)$ содержит циклическую субнормальную подгруппу, полный прообраз которой абелев и субнормален в C и, следовательно, должен лежать в $\mathrm{F}^*(C)$, противоречие. Значит, $C \cap R = \mathrm{F}^*(C)$. Отсюда заключаем, что $C/\mathrm{F}^*(C)$ является нетривиальной нормальной подгруппой в $\overline{G}/R$. Из теоремы 5 следует, что цоколь группы $\overline{G}/R$ — это прямое произведение конечного числа простых групп и централизатор цоколя тривиален. Это означает, что $C \cap \mathrm{Soc}(\overline{G}/R) \neq 1$ и группа C содержит минимальную субнормальную подгруппу, которая является неабелевой простой группой. Пусть E — ее полный прообраз в C. Тогда $E = E'\,\mathrm{Z}(C)$, при этом коммутант E' группы E является компонентой группы C, что противоречит тому, что $\mathrm{F}^*(C) = \mathrm{Z}(C)$. Следовательно, $C = \mathrm{F}^*(C) = \mathrm{Z}(C)$ и содержится в $\mathrm{F}^*(\overline{G})$.

Поскольку $C \leqslant \mathrm{F}^*(\overline{G})$, группа $\overline{G}/C$ лежит в прямом произведении групп $\mathrm{Aut}_{\overline{G}}(\mathrm{E}(\overline{G}))$

и $\mathrm{Aut}_{\overline{G}}(\mathrm{F}(\overline{G}))$. Порядок группы $\mathrm{F}(\overline{G})$ ограничен в терминах k, а значит и порядок группы $\mathrm{Aut}_{\overline{G}}(\mathrm{F}(\overline{G}))$ также ограничен функцией от k. Поэтому требуется рассмотреть только группу $\mathrm{Aut}_{\overline{G}}(\mathrm{E}(\overline{G}))$. Если $C_1, \ldots, C_s$ — компоненты группы $\overline{G}$, то $\mathrm{Aut}_{\overline{G}}(\mathrm{E}(\overline{G}))$ — это подгруппа в полупрямом произведении групп

$$\mathrm{Aut}(C_1) \times \cdots \times \mathrm{Aut}(C_s) \text{ и } H,$$

где H — это соответствующая подгруппа из Sym_s. Поскольку число s ограничено в терминах k, можно считать, что $\mathrm{Aut}_{\overline{G}}(\mathrm{E}(\overline{G}))$ является подгруппой в прямом произведении групп автоморфизмов компонент. Теперь теорема следует из леммы 1.3.9 и теоремы 5. □

§ 1.4. Периодические локально нильпотентные группы конечной c-размерности

Согласно результату Брайанта [35] периодическая локально нильпотентная группа с условием минимальности на централизаторы содержит нормальную нильпотентную подгруппу конечного индекса. В этом параграфе мы получим уточнение этого результата на случай конечной c-размерности.

Теорема 7. *Пусть G — локально нильпотентная p-группа c-размерности k. Тогда индекс ее нильпотентного радикала ограничен в терминах p и k.*

Из этой теоремы непосредственно вытекает следующее утверждение.

Следствие 1.4.1. *Пусть G — периодическая локально нильпотентная группа c-размерности k. Тогда индекс ее нильпотентного радикала ограничен в терминах p и k, где p — наибольшее простое число такое, что силовская p-подгруппа группы G неабелева.*

Доказательство теоремы 7 существенным образом опирается на доказательство оригинальной теоремы Брайанта, поэтому нам понадобятся некоторые утверждения, доказанные в [35].

Через $Z_k(G)$ обозначим k-й член верхнего центрального ряда группы G.

Лемма 1.4.2. [35, следствие 2.2] *Пусть G — локально нильпотентная $\mathfrak{M}_c$-группа, причем для некоторого k выполняется $Z_k(G) < G$. Тогда $Z_k(G) < Z_{k+1}(G)$.*

Лемма 1.4.3. [35, лемма 2.6] *Пусть G — периодическая нильпотентная $\mathfrak{M}_c$-группа. Тогда фактор-группа $G/Z_1(G)$ имеет конечный период.*

Лемма 1.4.4. [35, лемма 2.7] *Пусть G — локально нильпотентная $\mathfrak{M}_c$-группа, причем фактор-группа $G/Z_k(G)$ имеет конечный период для некоторого k. Тогда G нильпотентна.*

Лемма 1.4.5. [35, лемма 2.8] *Пусть D — элементарная абелева группа порядка p^2 для некоторого простого p. Положим $n = \frac{1}{2}p(p+1)$. Тогда существуют нетривиальные элементы $x_1, \ldots, x_n$ из D такие, что в целочисленном групповом кольце группы D*

выполняется

$$(x_1 - 1)(x_2 - 1)\dots(x_n - 1) = 0.$$

Будем далее писать $G = A.B$, если в G существует нормальная подгруппа N, изоморфная A, такая, что фактор-группа G/N изоморфна B.

Пусть для простого числа p функции $\psi_p(h,k),\ h = 0,\dots,k;\ k \in \mathbb{N}$ и $\varphi_p(k),\ k \in \mathbb{N}$ заданы следующими соотношениями:

$$\varepsilon_p = \begin{cases} p, & \text{если } p \neq 2; \\ 4 & \text{если } p = 2. \end{cases}$$

$$\psi_p(h,k) = 1,\ k \in \{0,1\},$$

$$\psi_p(k,k) = \varepsilon_p,\ k > 1,$$

$$\psi_p(h,k) = \varphi_p^{h+1}(k-1)\psi_p(h+1,k)^{\frac{p(p+1)}{2}},$$

$$\varphi_p(k) = \psi_p(0,k)!.$$

Докажем более точную формулировку теоремы 7.

Теорема 8. *Пусть G — локально нильпотентная p-группа c-размерности k. Тогда индекс ее нильпотентного радикала не превосходит $\varphi_p(k)$.*

Доказательство. Будем вести индукцию по c-размерности группы G. Можно считать, что G неабелева, т.е. $\operatorname{cdim}(G) > 0$. По лемме 1.4.2 имеем $Z_1(G) < Z_2(G)$, следовательно, существует $u \in Z_2(G) \setminus Z_1(G)$ такой, что его образ в фактор-группе $Z_2(G)/Z_1(G)$ имеет порядок p. Отображение $g \mapsto [g,u]$ — гомоморфизм из G в $Z_1(G)$ с ядром $C = C_G(u)$. Обозначим образ группы G под действием этого гомоморфизма через E. Заметим, что E — элементарная абелева группа в силу равенств $[g,u]^p = [g,u^p] = 1$. Так как $\operatorname{cdim}(C) < \operatorname{cdim}(G)$, по предположению индукции имеем $C = N.F$, где N — нильпотентный радикал группы C и $|F| \leqslant \varphi_p(k-1)$. При этом N нормальна в G и $G/N \cong F.E$.

Если мы найдем нильпотентную подгруппу $G_0 \leqslant G$ такую, что $|G : G_0| \leqslant \psi_p(0,k)$, то в G найдется нормальная нильпотентная подгруппа с индексом, не превосходящим $\psi_p(0,k)! = \varphi_p(k)$, и теорема будет доказана.

Построим ориентированное дерево Γ, в котором каждая вершина γ будет помечена некоторым централизатором M_γ из $Z_1(N)$, причем некоторые метки могут совпадать. Будем говорить, что вершина γ дерева Γ имеет уровень h, если длина минимального пути от корня дерева до этой вершины равна h. Корень дерева пометим $Z_1(N)$. Пусть теперь у нас есть вершина γ уровня h. Будем присоединять к ней дочерние вершины по следующей схеме.

Положим $H = N_G(M_\gamma)$, $K = C_G(M_\gamma)$. Отображение $\overline{}: H \to H/K$ — естественный гомоморфизм. Если в $\overline{H}$ нет нециклических элементарных абелевых подгрупп, то γ — концевая вершина. Пусть теперь $\overline{D} \leqslant \overline{H}$ — элементарная абелева группа порядка p^2, $D \leqslant H$ — ее полный прообраз. По лемме 1.4.5 для $n = \frac{p(p+1)}{2}$ существуют элементы

$x_1, \cdots x_n \in D \setminus K$ такие, что

$$(\overline{x}_1 - 1)(\overline{x}_2 - 1) \cdots (\overline{x}_n - 1) = 0$$

в целочисленном групповом кольце группы $\overline{D}$. Добавим в дерево n новых вершин γ_i, дочерних к γ, с метками $M_{\gamma_i} = C_{M_\gamma}(x_i) < M_\gamma$. Каждая из них будет иметь уровень $h+1$ в дереве. Заметим, что путь от корня дерева до любой концевой вершины соответствует некоторой цепочке строго вложенных централизаторов, а значит, так как $\operatorname{cdim} G = k$, дерево конечно и уровень каждой вершины не превосходит k.

Лемма 1.4.6. *Если γ — вершина дерева Γ уровня h, то $|G : N_G(M_\gamma)| \leqslant \varphi_p^h(k-1)$.*

Доказательство. Будем вести индукцию по h. Если $h = 0$, тогда $M_\gamma = Z_1(N)$ и $|G : N_G(M_\gamma)| = 1 = \varphi_p^0(k-1)$.

Пусть теперь γ — вершина уровня $h \geqslant 0$, γ_i — ее дочерние вершины, $i = 1, \ldots, n$. Положим $\overline{L} = C_{\overline{H}}(\overline{D})$, и пусть L — ее полный прообраз. Группа L нормализует M_{γ_i}, следовательно,

$$|G : N_G(M_{\gamma_i})| \leqslant |G : L| = |G : H||\overline{H} : \overline{L}|.$$

Заметим, что индекс $\overline{L}$ в $\overline{H}$ не превосходит порядка коммутанта $\overline{H}'$ группы $\overline{H}$. Действительно, пусть $\overline{d_1}, \ldots, \overline{d_s}$ — представители различных смежных классов $\overline{H}$ по $\overline{L}$. Тогда для любого $i > 1$ существует $\overline{d}$ из $\overline{D}$ такой, что $\left[\overline{d}, \overline{d_i}\right] \neq \left[\overline{d}, \overline{d_1}\right]$. Следовательно, элементов в группе $\overline{H}'$ не меньше, чем различных смежных классов $\overline{H}$ по $\overline{L}$.

Так как M_γ — центральная подгруппа в N, группа $\overline{H}$ — гомоморфный образ некоторой подгруппы $F.E$, значит, $|\overline{H}'| \leqslant |F| \leqslant \varphi_p(k-1)$. По предположению индукции $|G : H| \leqslant \varphi_p^h(k-1)$, следовательно,

$$|G : N_G(M_{\gamma_i})| \leqslant \varphi_p^{h+1}(k-1).$$

□

Лемма 1.4.7. *Пусть γ — вершина дерева Γ уровня h. Тогда существует $G_0 \leqslant G$ такая, что $|G : G_0| \leqslant \psi_p(h,k)$ и $M_\gamma \leqslant Z_m(G_0)$ для некоторого m.*

Доказательство. Будем вести индукцию по убыванию уровня h. Пусть γ — концевая вершина уровня h. Тогда группа $\overline{H}$ не имеет нециклических элементарных абелевых подгрупп, кроме того, она конечна. Действительно, предположим, что $\overline{H}$ бесконечна. Она имеет конечный период, значит, существует элемент $\overline{v}$ из $\overline{H}$ наибольшего порядка. Так как коммутант $\overline{H}'$ конечен, централизатор $C_{\overline{H}}(\overline{v})$ имеет конечный индекс, а значит, бесконечен. Тогда существует элемент $\overline{w} \in C_{\overline{H}}(\overline{v}) \setminus \langle \overline{v} \rangle$. Группа $\langle \overline{v}, \overline{w} \rangle$ абелева и нециклическая, следовательно, содержит нециклическую элементарную абелеву подгруппу, что противоречит предположению. Значит, $\overline{H}$ конечна и может быть либо циклической, либо обобщенной группой кватернионов при $p = 2$ (см., например, [67, теорема 6.11]). Имеем $|\overline{H} : \Phi(\overline{H})| \leqslant \varepsilon_p$, где $\Phi(\overline{H})$ — подгруппа Фраттини для $\overline{H}$, а число ε_p определено перед теоремой 8. Положим $G_0 = K$. Имеем $M_\gamma \leqslant C_G(G_0) \cap G_0 = Z_1(G_0)$ и

$$|G : G_0| \leqslant |G : H||H : K| \leqslant \varphi_p^h(k-1)|\overline{H}|,$$

$$|\overline{H}| = |\overline{H} : \Phi(\overline{H})||\Phi(\overline{H})|,$$

$$|\Phi(\overline{H})| = |\Phi(H/K)| \leqslant |\Phi(H/N)| \leqslant |F|.$$

Таким образом,

$$|G : G_0| \leqslant \varepsilon_p \varphi_p^h(k-1)\varphi_p(k-1) \leqslant \varphi_p^{h+1}(k-1)\psi_p(h+1,k) = \psi_p(h,k).$$

Пусть теперь γ — неконцевая вершина уровня h, γ_i — ее дочерние вершины. Тогда по предположению индукции для $i = 1, \ldots, n$ существуют подгруппы G_i группы G такие, что $|G : G_i| \leqslant \psi_p(h+1,k)$ и $M_{\gamma_i} \leqslant Z_{m_i}(G_i)$. Положим $m = \max\{m_1, \ldots, m_n\}$ и $G_0 = L \cap G_1 \cap \cdots \cap G_n$. Имеем

$$|G : G_0| \leqslant |G : L| \prod_{i=1}^{n} |G : G_i| \leqslant \varphi_p^{h+1}(k-1)(\psi_p(h+1,k))^n = \psi_p(h,k).$$

Покажем теперь, что $M_\gamma \leqslant Z_{nm}(G_0)$. Группа $\overline{L}$ действует на M_γ сопряжениями, поэтому можем рассматривать M_γ как $\overline{L}$-модуль. Заметим, что $M_{\gamma_i} \leqslant Z_m(G_0)$.

Получаем $M_\gamma(\overline{x}_1 - 1)(\overline{x}_2 - 1)\cdots(\overline{x}_n - 1) = 0$, следовательно,

$$M_\gamma(\overline{x}_1 - 1)(\overline{x}_2 - 1)\cdots(\overline{x}_{n-1} - 1) \leqslant C_{M_\gamma}(x_n) = M_{\gamma_n} \leqslant Z_m(G_0).$$

Тогда $M_\gamma(\overline{x}_1 - 1)(\overline{x}_2 - 1)\cdots(\overline{x}_{n-1} - 1)(\overline{G_0} - 1)^m = 0$. Так как все $\overline{x_i}$ — центральные элементы в $\overline{L}$, мы получаем

$$M_\gamma(\overline{G_0} - 1)^m(\overline{x}_1 - 1)(\overline{x}_2 - 1)\cdots(\overline{x}_{n-1} - 1) = 0.$$

Продолжая аналогично для остальных x_i, приходим к тому, что $M_\gamma(\overline{G_0} - 1)^{nm} = 0$, что эквивалентно включению $M_\gamma \leqslant Z_{nm}(G_0)$. □

Завершим доказательство теоремы 8, применив лемму 1.4.7 к корню дерева γ. Тогда $M_\gamma = Z_1(N) \leqslant Z_m(G_0)$. По лемме 1.4.3 группа $N/Z_1(N)$ имеет конечный период, значит, и $G_0/Z_m(G_0)$ имеет конечный период. По лемме 1.4.4 группа G_0 нильпотентна, и ее индекс в группе G не превышает $\psi_p(0,k)$. □

Из теоремы 8 несложно вывести следствие 1.4.1.

Доказательство следствия 1.4.1. Периодическая локально нильпотентная группа может быть представлена как прямое произведение своих силовских подгрупп $G = \prod O_p(G)$. Так как $\operatorname{cdim}(G \times H) = \operatorname{cdim} G + \operatorname{cdim} H$, среди всех $O_p(G)$ есть лишь конечное число неабелевых групп, т.е. таких, что $\operatorname{cdim} O_p(G) > 0$. Для каждого такого p применим теорему 8 к $O_p(G)$. Тогда $O_p(G) = N_p.F_p$, где N_p — нильпотентный радикал группы $O_p(G)$, и $|F_p| \leqslant \varphi_p(k)$. Все N_p нормальны и нильпотентны в G, значит, их прямое произведение N — нормальная нильпотентная подгруппа в G такая, что

$$|G : N| \leqslant \prod \varphi_p(k),$$

где произведение берется по всем таким простым p, что группа $O_p(G)$ неабелева.

Заметим, что правую часть можно оценить функцией, зависящей только от k и максимального простого числа p такого, что группа $O_p(G)$ неабелева. □

В заключение мы приведем небольшое уточнение результата Брайанта о структуре локально нильпотентных групп с условием минимальности на централизаторы.

Теорема 9. *Пусть G — периодическая локально нильпотентная группа с условием минимальности на централизаторы, N — ее нильпотентный радикал. Тогда $Z_1(N) = C_G(N)$.*

Доказательство. Обозначим через C централизатор $Z_1(N)$ в G. Для начала докажем, что $C = N$. Включение $C \geqslant N$ очевидно. Чтобы показать обратное, докажем, что группа C нильпотентна. Так как $Z_1(C) \geqslant Z_1(N)$, фактор-группа $C/Z_1(C)$ — гомоморфный образ группы $C/Z_1(N)$. По лемме 1.4.3 группа $G/Z_1(N)$ имеет конечный период, а значит, и $C/Z_1(C)$ имеет конечный период, и по лемме 1.4.4 группа C нильпотентна. Таким образом, C — нильпотентная нормальная подгруппа G, следовательно, $C = N$.

Получаем $N = C_G(Z_1(N)) \geqslant C_G(N)$, следовательно, $C_G(N) = Z_1(N)$. □

2. Спектры исключительных групп лиева типа

Напомним, что множество порядков элементов конечной группы G называется ее спектром и обозначается через $\omega(G)$. Через $\mu(G)$ обозначается множество максимальных по делимости элементов множества $\omega(G)$. Поскольку $\omega(G)$ замкнуто относительно взятия делителей, оно однозначно определяется любым множеством $\nu(G)$ таким, что $\mu(G) \subseteq \nu(G) \subseteq \omega(G)$.

Пусть G — конечная группа лиева типа над полем характеристики p. Тогда множество $\omega(G)$ может быть представлено как объединение трех подмножеств: множества $\omega_p(G)$ порядков всех унипотентных элементов, т.е. элементов, чей порядок является степенью числа p, множества $\omega_{p'}(G)$ порядков всех полупростых элементов, т.е. элементов, чей порядок взаимно прост с p, и множества $\omega_m(G)$ всех остальных, «смешанных», порядков. Таким образом, задача описания спектра конечной группы лиева типа распадается на три подзадачи. Определим множества $\mu_p(G)$, $\mu_{p'}(G)$ и $\mu_m(G)$ как пересечения $\mu(G)$ с соответствующими подмножествами из $\omega(G)$.

В данной главе мы дадим описание спектров конечных простых и односвязных групп лиевых типов E_6, ${}^2E_6$, E_7 и E_8 (в случае типа E_8 односвязная группа является простой). Для простых групп мы используем обозначения $E_6(q)$, $E_7(q)$ и т. д., а для односвзяных — обозначения вида $(E_6)_{sc}(q)$. Кроме того, нам будет удобно обозначать $E_6(q)$ через $E_6^+(q)$, а ${}^2E_6(q)$ — через $E_6^-(q)$.

Напомним, что максимальный порядок унипотентного элемента группы лиева типа над полем характеристики p зависит только от p и максимальной высоты корня в системе корней группы G (см. лемму 2.1.3 ниже). Через $p(\Phi)$ обозначается максимальная степень p, лежащая в спектре группы лиева типа Φ над полем характеристики p.

Для натуральных чисел $n_1, \ldots, n_s$ будем обозначать через $(n_1, \ldots, n_s)$ и $[n_1, \ldots, n_s]$ их наибольший общий делитель и наименьшее общее кратное соответственно.

В этой главе доказаны следующие теоремы.

Теорема 10. *Пусть G — простая группа $E_6^\varepsilon(q)$, где $\varepsilon \in \{+,-\}$ и q — степень простого числа p. Положим $d = (3, q-\varepsilon 1)$. Пусть множество $\nu(G)$ есть объединение следующих множеств:*

1) $\{\frac{q^6-1}{d}, \frac{q^6+\varepsilon q^3+1}{d}, \frac{(q^2+\varepsilon q+1)(q^4-q^2+1)}{d}, \frac{(q-\varepsilon 1)(q^2+1)(q^3+\varepsilon 1)}{d}, \frac{(q^2-1)(q^4+1)}{d}, \frac{(q+\varepsilon 1)(q^5-\varepsilon 1)}{d}, q^5-\varepsilon 1\}$,

2) $p \cdot \{\frac{q^6-1}{d(q-\varepsilon 1)}, \frac{q^5-\varepsilon 1}{d}, q^4-1, (q^3-\varepsilon 1)(q+\varepsilon 1), \frac{(q-\varepsilon 1)(q^3+\varepsilon 1)}{d}\}$,

3) $p(A_2) \cdot \{\frac{(q^3-\varepsilon 1)(q+\varepsilon 1)}{d}, \frac{q^4+q^2+1}{d}, \frac{q^4-1}{d}\}$,

4) $p(A_3) \cdot \{\frac{(q^2+1)(q-\varepsilon 1)}{d}, q^2-1\}$,

5) $p(D_4) \cdot \{q-\varepsilon 1, \frac{(q^2-1)}{d}, \frac{(q^2+\varepsilon q+1)}{d}\}$,

6) $p(D_5)\cdot\{\frac{(q-\varepsilon 1)}{d}\}$,

7) $\{p(E_6)\}$.

Тогда $\mu(G)\subseteq\nu(G)\subseteq\omega(G)$.

Теорема 11. *Пусть* G *— односвязная группа* $(E_6^{\varepsilon})_{sc}(q)$, *где* $\varepsilon\in\{+,-\}$ *и* q *— степень простого числа* p. *Пусть множество* $\nu(G)$ *есть объединение следующих множеств:*

1) $\{\frac{q^6-1}{(3,q-\varepsilon 1)}, q^6+\varepsilon q^3+1, (q^2+\varepsilon q+1)(q^4-q^2+1), (q-\varepsilon 1)(q^2+1)(q^3+\varepsilon 1),$
$(q^2-1)(q^4+1), (q+\varepsilon 1)(q^5-\varepsilon 1)\}$,

2) $p\cdot\{\frac{q^6-1}{q-\varepsilon 1}, q^5-\varepsilon 1, (q^3-\varepsilon 1)(q+\varepsilon 1), (q-\varepsilon 1)(q^3+\varepsilon 1)\}$,

3) $p(A_2)\cdot\{\frac{(q^3-\varepsilon 1)(q+\varepsilon 1)}{(3,q-\varepsilon 1)}, q^4+q^2+1, q^4-1\}$,

4) $p(A_3)\cdot\{(q^2+1)(q-\varepsilon 1)\}$,

5) $p(D_4)\cdot\{(q^2-1),(q^2+\varepsilon q+1)\}$,

6) $p(D_5)\cdot\{(q-\varepsilon 1)\}$,

7) $p(E_6)\cdot\{(3,q-\varepsilon 1)\}$.

Тогда $\mu(G)\subseteq\nu(G)\subseteq\omega(G)$.

Теорема 12. *Пусть* G *— простая группа* $E_7(q)$, *где* q *— степень простого числа* p. *Положим* $d=(2,q-1)$. *Пусть множество* $\nu(G)$ *есть объединение следующих множеств:*

1) $\Big\{\frac{(q^2-q+1)(q^5+1)}{d}, \frac{(q^2+q+1)(q^5-1)}{d}, \frac{(q+1)(q^6-q^3+1)}{d}, \frac{(q-1)(q^6+q^3+1)}{d}, \frac{q^7+1}{d}, \frac{q^7-1}{d}, \frac{(q^3-1)(q^4-q^2+1)}{d},$
$\frac{(q^3+1)(q^4-q^2+1)}{d}$, $(q^2-q+1)(q^4-1)$, $(q^2+q+1)(q^4-1)$, $(q+1)(q^5-1)$, $(q-1)(q^5+1)$,
$(q^3+1)(q^2+1)(q-1)$, $(q^3-1)(q^2+1)(q+1)$, $\frac{q^8-1}{(q-1)(4,q-1)}$, $\frac{q^8-1}{(q+1)(4,q+1)}$, $(q^4+1)(q^2-1)$,
$q^6-1\}$;

2) $p\cdot\Big\{\frac{q^6-1}{d}, q^5-1, q^5+1, \frac{(q^4+1)(q^2+1)}{d}, \frac{(q^4+1)(q^2-1)}{d}, \frac{(q^3+1)(q^2+1)(q-1)}{d}, \frac{(q^3-1)(q^2+1)(q+1)}{d}, q^4-q^2+1\}$;

3) $p(A_2)\cdot\Big\{\frac{q^6-1}{(q-1)d}, \frac{q^6-1}{(q+1)d}, \frac{q^5-1}{d}, \frac{q^5+1}{d}, q^4-1, (q^3+1)(q-1), (q^3-1)(q+1)\}$;

4) $p(A_3)\cdot\Big\{\frac{q^4-1}{d}, \frac{(q^3+1)(q-1)}{d}, \frac{(q^3-1)(q+1)}{d}\Big\}$;

5) $p(D_4)\cdot\Big\{\frac{q^3-1}{d}, \frac{q^3+1}{d}, \frac{(q^2+1)(q+1)}{d}, \frac{(q^2+1)(q-1)}{d}, q^2-1\Big\}$;

6) $p(D_5)\cdot\Big\{\frac{q^2-1}{d}\Big\}$;

7) $p(D_6)\cdot\{q-1, q+1\}$;

8) $p(E_6)\cdot\Big\{\frac{q-1}{d}, \frac{q+1}{d}\Big\}$;

9) $\{p(E_7)\}$.

Тогда $\mu(G) \subseteq \nu(G) \subseteq \omega(G)$.

Теорема 13. *Пусть* G *— односвязная группа* $(E_7)_{sc}(q)$*, где* q *— степень простого числа* p*. Положим* $d = (2, q-1)$*. Пусть множество* $\nu(G)$ *есть объединение следующих множеств:*

1) $\{(q^2-q+1)(q^5+1),\ (q^2+q+1)(q^5-1),\ (q+1)(q^6-q^3+1),\ (q-1)(q^6+q^3+1),\ q^7+1,$ $q^7-1,\ (q^3-1)(q^4-q^2+1),\ (q^3+1)(q^4-q^2+1),\ (q^2-q+1)(q^4-1),\ (q^2+q+1)(q^4-1),$ $(q+1)(q^5-1),\ (q-1)(q^5+1),\ \frac{q^8-1}{(q-1)d},\ \frac{q^8-1}{(q+1)d},\ (q^4+1)(q^2-1),\ q^6-1\}$;

2) $p\cdot\left\{\frac{q^6-1}{d},\ q^5-1,\ q^5+1,\ \frac{(q^4+1)(q^2+1)}{d},\ \frac{(q^4+1)(q^2-1)}{d},\ \frac{(q^3+1)(q^2+1)(q-1)}{d},\ \frac{(q^3-1)(q^2+1)(q+1)}{d}, q^4-q^2+1\right\}$;

3) $p(A_2)\cdot\left\{\frac{q^6-1}{(q-1)d},\ \frac{q^6-1}{(q+1)d},\ \frac{q^5-1}{d},\ \frac{q^5+1}{d},\ q^4-1,\ (q^3+1)(q-1),\ (q^3-1)(q+1)\right\}$;

4) $p(A_3)\cdot\left\{\frac{q^4-1}{d},\ \frac{(q^3+1)(q-1)}{d},\ \frac{(q^3-1)(q+1)}{d}\right\}$;

5) $p(D_4)\cdot\{q^3-1, q^3+1, (q^2+1)(q+1), (q^2+1)(q-1), q^2-1\}$;

6) $p(D_5)\cdot\left\{\frac{q^2-1}{d}\right\}$;

7) $p(E_6)\cdot\{q-1, q+1\}$;

8) $p(E_7)\cdot\{d\}$.

Тогда $\mu(G) \subseteq \nu(G) \subseteq \omega(G)$.

Теорема 14. *Пусть* G *— это простая группа* $E_8(q)$*, где* q *— степень простого числа* p*. Пусть множество* $\nu(G)$ *есть объединение следующих множеств:*

1) $\{(q+1)(q^2+q+1)(q^5-1),\ (q-1)(q^2-q+1)(q^5+1),\ (q+1)(q^2+1)(q^5-1),$ $(q-1)(q^2+1)(q^5+1),\ (q+1)(q^7-1),\ (q-1)(q^7+1),\ q^8-1,\ (q+1)(q^3-1)(q^4+1),$ $(q-1)(q^3+1)(q^4+1),\ (q^2+1)(q^6-1),\ (q^2-1)(q^6+1),\ (q^2-1)(q^2+q+1)(q^4-q^2+1),$ $(q^2-1)(q^2-q+1)(q^4-q^2+1),\ (q^2-1)(q^6-q^3+1),\ (q^2-1)(q^6+q^3+1),\ \frac{(q^2+q+1)(q^6+q^3+1)}{(3,q-1)},$ $\frac{(q^2-q+1)(q^6-q^3+1)}{(3,q+1)},\ q^8+q^7-q^5-q^4-q^3+q+1,\ q^8-q^7+q^5-q^4+q^3-q+1,\ q^8-q^4+1,$ $q^8-q^6+q^4-q^2+1\}$;

2) $p\cdot\{(q^2-q+1)(q^5+1),\ (q^2+q+1)(q^5-1),(q+1)(q^6-q^3+1),\ (q-1)(q^6+q^3+1),$ $q^7+1,\ q^7-1,\ (q^3-1)(q^4-q^2+1),\ (q^3+1)(q^4-q^2+1),\ \frac{q^8-1}{(q-1)(2,q-1)},\ \frac{q^8-1}{(q+1)(2,q-1)},\ q^6+1\}$;

3) $p(A_2)\cdot\{q^6-1, q^6+q^3+1, q^6-q^3+1, (q^2+q+1)(q^4-q^2+1), (q^2-q+1)(q^4-q^2+1), (q^2-q+1)(q^4-1), (q^2+q+1)(q^4-1), (q^2-1)(q^4+1), (q+1)(q^5-1), (q-1)(q^5+1)\}$;

4) $p(A_3)\cdot\{q^5-1, q^5+1, (q^4+1)(q-1), (q^4+1)(q+1), (q^3-1)(q^2+1), (q^3+1)(q^2+1)\}$;

5) $p(A_4)\cdot\left\{\frac{q^5-1}{q-1}, \frac{q^5+1}{q+1}, q^4-1\right\}$;

6) $p(A_5)\cdot\left\{(q^3-1)(q+1), (q^3+1)(q-1), q^4+1, \frac{q^4-1}{(2,q-1)}, q^4-q^2+1\right\}$;

7) $p(D_5) \cdot \{(q^2+1)(q-1), (q^2+1)(q+1), q^3-1, q^3+1\}$;

8) $p(D_6) \cdot \{q^2+1\}$;

9) $p(E_6) \cdot \{q^2-q+1, q^2+q+1, q^2-1\}$;

10) $p(E_7) \cdot \{q-1, q+1\}$;

11) $\{p(E_8)\}$.

Тогда $\mu(G) \subseteq \nu(G) \subseteq \omega(G)$.

§ 2.1. Предварительные сведения и обозначения

Используемые далее сведения из теории алгебраических групп изложены в [41, главы 1 и 3] и приводятся без указания точных ссылок.

Пусть p — простое число и $\overline{G}$ — связная редуктивная алгебраическая группа над алгебраическим замыканием $\overline{\mathrm{F}}_p$ поля Галуа F_p. Максимальная связная диагонализируемая подгруппа группы $\overline{G}$ называется максимальным тором. Редуктивная подгруппа группы $\overline{G}$ называется редуктивной подгруппой максимального ранга, если она содержит некоторый максимальный тор группы $\overline{G}$. Известно, что группу $\overline{G}$ можно вложить в общую линейную группу $GL_n(\overline{\mathrm{F}}_p)$ для некоторого n. Отображение, действующее по правилу $(a_{ij}) \mapsto (a_{ij}^q)$, где q — это некоторая степень числа p, называется стандартным отображением Фробениуса группы G. Гомоморфизм группы G в себя называется отображением Фробениуса, если некоторая его степень является стандартным отображением Фробениуса. Сюръективный эндоморфизм σ группы $\overline{G}$ называется эндоморфизмом Стейнберга, если группа неподвижных точек $\overline{G}_\sigma = \{g \in \overline{G} \mid g^\sigma = g\}$ конечна. Для связных полупростых групп понятия отображения Фробениуса и эндоморфизма Стейнберга совпадают. Поскольку мы будем иметь дело только с такими группами и их подгруппами мы не будем различать эти два понятия. Если σ — некоторый эндоморфизм Стейнберга группы $\overline{G}$, то конечная группа G такая, что $O^{p'}(\overline{G}_\sigma) \leqslant G \leqslant \overline{G}_\sigma$, называется конечной группой лиева типа. Редуктивной подгруппой максимального ранга такой группы G называется подгруппа вида $(\overline{G}_1)_\sigma \cap G$, где $\overline{G}_1$ — это σ-инвариантная редуктивная подгруппа максимального ранга группы $\overline{G}$. Если $\overline{G}_1$ — это максимальный тор, то подгруппа $(\overline{G}_1)_\sigma \cap G$ называется максимальным тором группы G.

Произвольный элемент g группы лиева типа G может быть единственным образом представлен в виде произведения su, где элемент s полупрост, а u — это унипотентный элемент из $C_G(s)$. Компонента связности $C_{\overline{G}}(s)^0$, содержащая единицу, является редуктивной подгруппой максимального ранга группы $\overline{G}$. Подгруппа $C_{\overline{G}}(s)^0$ содержит s и все унипотентные элементы из $C_{\overline{G}}(s)$. Таким образом, редуктивная подгруппа $(C_{\overline{G}}(s)^0)_\sigma$ группы $\overline{G}_\sigma$ содержит s и все унипотентные элементы из $C_{\overline{G}_\sigma}(s)$. Для редуктивной подгруппы H группы $\overline{G}_\sigma$ обозначим через $\eta(H)$ произведение периода ее центра и максимального

элемента из $\omega_p(H)$. В силу вышесказаного, произвольный элемент из $\mu(\overline{G}_\sigma)$ равен $\eta(H)$ для некоторой редуктивной подгруппы максимального ранга H группы $\overline{G}_\sigma$.

Пусть $\overline{T}$ — некоторый максимальный тор группы $\overline{G}$ и Φ — корневая система группы $\overline{G}$ относительно тора $\overline{T}$. Подсистема Φ_1 системы Φ называется *аддитивно замкнутой*, если для любых $r_1, r_2 \in \Phi_1$ из условия $r_1 + r_2 \in \Phi$ следует, что $r_1 + r_2 \in \Phi_1$. Для корня $r \in \Phi$, обозначим через $\overline{X}_r$ корневую подгруппу, соответствующую корню r. Если все корни системы Φ имеют одинаковую длину, то все редуктивные подгруппы, содержащие тор $\overline{T}$, имеют вид $\langle \overline{T}, \overline{X}_r, r \in \Phi_1 \rangle$, где Φ_1 — аддитивно замкнутая подсистема системы Φ. Далее под термином «подсистема» мы всегда будем подразумевать аддитивно замкнутую подсистему.

Пусть $\overline{G}_1$ — σ-инвариантная редуктивная подгруппа группы $\overline{G}$. Тогда $\overline{G}_1$ содержит σ-инвариантный максимальный тор $\overline{T}$. Пусть сопряженная подгруппа $\overline{G}_1^g$ также σ-инвариантна. Тогда $\overline{G}_1^g$ содержит σ-инвариантный максимальный тор. Поскольку любые два максимальных тора группы $\overline{G}_1^g$ сопряжены, можно считать, что тор $\overline{T}^g$ является σ-инвариантным. Имеем $g^\sigma g^{-1} \in N_{\overline{G}}(\overline{T}) \cap N_{\overline{G}}(\overline{G}_1)$. Пусть W — это группа Вейля группы $\overline{G}$ и W_1 — группа Вейля группы $\overline{G}_1$. Обозначим через π канонический эпиморфизм из $N_{\overline{G}}(\overline{T})$ на W. В доказательстве предложения 2 из [39] показано, что $\pi(N_{\overline{G}}(\overline{T}) \cap N_{\overline{G}}(\overline{G}_1)) = N_W(W_1)$.

Поскольку тор $\overline{T}$ является σ-инвариантным, σ действует на группе $W = N_{\overline{G}}(\overline{T})/\overline{T}$. Поскольку группа W_1 также σ-инвариантна, σ действует на $N_W(W_1)/W_1$. Два элемента $W_1 w_1$ и $W_1 w_2$ группы $N_W(W_1)/W_1$ называются σ-сопряженными, если существует $w \in W$ такой, что $W_1 w_2 = (W_1 w)^\sigma (W_1 w_1)(W_1 w)^{-1}$.

Лемма 2.1.1. [39, предложение 3] *Пусть $\overline{G}$ — связная редуктивная алгебраическая группа и σ — отображение Фробениуса группы $\overline{G}$. Пусть $\overline{G}_1$ — σ-инвариантная редуктивная подгруппа максимальноого ранга группы $\overline{G}$. Пусть $\mathfrak{C}$ — множество всех σ-инвариантных подгрупп, сопряженных с $\overline{G}_1$ в группе $\overline{G}$, и $\mathfrak{C}/\overline{G}_\sigma$ — множество $\overline{G}_\sigma$-орбит на $\mathfrak{C}$. Функция, отображающая подгруппу $\overline{G}_1^g$ в элемент $W_1\pi(g^\sigma g^{-1})$, индуцирует биекцию между множеством $\mathfrak{C}/\overline{G}_\sigma$ и классами σ-сопряженности элементов группы $N_W(W_1)/W_1$.*

Следующая лемма является следствием теоремы Лэнга – Стейнберга (см., например, [55, теорема 2.1.1]).

Лемма 2.1.2. *Пусть $\overline{G}$ — связная редуктивная алгебраическая группа и σ — отображение Фробениуса группы $\overline{G}$. Пусть $\overline{G}_1$ — это σ-инвариантная редуктивная подгруппа максимального ранга группы $\overline{G}$. Пусть сопряженная подгруппа $\overline{G}_1^g$ также σ-инвариантна. Положим $n = g^\sigma g^{-1}$. Тогда $(\overline{G}_1^g)_\sigma = ((\overline{G}_1)_{\sigma \circ n})^g$. Более того, для произвольного $n \in N_{\overline{G}}(\overline{T}) \cap N_{\overline{G}}(\overline{G}_1)$ группа $(\overline{G}_1)_{\sigma \circ n}$ сопряжена в $\overline{G}$ некоторой редуктивной подгруппе группы $\overline{G}_\sigma$.*

Из лемм 2.1.1 и 2.1.2 следует, что описание структуры редуктивных подгрупп конечной группы $\overline{G}_\sigma$ можно получить по следующей схеме. Выбирается некоторое множество σ-инвариантных редуктивных подгрупп максимального ранга $\mathfrak{M}$, содержащее полную си-

стему представителей классов сопряженности. Затем для каждой $\overline{G}_1$ из $\mathfrak{M}$ описывается структура групп вида $(\overline{G}_1)_{\sigma\circ n}$, где $W_1\pi(n)$ пробегает полную систему представителей классов σ-сопряженности группы $N_W(W_1)/W_1$. В дальнейшем множество $\mathfrak{M}$ будет состоять из редуктивных подгрупп содержащих фиксированный σ-инвариантный максимальный тор группы $\overline{G}$.

Лемма 2.1.3. [82, предложение 0.5] *Пусть $\overline{G}$ — простая алгебраическая группа над алгебраически замкнутым полем положительной характеристики p и σ — отображение Фробениуса группы $\overline{G}$. Тогда p-период группы $\overline{G}_\sigma$ равен минимальной степени числа p большей, чем максимальная высота корня в системе корней группы $\overline{G}$.*

Для системы корней Φ обозначим через $mh(\Phi)$ максимальную высоту корня в системе Φ. Из леммы 2.1.3 следует, что p-период группы лиева типа над полем характеристики p зависит только от ее корневой системы и равен $p^{[\log_p(mh(\Phi))]+1}$, где $[\alpha]$ обозначает целую часть числа α. В таблице 1 для каждой неразложимой системы корней Φ приведена максимальная высота корня $mh(\Phi)$.

Таблица 1. Максимальная высота корня

Φ	$mh(\Phi)$	Φ	$mh(\Phi)$	Φ	$mh(\Phi)$
A_n	n	D_n	$2n-3$	E_8	29
B_n	$2n-1$	E_6	11	F_4	11
C_n	$2n-1$	E_7	17	G_2	5

Доказательство следующей леммы не представляет труда.

Лемма 2.1.4. *Пусть C_i, $1 \leqslant i \leqslant s$, — циклические группы и $B = C_1 \times C_2 \times \cdots \times C_s$, где $s > 1$. Пусть A — подгруппа группы B простого порядка p такая, что $A \cap C_i = 1$ для некоторого i такого, что $\exp(C_i) = \exp(B)$. Тогда $\exp(B) = \exp(B/A)$.*

Напомним, что если r и s — это корни некоторой корневой системы Φ, то через A_{rs} обозначается дробь $\frac{2(r,s)}{(r,r)}$.

§ 2.2. Порядки полупростых элементов

Сначала мы дадим описание порядков полупростых элементов рассматриваемых групп. Напомним, что в [47] описано строение максимальных торов соответствующих односвязных групп. Таким образом, в случае групп E_8 для описания спектра остается описать порядки смешанных элементов, что будет сделано в последнем параграфе главы.

Далее $\overline{G}$ — односвязная простая алгебраическая группа типа E_n, где $n \in \{6, 7, 8\}$, над алгебраическим замыканием $\overline{\mathrm{F}}_p$ поля Галуа F_p для простого p. Пусть q — степень числа p. Через σ будем обозначать эндоморфизм Стейнберга группы $\overline{G}$, действующее на корневых элементах по правилу $x_r(t) \mapsto x_r(t^q)$ для каждого $r \in \Phi$ и $t \in \mathrm{F}_p$. Тогда $\overline{G}_\sigma$ — это односвязная группа $(E_l)_{sc}(q)$. Несложно проверить, что σ централизует группу Вейля

W группы $\overline{G}$. Следовательно, классы σ-сопряженности группы W — это обычные классы сопряженности группы W.

Пусть r_1, r_2, …, r_n, где $n \in \{6, 7, 8\}$ — это простые корни системы корней группы $\overline{G}$, пронумерованные в соответствии со следующей диаграммой Дынкина.

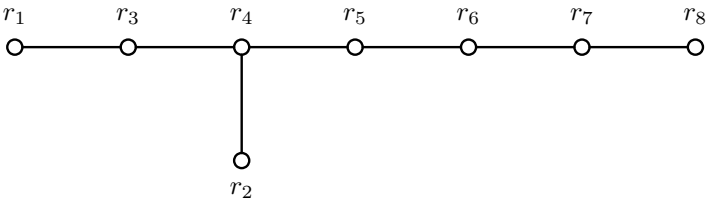

Рис. 1

Заметим, что отображение $-id$ системы корней E_6, переводящее каждый корень в противоположный, является автоморфизмом системы корней, не лежащим в группе Вейля W. Это отображение индуцирует автоморфизм группы $\overline{G}$, отличающийся от графового автоморфизма γ группы $\overline{G}$ на внутренний автоморфизм. Из леммы 2.1.2 следует, что группа неподвижных точек отображения Фробениуса $\sigma \circ (-id)$ сопряжена в $\overline{G}$ группе ${}^2E_6(q)$.

Каждый полупростой элемент содержится в некотором максимальном торе. Поскольку любые два максимальных тора сопряжены в группе $\overline{G}$, из леммы 2.1.1 следует, что классы сопряженности максимальных торов группы $\overline{G}_\sigma$ находятся во взаимно однозначном соответствии с классами сопряженности группы W.

Подгруппа $\overline{T}$, состоящая из всех элементов вида $h_{r_1}(t_1)h_{r_2}(t_2)\dots h_{r_n}(t_n)$, является максимальным тором группы $\overline{G}$ (определение элементов $h_r(t)$ можно найти, например, в [37, теорема 12.1.1]). Поскольку $h_r(t)^\sigma = h_r(t^q)$ для всех r и t, тор $\overline{T}$ является σ-инвариантным. Таким образом, для любого максимального тора S группы $\overline{G}_\sigma$ существует элемент w группы W такой, что тор S сопряжен в группе $\overline{G}$ подгруппе $\overline{T}_{\sigma\circ w}$. Для $r \in \Phi$ обозначим через w_r элемент группы Вейля, являющийся отражением в гиперплоскости, ортогональной корню r. Пусть r, $s \in \Phi$. Тогда $h_{sw_r} = h_s(t^{-A_{sr}})h_r(t)$ (см. [37, стр. 196]). Теперь если $r = \alpha_1 r_1 + \alpha_2 r_2 + \dots + \alpha_n r_n$ — корень системы Φ, то из следствия ил леммы A на стр. 68 в [22] следует, что $h_r(t) = h_{r_1}(t^{\alpha_1})h_{r_2}(t^{\alpha_2})\dots h_{r_n}(t^{\alpha_n})$. Пусть $h \in \overline{T}_{\sigma\circ w}$, тогда $h^{\sigma\circ w} = h$. Поскольку $h = h_{r_1}(t_1)h_{r_2}(t_2)\dots h_{r_n}(t_n)$, имеем

$$h_{r_1 w}(t_1^q)h_{r_2 w}(t_2^q)\dots h_{r_n w}(t_n^q) = h_{r_1}(t_1)h_{r_2}(t_2)\dots h_{r_n}(t_n).$$

Таким образом, если мы обозначим через M_w матрицу отображения w в базисе $r_1, r_2, \dots, r_n$, то матрица $qM_w - 1$ — это матрица определяющих соотношений абелевой группы $\overline{T}_{\sigma\circ w}$. Пусть A и B — это унимодулярные матрицы над кольцом многочленов с рациональными коэффициентами от переменной q такие, что матрица $A(qM_w - 1)B$ является диагональной с элементами $d_1, d_2, \dots, d_n$ на главной диагонали и при любом допустимом значении q матрицы A и B целочисленны (такое представление называют нормальной формой Смита). Тогда тор S изоморфен прямому произведению циклических групп $\mathbb{Z}_{|d_1|}$, $\mathbb{Z}_{|d_2|}$, …, $\mathbb{Z}_{|d_n|}$. Более того, если обозначить элементы матрицы A через a_{ij} для $1 \leqslant i, j \leqslant n$, то каждый элемент группы $\overline{T}_{\sigma\circ w}$ имеет вид $h_{r_1}(s_1^{a_{11}}s_2^{a_{21}}\dots s_n^{a_{n1}})h_{r_2}(s_1^{a_{12}}s_2^{a_{22}}\dots s_n^{a_{n2}})\dots h_{r_n}(s_1^{a_{1n}}s_2^{a_{2n}}\dots s_n^{a_{nn}})$, где s_1, $s_2, \dots, s_n$ — элементы поля $\overline{\mathrm{F}}_p$ такие, что $s_1^{d_1} = 1$, $s_2^{d_2} = 1, \dots, s_n^{d_n} = 1$.

Поскольку группа неподвижных точек отображения Фробениуса $\sigma \circ (-id)$ изоморфна ${}^2E_6(q)$, получаем, что матрица определяющих соотношений абелевой группы $\overline{T}_{\sigma\circ(-id)\circ w}$, сопряженной максимальному тору группы ${}^2E_6(q)$, равна $(-q)M_w - 1$. Таким образом, все дальнейшие результаты о максимальных торах группы $E_6(q)$ после замены q на $-q$(при этом следует использовать договоренность, что если в записи возникает группа или элемент отрицательного порядка x, то x следует заменить на $-x$) дают аналогичные результаты о максимальных торах группы ${}^2E_6(q)$.

Напомним, что центр односвязной группы $(E_6)_{sc}(q)$ состоит из элементов вида

$$h_{r_1}(t)h_{r_3}(t^2)h_{r_5}(t)h_{r_6}(t^2), \text{ где } t^3 = 1,$$

и имеет порядок $(3, q-1)$ (соответственно, в случае группы ${}^2E_6(q)$ порядок центра равен $(3, q+1)$). Центр односвязной группы $(E_7)_{sc}(q)$ состоит из элементов

$$h_{r_2}(t)h_{r_5}(t)h_{r_7}(t), \text{ где } t^2 = 1,$$

и его порядок равен $(2, q-1)$.

Пусть $\overline{G}$ имеет тип E_6. По леммам 2.1.1 и 2.1.2 для описания полупростой части спектра простой группы $E_6(q)$ достаточно описать строение образа группы $\overline{T}_{\sigma\circ w}$ в группе $\overline{G}_\sigma/Z(\overline{G}_\sigma)$, где w пробегает полную систему представителей классов сопряженности группы W. Следующий результат получен в [47].

Предложение 2.2.1. *Пусть S — это максимальный тор группы $\overline{G}_\sigma$. Тогда S изоморфен одной из групп* $(\mathbb{Z}_{q-1})^6$, $(\mathbb{Z}_{q-1})^4 \times \mathbb{Z}_{q^2-1}$, $(\mathbb{Z}_{q-1})^2 \times (\mathbb{Z}_{q^2-1})^2$, $(\mathbb{Z}_{q-1})^3 \times \mathbb{Z}_{q^3-1}$, $(\mathbb{Z}_{q^2-1})^3$, $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q^2-1} \times \mathbb{Z}_{q^3-1}$, $(\mathbb{Z}_{q-1})^2 \times \mathbb{Z}_{q^4-1}$, $(\mathbb{Z}_{q+1})^2 \times (\mathbb{Z}_{q^2-1})^2$, $\mathbb{Z}_{q^2-1} \times \mathbb{Z}_{(q+1)(q^3-1)}$, $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q^2+q+1} \times \mathbb{Z}_{q^3-1}$, $\mathbb{Z}_{q^2-1} \times \mathbb{Z}_{q^4-1}$, $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q^5-1}$, $\mathbb{Z}_{q^2-1} \times \mathbb{Z}_{(q-1)(q^3+1)}$, $(\mathbb{Z}_{(q-1)(q^2+1)})^2$, $\mathbb{Z}_{q^2+q+1} \times \mathbb{Z}_{(q+1)(q^3-1)}$, $(\mathbb{Z}_{q+1})^2 \times \mathbb{Z}_{q^4-1}$, $\mathbb{Z}_{(q+1)(q^5-1)}$, $\mathbb{Z}_{q^2+q+1} \times \mathbb{Z}_{(q-1)(q^3+1)}$, $\mathbb{Z}_{(q^2-1)(q^4+1)}$, $\mathbb{Z}_{(q-1)(q^2+1)(q^3+1)}$, $(\mathbb{Z}_{q^2+q+1})^3$, $\mathbb{Z}_{q+1} \times \mathbb{Z}_{q^5+q^4+q^3+q^2+q+1}$, $\mathbb{Z}_{(q^2+q+1)(q^4-q^2+1)}$, $\mathbb{Z}_{q^6+q^3+1}$, $\mathbb{Z}_{q^2-q+1} \times \mathbb{Z}_{q^4+q^2+1}$.

Если $(3, q-1) = 1$, то этот результат дает описание полупростой части спектра простой группы $E_6(q)$. В случае $(3, q-1) = 3$ полезны следующие два простых замечания. Пусть A — конечная группа p-периода p^k, содержащая нормальную подгруппу Z порядка p. Если A содержит подгруппу, изоморфную $(\mathbb{Z}_{p^k})^2$, то p-период фактор-группы A/Z также равен p^k. Кроме того, легко видеть, что 3-часть числа $q^k - 1$ равна произведения 3-частей чисел k и $q-1$. С помощью этих замечаний можно получить периоды образов всех максимальных торов, перечисленных в лемме 2.2.1, кроме торов изоморфных $(\mathbb{Z}_{q-1})^3 \times \mathbb{Z}_{q^3-1}$, $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q^2-1} \times \mathbb{Z}_{q^3-1}$, $\mathbb{Z}_{q^2-1} \times \mathbb{Z}_{(q+1)(q^3-1)}$, $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q^2+q+1} \times \mathbb{Z}_{q^3-1}$, $\mathbb{Z}_{q^2+q+1} \times \mathbb{Z}_{(q+1)(q^3-1)}$, $\mathbb{Z}_{q^2+q+1} \times \mathbb{Z}_{(q-1)(q^3+1)}$. В таблице 2 для этих торов указаны матрицы M_w элементов группы Вейля w таких, что тор $\overline{T}_{\sigma\circ w}$ изоморфен одной из указанных групп. Кроме того, для каждой матрицы указаны матрицы A и B такие, что матрица $A(qM_w - 1)B$ диагональна. При этом, если $(3, q-1) = 3$, то все перечисленные матрицы целочисленны. Отметим, что вычисления были проведены в системе MAGMA.

Таблица 2

M_w	A	B	$A(qM_w-1)B$
$\begin{pmatrix} 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & -2 & -1 & -1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & 2 & 1 \\ 0 & -1 & -1 & -2 & -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & q-1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 & 1 & 0 \\ q+1 & 1 & -q^2+1 & 2 & 1 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & q & 0 & 0 & 0 & q^2 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & -q \\ 1 & -q & 0 & 1 & 0 & -q^2 \\ -1 & q+1 & 0 & 0 & 1 & q^2+q \\ 0 & -1 & 1 & -2 & -1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & q-1 & 0 & 0 & 0 \\ 0 & 0 & 0 & q-1 & 0 & 0 \\ 0 & 0 & 0 & 0 & q-1 & 0 \\ 0 & 0 & 0 & 0 & 0 & q^3-1 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 & 2 & 3 & 2 & 1 \\ 0 & 0 & -1 & -1 & -1 & 0 \\ -1 & -1 & -1 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ -1 & 0 & -1 & -1 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 & 0 \\ q^2+1 & 2q^2+q+2 & -2q+1 & -q+2 & -q+1 & 1 \\ q^3+q^2+q+1 & 2q^3+3q^2+4q+2 & -2q^2-q & -q^2+q+1 & -q^2 & q+1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & 0 & 0 & 2q & -2q^3-2q^2-q \\ 0 & -1 & 0 & 0 & -q & q^3+q^2+q \\ q & q & -1 & 0 & -q^2-q & q^4+2q^3+q^2+q \\ 1 & 2 & 0 & 1 & 0 & -q \\ -q-1 & -q-2 & 1 & -1 & q^2+q+1 & -q^4-2q^3-2q^2-q-1 \\ 0 & 0 & 0 & -1 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & q-1 & 0 & 0 \\ 0 & 0 & 0 & 0 & q-1 & 0 \\ 0 & 0 & 0 & 0 & 0 & (q+1)(q^3-1) \end{pmatrix}$
$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & -1 & -1 & 0 \\ -1 & -1 & -2 & -2 & -1 & -1 \\ 1 & 1 & 1 & 2 & 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ q^2-q+1 & -q+1 & -2q+1 & -2q+2 & -q+2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ q^2-q+1 & -q+1 & -2q+2 & -2q+3 & -q+2 & 1 \\ -q^3 & q^2-1 & 2q^2-1 & 2q^2-q-1 & q^2-q-1 & -q-1 \\ q^3 & -q^2 & -2q^2-q & -2q^2 & -q^2+q+1 & q+1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & q \\ 0 & -1 & 0 & 1 & q-1 & q^3-1 \\ q & -q & -1 & 0 & 0 & q^4-q^2-q \\ -q & q+1 & 1 & -1 & -q & -q^4-q^3 \\ q+1 & -q-2 & -1 & 1 & q+1 & q^4+2q^3+q^2 \\ -q-1 & q+2 & 1 & -1 & -q-1 & -q^4-2q^3-q^2+1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & q^2-1 & 0 \\ 0 & 0 & 0 & 0 & 0 & (q+1)(q^3-1) \end{pmatrix}$
$\begin{pmatrix} -1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ q & 0 & q+1 & q+1 & 0 & 0 \\ q^2 & 0 & q^2+q & q^2+q+1 & q^2+q & q^2 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -q & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & -q-1 & -q^3-q^2+q+1 & -q^3-2q^2-q & -q^4-2q^3-q^2 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & q^2-1 & q^2+q & q^3+q^2 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & q \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & q-1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & q^3-1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -q^2-q-1 \end{pmatrix}$
$\begin{pmatrix} -1 & 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -2 & -2 & -3 & -2 & -1 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -q & -q^2-1 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -q & 1 & 1 & 1 & 0 \\ 1 & q+1 & q^2+q+1 & q^3+q^2+q+1 & q+1 & q+1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & q & q & 0 & q^4-q^2-q \\ 0 & -1 & 0 & 0 & -q & 0 \\ 1 & 0 & -q-1 & -q & 0 & -q^4-q^3+q^2+q+1 \\ 0 & 0 & 0 & -1 & 0 & q \\ -1 & 0 & q+1 & q+1 & -1 & q^4+q^3-q^2-2q-1 \\ 1 & 1 & -q & -q & q+1 & -q^4+q^2+q+1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & q^2+q+1 & 0 \\ 0 & 0 & 0 & 0 & 0 & (q+1)(q^3-1) \end{pmatrix}$
$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & -1 & 0 & -1 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	смотри ниже	смотри ниже	$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -\frac{1}{3}(q^6-1) \end{pmatrix}$

В последней строке таблицы 2 матрицы A и B равны соответственно

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ -q & 1 & q^2 & -q+1 & -q & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & q^2 & 1 & -q & 0 \\ 0 & 0 & -q & 0 & 1 & 0 \\ \frac{-q(q-1)(q^4-q^3-2q-1)}{3} & \frac{(q-2)(q^4+q^2+1)}{3} & \frac{q^2(q-1)^2(q^3-2)}{3} & \frac{-(q-1)(q-2)(q^4+q^2+1)}{3} & \frac{-q(q-1)^2(q^3-2)}{3} & \frac{(q-1)(q^4-q^3-2q-1)}{3} \end{pmatrix},$$

$$\begin{pmatrix} 1 & q^4-2q^3+q^2-2q & 0 & 0 & q & \frac{1}{3}(q^5-q) \\ 0 & q^4-q^3-2q-1 & 0 & -1 & 0 & \frac{q^6-1}{3(q-1)} \\ 0 & -q^2+2q & 1 & 0 & 0 & -\frac{1}{3}(q^3-q) \\ 0 & -q^4+q^3+q^2+q & 0 & 1 & 0 & -\frac{1}{3}(q^5+q^4+q) \\ 0 & q^3-2q^2 & 0 & 0 & 1 & \frac{1}{3}(q^4-q^2) \\ 0 & q-2 & 0 & 0 & 0 & \frac{1}{3}(q^2-1) \end{pmatrix}.$$

Предложение 2.2.2. *Пусть S — это некоторый нециклический максимальный тор группы $\overline{G}_\sigma$. Тогда периоды тора S и фактор-группы тора S по центру группы $\overline{G}_\sigma$ совпадают.*

Доказательство. Предложение необходим проверить только для пяти указанных выше торов. Для них нужно показать, что центр не содержится в циклическом прямом сомножителе максимального 3-периода. Это делается непосредственной проверкой с использованием информации из таблицы 2. В качестве иллюстрации мы приведем рассуждение для случая, когда тор S изоморфен группе $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1} \times \mathbb{Z}_{q^3-1}$. Согласно таблице 2 тор S сопряжен в группе $\overline{G}$ подгруппе, состоящей из элементов вида

$$h_{r_1}(s_2 s_3^{-1} s_4^{q+1}) h_{r_2}(s_1^{-1} s_4) h_{r_3}(s_1^{q-1} s_3 s_4^{-q^2+1}) h_{r_4}(s_2 s_4^2) h_{r_5}(s_3 s_4) h_{r_6}(s_4), \tag{2.9}$$

где $s_1^{q-1} = s_2^{q-1} = s_3^{q-1} = s_4^{q^3-1} = 1$. Напомним, что центр Z группы $\overline{G}_\sigma$ состоит из элементов вида $h_{r_1}(t) h_{r_3}(t^2) h_{r_5}(t) h_{r_6}(t^2)$, где $t^{(3,q-1)} = 1$. Если мы положим $s_1 = s_2 = s_3 = 1$ в формуле 2.9, то мы получим элементы вида

$$h_{r_1}(s_4^{q+1}) h_{r_2}(s_4) h_{r_3}(s_4^{-q^2+1}) h_{r_4}(s_4^2) h_{r_5}(s_4) h_{r_6}(s_4).$$

Эти элементы образуют циклическую подгруппу порядка $q^3 - 1$, которая пересекается с центром по единице, что и требовалось показать. □

Пусть теперь $\overline{G}$ имеет тип E_7. Напомним, что группа $\overline{G}_\sigma$ является односвзяной группой, а ее фактор по центру прост. Результат для этого случая, аналогичный предложению 2.2.1, был также получен в [47]. Мы не приводим его здесь, поскольку в этом нет необходимости, при этом список максимальных торов конечной односвязной группы типа E_7 гораздо длиннее. Отметим, лишь, что из этого результат напрямую следует описание полупростой части спектра односвязной группы. Здесь мы докажем следующее утверждение.

Предложение 2.2.3. *Пусть $d = (2, q-1)$ и $\nu_{p'}(\overline{G}_\sigma / Z(\overline{G}_\sigma))$ — это множество* $\left\{ \frac{(q^2-q+1)(q^5+1)}{d}, \frac{(q^2+q+1)(q^5-1)}{d}, \frac{(q+1)(q^6-q^3+1)}{d}, \frac{(q-1)(q^6+q^3+1)}{d}, \frac{q^7+1}{d}, \frac{q^7-1}{d}, \frac{(q^3-1)(q^4-q^2+1)}{d}, \right.$ $\left. \frac{(q^3+1)(q^4-q^2+1)}{d}, (q^2-q+1)(q^4-1), (q^2+q+1)(q^4-1), (q+1)(q^5-1), (q-1)(q^5+1), \frac{q^8-1}{(q-1)(4,q-1)}, \right.$ $\left. \frac{q^8-1}{(q+1)(4,q+1)}, (q^4+1)(q^2-1), q^6-1 \right\}$.

Тогда $\mu_{p'}(\overline{G}_\sigma/Z(\overline{G}_\sigma)) \subseteq \nu_{p'}(\overline{G}_\sigma/Z(\overline{G}_\sigma)) \subseteq \omega(\overline{G}_\sigma/Z(\overline{G}_\sigma))$.

Доказательство. Сначала покажем, что все числа из $\nu_{p'}(\overline{G}_\sigma)$ являются периодами некоторых максимальных торов группы $\overline{G}_\sigma$. Положим $Z = Z(G)$. Первые восемь чисел в формулировке имеют вид $\frac{m}{d}$, где m — это порядок некоторого циклического максимального тора группы G, таким образом, эти числа очевидно являются периодами максимальных торов группы $\overline{G}_\sigma$. Пусть T — это некоторый максимальный тор группы G. Тогда периоды торов T и T/Z совпадают тогда и только тогда, когда $C \cap Z = 1$ для некоторой максимальной циклической 2-подгруппы C группы T. По [47, таблицы 2, 3] группа G содержит торы, изоморфные следующим группам: $\mathbb{Z}_{q-1} \times \mathbb{Z}_{(q^2-q+1)(q^4-1)}$, $\mathbb{Z}_{q+1} \times \mathbb{Z}_{(q^2+q+1)(q^4-1)}$, $\mathbb{Z}_{q-1} \times \mathbb{Z}_{(q+1)(q^5-1)}$, $\mathbb{Z}_{q+1} \times \mathbb{Z}_{(q-1)(q^5+1)}$, $\mathbb{Z}_{q+1} \times \mathbb{Z}_{q^6-1}$, $\mathbb{Z}_{q-1} \times \mathbb{Z}_{(q^4+1)(q^2-1)}$, $\mathbb{Z}_{(q^2+1)(q-1)} \times \mathbb{Z}_{q^4+1}$, $\mathbb{Z}_{(q^2+1)(q+1)} \times \mathbb{Z}_{q^4+1}$. Для всех этих торов, за исключением последних двух, период при переходе к простой группе сохраняется, периоды последних двух торов делятся на $(2, \frac{q+1}{d})$ и $(2, \frac{q-1}{d})$ соответственно. Для доказательства этого факта мы использовали систему компьютерных вычислений MAGMA. Ввиду большого объема данных, мы ограничимся примером. Покажем, что период тора $\mathbb{Z}_{q+1} \times \mathbb{Z}_{q^6-1}$ сохраняется при факторизации по Z. Отождествим W с ее матричным представлением в базисе $r_1, \ldots, r_7$. Пусть

$$M = \begin{pmatrix} -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 0 & 1 & 1 & 2 & 2 & 2 & 1 \\ -1 & -1 & -2 & -3 & -2 & -1 & 0 \\ 1 & 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & -1 & 0 & -1 & -1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & -1 & -1 & -1 & 0 & 0 & 0 \end{pmatrix}.$$

Тогда $M \in W$ и $A(qM-1)B = D$, где $D = \mathrm{diag}(1,1,1,1,1,q+1,q^6-1)$, B — это матрица над кольцом целочисленных многочленов от q с определителем 1, а A равна

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ -q^2+q-1 & q-1 & -q^2+q-1 & q-1 & -1 & -1 & -1 \\ -q^4-q^3-q^2-2 & q^3+q^2-2 & -q^4-q^3-q^2-q-3 & q^3+q^2-3 & -q^2-2q-3 & -q^2-2q-3 & -q^2-2q-2 \\ q^5-q^4+q^3-q^2+q-2 & -q^4+q^3+q-2 & q^5-q^4+q^3+q-3 & -q^4+q^3+q-4 & q^3+q-3 & q^3+q-2 & q^3-1 \end{pmatrix}.$$

Положим $h(s) = \prod_{i=1\ldots7} h_{r_i}(s^{a_{7i}})$, где a_{7i} обозначает i-ый элемент седьмой строки матрицы A, а $s^{q^6-1} = 1$. Тогда соответствующая группа $\overline{T}_{\sigma\circ w}$ содержит циклическую подгруппу C порядка q^6-1, состоящую из элементов $h(s)$. Если $C \cap Z = Z$, то $Z = \langle h(s) \rangle$, где $s^2 = 1$. Непосредственная проверка показывает, что это не так.

Осталось показать, что период произвольного максимального тора делит некоторый элемент из $\nu_{p'}(\overline{G}_\sigma)$. Из [47, таблицы 2, 3] непосредственной проверкой получаем, что либо период максимального тора односвязной группы G делит одно из чисел в $\nu_{p'}(\overline{G}_\sigma)$, либо тор циклический, либо это один из торов $\mathbb{Z}_{(q^2+1)(q-1)} \times \mathbb{Z}_{q^4+1}$, $\mathbb{Z}_{(q^2+1)(q+1)} \times \mathbb{Z}_{q^4+1}$. Таким образом, предложение доказано. □

§ 2.3. Смешанная часть спектра групп $E_6^\varepsilon(q)$

Напомним, что для описания смешанной части спектра нужно выбрать некоторое множество $\mathfrak{M}$, содержащее полную систему представителей классов сопряженности σ-инвариантных редуктивных подгрупп максимального ранга группы $\overline{G}$, и для каждой подгруппы $\overline{G}_1$ из $\mathfrak{M}$ описать структуру группы вида $(\overline{G}_1)_{\sigma on}$. Следующая лемма показывает, что если две редуктивные группы максимального ранга группы $\overline{G}$ имеют изоморфные системы корней, то они сопряжены. Таким образом, можно считать, что различные подгруппы из $\mathfrak{M}$ имеют неизоморфные системы корней.

Лемма 2.3.1. *Пусть Ψ_1 и Ψ_2 — изоморфные подсистемы корневой системы E_6. Тогда существует элемент w группы Вейля W такой, что образ подсистемы Ψ_1 под действием w совпадает с Ψ_2. В частности, если $\overline{G}_1$ и $\overline{G}_2$ — редуктивные подгруппы максимального ранга группы $\overline{G}$ с корневыми системами Ψ_1 и Ψ_2 соответственно, то существует элемент g группы $\overline{G}$ такой, что $(\overline{G}_1)^g = \overline{G}_2$.*

Доказательство. См. [14, таблица 11]. □

В таблице 3 приведен список всех изоморфных типов подсистем Ψ системы корней типа E_6, а также их ортогональных дополнений $\Psi^\perp$.

Таблица 3. Подсистемы системы E_6.

Ψ	$\Psi^\perp$	Ψ	$\Psi^\perp$	Ψ	$\Psi^\perp$	Ψ	$\Psi^\perp$
A_1	A_5	$A_2 \times 2A_1$	$\varnothing$	$A_4 \times A_1$	$\varnothing$	$2A_1$	A_3
$2A_2$	A_2	A_5	A_1	A_2	$2A_2$	$A_3 \times A_1$	A_1
D_5	$\varnothing$	$3A_1$	A_1	A_4	A_1	$3A_2$	$\varnothing$
$A_2 \times A_1$	A_2	D_4	$\varnothing$	$A_5 \times A_1$	$\varnothing$	A_3	$2A_1$
$2A_2 \times A_1$	$\varnothing$	E_6	$\varnothing$	$4A_1$	$\varnothing$	$A_3 \times 2A_1$	$\varnothing$

Обозначим через ν_1 и ν_2 множества, состоящее из чисел $\eta(H)$, где H пробегает все редуктивные подгруппы максимального ранга простой группы $E_6(q)$ с системой корней типа A_1 и, соответственно, A_2. Следующая лемма дает описание множеств ν_1 и ν_2.

Лемма 2.3.2. *Имеют место равенства*

$$\nu_1 = p \cdot \omega_{p'}(SL_6(q)/Z) \text{ и}$$

$$\nu_2 = p(A_2) \cdot (\omega_{p'}((SL_3(q) \times SL_3(q))/Z) \cup \omega_{p'}(SL_3(q^2)/Z)),$$

где во всех случаях Z — это центральная подгруппа порядка $(3, q-1)$ в соответствующей группе, причем в случае группы $SL_3(q) \times SL_3(q)$ группа Z имеет нетривиальную проекцию на оба сомножителя.

Доказательство. Докажем первое равенство. Пусть H — редуктивная подгруппа максимального ранга группы $\overline{G}_\sigma$. В силу леммы 2.3.1 можем считать, что фундаментальный корень системы корней Ψ_1 группы H — это корень r_0. Пусть $\overline{H}$ — соответствующая

σ-инвариантная редуктивная подгруппа максимального ранга группы $\overline{G}$. Без ограничения общности можем считать, что $\overline{H}$ содержит максимальный тор $\overline{T}$, состоящий из всех элементов вида $h_{r_1}(t_1)h_{r_2}(t_2)\dots h_{r_6}(t_6)$. Поскольку $h_r(t)x_s(u)h_r(t)^{-1} = x_s(t^{A_{rs}}u)$ для любых корней r и s, элемент максимального тора $\overline{T}$ централизует корневую подгруппу X_{r_0} тогда и только тогда, когда $t_2 = 1$. Таким образом, центр группы $\overline{H}$ состоит из всех элементов вида $h_{r_1}(t_1)h_{r_3}(t_3)\dots h_{r_6}(t_6)$. По лемме 2.1.2 группа H сопряжена в $\overline{G}$ группе $\overline{H}_{\sigma\circ n}$, где $n \in N_{\overline{G}}(\overline{T}) \cap N_{\overline{G}}(\overline{H})$. Пусть $w = \pi(n)$ (напомним, что π — это канонический гомоморфизм из $N_{\overline{G}}(\overline{T})$ на W). Поскольку система корней Ψ_1 инвариантна относительно w, ее ортогональное дополнение Ψ_2 также w-инвариантно. Фундаментальная система корней системы Ψ_2 состоит из корней r_1, r_3, r_4, r_5 и r_6. Согласно [38, таблица 9] группа Вейля W не содержит элементов, индуцирующих графовый автоморфизм на подсистеме Ψ_2. Следовательно, действие элемента w на Ψ_2 совпадает с действием некоторого элемента из $W(\Psi_2) \simeq W(A_5)$. Корневые подгруппы, соответствующие корням $\pm r_1$, $\pm r_3$, $\pm r_4$, $\pm r_5$ и $\pm r_6$, порождают в $\overline{G}$ подгруппу $\overline{K}$, изоморфную $SL_6(\overline{\mathrm{F}}_p)$. Поскольку подгруппа $\overline{K}$ содержит центр группы $\overline{H}$ и группа неподвижных точек $\overline{K}_{\sigma\circ n}$ изоморфна $SL_6(q)$ (см., например, [55, предложение 2.6.2 (d)]), центр группы $\overline{H}_{\sigma\circ n}$ изоморфен некоторому максимальному тору группы $SL_6(q)$. Очевидно, верно и обратное, т.е. для любого максимального тора группы $SL_6(q)$ можно подобрать редуктивную подгруппу максимального ранга группы $\overline{G}_\sigma$ такую, что ее центр изоморфен данному тору. Для завершения доказательства первого равенства остается заметить, что группа $\overline{K}$ содержит центр группы $\overline{G}_\sigma$.

Докажем второе равенство. Как и раньше можно считать, что редуктивная подгруппа H сопряжена в $\overline{G}$ группе $\overline{H}_{\sigma\circ n}$, где $\overline{H} = \langle \overline{T}, X_{\pm r_0}, X_{\pm r_2}\rangle$, для некоторого $n \in N_{\overline{G}}(\overline{T}) \cap N_{\overline{G}}(\overline{H})$. При этом элемент тора $\overline{T}$ централизует группы X_{r_0} и X_{r_2} тогда и только тогда, когда $t_2 = t_4 = 1$. Группа, состоящая из всех элементов вида $h_{r_1}(t_1)h_{r_3}(t_3)h_{r_5}(t_5)h_{r_6}(t_6)$, содержится в группе $\overline{L} = \langle X_{\pm r_1}, X_{\pm r_3}, X_{\pm r_5}, X_{\pm r_6}\rangle \simeq SL_3(\overline{\mathrm{F}}_p) \times SL_3(\overline{\mathrm{F}}_p)$. Поскольку $\overline{L}$ — подгруппа группы $\overline{K}$ и согласно [38, таблица 9] группа автоморфизмом подсистемы типа $2A_2$, индуцированных группой Вейля W, имеет порядок 2, в зависимости от выбора n имеем либо $\overline{L}_{\sigma\circ n} \simeq SL_3(q) \times SL_3(q)$, либо $\overline{L}_{\sigma\circ n} \simeq SL_3(q^2)$. □

Для множества натуральных чисел A обозначим через $\omega(A)$ множество, состоящее из всех делителей элементов A. Для двух множеств натуральных чисел A и B запись $A \sim B$ будет означать, что $\omega(A) = \omega(B)$.

Следующее утверждение является непосредственным следствием леммы 2.3.2 и [3, теорема 1].

Следствие 2.3.3. *Пусть* $d = (3, q-1)$. *Имеем*

$$\nu_1 \sim p \cdot \left\{ \frac{q^6-1}{d(q-1)}, \frac{q^5-1}{d}, q^4-1, (q^3-1)(q+1) \right\},$$

$$\nu_2 \sim p(A_2) \cdot \left\{ \frac{(q^3-1)(q+1)}{d}, \frac{q^4+q^2+1}{d}, \frac{q^4-1}{d} \right\}.$$

Следующее наблюдение позволяет сузить класс групп, которые необходимо включить в множество $\mathfrak{M}$. Пусть $\overline{H}$ — редуктивная подгруппа максимального ранга группы

$\overline{G}$ с системой корней Ψ и $\overline{T}$ — σ-инвариантный максимальный тор, содержащийся в $\overline{H}$. Пусть $n \in N_{\overline{G}}(\overline{T}) \cap N_{\overline{G}}(\overline{H})$ и $w = \pi(n)$. Пусть Ψ_1 — аддитивно замкнутая подсистема системы Ψ, инвариантная относительно действия w, такая, что $p(\Psi_1) = p(\Psi)$. Положим $\overline{K} = \langle \overline{T}, \overline{X}_r,\ r \in \Psi_1 \rangle$. Тогда центр $Z(\overline{H}_{\sigma\circ n})$ является подгруппой центра $Z(\overline{K}_{\sigma\circ n})$. В частности, $\eta(\overline{H}_{\sigma\circ n})$ делит $\eta(\overline{K}_{\sigma\circ n})$.

Из этого замечания следует, что нам остается рассмотреть редуктивные группы с системой корней из следующего списка: $2A_1$, $3A_1$, A_3, $4A_1$, $2A_2$, A_4, D_4, A_5, D_5, $3A_2$. При этом в случаях разложимых подсистем мы можем считать, что скручивающий элемент не имеет инвариантных подсистем.

Пусть $\overline{T}$ — максимальный тор, состоящий из всех элементов вида $h_{r_1}(t_1)h_{r_2}(t_2)\dots h_{r_6}(t_6)$, $\overline{H}$ — σ-инвариантная редуктивная подгруппа, содержащая тор $\overline{T}$. Пусть $n \in N_{\overline{G}}(\overline{T}) \cap N_{\overline{G}}(\overline{H})$. Тогда $Z(\overline{H}_{\sigma\circ n}) = Z(\overline{H})_{\sigma\circ n}$. Центр группы $\overline{H}$ состоит из тех элементов максимального тора $\overline{T}$, которые централизуют все корневые подгруппы $\overline{X}_r$, где r пробегает фундаментальную систему корней группы $\overline{H}$.

Отметим, что если некоторое соотношение в группе $Z(\overline{H})$ имеет вид

$$t_i = t_1^{a_1} \dots t_{i-1}^{a_{i-1}} t_{i+1}^{a_{i+1}} \dots t_6^{a_6}$$

для некоторого i (например, в случае, $\Psi = 2A_1$ имеем $t_3 = t_1^2$). Пусть M_w — это матрица элемента $w = \pi(n)$ в базисе фундаментальных корней. Тогда умножим матрицу M_w слева на соответствующую этой замене матрицу и вычеркнем i-ую строку из матрицы M_w. Заметим, что i-ый столбец получившейся матрицы можно также вычеркнуть, поскольку соотношение, задаваемое этим столбцом, следует из остальных соотношений. Действительно, пусть $h_{r_1}(t_1)\dots h_{r_6}(t_6)$ — это элемент центра редуктивной подгруппы $\overline{H}_{\sigma\circ n}$. Имеем

$$(h_{r_1}(t_1)\dots h_{r_6}(t_6))^{\sigma\circ n} = h_{r_1 w}(t_1^q)\dots h_{r_6 w}(t_6^q) = h_{r_1}(t_1)\dots h_{r_6}(t_6).$$

Пусть $h_{r_1 w}(t_1^q)\dots h_{r_6 w}(t_6^q) = h_{r_1}(\tilde{t}_1)\dots h_{r_6}(\tilde{t}_6)$, где $\tilde{t}_i$ — это произведение степеней t_1, $\dots$, t_6. В силу выбора элемента имеем $\tilde{t}_i = \tilde{t}_1^{a_1} \dots \tilde{t}_{i-1}^{a_{i-1}} \tilde{t}_{i+1}^{a_{i+1}} \dots \tilde{t}_6^{a_6}$. Таким образом, равенство $\tilde{t}_i = t_i$ является следствием равенств $\tilde{t}_j = t_j$ для $j \neq i$ и равенства $t_i = t_1^{a_1} \dots t_{i-1}^{a_{i-1}} t_{i+1}^{a_{i+1}} \dots t_6^{a_6}$.

Таким образом, после умножения матрицы M_w на матрицы, соответствующие соотношениям группы $Z(\overline{H})$, и вычеркивания строк и столбцов получаем квадратную матрицу, которую необходимо представить в виде ADB, где D — диагональная, а A и B — унимодулярные.

В таблицах 4–11 в названии указаны система корней Ψ рассматриваемой редуктивной группы с фундаментальной системой Π и соотношения на t_1, $t_2, \dots, t_6$, выполненные для элементов тора $\overline{T}$, лежащих в центре $\overline{H}$. В таблицах M обозначает матрицу соотношений группы $Z(\overline{H}_{\sigma\circ n})$. Матрицы A и B в таблицах имеют определитель 1. Все вычисления выполнены в системе MAGMA.

В таблице 7 матрица M не является матрицей соотношений группы $Z(\overline{H}_{\sigma\circ n})$. Для того, чтобы получить матрицу соотношений группы $Z(\overline{H}_{\sigma\circ n})$, необходимо добавить столбец,

Таблица 4. $\Psi = 2A_1$, $\Pi = \{-r_0, r_1\}$, $t_2 = 1$, $t_3 = t_1^2$

M	A	B	$A(qM-1)B$
$\begin{pmatrix} q-1 & 3q & 2q & q \\ 0 & -q-1 & 0 & 0 \\ 0 & 0 & -q-1 & 0 \\ 0 & 0 & 0 & -q-1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ q+1 & 3 & 2 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & 0 & q \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 1 & 3 & 2 & -q+1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & q+1 & 0 & 0 \\ 0 & 0 & q+1 & 0 \\ 0 & 0 & 0 & q^2-1 \end{pmatrix}$
$\begin{pmatrix} q-1 & q & 2q & q \\ 0 & q-1 & 0 & 0 \\ 0 & -q & -q-1 & -q \\ 0 & 0 & 0 & q-1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ q+1 & 1 & 2 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & 0 & q \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & -q \\ -1 & -1 & -2 & q+1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & q-1 & 0 & 0 \\ 0 & 0 & q-1 & 0 \\ 0 & 0 & 0 & q^2-1 \end{pmatrix}$
$\begin{pmatrix} q-1 & q & 2q & q \\ 0 & q-1 & 0 & 0 \\ 0 & -q & -q-1 & 0 \\ 0 & 0 & 0 & -q-1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & q-1 & 0 \\ q+1 & 1 & 2 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & 0 & q \\ 0 & 1 & -q-1 & 0 \\ 0 & -1 & q & 0 \\ 1 & 1 & -q+1 & -q+1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & q^2-1 & 0 \\ 0 & 0 & 0 & q^2-1 \end{pmatrix}$
$\begin{pmatrix} q-1 & q & 2q & q \\ 0 & -1 & -q & 0 \\ 0 & 0 & -1 & -q \\ 0 & q & q & q-1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ q^2+1 & q^2+q+1 & q+1 & 1 \end{pmatrix}$	$\begin{pmatrix} q-1 & q & q & -q^2+q \\ -q & -q-1 & -q & q^2 \\ 1 & 1 & 1 & -q \\ 0 & 0 & -1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & q-1 & 0 \\ 0 & 0 & 0 & (q-1)(q^2+1) \end{pmatrix}$
$\begin{pmatrix} q-1 & 3q & 2q & q \\ 0 & -q-1 & -q & 0 \\ 0 & 0 & -1 & -q \\ 0 & 0 & q & q-1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ q^3+1 & q^3+q^2-q+2 & q^2+1 & 1 \end{pmatrix}$	$\begin{pmatrix} -q^2-1 & -q^2-q & -q & q^3-q^2+q \\ q^2 & q^2+q-1 & q & -q^3+q^2 \\ -q^2-q & -q^2-2q & -q-1 & q^3-q \\ q+1 & q+2 & 1 & -q^2+1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & (q-1)(q^3+1) \end{pmatrix}$

Таблица 5. $\Psi = 3A_1$, $\Pi = \{-r_0, r_1, r_6\}$, $t_2 = 1$, $t_3 = t_1^2$, $t_5 = t_6^2$

M	A	B	$A(qM-1)B$
$\begin{pmatrix} -1 & 2q & q \\ 0 & -q-1 & 0 \\ -q & -q & -q-1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ q & -1 & -1 \\ -q^2-q & q+2 & q+1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & -q \\ 0 & -1 & -q^2-q-1 \\ 0 & 2 & 2q^2+2q+1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (q+1)(q^2+q+1) \end{pmatrix}$

Таблица 6. $\Psi = A_3$, $\Pi = \{-r_0, r_2, r_4\}$, $t_2 = t_4 = 1$, $t_3 = t_5^{-1}$

M	A	B	$A(qM-1)B$
$\begin{pmatrix} q-1 & 0 & 0 \\ 0 & q-1 & 0 \\ 0 & 0 & q-1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} q-1 & 0 & 0 \\ 0 & q-1 & 0 \\ 0 & 0 & q-1 \end{pmatrix}$
$\begin{pmatrix} -q-1 & 0 & 0 \\ q & q-1 & -q \\ 0 & 0 & -q-1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 \\ -1 & q+1 & 0 \\ -1 & -q-1 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 & 0 \\ -1 & 0 & -q \\ -2 & 1 & -q+1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & q+1 & 0 \\ 0 & 0 & q^2-1 \end{pmatrix}$
$\begin{pmatrix} q-1 & 0 & 0 \\ 0 & q-1 & -q \\ 0 & 0 & -q-1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 \\ -1 & q-1 & 0 \\ 0 & -q-1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & -q \\ -1 & 0 & -q+1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & q-1 & 0 \\ 0 & 0 & q^2-1 \end{pmatrix}$
$\begin{pmatrix} -1 & 0 & -q \\ 0 & q-1 & 0 \\ -q & 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -q & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & -q \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & q-1 & 0 \\ 0 & 0 & q^2-1 \end{pmatrix}$
$\begin{pmatrix} -1 & 0 & q \\ 0 & q-1 & -q \\ -q & 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -q & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & -q \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (q-1)(q^2+1) \end{pmatrix}$

Таблица 7. $\Psi = 4A_1$, $\Pi = \{-r_0, r_1, r_4, r_6\}$, $t_2 = 1$, $t_3 = t_1^2$, $t_5 = t_6^2$, $t_4^2 = t_1^2 t_6^2$

M	A	B	$A(qM-1)B$
$\begin{pmatrix} -1 & -q & -2q \\ 0 & -1 & q \\ -q & -q & -q-1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -q & q^2-q & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & q & -q^2-2q \\ 0 & -1 & q \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (q+1)(q^2-1) \end{pmatrix}$

Таблица 8. $\Psi = 2A_2$, $\Pi = \{-r_0, r_2, r_1, r_3\}$, $t_2 = t_4 = 1$, $t_3 = t_1^2$, $t_1^3 = 1$

M	A	B	$A(qM-1)B$
$\begin{pmatrix} -2q-1 & -4q & -2q \\ 0 & -q-1 & 0 \\ 0 & 0 & -q-1 \end{pmatrix}$			
$\begin{pmatrix} -2q-1 & -4q & -2q \\ 0 & -1 & q \\ 0 & q & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & q \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & -q & 1 \end{pmatrix}$	$\begin{pmatrix} -2q-1 & 0 & 0 \\ 0 & -q^2-1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$
$\begin{pmatrix} -2q-1 & -4q & -2q \\ 0 & q-1 & q \\ 0 & -q & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 0 \\ -q^2+q-1 & -2q^2+2q-1 & q \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 2q+2 & -1 & 0 \\ -2q-1 & 1 & 0 \\ 2q^2+q & -q & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 & 0 \\ (2q+1)(q^2-q+1) & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$

Таблица 9. $\Psi = A_4$, $\Pi = \{-r_0, r_2, r_4, r_3\}$, $t_2 = t_4 = 1$, $t_3 = t_5^{-1}$, $t_1 = t_3^2$

M	A	B	$A(qM-1)B$
$\begin{pmatrix} q-1 & 0 \\ 0 & q-1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} q-1 & 0 \\ 0 & q-1 \end{pmatrix}$
$\begin{pmatrix} q-1 & -q \\ 0 & -q-1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ -q-1 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & -q \\ -1 & -q+1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & q^2-1 \end{pmatrix}$

Таблица 10. $\Psi = D_4$, $\Pi = \{-r_0, r_2, r_4, r_1+r_3+r_4+r_5+r_6\}$, $t_2 = t_4 = 1$, $t_3 = t_5^{-1}$, $t_1 = t_6^{-1}$

M	A	B	$A(qM-1)B$
$\begin{pmatrix} q-1 & 0 \\ 0 & q-1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} q-1 & 0 \\ 0 & q-1 \end{pmatrix}$
$\begin{pmatrix} -q-1 & 0 \\ q & q-1 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & q+1 \end{pmatrix}$	$\begin{pmatrix} -1 & -q+1 \\ 1 & q \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & q^2-1 \end{pmatrix}$
$\begin{pmatrix} -1 & q \\ -q & -q-1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & -q \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & q^2+q+1 \end{pmatrix}$

Таблица 11. $\Psi = A_5$, $\Pi = \{-r_0, r_2, r_4, r_1, r_3\}$, $t_2 = t_4 = 1$, $t_3 = t_5^{-1} = t_1^2$, $t_1^3 = 1$

M	A	B	$A(qM-1)B$
$\begin{pmatrix} q-1 & 0 \\ 0 & q-1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} q-1 & 0 \\ 0 & q-1 \end{pmatrix}$
$\begin{pmatrix} q-1 & q \\ 0 & -q-1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ q+1 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & q \\ 1 & -q+1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & q^2-1 \end{pmatrix}$

задающий соотношение $t_4^2 = t_1^2 t_6^2$. Поскольку $\eta(\overline{H}_{\sigma\circ n})$ в этом случае делит $p(q+1)(q^2-1)$, из следствия 2.3.3 следует, что $\eta(\overline{H}_{\sigma\circ n})$ не лежит в $\mu(E_6(q))$.

В таблице 8 при вычислении матрицы M не учитывалось соотношение $t_1^3 = 1$. В первой строчке этой таблицы не приведены результаты вычислений, поскольку из соотношений $t_1^{-4q} t_5^{-q-1} = 1$, $t_1^{-2q} t_6^{-q-1} = 1$ следует, что период данной группы делит $(3, q-1)(q+1)$, что с учетом следствия 2.3.3 влечет, что $\eta(\overline{H}_{\sigma\circ n})$ в этом случае не лежит в $\mu(E_6(q))$. Поскольку $t_1^3 = 1$, для второй строки имеем, что $\eta(\overline{H}_{\sigma\circ n})$ делит $(3, q-1)(q^2+1)$. Период центра соответствующей подгруппы простой группы делит q^2+1, по следствию 2.3.3 этот элемент не лежит в $\mu(E_6(q))$. В последнем случае имеем, что центр задается одним параметром s, где $|s| = (2q+1)(q^2-q+1)$, причем $t_1 = s^{-q^2+q-1}$. Таким образом, в этом случае $\eta(\overline{H}_{\sigma\circ n})$ делит $(3, q-1)(q^2-q+1)$. Поскольку группа $\overline{H}_{\sigma\circ n}$ циклическая, период центра соответствующей редуктивной подгруппы простой группы равен числу q^2-q+1, которое делит $(q^4+q^2+1)/(3, q-1)$. По следствию 2.3.3 число $p(A_2)(q^2-q+1)$ не максимально по делимости в спектре $E_6(q)$.

В таблице 11 приведены результаты вычислений без учета соотношения $t_1^3 = 1$. При этом, в первом случае очевидно, что период центра соответствующей подгруппы простой группы равен $q-1$. Во втором случае имеем циклическую группу, чьи элементы задаются параметром s таким, что $s^{q^2-1} = 1$, $t_1 = s^{q+1}$, $t_6 = s$. Отсюда получаем, что центр имеет порядок $(3, q-1)(q+1)$, и следовательно, период центра в простой группе равен $q+1$.

Доказательство теоремы 10. Как и в случае максимальных торов, результат для ${}^2E_6(q)$ может быть получен из результата для $E_6(q)$ заменой q на $-q$. Таким образом, можно считать, что $G = E_6(q)$. Нам достаточно показать, что для произвольной редуктивной группы максимального ранга H, значение $\eta(H)$ делит одно из чисел, перечисленных в теореме. Если H — максимальный тор, то из предложений 2.2.1 и 2.2.2 следует, что период

тора делит одно из чисел пункта (1). Кроме того, из этих предложений следует, что все числа из пункта 1) лежат в спектре группы G. Если H имеет систему корней, изоморфную A_1 или A_2, то требуемое было показано в следствии 2.3.3. Как и раньше, можно не рассматривать редуктивные группы, чья система корней имеет собственную подсистему, инвариантную относительно действия скручивающего элемента.

Пусть система корней Ψ группы H изоморфна $2A_1$. Из таблицы 4 следует, что период центра группы H равен одному из следующих чисел: $\frac{q^2-1}{d}$, q^2-1, $(q-1)(q^2+1)$, $\frac{(q-1)(q^3+1)}{d}$. Следовательно, $\eta(H)$ делит одно из чисел пункта (2).

Если система Ψ изоморфна $3A_1$, то из таблицы 5 следует, что число $\eta(H)$ равно $p\frac{(q+1)(q^2+q+1)}{d}$ и делит $p\frac{q^6-1}{d(q-1)}$.

Пусть система Ψ изоморфна A_3. Из таблицы 6 следует, что период центра группы H равен одному из следующих чисел: $q-1$, $\frac{q^2-1}{d}$, q^2-1, $\frac{(q-1)(q^2+1)}{d}$. Следовательно, $\eta(H)$ делит одно из чисел пункта (4).

Если система Ψ изоморфна $4A_1$, то из таблицы 7 следует, что центр задается следующими равенствами $t_1 = t_6^{-q}$, $t_4 = t_6^{q^2-q}$, $t_6^{(q+1)(q^2-1)} = 1$ и $t_4^2 = t_1^2 t_6^2$. Подставляя выражения для t_1 и t_4 в последнее равенство, получаем, что период тора равен $(2, q-1)(q^2-1)$, что делит $p(q^4-1)$.

Как показано выше, из таблицы 8 следует, что для каждой подгруппы H с системой корней типа $2A_2$ существует редуктивная подгруппа K с системой корней типа A_2 такая, что $\eta(H)$ делит $\eta(K)$.

Если система Ψ изоморфна A_4, то из таблицы 9 следует, что число $\eta(H)$ равно $p(A_4)\frac{q^2-1}{d}$ или $p(A_4)(q-1)$. Поскольку $p(D_4) \geqslant p(A_4)$, эти числа делят одно из чисел пункта (5).

Если система Ψ изоморфна A_5, то, как показано выше, из таблицы 11 следует, что число $\eta(H)$ равно $p(A_5)(q-1)$ или $p(A_5)(q+1)$. Поскольку $p(D_4) = p(A_5)$, эти числа делят одно из чисел пункта (5).

Нормализатор подсистемы типа D_5 в группе Вейля совпадает с ее группой Вейля. Таким образом, существует только один класс сопряженных редуктивных подгрупп максимального ранга с такой системой корней. Тривиально проверяется, что центр в этом случае циклический порядка $\frac{q-1}{d}$.

Редуктивная подгруппа с системой корней типа $3A_2$ имеет центр порядка d.

Теорема доказана. □

Теорема 11 напрямую следует из данных, использованных в доказательстве теоремы 10.

§ 2.4. Смешанная часть спектра групп $E_7(q)$

Пусть $\overline{G}$ — это односвязная группа лиева типа E_7 над алгебраическим замыканием поля Галуа F_p для некоторого простого числа p. Пусть σ — это отображение Фробениуса группы $\overline{G}$, переводящее корневой элемент $x_r(t)$ в $x_r(t^q)$. Обозначим через G группу $\overline{G}_\sigma$

Как и ранее, через r_0 будем обозначать корень максимальной высоты. Через Z обозначим центр группы $\overline{G}$.

Напомним, что при описании спектра можно рассматривать только те редуктивные группы, у которых система корней не имеет инвариантных подсистем. В таблице 12 указаны все аддитивно замкнутые подсистемы системы E_7 с изоморфными неразложимыми компонентами с точностью до эквивалентности относительно действия группы W, а также ортогональные дополнения к этим подсистемам (см. [45, таблица 1] или [14, таблица 11]).

Таблица 12. Подсистемы системы E_7

Ψ	$\Psi^\perp$	Ψ	$\Psi^\perp$	Ψ	$\Psi^\perp$	Ψ	$\Psi^\perp$	Ψ	$\Psi^\perp$
A_1	D_6	$(A_5)_2$	A_1	D_6	A_1	$(3A_1)_2$	$4A_1$	$7A_1$	$\varnothing$
A_2	A_5	A_6	$\varnothing$	E_6	$\varnothing$	$(4A_1)_1$	$3A_1$	$2A_2$	A_2
A_3	A_3+A_1	A_7	$\varnothing$	E_7	$\varnothing$	$(4A_1)_2$	$3A_1$	$3A_2$	$\varnothing$
A_4	A_2	D_4	$3A_1$	$2A_1$	D_4+A_1	$5A_1$	$2A_1$	$2A_3$	A_1
$(A_5)_1$	A_2	D_5	A_1	$(3A_1)_1$	D_4	$6A_1$	A_1		

Заметим, что существует два класса эквивалентности подсистем типа $4A_1$. Для одного из этих классов двойной переход к ортогональному дополнению дает исходную подсистему, для второго класса получается подсистема типа D_4.

Лемма 2.4.1. *Пусть H — редуктивная подгруппа максимального ранга группы G с системой корней типа $5A_1$, $6A_1$ или $7A_1$. Тогда существует редуктивная подгруппа максимального ранга H_1 группы G с системой корней, отличной от $5A_1$? $6A_1$ и $7A_1$, такая, что $\eta(H)$ делит $\eta(H_1)$.*

Доказательство. Пусть s — это элемент цента группы H порядка, совпадающего с периодом центра. Положим $\overline{H}_1 = C_{\overline{G}}(s)$. По [46, предложение 2.3.4] система корней группы $\overline{H}_1$ отлична от $6A_1$ и $7A_1$. Очевидно, $H \subseteq \overline{H}_1$. Таким образом, $H \subseteq H_1 = (\overline{H}_1)_\sigma$ и, следовательно, $\eta(H)$ делит $\eta(H_1)$.

В случае системы $5A_1$ из [38, таблица 11] следует, что группа автоморфизмов этой подсистемы, индуцированных группой Вейля, имеет порядок 8. Следовательно, любой элемент группы Вейля нормализующий, эту подсистему, нормализует некоторую собственную подсистему системы $5A_1$ и утверждение в этом случае следует из вышеприведенных рассуждений. □

Из леммы 2.4.1 следует, что системы $5A_1$, $6A_1$ и $7A_1$ можно не рассматривать при описании спектра группы G.

В таблице 13 для каждого класса подсистем из таблицы 12 (за исключением $5A_1$, $6A_1$ и $7A_1$) указана фундаментальная система корней Π некоторого представителя данного класса, при этом

$$r_8 = (0, 1, 1, 2, 2, 1, 0),$$

Таблица 13. Центры редуктивных подгрупп в E_7

Ψ	Π	Центр
A_1	$-r_0$	$t_1 = 1$
A_2	$-r_0$, r_1	$t_1 = t_3 = 1$
A_3	$-r_0$, r_1, r_3	$t_1 = t_3 = t_4 = 1$
A_4	$-r_0$, r_1, r_3, r_4	$t_1 = t_3 = t_4 = 1$, $t_2 = t_5^{-1}$
$(A_5)_1$	$-r_0$, r_1, r_2, r_3, r_4	$t_1 = t_3 = t_4 = 1$, $t_2 = t_5^{-1}$, $t_2^2 = 1$
$(A_5)_2$	$-r_0$, r_1, r_3, r_4, r_5	$t_1 = t_3 = t_4 = 1$, $t_2 = t_5^{-1}$, $t_6 = t_5^2$
A_6	$-r_0$, r_1, r_3, r_4, r_5, r_6	$t_1 = t_3 = t_4 = 1$, $t_2 = t_5^{-1}$, $t_6 = t_5^2$, $t_7 = t_5^3$
A_7	$-r_0$, r_1, r_3, r_4, r_5, r_6, r_7	$t_1 = t_3 = t_4 = 1$, $t_2 = t_5^{-1}$, $t_6 = t_5^2$, $t_7 = t_5^3$, $t_7^4 = 1$
D_4	$-r_0$, r_1, r_3, r_8	$t_1 = t_3 = t_4 = 1$, $t_7 = t_5$
D_5	$-r_0$, r_1, r_3, r_4, r_8	$t_1 = t_3 = t_4 = 1$, $t_2 = t_5^{-1}$, $t_7 = t_5$
D_6	$-r_0$, r_1, r_2, r_3, r_4, r_5	$t_1 = t_3 = t_4 = t_6 = 1$, $t_2 = t_5^{-1}$, $t_2^2 = 1$
E_6	r_1, r_2, r_3, r_4, r_5, r_6	$t_3 = t_1^2$, $t_4 = t_2^2 = t_1^3$, $t_5 = t_1 t_2$, $t_6 = t_1^2$, $t_7 = t_2$
$2A_1$	$-r_0$, r_9	$t_1 = t_6 = 1$
$(3A_1)_1$	$-r_0$, r_7, r_9	$t_1 = t_6 = 1$, $t_7^2 = 1$
$(3A_1)_2$	$-r_0$, r_9, r_{10}	$t_1 = t_4 = t_6 = 1$
$(4A_1)_1$	$-r_0$, r_2, r_9, r_{10}	$t_1 = t_4 = t_6 = 1$, $t_2^2 = 1$
$(4A_1)_2$	$-r_0$, r_3, r_9, r_{10}	$t_1 = t_4 = t_6 = 1$, $t_3^2 = 1$
$2A_2$	$-r_0$, r_1, r_6, r_7	$t_1 = t_3 = 1$, $t_6 = t_7^2$, $t_5 = t_7^3$
$3A_2$	$-r_0$, r_1, r_2, r_4, r_6, r_7	$t_1 = t_3 = 1$, $t_6 = t_7^2$, $t_5 = t_7^3$, $t_4 = t_2^2$, $t_2^3 = t_7^3$
$2A_3$	$-r_0$, r_1, r_3, r_5, r_6, r_7	$t_1 = t_3 = t_4 = 1$, $t_6 = t_7^2$, $t_5 = t_7^3$, $t_7^4 = 1$

$$r_9 = (0, -1, -1, -2, -2, -2, -1),$$

$$r_{10} = (0, -1, -1, -2, -1, 0, 0)$$

(здесь указаны коэффициенты разложения по фундаментальным корням). В третьем столбце указаны необходимые и достаточные условия того, что элемент $\prod_{i=1\ldots7} h_{r_i}(t_i)$ лежит в центре редуктивной подгруппы максимального ранга группы $\overline{G}$, содержащей тор $\overline{T}$ и имеющей систему корней Ψ.

Нам понадобится описание полупростой части спектра спинорных групп (см. [15]) и группы ${}^3D_4(q)$, а также следующая лемма.

Лемма 2.4.2. $\omega_{p'}(HSpin_{2n}(q)) = \omega_{p'}(Spin^+_{2n}(q))$.

Доказательство. Группа $HSpin_{2n}(q)$ определена при n четном и q нечетном. При этих условиях центр группы $Spin^+_{2n}(q)$ изоморфен элементарной абелевой группе порядка 4. Фактор-группа по одной из центральных инволюций дает группу $\Omega^+_{2n}(q)$, факторгруппы по двум другим центральным инволюциям изоморфны (изоморфизм осуществляется графовым автоморфизмом τ порядка 2) и обозначаются $HSpin_{2n}(q)$. Пусть T — это некоторый максимальный тор группы $Spin^+_{2n}(q)$, C — максимальная по порядку цикличе-

ская 2-подгруппа группы T и z — центральная инволюция группы $Spin^+_{2n}(q)$ такая, что $Spin^+_{2n}(q)/\langle z\rangle \simeq HSpin_{2n}(q)$. Предположим, что $z \in C$, тогда $z^\tau \notin C$. Таким образом, периоды торов T и $T/\langle z^\tau\rangle$ совпадают. Следовательно, если T — это максимальный тор, период которого делится на два при факторизации по подгруппе $\langle z\rangle$, то существует изоморфный тор, период которого сохраняется. Таким образом, имеем требуемое равенство. □

Обозначим через $\upsilon(\Psi)$ и $\nu(\Psi)$ множество всех $\eta(H)$ и $\eta(H/Z)$, где H пробегает все редуктивные подгруппы максимального ранга группы G с системой корней Ψ. Положим $d = (2, q-1)$.

Предложение 2.4.3. *Имеют место следующие равенства.*

1) $\upsilon(A_1) = p(A_1)\cdot\omega_{p'}(Spin^+_{12}(q))$;

2) $\upsilon(A_2) = p(A_2)\cdot(\omega_{p'}(SL_6(q))\cup\omega_{p'}(SU_6(q)))$;

3) $\upsilon(A_3) = p(A_3)\cdot(\omega_{p'}(SL_4(q)\times SL_2(q))\cup\omega_{p'}(SU_4(q)\times SL_2(q)))$;

4) $\upsilon(2A_1) = p(A_1)\cdot(\omega_{p'}(Spin^+_8(q)\times SL_2(q))\cup\omega_{p'}(Spin^-_8(q)\times SL_2(q)))$;

5) $\upsilon((3A_1)_1) = p(A_1)\cdot(\omega_{p'}(Spin^+_8(q)\times d)\cup\omega_{p'}(Spin^-_8(q)\times d)\cup\omega_{p'}({}^3D_4(q)\times d))$;

6) $\upsilon((3A_1)_2) = p(A_1)\cdot(\omega_{p'}(SL_2(q)^4)\cup\omega_{p'}(SL_2(q^2)\times SL_2(q)^2)\cup\omega_{p'}(SL_2(q^3)\times SL_2(q)))$;

7) $\upsilon((4A_1)_1) = p(A_1)\cdot(\omega_{p'}(SL_2(q)^3\times d)\cup\omega_{p'}(SL_2(q^2)\times SL_2(q)\times d)\cup\omega_{p'}(SL_2(q^3)\times d))$;

8) $\upsilon((4A_1)_2) = p(A_1)\cdot(\omega_{p'}(SL_2(q)^3\times d)\cup\omega_{p'}(SL_2(q^2)\times SL_2(q)\times d)\cup\omega_{p'}(SL_2(q^3)\times d))$.

Доказательство. Для каждой из указанных в предложении подсистем Ψ центр редуктивной подгруппы максимального ранга $\overline{H}$ группы $\overline{G}$ представляется в виде прямого произведения подгрупп $\overline{M}$ и $\overline{S}$, где $\overline{M} = 1$ или $\overline{M} = Z$, а $\overline{S}$ — это тор, порожденный элементами $h_r(t)$, где r пробегает ортогональное дополнение $\Psi^\perp$ к подсистеме Ψ в системе E_7. Обозначим через $\overline{K}$ — подгруппу группы $\overline{G}$, порожденную корневыми подгруппами, соответствующими корням из $\Psi^\perp$. Во всех случаях фундаментальная подсистема системы $\Psi^\perp$ может быть выбрана как подмножество фундаментальной системы группы $\overline{G}$. Таким образом, из [55, предложение 2.6.2 (d)] следует, что $\overline{K}$ — это односвязная группа. Поскольку подсистема $\Psi^\perp$ инвариантна относительно действия $N_W(W_1)$, произвольный элемент $w \in N_W(W_1)$ индуцирует на группе $\overline{K}$ некоторый автоморфизм, являющийся композицией графового автоморфизма и автоморфизма индуцированного элементом группы Вейля системы $\Psi^\perp$. Таким образом, центр группы $\overline{H}_{\sigma\circ w}$ изоморфен $\overline{M}_{\sigma\circ w}\times\overline{S}_{\sigma\circ w}$, где $\overline{S}_{\sigma\circ w}$ — максимальный тор группы $\overline{K}_{\sigma\circ\tau}$ для некоторого графового автоморфизма группы $\overline{K}$. Таким образом, для доказательства предложения необходимо определить, какие автоморфизмы подсистем $\Psi^\perp$ содержатся в группе W. Группы автоморфизмов подсистем $\Psi^\perp$ мы определили с помощью системы MAGMA. В частности, мы получили, что группа автоморфизмов подсистемы $\Psi^\perp$, индуцированных группой W, отлична от полной группы автоморфизмов только в случаях $\Psi^\perp = D_6$, $2A_1$, $(3A_1)_2$. Пусть $\Psi = k\Psi_1$ для неприводимой

подсистемы Ψ_1, и w — элемент группы $N_W(W_1)$, переставляющий подсистемы Ψ_1 по циклу. Пусть $\overline{K}_1$ — подсистемная подгруппа группы $\overline{K}$, соответствующая Ψ_1. Пусть $x \in \overline{K}$, тогда $x = x_1 x_2 \dots x_k$, где $x_i \in \overline{K}_1^{w^{i-1}}$. Имеем $x \in \overline{K}$ тогда и только тогда, когда $x_i^\sigma = x_{i+1}$, где $x_{k+1} = x_1$. Отсюда следует, что $x_1^{\sigma^k} = x_1$ и группа $\overline{K}_{\sigma\circ w}$ изоморфна $(\overline{K}_1)_{\sigma^k}$, что завершает доказательство предложения. □

Следствие 2.4.4. *Имеют место следующие равенства.*

1) $\nu(A_1) = p(A_1) \cdot \omega_{p'}(Spin_{12}^+(q))$;

2) $\nu(A_2) = p(A_2) \cdot (\omega_{p'}(SL_6(q)/Z) \cup \omega_{p'}(SU_6(q)/Z))$;

3) $\nu(A_3) = p(A_3) \cdot (\omega_{p'}((SL_4(q) \times SL_2(q))) \cup \omega_{p'}((SU_4(q) \times SL_2(q))))$;

4) $\nu(2A_1) = p(A_1) \cdot (\omega_{p'}(Spin_8^+(q) \times SL_2(q)) \cup \omega_{p'}(Spin_8^-(q) \times SL_2(q)))$;

5) $\nu((3A_1)_1) = p(A_1) \cdot (\omega_{p'}(Spin_8^+(q)) \cup \omega_{p'}(Spin_8^-(q)) \cup \omega_{p'}({}^3D_4(q)))$;

6) $\nu((3A_1)_2) = p(A_1) \cdot (\omega_{p'}(SL_2(q)^4) \cup \omega_{p'}(SL_2(q^2) \times SL_2(q)^2) \cup \omega_{p'}(PSL_2(q^3) \times SL_2(q)))$;

7) $\nu((4A_1)_1) = p(A_1) \cdot (\omega_{p'}(SL_2(q)^3) \cup \omega_{p'}(SL_2(q^2) \times SL_2(q)) \cup \omega_{p'}(SL_2(q^3)))$;

8) $\nu((4A_1)_2) = p(A_1) \cdot (\omega_{p'}(SL_2(q)^3 \times d) \cup \omega_{p'}(SL_2(q^2) \times SL_2(q) \times d) \cup \omega_{p'}(PSL_2(q^3) \times d))$.

Доказательство. При доказательстве мы будем использовать обозначения, введенные в доказательстве предыдущего предложения. В пунктах 1) и 2) подгруппа $\overline{K}_{\sigma\circ\tau}$ содержит центр редуктивной подгруппы, а значит, и центр группы G. Это доказывает 2), и 1) теперь следует из леммы 2.4.2.

В остальных случаях полезно следующее простое замечание. Пусть A, B — конечные группы и N — нормальная подгруппа группы $A \times B$ такая, что $A \cap N = B \cap N = 1$. Тогда спектр группы $A \times B$ совпадает со спектром ее фактор-группы по N. Например, в 3) группа $\overline{K}$ порождается элементами $x_{\pm r_2}(t)$, $x_{\pm r_5}(t)$, $x_{\pm r_6}(t)$, $x_{\pm r_7}(t)$, таким образом, группа $\overline{K}_{\sigma\circ\tau}$ есть прямое произведение подгрупп, каждая из которых пересекается с центром по единице. В 4) прямой множитель $SL_2(q)$, порождается $x_{\pm r_2}(t)$. В случаях 5) и 7) группа $\overline{M}_{\sigma\circ w}$ равна Z. В 6) в случаях $K_{\sigma\circ\tau} \simeq SL_2(q)^4$ или $SL_2(q^2) \times SL_2(q)^2$ спектр не может измениться при факторизации, поскольку каждый из прямых сомножителей содержит не более двух корневых подгрупп, соответствующих фундаментальным корням. Случай $K_{\sigma\circ\tau} \simeq SL_2(q^3) \times SL_2(q)$ соответствует элементу группы W, переставляющему по циклу корни r_2, r_5, r_7 и оставляющему корень r_3 на месте. Таким образом, множитель $SL_2(q^3)$ содержит центр группы G. Пункт 8) аналогичен пункту 6). Следствие доказано. □

Напомним, что двух множеств натуральных чисел A и B запись $A \sim B$ означает, что $\omega(A) = \omega(B)$.

Предложение 2.4.5. *Имеют место следующие равенства.*

1) $\upsilon(A_4) \sim p(A_4) \cdot \{q^2 - 1, q^3 - 1, q^3 + 1\}$,

$\nu(A_4) \sim p(A_4) \cdot \left\{q^2-1, \frac{q^3-1}{d}, \frac{q^3+1}{d}\right\}$;

2) $\upsilon((A_5)_1) \sim p(A_5) \cdot \{q^2-1, d(q^2-q+1), d(q^2+q+1)\}$,
$\nu((A_5)_1) \sim p(A_5) \cdot \{q^2-1, q^2-q+1, q^2+q+1\}$;

3) $\upsilon((A_5)_2) \sim p(A_5) \cdot \left\{\frac{q^2-1}{d}\right\}$,
$\nu((A_5)_2) \sim p(A_5) \cdot \left\{\frac{q^2-1}{d}\right\}$;

4) $\upsilon(A_6) \sim p(A_6) \cdot \{q-1, q+1\}$,
$\nu(A_6) \sim p(A_6) \cdot \left\{\frac{q-1}{d}, \frac{q+1}{d}\right\}$;

5) $\upsilon(A_7) \sim p(A_7) \cdot \{d^2\}$,
$\nu(A_7) \sim p(A_7) \cdot \{d\}$;

6) $\upsilon(D_4) \sim p(D_4) \cdot \{q^3-1, q^3+1, (q^2+1)(q+1), (q^2+1)(q-1), q^2-1\}$,
$\nu(D_4) \sim p(D_4) \cdot \left\{\frac{q^3-1}{d}, \frac{q^3+1}{d}, \frac{(q^2+1)(q+1)}{d}, \frac{(q^2+1)(q-1)}{d}, q^2-1\right\}$;

7) $\upsilon(D_5) \sim p(D_5) \cdot \left\{\frac{q^2-1}{d}\right\}$,
$\nu(D_5) \sim p(D_5) \cdot \left\{\frac{q^2-1}{d}\right\}$;

8) $\upsilon(D_6) \sim p(D_6) \cdot \{q-1, q+1\}$,
$\nu(D_6) \sim p(D_6) \cdot \{q-1, q+1\}$;

9) $\upsilon(E_6) \sim p(E_6) \cdot \{q-1, q+1\}$,
$\nu(E_6) \sim p(E_6) \cdot \left\{\frac{q-1}{d}, \frac{q+1}{d}\right\}$;

10) $\upsilon(2A_2) \sim p(A_2) \cdot \{q^2-1, (q-1)(q^2-q+1), (q+1)(q^2+q+1)\}$,
$\nu(2A_2) \sim p(A_2) \cdot \left\{q^2-1, \frac{(q-1)(q^2-q+1)}{d}, \frac{(q+1)(q^2+q+1)}{d}\right\}$;

11) $\upsilon(3A_2) \sim p(A_2) \cdot \{(q-1)(3, q-1), (q+1)(3, q+1), \}$,
$\nu(3A_2) \sim p(A_2) \cdot \left\{\frac{(q-1)(3,q-1)}{d}, \frac{(q+1)(3,q+1)}{d}, \right\}$;

12) $\upsilon(2A_3) \sim p(A_3) \cdot \left\{\frac{(q-1)(4,q-1)}{d}, \frac{(q+1)(4,q+1)}{d}\right\}$,
$\nu(2A_3) \sim p(A_3) \cdot \left\{\frac{(q-1)(4,q-1)}{d}, \frac{(q+1)(4,q+1)}{d}\right\}$.

Доказательство. Это утверждение получено с помощью вычислений в MAGMA. Опишем схему этих вычислений. Для каждого множества корней Π из таблицы 13 определяется группа $N_W(\Pi)$. Затем из каждого класса сопряженности группы $N_W(\Pi)$ выбирается представитель w и составляется матрица $M_w = qw - 1$ (напомним, что в случае, когда подсистема, порожденная корнями из Π, имеет вид $k\Psi_1$ для некоторой неприводимой подсистемы Ψ_1, элемент w должен действовать на $k\Psi_1$, переставляя прямые слагаемые по циклу). При этом столбцы матрицы M_w задают соотношения группы $\overline{T}_{\sigma\circ w}$. Имеем

$Z(\overline{H}_{\sigma\circ w}) = Z(\overline{H})_{\sigma\circ w} = \overline{T}_{\sigma\circ w} \cap Z(\overline{H})$. Таким образом, для нахождения центра группы $\overline{H}_{\sigma\circ w}$ необходимо к соотношениям, задаваемым столбцами матрицы M_w, добавить соотношения из третьего столбца таблицы 13.

Приведем в качестве примера вычисления для системы A_4. Для системы A_4 есть два случая, когда центр группы $\overline{H}_{\sigma\circ w}$ циклический и имеет порядок q^3-1 или q^3+1. В остальных случаях период центра группы $\overline{H}_{\sigma\circ w}$ делит q^2-1. Таким образом, верно первое утверждение пункта (1), и для доказательства второго требуется показать, что существует редуктивная подгруппа с центром периода q^2-1 такая, что период центра не меняется при переходе к простой группе. Пусть

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

После преобразований и исключения параметров t_1, t_3, t_4 и t_5 из матрицы $qw-1$ получаем матрицу

$$\begin{pmatrix} q-1 & -q & -q \\ 0 & -1 & -q \\ 0 & -q & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -q-1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & q-1 & 0 \\ 0 & 0 & q^2-1 \end{pmatrix} \begin{pmatrix} -1 & 0 & -q \\ -1 & 1 & -q \\ 0 & -1 & 1 \end{pmatrix}.$$

Следовательно, элементы центра в этом случае задаются двумя параметрами s_1 и s_2, причем $s_1^{q-1}=1$ и $s_2^{q^2-1}=1$. Более точно, имеем $t_2 = s_1^{-1}s_2^{-q-1} = t_5^{-1}$, $t_6 = s_1 s_2$, $t_7 = s_2$. Таким образом, группа $\overline{T}_{\sigma\circ w}$ содержит циклическую подгруппу порядка q^2-1, состоящую из элементов вида $h_{r_2}(s_2^{-q-1})h_{r_5}(s_2^{q+1})h_{r_6}(s_2)h_{r_7}(s_2)$, которая тривиально пересекается с центром группы G. Предложение доказано. □

Теорема 13 теперь непосредственно следует из предложений 2.4.3, 2.4.5, описания максимальных торов в спинорных группах (см. [15, теорема 1]), в группах ${}^3D_4(q)$ (см. [48, предложение 1.2]) и в линейных и унитарных группах (см. [3]).

Теорема 12 следует из следствия 2.4.4 и предложения 2.4.5.

§ 2.5. Смешанная часть спектра групп $E_8(q)$

Пусть $\overline{G}$ — это группа лиева типа E_8 над алгебраическим замыканием поля Галуа F_p для некоторого простого числа p. Пусть σ — это отображение Фробениуса группы $\overline{G}$, переводящее корневой элемент $x_r(t)$ в $x_r(t^q)$. Обозначим через G группу $\overline{G}_\sigma$ Как и ранее, через r_0 будем обозначать корень максимальной высоты.

В таблице 14 указаны все собственные аддитивно замкнутые подсистемы системы E_8 с изоморфными неразложимыми компонентами с точностью до эквивалентности от-

Таблица 14. Подсистемы системы E_8

Ψ	$\Psi^\perp$	Ψ	$\Psi^\perp$	Ψ	$\Psi^\perp$	Ψ	$\Psi^\perp$	Ψ	$\Psi^\perp$	Ψ	$\Psi^\perp$
A_1	E_7	A_6	A_1	D_5	A_3	E_7	A_1	$5A_1$	$3A_1$	$3A_2$	A_2
A_2	E_6	$(A_7)_1$	A_1	D_6	$2A_1$	$2A_1$	D_6	$6A_1$	$2A_1$	$4A_2$	$\varnothing$
A_3	D_5	$(A_7)_2$	$\varnothing$	D_7	$\varnothing$	$3A_1$	$D_4 + A_1$	$7A_1$	A_1	$(2A_3)_1$	$2A_1$
A_4	A_4	A_8	$\varnothing$	D_8	$\varnothing$	$(4A_1)_1$	D_4	$8A_1$	$\varnothing$	$(2A_3)_2$	$\varnothing$
A_5	$A_2 + A_1$	D_4	D_4	E_6	A_2	$(4A_1)_2$	$4A_1$	$2A_2$	$2A_2$	$2A_4$	$\varnothing$
										$2D_4$	$\varnothing$

носительно действия группы W, а также ортогональные дополнения к этим подсистемам (см. [45, таблица 2] или [14, таблица 111]).

Лемма 2.5.1. *Пусть H — редуктивная подгруппа максимального ранга группы G с системой корней типа $6A_1$, $7A_1$, $8A_1$, $4A_2$, $2D_4$. Тогда существует редуктивная подгруппа максимального ранга H_1 группы G с системой корней, отличной от перечисленных, такая, что $\eta(H)$ делит $\eta(H_1)$.*

Доказательство. Пусть s — это элемент центра группы H порядка, совпадающего с периодом центра. Положим $\overline{H}_1 = C_{\overline{G}}(s)$. По [46, предложение 2.3.4] система корней группы $\overline{H}_1$ отлична от $6A_1$, $7A_1$, $8A_1$, $4A_2$, $2D_4$. Очевидно, $H \subseteq \overline{H}_1$. Таким образом, $H \subseteq H_1 = (\overline{H}_1)_\sigma$ и, следовательно, $\eta(H)$ делит $\eta(H_1)$. □

Из леммы 2.5.1 следует, что указанные в ней системы можно не рассматривать при описании спектра группы G.

Как уже отмечалось выше, полупростая и унипотентная части спектров рассматриваемых групп известны. Описание смешанной части спектра проводится по той же схеме, что и предыдущих параграфах.

В таблице 15 через Π обозначена фундаментальная система корней подсистемы Ψ, при этом

$$r_9 = (2, 2, 3, 4, 3, 2, 1, 0),$$

$$r_{10} = (1, 1, 2, 3, 2, 1, 0, 0),$$

$$r_{11} = (1, 1, 2, 2, 1, 0, 0, 0),$$

$$r_{12} = (-2, -2, -3, -4, -3, -2, -1, 0),$$

$$r_{13} = (0, -1, -1, -2, -2, -2, -1, 0),$$

$$r_{14} = (0, -1, -1, -2, -1, 0, 0, 0),$$

$$r_{15} = (-1, -2, -2, -3, -2, -1, 0, 0).$$

В третьем столбце указаны необходимые и достаточные условия того, что элемент $\prod_{i=1\ldots8} h_{r_i}(t_i)$ лежит в центре редуктивной подгруппы максимального ранга группы $\overline{G}$, содержащей тор $\overline{T}$ и имеющей систему корней Ψ.

Таблица 15. Центры редуктивных подгрупп в E_8

Ψ	Π	Центр
A_1	$-r_0$	$t_8 = 1$
A_2	$-r_0$, r_8	$t_7 = t_8 = 1$
A_3	$-r_0$, r_7, r_8	$t_6 = t_7 = t_8 = 1$
A_4	$-r_0$, r_6, r_7, r_8	$t_5 = t_6 = t_7 = t_8 = 1$
A_5	$-r_0$, r_5, r_6, r_7, r_8	$t_4 = t_5 = t_6 = t_7 = t_8 = 1$
A_6	$-r_0$, r_4, r_5, r_6, r_7, r_8	$t_4 = t_5 = t_6 = t_7 = t_8 = 1$, $t_2 = t_3^{-1}$
$(A_7)_1$	$-r_0$, r_2, r_4, r_5, r_6, r_7, r_8	$t_4 = t_5 = t_6 = t_7 = t_8 = 1$, $t_3 = t_2^{-1}$, $t_2^2 = 1$
$(A_7)_2$	$-r_0$, r_3, r_4, r_5, r_6, r_7, r_8	$t_4 = t_5 = t_6 = t_7 = t_8 = 1$, $t_2 = t_3^{-1}$, $t_1 = t_3^2$
A_8	$-r_0$, r_1, r_3, r_4, r_5, r_6, r_7, r_8	$t_4 = t_5 = t_6 = t_7 = t_8 = 1$, $t_2 = t_3^{-1}$, $t_1 = t_3^2$, $t_3^3 = 1$
D_4	$-r_0$, r_7, r_8, r_9	$t_1 = t_6 = t_7 = t_8 = 1$
D_5	$-r_0$, r_6, r_7, r_8, r_9	$t_1 = t_5 = t_6 = t_7 = t_8 = 1$
D_6	$-r_0$, r_5, r_6, r_7, r_8, r_9	$t_1 = t_4 = t_5 = t_6 = t_7 = t_8 = 1$
D_7	$-r_0$, r_4, r_5, r_6, r_7, r_8, r_9	$t_1 = t_4 = t_5 = t_6 = t_7 = t_8 = 1$, $t_2 = t_3^{-1}$
D_8	$-r_0$, r_4, r_5, r_6, r_7, r_8, r_9	$t_1 = t_4 = t_5 = t_6 = t_7 = t_8 = 1$, $t_2 = t_3^{-1}$, $t_3^2 = 1$
E_6	$-r_0$, r_5, r_6, r_7, r_8, r_{10}	$t_2 = t_4 = t_5 = t_6 = t_7 = t_8 = 1$
E_7	$-r_0$, r_4, r_5, r_6, r_7, r_8, r_{11}	$t_2 = t_3 = t_4 = t_5 = t_6 = t_7 = t_8 = 1$
$2A_1$	$-r_0$, r_{12}	$t_1 = t_8 = 1$
$3A_1$	$-r_0$, r_{12}, r_{13}	$t_1 = t_6 = t_8 = 1$
$(4A_1)_1$	$-r_0$, r_7, r_{12}, r_{13}	$t_1 = t_6 = t_8 = 1$, $t_7^2 = 1$
$(4A_1)_2$	$-r_0$, r_{12}, r_{13}, r_{14}	$t_1 = t_4 = t_6 = t_8 = 1$
$5A_1$	$-r_0$, r_7, r_{12}, r_{13}, r_{14}	$t_1 = t_4 = t_6 = t_8 = 1$, $t_7^2 = 1$
$2A_2$	$-r_0$, r_2, r_8, r_{15}	$t_2 = t_4 = t_7 = t_8 = 1$
$3A_2$	$-r_0$, r_1, r_2, r_3, r_8, r_{15}	$t_2 = t_4 = t_7 = t_8 = 1$, $t_3 = t_1^2$, $t_1^3 = 1$
$(2A_3)_1$	$-r_0$, r_1, r_3, r_7, r_8, $-r_{11}$	$t_3 = t_6 = t_7 = t_8 = 1$, $t_4 = t_1^{-1}$, $t_1^2 = 1$
$(2A_3)_2$	$-r_0$, r_3, r_4, r_7, r_8, $-r_{11}$	$t_3 = t_6 = t_7 = t_8 = 1$, $t_4 = t_1^{-1}$, $t_5 = t_1^{-2}t_2^{-1}$
$2A_4$	$-r_0$, r_1, r_2, r_3, r_4, r_6, r_7, r_8	$t_5 = t_6 = t_7 = t_8 = 1$, $t_3 = t_1^2$, $t_4 = t_1^3$, $t_2 = t_1^4$,

Обозначим через $\upsilon(\Psi)$ множество всех $\eta(H)$, где H пробегает все редуктивные группы максимального ранга группы G с системой корней Ψ.

Предложение 2.5.2. *Имеют место следующие равенства.*

1) $\upsilon(A_1) = p(A_1) \cdot \omega_{p'}(E_7(q))$;

2) $\upsilon(A_2) = p(A_2) \cdot (\omega_{p'}(E_6(q)) \cup \omega_{p'}({}^2E_6(q)))$;

3) $\upsilon(A_3) = p(A_3) \cdot \big(\omega_{p'}(Spin_{10}^+(q)) \cup \omega_{p'}(Spin_{10}^-(q))\big)$;

4) $\upsilon(A_4) = p(A_4) \cdot (\omega_{p'}(SL_5(q)) \cup \omega_{p'}(SU_5(q)))$;

5) $\upsilon(A_5) = p(A_5) \cdot (\omega_{p'}(SL_3(q) \times SL_2(q)) \cup \omega_{p'}(SU_3(q) \times SL_2(q)))$;

6) $\upsilon(D_4) = p(D_4) \cdot \big(\omega_{p'}(Spin_8^+(q)) \cup \omega_{p'}(Spin_8^-(q)) \cup \omega_{p'}({}^3D_4(q))\big)$;

7) $\upsilon(D_5) = p(D_5) \cdot (\omega_{p'}(SL_4(q)) \cup \omega_{p'}(SU_4(q)))$;

8) $\upsilon(D_6) = p(D_6) \cdot (\omega_{p'}(SL_2(q)^2) \cup \omega_{p'}(SL_2(q^2)))$;

9) $\upsilon(2A_1) = p(A_1) \cdot (\omega_{p'}(Spin_{12}^+(q)) \cup \omega_{p'}(Spin_{12}^-(q)))$;

10) $\upsilon(3A_1) = p(A_1) \cdot (\omega_{p'}(Spin_8^+(q) \times SL_2(q)) \cup \omega_{p'}(Spin_8^-(q) \times SL_2(q)) \cup \omega_{p'}({}^3D_4(q) \times SL_2(q)))$;

11) $\upsilon((4A_1)_1) = p(A_1) \cdot (\omega_{p'}(Spin_8^+(q) \times 2) \cup \omega_{p'}(Spin_8^-(q) \times 2) \cup \omega_{p'}({}^3D_4(q) \times 2))$;

12) $\upsilon((4A_1)_2) = p(A_1) \cdot (\omega_{p'}(SL_2(q)^4) \cup \omega_{p'}(SL_2(q^2) \times SL_2(q)^2) \cup \omega_{p'}(SL_2(q^3) \times SL_2(q)) \cup \omega_{p'}(SL_2(q^4)))$;

13) $\upsilon(5A_1) = p(A_1) \cdot (\omega_{p'}(SL_2(q)^3 \times 2) \cup \omega_{p'}(SL_2(q^2) \times SL_2(q) \times 2) \cup \omega_{p'}(SL_2(q^3) \times 2))$;

14) $\upsilon(2A_2) = p(A_2) \cdot (\omega_{p'}(SL_3(q)^2) \cup \omega_{p'}(SU_3(q)^2) \cup \omega_{p'}(SL_3(q) \times SU_3(q)) \cup \omega_{p'}(SL_3(q^2)) \cup \omega_{p'}(SU_3(q^2)))$;

15) $\upsilon(3A_2) = p(A_2) \cdot (\omega_{p'}(SL_3(q) \times 3) \cup \omega_{p'}(SU_3(q) \times 3))$;

16) $\upsilon(2A_4) = p(A_4) \cdot \{5_{p'}\}$;

17) $\upsilon(E_6) = p(E_6) \cdot (\omega_{p'}(SL_3(q)) \cup \omega_{p'}(SU_3(q)))$;

18) $\upsilon(E_7) = p(E_7) \cdot \omega_{p'}(SL_2(q))$.

Доказательство. Пусть Ψ — это одна из подсистем, указанных в предложении. Обозначим через $\overline{H}$ редуктивную подгруппу максимального ранга группы $\overline{G}$ с корневой системой Ψ. Обозначим через $\Psi^\perp$ ортогональное дополнение к подсистеме Ψ в системе E_8, а через $\overline{K}$ — подгруппу группы $\overline{G}$, порожденную корневыми подгруппами, соответствующими корням из $\Psi^\perp$. Во всех случаях фундаментальная подсистема системы $\Psi^\perp$ может быть выбрана как подмножество фундаментальной системы группы $\overline{G}$. Таким образом, из [55, предложение 2.6.2 (d)] следует, что $\overline{K}$ — это односвязная группа. Во всех указанных случаях, за исключением пунктов 11), 13), 15), 16), центр группы $\overline{H}$ является максимальным тором подгруппы $\overline{K}$. Таким образом, для вычисления возможных периодов групп $Z(\overline{H}_{\sigma\circ w})$ достаточно понять, какие графовые автоморфизмы группы $\overline{K}$ индуцируются группой $N_W(W_1)$, где W_1 — это группа Вейля подсистемы Ψ. Соответствующие вычисления были проведены в системе MAGMA.

В пунктах 11), 13), 15) центр группы $\overline{H}$ является прямым произведением максимального тора группы $\overline{K}$ и некоторой циклической группы C. Например, в случае 11) группа C состоит из элементов $h_{r_7}(t_7)$, где $t_7^2 = 1$. Таким образом, центр группы $H_{\sigma\circ w}$ в этих случаях является прямым произведением максимального тора группы $\overline{K}_{\sigma\circ\tau\circ w_1}$ для подходящего графового автоморфизма τ группы $\overline{K}$ и w_1 из группы Вейля группы $\overline{K}$ и группы

неподвижным точек $C_{\sigma\circ w}$. Непосредственные вычисления показывают, что в этих случаях w всегда можно выбрать так, чтобы группа $C_{\sigma\circ w}$ совпадала с C.

В случае 16) центр группы $\overline{H}$ состоит из элементов $h_{r_1}(t_1)h_{r_2}(t_1^4)h_{r_3}(t_1^2)h_{r_4}(t_1^3)$, где $t_1^5 = 1$. Вычисления в MAGMA показывают, в зависимости от выбора элемента w элементы группы $Z(\overline{H}_{\sigma\circ w})$ должны удовлетворять одному из соотношений: $t_1^{q-1} = 1$, $t_1^{q+1} = 1$ или $t_1^{q^2+1} = 1$. Предложение доказано. □

Предложение 2.5.3. *Имеют место следующие равенства.*

1) $\upsilon(A_6) \sim p(A_6) \cdot \{q^2 - 1\}$,

2) $\upsilon((A_7)_1) \sim p(A_7) \cdot \{(q-1)(2, q-1), (q+1)(2, q-1)\}$,

3) $\upsilon((A_7)_2) \sim p(A_7) \cdot \{q - 1, q + 1\}$,

4) $\upsilon(A_8) \sim p(A_8) \cdot \{(3, q^2 - 1)\}$,

5) $\upsilon(D_7) \sim p(D_7) \cdot \{q - 1, q + 1\}$,

6) $\upsilon(D_8) \sim p(D_8) \cdot \{(2, q - 1)\}$,

7) $\upsilon((2A_3)_1) \sim p(A_3) \cdot \{(2, q-1)(q^2 - 1)\}$,

8) $\upsilon((2A_3)_1) \sim p(A_3) \cdot \{q^2 - 1, q^2 + 1\}$.

Доказательство. Это утверждение получено с помощью вычислений в MAGMA. Схема вычислений описана в предложении 2.5.3. □

Теорема 14 теперь непосредственно следует из предложений 2.5.2, 2.5.3, описания максимальных торов в спинорных группах (см. [15, теорема 1]), в группах ${}^3D_4(q)$ (см. [48, предложение 1.2]) и в линейных и унитарных группах (см. [3]).

3. Алгоритм распознавания конечной простой группы по спектру

Для данного множества $\mathcal{M}$ натуральных чисел обозначим через $\mu(\mathcal{M})$ множество всех элементов из $\mathcal{M}$, которые максимальны относительно делимости. В этой главе нам будет удобно использовать следующую терминологию, множество $\omega(\mathcal{M})$ мы будем называть *(полным) спектром* множества $\mathcal{M}$, а $\mu(\mathcal{M})$ — *минимальным спектром*.

Для конечной группы G назовем конечное множество натуральных чисел $\mathcal{M}$ *почти G-спектральным*, если $\mathcal{M} \subseteq \omega(G)$ и $\omega(\mathcal{M}) \neq \omega(H)$ для любой простой группы H, чей спектр отличается от спектра группы G. Для конечного множества натуральных чисел $\mathcal{M}$ обозначим через $\Omega(\mathcal{M})$ множество неабелевых простых групп G таких, что множество $\mathcal{M}$ почти G-спектрально. Если $\omega(\mathcal{M}) = \omega(G)$ для некоторой неабелевой простой группы G, то множество $\Omega(\mathcal{M})$ либо состоит из одного элемента, либо совпадает с одним из множеств $\{O_8^+(2), S_6(2)\}$, $\{O_8^+(3), O_7(3)\}$ [4]. Если такой простой группы нет, то мощность множества $\Omega(\mathcal{M})$ может принимать различные значения (например, если $\mathcal{M} = \{2\}$, то $\Omega(\mathcal{M})$ состоит из всех неабелевых простых групп).

Следующая теорема является основным результатом данной главы.

Теорема 15. *Пусть $\mathcal{M}$ — конечное множество натуральных чисел, $m = |\mathcal{M}|$ и $M = \max \mathcal{M}$. Тогда существует алгоритм, который, получая на вход множество $\mathcal{M}$, выдает либо группу из $\Omega(\mathcal{M})$, либо пустое множество. В последнем случае не существует конечной неабелевой группы H такой, что $\omega(H) = \omega(\mathcal{M})$. Время работы алгоритма ограничено полиномом от $m \log M$.*

Говоря «выдает группу G», мы имеем ввиду, что алгоритм выдает «имя» группы G в соответствии с классификацией конечных простых групп (CFSG), т.е. название спорадической группы, степень знакопеременной группы, и тип, ранг и порядок поля определения группы лиева типа.

В силу теоремы 15, если заранее известно, что множество $\mathcal{M}$ является спектром некоторой конечной простой группы G, то группа G может быть определена за полиномиальное время (или одна из двух групп с одинаковым спектром из $\Omega(\mathcal{M})$, если $\Omega(\mathcal{M})$ состоит из двух элементов).

Даже если $\mathcal{M}$ — произвольное конечное множество натуральных чисел, то алгоритм все равно выдает единственного кандидата для G. Для завершения «распознавания» требуется вычислить множество $\mu(G)$, причем способом, позволяющим сравнивать его с $\mu(\mathcal{M})$ (т.е., требуется процедура, которая позволяет вовремя «понять», что множество $\mu(G)$ слишком большое). К сожалению, имеющееся описание спектров конечных простых групп лиева типа не позволяет очевидным образом сделать это за время, поли-

номиально зависящее от $m \log M$.

§ 3.1. Обозначения и предварительные результаты

Следующее утверждение элементарно.

Лемма 3.1.1. *Пусть a, s, t — целые числа и $|a| > 1$, $s, t > 0$. Тогда*

(1) $(a^s - 1, a^t - 1) = a^{(s,t)} - 1$;

(2) $(a^s + 1, a^t - 1) = \begin{cases} a^{(s,t)} + 1, & \text{если число } \frac{s}{(s,t)} \text{ нечетно и } \frac{t}{(s,t)} \text{ четно,} \\ (2, a - 1) & \text{в противном случае;} \end{cases}$

(3) $(a^s + 1, a^t + 1) = \begin{cases} a^{(s,t)} + 1, & \text{если } \frac{s}{(s,t)} \text{ и } \frac{t}{(s,t)} \text{ нечетны,} \\ (2, a - 1) & \text{в противном случае.} \end{cases}$

Пусть r — ненулевое целое число и ν — множество ненулевых целых чисел. Через $\pi(\nu)$ обозначается множество всех простых делителей чисел из ν. Через $(r)_\nu$ обозначается ν-часть числа r, т. е. наибольший положительный делитель d числа r такой, что $\pi(\{d\}) \subseteq \pi(\nu)$. Кроме того, ν'-часть $(r)_{\nu'}$ числа r — это число $|r|/(r)_\nu$. Если ν состоит из одного элемента n, то мы используем краткие обозначения $\pi(n)$, $(r)_n$ и $(r)_{n'}$.

Для вещественного числа x обозначим через $\lfloor x \rfloor$ целую часть числа x, т. е. наибольшее целое число, не превосходящее x.

Пусть a — целое число и $|a| > 1$. Простое число r называется *примитивным простым делителем* числа $a^i - 1$, если r делит $a^i - 1$ и не делит $a^j - 1$ для $j < i$. Обозначим через $r_i(a)$ некоторый примитивный простой делитель числа $a^i - 1$, если он существует, и через $R_i(a)$ — множество всех таких делителей. К. Жигмонди [89] показал, что примитивные простые делители существуют для почти всех пар (a, i).

Лемма 3.1.2. *Пусть a и i — целые числа и $|a| > 1$, $i > 0$. Тогда существует примитивный простой делитель $r_i(a)$ за исключением следующих случаев:*

(1) $(a, i) = (2, 1)$;

(2) $(a, i) = (2, 6)$;

(3) $(a, i) = (2^l - 1, 2)$ *для некоторого* $l \geqslant 2$;

(4) $(a, i) = (-2, 3)$;

(5) $(a, i) = (-2^l - 1, 2)$ *для некоторого* $l \geqslant 0$.

Положим $\Phi_i^*(a) = (a^i - 1)_{R_i(a)}$ (это определение эквивалентно определению числа $\Phi_i^*(a)$ в [52]). Число $\Phi_i^*(a)$ будем называть *наибольшим примитивным делителем* числа $a^i - 1$.

Поскольку мы несколько раз цитируем работы [7, 84], заметим, что определение примитивного простого делителя, а следовательно, и наибольшего примитивного делителя немного отличаются от определений в этих статьях. Согласно нашему определению число 2 может содержаться только в $R_1(a)$, в то время как в [7, 84] оно является примитивным делителем числа $a^2 - 1$, если a сравнимо с -1 по модулю 4. В остальном определения совпадают.

Лемма 3.1.3. *Пусть p — простое число, q — степень числа p, а n и A — натураль-*

ные числа. Существует алгоритм, который проверяет найдутся ли неотрицательное целое число m и натуральные числа $n_1, \ldots, n_k$ такие, что

(1) $A = p^m[(\varepsilon q)^{n_1} - 1, \ldots, (\varepsilon q)^{n_k} - 1]$, *где* $\varepsilon = \pm 1$ *и* $\lfloor p^{m-1} \rfloor + n_1 + \cdots + n_k \leqslant n$ *или*

(2) $A = p^m[q^{n_1} - 1, \ldots, q^{n_s} - 1, q^{n_{s+1}} + 1, \ldots, q^{n_k} + 1]$ *и* $\lfloor p^{m-1} \rfloor + 2(n_1 + \cdots + n_k) \leqslant n$.

Более того, в случае (2) *алгоритм также проверяет существование требуемого представления числа A с заданной четностью числа $k - s$. Время работы алгоритма ограничено полиномом от $n \log(qA)$.*

Доказательство. Поскольку максимальная степень числа p, делящая A, определена однозначно и может быть определена за время, ограниченное полиномом от $\log(pA)$, без ограничения общности можем считать, что A является p'-числом.

Сначала мы построим алгоритм для случая (1). Пусть S обозначает множество делителей числа A вида $(\varepsilon q)^x - 1$ для натурального $x \leqslant n$. Если число A не равно наименьшему общему кратному элементов множества S, то оно не представимо в требуемом виде.

Пусть минимальный спектр $\mu(S)$ равен

$$\{(\varepsilon q)^{n_1} - 1, \ldots, (\varepsilon q)^{n_k} - 1\}.$$

Если $n_1 + \cdots + n_k \leqslant n$, то мы получили требуемое. Предположим, что равенство не выполнено и существует другое представление

$$A = [(\varepsilon q)^{l_1} - 1, \ldots, (\varepsilon q)^{l_t} - 1],$$

для которого $l_1 + \cdots + l_t \leqslant n$. Пусть $i \in \{1, \ldots, k\}$ таково, что число $(\varepsilon q)^{n_i} - 1$ имеет примитивный простой делитель $r_{n_i}(\varepsilon q)$. Поскольку число $r_{n_i}(q)$ делит A, оно должно делить одно из чисел $(\varepsilon q)^{l_j} - 1$. Из леммы 3.1.1 следует, что тогда n_i делит l_j. Значит $(\varepsilon q)^{n_i} - 1$ делит $(\varepsilon q)^{l_j} - 1$, но первое из этих чисел лежит в $\mu(S)$ и максимально относительно делимости. Следовательно, модули чисел $(\varepsilon q)^{n_i} - 1$ и $(\varepsilon q)^{l_j} - 1$ совпадают. Отсюда либо $n_i = l_j$, либо $q = 2$, $\varepsilon = -1$ и $\{n_i, l_j\} = \{1, 2\}$. В последнем случае 3 является единственным неединичным делителем числа A, и в этом случае 3 всегда представляется в виде $(-q) - 1$. Таким образом, любой элемент из $\mu(S)$, имеющий примитивный простой делитель, должен присутствовать во втором представлении. Предположим, что $(\varepsilon q)^{n_i} - 1$ не имеет примитивного простого делителя. Тогда пара $(\varepsilon q, n_i)$ указана в лемме 3.1.2. В случае (1) леммы 3.1.2 число A равно 1 и утверждение леммы тривиально. В остальных случаях существует делитель числа $(\varepsilon q)^{n_i} - 1$, который можно взять вместо $r_{n_i}(\varepsilon q)$ в предыдущем рассуждении. Если пара $(\varepsilon q, n_i)$ равна $(2, 6)$ или $(-2, 3)$, то этим делителем является 9. Если $(\varepsilon q, n_i)$ равна $(2^l - 1, 2)$ или $(-2^l - 1, 2)$, то можно взять 2-часть числа $q^2 - 1$. Отсюда заключаем, что $\{n_i, 1 \leqslant i \leqslant k\}$ — подмножество в $\{l_j, 1 \leqslant j \leqslant t\}$; противоречие.

Рассмотрим случай (2). Как и прежде, можно предполагать, что A есть наименьшее общее кратное своих делителей вида $q^x \pm 1$ для $x \leqslant n/2$ (в противном случае A не имеет желаемого вида). Пусть

$$A = [q^{n_1} - 1, \ldots, q^{n_s} - 1, q^{n_{s+1}} + 1, \ldots, q^{n_k} + 1],$$

для некоторых $n_1, \ldots, n_k$.

Можно считать, что максимум одно из чисел n_i для $i \leqslant s$ четно. Действительно, если n_i четно, то можно заменить $q^{n_i} - 1$ в представлении на два члена $q^{n_i/2} - 1$ и $q^{n_i/2} + 1$, если только эта операция не уменьшает 2-часть соответствующего наименьшего общего кратного. Таким образом, можно выбрать один элемент, делящийся на 2-часть числа A, а к остальным применить вышеуказанную операцию. Повторяя эту процедуру необходимое количество раз, получим представление с одним элементом с четной степенью и такой же суммой степеней. Также, можем считать, что никакой элемент представления не делит другой элемент.

Пусть представление числа A содержит четный член, равный $q^{2^\alpha (n_j)_{2'}} - 1$ для $\alpha > 0$. Покажем, что если мы заменим это число на набор элементов $q^{(n_j)_{2'}} - 1$, $q^{2(n_j)_{2'}} + 1$, $\ldots$, $q^{2^{\alpha-1}(n_j)_{2'}} + 1$ и удалим все элементы, которые не максимальны относительно делимости, то результат этого преобразования не зависит от исходного представления. Легко видеть, что наименьшее общее кратное получившихся чисел равно $A/2^\alpha$. Поскольку α зависит только от A и q, это наименьшее общее кратное однозначно определено. Пусть S — это множество делителей числа $A/2^\alpha$ вида $q^x - 1$ с нечетным x и $q^x + 1$, где $x \leqslant n/2$ в обоих случаях. Рассуждая аналогично случаю (1), можно показать, что представление числа $A/2^\alpha$ с наименьшей суммой степеней является наименьшим общим кратным элементов $\mu(S)$. Следовательно, можно найти требуемое представление числа A с наименьшей суммой степеней $n_1, \ldots, n_k$, используя следующую процедуру. Сначала вычисляется α. Затем строится множество S. После этого находятся те множества $\mu(\mu(S) \cup \{q^{2^\alpha y} - 1\})$ с $2^\alpha y \leqslant n$, у которых наименьшее общее кратное элементов равно A. Наконец, среди найденных выбирается множество с наименьшей суммой степеней. Это дает требуемое представление.

Что касается четности числа $k - s$, то алгоритм для случая (2) дает представление A с минимальной суммой степеней n_i. Если $k - s$ имеет требуемую четность, то ничего делать не надо. Предположим противное. Если представление имеет пару членов вида $q^x - 1$ и $q^x + 1$ таких, что число $q^{2x} - 1$ также делит A, то можно заменить эту пару на $q^{2x} - 1$, не меняя суммы степеней и меняя четность $k - s$. Если такой пары не существует и A делится на некоторое число вида $q^y + 1$, то следует выбрать минимальное y, удовлетворяющее этому условию и добавить соответствующий элемент к представлению. Если эта операция не увеличивает сумму степеней больше необходимого, то мы имеем желаемый результат. В противном случае, A не может быть представлено в требуемой форме. Наконец, если A не делится на числа вида $q^y + 1$, то $k - s$ равно нулю в любом представлении числа A. $\square$

Следуя [43], мы используем однобуквенные обозначения для простых классических групп, например, $L_n(q)$ означает $PSL_n(q)$. Мы также используем стандартное обозначение $L_n^\varepsilon(q)$, где $\varepsilon \in \{+, -\}$, при этом $L_n^+(q) = L_n(q)$ и $L_n^-(q) = U_n(q)$.

Лемма 3.1.4. [4, теорема 1] *Пусть G и H — неизоморфные конечные простые группы с $\omega(H) = \omega(G)$. Тогда либо $\{G, H\} = \{S_6(2), O_8^+(2)\}$, либо $\{G, H\} = \{O_7(3), O_8^+(3)\}$. В частности, не существует трех попарно неизоморфных простых группы с одинаковыми*

спектрами.

Напомним, что граф простых чисел (или граф Грюнберга–Кегеля) $\mathrm{GK}(G)$ конечной группы G — это граф со множеством вершин $\pi(G)$ (мы пишем $\pi(G)$ вместо $\pi(|G|)$), в котором две различные вершины p и q смежны тогда и только тогда, когда $pq \in \omega(G)$. Структура графов простых чисел конечных простых групп хорошо изучена. Например, в [7] получен критерий смежности в графе $\mathrm{GK}(G)$ для всех конечных простых групп G.

Лемма 3.1.5 является непосредственным следствием основного результата работы [16].

Лемма 3.1.5. *Пусть G — конечная простая группа. Если $\mathrm{GK}(G) = \mathrm{GK}(A_n)$ для некоторого n, то G либо является знакопеременной группой, либо одна из групп $L_2(49)$, $U_4(3)$, J_2, $S_6(2)$ и $O_8^+(2)$.*

Для классической группы G обозначим через $\mathrm{prk}(G)$ размерность группы G для линейных и унитарных групп и лиев ранг группы G для симплектических и ортогональных групп. Следуя [8], через $t(G)$ обозначим размер максимальной коклики графа $\mathrm{GK}(G)$, где G — конечная группа.

Лемма 3.1.6. *Пусть G — конечная простая классическая группа с $\mathrm{prk}(G) \geqslant 12$. Тогда значения $t(G)$ перечислены в таблице* 16.

Таблица 16. Размеры максимальных коклик

G	$t(G)$
$L_n^{\varepsilon}(q)$	$\left\lfloor \frac{n+1}{2} \right\rfloor$
$S_{2n}(q)$, $O_{2n+1}(q)$	$\left\lfloor \frac{3n+5}{4} \right\rfloor$
$O_{2n}^+(q)$, $n \not\equiv 3 (\mathrm{mod}\ 4)$	$\left\lfloor \frac{3n+1}{4} \right\rfloor$
$O_{2n}^+(q)$, $n \equiv 3 (\mathrm{mod}\ 4)$	$\frac{3n+3}{4}$
$O_{2n}^-(q)$	$\left\lfloor \frac{3n+4}{4} \right\rfloor$

Доказательство. Таблица 16 является извлечением из [8, таблицы 2, 3]. □

Лемма 3.1.7. *Пусть G — конечная простая классическая группа над полем порядка q и характеристики p с $\mathrm{prk}(G) \geqslant 8$. Определим подмножество $\zeta(G)$ множества $\mu(G)$ следующим образом: $m \in \zeta(G)$ тогда и только тогда, когда существует $r \in \pi(m)$ такое, что $pr \notin \omega(G)$. Тогда множество $\zeta(G)$ приведено в таблице* 17. *В частности, если s — это общий делитель двух различных элементов из $\zeta(G)$, то $ps \in \omega(G)$.*

Доказательство. Следует из [7, предложение 3.1] и описания спектров простых классических групп [1, 2]. □

Пусть $m_i(G)$ — это i-ый наибольший элемент множества $\omega(G)$.

Лемма 3.1.8. [69, теоремы 1.2, 1.3] *Пусть G и H — простые группы лиева типа над полями нечетных характеристик. Если $m_1(G) = m_1(H)$ и $m_2(G) = m_2(H)$, тогда выполнено одно из следующих утверждений:*

(1) *Характеристики полей определения групп G и H совпадают;*

Таблица 17. Подмножества $\zeta(G)$

G	$\zeta(G)$
$L_n(q)$	$\frac{q^n-1}{(q-1)(n,q-1)}, \frac{q^{n-1}-1}{(n,q-1)}$
$U_n(q)$	$\frac{q^n-(-1)^n}{(q+1)(n,q+1)}, \frac{q^{n-1}-(-1)^{n-1}}{(n,q+1)}$
$S_{2n}(q)$, $O_{2n+1}(q)$, n четно	$\frac{q^n+1}{(2,q-1)}$
$S_{2n}(q)$, $O_{2n+1}(q)$, n нечетно	$\frac{q^n-1}{(2,q-1)}$, $\frac{q^n+1}{(2,q-1)}$
$O^+_{2n}(q)$, n четно	$\frac{q^{n-1}-1}{(2,q-1)}$, $\frac{q^{n-1}+1}{(2,q-1)}$
$O^+_{2n}(q)$, n нечетно	$\frac{(q^{n-1}+1)(q+1)}{(4,q^n-1)}$, $\frac{q^n-1}{(4,q^n-1)}$
$O^-_{2n}(q)$, n четно	$\frac{q^n+1}{(2,q-1)}$, $\frac{(q^{n-1}+1)(q-1)}{(2,q-1)}$, $\frac{(q^{n-1}-1)(q+1)}{(2,q-1)}$
$O^-_{2n}(q)$, n нечетно	$\frac{q^n+1}{(4,q^n+1)}$, $\frac{(q^{n-1}+1)(q-1)}{(4,q^n+1)}$

(2) $\{G, H\} = \{PSL_2(q), G_2(r)\}$;

(3) *G и H являются симплектическими группами размерности не меньше* 8 *или унитарными группами размерности не меньше* 4*, определенными над простыми полями.*

Если, кроме того, $m_3(G) = m_3(H)$, то характеристики полей определения групп G и H совпадают.

Лемма 3.1.9. *Если G — простая группа лиева типа над полем порядка q, то*

$$m_1(G) \geqslant \frac{q+1}{2}.$$

Доказательство. Каждая простая группа лиева типа содержит подгруппу типа A_1, или ${}^2A_2$, или ${}^2B_2$, или ${}^2G_2$, определенную над тем же полем (см. [55, предложение 2.6.2]). Поскольку $\frac{q+1}{(2,q-1)} \in \omega(PSL_2(q))$, $q+1 \in \omega(PSU_3(q))$, $q+\sqrt{2q}+1 \in \omega({}^2B_2(q))$, $\frac{q+1}{2} \in \omega({}^2G_2(q))$, лемма доказана. □

Лемма 3.1.10. *Существует функция $f : \mathbb{N} \to \mathbb{N}$ такая, что если G — простая группа лиева типа лиева ранга k над полем порядка q, то спектр группы G содержит подмножество $\nu(G)$, удовлетворяющее следующим условиям:*

(1) $\mu(G) \subseteq \nu(G)$;

(2) $|\nu(G)| \leqslant f(k)$;

(3) *каждый элемент из $\nu(G)$ может быть вычислен за время, ограниченное полиномом от $k \log q$.*

В частности, если лиев тип и лиев ранг группы G зафиксированы, то минимальный спектр группы G может быть найден за время, полиномиально зависящее от $\log q$.

Доказательство. Утверждение леммы напрямую следует из описания спектров конечных простых групп лиева типа (см. [2, 92] и ссылки в них, а также результаты предыдущей главы). □

Из леммы 3.1.10 также следует, что мощность множества $\mu(G)$ также ограничена функцией от лиева ранга группы G.

Идея доказательства следующей леммы взята из [19, лемма 2].

Лемма 3.1.11. *Существует алгоритм, который для любого целого $n > 1$ находит элемент из $\omega(A_{n+1}) \setminus \omega(A_n)$ за время, ограниченное полиномом от n.*

Доказательство. Положим $a_7 = 7$, $a_6 = 4$, $a_5 = 5$, $a_4 = 2$, $a_3 = 3$. Легко видеть, что a_i лежит в $\omega(A_i) \setminus \omega(A_{i-1})$. Значит утверждение для $n \leqslant 6$ доказано.

Пусть $n > 6$. Сначала мы используем решето Эратосфена, чтобы получить список всех простых чисел, не превосходящих n. Согласно теореме Бертрана–Чебышева, существует простое число p_1, удовлетворяющее $\frac{n}{2} < p_1 \leqslant n - 2$. Положим $\sigma_1 = p_1$. Определим p_i и σ_i для $i > 1$ следующим образом: p_i — это простое число, удовлетворяющее

$$\frac{n - \sigma_{i-1}}{2} < p_i \leqslant n - \sigma_{i-1} - 2,$$

и $\sigma_i = \sigma_{i-1} + p_i$. Пусть s — максимальный индекс, для которого число p_s определено. Тогда $n - \sigma_s \leqslant 6$ и $p_s > n - \sigma_s$.

Если a — натуральное число, то согласно выбору числа p_i, условие $p_1 \dots p_s a \in \omega(A_{n+1})$ эквивалентно тому, что $a \in \omega(A_{n-\sigma_s+1})$. Следовательно, $p_1 p_2 \dots p_s a_{n-\sigma_s+1}$ лежит в $\omega(A_{n+1}) \setminus \omega(A_n)$.

Поскольку все шаги требует времени полиномиального от n, лемма доказана. □

Лемма 3.1.12. *Пусть p — простое число и q — степень числа p. Выполнены следующие утверждения:*

(1) *если $p \neq 2$, то $p(q^{n-1} + 1) \in \omega(S_{2n}(q)) \setminus \omega(O_{2n+1}(q))$;*

(2) *если $n > 5$, то $\frac{q^{n+1}-1}{(4,q^{n+1}-1)}$ лежит в $\omega(O^+_{2n+2}(q))$ и не лежит в $\omega(S_{2n}(q)) \cup \omega(\Omega_{2n+1}(q))$.*

Доказательство. Утверждение леммы напрямую следует из [2, следствия 2, 3, 4, 6, 8, 9]. □

Граф называется *расщепляемым*, если его вершины можно разделить на клику и коклику.

Лемма 3.1.13. *Существует алгоритм, который по данному графу Γ находит его разбиение на клику и коклику в случае, если он расщепляемый или сообщает, что он не расщепляемый, в противном случае. Время работы алгоритма ограничено полиномом от числа вершин графа Γ.*

Доказательство. См. [63, теорема 6 и доказательство теоремы 9]. □

§ 3.2. Атомарные делители и AD-граф

Пусть $\mathcal{M}$ — конечное множество натуральных чисел, M — максимальный элемент множества $\mathcal{M}$ и m — мощность множества $\mathcal{M}$.

Мы дадим два эквивалентных определения атомарных делителей множества натуральных чисел.

Определение 1. *Для непустого подмножества $\mathcal{S}$ множества $\mathcal{M}$ обозначим через $v = v_{\mathcal{M}}(\mathcal{S})$ наибольшее натуральное число такое, что v делит каждый элемент из $\mathcal{S}$ и*

взаимно просто с элементами из $\mathcal{M} \setminus \mathcal{S}$. *Положим* $V(\mathcal{M}) = \{v_{\mathcal{M}}(\mathcal{S}) > 1 \mid \varnothing \neq \mathcal{S} \subseteq \mathcal{M}\}$. *Элементы множества* $V(\mathcal{M})$ *называются атомарными делителями множества* $\mathcal{M}$.

Определение 2. *Рассмотрим две бинарные операции на множестве натуральных чисел: взятие наибольшего общего делителя и взятие* m'*-части числа* n *для чисел* n *и* m. *Пусть* $\overline{\mathcal{M}}$ *— замыкание* $\mathcal{M}$ *относительно этих операций. Множество атомарных делителей множества* $\mathcal{M}$ *— это множество неединичных элементов множества* $\overline{\mathcal{M}}$, *которые минимальны относительно делимости, т.е. атомов соответствующей решетки.*

Как правило, множество $\mathcal{M}$ фиксировано и мы пишем $v(S)$ вместо $v_{\mathcal{M}}(S)$.

Лемма 3.2.1. *Определения* 1 *и* 2 *эквивалентны.*

Доказательство. Очевидно, что каждое число $v(\mathcal{S})$ лежит в $\overline{\mathcal{M}}$. Пусть $\hat{V}(\mathcal{M})$ — множество чисел d из $\omega(\mathcal{M})$ таких, что для любого $m \in \mathcal{M}$ либо d делит m, либо d и m взаимно просты. Тогда $V(\mathcal{M}) = \mu(\hat{V}(\mathcal{M}))$. Следовательно, $V(\mathcal{M})$ состоит из атомов решетки делимости на множестве $\overline{\mathcal{M}}$. Теперь, если d — атом из $\overline{\mathcal{M}}$, то для любого $m \in \overline{\mathcal{M}}$ либо d делит m, либо $(d, m) = 1$. Положим $\mathcal{S}(d) = \{m \in \mathcal{M} \mid d \text{ делит } m\}$. По определению d делит $v(\mathcal{S}(d))$, последнее число также является атомом. Отсюда $d = v(\mathcal{S}(d))$ и лемма доказана. □

В следующей лемме перечислены некоторые базовые свойства атомарных делителей.

Лемма 3.2.2. *Выполнены следующие утверждения.*

(1) *Различные атомарные делители множества* $\mathcal{M}$ *взаимно просты.*

(2) $\pi(V(\mathcal{M})) = \pi(\mathcal{M})$.

(3) *Если* $p \in \pi(\mathcal{M})$, $v \in V(\mathcal{M})$ *и* p *делит* v, *то* $v = v(\mathcal{S})$, *где* $\mathcal{S}$ *— подмножество множества* $\mathcal{M}$, *состоящее из чисел, делящихся на* p.

Доказательство. Пункт (1) следует напрямую из определений. Если $p \in \pi(\mathcal{M})$ и $\mathcal{S} = \{m \in \mathcal{M} \mid p \text{ делит } m\}$, то p делит $v(\mathcal{S})$. Это наблюдение дает пункты (2) и (3). □

Лемма 3.2.3. *Пусть* $\mathcal{M}_1$ *и* $\mathcal{M}_2$ *— конечные множества натуральных чисел. Тогда*

$$V(\mathcal{M}_1 \cup \mathcal{M}_2) = V(V(\mathcal{M}_1) \cup V(\mathcal{M}_2)).$$

В частности, если $\mathcal{M}_2$ *состоит из одного элемента, то* $V(\mathcal{M}_1 \cup \mathcal{M}_2) = V(V(\mathcal{M}_1) \cup \mathcal{M}_2)$.

Доказательство. Поскольку замыкание $\overline{\mathcal{M}_1 \cup \mathcal{M}_2}$ (в смысле определения 2) содержит замыкание $\overline{\mathcal{N}}$ множества $\mathcal{N} = V(\mathcal{M}_1) \cup V(\mathcal{M}_2)$, каждый атомарный делитель множества $\mathcal{N}$ делится на некоторый атомарный делитель множества $\mathcal{M}_1 \cup \mathcal{M}_2$. Следовательно, для доказательства леммы достаточно показать, что каждый элемент множества $V(\mathcal{M}_1 \cup \mathcal{M}_2)$ лежит в $\overline{\mathcal{N}}$.

Пусть $\mathcal{T}$ — некоторое подмножество множества $\mathcal{M}_1 \cup \mathcal{M}_2$ такое, что $v = v_{\mathcal{M}_1 \cup \mathcal{M}_2}(\mathcal{T}) > 1$. Положим $v_i = v_{\mathcal{M}_i}(\mathcal{T} \cap \mathcal{M}_i)$ для $i = 1, 2$. Из определения 1 легко видеть, что если оба элемента v_1 и v_2 определены (а значит, оба подмножества $\mathcal{T} \cap \mathcal{M}_1$ и $\mathcal{T} \cap \mathcal{M}_2$ непусты), то число v равно их наибольшему общему делителю. Если одно из них, например v_1, не

определено, то v_2 должно быть определено, и v равно $(v_2)_{(\mathcal{M}_1)'}$. Следовательно, v в любом случае лежит в $\overline{\mathcal{N}}$, и лемма доказана. □

Определение 3. *Назовем* AD*-графом* $\mathrm{AD}(\mathcal{M})$ *множества* $\mathcal{M}$ *граф с множеством вершин* $V(\mathcal{M})$*, в котором две различные вершины* v_1 *и* v_2 *смежны тогда и только тогда, когда* $v_1v_2 \in \omega(\mathcal{M})$.

Замечание. Отметим, что вершины AD-графа, аналогично вершинам графа простых чисел, являются числами. Таким образом, AD-граф — это не абстрактный граф, а реализация абстрактного графа на множестве натуральных чисел.

Поскольку вершины AD-графа параметризуются подмножествами множества $\mathcal{M}$, размер этого графа может быть большим в сравнении с размером множества $\mathcal{M}$. Тем не менее, существует эффективный метод построения графа $\mathrm{AD}(\mathcal{M})$, если его размер ограничен.

Лемма 3.2.4. *Существует алгоритм, который по данному натуральному числу* l *и множеству* $\mathcal{M}$ *строит граф* $\mathrm{AD}(\mathcal{M})$*, если число атомарных делителей множества* $\mathcal{M}$ *не превосходит* l *или сообщает, что это условие не выполнено. Время работы алгоритма ограничено полиномом от* $lm \log M$.

Доказательство. Пусть $\mathcal{M} = \{a_1, a_2, \ldots, a_m\}$. Положим $\mathcal{S}_i = \{a_1, \ldots, a_i\}$ и обозначим $\mathrm{AD}(\mathcal{S}_i)$ через Γ_i. Из леммы 3.2.3 следует, что атомарные делители множеств $\mathcal{S}_i$ и $V(\mathcal{S}_{i-1}) \cup \{a_i\}$ совпадают. Поскольку все элементы множества $V(\mathcal{S}_{i-1})$ попарно взаимно просты,

$$V(\mathcal{S}_i) = \{(v, a_i), (v)_{a_i'}, (a_i)_{\mathcal{S}_{i-1}'} \mid v \in V(\mathcal{S}_{i-1})\} \setminus \{1\}.$$

В частности, $|V(\mathcal{S}_i)| \leqslant 2|V(\mathcal{S}_{i-1})| + 1$. Значит, граф Γ_i может быть построен по графу Γ_{i-1} за время, ограниченное полиномом от $|V(\mathcal{S}_{i-1})| \log M$. Поскольку как минимум одно из чисел (v, a_i) и $(v)_{a_i'}$ не равно единице, имеем $|V(\mathcal{S}_i)| \geqslant |V(\mathcal{S}_{i-1})|$. Следовательно, если количество вершин графа Γ_i превосходит l, алгоритм выдает, что число вершин графа $\mathrm{AD}(\mathcal{M})$ также больше l. □

§ 3.3. AD-граф конечной группы

Пусть G — конечная группа. Заметим, что граф $\mathrm{AD}(\omega(G))$ совпадает с $\mathrm{GK}(G)$. Действительно, поскольку $\pi(G)$ — подмножество $\omega(G)$, вершины графа $\mathrm{AD}(\omega(G))$ — это простые числа, а смежность вершин в графах $\mathrm{AD}(\omega(G))$ и $\mathrm{GK}(G)$ определяется одинаковым образом.

Если рассмотреть графы $\mathrm{AD}(\nu(G))$ для множеств $\nu(G)$, заключенных между $\mu(G)$ и $\omega(G)$, то эти графы наследуют структуру решетки с множеств из интервала $[\mu(G), \omega(G)]$. При этом, граф простых чисел является максимальным элементом этой решетки.

Определение 1. *Граф атомарных делителей (или* AD*-граф)* $\mathrm{AD}(G)$ *группы* G *— это граф* $\mathrm{AD}(\mu(G))$.

Пусть $V(G)$ — это множество вершин графа $\mathrm{AD}(G)$, т.е. множество атомарных дели-

телей множества $\mu(G)$. Заметим, что $\pi(V(G)) = \pi(G)$ и элементы $V(G)$ попарно взаимно просты по лемме 3.2.2, т.е. для любого простого делителя r порядка группы G есть единственная вершина $\mathrm{AD}(G)$, делящаяся на r.

Обозначим через φ отображение из $\mathrm{GK}(G)$ на $\mathrm{AD}(G)$, действующее следующим образом: если $r \in \pi(G)$ и v — это вершина графа $\mathrm{AD}(G)$, делящаяся на r, то $r\varphi = v$.

Лемма 3.3.1. *Пусть G — конечная группа, а отображение φ определено выше. Различные вершины r и s графа $\mathrm{GK}(G)$ смежны тогда и только тогда, когда $r\varphi$ и $s\varphi$ смежны или совпадают. В частности, множество вершин образует коклику в $\mathrm{GK}(G)$ тогда и только тогда, когда образы этих вершин относительно φ попарно различны и образуют коклику в $\mathrm{AD}(G)$.*

Доказательство. Если $r\varphi = s\varphi$, то $rs \in \omega(G)$ и вершины r, s смежны в $\mathrm{GK}(G)$. Если вершина $r\varphi$ смежна с $s\varphi$, то $(r\varphi)(s\varphi) \in \omega(G)$ и r, s смежны в $\mathrm{GK}(G)$. Наконец, предположим, что $r\varphi$ и $s\varphi$ несмежны. Из определения атомарного делителя следует, что если элемент a множества $\mu(G)$ делится на r (или s), то a делится на $r\varphi$ (соответственно на $s\varphi$). Значит, r и s несмежны в $\mathrm{GK}(G)$, поскольку в противном случае множество $\omega(G)$ содержало элемент, делящийся на $(r\varphi)(s\varphi)$. □

Отметим, что из леммы 3.3.1 вытекает, что размеры максимальных коклик в графах $\mathrm{AD}(G)$ и $\mathrm{GK}(G)$ равны, и следовательно, для конечных простых классических групп даны в лемме 3.1.6.

Лемма 3.3.2. *Если G — конечная классическая группа с $\mathrm{prk}(G) \geqslant 4$ или знакопеременная группа, то граф $\mathrm{AD}(G)$ расщепляем.*

Доказательство. В случае знакопеременных групп граф простых чисел группы G является объединением максимальной клики и максимально коклики, значит, таковым является и граф $\mathrm{AD}(G)$. В случае классических групп доказательство может быть легко извлечено из доказательства [8, предложения 3.9 и 3.10]. □

Лемма 3.3.3. *Пусть G — конечная простая классическая группа с $\mathrm{prk}(G) \geqslant 12$ или знакопеременная группа. Пусть M — это максимальный элемент множества $\omega(G)$. Тогда мощность множества $V(G)$ не превосходит*

$$C(M) = \max(140, (\ln(2M)/0.99)^2, 2(\log M + 3)).$$

Доказательство. Пусть G — классическая группа. Положим $n = \mathrm{prk}(G)$. Поскольку $\omega(G)$ содержит число $q^{n-2} - 1$ (см., например, [3]), имеем $\log M > n - 3$. По лемме 3.3.4 число вершин графа $\mathrm{AD}(G)$ меньше $2n$. Следовательно, число вершин графа $\mathrm{AD}(G)$ меньше $2(\log M + 3)$.

Пусть G — знакопеременная группа степени n. Пусть $g(n)$ — функция Ландау от n, т.е. наибольший порядок элемента симметрической группы S_n. Очевидно, $2M \geqslant g(n)$. Из [76, теорема 1] следует, что $\ln g(n) > 0.99\sqrt{n \ln n}$, откуда $n < (\ln(2M)/0.99)^2$, для $n \geqslant 810$. Следовательно, число вершин графа $\mathrm{AD}(G)$ не превосходит максимума $(\ln(2M)/0.99)^2$ и числа простых чисел, не превосходящих 810, т.е. 140. Лемма доказана. □

Замечание. Из доказательства леммы 3.3.3 следует, что если G — классическая группа, то число вершин графа $\mathrm{AD}(G)$ не превосходит $2(\log M + 3)$, в то время как для знакопеременных групп граница — $\max(140, (\ln(2M)/0.99)^2)$.

Следующая лемма является ключевым техническим инструментом данной главы. Для натурального i положим $\eta(i) = i/(2, i)$. Напомним, что $\Phi_i^*(a)$ обозначает наибольший примитивный делитель числа $a^i - 1$.

Лемма 3.3.4. *Пусть G — конечная простая классическая группа над полем характеристики p и порядка q с $\mathrm{prk}(G) \geqslant 12$. Положим $t = (2, q-1)$. Тогда $V(G) \subseteq \theta(G)$, где $\theta(G)$ определено в таблице* 18. *Более того,* $\mathrm{prk}(G) - 1 \leqslant |V(G)| \leqslant 2\,\mathrm{prk}(G)$.

Таблица 18. Вид атомарных делителей

G	$\theta(G)$
$L_n^\varepsilon(q)$	p, a и $a\lvert\varepsilon q-1\rvert_{n'}$ для делителей a числа $(\varepsilon q-1)_n$, $\Phi_i^*(\varepsilon q)$ для $2 \leqslant i \leqslant n$
$O_{2n+1}(q)$, $S_{2n}(q)$	2^α, p, $(\Phi_1^*(q))_{t'}$, $\Phi_i^*(q)$ для $i \geqslant 2$ и $\eta(i) \leqslant n$
$O_{2n}^\varepsilon(q)$	2^α, $t^\beta p$, $t^\gamma(\Phi_1^*(q))_{t'}$, $t^\delta\Phi_2^*(q)$, $\Phi_i^*(q)$ для $2 \leqslant \eta(i) \leqslant n$.

Доказательство. Положим $n = \mathrm{prk}(G)$. Начнем со случая $G = L_n^\varepsilon(q)$. Спектр группы G — подмножество в множестве $\omega(GL_n^\varepsilon(q))$. Последнее состоит из всех делителей следующих чисел:

$[(\varepsilon q)^{n_1} - 1, (\varepsilon q)^{n_2} - 1, \ldots, (\varepsilon q)^{n_s} - 1]$, где $n_1 + n_2 + \cdots + n_s = n$;

$p^k[(\varepsilon q)^{n_1} - 1, (\varepsilon q)^{n_2} - 1, \ldots, (\varepsilon q)^{n_s} - 1]$, где $p^{k-1} + 1 + n_1 + n_2 + \cdots + n_s = n$;

$p^k(\varepsilon q - 1)$, если $n = p^{k-1} + 1$.

Следовательно, если $\Phi_i^*(\varepsilon q)$ делит порядок группы G, то каждый элемент множества $\mu(GL_n^\varepsilon(q))$ либо делится на $\Phi_i^*(\varepsilon q)$, либо взаимно прост с ним. Значит, каждое число $\Phi_i^*(\varepsilon q)$, где $1 \leqslant i \leqslant n$, делит некоторую вершину графа $\mathrm{AD}(GL_n^\varepsilon(q))$. Поскольку $|L_n^\varepsilon(q)| = |GL_n^\varepsilon(q)|/\left(|\varepsilon q - 1|(n, \varepsilon q - 1)\right)$, числа $\Phi_i^*(\varepsilon q)$ для $i \geqslant 2$ делят вершины графа $\mathrm{AD}(G)$.

Для $2 \leqslant i \leqslant n$ обозначим через v_i вершину графа $\mathrm{AD}(G)$, делящуюся на $\Phi_i^*(\varepsilon q)$. Отметим, что согласно лемме 3.1.2 некоторые вершины могут отсутствовать: v_2, если $G = L_n^\varepsilon(q)$, где $q + \varepsilon 1$ — степень числа 2; v_6, если $G = L_n(2)$; и v_2, v_3, если $G = U_n(2)$. Покажем, что если $i \neq j$, то $v_i \neq v_j$. Пусть Γ — подграф графа $\mathrm{AD}(G)$, порожденный вершинами $v_2, \ldots, v_n$. Для вершины v графа $\mathrm{AD}(G)$ обозначим через $\triangle(v)$ множество вершин графа Γ, отличных от v и несмежных с v в $\mathrm{AD}(G)$.

По [7, предложения 2.1, 2.2] множество примитивных простых делителей $r_i(\varepsilon q)$ для $i > n/2$ образует коклику в $\mathrm{GK}(G)$. Из леммы 3.3.1 следует, что соответствующие вершины v_i попарно различны и также образуют коклику. В частности,

$$|\triangle(v_i)| \geqslant n - (n+1)/2 = (n-1)/2, \text{ если } i > n/2.$$

Для $2 \leqslant i \leqslant n/2$ имеем

$$\triangle(v_i) = \{v_{n-i+1}, v_{n-i+2}, \ldots, v_n\} \setminus \{v_k\},$$

где k — единственный индекс, делящийся на i (даже если некоторые из v_i не существуют, ни одно из них не могло бы лежать в $\triangle(v_i)$). В частности,

$$|\triangle(v_i)| = i - 1 \leqslant n/2 - 1.$$

Заключаем, что все вершины v_i для $2 \leqslant i \leqslant n/2$ попарно различны и не совпадают с вершинами v_j для $j > n/2$.

Таким образом, v_2, v_3, …, v_n — попарно различные вершины графа Γ. Это означает, что все вершины v_i имеют вид $\Phi_i^*(\varepsilon q)d_i$, где $\pi(d_i) \subseteq \pi(p(\varepsilon q - 1))$. Теперь покажем, что $d_i = 1$ для каждого $i \geqslant 2$.

Для $r \in \pi(p(\varepsilon q - 1))$ обозначим через u_r вершину графа $\mathrm{AD}(G)$, делящуюся на r. По [7, предложения 4.1, 4.2] выполнено одно из следующих утверждений:

(1) $r \in \pi(\varepsilon q - 1)$, $(\varepsilon q - 1)_r > (n)_r$ и $\triangle(u_r) = \{v_n\}$;

(2) $r \in \pi(\varepsilon q - 1)$, $(\varepsilon q - 1)_r < (n)_r$ или $(\varepsilon q - 1)_r = (n)_r = 2$, а $\triangle(u_r) = \{v_{n-1}\}$;

(3) $r \in \pi(\varepsilon q - 1)$, $(\varepsilon q - 1)_r = (n)_r > 2$ и $\triangle(u_r) = \{v_{n-1}, v_n\}$;

(4) $r = p$, $\triangle(u_r) = \{v_{n-1}, v_n\}$.

Сравнивая размер $\triangle(u_r)$ с размером $\triangle(v)$, получаем, что u_r может совпадать только с v_2 или v_3.

Из определения следует, что для любой пары атомарных делителей множества $\mathcal{N}$ существует число $n \in \mathcal{N}$ такое, что n делится на один из них и взаимно просто с другим. Будем называть такой элемент разделяющим.

Разделяющие элементы для всех пар вида v_i, u_r и пары u_p, u_r для $r \neq p$ перечислены в таблице 19. Поскольку эти разделяющие элементы всегда существуют, имеем $v_i = \Phi_i^*(\varepsilon q)$ для $i \geqslant 2$ и $u_p = p$. Отметим, что равенства $\triangle(u_r) = \triangle(v_i)$ и $\triangle(u_r) = \triangle(u_p)$ могут быть выполнены только при некоторых ограничениях на параметры группы G; эти ограничения перечислены во втором столбце таблицы 19. Например, $\triangle(u_p) = \triangle(v_3)$ влечет, что 3 делит $n - 2$. Действительно, $\triangle(v_3) = \{v_{n-2}, v_{n-1}, v_n\} \setminus \{v_k\}$, где $k \in \{n-2, n-1, n\}$ делится на 3, и $\triangle(u_p) = \{v_{n-1}, v_n\}$. Максимальность элементов из таблицы 19 следует из [1, следствие 3].

Таблица 19. Разделяющие элементы для u_p, u_r, v_2 и v_3

Вершины	Ограничения	Разделяющие элементы
u_p, v_3	$3 \mid (n-2)$	$\frac{[(\varepsilon q)^3-1,(\varepsilon q)^{n-3}-1]}{(n,\varepsilon q-1)}$
u_p, u_r	$(n)_r = (\varepsilon q - 1)_r > 2$	$[(\varepsilon q)^k - 1, (\varepsilon q)^{n-k-1} - 1]$, $n/3 < k < (n-1)/2$
u_r, v_3	$(n)_r = (\varepsilon q - 1)_r > 2$, $3 \mid (n-2)$	$\frac{[(\varepsilon q)^3-1,(\varepsilon q)^{n-3}-1]}{(n,\varepsilon q-1)}$
u_r, v_2	$(n)_r < (\varepsilon q - 1)_r$, $2 \mid (n-1)$	$\frac{p((\varepsilon q)^{n-2}-1)}{(n,\varepsilon q-1)}$
u_r, v_2	$2 \mid n$ и либо $(n)_r > (\varepsilon q - 1)_r$, либо $(n)_r = (\varepsilon q - 1)_r = 2$	$p((\varepsilon q)^{n-3} - 1)$

Таким образом, уже гарантировано наличие некоторого числа различных вершин:

u_p, v_2, …, v_n и вершины вида u_r для $r \neq p$. Помимо указанных выше вершин, из указанных может отсутствовать вершина u_r в случае $G = L_n(2)$. Таким образом, для каждой рассматриваемой группы не более двух вершин из этого списка могут отсутствовать, что дает неравенство $|V(G)| \geqslant n - 1$.

Может быть несколько вершин вида u_r для $r \neq p$. Информация о $\triangle(u_r)$ показывает, что вершины этого множества зависят от соотношения между $(n)_r$ и $(\varepsilon q - 1)_r$. Если $(n)_r < (\varepsilon q - 1)_r$, то из [1, следствие 3] вытекает, что элементы множества $\mu(G)$, не делящиеся на r, — это $((\varepsilon q)^n - 1)/((n, \varepsilon q - 1)|\varepsilon q - 1|)$ и p^k (последнее число лежит в $\mu(G)$ только если $n = p^{k-1} + 1$). Значит, множество максимальных порядков элементов, делящихся на такое r, не зависит от самого простого числа. Следовательно, все вершины u_r для таких r являются одной вершиной, делящейся на $(\varepsilon q - 1)_{n'}$. Остальные простые делители числа $\varepsilon q - 1$ делят $(n, \varepsilon q - 1)$. Вершины, соответствующие таким простым числам, могут быть различны с разделяющими числами вида

$$\frac{[(\varepsilon q)^{n_1} - 1, (\varepsilon q)^{n_2} - 1]}{\left(\frac{n}{(n_1,n_2)}, \varepsilon q - 1\right)}, \text{ где } n_1 + n_2 = n.$$

Поскольку число неединичных делителей числа $(n, \varepsilon q - 1)$ меньше n, имеем $|V(G)| \leqslant 2n$. Таким образом, лемма в этом случае доказана.

Пусть $G = O_{2n+1}(q)$ или $S_{2n}(q)$. Из описания спектров этих групп (см. [2, следствия 2, 3, 6]) следует, что числа $\Phi_i^*(q)$, где $i \geqslant 2$ и $\eta(i) \leqslant n$, а также число $(\Phi_1^*(q))_{2'}$ делят некоторые вершины графа $\mathrm{AD}(G)$. Действительно, каждое из этих чисел либо делит элемент множества $\mu(G)$, либо взаимно просто с ним. Обозначим через v_i вершины графа $\mathrm{AD}(G)$, делящуюся на $\Phi_i^*(q)$ для $i \geqslant 2$, и вершину, делящуюся на $(\Phi_1^*(q))_{2'}$ для $i = 1$.

Из [7, предложение 2.3] и леммы 3.3.1 следует, что вершины v_i с $\eta(i) > n/2$ попарно различны и образуют коклику графа $\mathrm{AD}(G)$.

Рассмотрим различные индексы i и j такие, что $1 < \eta(i) \leqslant \eta(j) \leqslant n/2$. Положим $a_1 = q^{n-\eta(i)} + 1$, $a_2 = q^{n-\eta(i)-1} + 1$ и либо $a_3 = q^{n-\eta(i)} - 1$, если $n - \eta(i)$ нечетно, либо $a_3 = q^{n-\eta(i)-1} - 1$ в противном случае. Наибольший общий делитель любой пары из этих чисел делит $(2, q-1)(q+1)$. Следовательно, каждое из чисел $\Phi_i^*(q)$ и $\Phi_j^*(q)$ делит максимум одно из этих чисел. Значит, как минимум одно из чисел a_k для $k \in \{1, 2, 3\}$ взаимно просто с $\Phi_i^*(q)\Phi_j^*(q)$. По [2, следствия 2, 3, 6] одно из чисел $[q^{\eta(i)} + (-1)^{i/\eta(i)}, a_k]$ и $p[q^{\eta(i)} + (-1)^{i/\eta(i)}, a_k]$ лежит в $\mu(G)$. Эти числа делятся на $\Phi_i^*(q)$ и не делятся на $\Phi_j^*(q)$. Отсюда $v_i \neq v_j$.

Рассмотрим индексы i и j такие, что $\eta(i) \leqslant n/2 < \eta(j)$. Предположим, что существует натуральное число l такое, что $\eta(l) = \left\lfloor \frac{n+1}{2} \right\rfloor$ и $l \neq i$. Тогда по [2, следствия 2,3,6] число $\Phi_i^*(q)\Phi_l^*(q)$ лежит в $\omega(G)$, а число $\Phi_j^*(q)\Phi_l^*(q)$ нет. Это разделяет вершины v_i и v_j. Такое l не существует, только если число $n/2$ четно и $\eta(i) = n/2$. В этом случае $\Phi_i^*(q)\Phi_j^*(q) \notin \omega(G)$ и $v_i \neq v_j$. Следовательно, все вершины v_i для $i \geqslant 3$ попарно различны.

Теперь покажем, что v_1 и v_2 имеют вид $t^\alpha(\Phi_1^*)(q)_{t'}$ и $t^\beta\Phi_2^*(q)$ соответственно для некоторых α и β (напомним, что $t = (2, q-1)$). Положим $t_1 = t$, если $G = O_{2n+1}(q)$, и $t_1 = 1$ в противном случае. Согласно [2, следствия 2, 3, 6] множество $\mu(G)$ содержит числа $(q^n \pm 1)/t$

и $p(q^{n-1} \pm 1)/t_1$. Поскольку

$$\left(\frac{q^n - 1}{t}, p\frac{q^{n-1} - 1}{t}\right) = \frac{q-1}{t},$$

имеем требуемое для v_1. По лемме 3.1.1 всегда можно выбрать $\epsilon \in \{+, -\}$ так, чтобы

$$\left(\frac{q^n - \epsilon 1}{t}, p\frac{q^{n-1} + \epsilon 1}{t}\right) = \frac{q+1}{t}.$$

Это дает требуемое для v_2.

Рассмотрим вершины u и v, делящиеся на 2 и p соответственно. Во-первых, заметим, что если $p \neq 2$, то $u \neq v$. Действительно, $(q^n \pm 1)/t \in \mu(G)$ и одно из этих чисел нечетно и взаимно просто с p. Далее,

$$p\frac{q^{n-1} \pm 1}{t_1} \in \mu(G) \text{ и } \left(p\frac{q^{n-1}+1}{t_1}, p\frac{q^{n-1}-1}{t_1}\right) = p\frac{t}{t_1}.$$

Следовательно, $v = p$.

Покажем, что $u = 2^\alpha$ для некоторого натурального α, если $p \neq 2$. Из [7, предложение 4.3] следует, что существует единственная вершина w графа $\mathrm{AD}(G)$ несмежная с u. Более того, число w равно $\Phi_i^*(q)$, где i удовлетворяет следующим условиям: $i = n$, если n нечетно и $q \equiv 3(4)$, и $i = 2n$ в противном случае. Из [7, предложение 2.3] следует, что вершина v_j для $j > 2$ несмежна как минимум с двумя вершинами графа $\mathrm{AD}(G)$ и, следовательно, не может совпадать с u. Таблица 20 содержит список разделяющих чисел для u и v_j, где $j \in \{1, 2\}$. Если условия на группу G из таблицы не выполнены, то множество вершин, несмежных с u в $\mathrm{AD}(G)$, и соответствующее множество для v_i различны.

Таблица 20. Разделяющие элементы для v и v_i при $i = 1, 2$

Вершина	Ограничения	Разделяющий элемент
v_1	$2 \mid n$	$p[q+1, q^{n-2}+1]$
v_1	$2 \mid (n-1)$, $4 \mid (q-1)$	$[q+1, q^{n-1}+1]$
v_2	$2 \mid n$	$p[q-1, q^{n-2}+1]$
v_2	$2 \mid (n-1)$, $4 \mid (q-3)$	$[q-1, q^{n-1}+1]$

Таким образом, $V(G) = \{2^\alpha, p, (\Phi_1^*(q))_{t'}, \Phi_i^*(q), \text{ где } i \geqslant 2, \eta(i) \leqslant n\}$, что и требовалось показать. Остается проверить ограничения на мощность $V(G)$. Поскольку неравенство $\eta(i) \leqslant n$ имеет $\left\lfloor \frac{3n}{2} \right\rfloor$ натуральных решений и из перечисленных чисел максимум два могут отсутствовать ($\Phi_1^*(q)$ и $\Phi_2^*(q)$ могут быть степенями двойки, в худшем случае при $q = 3$ они оба степени двойки), получаем неравенства

$$\left\lfloor \frac{3n}{2} \right\rfloor - 2 \leqslant |V| \leqslant \left\lfloor \frac{3n}{2} \right\rfloor + 2.$$

Это неравенство очевидно сильнее, чем неравенство из формулировки предложения, что завершает доказательство для этого случая.

Наконец, пусть $G = O^{\varepsilon}_{2n}(q)$. Описание спектров этих групп (см., например, [2, следствия 4, 8, 9]) показывают, что найдутся вершины графа $\mathrm{AD}(G)$, делящиеся на следующие числа: $(\Phi^*_1(q))_{t'}$; $\Phi^*_i(q)$, где $i \geqslant 2$ и $\eta(i) < n$; $\Phi^*_n(q)$, если $\varepsilon = +$, и $\Phi^*_{2n}(q)$, если $\varepsilon = -$.

Как и ранее, обозначим через v_i вершину графа $\mathrm{AD}(G)$, делящуюся на $\Phi^*_i(q)$ при $i \geqslant 2$, и вершину, делящуюся на $(\Phi^*_1(q))_{t'}$ при $i = 1$.

Вершины v_i с $\eta(i) > n/2$ попарно различны и образуют коклику в $\mathrm{AD}(G)$ [8, предложение 2.5].

Пусть i и j — различные числа такие, что $1 < \eta(i) \leqslant \eta(j) \leqslant n/2$. Рассмотрим числа $q^{n-\eta(i)} \pm 1$, $q^{n-\eta(i)-1} \pm 1$. Поскольку наибольший общий делитель любой пары из этих чисел делит $q^2 - 1$, максимум одно из этих чисел делится на $\Phi^*_i(q)$ или $\Phi^*_j(q)$. Следовательно, не менее двух из них взаимно просты с $\Phi^*_i(q)\Phi^*_j(q)$. Если $q^{n-\eta(i)-1} + \varepsilon_1$ взаимно просто с $\Phi^*_i(q)\Phi^*_j(q)$ для некоторого $\varepsilon_1 \in \{1, -1\}$, то элемент

$$[q^{\eta(i)} + (-1)^{i/\eta(i)}, q^{n-\eta(i)-1} + \varepsilon_1, q - (-1)^{i/\eta(i)}\varepsilon_1]$$

множества $\mu(G)$ кратен $\Phi^*_i(q)$ и взаимно прост с $\Phi^*_j(q)$. В противном случае элемент

$$a = [q^{\eta(i)} + (-1)^{i/\eta(i)}, q^{n-\eta(i)} + \varepsilon(-1)^{i/\eta(i)}]$$

множества $\mu(SO^{\varepsilon}_{2n}(q))$ делится на $\Phi^*_i(q)$ и взаимно прост с $\Phi^*_j(q)$. Значит, для некоторого целого $\xi \geqslant 0$ множество $\mu(G)$ содержит элемент вида $t^{\xi}(a)_{t'}$, который является разделяющим для $\Phi^*_i(q)$ и $\Phi^*_j(q)$.

Тот факт, что v_i и v_j, где $\eta(i) \leqslant n/2 < \eta(j)$, — это различные вершины, доказывается так же как в случае симплектических групп и ортогональных групп нечетной размерности. Следовательно, вершины v_i для $i \geqslant 3$ попарно различны.

Покажем, что v_1 и v_2 имеют вид $t^{\gamma}(\Phi^*_1(q))_{t'}$ и $t^{\delta}\Phi^*_2(q)$ соответственно для некоторых целых γ и δ. Сначала предположим, что $G = O^+_{2n}(q)$. Заметим, что

$$(p[q+1, q^{n-2} - 1], [q^{n-1} + 1, q + 1]) = q + 1.$$

Кроме того,

$$(p[q+1, q^{n-2} - 1], q^n - 1) = q - 1,$$

если n нечетно, и

$$(p[q+1, q^{n-2} - 1], q^{n-1} - 1) = q - 1,$$

если n четно. Все числа, от которых вычисляется наибольшие общие делители, лежат в $\mu(SO^+_{2n}(q))$. Значит, вершины v_1 и v_2 имеют требуемые виды. Поскольку ни одна из этих вершин не делится на p, вершина, делящаяся на p, имеет требуемый вид.

Пусть $G = O^-_{2n}(q)$. Если n четно, то

$$([q-1, q^{n-1} + 1], p[q^{n-2} + 1, q + 1]) = q + 1$$

и

$$([q-1, q^{n-1} + 1], p[q^{n-2} + 1, q - 1]) = q - 1.$$

Если n нечетно, то

$$(q^n+1, q^{n-1}-1) = q+1 \text{ и } ([q^{n-1}+1, q-1], q^{n-1}-1) = q-1.$$

Поскольку все числа, от которых вычисляется наибольшие общие делители, лежат в $\mu(SO^-_{2n}(q))$, мы получили требуемое. Как и ранее, вершина, делящаяся на p, имеет требуемый вид.

Для завершения доказательства остается заметить, что все нечетные вершины графов $\mathrm{AD}(O^\varepsilon_{2n}(q))$ и $\mathrm{AD}(O_{2n+1}(q))$ совпадают, за возможным исключением одной из вершин $\Phi^*_n(q)$ или $\Phi^*_{2n}(q)$ (они могут отсутствовать в графе $\mathrm{AD}(O^\varepsilon_{2n}(q))$). Следовательно, ограничения на количество вершин следуют из соответствующих неравенств, полученных в случае $G = O_{2n+1}(q)$. Лемма доказана. □

Для конечной группы G обозначим через $\rho^*(4, G)$ коклику графа $\mathrm{GK}(G)$, удовлетворяющую условию $4r \notin \omega(G)$ для любого $r \in \rho^*(4, G)$ и имеющую максимальный размер среди коклик с таким свойством. Положим $t^*(4, G) = |\rho^*(4, G)|$.

Пусть $\theta^*(4, \mathrm{AD}(G))$ — множество вершин v графа $\mathrm{AD}(G)$ таких, что $4v \notin \omega(G)$. Очевидно, если $r \in \rho^*(4, G)$ и v — вершина графа $\mathrm{AD}(G)$, делящаяся на r, то $v \in \theta^*(4, \mathrm{AD}(G))$. Таким образом, $|\theta^*(4, \mathrm{AD}(G))| \geqslant t^*(4, G)$.

Идея следующего утверждения впервые появилась в [84, леммы 5.1, 5.2].

Лемма 3.3.5. *Пусть G — конечная простая классическая группа с $\mathrm{prk}(G) \geqslant 9$. Если характеристика поля определния группы G равна 2, то $t^*(4, G) \geqslant 3$, в противном случае $t^*(4, G) < 3$. Более того, $t^*(4, G) = |\theta^*(4, \mathrm{AD}(G))|$.*

Доказательство. Неравенство $t^*(4, G) < 3$ в случае нечетной характеристики доказано в [9, лемма 3.5]. Неравенство $t^*(4, G) \geqslant 3$ в случае характеристики 2 доказано в [9, лемма 3.4] для всех классических групп за исключением групп $L^\varepsilon_n(q)$. В этом оставшемся случае из [1, следствие 3] вытекает, что $\rho^*(4, G)$ состоит из $r_n(\varepsilon q)$, $r_{n-1}(\varepsilon q)$ и $r_{n-2}(\varepsilon q)$.

Для завершения доказательства требуется показать, что $|\theta^*(4, \mathrm{AD}(G))| \leqslant t^*(4, G)$. Если порядок q поля определения группы G нечетен, то 4 делит $q^2 - 1$. Из описания спектров простых классических групп [1, 2] и леммы 3.3.4 следует, что все $\Phi^*_i(q)$, для которых $\Phi^*_i(q)(q^2-1) \notin \omega(G)$, являются попарно несмежными вершинами графа $\mathrm{AD}(G)$. В случае характеристики 2 рассуждение аналогично. □

§ 3.4. Вспомогательные алгоритмы

Напомним, что M обозначает максимальный элемент множества $\mathcal{M}$, m — его мощность. Следующая лемма позволяет исключить знакопеременные группы из доказательства теоремы 15.

Лемма 3.4.1. *Существует алгоритм, который по заданному конечному множеству натуральных чисел $\mathcal{M}$ выдает знакопеременную группу из $\Omega(\mathcal{M})$ или пустое множество, если такой группы не существует. Время работы алгоритма ограничено полиномом от $m \log M$.*

Доказательство. Как было показано в доказательстве леммы 3.3.3, если $\omega(\mathcal{M}) = \omega(A_n)$ при $n \geqslant 5$ (напомним, что $\Omega(\mathcal{M})$ состоит из неабелевых простых групп), то

$$n < \max\{(\ln(2M)/0.99)^2, 810\} = A.$$

Положим, $\tau' = \{r \leqslant A \,|\, r$ — простое число$\}$. Это множество может быть построено за время, ограниченное полиномом от $\log M$. Пусть t — это максимальный элемент множества τ' такой, что

$$\tau = \{s \in \tau' \,|\, s \leqslant t\} \subseteq \pi(\mathcal{M}).$$

Если $\tau \neq \pi(\mathcal{M})$, то $\omega(\mathcal{M})$ не является спектром знакопеременной группы и ответ получен. В противном случае, если $\omega(\mathcal{M}) = \omega(A_n)$, то $t \leqslant n < 2t$ по теореме Бертрана–Чебышева. По лемме 3.1.11 для каждой знакопеременной группы из этого интервала можно построить элемент спектра, отличающий ее от других групп из списка. Следовательно, можно считать, что имеется только один вариант для степени n.

Поскольку множество $\pi(\mathcal{M})$ уже известно, граф $\mathrm{AD}(\omega(\mathcal{M}))$ может быть построен за время, ограниченное полиномом от $m \log M$. Если построенный граф не совпадает с графом $\mathrm{GK}(A_n)$, то алгоритм выдает пустое множество. В противном случае из леммы 3.1.5 следует, что если $\omega(\mathcal{M})$ не является спектром знакопеременной группа, то либо $\omega(\mathcal{M})$ не является спектром неабелевой простой группы, либо это спектр одной из групп, перечисленных в лемме. В последнем случае множество $\pi(\mathcal{M})$ должно совпадать с $\{2, 3, 5, 7\}$, а значит степень n должна лежать в множестве $\{7, 8, 9, 10\}$. Спектры этих знакопеременных групп известны и их можно сравнить с $\mathcal{M}$ за время, линейно зависящее от m. Если для некоторого n имеет место совпадение, то лемма 3.1.4 гарантирует, что $\omega(\mathcal{M})$ не является спектром никакой другой группы и алгоритм выдает степень n. В противном случае алгоритм выдает пустое множество.

В остальных случаях существует две возможности: либо $\omega(\mathcal{M}) = \omega(A_n)$, либо $\omega(\mathcal{M})$ не является спектром конечной неабелевой простой группы. При этих условиях группа A_n лежит в $\Omega(\mathcal{M})$ тогда и только тогда, когда $\mathcal{M}$ — это подмножество в $\omega(A_n)$. Возьмем $a \in \mathcal{M}$. Если $(a)_\tau \neq a$, то $a \notin \omega(A_n)$ и ответ получен. В противном случае

$$a = \prod_{p \in \tau} p^{\alpha_p},$$

и $a \in \omega(A_n)$ тогда и только тогда, когда

$$\sum_{p \in \tau} p^{\alpha_p} + x \leqslant n,$$

где число x равно 0, если a нечетно, и равно 2 в противном случае. Это проверка требует времени, полиномиально зависящего от $\log M$, что завершает доказательство леммы. □

Лемма 3.4.2. *Существует алгоритм, который по заданным натуральным числам k и B, выдает множество конечных простых групп лиева типа G лиева ранга k над полем нечетной характеристики таких, что B — это наибольший элемент в $\omega(G)$. Размер*

этого множества ограничен сверху линейной функцией от k. Время работы алгоритма ограничено полиномом от $k \log B$.

Доказательство. Напомним, что $m_i(G)$ обозначает i-ый максимальный элемент спектра $\omega(G)$ конечной группы G.

Рассмотрим уравнение $m_1(G) = B$ в классе конечных простых групп лиева типа над полями нечетных характеристик. Таблицы 1, A.1-A.7 из [69] содержат списки $m_1(G)$ для всех таких групп. Согласно этим таблицам, число $m_1(G)$ всегда имеет вид $cf(q)$, где $f(x)$ — многочлен со старшим коэффициентом 1 степени, не превосходящей k, чьи корни лежат внутри единичной окружности, а c — положительный коэффициент, зависящий от типа группы G и q, т.е. порядка поля, над которым определена группа G[2]. Следовательно, для данных c и f решение диофантова уравнения $cf(q) = B$ может быть найдено за время, полиномиально зависящее от $k \log B$. Действительно, если $x_1, \ldots, x_d$ — это все корни многочлена f, то

$$f(x) = \prod_{i=1}^{d} (x - x_i).$$

Из неравенства треугольника получаем, что

$$c(q-1)^d \leqslant cf(q) \leqslant c(q+1)^d,$$

и, следовательно, решения уравнения лежат в интервале $\left[\sqrt[d]{B/c} - 1, \sqrt[d]{B/c} + 1\right]$.

Ограничим теперь число возможных значений для c и f. Существует не более трех возможностей для f для каждой комбинации лиева типа и лиева ранга. Если G не является линейной или унитарной группой, то существует не более четырех возможных значений для c: 1, 1/2, 1/3 и 1/4. В случае линейной или унитарной группы лиева ранга k коэффициент c равен либо 1, либо $1/(k+1, \varepsilon q - 1)$. Значит, c имеет вид $1/d$ для d, делящего $k+1$. Отсюда заключаем, что существует не более $11 \cdot 12 + 6(k+1)$ возможных пар (c, f) и размер списка, генерируемого алгоритмом ограничен линейной функцией от k, что и требовалось показать.

Поскольку многие пары (c, f) возникаю только при некоторых ограничениях на группу G, в частности, на q (см. [69, таблицы 1, A.1-A.7]), некоторые решения могут быть не совместимы с этими условиями и должны быть исключены. Последний шаг в работе алгоритма — это исключение тех q, которые не являются степенями простых чисел. Это также можно сделать за полиномиальное время. Действительно, для данного q можно найти наименьшее r такое, что q является степенью r, за время, полиномиально зависящее от $\log q$. Хорошо известно, что проверка простоты числа может быть проведена за полиномиальное время [23]. Лемма доказана. □

Лемма 3.4.3. *Пусть k — натуральное число. Существует алгоритм, который по данному множеству натуральных чисел $\mathcal{M}$, выдает конечную простую группу G лие-*

[2]В случае групп ${}^2G_2(q)$, f является многочленом не от q, а от $\sqrt{q}$. Однако, это не мешает применить дальнейшее рассуждение к этим группам.

ва типа лиева ранга k такую, что $\omega(G) = \omega(\mathcal{M})$, или говорит, что такой группы не существует. Время работы алгоритма ограничено полиномом от $m \log M$.

Доказательство. Без ограничения общности можно считать, что $\mathcal{M} = \mu(\mathcal{M})$. Если группа G с $\omega(G) = \omega(\mathcal{M})$ существует, то $m \leqslant f(k)$, где функция f определена в лемме 3.1.10. Следовательно, если $m > f(k)$, то такой группы не существует.

Сначала предположим, что $\mathcal{M} = \mu(G)$ для группы G над полем нечетной характеристики. Согласно лемме 3.4.2 можно получить список конечных простых групп H лиева типа над полями нечетных характеристик таких, что $m_1(H) = M$. По лемме 3.1.10 минимальные спектры этих групп могут быть вычислены за полиномиальное время. Если один из минимальных спектров совпадает с $\mu(\mathcal{M})$, то алгоритм выдает соответствующую группу. В противном случае можно считать, что характеристика поля определения группы G равна 2. В этом случае лемма 3.1.9 влечет, что порядок поля определения группы q не превосходит $2M-1$, и следовательно, количество вариантов для q не превосходит $\log_2(2M+1)$ вне зависимости от лиева типа группы G. Теперь лемма следует из леммы 3.1.10. □

Лемма 3.4.4. *Существует алгоритм, который по заданному простому числу p и натуральным числам k и A, выдает конечную простую классическую группу G лиева ранга k и характеристики p такую, что A лежит в $\mu(G)$ и некоторый простой делитель числа A не смежен с p в графе $\mathrm{GK}(G)$, или говорит, что такой группы не существует. Время работы алгоритма полиномиально зависит от $k \log(pA)$*

Доказательство. Из леммы 3.1.7 следует, что если такая группа G существует, то число A должно быть равно одному из выражений $f(q)$ из второго столбца таблицы 17. Число получаемых уравнений ограничено полиномом от k. Поскольку корни каждого из полиномов $f(q)$ лежат в единичной окружности, целые решения этих уравнений могут быть найдены за время, ограниченное полиномом от $k \log A$. Время необходимое для проверки, являются ли полученные решения степенями числа p, ограничено полиномом от $\log(pA)$, что завершает доказательство. □

В следующей лемме мы используем обозначение $\zeta(G)$, введенное в лемме 3.1.7. Напомним, что $t(G)$ обозначает максимальный размер коклики в $\mathrm{GK}(G)$ и $\mathrm{AD}(G)$.

Лемма 3.4.5. *Пусть p — простое число, $t \geqslant 5$ — натуральное число, $\mathcal{S}$ — конечное множество натуральных чисел, взаимно простых с p, и $S = \max \mathcal{S}$. Существует алгоритм, который по заданным p, t и $\mathcal{S}$ выдает множество конечных простых классических групп G с $\mathrm{prk}(G) \geqslant 8$ над полем характеристики p, у которых $t(G) = t$ и $\zeta(G) = \mathcal{S}$. Это множество либо пусто, либо состоит из одного элемента, либо равно $\{S_{2n}(q), O_{2n+1}(q)\}$, где n четно, либо равно $\{S_{2n}(q), O_{2n+1}(q), O^+_{2n+2}(q)\}$, где n нечетно. Время работы алгоритма ограничено полиномом от $t \log(pS)$.*

Доказательство. По лемме 3.1.6 если G — конечная классическая группа данного типа, то $t(G)$ является линейной функцией лиева ранга группы G. Более того, значения $t(G)$ могут совпадать только для двух последовательных значений лиева ранга.

Из леммы 3.1.7 следует, что если $|\mathcal{S}| > 3$, то группы G не существует.

Если $|\mathcal{S}| = 1$, то группа G изоморфна $S_{2n}(q)$ или $O_{2n+1}(q)$ для четного n по лемме 3.1.7. В частности, число n определено однозначно. Порядок поля q может быть найден из уравнения $\frac{q^n+1}{(2,q-1)} = S$ согласно лемме 3.1.7. Целые решения этого уравнения вычисляются за полиномиальное время.

Если $|\mathcal{S}| = 3$, то $G = O^-_{2n}(q)$ для четного n. Следовательно, n определено однозначно, при этом q удовлетворяет равенству $[q^{n-1} - 1, q + 1] = S$. Если q определено, то легко проверяется совпадают ли $\mathcal{S}$ и $\zeta(G)$.

Предположим, что $|\mathcal{S}| = 2$. По лемме 3.1.7 равенство $\zeta(G) = \mathcal{S}$ может рассматриваться как система уравнений относительно переменной q, в которой лиев тип и лиев ранг группы G являются параметрами. Как и ранее, эта система может быть решена за полиномиальное время. Покажем, что существует не более трех решений этой системы для всех выборов значений параметров и все случаи, когда количество решений больше одного, перечислены в формулировке леммы.

Далее через $e(n, r)$ обозначается мультипликативный порядок числа n по модулю r, где r и n — взаимно простые целые числа.

Пусть $\mathcal{S} = \{s_1, s_2\}$. Предположим, что $q = p^\alpha$ — это решение системы $\zeta(G) = \mathcal{S}$ для некоторого выбора параметров. Обозначим через m_1 и m_2 максимумы значений функции $e(q, r)$, где r пробегает простые делители чисел s_1 и s_2 соответственно. По лемме 3.1.7 пара m_1, m_2 — это одна из пар второго столбца таблицы 21. Третий столбец этой таблицы содержит отношения m_1/m_2 в предположении, что $m_1 < m_2$. Заметим, что это отношение зависит только от p, s_1 и s_2 и не зависит от q. Действительно, по лемме 3.1.2 существую простые делители чисел $\Phi^*_{m_1}(q)$ и $\Phi^*_{m_2}(q)$, делящие $\Phi^*_{m_1\alpha}(p)$ и $\Phi^*_{m_2\alpha}(p)$. Следовательно, $m_1\alpha$ и $m_2\alpha$ являются максимумами значений $e(p, r)$, где r пробегает множества $\pi(s_1)$ и $\pi(s_2)$ соответственно.

Таблица 21. Числа m_1 и m_2

Группа	m_1, m_2	m_1/m_2
$L_n(q)$	$n-1$, n	$\frac{n-1}{n}$
$U_n(q)$, n четно	n, $2n-2$	$\frac{n}{2n-2}$
$U_n(q)$, n нечетно	$2n$, $n-1$	$\frac{n-1}{2n}$
$S_{2n}(q)$, $O_{2n+1}(q)$, n нечетно	n, $2n$	$\frac{1}{2}$
$O^+_{2n}(q)$, n четно	$n-1$, $2n-2$	$\frac{1}{2}$
$O^+_{2n}(q)$, n нечетно	n, $2n-2$	$\frac{n}{2n-2}$
$O^-_{2n}(q)$, n нечетно	$2n-2$, $2n$	$\frac{n-1}{n}$

Пусть F — это множество функций переменной x, состоящее из $\frac{1}{2}$, $\frac{x-1}{x}$, $\frac{x}{2x-2}$, $\frac{x-1}{2x}$. Следующее утверждение доказывается прямой проверкой.

Если f_1, $f_2 \in F$ и n, m — натуральные числа такие, что $f_1(n) = f_2(m)$, то $f_1 = f_2$ и $n = m$, или $f_1 = f_2 = \frac{1}{2}$, или f_1, f_2, n и m перечислены в таблице 22.

Таким образом, лиев ранг группы G данного лиева типа однозначно определяется

Таблица 22. Исключительные f_1, f_2, n и m

f_1	f_2	n	m
$\frac{x-1}{x}$	$\frac{1}{2}$	2	любое
$\frac{x-1}{x}$	$\frac{x}{2x-2}$	3	4
$\frac{x-1}{x}$	$\frac{x-1}{2x}$	1	1

исходными данными, и либо есть единственный кандидат для группы G, либо выполнено одно из утверждений:

(1) $G \in \{S_{2n}(q), O_{2n+1}(q), O^+_{2n+2}(q)\}$, n нечетно;

(2) $G \in \{L_n(q^2), O^-_{2n}(q)\}$, n нечетно.

При этом, $t(L_n(q^2)) = \left\lfloor \frac{n+1}{2} \right\rfloor$ и $t(O^-_{2n}(q))) = \left\lfloor \frac{3n+4}{4} \right\rfloor$ (см. таблица 16). Следовательно, равенство $t(G) = t$ не может быть выполнено для обеих групп и случай (2) невозможен, что завершает доказательство леммы. □

§ 3.5. Доказательство теоремы 15

Поскольку множество $\mu(\mathcal{M})$ строится по $\mathcal{M}$ за время, полиномиально зависящее от $m \log M$, далее будем считать, что $\mathcal{M} = \mu(\mathcal{M})$.

Предположим, что конечная простая неабелева группа G, удовлетворяющая равенству $\mu(G) = \mathcal{M}$, существует. Число спорадических групп конечно. Знакопеременные группы разобраны в лемме 3.4.1, в то время как в лемме 3.4.3 рассмотрены группы лиева типа ограниченного лиева ранга. Следовательно, можно считать что группа G — это группа лиева типа, чей ранг превосходит некоторую константу k (для наших целей будет достаточно взять $k = 12$); в частности, G — классическая группа.

Первой задачей является определение возможных значений лиева ранга группы G. По лемме 3.2.4 существует алгоритм с полиномиальным временем работы, который строит $\mathrm{AD}(\mathcal{M})$ при условии, что количество атомарных делителей множества $\mathcal{M}$ не превосходит числа $C(M)$, определенного в лемме 3.3.3, либо говорит, что это условие не выполнено. По лемме 3.3.3 в последнем случае $\mathcal{M}$ не может быть равно $\mu(G)$.

Согласно лемме 3.1.13 существует полиномиальный алгоритм, который проверяет является ли граф $\mathrm{AD}(\mathcal{M})$ расщепляемым. Если не является, то лемма 3.3.2 влечет, что $\mathrm{AD}(\mathcal{M}) \neq \mathrm{AD}(G)$ и алгоритм завершает работу. В противном случае из той же леммы следует, что максимальная коклика графа $\mathrm{AD}(\mathcal{M})$ может быть найдена за полиномиальное время.

Из лемм 3.1.6 и 3.3.1 следует, что если зафиксировать лиев тип группы G, то размер максимальной коклики графа $\mathrm{AD}(\mathcal{M})$ определяет лиев ранг группы G с точностью до двух последовательных значений.

Теперь, когда лиев ранг G “почти определен”, мы определим характеристику группы G.

Согласно лемме 3.3.5, если характеристики группы G равна 2, то $t^*(4, G) \geqslant 3$, и $t^*(4, G) < 3$ в противном случае. Более того, по этой лемме число $t^*(4, G)$ равно количеству нечетных вершин v графа $\mathrm{AD}(G)$, для которых $4v \notin \omega(G)$. Следовательно, можно найти вершины графа $\mathrm{AD}(\mathcal{M})$, удовлетворяющие этому условию. Если их число больше либо равно 3, то характеристика группы G равна 2, в противном случае характеристика нечетна.

Если характеристика нечетна, то из леммы 3.4.2 следует, что полный список простых классических групп H, у которых максимальный порядок элемента равен M, может быть получен за полиномиальное время. Напомним, что по лемме 3.1.8 три максимальных порядка элементов конечной простой группы лиева типа однозначно определяют его характеристику. Используя [69, таблицы 1, A.1-A.6], содержащие выражения для $m_1(H)$, $m_2(H)$ и $m_3(H)$ (последнее только для случаев, когда двух максимальных элементов не достаточно), можно вычислить эти элементы для всех групп из списка. Заметим, что согласно этим таблицам множества соответствующих $m_i(H)$ являются подмножествами в $\mu(H)$ во всех интересующих нас случаях (это не так только при $H = L_2(q)$ и $H = O_8^+(q)$). Таким образом, те группы H, у которых вычисленные числа не являются тремя максимальными элементами множества $\mathcal{M}$, исключаются из списка. Остальные группы должны иметь характеристику, равную характеристике группы G.

После того, как характеристика группы G найдена, применяется алгоритм из леммы 3.4.5. Если этот алгоритм выдает более одной группы, то лемма 3.1.12 позволяет оставить единственного кандидата.

Остается проверить включение $\mathcal{M} \subseteq \omega(G)$. Согласно описанию спектров конечных классических групп [1, 2], каждый элемент множества $\mu(G)$ либо имеет вид, описанный в лемме 3.1.3, либо равен одному из полиномов от q из фиксированного списка. Степени полиномов в обоих случаях ограничены линейной функцией от лиева ранга группы G. Следовательно, для каждого элемента $\mathcal{M}$ можно проверить, имеет ли он требуемый вид, за полиномиальное время, в частности, можно проверить, является ли $\mathcal{M}$ подмножеством в $\omega(G)$. Теорема доказана.

4. Холловы подгруппы конечных групп

Пусть π — это некоторое множество простых чисел. Будем обозначать через π' дополнение к π в множестве всех простых чисел. Напомним, что подгруппа H конечной группы G называется π-холловой, если ее порядок $|H|$ является π-числом (т.е. все простые делители порядка группы H лежат в π), а индекс $|G : H|$ — это π'-число. Подгруппа, являющаяся π-холловой для некоторого множества простых чисел π, называется холловой подгруппой.

Основной целью данной главы является доказательство следующего результата.

Теорема 16. *Пусть G — конечная группа и π — это некоторое множество простых чисел. Группа G содержит разрешимую π-холлову подгруппу тогда и только тогда, когда G содержит $\{p, q\}$-холлову подгруппу для любых $p, q \in \pi$.*

Кроме того, в последнем параграфе данной главы мы построим пример группы с неизоморфными p-дополнениями.

§ 4.1. Предварительные сведения и обозначения

Субнормальная подгруппа A группы G называется атомом, если она совершенна, т.е. совпадает со своим коммутантом, и содержит единственную максимальную нормальную подгруппу, которая обозначается как A^*. Будем обозначать через $\mathcal{A}(G)$ множество атомов группы G.

Если H/K — некоторая секция группы G, то нормализатор $N_G(H/K)$ секции H/K в G — это пересечение $N_G(H) \cap N_G(K)$, а его образ в группе автоморфизмов $Aut(H/K)$ называется группой индуцированных автоморфизмов и обозначается $Aut_G(H/K)$. Если $K = 1$, то вместо $Aut_G(H/K)$ мы будем использовать введенное ранее обозначение $Aut_G(H)$.

Лемма 4.1.1. [59, леммы 2.1–2.3] *Пусть H/K — неабелев композиционный фактор конечной группы G.*

1) *Существует единственная подгруппа $A \in \mathcal{A}(G)$ такая, что $H = AK$. Более того, $A^* = H \cap K$, $H/K \cong A/A^*$, $N_G(H/K) \leqslant N_G(A)$ и $Aut_G(H/K)$ изоморфна группе L, где*

$$Inn(A/A^*) \leqslant L \leqslant Aut_G(A/A^*).$$

2) $G^{(\infty)} = \langle A | A \in \mathcal{A}(G) \rangle$.

3) *Если $A \in \mathcal{A}(G)$ и $A \leqslant \langle H_1, \ldots, H_m \rangle$, где $H_1, \ldots, H_m$ — субнормальные подгруппы группы G, то $A \leqslant H_i$ для некоторого i.*

Следуя Ф. Холлу [62], мы будем говорить, что G обладает свойством

E_π: если группа G содержит π-холлову подгруппу;

C_π: если группа обладает свойством E_π и все π-холловы подгруппы сопряжены;

D_π: если группа обладает свойством C_π и произвольная π-подгруппа содержится в π-холловой.

В качестве эквивалента выражения «группа G обладает свойством E_π» будем также использовать выражение «G является E_π-группой», а также запись «$G \in E_\pi$» (аналогично для свойств C_π и D_π). Кроме того, E_π^s, C_π^s и D_π^s обозначают аналогичные свойства разрешимых π-подгрупп.

Лемма 4.1.2. *Пусть M — нормальная подгруппа группы G, H — некоторая надгруппа группы M в G. Предположим, что $G \in E_\pi^s$, $H/M \in E_\pi$ и $G/M \in D_\pi$. Тогда H содержит разрешимую π-холлову подгруппу. Более того, существует разрешимая π-холлова подгруппа A группы G такая, что $A \cap H$ — разрешимая π-холлова подгруппа группы H.*

Доказательство. Следует из доказательства леммы 3.1 в [59]. □

Следующее утверждение непосредственно вытекает из леммы 4.1.2.

Следствие 4.1.3. *Пусть $G \in E_\pi^s$ и $G^{(\infty)} \leqslant H \leqslant G$. Тогда $H \in E_\pi^s$.*

Следствие 4.1.4. *Пусть $A \in \mathcal{A}(G)$, $A \leqslant H \leqslant G$ и $Aut_G(A/A^*) \in E_\pi^s$. Тогда $Aut_H(A/A^*) \in E_\pi^s$.*

Доказательство. Поскольку группа внешних автоморфизмов $Out(A/A^*)$ разрешима, имеем

$$Aut_G(A/A^*)^{(\infty)} \leqslant Inn(A/A^*) = Aut_A(A/A^*) \leqslant Aut_H(A/A^*).$$

Применение следствия 4.1.3 к группе $Aut_G(A/A^*)$ завершает доказательство. □

Лемма 4.1.5. *Пусть $M \trianglelefteq G$. Если $M \in C_\pi^s$ и $G/M \in E_\pi^s$, то $G \in E_\pi^s$.*

Доказательство. Без ограничения общности можем считать, что группа G/M — разрешимая π-группа. Пусть A — это разрешимая π-холлова подгруппа группы G. По аргументу Фраттини $G = MN_G(A)$. Группа $N_G(A)$ является π-разрешимой. Следовательно, $N_G(A) \in D_\pi^s$. □

Лемма 4.1.6. [85, лемма 2.1(e)] *Пусть G — конечная группа, $A \trianglelefteq G$, $\pi(G/A) \subseteq \pi$, и M — π-холлова подгруппа A. Тогда G содержит π-холлову подгруппу H такую, что $H \cap A = M$, тогда и только тогда, когда $M^A = M^G$.*

Лемма 4.1.7. *Пусть $M \trianglelefteq G$, G/M — π-группа, и $M = S_1 \times \cdots \times S_n$, где $S_1, \ldots, S_n$ — класс сопряженности подгрупп в G. Пусть $N = N_G(S_1)$ и $K = S_2 \times \cdots \times S_n$, а L — подгруппа в N такая, что L/C — разрешимая π-холлова подгруппа в N/C. Тогда существует π-холлова подгруппа H в G такая что $G = HM$, $H \cap S_1 = L \cap S_1$, $L = (H \cap N)K$, $H \cap M = (H \cap S_1) \times \cdots \times (H \cap S_n)$.*

Доказательство. Следует доказательству [59, теорема 3.4]. □

Лемма 4.1.8. [62, теорема A4] *Пусть S_n — симметрическая группа, $p < q$ — простые числа. Тогда $S_n \in E_{\{p,q\}}$ тогда и только тогда, когда $p = 2$, $q = 3$ и $n \in \{3, 4, 5, 7, 8\}$.*

Лемма 4.1.9. [21, теорема 3.3] *Пусть G — конечная группа лиева типа над полем*

характеристики p и π — множество простых чисел такое, что $p \in \pi$. Если H — π-холлова подгруппа группы G, то H либо содержится в подгруппе Бореля, либо является параболической подгруппой группы G.

Лемма 4.1.10. [61, теорема 4.9] *Пусть G — классическая группа над полем характеристики p и π — множество простых чисел такое, что $2, p \notin \pi$. $G \in E_\pi$ тогда и только тогда, когда $G \in E_{\{r,s\}}$ для любых $r, s \in \pi$.*

Лемма 4.1.11. [60, теорема A] *Если π — некоторое множество простых чисел и $2 \notin \pi$, то $E_\pi = C_\pi$.*

Если q — степень нечетного простого числа p, то $\varepsilon \in \{+1, -1\}$ определяется сравнением $q \equiv \varepsilon \pmod 4$. Также ε обозначает соответствующий символ из $\{+, -\}$.

Лемма 4.1.12. [80, теорема 8.9] *Пусть G — простая группа лиева типа над полем характеристики p и π — множество простых чисел такое, что $2 \in \pi$ и $3, p \notin \pi$, и t — произвольный элемент из $\pi \setminus \{2\}$. Группа G обладает свойством E_π тогда и только тогда, когда либо $G = {}^2G_2(q)$ и $\pi = \{2, 7\}$, либо выполняются условия:*

(1) *$\pi \subseteq \pi(q - \varepsilon)$;*

(2) *если G — одна из групп $PSL_n^\pm(q)$, $PSp_{2n}(q)$, $P\Omega_{2n}^\pm(q)$, то $n < t$;*

(3) *если $G = PSL_n^{-\varepsilon}(q)$, то $(n + 1)/2 < t$;*

(4) *если $G = P\Omega_{2n}^{-\varepsilon}(q)$, то $n - 1 < t$ и n нечетно;*

(5) *если $G = E_6^{-\varepsilon}(q)$, то $5 \notin \pi$;*

(6) *если $G = E_7(q)$ или $G = E_8(q)$, то $5, 7 \notin \pi$.*

Кроме того, при $|\pi| \geqslant 3$ каждая π-холлова подгруппа H группы G обладает нормальным 2-дополнением и все π-холловы подгруппы сопряжены в G.

Напомним, что для взаимно простых целых чисел n и r через $e(n, r)$ обозначается мультипликативный порядок числа n по модулю r.

Лемма 4.1.13. *Пусть G — одна из групп $PSL_n^\pm(q)$ или $PSp_{2n}(q)$, где q — степень простого числа p, а s — простое число такое, что $s \notin \{2, p\}$ и $s \in \pi(q - \varepsilon)$. Группа G обладает свойством $E_{\{3,s\}}$ тогда и только тогда, когда выполнено одно из условий:*

(1) *$G = PSL_n(q)$, $e(q, 3) = e(q, s) = a$ и $n < as$;*

(2) *$G = PSL_3(q)$, $e(q, 3) = 2$, $e(q, s) = 1$ и $(q^2 - 1)_3 = 3$;*

(3) *$G = PSL_n^-(q)$, $e(q, 3) = e(q, s)$ и $n < 2s$;*

(4) *$G = PSL_3^-(q)$, $e(q, 3) = 1$, $e(q, s) = 2$ и $(q^2 - 1)_3 = 3$;*

(5) *$G = PSp_{2n}(q)$, $e(q, 3) = e(q, s)$ и $n < s$.*

Доказательство. Лемма является непосредственным следствием из [61, теоремы 4.1, 4.3, 4.5]. □

§ 4.2. Сведение к почти простым группам

Первым шагом в нашем доказательстве критерия существования разрешимой хол-

ловой подгруппы является сведение общей ситуации к случаю почти простой группы. В работе [59] Ф. Гросс получил достаточное условие существования π-холловой подгруппы в конечной группе в терминах свойств групп индуцированных автоморфизмов секций некоторого ее композиционного ряда. Однако, оно не позволяет установить существование разрешимой π-холловой подгруппы в конечной группе. Следующая теорема является частичным аналогом теоремы Ф. Гросса для случая разрешимых холловых подгрупп.

Теорема 17. *Пусть G — конечная группа и π — некоторое множество простых чисел. Пусть композиционный ряд*

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n = G$$

является уплотнением главного ряда группы G. Если группа индуцированных автоморфизмов $Aut_G(G_i/G_{i-1})$ обладает разрешимой π-холловой подгруппой для любого $1 \leqslant i \leqslant n$, то группа G обладает разрешимой π-холловой подгруппой.

Сначала мы докажем следующее утверждение.

Предложение 4.2.1. *Пусть $M \trianglelefteq G$ и предположим, что M, $G/M \in E_\pi^s$, но $G \notin E_\pi^s$. Тогда существует неабелев композиционный фактор H/K в G такой, что $H \leqslant M$ и $K \trianglelefteq G$, при этом $H/K \in E_\pi^s$, но $Aut_G(H/K) \notin E_\pi^s$.*

Доказательство. Рассмотрим контрпример, для которого число $|G| + |M|$ минимальное. Пусть L — нормальная подгруппа группы G такая, что $L < M$ и M/L — минимальная нормальная подгруппа в G/L. По условию $M \in E_\pi^s$ и, значит, $L \in E_\pi^s$ по [62, лемма 1].

Если $G/L \in E_\pi^s$, то получаем противоречие с минимальностью контрпримера заменой M на L. Если $G/L \notin E_\pi^s$, то получаем противоречие с минимальностью контрпримера факторизацией групп G и M по L. Следовательно, $L = 1$, и M — главный фактор группы G.

Лемма 4.1.5 влечет, что $M \notin C_\pi$, поскольку если $G/M \in E_\pi^s$, то $G \in E_\pi^s$. Следовательно, M неразрешима. Значит, $M = S_1 \times \cdots \times S_n$, где $\{S_1, \ldots, S_n\}$ — класс сопряженности подгрупп в G, и для каждого i группа S_i является неабелевым композиционным фактором группы G. Поскольку $G \in E_\pi^s$, получаем, что $S_i \in E_\pi^s$ для каждого i.

Если $Aut_G(S_i) \notin E_\pi^s$ для некоторого i, то предложение справедливо для $K = 1$ и $H = S_i$. Следовательно, можно считать, что $Aut_G(S_i) \in E_\pi^s$ для всех i. Из следствия 4.1.4 вытекает, что $Aut_A(S_i) \in E_\pi^s$ для любой подгруппы A такой, что $M \leqslant A \leqslant G$. Тогда $A \in E_\pi^s$ для любой собственной подгруппы A такой, что $A/M \in E_\pi^s$, иначе заменой G на A получим контрпример к теореме. Но $G/M \in E_\pi^s$. Если A/M — π-холлова подгруппа группы G/M, то $A \in E_\pi^s$ тогда и только тогда, когда $G \in E_\pi^s$, что противоречит условию теоремы. Значит, G/M — это π-группа.

Пусть $S = S_1$, $K = S_2 \times \cdots \times S_n$, $N = N_G(S)$ и $C = C_G(S)$. Пусть L/C — разрешимая π-холлова подгруппа группы N/C. Поскольку G/M — π-группа, получаем, что $N = LM$. По лемме 4.1.7 группа G содержит π-холлову подгруппу B такую, что $G = BM$, $L = (B \cap N)K$,

$B \cap S = L \cap S$ и $B \cap M = (B \cap S_1) \times \cdots \times (B \cap S_n)$.

Рассмотрим подгруппу $(L \cap S)C/C$ группы L/C. Эта подгруппа изоморфна

$$(L \cap S)/(L \cap S \cap C),$$

но $S \cap C = 1$. Значит, $B \cap S = L \cap S$ — разрешимая π-холлова подгруппа группы S. Поскольку $G/M = BM/M \in E_\pi^s$, группа B разрешима и $G \in E_\pi^s$, что противоречит условию. □

Теперь мы докажем теорему 17.

Доказательство. Доказательство проведем индукцией по $|G|$. Из [59, лемма 2.5] следует, что $Aut_G(A/A^*) \in E_\pi^s$ для всех $A \in \mathcal{A}(G)$. Пусть M — минимальная нормальная подгруппа G. Из [59, лемма 2.4] вытекает, что $Aut_{G/M}(A/A^*) \in E_\pi^s$ для всех $A \in \mathcal{A}(G/M)$. По предположению индукции $G/M \in E_\pi^s$. Если M абелева, то $G \in E_\pi^s$ по лемме 4.1.5. Если M неабелева, то $M = A_1 \times \cdots \times A_n$, где A_i — неабелева простая группа. Тогда $A_i \in \mathcal{A}(G)$ для всех i. Поскольку $Aut_G(A_i) \in E_\pi^s$ и $Inn(A_i) \trianglelefteq Aut_G(A_i)$, получаем, что $A_i \in E_\pi^s$ и, значит, $M \in E_\pi^s$. По предложению 4.2.1 имеем $G \in E_\pi^s$, и теорема доказана. □

§ 4.3. Случай простых групп

Предложение 4.3.1. *Пусть S — конечная простая группа и π — некоторое множество простых чисел такое, что $|\pi \cap \pi(S)| \geqslant 3$. Группа S содержит $\{p, q\}$-холлову подгруппу для любых p, $q \in \pi$ тогда и только тогда, когда S содержит разрешимую π-холлову подгруппу. Кроме того, все классы сопряженности таких подгрупп инвариантны относительно группы автоморфизмов.*

Доказательство. Если S — знакопеременная группа, то по лемме 4.1.8 группа S не содержит бипримарных холловых подгрупп, кроме $\{2, 3\}$-холловых, и в этом случае доказывать нечего. Пусть S — простая группа лиева типа над полем характеристики p. Рассмотрим случай, когда $p \in \pi$.

Ввиду леммы 4.1.6 это предложение доказывает теорему 16 в случае почти простой группы G с цоколем S при условии, что $\pi \cap \pi(S)$ содержит не менее трех элементов.

Предложение 4.3.2. *Пусть S — конечная простая группа лиева типа над полем характеристики p, B — подгруппа Бореля группы S и π — множество простых чисел такое, что $p \in \pi$. Если $|\pi \cap \pi(S)| \geqslant 3$ и группа S содержит $\{r, s\}$-холлову подгруппу для любых $r, s \in \pi$, то $|S|_\pi = |B|_\pi$.*

Доказательство. Положим $\pi^* = (\pi \cap \pi(S)) \setminus \{p\}$. По лемме 4.1.9 для доказательства предложения нужно показать, что ни одна из $\{r, s\}$-холловых подгрупп группы S не может быть параболической.

Предположим противное, т.е. что $\{p, r\}$-холлова подгруппа является параболической для некоторого $r \in \pi^*$. Тогда $\{p, s\}$-холлова подгруппа является параболической для любого $s \in \pi^*$. Действительно, по лемме 4.1.9 если $\{p, s\}$-холлова подгруппа не является

параболической, то она содержится в подгруппе Бореля, и, следовательно, в любой параболической, в частности, в $\{p, r\}$-холловой параболической подгруппе, что невозможно.

Однако, порядок произвольной параболической подгруппы, отличной от подгруппы Бореля, делится на 6; противоречие. □

Таким образом, если $S \in E_{\{r,s\}}$ для любых $r, s \in \pi$, то π-холлова подгруппа H группы S содержится в подгруппе Бореля, а значит, H разрешима. Поскольку все подгруппы Бореля сопряжены, сопряжены и все разрешимые π-холловы подгруппы.

Следующие леммы полностью покрывают случай, когда характеристика поля p не лежит в π.

Лемма 4.3.3. *Пусть G — простая группа лиева типа над полем характеристики p и π — множество простых чисел такое, что $2, p \notin \pi$. Группа G обладает свойство E_π тогда и только тогда, когда $G \in E_{\{r,s\}}$ для любых $r, s \in \pi$. Кроме того, все разрешимые π-холловы подгруппы сопряжены в G.*

Доказательство. Сопряженность π-холловых подгрупп в данном случае доказана в лемме 4.1.11.

Если G — классическая группа, то утверждение выполнено по лемме 4.1.10.

Пусть G — группа Ри или Сузуки. Тогда G удовлетворяет E_π в случае, если $\pi \cap \pi(G)$ содержится в одном из множеств, указанных в таблице 23 (согласно [11, лемма 14]).

Таблица 23

G	$\pi \cap \pi(G) \subseteq$
${}^2B_2(2^{2n+1})$	$\pi(2^{2n+1}-1)$
	$\pi(2^{2n+1} \pm 2^{n+1}+1)$
${}^2G_2(3^{2n+1})$	$\pi(3^{2n+1}-1)$
	$\pi(3^{2n+1} \pm 3^{n+1}+1)$
${}^2F_4(2^{2n+1})$	$\pi(2^{2(2n+1)} \pm 1)$
	$\pi(2^{2n+1} \pm 2^{n+1}+1)$
	$\pi(2^{2(2n+1)} \pm 2^{3n+2} \mp 2^{n+1}-1)$
	$\pi(2^{2(2n+1)} \pm 2^{3n+2} + 2^{2n+1} \pm 2^{n+1}-1)$

Прямые вычисления показывают, что соответствующие множества простых делителей пересекаются тривиально. В силу этого утверждение леммы в обратную сторону верно.

В случае, если G — одна из групп ${}^3D_4(q)$, $E_6^{\pm}(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, $G_2(q)$, то согласно [11, леммы 7–12] G удовлетворяет E_π тогда и только тогда, когда выполняются условия:

(1) Для $r = \min(\pi \cap \pi(G))$ и любого $s \in \pi \cap \pi(G) \setminus \{r\}$ выполнено $e(q, r) = e(q, s)$;

(2) Если $G = E_6^{\pm}(q)$, то $(q \mp 1)_\pi \not\equiv 0 \pmod{15}$;

(3) Если $G = E_7(q)$, то $e(q, r) = 1$ и $(q-1)_\pi$ не делится на 15, 21 и 35;

(4) Если $G = E_8(q)$, то $e(q, r) = 2$ и $(q+1)_\pi$ не делится на 15, 21 и 35.

Ясно, что условие (1) выполняется для любой пары $r, s \in \pi$ тогда и только тогда, когда оно выполняется для всего π.

Пусть $G = E_7(q)$. Условие, что $(q-1)_{\{r,s\}}$ не делится на 15, 21 и 35, выполнено для любых $r, s \in \pi$ тогда и только тогда, когда π содержит не более одного элемента из $\{3, 5, 7\}$. Тогда $(q-1)_\pi \not\equiv 0 \pmod{k}$ для $k \in \{15, 21, 35\}$.

Условия для $G = E_6^{\pm}(q)$ и $G = E_8(q)$ проверяются аналогично. □

Лемма 4.3.4. *Пусть G — простая группа лиева типа над полем характеристики p, и π — множество простых чисел такое, что $2 \in \pi$ и $3, p \notin \pi$. Тогда $G \in E_\pi^s$ тогда и только тогда, когда $G \in E_{\{r,s\}}$ для любых $r, s \in \pi$. Кроме того, все разрешимые π-холловы подгруппы сопряжены в G.*

Доказательство. По лемме 4.1.12 в этом случае $G \in E_{\{r,s\}}$ для любых $r, s \in \pi$ тогда и только тогда, когда $G \in E_\pi$. Кроме того, при $|\pi| \geq 3$ каждая π-холлова подгруппа H группы G обладает нормальным 2-дополнением и, следовательно, разрешима. При этом, при $|\pi| \geqslant 3$ все π-холловы подгруппы сопряжены в G согласно той же лемме. □

Пусть η обозначает некоторый символ множества $\{+, -, \circ\}$, где $\circ$ — пустой символ. Причем если $\eta \in \{+, -\}$, то число $\eta 1$ также обозначается как η.

Лемма 4.3.5. *Пусть G — простая группа лиева типа над полем характеристики p, π — множество простых чисел такое, что $2, 3 \in \pi$ и $p \notin \pi$. Тогда $G \in E_\pi^s$ тогда и только тогда, когда $G \in E_{\{r,s\}}$ для любых $r, s \in \pi$. Кроме того, если $|\pi \cap \pi(G)| > 2$, то классы сопряженности разрешимых π-холловых подгрупп инвариантны относительно группы автоморфизмов.*

Доказательство. Положим $\tau = \pi \setminus \{2, 3\}$. Можем считать, что τ непусто. Далее s обозначает произвольный элемент из τ.

Пусть $G = PSL_2^\eta(q)$. Поскольку $G \in E_{\{2,s\}}$, из леммы 4.1.12 следует, что s лежит в $\pi(q - \varepsilon)$. Если 3 делит $q - \varepsilon$, то по [85, лемма 3.11] группа G содержит разрешимую π-холлову подгруппу и все такие подгруппы сопряжены. Пусть 3 не делит $q - \varepsilon$ и G содержит $\{3, s\}$-холлову подгруппу. Согласно лемме 4.1.13, если $PSL_2^{\pm}(q)$ содержит $\{3, s\}$-холлову подгруппу, то $e(q, 3) = e(q, s)$, что с учетом условия $s \in \pi(q - \varepsilon)$ противоречит предположению о том, что 3 не делит $q - \varepsilon$.

Пусть $G = PSL_n^\eta(q)$ для $n > 2$. По [85, лемма 4.3] для того, чтобы показать, что $G \in E_\pi^s$, достаточно показать, что выполняется одно из двух условий:

(А) либо $q \equiv \eta \pmod{12}$, либо $n = 3$ и $q \equiv \eta \pmod{4}$; $S_n \in E_\pi$; $\pi \cap \pi(G) \subseteq \pi(q - \eta) \cup \pi(n!)$; если $r \in \pi \cap \pi(n!) \setminus \pi(q - \eta)$, то $|G|_r = |S_n|_r$.

Кроме того, π-холлова подгруппа в этом случае содержится в проективном образе подгруппы M, которая изоморфна $Z^{n-1}.S_n$, где $Z = GL_1^\eta(q)$, и все π-холловы подгруппы этого типа сопряжены (мы пишем $G{=}N.H$, если N — нормальная подгруппа G такая, что группа G/N изоморфна H).

(Б) $q \equiv -\eta \pmod{3}$; $S_m \in E_\pi$, $m = \left\lfloor \frac{n}{2} \right\rfloor$; $GL_2^\eta(q) \in E_\pi$; $\pi \cap \pi(G) \subseteq \pi(q^2 - 1)$.

Кроме того, π-холлова подгруппа в этом случае содержится в проективном образе

подгруппы M, которая изоморфна

$$(GL_2^\eta(q) \circ \dots GL_2^\eta(q)).S_m \circ Z,$$

где Z — циклическая группа порядка $q - \eta$, если n нечетно, и тривиальная группа в противном случае (напомним, что $H \circ K$ обозначает центральное произведение групп H и K). При этом, все такие подгруппы M сопряжены в G и две π-холловы подгруппы в M сопряжены в G тогда и только тогда, когда они сопряжены в M.

Так как $G \in E_{\{2,s\}}$, из леммы 4.1.12 следует, что $\tau \subseteq \pi(q - \varepsilon)$, и либо $n < s$, либо $\eta = -\varepsilon$ и $\frac{n+1}{2} < s$. Поскольку $G \in E_{\{2,3\}}$, по [85, лемма 4.3] выполняется одно из следующих условий:

(1) $q \equiv \eta \pmod{12}$ или $n = 3$ и $q \equiv \eta \pmod 4$; $S_n \in E_{\{2,3\}}$; если $3 \notin \pi(q - \eta)$, то $|G|_3 = 3$;

(2) $q \equiv -\eta \pmod 3$; $S_m \in E_{\{2,3\}}$, где $m = \lfloor \frac{n}{2} \rfloor$; $GL_2^\eta(q) \in E_{\{2,3\}}$.

Пусть выполнено условие (1). Тогда $\eta = \varepsilon$, а значит, $n < s$. Следовательно, $S_n \in E_\pi$. Поскольку $s \in \pi(q - \varepsilon)$ для любого s из τ, имеем $(\pi \cap \pi(n!)) \setminus \pi(q - \eta) \subseteq \{3\}$. В последней формуле равенство возможно только если $n = 3$, в этом случае $|G|_3 = |S_3|_3 = 3$. Таким образом, выполняется условие (А), $G \in E_\pi^s$ и все π-холловы подгруппы данного типа сопряжены.

Пусть выполнено условие (2). По [85, лемма 3.2] из $GL_2^\eta(q) \in E_{\{2,3\}}$ следует, что $3 \in \pi(q - \varepsilon)$ или $(q^2 - 1)_{\{2,3\}} = 24$.

Пусть $3 \in \pi(q - \varepsilon)$. Так как $s \in \pi(q - \varepsilon)$, по [85, лемма 3.2] имеем $GL_2^\eta(q) \in E_\pi$ и все π-холловы подгруппы группы $GL_2^\eta(q)$ сопряжены. Заметим, что $q \equiv -\eta \pmod 3$ влечет $\eta = -\varepsilon$. Так как $\{3, s\} \subseteq \pi(q - \varepsilon)$, то $e(q, 3) = e(q, s)$ для любого s из τ. Поскольку $G \in E_{\{3,s\}}$, имеем $n < 2s$ по лемме 4.1.13. Тогда $m < s$, а значит, $S_m \in E_\pi^s$ и все π-холловы подгруппы группы S_m сопряжены (см. [12, теорема 8.1]). Итак, $q \equiv -\eta \pmod 3$, группы S_m и $GL_2^\eta(q)$ лежат в $E_\pi^s \cap C_\pi$ и $\pi \cap \pi(G) \subseteq \pi(q^2 - 1)$ (так как $s \in \pi(q - \varepsilon)$). Значит, выполняется условие (Б) и $G \in E_\pi^s$. Более того, из [62, теоремы С1 и С2] следует, что $M \in C_\pi$. Таким образом, все π-холловы подгруппы этого типа сопряжены в G.

Пусть $3 \notin \pi(q - \varepsilon)$ и $(q^2 - 1)_{\{2,3\}} = 24$. Из того, что 3 делит $q + \eta$, следует, что $\eta = \varepsilon$. В частности, $e(q, 3) \neq e(q, s)$, и из условия $G \in E_{\{3,s\}}$ по лемме 4.1.13 следует, что $n = 3$. Отсюда $\pi \cap \pi(G) \subseteq \pi(q - \eta) \cup \pi(n!)$ и $q \equiv \eta \pmod 4$. Также $(q + \eta)_3 = 3$ влечет $|G|_3 = 3$, значит, для любого $r \in (\pi \cap \pi(n!)) \setminus \pi(q - \eta) = \{3\}$ выполнено $|G|_r = |S_3|_r = 3$. Наконец, поскольку $S_3 \in E_\pi$, выполнено (Б). Кроме того, подгруппа M разрешима в этом случае и $G \in E_\pi^s$.

Пусть $G = PSp_{2n}(q)$. По [85, лемма 4.4] для доказательства того, что G обладает свойством E_π^s достаточно показать, что $S_n \in E_\pi$, $SL_2(q) \in E_\pi$ и $\pi \cap \pi(G) \subseteq \pi(q^2 - 1)$. В этом случае π-холловы подгруппы содержатся в проективном образе подгруппы M, изоморфной $Sp_2(q) \wr S_n$. Более того, две π-холловы подгруппы группы M сопряжены в G тогда и только тогда, когда они сопряжены в M, и все подгруппы M сопряжены в G.

Так как $G \in E_{\{2,s\}}$, по лемме 4.1.12 имеем $s \in \pi(q - \varepsilon)$ и $n < s$. Так как помимо

этого $G \in E_{\{3,s\}}$, по лемме 4.1.13 выполняется $e(q,3) = e(q,s)$, значит, $3 \in \pi(q-\varepsilon)$, и тогда $SL_2(q) \in E_\pi^s \cap C_\pi$ по [85, лемма 3.2]. Поскольку $G \in E_{\{2,3\}}$, из [85, лемма 4.4] следует, что $S_n \in E_{\{2,3\}}$, а так как $n < s$, получаем $S_n \in E_\pi^s \cap C_\pi$. Наконец, поскольку условие $\pi \cap \pi(G) \subseteq \pi(q^2-1)$ также выполняется, G обладает π-холловой подгруппой и все π-холловы подгруппы разрешимы и сопряжены в G.

Пусть $G = P\Omega_n^\eta(q)$ и $m = \left\lfloor \frac{n}{2} \right\rfloor$. По [85, лемма 6.7] для доказательства существования разрешимой π-холловой подгруппы достаточно показать, что выполнено одно из трех условий ниже.

(А) n — нечетное; $\pi \cap \pi(G) \subseteq \pi(q-\varepsilon)$; $q \equiv \varepsilon \pmod{12}$; $S_m \in E_\pi^s$.

(Б) n — четное; $\eta = \varepsilon^m$; $\pi \cap \pi(G) \subseteq \pi(q-\varepsilon)$; $q \equiv \varepsilon \pmod{12}$; $S_m \in E_\pi^s$.

(В) n — четное; $\eta = -\varepsilon^m$; $\pi \cap \pi(G) \subseteq \pi(q-\varepsilon)$; $q \equiv \varepsilon \pmod{12}$; $S_{m-1} \in E_\pi^s$.

Более того, все π-холловы подгруппы, появляющиеся в этих условиях, сопряжены в G.

По лемме 4.1.12 из условия $G \in E_{\{2,s\}}$ следует, что $s \in \pi(q-\varepsilon)$. Кроме того, $m < s$ либо если $\eta = -\varepsilon$, то m нечетно и $m - 1 < s$.

По [85, лемма 6.7] группа G является $E_{\{2,3\}}$-группой, если выполнено одно из условий $(1-5)$.

(1) $n = 2m+1$; $3 \in \pi(q-\varepsilon)$; $S_m \in E_{\{2,3\}}$.

Тогда $\pi \cap \pi(G) \subseteq \pi(q-\varepsilon)$, и $S_m \in E_\pi^s$, так как $m < s$. Значит, выполняется (А) и $G \in E_\pi^s$.

(2) $n = 2m$; $\eta = \varepsilon^m$; $3 \in \pi(q-\varepsilon)$; $S_m \in E_{\{2,3\}}$.

Если $\eta = -\varepsilon$, то m нечетно, что противоречит условию $\eta = \varepsilon^m$. Значит, $\eta = \varepsilon$, тогда $m < s$ и $S_m \in E_\pi^s$. Значит, выполняется (Б) и $G \in E_\pi^s$.

(3) $n = 2m$; $\eta = -\varepsilon^m$; $3 \in \pi(q-\varepsilon)$; $S_{m-1} \in E_{\{2,3\}}$.

Тогда $m - 1 < s$, значит, $S_{m-1} \in E_\pi^s$, и в силу условия (В) группа G содержит разрешимую π-холлову подгруппу.

(4) $n = 11$; $3 \in \pi(q-\varepsilon)$; $(q^2-1)_{\{2,3\}} = 24$.

Поскольку $\pi \cap \pi(G) \subseteq \pi(q-\varepsilon)$ и $S_5 \in E_\pi^s$, условие (А) выполняется и $G \in E_\pi^s$.

(5) $n = 12$; $\eta = -1$; $3 \in \pi(q-\varepsilon)$; $(q^2-1)_{2,3} = 24$.

Так как $m = 6$ четно, получаем, что $\eta = \varepsilon = -1$ и $\eta = -\varepsilon^m$. Поскольку при этом $\pi \cap \pi(G) \subseteq \pi(q-\varepsilon)$ и $S_5 \in E_\pi^s$, выполняется условие (В) и G содержит разрешимую π-холлову подгруппу.

Пусть G — исключительная группа. По [85, леммы 7.1–7.6] для доказательства того, что $G \in E_\pi^s$, достаточно показать, что $\pi \cap \pi(G) \subseteq \pi(q-\varepsilon)$. Так как $G \in E_{\{2,3\}}$, из [85, леммы 7.1–7.6] получаем, что $3 \in \pi(q-\varepsilon)$, и при этом G — одна из групп $F_4(q)$, $G_2(q)$, ${}^3D_4(q)$, $E_6^{-\varepsilon}(q)$. По лемме 4.1.12 эти группы обладают свойством $E_{\{2,s\}}$, если $s \in \pi(q-\varepsilon)$. Тогда $\pi \cap \pi(G) \subseteq \pi(q-\varepsilon)$, что и требовалось показать. □

Таким образом, разобраны все возможности для множества π и предложение 4.3.1 доказано. □

§ 4.4. Доказательство теоремы 16.

Пусть $G \in E_{\{p,q\}}$. Пусть композиционный ряд

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n = G$$

является уплотнением главного ряда группы G. Тогда по критерию свойства E_π из [80, следствие 5] группа $Aut_G(G_i/G_{i-1})$ обладает свойством $E_{\{p,q\}}$ для любого i. С другой стороны, согласно теореме 17, если $Aut_G(G_i/G_{i-1}) \in E^s_\pi$, то $G \in E^s_\pi$. Следовательно, для доказательства теоремы достаточно рассмотреть случай, когда G — почти простая группа.

Пусть G — почти простая группа и $S = Soc(G)$. Пусть $\pi \cap \pi(S) = \{r, s\}$ для различных простых r и s и $\pi \cap \pi(G) = \{r, s\} \cup \tau$, где τ непусто. Поскольку $G \in E_{\{r,s\}}$, существует π-холлова подгруппа H группы S. Легко видеть, что группа $N_G(H)$ является π-разрешимой. Следовательно, она содержит разрешимую π-холлову подгруппу. Более того, $N_G(H)$ содержит $\{r, s\}$-холлову подгруппу группы G. По гипотезе Шрайера G содержит τ-холлову подгруппу T. Поскольку порядки T и H взаимно просты, можно считать, что $T \leqslant N_G(H)$. Значит, π-холлова подгруппа группы $N_G(H)$ также является π-холловой подгруппой группы G.

Пусть $|\pi \cap \pi(S)| > 2$. По предложению 4.3.1 утверждение теоремы выполнено для S, и все классы сопряженности разрешимых π-подгрупп инвариантны относительно G. Теперь применение леммы 4.1.6 завершает доказательство теоремы.

§ 4.5. Неизомофрные p-дополнения

Напомним, что p'-холлова подгруппа называется p-дополнением. На семинаре «Введение в теорию конечных групп» 21 февраля 2013 года В. Д. Мазуров, комментируя теорему 3.15 из [67] о разрешимости групп, обладающих p-дополнениями для всех простых p и примеры несопряженных p-дополнений в неразрешимых группах, сформулировал перед участниками семинара следующие вопросы.

(1) Всегда ли в конечной группе любые два p-дополнения изоморфны?

(2) Всегда ли в конечной группе любые два p-дополнения сопряжены некоторым автоморфизмом?

В этом небольшом параграфе мы построим пример конечной группы с неизморфными p-дополнениями. Пример группы с изоморфными, но не автоморфно сопряженными p-дополнениями, был построен Д.О. Ревиным в совместной с автором работе [98].

Отметим два следствия классификации конечных простых групп, дающие положительные ответы на вопросы (1) и (2) в некоторых важных частных случаях.

Предложение 4.5.1. *Пусть G — конечная простая группа. Если H и K — p-дополнения в G, то $K = H^\varphi$ для некоторого $\varphi \in \mathrm{Aut}(G)$.*

Предложение 4.5.2. *В любой конечной группе все 2-дополнения сопряжены.*

Справедливость предложения 4.5.1 вытекает из [26, следствие 5.3] и леммы 4.5.3 (см. ниже). Предложение 4.5.2 доказано в [27, следствие 4.5].

Следующее утверждение хорошо известно и является простым следствием элементарных фактов линейной алгебры.

Лемма 4.5.3. *Пусть V — векторное пространство над некоторым конечным полем F и $G = \mathrm{GL}(V)$. Пусть U и W — подпространства пространства V. Положим*

$$H = \{g \in G \mid U^g = U\} \text{ и } K = \{g \in G \mid W^g = W\}.$$

Тогда

(1) *подгруппы H и K сопряжены в G если и только если $\dim U = \dim W$;*

(2) *если $\dim U + \dim W = \dim V$ то подгруппы H и K сопряжены в $\mathrm{Aut}(G)$.*

В частности, если $\dim V > 2$, то стабилизаторы прямой и гиперплоскости не сопряжены в G, но сопряжены в $\mathrm{Aut}(G)$.

Построим пример группы с неизоморфными p-дополнениями. Пусть V — трехмерное векторное пространство над полем порядка 2 и $G = \mathrm{GL}(V) \simeq \mathrm{GL}_3(2)$. Пусть U и W — подпространства пространства V размерностей 1 и 2 соответственно и пусть

$$H = \{g \in G \mid U^g = U\}, K = \{g \in G \mid W^g = W\}.$$

Обозначим через G^* естественное полупрямое произведение V на G. Пусть также $H^* = \langle V, H\rangle$ и $K^* = \langle V, K\rangle$. Покажем, что подгруппы H^* и K^* являются 7-дополнениями в группе G^* и при этом не изоморфны.

Как известно, $|G| = 168 = 2^3 \cdot 7 \cdot 3$. Матрицы, отвечающие элементам подгрупп H и K в базисах пространства V, содержащих соответственно базисы подпространств U и W, записываются соответственно в виде

$$\left(\begin{array}{cc|c} & A & \\ \hline * & * & 1 \end{array}\right) \text{ и } \left(\begin{array}{c|cc} 1 & & \\ \hline * & & \\ * & \multicolumn{2}{c}{A} \end{array}\right),$$

где $A \in \mathrm{GL}_2(2)$. Поэтому $|H| = |K| = 2^2 \cdot |\mathrm{GL}_2(2)| = 2^3 \cdot 3$ и $|G : H| = |G : K| = 7$. Отсюда следует, что $|H^*| = |K^*| = 2^6 \cdot 3$, а $|G^* : H^*| = |G^* : K^*| = 7$. Таким образом, подгруппы H^* и K^* являются 7-дополнениями в G^*.

Заметим, что подпространство U обладает ровно одним ненулевым вектором u и поэтому $u^h = u$ для любого $h \in H$. Следовательно, $u \in Z(H^*)$. Покажем, что $Z(K^*) = 1$. Отсюда будет следовать неизоморфность подгрупп H^* и K^*.

Любой элемент подгруппы K^*, не лежащий в V, нетривиальным образом действует на подгруппе V группы K^* и поэтому не лежит в $Z(K^*)$. Если бы теперь оказалось,

что некоторый ненулевой вектор $v \in V$ содержится в центре группы K^*, то подгруппа $K \leq K^*$ оставляла бы инвариантным одномерное подпространство $\langle v \rangle$ пространства V и, следовательно, была бы сопряжена в G с подгруппой из H. Ввиду равенства порядков подгрупп H и K, отсюда следовала бы их сопряженность, вопреки лемме 4.5.3. Значит, $Z(K^*) = 1$ и подгруппы H^* и K^* группы G^* неизоморфны.

Заметим, что из предложения 4.5.2 следует, что существуют простые числа p такие, что в любой конечной группе любые два p-дополнения сопряжены (в частности, изоморфны и сопряжены в группе автоморфизмов). Поэтому интерес представляет вопрос о классификации простых чисел p таких, что для любой конечной группы G выполнено одно из следующих утверждений:

(1) В группе G группе любые два p-дополнения сопряжены.

(2) В группе G группе любые два p-дополнения сопряжены некоторым автоморфизмом.

(3) В группе G группе любые два p-дополнения изоморфны.

Основываясь на примерах, полученных в [98], М.Н. Нестеров в работе [20] свел эту проблему к известной проблеме Нагеля—Люнггрена из теории чисел.

Заключение

В диссертации решены следующие проблемы:

1) доказано первое утверждение гипотезы Боровика–Хухро об ограниченности числа неабелевых композиционных факторов локально конечной группы конечной c-размерности (теорема 1; совместно с А. В. Васильевым);

2) построен контрпример ко второму утверждению гипотезы Боровика–Хухро о строении локально конечной группы конечной c-размерности (теорема 3; совместно с А. В. Васильевым и Д. О. Ревиным);

3) описано строение локально конечных групп конечной c-размерности (теорема 5);

4) показано, что c-размерность фактор-группы локально конечной группы конечной c-размерности k по локально разрешимому радикалу ограничена в терминах k (теорема 4);

5) получено ограничение на индекс нильпотентного радикала в периодической локально нильпотентной группе конечной c-размерности (следствие 1.4.1; совместно с И. Е. Девятковой);

6) описаны спектры конечных простых исключительных групп лиевых типов E_6, ${}^2E_6$, E_7 и E_8 (теоремы 10, 12, 14);

7) построен полиномиальный алгоритм распознавания конечной простой группы по спектру (теорема 15; совместно с А. В. Васильевым);

8) получен критерий существования разрешимой холловой подгруппы (теорема 16; совместно с А. П. Храмовой);

9) построен пример конечной группы с неизоморфными p-дополнениями (параграф 4.5; получено в совместной работе с Д. О. Ревиным).

Результаты о локально конечных группах дают достаточно точное описание их строения и предоставляют новые методы изучения этих групп. Отметим, что если сравнить формулировку опровергнутого утверждения гипотезы Боровика–Хухро и теорему 5 (или даже более близкую к нему по форме теорему 6), то очевидно, что между ними есть зазор. Например, естественным является вопрос о том, можно ли в формулировке теоремы 6 третий радикал Хирша–Плоткина заменить на второй. Кроме того, из результатов о группах c-размерности 2, т. е. группах с абелевыми централизаторами, следует, что для них гипотеза Боровика–Хухро справедлива в полном объеме. Контрпримеры, построенные в

диссертации, имеют размерность, не превосходящую 50. Таким образом, не известно для каких значений c-размерности гипотеза Боровика–Хухро справедлива в полном объеме.

Описание спектров исключительных групп завершило описание спектров конечных простых групп. Кроме того, методы разработанные при их вычислении можно использовать для вычисления спектров групп внутренне-диагональных автоморфизмов исключительных групп.

Как говорилось выше, алгоритм распознавания простой группы по спектру не только представляет самостоятельный интерес, но и может служить источником полезных инструментов для построения других алгоритмов распознавания конечных простых групп по порядкам элементов. Также он актуализирует и без того интересную задачу эффективного вычисления спектра конечной простой группы по набору ее стандартных параметров.

В связи с доказательством критерия существования разрешимой холловой подгруппы отметим теорему 17, сводящую вопрос существования разрешимой подгруппы к изучению групп автоморфизмов некоторого ее субнормального ряда. Здесь есть два направления дальнейшего развития. Во-первых, эта теорема дает достаточное условие существования разрешимой холловой подгруппы, по-видимому, оно является и необходимым, но это только гипотеза. Во-вторых, полезно было бы иметь аналогичные утверждения для других классов групп, помимо разрешимых.

Список литературы

[1] Бутурлакин А. А. Спектры конечных линейных и унитарных групп // Алгебра и логика — 2008. — Т. 47, № 2. — С. 157–173.

[2] Бутурлакин А. А. Спектры конечных симплектических и ортогональных групп // Матем. тр. — 2010. — Т. 13, № 2. — С. 33–83.

[3] Бутурлакин А. А., Гречкосеева М. А. Циклическое строение максимальных торов в конечных классических группах // Алгебра и логика — 2007. — Т. 46, № 2. — С. 129–156.

[4] Buturlakin A. A. Isospectral finite simple groups // Сиб. электрон. матем. изв.— 2010. — Т. 7. — С. 111–114.

[5] Беляев В. В. Локально конечные группы Шевалле // Исследования по теории групп. Свердловск: УНЦ АН СССР — 1984. — С. 39–50.

[6] Боровик А. В. Периодические линейные группы нечетной характеристики // Докл. АН СССР — 1982. — Т. 266, № 6. — С. 1289–1291.

[7] Васильев А. В., Вдовин Е. П. Критерий смежности в графе простых чисел конечной простой группы // Алгебра и логика — 2005. — Т. 44, № 6. — С. 682–725.

[8] Васильев А. В., Вдовин Е. П. Коклики максимального размера в графе простых чисел конечной простой группы // Алгебра и логика — 2011. — Т. 50, № 4. — С. 425–470.

[9] Васильев А. В., Гречкосеева М. А. Распознаваемость по спектру для простых классических групп в характеристике 2 // Сиб. матем. журн. — 2015. — Т. 56, № 6. — С. 1264–1276.

[10] Васильев А. В., Старолетов А. М. Распознаваемость групп $G_2(q)$ по спектру // Алгебра и логика — 2013. — Т. 52, № 1. — С. 3–21.

[11] Вдовин Е. П., Ревин Д. О. Холловы подгруппы нечетного порядка в конечных группах // Алгебра и логика — 2002. — Т. 41, № 1. — С. 15–56.

[12] Вдовин Е. П., Ревин Д. О. Теоремы силовского типа // УМН — 2011. — Т. 66, № 5(401). — С. 3–46.

[13] Горшков И. Б. Распознаваемость знакопеременных групп по спектру // Алгебра и логика — 2013. — Т. 52, № 1. — С. 57—63.

[14] Дынкин Е. Б. Полупростые подалгебры полупростых алгебр Ли // Матем. сб. — 1952. — Т. 30(72), № 2. — С. 349—462.

[15] Заварницин А. В. Строение максимальных торов в спинорных группах // Сиб. матем. журн. — 2015. — Т. 56, № 3. — С. 537–548.

[16] Звездина М. А. О неабелевых простых группах с графом простых чисел как у знакопеременной группы // Сиб. матем. журн. — 2013. — Т. 54, № 1. — С. 65—76.

[17] Каргаполов М. И. О периодических группах матриц // Сиб. матем. журн. — 1962. — Т. 3, № 6. — С. 834–838.

[18] Каргаполов М. И. Замечания к статье [автора] «О периодических группах матриц» // Сиб. матем. журн. — 1963. — Т. 4, № 5. — С. 1198–1199.

[19] Кондратьев А. С., Мазуров В. Д. Распознавание знакопеременных групп простой степени по порядкам их элементов // Сиб. матем. журн. — 2000. — Т. 41, № 2. — С. 359–369.

[20] Нестеров М. Н. Арифметика сопряжённости p-дополнений // Алгебра и логика — 2015. — Т. 54, № 1. — С. 53–69.

[21] Ревин Д. О. Холловы π-подгруппы конечных групп Шевалле, характеристика которых принадлежит π // Матем. тр. — 1999. — Т. 2, № 1. — С. 160–208.

[22] Хамфрис Дж. Введение в теория алгебр Ли и их представлений. — М.:МЦНМО — 2003.

[23] Agrawal M., Kayal N., and Saxena N. Primes in P // Ann. of Math.— 2004. — Vol. 160, no. 2. — P. 781–793.

[24] Alladi K., Solomon R., Turull A. Finite simple groups of bounded subgroup chain length // J. Algebra— 2000. — Vol. 231. — P. 374–386.

[25] Alperin J.L., Fong P. Weights for symmetric and general linear groups // J. Algebra— 1990. — Vol. 131. — P. 2–22.

[26] Arad Z., Fisman E. On finite factorizable groups // J. Algebra— 1984. — Vol. 86, no. 2. — P. 522–548.

[27] Arad Z., Ward M. B. New criteria for the solvability of finite groups // J. Algebra— 1982. — Vol. 77, no. 1. — P. 234–246.

[28] Aschbacher M. Finite group theory — Cambridge Univ. Press, Cambridge. — 1986.

[29] Babai L., Kantor W. M., Pálfy P. P., and Seress Á. Black-box recognition of finite simple groups of Lie type by statistics of element orders // J. Group Theory— 2002. — Vol. 5, no. 4. — P. 383–401.

[30] Borovik A. V., Karhumäki U. Locally finite groups of finite centralizer dimension // J. Group Theory— 2019. — Vol. 22, no. 4. — P. 729—740

[31] Bosma W., Cannon J., Playoust C. The Magma algebra system. I. The user language. // J. Symbolic Comput.— 1997. — Vol. 24. — P. 235–265.

[32] Brandl R. Finite groups all of whose elements are of prime power order // Boll. Un. Mat. It. A (5)— 1981. — Vol. 18. — P. 491–493.

[33] Brandl R., Shi W. J. A characterization of finite simple groups with abelian Sylow 2-subgroups // Ricerche Mat.— 1993. — Vol. 42, no. 1. — P. 193–198.

[34] Brawley J.V., Schnibben G.E. Infinite algebraic extensions of finite field (Contemporary Mathematics 95). — Amer. Math Soc., Providence, RI. — 1989.

[35] Bryant R. M. Groups with the minimal condition on centralizers // J. Algebra— 1979. — Vol. 60. — P. 371–383.

[36] Bryant R. M., Hartley B. Periodic locally soluble groups with the minimal condition on centralizers // J. Algebra— 1979. — Vol. 61. — P. 328–334.

[37] Carter R. W. Simple groups of Lie type (Pure and Applied Mathematics, Vol. 28) — John Wiley & Sons.— 1972.

[38] Carter R. W. Conjugacy classes in the Weyl group //Compositio mathematica— 1972. — Vol. 25, Fasc. 1. — P. 1–59.

[39] Carter R. W. Centralizers of semisimple elements in finite groups of Lie type // Proc. Lond. Math. Soc. (3).— 1978. — Vol. 37. — P. 491–507.

[40] Carter R. W. Centralizers of semisimple elements in the finite classical group // Proc. Lond. Math. Soc. (3).— 1981. — Vol. 42, no. 1.— P. 1–41.

[41] Carter R. W. Finite Groups of Lie Type, Conjugacy Classes and Complex Characters. — New York: John Wiley and Sons.— 1985.

[42] Collins M. J. Modular analogues of Jordan's theorem for finite linear groups // J. Reine Angew. Math.— 2008. — Vol. 2008, no. 624. — P. 143–171.

[43] Conway J. H., Curtis R. T., Norton S. P., Parker R. A., and Wilson R. A. Atlas of finite groups — Clarendon Press, Oxford. — 1984.

[44] Deng H. W., Shi W. J. The characterization of Ree groups ${}^2F_4(q)$ by their element orders // J. Algebra— 1999. — Vol. 217, no. 1. — P. 180–187.

[45] Deriziotis D. I. The centralizers of semisimple elements of the Chevalley groups E_7 and E_8 // Tokyo J. Math.— 1983. — Vol. 6, no. 1. — P. 191–216.

[46] Deriziotis D. I. Conjugacy classes of centralizers of semisimple elements in finite groups of Lie type (Vorlesungen Fachbereich Math. Univ. Essen 11) — Universität Essen Fachbereich Mathematik, Essen. — 1984.

[47] Deriziotis D. I., Fakiolas A. P. The maximal tori in the finite Chevalley groups of type E_6, E_7 and E_8 // Commun. Algebra.— 1991. — Vol. 19, no. 3. — P. 889–903.

[48] Deriziotis D. I., Michler G. O. Character table and blocks of finite simple triality groups ${}^3D_4(q)$ // Trans. Amer. Math. Soc.— 1987. — Vol. 303. — P. 39–70.

[49] Duncan A.J., Kazatchkov I.V., Remeslennikov V.N. Centraliser dimension and universal classes of groups. // Сиб. электрон. матем. изв.— 2006. — Vol. 3. — P. 197–215.

[50] Easdown D., Praeger C.E. On minimal faithful permutation representations of finite groups // Bull. Austral. Math. Soc.— 1988. — Vol. 38. — P. 207–220.

[51] Feit W., Thompson J.G. Solvability of groups of odd order. // Pacific J. Math.— 1963. — Vol. 13, no. 3. —

[52] Glasby S. P., Lübeck F., Niemeyer A. C., and Praeger C. E. Primitive prime divisors and the n-th cyclotomic polynomial // J. Aust. Math. Soc.— 2017. — Vol. 102, no. 1. — P. 122–135.

[53] Glauberman G. Factorization in local subgroups of finite groups (CBMS Reg. Conf. Ser. Math. 33). — Amer. Math. Soc., Providence, RI.— 1976.

[54] Gorenstein D., Lyons R. The local structure of finite groups of characteristic 2 type // Mem. Amer. Math. Soc.— 1983. — Vol. 42, no. 276.

[55] Gorenstein D., Lyons R., Solomon R. The classification of the finite simple groups. Number 3. — Amer. Math. Soc., Providence, RI. — 1998.

[56] Grechkoseeva M. A., Vasil'ev A. V. On the structure of finite groups isospectral to finite simple groups // J. Group Theory— 2015. — Vol. 18, no. 5. — P. 741–759 .

[57] Grechkoseeva M. A., Zvezdina M. A. On spectra of automorphic extensions of finite simple groups $F_4(q)$ and ${}^3D_4(q)$ // J. Algebra Appl. — 2016. — Vol. 15, no. 4. — 1650168 [13 pages].

[58] Griess R. Automorphisms of extra special groups and nonvanishing degree 2 cohomology // Pacific J. Math.— 1973. — Vol. 48. — P. 403–411.

[59] Gross F. On the existence of Hall subgroups // J. Algebra — 1986. — Vol. 98, no. 1. — P. 1–13.

[60] Gross F. Conjugacy of odd order Hall subgroups // Bull. London Math. Soc. — 1987. — Vol. 19, no. 4. — P. 311–319.

[61] Gross F. Odd order Hall subgroups of the classical linear groups // Proc. London Math. Soc.(3) — 1995. — Vol. 220. — P. 317–336.

[62] Hall P. Theorems like Sylow's // Proc. London Math. Soc. — 1956. — Vol. s3-6, no. 2. — P. 286–304.

[63] Hammer P. L., Simeone B. The splittance of a graph // Combinatorica — 1981. — Vol. 1, no. 3. — P. 275–284.

[64] Hartley B., Shute G. Monomorphisms and direct limits of finite groups of Lie type // Quarterly Journal Of Mathematics (Ser. 2). — 1984. — Vol. 35.— P. 49–71.

[65] Higman G. Finite groups in which every element has prime power order // J. London Math. Soc. — 1957. — Vol. 32. — P. 335–342.

[66] Holt D.F. Representing quotients of permutation groups // Quarterly Journal Of Mathematic — 1997. — Vol. 48, no. 2— P. 347–350.

[67] Isaacs I.M. Finite Group Theory (Graduate Studies in Mathematics 92) — Amer. Math. Soc., Providence, RI.— 2008.

[68] Kantor W. M., Seress Á. Prime power graphs for groups of Lie type // J. Algebra — 2002. — Vol. 247, no. 2. — P. 370–434.

[69] Kantor W. M., Seress Á. Large element orders and the characteristic of Lie-type simple groups // J. Algebra — 2009. — Vol. 322, no. 3. — P. 802–832.

[70] Kegel O. H. Four lectures on Sylow theory in locally finite groups // in Group theory: Proceedings of the Singapore Group Theory Conference 1987 (Eds. K. N. Cheng and Y. K. Leong). — de Gruyter, Berlin – New York. — 1989.

[71] Kegel O. H., Wehrfritz B. A. F. Locally Finite Groups (North-Holland Mathematical Library 3) — Elsevier, New York. — 1973.

[72] Khukhro E. I. On solubility of groups with bounded centralizer chains // Glasgow Math. J.— 2009. — Vol. 51. — P. 49–54.

[73] Kleidman P.B., Liebeck M.W. The subgroup structure of finite classical groups — Cambridge University Press, Cambridge. — 1990.

[74] Unsolved problems in group theory. The Kourovka notebook. No. 19 (eds. V.D. Mazurov, E.I. Khukhro) — Rus. Acad. Sci. Sib. Branch Inst. Math., Novosibirsk. — 2018.

[75] Liebeck M. W., O'Brien E. A. Finding the characteristic of a group of Lie type // J. Lond. Math. Soc. (2).— 2007. — Vol. 75, no. 3. — P. 741–754.

[76] Massias J. P., Nicolas J. L., and Robin G. Effective bounds for the maximal order of an element in the symmetric group // Math. Comp.— 1989. — Vol. 53, no. 188. — P. 665–678.

[77] Meierfrankenfeld U. Locally finite groups // https://users.math.msu.edu/users/meier/Classnotes/LFG/LFG.pdf.

[78] Moretó A. Sylow numbers and nilpotent Hall subgroups // J. Algebra. — 2013. — Vol. 379. — P. 80–84.

[79] Myasnikov A., Shumyatsky P. Discriminating groups and c-dimension // J. Group Theory. — 2004. — Vol. 7. — P. 135–142.

[80] Revin D. O., Vdovin E. P. Existence criterion for Hall subgroups of finite groups // J. Group Theory — 2011. — Vol. 14, no. 1. — P. 93–101.

[81] Suzuki M. On a class of doubly transitive groups // Ann. of Math. (2) — 1962. — Vol. 75. — P. 105–145.

[82] Testerman D. M. A_1-type overgroups of elements of order p in semisimple algebraic groups and the associated finite groups // J. Algebra — 1995. — Vol. 177, no. 1. — P. 34–76.

[83] Thomas S. The classification of the simple periodic linear groups // Arch. Math. — 1983. — Vol. 41. — P. 103–116.

[84] Vasil'ev A. V. On finite groups isospectral to simple classical groups // J. Algebra — 2015. — Vol. 423. — P. 318–374.

[85] Revin D. O., Vdovin E. P. On the number of classes of conjugate Hall subgroups in finite simple groups // J. Algebra — 2010. — Vol. 324, no. 12. — P. 3614–3652.

[86] Wehrfritz B. A. F. Infinite linear groups (Ergebnisse der Mathematik und ihrer Grenzgebiete 76) — Springer-Verlag, Berlin.— 1973.

[87] Williams J. S. Prime graph components of finite groups // J. Algebra — 1981. — Vol. 69. — P. 487–513.

[88] Winter D.J. Representations of locally finite groups // Bull. Amer. Math. Soc. — 1968. — Vol. 74. — P. 145–148.

[89] Zsigmondy K. Zur Theorie der Potenzreste // Monatsh. Math. Phys. — 1892. — Vol. 3. — P. 265–284.

Публикации автора по теме диссертации.

[90] Бутурлакин А. А. Спектры конечных простых групп $E_6(q)$ и ${}^2E_6(q)$ // Алгебра и логика — 2013. — Т. 52, № 3. — С. 284–304.

[91] Бутурлакин А. А. Спектры конечных простых групп $E_7(q)$ // Сиб. матем. журн. — 2016. — Т. 57, № 5. — С. 988–998.

[92] Бутурлакин А. А. Спектры групп $E_8(q)$ // Алгебра и логика — 2018. — Т. 57, № 1. — С. 3–13.

[93] Бутурлакин А. А., Васильев А. В. О локально конечных группах с ограниченными рядами централизаторов // Алгебра и логика — 2013. — Т. 52, № 5. — С. 553–558.

[94] Бутурлакин А. А., Васильев А. В. О конструктивном распознавании конечных простых групп по порядкам их элементов // Алгебра и логика — 2014. — Т. 53, № 4. — С. 541–544.

[95] Buturlakin A. A. The structure of locally finite groups of finite c-dimension // J. Algebra Appl. — 2019. — Vol. 18, no. 12. — 1950223, 12 pp.

[96] Buturlakin A. A., Devyatkova I. E. Periodic locally nilpotent groups of finite c-dimension // Сиб. электрон. матем. изв. — 2020. — Т. 17. — С. 1100–1105.

[97] Buturlakin A. A., Khramova A. P. A criterion for the existence of a solvable π-Hall subgroup in a finite group // Comm. Algebra — 2020. — Vol. 48, no. 3. — P. 1305–1313.

[98] Buturlakin A. A., Revin D. O. On p-complements of finite groups // Сиб. электрон. матем. изв. — 2013. — Т. 10. — С. 414–417.

[99] Buturlakin A. A., Revin D. O., Vasil'ev A. V. Groups with bounded centralizer chains and the Borovik–Khukhro conjecture // J. Group Theory — 2018. — Vol. 21, no. 6. — P. 1095–1110.

[100] Buturlakin A. A., Vasil'ev A. V. The graph of atomic divisors and recognition of finite simple groups // J. Algebra — 2019. — Vol. 537. — P. 478–502.