Федеральное государственное бюджетное учреждение науки

Институт математики им. С. Л. Соболева

Сибирского отделения Российской академии наук

На правах рукописи

Звездина Мария Анатольевна

КОНЕЧНЫЕ ПОЧТИ ПРОСТЫЕ ГРУППЫ, ИЗОСПЕКТРАЛЬНЫЕ ПРОСТЫМ

01.01.06 — математическая логика, алгебра и теория чисел

Диссертация на соискание ученой степени кандидата физико-математических наук

Научный руководитель

доктор физико-математических наук

Гречкосеева Мария Александровна

Новосибирск – 2017

Оглавление

Введение

Постановка задачи и актуальность темы исследования

В диссертации рассматривается вопрос о том, насколько точно конечные простые группы определяются порядками своих элементов. Полученные автором результаты завершают исследование этого вопроса для исключительных групп лиева типа и для групп лиева типа в характеристике 2.

Множество порядков элементов, или *спектр*, является одним из самых естественных числовых параметров конечной группы, и результаты, ограничивающие строение группы в терминах порядков ее элементов, закономерным образом появляются в теории групп начиная с первой половины прошлого века. В 1900 г. Бернсайд [42] классифицировал конечные группы, спектр которых содержит число 2 и не содержит других четных чисел: это в точности группы симметрий правильного многоугольника с нечетным числом вершин, подгруппы четного порядка естественного полупрямого произведения аддитивной группы поля порядка 2^m и его мультипликативной группы и, наконец, проективные специальные линейные группы $PSL_2(2^m)$. В 1957 г. Хигмен [60] показал, что непримарная конечная группа, порядки нетривиальных элементов которой являются степенями простых чисел, либо разрешима и бипримарна, либо имеет единственный неабелев композиционный фактор. Своего рода обобщением этих результатов Бернсайда и Хигмена можно считать теорему Грюнберга–Кегеля [87, теорема A] о строении групп с несвязным графом простых чисел: *графом простых чисел* конечной группы называется граф на множестве простых делителей ее порядка, в котором два различных простых числа смежны тогда и только тогда, когда их произведение лежит в спектре, и теорема гласит, что конечная группа с несвязным графом простых чисел либо является группой Фробениуса или двойной группой Фробениуса, либо имеет единственный неабелев композиционный фактор.

Следует отметить, что многие неабелевы простые группы малого порядка имеют несвязный граф простых чисел и, более того, их спектр зачастую состоит из степеней простых чисел или не содержит других четных чисел, кроме 2. Например, знакопеременная группа степени 5, самая маленькая по

порядку неабелева простая группа, имеет спектр $\{1, 2, 3, 5\}$. Таким образом, можно ожидать, что любая конечная группа, имеющая такой же спектр, как неабелева простая группа S небольшого порядка, будет иметь не более одного неабелева композиционного фактора и этот фактор будет близок к S. Более того, в 1980-х годах Ши [75–77] обнаружил целый ряд неабелевых простых групп, которые однозначно задаются своим спектром в классе конечных групп: спорадические группы M_{12}, Co_2 и J_1, унитарная группа $PSU_6(2)$ и линейные группы $PSL_2(2^m)$, где $m > 1$ (среди последних, в силу изоморфизма $PSL_2(4) \simeq A_5$, есть и самая маленькая неабелева простая группа). Интересно, что распознаваемость по спектру простых групп $PSL_2(2^m)$ несложно вывести из вышеупомянутой работы Бернсайда [42], но эта работа была мало известна в 1980-х. Эти и более поздние результаты Ши и его коллег положили начало широкому направлению исследований распознаваемости простых групп по спектру.

Будем обозначать спектр конечной группы G через $\omega(G)$ и называть группы с одинаковым спектром *изоспектральными*. Через $h(G)$ обозначим число попарно неизоморфных конечных групп, изоспектральных G. В частности, распознаваемость группы G по спектру эквивалентна равенству $h(G) = 1$. Если $h(G)$ — конечное число, большее 1, группа G *почти распознаваема*, а если $h(G) = \infty$ — *нераспознаваема*. Говорят, что для группы G решена *проблема распознаваемости по спектру*, если $h(G)$ известно и в случае конечного $h(G)$ группы, изоспектральные G, явно описаны.

Напомним, что согласно классификационной теореме конечных простых групп любая конечная неабелева простая группа является либо знакопеременной группой, либо одной из 26 спорадических групп, либо группой лиева типа. Последние, в свою очередь делятся на классические группы $PSL_n(q)$, $PSU_n(q)$, $PSp_{2n}(q)$, $P\Omega_{2n+1}(q)$, $P\Omega^{\pm}_{2n}(q)$ и исключительные группы лиева типа. К 1998 г. было доказано, что все спорадические группы, кроме группы J_2, распознаваемы (см. [71]). В 2015 г. было завершено доказательство распознаваемости всех знакопеременных групп, кроме A_6 и A_{10} [14]. Группы J_2, A_6 и A_{10} нераспознаваемы по спектру, но изоспектральные им группы описаны в [34, 70, 71]. Таким образом, проблема распознаваемости по спектру полностью решена для всех знакопеременных и спорадических групп. Некоторые группы лиева типа также распознаваемы по спектру, например, уже

упомянутые линейные группы $PSL_2(q)$ (их распознаваемость при нечетном $q \neq 9$ доказана в [40]), но общая картина для групп лиева типа гораздо более разнообразна (см., например, обзоры [29,56]). В частности, для любого натурального k найдется простая группа S лиева типа, такая что $h(S) > k$ [89]. Однако в 2007 г. Мазуровым была высказана гипотеза о том, что начиная с некоторого лиева ранга все простые группы лиева типа будут почти распознаваемы по спектру. В результате усилий нескольких групп математиков эта гипотеза была доказана в 2015 г. и, более того, имеет место следующая теорема (см. [8, 12, 58, 85]).

Теорема А. *Пусть S — одна из следующих неабелевых простых групп:*

1) *исключительные группы, кроме ${}^3D_4(2)$;*

2) *$PSL_n(q)$, $PSU_n(q)$, где $n \geq 45$ или q четно, кроме $PSU_4(2)$ и $PSU_5(2)$;*

3) *$PSp_{2n}(q)$, $P\Omega_{2n+1}(q)$, где $n \geq 28$ или q четно, кроме $PSp_6(2)$, $PSp_4(2^m)$ и $PSp_8(2^m)$;*

4) *$P\Omega^+_{2n}(q)$, где $n \geq 31$ или q четно, кроме $P\Omega^+_8(2)$;*

5) *$P\Omega^-_{2n}(q)$, где $n \geq 30$ или q четно.*

Тогда любая конечная группа, изоспектральная S, изоморфна группе G, такой что $S \leq G \leq \operatorname{Aut} S$. В частности, $h(S)$ конечно.

Группы G, удовлетворяющие условию $S \leq G \leq \operatorname{Aut} S$ для некоторой конечной неабелевой простой группы S, принято называть *почти простыми* группами (с цоколем S). Мы также будем называть такие группы *почти простыми расширениями* или *автоморфными расширениями* группы S (назовем расширение *нетривиальным*, если $G \neq S$). Хорошо известно, что порядок группы $\operatorname{Aut} S/S$ мал по сравнению с порядком группы S, поэтому почти простые группы с цоколем S очень близки к S. Таким образом, теорема А говорит не просто о том, что $h(S)$ конечно, а том, что группы, изоспектральные S, близки к S. С другой стороны, ясно, что не всякая почти простая группа имеет такие же порядки элементов, как ее цоколь и, значит, для полного решения проблемы распознаваемости простых групп по спектру необходимо

описать почти простые группы с цоколем лиева типа, изоспектральные своему цоколю. Эта задача записана в "Коуровскую тетрадь" [26] как вопрос 17.36 и является первой из задач, рассматриваемых в диссертации.

Проблема 1. *Для каждой неабелевой простой группы S лиева типа описать все конечные группы G, такие что $S < G \leq \mathrm{Aut}\, S$ и $\omega(G) = \omega(S)$.*

Напомним, что граф простых чисел группы G — это помеченный граф на множестве $\pi(G)$ простых делителей группы G, в котором различные вершины, помеченные числами p и q, смежны тогда и только тогда, когда $pq \in \omega(G)$. Будем обозначать этот граф через $GK(G)$. Граф простых чисел является гораздо более компактным параметром, чем спектр, однако, как показывает, например, вышеупомянутая теорема Грюнберга–Кегеля, может сказать многое о строении группы. Неудивительно, что в ходе исследований распознаваемости групп по спектру делались естественные попытки усилить полученные результаты путем замены спектра на граф простых чисел. Например, простые группы Ри ${}^2G_2(q)$ распознаваемы не только по спектру, но и по графу простых чисел [18, 36]. С другой стороны, как уже говорилось, знакопеременная группа A_5 распознаваема по спектру, однако $GK(A_5) = GK(A_6)$, при этом $h(A_6) = \infty$ [38]. Также простые группы $PSp_6(2)$, $P\Omega_8^+(2)$, A_9 и J_2 имеют одинаковые графы простых чисел [59], при этом $h(PSp_6(2)) = h(P\Omega_8^+(2)) = 2$, $h(A_9) = 1$ и $h(J_2) = \infty$ [17,27,71,73,79]. Несмотря на свою частность, эти примеры демонстрируют общую тенденцию, которая состоит в том, что проблема распознаваемости по графу простых чисел значительно сложнее проблемы распознаваемости по спектру, даже если ограничиться классом конечных простых групп. Так, до сих пор не существует полного описания всех пар неизоморфных неабелевых простых групп, графы простых чисел которых совпадают (см. также [26, вопрос 16.26]). Это вторая проблема, рассматриваемая в диссертации.

Проблема 2. *Для каждой неабелевой простой группы описать все простые группы с таким же графом простых чисел.*

Степень разработанности темы и цели исследования

Как было уже сказано, начиная с 1980-х годов стали появляться отдельные результаты о распознаваемости по спектру групп лиева типа небольшого

лиева ранга. Эти результаты, в частности, включали в себя и решение проблемы 1 для соответствующих групп. Так, в [40] эта проблема была решена для групп $PSL_2(q)$, в [39, 47, 78] — для групп Ри и Сузуки, в [31, лемма 5] — для групп $PSL_3(2^m)$, $PSU_3(2^m)$, в [28] — для групп $PSp_4(3^{2m+1})$, в [9] — для групп $F_4(2^m)$. Однако использовавшиеся в этих работах методы решения проблемы 1 были специфическими и не допускали простого обобщения на произвольные группы лиева типа. В 2004–2006 гг. Заварниciным [19, 89] была решена проблема распознаваемости для групп $PSL_3(q)$ и $PSU_3(q)$, где q нечетно, и в [19] им был предложен подход к вычислению спектра расширения произвольной группы лиева типа полевым автоморфизмом. Этот подход позволил решить проблему 1 для всех линейных и унитарных групп над полями характеристики 2 [15, 57]. Также в [11] и [23] было доказано, что группы $G_2(q)$ и $E_8(q)$ распознаваемы по спектру. Таким образом, к началу настоящего исследования проблема 1 была не решена для классических групп в нечетной характеристике, для симплектических и ортогональных групп в характеристике 2, а также для групп $F_4(q)$, где q нечетно, ${}^3D_4(q)$, $E_6(q)$, ${}^2E_6(q)$ и $E_7(q)$. Отметим, что сложность проблемы 1 для групп $F_4(q)$ и ${}^3D_4(q)$ состоит, в частности, в отсутствии явного описания их спектров, а для групп $E_6(q)$, ${}^2E_6(q)$ и $E_7(q)$ — в более сложном, по сравнению с остальными исключительными группами, строении группы внешних автоморфизмов. Также стоит отметить, что все эти исключительные группы, кроме групп $E_7(q)$, имеют несвязный граф простых чисел, поэтому некоторые ограничения на группу G в проблеме 1 следуют из работы [68] о почти простых группах с несвязным графом простых чисел. Одна из целей диссертации — завершить изучение проблемы 1 для классических групп в характеристике 2 и для исключительных групп лиева типа в произвольной характеристике.

Исследование распознаваемости конечных групп по графу простых чисел имеет недолгую историю по сравнению с изучением распознаваемости по спектру, и все существовавшие к началу диссертационного исследования результаты в этой области носят частный характер. В [59] описано строение конечных групп с графом простых чисел как у спорадической группы. В частности, получено решение проблемы 2 для спорадических групп [59, следствие 2]. Знакопеременная группа A_{10} однозначно характеризуется своим графом простых чисел в классе конечных простых групп (см. [25]). В [18] доказана

распознаваемость по графу простых чисел групп J_4, $G_2(7)$ и ${}^2G_2(q)$ при $q > 3$. Из этой работы также следует решение проблемы 2 для группы $PSL_3(7)$. В [91] доказана распознаваемость по графу группы $PSL_{16}(2)$. Распознаваемость по графу групп $PSL_2(q)$ для некоторых q доказана в [37,61,63–66] (см. также обзор [62]). В диссертации проблема 2 рассматривается для простых знакопеременных групп.

Основные результаты диссертации

1. Доказано, что спектр нетривиального автоморфного расширения конечной простой симплектической или ортогональной группы над полем характеристики 2 не может совпадать со спектром этой группы (теоремы 1 и 2).

2. Получено описание автоморфных расширений простых групп ${}^3D_4(q)$, $F_4(q)$, $E_6(q)$, ${}^2E_6(q)$ и $E_7(q)$, имеющих такой же спектр, как их цоколь (теоремы 3–6).

3. Показано, что за конечным числом явно описанных исключений конечная простая группа, имеющая такой же граф простых чисел, как знакопеременная группа, также является знакопеременной группой (теорема 7).

Методы исследования

Изучение порядков элементов почти простых групп с лиевым цоколем базируется на теореме Стейнберга [82] о том, что группа автоморфизмов группы лиева типа является расщепляемым расширением группы внутренне-диагональных автоморфизмов посредством полевых и графовых автоморфизмов. Для собственно вычисления порядков используется комбинация подхода, разработанного в [19] на основе некоторого следствия теоремы Ленга–Стейнберга [81], с хорошо известными результатами о классах сопряженности автоморфизмов и строении их централизаторов. Также используются явные арифметические описания спектров исследуемых групп и их универсальных версий из [2–4] и двойственность между группой внутренне-диагональных автоморфизмов группы лиева типа и универсальной версией ее дуальной группы [45]. Графы простых чисел неабелевых простых групп изучаются с помощью критериев смежности вершин в этих графах, полученных в [6, 7]. Для сравнения как спектров, так и графов простых чисел, применяются теорема Жигмонди [92] о существовании примитивного делителя и другие хорошо

известные теоретико-числовые результаты.

Новизна и научная значимость работы

Работа носит теоретический характер. Все полученные результаты являются новыми. Теоремы 3–6 завершают исследование распознаваемости по спектру простых исключительных групп, а теоремы 1 и 2 завершают исследование проблемы 1 для простых классических групп в характеристике 2. Построены бесконечные серии примеров почти простых расширений простых исключительных групп, не изоспектральных этим группам (см. [26, вопрос 16.24]). Теорема 7 используется в [33] при изучении характеризуемости знакопеременных групп порядком и графом простых чисел, а также в [32, 41] при изучении случаев совпадения графов простых чисел конечной простой группы и ее собственной подгруппы. Результаты диссертации могут быть использованы в дальнейших исследованиях в области теории групп, связанных с вопросами распознаваемости, а также могут быть включены в спецкурсы для студентов и аспирантов, специализирующихся в области алгебры.

Публикации

Результаты диссертации опубликованы в работах [93–102]. Основные результаты диссертации опубликованы в [93–96] в изданиях, входящих в перечень ВАК рецензируемых научных журналов, в которых должны быть опубликованы основные результаты диссертаций на соискание учёных степеней доктора и кандидата наук. Результаты работы [95] получены в неразделимом соавторстве с научным руководителем М. А. Гречкосеевой.

Апробация работы

Результаты диссертации докладывались на 9-ой Международной летней школе “Пограничные вопросы теории моделей и универсальной алгебры” (Новосибирск, 2011), Международной конференции по алгебре и геометрии, посвященной 80-летию со дня рождения А.И. Старостина (Екатеринбург, 2011), 43-й Всероссийской молодежной школе-конференции “Современные проблемы математики” (Екатеринбург, 2012), Международной конференции “Мальцевские чтения” (Новосибирск, 2013–2016), Международной конференции “Ischia Group Theory 2014” (Неаполь, Италия, 2014), Международной молодёжной школе-конференции “Алгоритмические вопросы теории

групп и смежных областей" (Новосибирск, 2014), Международной конференции "Finite Simple Groups and Related Topics" (Уорик, Великобритания, 2015), Международной конференции "Graphs and Groups, Spectra and Symmetries" (Новосибирск, 2016), а также неоднократно обсуждались на семинарах "Теория групп" и "Алгебра и логика" Института математики им. С. Л. Соболева и Новосибирского государственного университета.

Благодарности

Автор выражает глубокую признательность своему научному руководителю М. А. Гречкосеевой и профессору А. В. Васильеву за поставленные задачи, неоценимую помощь в работе и всестороннюю поддержку. Автор благодарен всему коллективу лаборатории теории групп ИМ СО РАН и кафедры алгебры и математической логики ММФ НГУ за сотрудничество и атмосферу, в которой была выполнена данная работа.

Результаты диссертации получены при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 12–01–33102), программы СО РАН проектов партнерских исследований на 2012–2014 гг. (проект № 14) и Российского научного фонда (проект №14-21-00065).

Структура и объем диссертации

Диссертация состоит из введения, 4 глав, заключения и списка литературы. Она изложена на 77 страницах, включает 3 таблицы и 3 рисунка. Главы диссертации подразделяются на параграфы. Основные результаты глав сформулированы в виде теорем и имеют сквозную нумерацию. Вспомогательные утверждения (леммы, предложения) имеют тройную нумерацию: первая цифра означает номер главы, вторая — номер параграфа в главе, третья — номер утверждения в текущем параграфе. Формулы имеют двойную нумерацию: номер главы и номер формулы внутри главы. Список литературы содержит 102 наименования. Работы автора по теме диссертации приведены отдельным списком.

Содержание диссертации

Глава 1. Эта глава содержит необходимые предварительные сведения. В начале главы вводятся обозначения для групп лиева типа и их групп автоморфизмов. В параграфе 1.1 приводятся некоторые теоретико-числовые

сведения, в том числе леммы о существовании и свойствах примитивных простых делителей. Параграф 1.2 содержит определения, связанные с порядками элементов конечных групп. Там же приводятся арифметические описания спектров простых симплектических и ортогональных групп лиева типа в характеристике 2 и исключительных групп типов E_6 и E_7, а также арифметические критерии смежности вершин в графах простых чисел простых классических групп. В параграфе 1.3 даются определения внутренне-диагональных, полевых и графовых автоморфизмов конечных групп лиева типа, рассматриваемых как группы неподвижных точек эндоморфизмов Стейнберга простых алгебраических групп, и описываются спектры расширений групп лиева типа полевыми автоморфизмами.

Глава 2. В этой главе изучаются спектры автоморфных расширений простых симплектических и ортогональных групп над полями характеристики 2. Для этих групп полностью решается проблема 1. В параграфе 2.1 доказываются вспомогательные арифметические леммы. В параграфе 2.2 доказывается, что спектр нетривиального автоморфного расширения простой симплектической группы в характеристике 2 не может совпадать со спектром этой группы (теорема 1). В параграфе 2.3 доказывается, что спектр нетривиального автоморфного расширения простой ортогональной группы четной размерности в характеристике 2 не может совпадать со спектром этой группы (теорема 2). В конце главы формулируется следствие из теорем 1, 2 и теоремы A о распознаваемости по спектру простых симплектических и ортогональных групп в характеристике 2.Результаты этой главы получены автором лично и опубликованы в [94].

Глава 3. Эта глава посвящена решению проблемы 1 для простых исключительных групп лиева типа, а именно, групп $F_4(q)$ для нечетного q, ${}^3D_4(q)$, $E_6(q)$, ${}^2E_6(q)$ и $E_7(q)$. Первая часть главы посвящена арифметическому описанию спектров простых групп $F_4(q)$ для нечетного q и ${}^3D_4(q)$ (параграф 3.2). Для этих целей в параграфе 3.1 изложена информация о связных централизаторах полупростых элементов в группах лиева типа. Далее в параграфах 3.3–3.5 доказываются критерии совпадения спектра нетривиального автоморфного расширения простой группы ${}^3D_4(q)$, $F_4(q)$, $E_6(q)$, ${}^2E_6(q)$ или $E_7(q)$ со спектром самой группы (теоремы 3–6). Поскольку эти результаты завершают исследование распознаваемости по спектру простых исключитель-

ных групп, в параграфе 3.6 сведена информация о распознаваемости всех простых исключительных групп. Для каждой почти распознаваемой группы приводится число попарно неизоморфных конечных групп с таким же спектром и описывается их строение (теорема B). Результаты теорем 3 и 4 получены в неразделимом соавторстве с научным руководителем М. А. Гречкосеевой и опубликованы в [95]. Результаты теорем 5 и 6 получены автором лично и опубликованы в [96].

Глава 4. Эта глава посвящена решению проблемы 2 для знакопеременных групп: описываются случаи совпадения графа простых чисел конечной простой группы G с графом простых чисел знакопеременной группы S. В параграфе 4.1 приводятся специфические свойства графа простых чисел знакопеременной группы. В параграфах 4.2–4.4 рассматриваются случаи, когда G — простая группа лиева типа или простая спорадическая группа. В параграфе 4.5 рассматривается случай, когда G — знакопеременная простая группа. Основным результатом главы является доказательство того факта, что конечная простая группа с графом простых чисел как у знакопеременной группы сама является знакопеременной группой, кроме нескольких непосредственно перечисленных случаев (теорема 7). В этой теореме также приводятся случаи совпадения графов простых чисел различных знакопеременных групп. Более того, доказано, что по модулю некоторого теоретико-числового утверждения, связанного с бинарной гипотезой Гольдбаха, других случаев совпадения графов простых чисел различных знакопеременных групп нет (теорема 8). Результаты теорем 7 и 8 получены автором лично и опубликованы в [93].

1. Предварительные сведения

В обозначениях неабелевых простых групп мы следуем [46]. В частности, простые классические группы обозначаются как $L_n(q)$, $U_n(q)$, $S_{2n}(q)$, $O_{2n+1}(q)$ и $O^{\pm}_{2n}(q)$. Если L — простая группа лиева типа, то через L_u обозначается ее универсальная версия (см. [54, теорема 2.2.6]). Мы также будем использовать сокращенную запись с $\varepsilon \in \{+,-\}$ для некоторых типов групп: $L^{\varepsilon}_n(q)$ означает $L_n(q)$ при $\varepsilon = +$ и $U_n(q)$ при $\varepsilon = -$, $E^{\varepsilon}_6(q)$ означает $E_6(q)$ при $\varepsilon = +$ и ${}^2E_6(q)$ при $\varepsilon = -$. Группа всех автоморфизмов, группа внутренних и группа внешних автоморфизмов группы G обозначаются через $\operatorname{Aut} G$, $\operatorname{Inn} G$ и $\operatorname{Out} G$ соответственно. Неабелева простая группа S отождествляется со своей группой внутренних автоморфизмов.

§ 1.1. Теоретико-числовые сведения и обозначения

Как обычно, через $(m_1, m_2, ..., m_k)$ и $[m_1, m_2, ..., m_k]$ обозначаются наибольший общий делитель и наименьшее общее кратное натуральных чисел m_1,...m_k соответственно. Если r — простое число, то *r-частью* натурального числа m называется наибольшая степень числа r, делящая m, а *r'-частью* числа m называется наибольший делитель m, взаимно простой с r. Через $(m)_r$ и $(m)_{r'}$ обозначаются r-часть и r'-часть натурального числа m соответственно. Ясно, что $(m)_{r'} = \frac{m}{(m)_r}$.

Лемма 1.1.1. *Пусть q — степень простого числа, $\epsilon \in \{1, -1\}$ и m — натуральное число.*

1) *Если нечетное простое число r делит $q-\epsilon$, то $(q^m-\epsilon^m)_r = (m)_r(q-\epsilon)_r$.*

2) *Если нечетное простое число r делит $q^m-\epsilon^m$, то оно делит $q^{(m)_{r'}}-\epsilon^{(m)_{r'}}$.*

3) *Если 4 делит $q-\epsilon$ или m нечетно, то $(q^m-\epsilon^m)_2 = (m)_2(q-\epsilon)_2$. В любом случае $(q^m - \epsilon^m)_2 \geqslant (m)_2(q-\epsilon)_2$.*

Доказательство. 1) См. [89, лемма 6]. 2) Утверждение следует из малой теоремы Ферма. 3) См. [15, лемма 8]. □

Лемма 1.1.2.([89, лемма 6]) *Пусть q, k и l — натуральные числа. Тогда*

1) $(q^k-1, q^l-1) = q^{(k,l)}-1$;

2) (q^k+1, q^l+1) *равен* $q^{(k,l)}+1$, *если* $\frac{k}{(k,l)}$ *и* $\frac{l}{(k,l)}$ *— нечетные числа, и* $(2, q+1)$ *в противном случае;*

3) (q^k-1, q^l+1) *равен* $q^{(k,l)}+1$, *если* $\frac{k}{(k,l)}$ *четно, а* $\frac{l}{(k,l)}$ *нечетно, и* $(2, q+1)$ *в противном случае.*

Пусть q — целое число, r — нечетное простое число и $(q, r) = 1$. Обозначим через $e(r, q)$ мультипликативный порядок числа q по модулю r. Для нечетного q положим $e(2, q) = 1$, если $q \equiv 1 \pmod 4$, и $e(2, q) = 2$, если $q \equiv 3 \pmod 4$. Простое число r, удовлетворяющее условию $e(r, q) = n$, называют *примитивным простым делителем* числа $q^n - 1$. Обозначим через $R_n(q)$ множество всех примитивных простых делителей числа $q^n - 1$ (в некоторых случаях это множество может оказаться пустым), а через $r_n(q)$ — произвольное число из множества $R_n(q)$, если это множество непусто. Из определения следует, что $R_n(q) \subseteq R_n(q^k)$, если $(n, k) = 1$. Существование примитивных простых делителей для почти всех пар чисел (n, q) установлено Жигмонди в [92].

Лемма 1.1.3. (следствие теоремы Жигмонди [92]) *Пусть q — целое число, по модулю большее* 1. *Тогда для каждого натурального числа n найдется простое число r такое, что $e(r, q) = n$, за исключением случаев*

$$(q, n) \in \{(2, 1), (2, 6), (-2, 2), (-2, 3), (3, 1), (-3, 2)\}.$$

Лемма 1.1.4. *Пусть i, k, q — различные натуральные числа, $(i, k) = 1$ и множества $R_i(q)$ и $R_{ik}(q)$ непусты. Тогда $|R_i(q^k)| > 1$.*

Доказательство. См. [16, лемма 6]. □

§ 1.2. Порядки элементов групп лиева типа

Прежде всего заметим, что спектр $\omega(G)$ группы G замкнут относительно взятия делителей, поэтому он однозначно определяется своим подмножеством элементов, максимальных относительно делимости. Это подмножество

обозначается через $\mu(G)$. Если p — простое число, назовем *p-частью* спектра группы G подмножество в $\omega(G)$, состоящее из всех степеней числа p, а *p'-частью* — подмножество в $\omega(G)$, состоящее из всех чисел, взаимно простых с p. Будем обозначать эти подмножества через $\omega_p(G)$ и $\omega_{p'}(G)$ соответственно. Наибольший порядок элемента в силовской p-подгруппе группы G называется *p-периодом* группы G. Нам удобно распространить обозначение множества порядков элементов на любые подмножества группы G, то есть если $A \subseteq G$, то $\omega(A)$ — это множество порядков элементов, лежащих в A.

В [2–4] получены арифметические описания спектров конечных простых симплектических и ортогональных групп, а также простых исключительных групп типов E_6 и E_7. Нам потребуются следующие результаты.

Лемма 1.2.1. ([3, следствие 3]) *Пусть $G = S_{2n}(q)$, где $n \geq 2$ и q — степень числа 2. Тогда $\omega(G)$ состоит из всех делителей следующих чисел:*

1) $[q^{n_1}+\varepsilon_1 1, q^{n_2}+\varepsilon_2 1, ..., q^{n_s}+\varepsilon_s 1]$ *для любых $s \geq 1$, $\varepsilon_i \in \{+,-\}$, $1 \leq i \leq s$, и $n_1, n_2, ..., n_s > 0$ таких, что $n_1 + n_2 + ... + n_s = n$;*

2) $2[q^{n_1}+\varepsilon_1 1, q^{n_2}+\varepsilon_2 1, ..., q^{n_s}+\varepsilon_s 1]$ *для любых $s \geq 1$, $\varepsilon_i \in \{+,-\}$, $1 \leq i \leq s$, и $n_1, n_2, ..., n_s > 0$ таких, что $n_1 + n_2 + ... + n_s = n - 1$;*

3) $2^k[q^{n_1}+\varepsilon_1 1, q^{n_2}+\varepsilon_2 1, ..., q^{n_s}+\varepsilon_s 1]$ *для любых $s \geq 1$, $k \geq 2$, $\varepsilon_i \in \{+,-\}$, $1 \leq i \leq s$, и $n_1, n_2, ..., n_s > 0$ таких, что $2^{k-2} + 1 + n_1 + n_2 + ... + n_s = n$;*

4) 2^k, *если $2^{k-2} + 1 = n$ для некоторого $k \geq 2$.*

Лемма 1.2.2. ([3, следствие 4]) *Пусть $G = O^{\varepsilon}_{2n}(q)$, где $n \geq 4$, $\varepsilon \in \{+,-\}$ и q — степень числа 2. Тогда $\omega(G)$ состоит из всех делителей следующих чисел:*

1) $[q^{n_1}+1, q^{n_2}+1, ..., q^{n_l}+1, q^{n_{l+1}}-1, q^{n_{l+2}}-1...q^{n_s}-1]$ *для любых $s \geq 1$, l четного, если $\varepsilon = +$, и нечетного, если $\varepsilon = -$, и $n_1, n_2, ..., n_s > 0$ таких, что $n_1 + n_2 + ... + n_s = n$;*

2) $2^k[q^{n_1}+1, q^{n_2}+1, ..., q^{n_l}+1, q^{n_{l+1}}-1, q^{n_{l+2}}-1...q^{n_s}-1]$ *для любых $s \geq 1$ и $n_1, n_2, ..., n_s > 0$ таких, что $2^{k-2} + 2 + n_1 + n_2 + ... + n_s = n$;*

3) $2[q^{n_1}+1, q^{n_2}+1, ..., q^{n_l}+1, q^{n_{l+1}}-1, q^{n_{l+2}}-1...q^{n_s}-1]$ *для любых $s \geq 1$ и $n_1, n_2, ..., n_s > 0$ таких, что $2 + n_1 + n_2 + ... + n_s = n$;*

4) $2[q \pm 1, q^{n_1}+1, q^{n_2}+1, ..., q^{n_l}+1, q^{n_{l+1}}-1, q^{n_{l+2}}-1...q^{n_s}-1]$ *для любых* $s \geq 1$, l *четного, если* $\varepsilon = +$, *и нечетного, если* $\varepsilon = -$, *и* $n_1, n_2, ..., n_s > 0$ *таких, что* $2 + n_1 + n_2 + ... + n_s = n$;

5) $4[q-1, q^{n_1}+1, q^{n_2}+1, ..., q^{n_s}+1]$ *для любых* $s \geq 1$, s *четного, если* $\varepsilon = +$, *и нечетного, если* $\varepsilon = -$, *и* $n_1, n_2, ..., n_s > 0$ *таких, что* $3+n_1+n_2+...+n_s = n$;

6) $4[q + 1, q^{n_1}+1, q^{n_2}+1, ..., q^{n_l}+1, q^{n_{l+1}}-1, q^{n_{l+2}}-1...q^{n_s}-1]$ *для любых* $s \geq 1$, l *нечетного, если* $\varepsilon = +$, *и четного, если* $\varepsilon = -$, *и* $n_1, n_2, ..., n_s > 0$ *таких, что* $3 + n_1 + n_2 + ... + n_s = n$;

7) 2^k, *если* $n = 2^{k-2} + 2$ *для некоторого* $k > 2$.

Лемма 1.2.3.([4, теорема 1]) *Пусть* $G = E_6^{\varepsilon}(q)$, *где* $\varepsilon \in \{+, -\}$, q — *степень простого числа* p. *Положим* $d = (3, q - \varepsilon 1)$. *Тогда* $\omega(G)$ *состоит из всех делителей следующих чисел:*

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) $4 \cdot \{\frac{(q^3-\varepsilon 1)(q+\varepsilon 1)}{d}, \frac{q^4+q^2+1}{d}, \frac{q^4-1}{d}, q^2-1\}$, $8 \cdot \{q-\varepsilon 1, \frac{q^2-1}{d}, \frac{q^2+\varepsilon q+1}{d}\}$, 16, *если* $p = 2$;

4) $9 \cdot \{\frac{(q^2+1)(q-\varepsilon 1)}{d}, q^2 - 1, \frac{q^2+\varepsilon q+1}{d}\}$, 27, *если* $p = 3$;

5) $25 \cdot \{q - \varepsilon 1, \frac{q^2-1}{d}, \frac{q^2+\varepsilon q+1}{d}\}$, *если* $p = 5$;

6) $49 \cdot \{\frac{q-\varepsilon 1}{d}\}$, *если* $p = 7$;

7) $\{121\}$, *если* $p = 11$.

Лемма 1.2.4.([2, теорема 2]) *Пусть* $G = E_7(q)$, *где* q — *степень простого числа* p. *Положим* $d = (2, q - 1)$. *Тогда* $\omega(G)$ *состоит из всех делителей следующих чисел:*

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

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

3) $4\cdot\{\frac{q^6-1}{(q\pm 1)d},\ \frac{q^5\pm 1}{d},\ q^4-1,\ (q^3\pm 1)(q\mp 1)\}$, $8\cdot\{\frac{q^3\pm 1}{d},\ \frac{(q^2+1)(q\pm 1)}{d},\ q^2-1\}$, $16\cdot\{q\pm 1\}$, 32, *если* $p=2$;

4) $9\cdot\{\frac{q^4-1}{d},\ \frac{(q^3\pm 1)(q\mp 1)}{d},\ \frac{(q^2+1)(q\pm 1)}{d},\ q^2-1\}$, $27\cdot\{q\pm 1\}$, *если* $p=3$;

5) $25\cdot\{\frac{q^3\pm 1}{d},\ \frac{(q^2+1)(q\pm 1)}{d},\ q^2-1\}$, *если* $p=5$;

6) $49\cdot\{\frac{q^2-1}{d},\ q\pm 1\}$, *если* $p=7$;

7) $121\cdot\{\frac{q\pm 1}{d}\}$, *если* $p=11$;

8) $\{p^2\}$, *если* $p=13$ *или* $p=17$.

В [49] описано строение максимальных торов универсальных групп типов E_6 и E_7. Из этого описания вытекают следующие две леммы.

Лемма 1.2.5. *Пусть* G *— универсальная группа* $(E_6^\varepsilon(q))_u$, *где* $\varepsilon\in\{+,-\}$, q *— степень простого числа* p. *Тогда* $\omega_{p'}(G)$ *состоит из всех делителей следующих чисел:* $q^6+\varepsilon q^3+1$, $(q^2+\varepsilon q+1)(q^4-q^2+1)$, $(q-\varepsilon 1)(q^2+1)(q^3+\varepsilon 1)$, $(q^2-1)(q^4+1)$, $(q+\varepsilon 1)(q^5-\varepsilon 1)$, $\frac{q^6-1}{(3,q-\varepsilon 1)}$.

Лемма 1.2.6. *Пусть* G *— универсальная группа* $(E_7(q))_u$, *где* q *— степень простого числа* p. *Тогда* $\omega_{p'}(G)$ *состоит из всех делителей следующих чисел:* $(q^2\pm q+1)(q^5\mp 1)$, $(q\pm 1)(q^6\mp q^3+1)$, $q^7\pm 1$, $(q^3\pm 1)(q^4-q^2+1)$, $(q^2\pm q+1)(q^4-1)$, $(q\pm 1)(q^5\mp 1)$, $\frac{q^8-1}{(q\pm 1)(2,q-1)}$, $(q^4+1)(q^2-1)$, q^6-1.

Напомним, что графом простых чисел группы G называется граф с множеством вершин $\pi(G)$, в котором две различные вершины r и s смежны тогда и только тогда, когда $rs\in\omega(G)$.

Лемма 1.2.7. *Граф простых чисел группы* $E_6^\varepsilon(q)$ *несвязен и его компонента связности, не содержащая число* 2, *равна* $\pi((q^6+\varepsilon q^3+1)/(3,q-\varepsilon 1))$.

Доказательство. См. [87], [21]. □

В [6] были получены критерии смежности вершин в графах простых чисел простых линейных и симплектических групп. Приведем здесь более удобные для наших целей переформулировки этих результатов из [10], использующие сокращение $L_n^\varepsilon(q)$.

Лемма 1.2.8. *Пусть $G = L_n^{\varepsilon}(q)$, где q — степень простого числа p. Пусть r, s — нечетные простые числа из $\pi(G)$, отличные от p. Положим $k = e(r, \varepsilon q)$, $l = e(s, \varepsilon q)$ и предположим, что $2 \leq k \leq l$. Тогда r и s несмежны в $GK(G)$ в том и только в том случае, если $k + l > n$ и k не делит l.*

Доказательство. См. [6, предложения 2.1, 2.2] и [10, лемма 2.1]. □

Лемма 1.2.9. *Пусть $G = L_n^{\varepsilon}(q)$, где q — степень простого числа p. Пусть $r \in \pi(G)$ и $r \neq p$. Тогда r и p несмежны в $GK(G)$ в том и только в том случае, если выполняется одно из следующих утверждений:*

1) *r нечетно и $e(r, \varepsilon q) > n - 2$;*

2) *$G = L_2(q)$ и $r = 2$;*

3) *$G = L_3^{\varepsilon}(q)$, $r = 3$ и $(\varepsilon q - 1)_3 = 3$.*

Доказательство. См. [6, предложение 3.1] и [10, лемма 2.2]. □

Определим функцию $\eta : \mathbb{N} \to \mathbb{N}$ следующим образом:

$$\eta(m) = \begin{cases} m, & \text{если } m \text{ нечетно,} \\ \frac{m}{2}, & \text{иначе.} \end{cases} \tag{1.1}$$

Лемма 1.2.10. ([7, предл. 2.4]) *Пусть G — одна из конечных простых групп $S_{2n}(q)$ или $O_{2n+1}(q)$, где q — степень простого числа p. Пусть r, s — нечетные простые числа и $r, s \in \pi(G) \setminus \{p\}$. Положим $k = e(r, q)$, $l = e(s, q)$ и предположим, что $1 \leq \eta(k) \leq \eta(l)$. Тогда r и s несмежны в том и только в том случае, если $\eta(k) + \eta(l) > n$, и k, l удовлетворяют следующему условию:*

$$\frac{l}{k} \text{ не является нечетным натуральным числом.} \tag{1.2}$$

Отметим, что условие (1.2) означает, что $q^{\eta(k)} + (-1)^k$ не делит $q^{\eta(l)} + (-1)^l$.

Лемма 1.2.11. ([7, предл. 2.5]) *Пусть $G = O_{2n}^{\varepsilon}(q)$, где q — степень простого числа p, $\varepsilon \in \{+, -\}$. Предположим, что r, s — нечетные простые числа и $r, s \in \pi(O_{2n}^{\varepsilon}(q)) \setminus \{p\}$. Положим $k = e(r, q)$, $l = e(s, q)$ и $1 \leq \eta(k) \leq \eta(l)$. Тогда r и s несмежны в том и только в том случае, если*

$$2\eta(k) + 2\eta(l) > 2n - (1 - \varepsilon(-1)^{k+l}),$$

k и l удовлетворяют условию (1.2), *а при $\varepsilon = +$ не выполнена система равенств:*

$$n = l = 2\eta(l) = 2\eta(k) = 2k.$$

Следующее утверждение является важным свойством графа простых чисел произвольной простой группы лиева типа.

Лемма 1.2.12. *Пусть G — простая группа лиева типа. Тогда для любого числа $r \in \pi(G)$ существует число $s \in \pi(G)$, такое что r и s несмежны в графе $GK(G)$.*

Доказательство. Следует из [6]. См. также [55, лемма 2.2]. □

§ 1.3. Автоморфизмы конечных групп лиева типа

Следующая простая лемма бывает полезна для работы с автоморфизмами.

Лемма 1.3.1. ([19, лемма 9]) *Пусть H — нормальная подгруппа конечной группы G. Если $x, y \in G$ порождают по модулю H одну и ту же циклическую подгруппу, то $\omega(Hx) = \omega(Hy)$.*

Следуя [54, глава 2], мы будем рассматривать конечные группы лиева типа как группы неподвижных точек эндоморфизмов Стейнберга простых алгебраических групп.

На протяжении всего этого параграфа p — некоторое простое число и $\overline{F}$ — алгебраическое замыкание поля порядка p. Пусть $\overline{G}$ — простая линейная алгебраическая группа над $\overline{F}$ и σ — *эндоморфизм Стейнберга* группы $\overline{G}$, т.е. σ сюръективен и группа $\overline{G}_\sigma = C_{\overline{G}}(\sigma)$ конечна. Положим $K = O^{p'}(\overline{G}_\sigma)$. Тогда за конечным числом исключений группа $S = K/Z(K)$ проста, и группами такого вида исчерпывается множество простых групп лиева типа.

Для данных $\overline{G}$ и S эндоморфизм σ можно выбрать так называемым стандартным способом. Нам не потребуется детально рассматривать группы Ри и Сузуки, поэтому для простоты изложения будем считать, что S не является группой Ри или Сузуки. Зафиксируем максимальный тор $\overline{T}$, систему корней Φ, ее фундаментальную подсистему Π и порождающие Шевалле $x_\alpha(t)$, $n_\alpha(t)$ и $h_\alpha(t)$ группы $\overline{G}$ (см. [54, определение 1.12.2]). Если q — степень числа p, то φ_q обозначает эндоморфизм группы $\overline{G}$, действующий на корне-

вых элементах $x_\alpha(t)$, где $\alpha \in \Phi$, $t \in \overline{F}$, по правилу $\varphi_q(x_\alpha(t)) = x_\alpha(t^q)$ [54, теорема 1.15.4a]. Если ρ — изометрия системы Π, то через γ_ρ обозначается соответствующий графовый автоморфизм группы $\overline{G}$, т.е. автоморфизм, удовлетворяющий условию: $\gamma_\rho(x_\alpha(t)) = x_{\rho(\alpha)}(t)$ для всех $\alpha \in \pm\Pi$, $t \in \overline{F}$ (такой автоморфизм существует не всегда, но для присоединенной и односвязной групп он существует [54, теорема 1.15.2a]). Согласно [54, теорема 2.2.3] мы можем считать, что в паре $(\overline{G}, \sigma)$ эндоморфизм σ имеет вид $\gamma_\rho\varphi_q$ для некоторой изометрии ρ системы Π и некоторой степени q числа p. При этом число q и порядок d изометрии ρ определены однозначно и группа S обозначается через ${}^d\Phi(q)$. Мы будем называть пару $(\overline{G}, \gamma_\rho\varphi_q)$ стандартным σ-представлением группы ${}^d\Phi(q)$.

Пусть $\overline{G}_a$ — присоединенная версия группы $\overline{G}$ и $(\overline{G}_a, \sigma)$ — стандартное σ-представление группы $S = {}^d\Phi(q)$, $q = p^m$. Тогда $Z(K_a) = 1$ и, значит, $S = K_a$. Группа $\overline{G}_\sigma$ действует сопряжением на S точно и ее можно отождествить с подгруппой группы $\operatorname{Aut} S$. Эта подгруппа называется группой внутренне-диагональных автоморфизмов группы S и обозначается через $\operatorname{Inndiag} S$. Эндоморфизм φ_p группы $\overline{G}_a$ индуцирует автоморфизм группы S порядка dm, который мы будем называть полевым и обозначать через φ. Если ρ' — нетривиальная симметрия системы Π, то графовый автоморфизм группы S, индуцированный эндоморфизмом $\gamma_{\rho'}$, обозначается через $\gamma_{\rho'}$, если $\Phi = D_4$, и просто γ, если $\Phi \neq D_4$ (в последнем случае ρ' определена однозначно).

Подход для описания спектров подгрупп группы $\operatorname{Inndiag} S \rtimes \langle\varphi\rangle$ был предложен А.В. Заварнициным в [19] и основан на следующей лемме.

Лемма 1.3.2. *Пусть $\overline{G}$ — простая линейная алгебраическая группа над полем $\overline{F}$ и τ — эндоморфизм Стейнберга группы $\overline{G}$. Тогда для любого k группа $\overline{G}_k = C_{\overline{G}}(\tau^k)$ конечна, τ индуцирует автоморфизм порядка k группы $\overline{G}_k$ и для смежного класса $\overline{G}_k\tau$ естественного полупрямого произведения $\overline{G}_k \rtimes \langle\tau\rangle$ выполнено*

$$\omega(\overline{G}_k\tau) = k\omega(\overline{G}_1).$$

Кроме того, $Z(\overline{G}_k) = Z(\overline{G}) \cap \overline{G}_k$, τ индуцирует автоморфизм группы $H_k = \overline{G}_k/Z(\overline{G}_k)$ и

$$\omega(H_k\tau) = k\omega(H_1).$$

В частности,

$$\omega(\overline{G}_k \rtimes \langle\tau\rangle) = \bigcup_{r|k} r\omega(\overline{G}_{k/r}), \quad \omega(H_k \rtimes \langle\tau\rangle) = \bigcup_{r|k} r\omega(H_{k/r}).$$

Доказательство. См. утверждение и доказательство [19, предложение 13]. В [19, предложение 13] во второй части утверждения вместо $Z(G)$ рассматривается $Sc(G)$ — подгруппа группы G, состоящая из всех скалярных матриц из G. Поскольку мы можем рассматривать G как подгруппу $GL(V)$, действующую на V неприводимо, мы можем считать, что $Sc(G) = Z(G)$. □

Лемма 1.3.3. *Пусть $S = {}^d\Phi(q)$ — простая группа лиева типа, отличная от групп Ри и Сузуки, и φ — ее полевой автоморфизм, определенный выше. Пусть β — элемент из $\langle\varphi\rangle$ порядка k и $(k, d) = 1$. Тогда*

$$\omega(S\beta) = k\omega({}^d\Phi(q_0)), \quad \omega(\operatorname{Inndiag} S\beta) = k\omega(\operatorname{Inndiag} {}^d\Phi(q_0)),$$

где $q_0 = q^{1/k}$. В частности,

$$\omega(S \rtimes \langle\beta\rangle) = \bigcup_{r|k} r\omega({}^d\Phi(q_0^{k/r})).$$

Доказательство. Перед доказательством отметим, что хотя φ определен как автоморфизм, индуцированный φ_p для $\overline{G}_a$, можно считать, что он индуцирован эндоморфизмом φ_p произвольной версии $\overline{G}$. Действительно, по [54, теорема 1.12.4] можно выбрать порождающие Шевалле групп $\overline{G}$ и $\overline{G}_a$ так, что найдется изогения $\overline{G} \to \overline{G}_a$, переводящая $x_\alpha(t)$ в $x_\alpha(t)$ для любых $\alpha \in \Phi$, $t \in \overline{F}$. В силу определения стандартного σ-представления эта изогения индуцирует сюръективный гомоморфизм $\psi : K \to K_a$ с ядром, равным $Z(K)$, причем если φ_1 — автоморфизм группы $K/Z(K)$, индуцированный эндоморфизмом φ_p группы $\overline{G}$, то $\psi(\varphi_1(xZ(K))) = \varphi(\psi(x))$.

Пусть $(\overline{G}, \sigma)$ — стандартное σ-представление группы S, $\sigma = \gamma\varphi_q$ и $q = p^m$. Поскольку k делит $|\varphi| = md$ и взаимно просто с d, оно делит m и $q_0 = p^{m/k}$. Выберем целое число i такое, что $ki \equiv 1 \pmod d$ и положим $\tau = \gamma^i\varphi_{q_0}$. Тогда $\tau^k = \sigma$. Более того, $\langle\tau\rangle$ индуцирует на $\overline{G}_\sigma$ ту же самую группу циклическую группу автоморфизмов, что и φ_{q_0}. Действительно, $\tau = \sigma\varphi^{-q}\varphi_{q_0} = \sigma(\varphi_{q_0})^{(1-ki)}$. По лемме 1.3.1 имеем $\omega(\overline{G}_\sigma\beta) = \omega(\overline{G}_\sigma\tau)$. Применяя лемму 1.3.2 получаем, что $\omega(\overline{G}_\sigma\beta) = k\cdot\omega(\overline{G}_\tau)$ и аналогичное равенство выполнено для фактор-групп по центрам. Для завершения доказательства осталось

заметить, что $\overline{G}_\sigma = \mathrm{Inndiag}\, S$, $\overline{G}_\tau \simeq \mathrm{Inndiag}\, {}^d\Phi(q_0)$, если $\overline{G}$ — присоединенная группа, и $\overline{G}_\sigma/Z(\overline{G}_\sigma) = S$, $\overline{G}_\tau/Z(\overline{G}_\tau) \simeq {}^d\Phi(q_0)$, если $\overline{G}$ — односвязная группа. $\square$

2. Симплектические и ортогональные группы над полями характеристики 2

Данная глава посвящена доказательству того, что спектр нетривиального автоморфного расширений простой симплектической или ортогональной группы над полем характеристики 2 не может совпадать со спектром самой группы. Основным результатом главы являются следующие теоремы.

Теорема 1. *Пусть S — конечная простая симплектическая группа $S_{2n}(q)$, где q четно. Если $S < G \leq \operatorname{Aut} S$, то $\omega(G) \neq \omega(S)$.*

Теорема 2. *Пусть S — конечная простая ортогональная группа $O^{\varepsilon}_{2n}(q)$, $\varepsilon \in \{+, -\}$, где q четно. Если $S < G \leq \operatorname{Aut} S$, то $\omega(G) \neq \omega(S)$.*

Замечание. Как следует из основного результата работы [8], если S — простая симплектическая группа $S_{2n}(q)$ или простая ортогональная группа $O^{\varepsilon}_{2n}(q)$ над полем характеристики 2 и $S \notin \{S_6(2), S_4(2^m), S_8(2^m), O^+_8(2)\}$, то любая конечная группа, изоспектральная S, изоморфна группе G, такой что $S \leq G \leq \operatorname{Aut} S$. Из этого результата и теорем 1, 2 вытекает следствие о распознаваемости группы S по спектру.

Следствие. *Пусть S — конечная простая симплектическая или ортогональная группа над полем характеристики 2, отличная от групп $S_6(2)$, $S_4(2^m)$, $S_8(2^m)$, $O^+_8(2)$. Тогда S распознаваема по спектру.*

§ 2.1. Предварительные сведения

Хорошо известно, что при четном q группы $S_{2n}(q)$ и $O_{2n+1}(q)$ изоморфны, поэтому мы не будем рассматривать группы $O_{2n+1}(q)$.

Отметим, что нечетное простое число r является примитивным простым делителем числа $q^m - 1$ и m четно, то r делит $q^{\frac{m}{2}} + 1$ и не делит $q^{\frac{m}{2}} - 1$. В этом случае мы будем также называть r примитивным простым делителем числа $q^{\frac{m}{2}} + 1$.

Лемма 2.1.1. *Пусть r — нечетный простой делитель натурального числа $n \geq 7$. Тогда существуют такие натуральные числа k и l, что $k+l = n$ и k, l удовлетворяют условию*

$$(k, r) = (l, r) = 1;\ k \text{ и } l \text{ не делят друг друга.} \tag{2.3}$$

Доказательство. Пусть n четно. Поскольку r нечетно, r делит $\frac{n}{2}$. Положим $k = \frac{n}{2} - 1$, $l = \frac{n}{2} + 1$. Ясно, что $(k, r) = (l, r) = 1$. Имеем $k > \frac{l}{2}$, так как $n > 6$. Поэтому k не делит l. Пусть n нечетно. Положим $k = \frac{n-1}{2}$, $l = \frac{n+1}{2}$. Ясно, что $(k, r) = (l, r) = 1$ и k, l не делят друг друга. □

Лемма 2.1.2. *Пусть r — нечетный простой делитель натурального числа $n \geq 6$. Тогда существуют натуральные числа k и l, такие что $k+l = n+1$, и если $n \neq 9$, то k, l удовлетворяют условию* (2.3), *иначе $(k, r) = (l, r) = 1$, $q^k + 1$ и $q^l + 1$ не делят друг друга.*

Доказательство. Пусть n четно. Тогда $k = \frac{n-2}{2}$, $l = \frac{n+4}{2}$. Пусть $n \neq 9$ нечетно. Если $r > 3$, то $k = \frac{n-1}{2}$, $l = \frac{n+3}{2}$. Пусть $r = 3$. Тогда $k = \frac{n-5}{2}$, $l = \frac{n+7}{2}$ при $n > 17$, $k = 5$, $l = 11$ при $n = 15$ и $k = 2$, $l = 8$ при $n = 9$. □

Лемма 2.1.3. *Пусть r — нечетный простой делитель натурального числа $n > 9$. Тогда существуют натуральные числа k и l, такие что $k+l = n-1$ и k, l удовлетворяют условию* (2.3).

Доказательство. Пусть n нечетно. Если $r > 3$, то $k = \frac{n-3}{2}$, $l = \frac{n+1}{2}$. Пусть $r = 3$. Тогда $k = \frac{n-7}{2}$, $l = \frac{n+5}{2}$ при $n > 19$ и $k = 4$, $l = 10$ при $n = 15$. Пусть n четно и $n \neq 10$. Тогда $k = \frac{n-4}{2}$, $l = \frac{n+2}{2}$. Пусть $n = 10$. Тогда $r \neq 7$ и $k = 2$, $l = 7$. □

Обозначим через G нетривиальное автоморфное расширение простой симплектической или ортогональной группы S над полем характеристики 2, т.е. $S < G \leq \operatorname{Aut} S$. Отметим, что у рассматриваемых простых групп нет внешних диагональных автоморфизмов, и все их автоморфные расширения являются расщепляемыми (см. [54, теорема 2.5.12]). Заметим также, что при доказательстве неравенства $\omega(G) \neq \omega(S)$ мы можем предполагать, что индекс $|G : S|$ — простое число (если неравенство $\omega(G) \neq \omega(S)$ выполняется для любого расширения G группы S, такого что $|G : S|$ — простое число, то оно выполняется и для произвольного расширения G группы S).

§ 2.2. Расширения симплектических групп

Доказательство теоремы 1. Всякая группа, изоспектральная группе $S_6(2)$, изоморфна либо самой группе $S_6(2)$, либо группе $O_8^+(2)$ [27]. Группа $S_6(4)$ распознаваема по спектру [13]. Из основного результата работы [35] следует, что группа $S_6(q)$ распознаваема по спектру при четном $q > 4$. Для доказательства теоремы остается рассмотреть группы $S_{2n}(q)$ при $n \neq 3$.

Пусть $S < G \leq \operatorname{Aut} S$. Можно считать, что $G = S \rtimes \langle \tau \rangle$, где τ — автоморфизм группы S простого порядка r.

Этап 1. Предположим, что τ — полевой автоморфизм. Для краткости обозначим $q^{\frac{1}{r}}$ через q_0, а $S_{2n}(q_0)$ через S_0. Из леммы 1.3.3 следует, что $r \cdot \omega(S_0) \subseteq \omega(G)$. Мы будем искать такое число $r_0 \in \omega(S_0)$, что $rr_0 \notin \omega(S)$.

Предположим, что $r = 2$. По лемме 1.2.1 выполнено следующее: $2^m \in \omega(S_0)$ тогда и только тогда, когда $2^m \in \omega(S)$. Пусть 2^m — максимальная степень двойки в $\omega(S_0)$ (а значит, и в $\omega(S)$). Тогда $2 \cdot 2^m \in 2 \cdot \omega(S_0) \subseteq \omega(G)$, но $2^{m+1} \notin \omega(S)$. Следовательно, $\omega(G) \neq \omega(S)$.

Теперь предположим, что r нечетно. Пусть $n = 2^{k-2} + 1$ для некоторого $k \geq 2$. Применяя лемму 1.2.1, получаем $2^k \in \mu(S_0)$, и аналогично $2^k \in \mu(S)$. Значит, $r \cdot 2^k \in r \cdot \omega(S_0) \subseteq \omega(G)$, но $r \cdot 2^k \notin \omega(S)$, и снова $\omega(G) \neq \omega(S)$.

Далее будем считать, что $n \neq 2^{k-2} + 1$. Обозначим $s = e(r, q)$. Подберем в качестве r_0 некоторый примитивный простой делитель числа $q_0^t - 1$, где $t \leq 2n$ удовлетворяет следующим условиям:

$$(t, r) = 1; \tag{2.4}$$

$$\left(\frac{t}{s}\right)^{sgn(t-s)} \textit{ не является нечетным натуральным числом;} \tag{2.5}$$

$$\eta(t) + \eta(s) > n. \tag{2.6}$$

Если выполнено (2.4), то r_0 также является примитивным простым делителем числа $q^t - 1$. По лемме 1.2.10 условия (2.5) и (2.6) гарантируют, что $rr_0 \notin \omega(S)$.

• Пусть $n = 4$. Предположим, что $\eta(s) = 1$, т.е. r делит $q - 1$ или $q + 1$. Выберем в качестве r_0 число $r_8(q_0)$ (напомним, что $r_8(q_0)$ обозначает примитивный простой делитель числа $q_0^8 - 1$). Поскольку $t = 8$ и r нечетно, $(t, r) = 1$ и условие (2.4) выполнено. Значит, r_0 является примитивным простым делителем числа $q^8 - 1$. Условия (2.5) and (2.6) очевидно выполнены:

$\eta(t)+\eta(s) = 4+1 > n$, при этом если r divides $q-1$, то $\frac{t}{s} = 8$, и если r divides $q+1$, то $\frac{t}{s} = 4$. По лемме 1.2.10 имеем $rr_0 \notin \omega(S)$.

Предположим, что $\eta(s) \in \{2, 3\}$. Положим $r_0 = r_8(q_0)$. Несложно проверить, что условия (2.4) и (2.6) выполнены.

Наконец, предположим, что $\eta(s) = 4$. Положим $t = 2$, т.е. $r_0 = r_2(q_0)$.

• Пусть $n = 6$. Предположим, что $\eta(s) = 1$. Если $r \neq 3$, положим $r_0 = r_{12}(q_0)$. Если $r = 3$, выберем в качестве r_0 произведение примитивных простых делителей двух различных чисел: $r_0 = r_8(q_0)r_4(q_0)$. Поскольку $(r, 8) = (r, 4) = 1$, числа $r_8(q_0)$ и $r_4(q_0)$ также являются примитивными простыми делителями чисел $q^8 - 1$ и $q^4 - 1$ соответственно. Ясно, что $r_8(q_0)r_4(q_0) \in \omega(S)$, а значит, $rr_8(q_0)r_4(q_0) \in r \cdot \omega(S_0)$. С другой стороны, $\eta(s) + \eta(8) + \eta(4) > n$ и числа $q^4 + 1$, $q^2 + 1$ и $q \pm 1$ попарно взаимно просты. по лемме 1.2.1 получаем, что $rr_8(q_0)r_4(q_0) \notin \omega(S)$.

Предположим, что $\eta(s) = 2$. Тогда $r_0 = r_8(q_0)r_2(q_0)$. Легко показать, что $rr_0 \in r\omega(S_0)$ и $rr_0 \notin \omega(S)$, следовательно, $\omega(G) \neq \omega(S)$.

Заметим, что r и q взаимно просты, поэтому из малой теоремы Ферма следует, что $r > 3$, если $s = e(r, q) > 2$ (последнее условие эквивалентно $\eta(s) \geq 2$).

Предположим, что $\eta(s) \in \{3, 5, 6\}$. Тогда $r_0 = r_8(q_0)$.

Предположим, что $\eta(s) = 4$. Если $r \neq 5$, положим $t = 10$, в противном случае положим $t = 6$. Тогда $r_0 = r_t(q_0)$. Отметим, что если $r = 5$ и $t = 6$, у числа $q_0^6 - 1$ существует примитивный простой делитель (в противном случае по лемме 1.1.3 выполнялось бы равенство $q_0^6 = 2^6$. Поскольку $q = q_0^5 = 2^5$, имеем $s = e(r, q) = e(5, 32) = 4$, а значит, $\eta(s) = 2$, но это противоречит предположению, что $\eta(s) = 4$).

• Пусть $n \geq 7$. Предположим, что $\eta(s) = 1$.

Случай 1: r делит $q + 1$. Если при этом r не делит n, положим $t = 2n$, если n четно (тогда $q + 1$ взаимно просто с $q^n + 1$), и $t = n$, если n нечетно (тогда $q + 1$ взаимно просто с $q^n - 1$). Если r делит n, то число $n \geq 7$ может быть представлено в виде суммы двух различных натуральных чисел k и l, удовлетворяющих условию (2.3) (лемма 2.1.1).

Предположим, что n четно. Если k и l — четные числа, $q + 1$ взаимно просто с $q^k + 1$ и $q^l + 1$, и мы можем положить $r_0 = r_{2k}(q_0)r_{2l}(q_0)$ (поскольку $(r, k) = (r, l) = 1$, числа $r_{2k}(q_0)$ и $r_{2l}(q_0)$ являются примитивными простыми

делителями чисел $q^{2k}-1$ и $q^{2l}-1$ соответственно). Если k и l — нечетные числа, $q+1$ взаимно просто с q^k-1 и q^l-1, и мы полагаем $r_0 = r_k(q_0)r_l(q_0)$. Теперь предположим, что n нечетно и $n = k+l$. Без ограничения общности считаем, что k четно, а l нечетно. Тогда $q+1$ взаимно просто с q^k+1 и q^l-1, и $r_0 = r_{2k}(q_0)r_l(q_0)$.

Случай 2: r делит $q-1$. Если при этом r не делит n, положим $t = 2n$ (поскольку $q-1$ взаимно просто с q^n+1). Если r делит n, положим $r_0 = r_{2k}(q_0)r_{2l}(q_0)$, где $k+l = n$ и k, l удовлетворяют условию (2.3) (поскольку $q-1$ взаимно просто с q^k+1 и q^l+1). Заметим, что если $n = 7$ (а значит, и $r = 7$) и $k = 3$, $l = 4$, то у числа $q_0^{2k}-1 = q_0^6-1$ существует примитивный простой делитель. (В противном случае выполнялись бы равенства $q_0 = 2$ и $q = 2^7$, но в этом случае r не может делить $q-1$. Значит, $q_0 \neq 2$).

Предположим, что $\eta(s) = 2$, т.е. r делит q^2+1.

Случай 1: r не делит то из чисел $\{n, n-1\}$, которое является нечетным. Если n нечетно (т.е. r не делит n), положим $r_0 = r_{2n}(q_0)$. Если n четно (т.е. r не делит $n-1$), то $r_0 = r_{2(n-1)}(q_0)$.

Случай 2: r делит нечетное из чисел $\{n, n-1\}$. Рассмотрим случай четного n (в противном случае можно провести аналогичное рассуждение, заменив n на $n-1$). Тогда r не делит n. Отметим, что q^2+1 не может одновременно делить числа q^n-1 и q^n+1 (при этом q^2+1 взаимно просто с тем из этих двух чисел, которое оно не делит). Выберем r_0 следующим образом. Если q^2+1 делит q^n-1 (это эквивалентно тому, что n делится на 4), то положим $r_0 = r_{2n}(q_0)$. Если q^2+1 делит q^n+1 (т.е. n четно и не делится на 4), положим $r_0 = r_n(q_0)r_{\frac{n}{2}}(q_0)$ (при этом выполняется равенство $\eta(s)+\eta(n)+\eta(\frac{n}{2}) = n+2 > n$, поскольку $\frac{n}{2}$ нечетно. Более того, q^2+1 взаимно просто с q^n-1).

Предположим, что $\eta(s) = 3$. Условие (2.6) влечет, что $\eta(t) \in \{n, n-1, n-2\}$. Два из этих трех чисел не делятся на $\eta(s) = 3$ (а значит, не делятся на 6. Отсюда следует существование примитивных простых делителей соответствующих чисел). Напомним, что $r > 3$ согласно малой теореме Ферма. Следовательно, по меньшей мере одно из двух чисел, не делящихся на 3, взаимно просто с r. Именно это число выбирается в качестве $\eta(t)$.

Предположим, что $\eta(s) \geq 4$. Тогда $\eta(t) \in \{n, n-1, n-2, n-3\}$. Хотя бы три числа из этого набора не делятся на $\eta(s)$. Отметим, что $\eta(t)$ не делит

$\eta(s)$, так как $\eta(t) > \frac{n}{2}$ и $\eta(t) \neq \eta(s)$. Поскольку $r > 3$, из этих трех чисел можно выбрать два, не делящихся также и на r, и по крайней мере одно из них не равно 6 — его мы и выбираем в качестве $\eta(t)$.

Мы нашли подходящие r_0 для всех возможных n и $\eta(s)$, тем самым этап 1 завершен.

Этап 2. Простые симплектические группы $S_{2n}(q)$, $n > 2$, не имеют ни внешних диагональных, ни внешних графовых автоморфизмов, поэтому для таких групп доказательство утверждения теоремы было проведено на этапе 1. Остается рассмотреть группу $S = S_4(q)$, где $q = 2^m > 2$. По [54, теорема 2.5.12] ее группа автоморфизмов устроена следующим образом: $\operatorname{Aut} S \simeq S \rtimes \langle\psi\rangle$, где $\langle\psi\rangle$ — циклическая группа порядка $2m$, порожденная графово-полевым (в терминах [54, определение 2.5.13]) автоморфизмом ψ группы S. Все элементы нечетного простого порядка в группе $\langle\psi\rangle$ являются полевыми автоморфизмами; они были рассмотрены на этапе 1. Единственная инволюция группы $\langle\psi\rangle$ — это автоморфизм ψ^m. Предположим,что m нечетно. Тогда централизатор автоморфизма ψ^m изоморфен группе ${}^2B_2(q)$ по [54, предложение 4.9.1]. Если r_0 — примитивный простой делитель q^2+1 (т.е. $r_0 = r_4(q)$), то $2 \cdot r_0 \in \omega(S\langle\psi^m\rangle)$ и $2 \cdot r_0 \notin \omega(S)$. Значит, $\omega(S\langle\psi^m\rangle) \neq \omega(S)$. Теперь предположим, что m четно. Тогда инволюция ψ^m являтся полевым автоморфизмом группы S. Теорема 1 доказана. □

§ 2.3. Расширения ортогональных групп четной размерности

Доказательство теоремы 2. Информация о группах со спектром как у группы $O_8^+(2)$ была приведена в параграфе 2.2. В [13] доказано, что группа $O_8^+(4)$ распознаваема по спектру. В [35] доказано, что группа $O_8^+(q)$ распознаваема по спектру при четном $q > 4$. Поэтому мы рассмотрим группы $O_{2n}^+(q)$ при $n > 4$ и $O_{2n}^-(q)$ при $n \geq 4$. Пусть S — простая ортогональная группа одной из указанных размерностей над полем характеристики 2, и пусть $S < G \leq \operatorname{Aut} S$, где группа G является расщепляемым расширением группы S посредством автоморфизма τ простого порядка r.

Этап 1. Предположим, что τ — полевой автоморфизм группы S (и в случае $S = O_{2n}^-(q)$ его порядок нечетен). Докажем, что в этом случае $\omega(G) \neq \omega(S)$. Мы обозначаем $q^{\frac{1}{r}}$ через q_0 и $O_{2n}^{\varepsilon}(q_0)$ через S_0.

Пусть τ — полевой автоморфизм порядка 2 группы $O^+_{2n}(q)$. По лемме 1.2.2 получаем, что 2^m — максимальная степень двойки в $\omega(S_0)$ тогда и только тогда, когда 2^m является максимальной степенью двойки в $\omega(S)$. Из леммы 1.3.3 следует, что $2\cdot 2^m \in 2\cdot\omega(S_0) \subseteq \omega(G)$, но $2^{m+1} \notin \omega(S)$. Значит, $\omega(G) \neq \omega(S)$.

Пусть теперь r — нечетное простое число. Если $n = 2^{k-2}+2$ для некоторого $k > 2$, то $2^k \in \mu(S_0)$ по лемме 1.2.2. Значит, $r\cdot 2^k \in r\omega(S_0) \subseteq \omega(G)$. Но $2^k \in \mu(S)$, поэтому $r\cdot 2^k \notin \omega(S)$. Имеем $\omega(G) \neq \omega(S)$.

Теперь предположим, что $n \neq 2^{k-2}+2$. Нам нужно подобрать примитивный простой делитель r_0 числа $q_0^t - 1$, где $t \leq 2n$ — некоторое натуральное число, удовлетворяющее (2.4), (2.5) и следующему условию:

$$2\eta(t) + 2\eta(s) > 2n - (1 - \varepsilon(-1)^{s+t}); \tag{2.7}$$

если $\varepsilon = +$, *то ни одна из цепочек равенств* (2.8)

$n = t = 2\eta(t) = 2\eta(s) = 2s$, $n = s = 2\eta(s) = 2\eta(t) = 2t$ *не выполняется.*

Условие (2.4) влечет, что r — примитивный простой делитель числа $q^t - 1$. Условия (2.5), (2.7), (2.8) дают возможность применять лемму 1.2.11 для доказательства несмежности вершин r и r_0 в графе $GK(S)$. Тем самым будет доказано, что $rr_0 \notin \omega(S)$.

• Пусть $n = 5$. Предположим, что $\eta(s) = 1$.

Случай 1: r делит $q - \varepsilon 1$ (напомним, что $\varepsilon = +$, если $S = O^+_{2n}(q)$, и $\varepsilon = -$, если $S = O^-_{2n}(q)$). Тогда $r_0 = r_8(q_0)$.

Случай 2: r делит $q + \varepsilon 1$. Если $\varepsilon = -$, то $r_0 = 8r_2(q_0)$. Из леммы 1.2.2 следует, что $r_0 \in \omega(S_0)$ и $rr_0 \notin \omega(S)$. Если $\varepsilon = +$ и у числа $q_0 - 1$ существует примитивный простой делитель, то $r_0 = 8r_1(q_0)$. Число $q_0 - 1$ не имеет примитивных простых делителей только в случае $q_0 = 2$. Отметим, что r делит $q + 1 = 2^r + 1$ и $2^{r-1} - 1$. Наибольший общий делитель этих трех чисел равен 3, следовательно, $r = 3$. Положим $r_0 = r_5(q_0)$.

Предположим, что $\eta(s) = 2$, т.е. r делит $q^2 + 1$. Тогда $r_0 = r_8(q_0)$.

Предположим, что $\eta(s) = 3$. Тогда из малой теоремы Ферма следует, что $r > 3$. Если r делит $q^3 - 1$, то $r_0 = r_6(q_0)$. Если r делит $q^3 + 1$, то $r_0 = r_3(q_0)$.

Предположим, что $\eta(s) \in \{4, 5\}$. Тогда $r_0 = r_4(q_0)$.

• Пусть $n \geq 7$. Предположим, что $\eta(s) = 1$.

Случай 1: r делит $q-1$. Обозначим

$$m = \begin{cases} n-1, & \text{если } \varepsilon = +, \\ n, & \text{если } \varepsilon = -. \end{cases} \tag{2.9}$$

Если r не делит m, то $r_0 = r_{2m}(q_0)$. Если r делит m, то существуют натуральные числа k и l, такие что $k+l = m+\varepsilon 1$ и k, l удовлетворяют условию (2.3) (если $\varepsilon = +$, такие k и l существуют для любого $n \geq 7$ по лемме 2.1.2; если $\varepsilon = -$, такие k и l существуют для любого $n > 9$ по лемме 2.1.3). Тогда $r_0 = r_{2k}(q_0)r_{2l}(q_0)$. Если $\varepsilon = -$ и $n = 7$, положим $r_0 = r_4(q_0)r_8(q_0)$, если $\varepsilon = -$ и $n = 9$, положим $r_0 = 4r_4(q_0)r_8(q_0)$. Во всех случаях имеем $rr_0 \notin \omega(S)$.

Случай 2: r делит $q+1$. Предположим, что r не делит n. Пусть $\varepsilon = +$. Если n нечетно, то $r_0 = r_n(q_0)$. Если n четно и r не делит $n-1$, то $r_0 = r_{n-1}(q_0)$. Если $n \geq 7$ четно и r делит $n-1$, то существуют числа k и l, удовлетворяющие условию (2.3), такие что $k+l = n$ (по лемме 2.1.2). Если k и l — четные числа, то $r_0 = r_{2k}(q_0)r_{2l}(q_0)$, в противном случае $r_0 = r_k(q_0)r_l(q_0)$.

Пусть $\varepsilon = -$. Если n нечетно и r не делит $n-1$, то $r_0 = r_{2(n-1)}(q_0)$. Если n нечетно и r делит $n-1$, то по лемме 2.1.2 существуют числа k и l, удовлетворяющие условию (2.3), такие что $k+l = n$. Считая, что k четно, а l нечетно, получаем, что $r_0 = r_{2k}(q_0)r_l(q_0)$. Если n четно, то $r_0 = r_{2n}(q_0)$.

Теперь предположим, что r делит n.

Пусть $\varepsilon = +$. Предположим, что n нечетно. По лемме 2.1.3 для любого $n > 9$ существуют числа k и l, удовлетворяющие условию (2.3), такие что $k+l = n-1$. Если k и l четны, то $r_0 = r_{2k}(q_0)r_{2l}(q_0)$, в противном случае $r_0 = r_k(q_0)r_l(q_0)$. Если $n = 7$, то $r_0 = r_4(q_0)r_8(q_0)$, если $n = 9$, то $r_0 = 4r_4(q_0)r_8(q_0)$. Теперь предположим, что n четно. Тогда $r_0 = r_{n-1}(q_0)$.

Пусть $\varepsilon = -$. Если n нечетно, то $r_0 = r_{2(n-1)}(q_0)$. Если n четно, то $n \neq 8$, поскольку n делится на нечетное число r, а значит, $n > 9$. По лемме 2.1.3 существуют числа k и l, удовлетворяющие условию (2.3), такие что $k+l = n-1$. Если k четно и l нечетно, то $r_0 = r_{2k}(q_0)r_l(q_0)$.

Предположим, что $\eta(s) = 2$. Обозначим через n' нечетное из чисел $\{n, n-1\}$. Допустим, r не делит n'. Тогда r_0 является примитивным простым делителем числа $q_0^{n'} - \varepsilon 1$. Теперь пусть r делит n'. Если n нечетно, то r_0 — примитивный простой делитель числа $q_0^{n-2} - \varepsilon 1$. Если n четно, то r делит $n-1$. Пусть $\varepsilon = +$. Поскольку $n-1 \geq 7$, по лемме 2.1.1 существуют

числа k и l, удовлетворяющие условию (2.3), такие что $k+l=n-1$. Следуя доказательству леммы 2.1.1, положим $\{k,l\}=\{\frac{n-2}{2},\frac{n}{2}\}$. Пусть k нечетно. Если $n\equiv 0 \pmod 8$ или $n\equiv 2 \pmod 8$, то l делится на 4. В этом случае $r_0=r_{2k}(q_0)r_{2l}(q_0)$. Если $n\equiv 4 \pmod 8$ или $n\equiv 6 \pmod 8$, то l четно и не делится на 4, т.е. $\frac{l}{2}$ нечетно. Тогда положим $r_0=r_{2k}(q_0)r_{\frac{l}{2}}(q_0)r_l(q_0)$ (несложно показать, что числа k и $\frac{l}{2}$ также не делят друг друга). Пусть $\varepsilon=-$. Если n делится на 4, то q^2+1 не делится на q^n+1. В этом случае $r_0=r_{2n}(q_0)$. Если $n\equiv 2 \pmod 4$, то q^2+1 не делит $q^{n-2}+1$. В этом случае $r_0=r_{2(n-2)}(q_0)$.

Предположим, что $\eta(s)=3$.

Случай 1: r делит q^3-1. Обозначим через n' то из чисел $\{n-1,n-2\}$, которое взаимно просто с r. Отметим, что числа q^3-1 и $q^{n'}+1$ взаимно просты при любом n'. Положим $r_0=r_{2n'}(q_0)$.

Случай 2: r делит q^3+1. Пусть $\varepsilon=+$. Если существует число $n'\in\{n-1,n-2\}$, взаимно простое и r и 3, то $r_0=r_{2n'}(q_0)$. В противном случае выберем нечетное число $n''\in\{n,n-3\}$. Это число взаимно просто с r и 3. Положим $r_0=r_{n''}(q_0)$. Пусть $\varepsilon=-$. Выберем число $n'\in\{n,n-1,n-2\}$, взаимно простое с r и 3, и положим $r_0=r_{2n'}(q_0)$.

Предположим, что $\eta(s)\geq 4$. Пусть $\varepsilon=+$. Если существует нечетное число $n'\in\{n,n-1,n-2,n-3\}$, взаимно простое с r и не делящееся на s, то $r_0=r_{n'}(q_0)$. В противном случае выберем наименьшее четное число $n'\in\{n,n-1,n-2,n-3\}$, взаимно простое с r и не делящееся на s. Тогда $r_0=r_{2n'}(q_0)$. Пусть $\varepsilon=-$. Существует $n'\in\{n,n-1,n-2,n-3\}$, взаимно простое с r и s и не равное 6. Положим $r_0=r_{2n'}(q_0)$.

Мы подобрали r_0 для всех возможных n и s. Таким образом, если τ — полевой автоморфизм группы S, то $\omega(S\rtimes\langle\tau\rangle)\neq\omega(S)$. Поскольку мы не рассматриваем группу $O_8^+(q)$, все внешние автоморфизмы нечетного простого порядка группы S являются полевыми автоморфизмами. В частности, далее мы можем предполагать, что $|G:S|=2$.

Этап 2. Рассмотрим инволютивные автоморфизмы группы $S=O_{2n}^{\varepsilon}(q)$, $q=2^m$. Пусть γ — графовый автоморфизм порядка 2 группы $O_{2n}^{\varepsilon}(q)$ (напомним, что мы не рассматриваем группы $O_8^+(q)$). Если m четно, обозначим через τ полевой автоморфизм порядка 2 группы $O_{2n}^+(q)$.

Пусть $S=O_{2n}^+(q)$. Тогда $\operatorname{Aut}S=S\rtimes(\langle\varphi\rangle\times\langle\gamma\rangle)$, где $\langle\varphi\rangle$ — группа полевых автоморфизмов порядка m. Таким образом, группа S имеет следующие

инволютивные автоморфизмы: γ, $\tau \in \langle\varphi\rangle$ (если m четно), $\tau\gamma$ (если m четно). Инволютивный полевой автоморфизм группы $O^+_{2n}(q)$ был рассмотрен на этапе 1. Для графового автоморфизма γ выполнено равенство $C_S(\gamma) = S_{2(n-1)}(q)$ в силу [54, предложение 4.9.2]. Подберем число $r_0 \in \omega(S_{2(n-1)}(q))$, такое что $2 \cdot r_0 \notin \omega(S)$. Пусть r_0 — примитивный простой делитель числа $q^{n-1} + 1$. По лемме 1.2.2 получаем, что $2 \cdot r_0 \notin \omega(S)$.

Для $\tau\gamma$ выполнено равенство $C_S(\tau\gamma) = O^-_{2n}(q^{1/2})$ в силу [54, предложение 4.9.1]. Подберем нечетное простое число r_0 в спектре централизатора, так чтобы выполнялось $2 \cdot r_0 \notin \omega(S)$. Выберем нечетное число $n' \in \{n, n-1\}$. Пусть $r_0 \in \omega(O^-_{2n}(q^{1/2}))$ — примитивный простой делитель числа $(q^{\frac{1}{2}})^{n'} + 1$. Тогда r_0 является примитивным простым делителем $q^{n'} - 1$, а значит, $2 \cdot r_0 \notin \omega(S)$.

Пусть $S = O^-_{2n}(q)$. Тогда $\operatorname{Aut} S$ является расщепляемым расширением группы S с помощью циклической подгруппы порядка $2m$, содержащей единственную инволюцию — графовый автоморфизм γ. В силу [54, предложение 4.9.2] выполнено равенство $C_S(\gamma) = S_{2(n-1)}(q)$. Пусть $r_0 \in \omega(S_{2(n-1)}(q))$ — примитивный простой делитель числа $q^{n-1} + 1$ (или $q^{n-1} - 1$, если $q = 2$ и $n = 4$). Из леммы 1.2.2 следует, что $2 \cdot r_0 \notin \omega(S)$. Теорема 2 доказана. $\square$

3. Исключительные группы

В данной главе доказываются критерии совпадения спектра нетривиального почти простого расширения исключительной группы S со спектром самой группы S, в случаях, когда S — одна из групп $F_4(q)$, где q нечетно, ${}^3D_4(q)$, $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$. Первая часть главы посвящена явному описанию спектров групп $F_4(q)$ и ${}^3D_4(q)$ (предложения 3.2.1 и 3.2.2). Основными результатами главы являются следующие теоремы.

Теорема 3. *Пусть $S = F_4(q)$, где q — степень нечетного простого числа p, и пусть $S < G \leqslant \operatorname{Aut} S$. Тогда $\omega(G) = \omega(S)$ в том и только том случае, если G/S является 2-группой и $p \notin \{3, 7, 11\}$.*

Теорема 4. *Пусть $S = {}^3D_4(q)$, где q — степень простого числа p, и пусть $S < G \leqslant \operatorname{Aut} S$. Тогда $\omega(G) = \omega(S)$ в том и только том случае, если G/S является 2-группой и $p \geq 7$.*

Теорема 5. *Пусть $S = E_6^{\varepsilon}(q)$, где q — степень простого числа p, и $S < G \leq \operatorname{Aut} S$. Тогда $\omega(G) = \omega(S)$ в том и только в том случае, когда G является расширением группы S с помощью полевого автоморфизма, G/S является 3-группой, 3 делит $q - \varepsilon 1$ и $p \notin \{2, 11\}$.*

Теорема 6. *Пусть $S = E_7(q)$, где q — степень простого числа p, и $S < G \leq \operatorname{Aut} S$. Тогда $\omega(G) = \omega(S)$ в том и только в том случае, когда G является расширением группы S с помощью полевого автоморфизма, G/S является 2-группой и $p \notin \{2, 13, 17\}$.*

Замечание. После доказательства основных теорем в параграфе 3.6 формулируется общая теорема B о распознаваемости по спектру простых исключительных групп лиева типа, поскольку теоремы 3–6 завершают исследование этой проблемы (см. теорему A). Для каждой простой исключительной группы S приводится число $h(S)$ попарно неизоморфных конечных групп G, изоспектральных S. В случаях, когда S почти распознаваема, все такие группы G изоморфны почти простым расширениям группы S, и их строение явно описывается в теореме B.

§ 3.1. Связные централизаторы полупростых элементов

Для описания спектров групп $F_4(q)$ и ${}^3D_4(q)$ мы используем подход, основанный на работе [44] о связных централизаторах полупростых элементов групп лиева типа.

Напомним, что для произвольного подмножества A группы G и произвольного простого числа p через $\omega_p(A)$ и $\omega_{p'}(A)$ обозначаются множества p-элементов и p'-элементов в A соответственно. Если σ — эндоморфизм группы G, то $G_\sigma = C_G(\sigma)$.

Пусть S — простая группа лиева типа над полем характеристики p, $\overline{F}$ — алгебраическое замыкание поля порядка p, $(\overline{G}, \sigma)$ — σ-представление для S, определенное в параграфе 1.3.

Спектр группы $G = \overline{G}_\sigma$ можно описать следующим образом. Для каждого элемента $g \in G$ существует единственное разложение $g = g_u g_s = g_s g_u$, где $|g_u|$ — степень числа p, а $|g_s|$ взаимно просто с p (это разложение Жордана-Шевалле для элемента g, где g_u и g_s — унипотентная и полупростая часть g соответственно). Обозначим через $\overline{C}^0$ компоненту связности единицы в группе $\overline{C} = C_{\overline{G}}(g_s)$. Тогда $\overline{C}^0$ является σ-инвариантной, и оба элемента g_u, g_s лежат в $\overline{C}^0$ [45, предложение 3.5.1 и теорема 3.5.3]. Определим связный централизатор элемента g_s как $C = (\overline{C}^0)_\sigma$. Тогда $|g_u| \in \omega_p(C)$ и $|g_s| \in \omega_{p'}(Z(C))$. Таким образом, для описания спектра группы S достаточно рассмотреть все связные централизаторы p'-элементов и найти порядки p-элементов в этих централизаторах, а также периоды их центров.

Далее мы кратко изложим результаты из [44].

Группа $\overline{C}^0$ — σ-инвариантная редуктивная подгруппа максимального ранга в $\overline{G}$. Зафиксируем некоторый максимальный тор $\overline{T}$ в $\overline{G}$ и рассмотрим корневую систему Φ группы $\overline{G}$ относительно $\overline{T}$. Обозначим через $\overline{X}_\alpha$ корневую подгруппу, соответствующую корню $\alpha \in \Phi$. Для любой замкнутой подсистемы Φ_1 в Φ группа $\overline{G}_1 = \langle \overline{T}, \overline{X}_\alpha \mid \alpha \in \Phi_1 \rangle$ является связной редуктивной группой в $\overline{G}$. И наоборот, всякая связная редуктивная группа в $\overline{G}$ максимального ранга может быть получена таким способом для некоторого максимального тора группы $\overline{G}$.

Предположим, что обе группы $\overline{T}$ и $\overline{G}_1 = \langle \overline{T}, \overline{X}_\alpha \mid \alpha \in \Phi_1 \rangle$ являются σ-инвариантными. Обозначим через $\mathcal{C}$ множество σ-инвариантных подгрупп,

сопряженных с $\overline{G}_1$. Если $\overline{G}_1^g \in \mathcal{C}$, то без ограничения общности можно считать, что $\overline{T}^g$ тоже σ-инвариантна. Тогда имеем $g^\sigma g^{-1} \in N_{\overline{G}}(\overline{G}_1) \cap N_{\overline{G}}(\overline{T})$. Пусть W и W_1 — группы Вейля групп $\overline{G}$ и $\overline{G}_1$ соответственно, и пусть π — естественный гомоморфизм из $N_{\overline{G}}(\overline{T})$ в W.

Лемма 3.1.1. [44, следствие 3] *Существует биекция между множеством G_σ-орбит на $\mathcal{C}$ и множеством классов σ-сопряженности группы $N_W(W_1)/W_1$, задаваемая правилом $G_1^g \to (wW_1)$, где $w = \pi(g^\sigma g^{-1})$.*

Лемма 3.1.2. [43, предложение 28] *Пусть W_2 — подгруппа W, порожденная отражениями в корнях, ортогональных всем корням из Φ_1. Тогда $W_1 \times W_2$ — нормальная подгруппа в $N_W(W_1)$, и $N_W(W_1)$ изоморфна группе симметрий, индуцированной W, на диаграмме Дынкина группы $\overline{G}_1$.*

Теперь опишем, как именно система Φ_1 и элемент $w \in N_W(W_1)$, где $w = \pi(g^\sigma g^{-1})$, определяют $\omega_p((\overline{G}_1^g)_\sigma)$ и структуру $Z(\overline{G}_1^g)_\sigma$.

Лемма 3.1.3. [83, предложение 0.5] *Пусть $\overline{G}$ — простая алгебраическая группа над алгебраически замкнутым полем характеристики $p > 0$, и пусть σ — сюръективный эндоморфизм группы $\overline{G}$, такой что $\overline{G}_\sigma$ конечна. Тогда период силовской p-подгруппы группы $\overline{G}_\sigma$ равен $min\{p^k \mid p^k > ht(\overline{G})\}$, где $ht(\overline{G})$ — наибольшая высота корня в корневой системе группы $\overline{G}$.*

Лемма 3.1.4. *Пусть $ht(\Phi_1)$ — максимум среди наибольших высот корней в неприводимых компонентах системы Φ_1. Тогда период силовской p-подгруппы группы $(\overline{G}_1^g)_\sigma$ равен to $p(\Phi_1) = min\{p^k \mid p^k > ht(\Phi_1)\}$.*

Доказательство. Это утверждение — несложное следствие леммы 3.1.3. Действительно, пусть $\overline{M} = \langle \overline{X}_\alpha \mid \alpha \in \Phi_1 \rangle$. Тогда $\overline{M}$ — коммутант группы $\overline{G}_1$, и $\overline{G}_1 = \overline{M}Z(\overline{G}_1)$. Поскольку $Z(\overline{G}_1) \leqslant \overline{T}$, все унипотентные элементы группы $\overline{G}_1$ лежат в $\overline{M}$, следовательно, $\omega_p((\overline{G}_1)_\sigma) = \omega_p(\overline{M}_\sigma)$. Группа $\overline{M}$ полупроста. Обозначим через $\overline{M}_1, \ldots, \overline{M}_l$ ее простые компоненты. Тогда $O^{p'}(\overline{M}_\sigma)$ — центральное произведение конечных групп, каждая из которых является фактор-группой группы $O^{p'}(C_{\overline{M}_i}(\sigma^{d_i}))$ по ее центральной подгруппе для некоторого i и некоторого положительного натурального числа d_i (см., например, [54, предложение 2.2.11]). Применяя лемму 3.1.3 к $C_{\overline{M}_i}(\sigma^{d_i})$, получаем требуемое. Это рассуждение также работает для $(\overline{G}_1^g)_\sigma$, поскольку σ — сюръективный эндоморфизм полупростой группы $\overline{M}^g$. □

Лемма 3.1.5. *Если* $w = \pi(g^\sigma g^{-1})$, *то* $(Z(\overline{G}_1)^g)_\sigma = (Z(\overline{G}_1)_{\sigma w})^g$, *и в частности,* $\omega(Z(\overline{G}_1^g)_\sigma) = \omega(Z(\overline{G}_1)_{\sigma w})$.

Доказательство. Пусть $x^g \in Z(\overline{G}_1)^g$. Тогда равенство $(x^g)^\sigma = x^g$ верно в том и только том случае, если $x^{\sigma g^\sigma g^{-1}} = x$, что эквивалентно $x^{\sigma n} = x$, где $n = g^\sigma g^{-1}$. Так как $n \in N_{\overline{G}}(\overline{G}_1)$ и $Z(\overline{G}_1) \leqslant \overline{T}$, мы можем определить действие элемента $w = \pi(n)$ на $Z(\overline{G}_1)$. Получаем

$$(Z(\overline{G}_1)^g)_\sigma = (Z(\overline{G}_1)_{\sigma w})^g$$

.

□

Обозначим множество $\bigcup_{\overline{H}\in\mathcal{C}} \omega(Z(\overline{H})_\sigma)$ через $p'(\Phi_1)$.

Лемма 3.1.6. *Предположим, что* $\Phi_1' \subseteq \Phi_1$ *и* $N_W(W_1)/W_1 = W_1W_2A/W_1$ *для некоторой* $A \leqslant N_W(W_1')$. *Тогда* $p'(\Phi_1) \subseteq p'(\Phi_1')$.

Доказательство. Пусть $Z = Z(\overline{G}_1)$ и $Z' = Z(\overline{G}_1')$. Из условия $\Phi_1' \subseteq \Phi_1$ следует, что $Z' \geqslant Z$ и $W_2' \geqslant W_2$. Если $w \in W_2A$, то Z' является w-инвариантной, а значит, $Z'_{\sigma w} \geqslant Z_{\sigma w}$. Применяя лемму 3.1.1, получаем, что

$$p'(\Phi_1) = \bigcup_{w\in W_2A} \omega(Z_{\sigma w}) \subseteq \bigcup_{w\in W_2'A} \omega(Z'_{\sigma w}) \subseteq p'(\Phi_1').$$

□

§ 3.2. Спектры групп $F_4(q)$ и ${}^3D_4(q)$

Как и в предыдущем параграфе, $\overline{F}$ — алгебраическое замыкание поля простого порядка p, $\overline{G}$ — простая алгебраическая группа над $\overline{F}$, $\overline{T}$ — фиксированный максимальный тор в $\overline{G}$, Φ — корневая система группы $\overline{G}$. Зафиксируем также фундаментальную подсистему $\Pi = \{\alpha_1, \ldots, \alpha_n\}$ в Φ и порождающие Шевалле $x_\alpha(t)$, $n_\alpha(t)$ и $h_\alpha(t)$ группы $\overline{G}$ относительно $\overline{T}$ [54, определение 1.12.2]. Для краткости обозначим $h_{\alpha_i}(t)$ через $h_i(t)$. Если $\overline{G}$ — односвязная группа, эти порождающие удовлетворяют следующим свойствам [54, теорема 1.12.1]:

$$\overline{T} = \langle h_\alpha(t) \mid \alpha \in \Pi, t \in \overline{F}^* \rangle, \tag{3.10}$$

$$\prod_{i=1}^{n} h_i(t_i) = 1 \Leftrightarrow t_i = 1 \text{ для всех } 1 \leqslant i \leqslant n, \tag{3.11}$$

$$h_\beta(t)^{-1}x_\alpha(u)h_\beta(t) = x_\alpha(ut^{\langle\alpha,\beta\rangle}), \text{ где } \langle\alpha,\beta\rangle = 2(\alpha,\beta)/(\beta,\beta), \qquad (3.12)$$

для всех $\alpha, \beta \in \Phi, u \in \overline{F}, t \in \overline{F}^*$.

Предложение 3.2.1. *Множество порядков элементов простой группы $S = F_4(q)$, где q — степень простого числа p, совпадает с множеством делителей следующих чисел:*

1) $q^4 - q^2 + 1$, $q^4 + 1$, $(q^2 \pm q + 1)(q^2 - 1)$, $(q^4 - 1)/(2, q - 1)$;

2) $p(q^3 \pm 1)$, $p(q^2 + 1)(q \pm 1)$, $p(q^2 - 1)$;

3) $4(q^2 \pm 1)$, $4(q^2 \pm q + 1)$, $8(q \pm 1)$, 16, *если* $p = 2$;

4) $9(q^2 \pm 1)$, 27, *если* $p = 3$;

5) $25(q \pm 1)$, *если* $p = 5$;

6) $49 \cdot 2$, *если* $p = 7$;

7) 121, *если* $p = 11$.

Доказательство. Если $p = 2$, утверждение доказано в [9, лемма 1.6]. Докажем утверждение для нечетного p.

Всякий полупростой элемент группы S лежит в некотором максимальном торе. Структура максимальных торов в S описана в [67, стр. 94–96]. Из этого описания следует, что $\omega_{p'}(S)$ состоит из всех делителей чисел, перечисленных в пункте 1) предложения.

Поскольку $ht(F_4) = 11$, из леммы 3.1.3 следует, что период силовской p-подгруппы в S равен 27 при $p = 3$, p^2 при $p \in \{5, 7, 11\}$ и p при $p > 11$.

Остается найти *смешанные* порядки элементов (т.е. порядки элементов, не являющихся ни p-, ни p'-элементами). В соответствии с предыдущим параграфом, достаточно найти множества $p(\Phi_1) \cdot p'(\Phi_1)$ для всех непустых собственных замкнутых подсистем Φ_1 в F_4 , для которых найдется σ-инвариантная подгруппа, сопряженная с соответствующей редуктивной подгруппой (при этом нам не требуется критерий того, что редуктивная подгруппа является связным централизатором, поскольку спектр любой подгруппы в $\overline{G}_\sigma$ очевидно является подмножеством в $\omega(\overline{G}_\sigma)$).

Пусть $(\overline{G}, \sigma)$ — стандартное σ-представление для S. Все необходимые подсистемы Φ_1, а также классы сопряженности группы $N_W(W_1)/W_1$, найдены в [80] и [48]. Пронумеруем корни в системе Φ типа F_4 в соответствии с [48, с. 126]. В частности, все фундаментальные корни пронумерованы как на рис. 1, и через α_0 обозначен корень наибольшей высоты. Кроме того, если $\{e_1, e_2, e_3, e_4\}$ — ортонормированный базис евклидова пространства, в которое вкладывается Φ, то $\alpha_1 = e_2 - e_3$, $\alpha_2 = e_3 - e_4$, $\alpha_3 = e_4$, $\alpha_4 = \frac{1}{2}(e_1 - e_2 - e_3 - e_4)$ и $\alpha_0 = e_1 + e_2$. Нам также потребуются корни $\alpha_8 = e_1$ и $\alpha_{15} = \frac{1}{2}(e_1 + e_2 + e_3 - e_4)$.

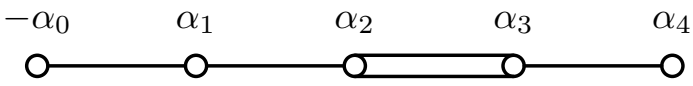

Рис. 1. Расширенная диаграмма Дынкина типа F_4

Для корневой системы типа Ψ будем обозначать через $\widetilde{\Psi}$ подсистему, состоящую из коротких корней. Отметим следующее полезное свойство корневой системы Φ: две ее подсистемы W-сопряжены тогда и только тогда, когда их типы совпадают.

Разделим все подсистемы на четыре класса в соответствии со значением $ht(\Phi_1)$. Для каждой подсистемы Φ_1 в таблице 1 содержится информация о выбранной фундаментальной подсистеме Π_1 в Φ_1 и структуре группы $N_W(W_1)$. В описании этой структуры через -1 обозначена единственная центральная инволюция группы W (эта инволюция переводит корень α в $-\alpha$), а через w_{15} — отражение в корне α_{15}. Информация, касающаяся $N_W(W_1)$, взята из [80, таблица 2].

Напомним, что $p(\Phi_1) = min\{p^k \mid p^k > ht(\Phi_1)\}$ и $p'(\Phi_1) = \bigcup_{w \in B} \omega(Z_{\sigma w})$, где $Z = Z(\overline{G}_1)$ и $\{wW_1 \mid w \in B\}$ — полный набор представителей классов сопряженности группы $N(W_1)/W_1$. Также напомним, что $ht(A_n) = n$ и $ht(B_n) = ht(C_n) = 2n - 1$.

Обозначим через Φ_2 подсистему в Φ, состоящую из корней, ортогональных всем корням из Φ_1. Тогда $Z(\overline{G}_1)$ содержит группу $\overline{T}_2 = \{h_\alpha(t) \mid \alpha \in \Phi_2, t \in \overline{F}^*\}$ согласно (3.12). Группа $\overline{T}_2$ представляет собой максимальный тор полупростой группы $\overline{G}_2 = \{\overline{X}_\alpha \mid \alpha \in \Phi_2\}$. Напомним, что $W_2 \leqslant W$ — подгруппа, порожденная отражениями в корнях из Φ_2. Поскольку W_2 вкладывается в $N_W(W_1)/W_1$ по лемме 3.1.2, а W_2 — группа Вейля группы $\overline{G}_2$, имеем $\omega_{p'}((\overline{G}_2)_\sigma) \subseteq p'(\Phi_1)$. Более того, если $Z(\overline{G}_1) = \overline{T}_2$ и $N_W(W_1) = W_1 \times W_2$,

Таблица 1. Подсистемы Φ_1

$ht(\Phi_1)$	Φ_1	Π_1	$N_W(W_1)$
1	A_1	$\{-\alpha_0\}$	$W_1 \times W_2$
	$\tilde{A}_1$	$\{\alpha_8\}$	$W_1 \times W_2$
	$2A_1$	$\{-\alpha_0, \alpha_2\}$	$\langle w_{15}\rangle W_1 \times W_2$
	$A_1 + \tilde{A}_1$	$\{-\alpha_0, \alpha_3\}$	$W_1 \times W_2$
	$2A_1 + \tilde{A}_1$	$\{-\alpha_0, \alpha_2, \alpha_4\}$	$\langle w_{15}\rangle W_1 \times \langle -1\rangle$
2	A_2	$\{-\alpha_0, \alpha_1\}$	$W_1 \times W_2 \times \langle -1\rangle$
	$\tilde{A}_2$	$\{\alpha_3, \alpha_4\}$	$W_1 \times W_2 \times \langle -1\rangle$
	$A_2 + \tilde{A}_1$	$\{-\alpha_0, \alpha_1, \alpha_3\}$	$W_1 \times W_2 \times \langle -1\rangle$
	$\tilde{A}_2 + A_1$	$\{-\alpha_0, \alpha_3, \alpha_4\}$	$W_1 \times W_2 \times \langle -1\rangle$
	$A_2 + \tilde{A}_2$	$\{-\alpha_0, \alpha_1, \alpha_3, \alpha_4\}$	$W_1 \times W_2 \times \langle -1\rangle$
3	B_2	$\{\alpha_2, \alpha_3\}$	$W_1 \times W_2$
	$B_2 + A_1$	$\{-\alpha_0, \alpha_2, \alpha_3\}$	$W_1 \times W_2$
	A_3	$\{-\alpha_0, \alpha_1, \alpha_2\}$	$W_1 \times W_2 \times \langle -1\rangle$
	$A_3 + \tilde{A}_1$	$\{-\alpha_0, \alpha_1, \alpha_2, \alpha_4\}$	$W_1 \times W_2 \times \langle -1\rangle$
≥ 5	B_3	$\{\alpha_1, \alpha_2, \alpha_3\}$	$W_1 \times W_2$
	C_3	$\{\alpha_2, \alpha_3, \alpha_4\}$	$W_1 \times W_2$
	$C_3 + A_1$	$\{-\alpha_0, \alpha_2, \alpha_3, \alpha_4\}$	W_1
	B_4	$\{-\alpha_0, \alpha_1, \alpha_2, \alpha_3\}$	W_1

мы получаем равенство. Заметим, что в силу односвязности $\overline{G}$ группа $\overline{G}_2$ тоже односвязна при условии того, что Φ_2 — подсистема, порожденная фундаментальными корнями, или по крайней мере эквивалентна такой подсистеме [54, предложение 2.6.2].

Пусть $p(\Phi_1) = p$. Предположим, что $A_1 \subseteq \Phi_1$ и $\Phi_1 \neq 2A_1, 2A_1 + \widetilde{A}_1$. Тогда, в соответствии с таблицей 1, имеем $N_W(W_1) = W_1 \times W_2$ или $N_W(W_1) = W_1 \times W_2 \times \langle -1\rangle$. Поскольку -1 центральна в W, получаем, что $N_W(W_1)$ удовлетворяет предположению леммы 3.1.6, где $\Phi_1' = A_1$. Таким образом, $p'(\Phi_1) \subseteq p'(A_1)$. Аналогично, если $\widetilde{A}_1 \subseteq \Phi_1$ и $A_1 \not\subseteq \Phi_1$, то $p'(\Phi_1) \subseteq p'(\widetilde{A}_1)$, и если $2A_1 \subseteq \Phi_1$, то $p'(\Phi_1) \subseteq p'(2A_1)$. Следовательно, достаточно рассмотреть A_1, $\widetilde{A}_1$ и $2A_1$.

Предположим, что $\Phi_1 = \widetilde{A}_1$, где $\Pi_1 = \{\alpha_8\}$. Тогда $\Phi_2 = \langle \alpha_1, \alpha_2, \alpha_3\rangle$

— система типа B_3. В силу того, что $\langle\alpha_8, \alpha_4\rangle = 1$ и $\langle\alpha_8, \alpha_i\rangle = 0$ для всех $1 \leqslant i \leqslant 3$, из (3.10)–(3.12) следует, что $Z(\overline{G}_1) = \{h_1(t_1)h_2(t_2)h_3(t_3) \mid t_i \in \overline{F}^*\}$. Иными словами, $Z(\overline{G}_1)$ — максимальный тор в $\overline{G}_2$. Учитывая, что $N_W(W_1) = W_1 \times W_2$, получаем, что $p'(\widetilde{A}_1) = \omega_{p'}((\overline{G}_2)_\sigma)$. Группа $\overline{G}_2$ — простая односвязная группа типа B_3. Следовательно, $(\overline{G}_2)_\sigma \simeq Spin_7(q)$, а значит, $p'(\widetilde{A}_1)$ состоит из всех делителей чисел $q^3 \pm 1$, $(q^2+1)(q \pm 1)$, (q^2-1) [20].

Предположим, что $\Phi_1 = A_1$, где $\Pi_1 = \{-\alpha_0\}$. Тогда $\Phi_2 = \langle\alpha_2, \alpha_3, \alpha_4\rangle$. Поскольку $\langle\alpha_0, \alpha_1\rangle = -1$ и $\langle\alpha_0, \alpha_i\rangle = 0$ для всех $2 \leqslant i \leqslant 4$, получаем $Z(\overline{G}_1) = \overline{T}_2$. Тем самым $p'(A_1) = \omega_{p'}(Sp_6(q)) \subseteq \omega_{p'}(Spin_7(q))$.

Предположим, что $\Phi_1 = 2A_1$, где $\Pi_1 = \{-\alpha_0, \alpha_2\}$. Тогда $\Phi_2 = \langle\alpha_4, \alpha_{13}\rangle$ и $N_W(W_1)/W_1 \simeq W_2 \times \langle w_{15}\rangle$. Вычисления показывают, что $Z(\overline{G}_1) = \overline{T}_2 \times \langle h_2(-1)\rangle$. Поскольку α_{15} ортогонален всем корням из Φ_2, получаем, что $(\overline{T}_2)_{\sigma w}$ изоморфна некоторому максимальному тору группы $(\overline{G}_2)_\sigma$ для любого $w \in W_2 \times \langle w_{15}\rangle$. Периоды максимальных торов в $(\overline{G}_2)_\sigma \simeq Sp_4(q)$ в точности равны $q^2 \pm 1$, $(q^2-1)/2$, $q \pm 1$ (см., например, [5]). Если $h \in Z(\overline{G}_1)$, то $h^2 \in \overline{T}_2$, а значит, период группы $Z(\overline{G}_1)_{\sigma w}$ может превосходить период группы $(\overline{T}_2)_{\sigma w}$ не больше, чем в два раза. Поскольку $2(q^2+1)$ делит $(q^2+1)(q-1)$, $2(q \pm 1)$ делит q^2-1, и $2(q^2-1) \notin \omega_{p'}(S)$ в силу (1), мы можем заключить, что $p'(2A_1) \subseteq p'(\widetilde{A}_1)$.

Тем самым мы проверили все числа из пункта 2) предложения.

Пусть $p(\Phi_1) = p^2$. Тогда $ht(\Phi_1) \geqslant 3$. Как показывает лемма 3.1.6, достаточно рассмотреть B_2 и A_3 при $p = 3$, B_3 и C_3 при $p = 5$, B_4 при $p = 7$. Если Φ_1 имеет тип B_2, B_3 или C_3, то $Z(\overline{G}_1) = \overline{T}_2$, $N_W(W_1) = W_1 \times W_2$, и, рассуждая как и выше, мы заключаем, что $p'(B_2) = \omega_{p'}(Spin_4(q))$ и $p'(B_3) = p'(C_3) = \omega_{p'}(SL_2(q))$. Если $\Phi_1 = B_4$, то $Z(\overline{G}_1) = \langle h_3(-1)\rangle$. Отсюда получаем элементы порядка $2 \cdot 49$ при $p = 7$. Наконец, если $\Phi_1 = A_3$, то $Z(\overline{G}_1) = \overline{T}_2 \times \langle h_3(-1)\rangle$. Следовательно, $p'(A_3)$ состоит из делителей чисел $2(q \pm 1)$, поэтому $p'(A_3) \subseteq p'(B_2)$.

Предложение доказано. □

Предложение 3.2.2. *Множество порядков элементов простой группы ${}^3D_4(q)$, где q — степень простого числа p, совпадает с множеством делителей следующих чисел:*

1) $(q^3-1)(q+1)$, $(q^3+1)(q-1)$, q^4-q^2+1;

2) $p(q^3 \pm 1)$;

3) $4(q^2 \pm q + 1)$, 8, *если* $p = 2$;

4) p^2, *если* $p \in \{3, 5\}$.

Доказательство. Пусть $S = {}^3D_4(q)$. Пронумеруем фундаментальные корни системы Φ типа D_4 как на рис. 2 и обозначим через α_0 корень наибольшей высоты.

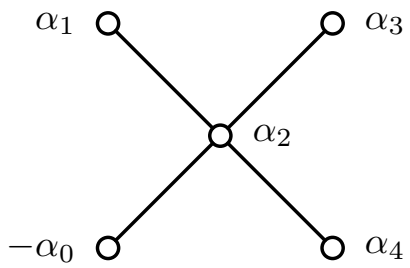

Рис. 2. Расширенная диаграмма Дынкина типа D_4

Пусть ρ — симметрия диаграммы Дынкина системы Φ, такая что $\rho : \alpha_1 \to \alpha_3 \to \alpha_4 \to \alpha_1$ и $\rho(\alpha_2) = \alpha_2$, и пусть $(\overline{G}, \sigma)$ — стандартное σ-представление для S с графовым автоморфизмом γ, индуцированным ρ. Поскольку $ht(D_4) = 5$, из леммы 3.1.3 следует, что p-период группы S равен 8 при $p = 2$, p^2 при $p = 3, 5$ и p при $p \geqslant 7$. Порядки полупростых элементов несложно получить из описания максимальных торов группы S в [50, таблица 1.1]. Кроме того, эта таблица показывает, что

$$\overline{T}_\sigma = \{h_1(t_1)h_2(t_2)h_3(t_1^q)h_4(t_1^{q^2}) \mid t_1^{q^3-1} = t_2^{q-1} = 1\},$$

и если w_0 — отражение в корне α_0, имеем

$$\overline{T}_{\sigma w_0} = \{h_1(t)h_2(t^{1-q^3})h_3(t^{q^4})h_4(t^{q^2}) \mid t^{(q^3-1)(q+1)} = 1\}.$$

Как и в доказательстве предложения 3.2.1, остается найти множества $p(\Phi_1) \cdot p'(\Phi_1)$ для всех непустых собственных замкнутых подсистем Φ_1 в системе D_4, для каждой из которых существует σ-инвариантная подгруппа, сопряженная с соответствующей редуктивной подгруппой. В соответствии с [50, таблица 1.0], эти подсистемы порождаются следующими наборами корней: $\{-\alpha_0\}$, $\{\alpha_2, -\alpha_0\}$, $\{\alpha_1, \alpha_3, \alpha_4\}$, $\{\alpha_1, \alpha_3, \alpha_4, -\alpha_0\}$.

В первых двух случаях $Z(\overline{G}_1)$ — связная группа, и структура групп $Z(\overline{G}_1^g)_\sigma$ описана в [50, таблицы 2.2a и 2.2b]. Эти таблицы также показывают, что множества $p'(\{-\alpha_0\})$ и $p'(\{\alpha_2, -\alpha_0\})$ состоят из делителей чисел $q^3 \pm 1$ и $q^2 \pm q + 1$ соответственно. Поскольку $p(A_2) = p$ при $p > 2$ и $p(A_2) = 4$ при $p = 2$, получаем элементы порядков $p(q^3 \pm 1)$ и, кроме того, порядков $4(q^2 \pm q + 1)$, если $p = 2$.

Предположим, что $\Phi_1 = \langle \alpha_1, \alpha_3, \alpha_4 \rangle$. Из (3.10)–(3.12) следует, что $Z(\overline{G}_1) = \{h_1(t_1)h_2(t_2)h_3(t_3)h_4(t_4) \mid t_1^2 = t_3^2 = t_4^2 = t_2\}$. Полный набор представителей классов σ-сопряженности группы $N_W(W_1)/W_1$ задается множеством $\{1, w_0\}$ [50, таблица 2.1]. Используя равенство $Z(\overline{G}_1)_{\sigma w} = Z(\overline{G}_1) \cap \overline{T}_{\sigma w}$, мы получаем

$$Z(G_1)_\sigma = \{h_1(t)h_2(t^2)h_3(t^q)h_4(t^{q^2}) \mid t^{2(q-1)} = t^{q^3-1} = 1\}$$

и

$$Z(G_1)_{\sigma w_0} = \{h_1(t)h_2(t^2)h_3(t^{q^4})h_4(t^{q^2}) \mid t^{2(q^2-1)} = t^{q^3+1} = 1\}.$$

Поскольку $(2(q-1), q^3-1)) = q-1$ и $(2(q^2-1), q^3+1) = q+1$, имеем $p'(\Phi_1) \subseteq p'(A_1)$.

Наконец, предположим, что $\Phi_1 = \langle \alpha_1, \alpha_3, \alpha_4, -\alpha_0 \rangle$. Тогда $N_W(W_1)/W_1$ имеет один класс σ-сопряженности [50, таблица 2.1], и

$$Z(\overline{G}_1) = \{h_1(t_1)h_2(t_2)h_3(t_3)h_4(t_4) \mid t_1^2 = t_3^2 = t_4^2 = t_2 = 1\}.$$

Тем самым, $p'(\Phi_1) = \{1, (2, q-1)\}$, и предложение доказано. □

§ 3.3. Расширения групп $F_4(q)$ и ${}^3D_4(q)$

Пусть S — одна из групп $F_4(q)$, где q нечетно, или ${}^3D_4(q)$. Пусть $q = p^m$, ϕ — полевой автоморфизм группы S, определенный в параграфе 1.3, и γ — графовый автоморфизм порядка 3 группы ${}^3D_4(q)$, определенный в доказательстве предложения 3.2.2.

Нам потребуется следующая числовая лемма.

Лемма 3.3.1. *Если $q_0 > 1$ — нечетное целое число, и $q = q_0^{2^l}$, то*

1) *$2^l(q_0^4 - q_0^2 + 1)$ и $2^l(q_0^2 \pm q_0 + 1)(q_0^2 - 1)$ делят $(q^2 + q + 1)(q^2 - 1)$ или $(q^2 - q + 1)(q^2 - 1)$;*

2) $2^l(q_0^4+1)$ *и* $2^{l-1}(q_0^4-1)$ *делят* $\frac{q^4-1}{2}$*;*

3) $2^l(q_0^3\pm 1)$ *делит* q^3-1*;*

4) $2^l(q_0^2+1)(q_0\pm 1)$ *и* $2^l(q_0^2-1)$ *делят* q^2-1*;*

5) $2^l(q_0\pm 1)$ *делит* $q-1$.

Доказательство. Если $l=1$, то $2(q_0^4-q_0^2+1)$ делит $q_0^6+1=q^3+1$, а значит, делит и $(q^2-q+1)(q^2-1)=(q^3+1)(q-1)$. Если $l>1$, то $2^l(q_0^4-q_0^2+1)$ делит число $2^l(q_0^6+1)$, в свою очередь делящее $(q_0^{3\cdot 2^l}-1)(q_0^{2^l}+1)=(q^2+q+1)(q^2-1)$. Действительно,

$$(q_0^{3\cdot 2^l}-1)(q_0^{2^l}+1)= \tag{3.13}$$

$$\underbrace{(q_0^{3\cdot 2^{l-1}}+1)(q_0^{3\cdot 2^{l-2}}+1)\dots(q_0^{3\cdot 2^1}+1)(q_0^3+1)(q_0^3-1)(q_0^{2^l}+1)}_{l+2\ \textit{четных сомножителей}},$$

поэтому $(q_0^{3\cdot 2^l}-1)(q_0^{2^l}+1)$ является произведением числа q_0^6+1 и $l+1$ четных чисел. Из (3.13) также получаем, что $2^l(q_0^2\pm q_0+1)(q_0^2-1)=2^l(q_0^3\pm 1)(q_0\mp 1)$ делит $(q_0^{3\cdot 2^l}-1)(q_0^{2^l}+1)$. Далее,

$$\frac{q^4-1}{2}=\frac{q_0^{2^{l+2}}-1}{2}= \tag{3.14}$$

$$\frac{1}{2}\underbrace{(q_0^{2^{l+1}}+1)(q_0^{2^l}+1)\dots(q_0^{2^2}+1)(q_0^{2^1}+1)(q_0^2-1)}_{l+2\ \textit{четных сомножителей}},$$

поэтому $\frac{q^4-1}{2}$ может быть представлено как произведение либо q_0^4+1 и числа, кратного 2^l, либо q_0^4-1 и числа, кратного 2^{l-1}. Далее, $2^l(q_0^3\pm 1)$ делит q^3-1 в силу

$$q^3-1=q_0^{3\cdot 2^l}-1=\underbrace{(q_0^{3\cdot 2^{l-1}}+1)\dots(q_0^{3\cdot 2^1}+1)(q_0^3+1)(q_0^3-1)}_{l+1\ \textit{четных сомножителей}}, \tag{3.15}$$

поэтому q^3-1 может быть представлено как произведение числа q_0^3-1 или q_0^3+1 и числа, кратного 2^l.

$$q^2-1=q_0^{2^{l+1}}-1=\underbrace{(q_0^{2^l}+1)\dots(q_0^{2^1}+1)(q_0+1)(q_0-1)}_{l+2\ \textit{четных сомножителей}}, \tag{3.16}$$

поэтому q^2-1 может быть представлено как произведение числа $(q_0^2+1)(q_0\pm1)$ или q_0^2-1 и числа, кратного 2^l, а значит, $2^l(q_0^2+1)(q_0\pm1)$ и $2^l(q_0^2-1)$ делят q^2-1. Наконец,

$$q-1=q_0^{2^l}-1=\underbrace{(q_0^{2^{l-1}}+1)\dots(q_0^{2^1}+1)(q_0+1)(q_0-1)}_{l+1\ \textit{четных сомножителей}}. \tag{3.17}$$

Аналогичное рассуждение показывает, что $2^l(q_0\pm1)$ делит $q-1$, и лемма доказана. □

Доказательство теоремы 3. Пусть $S=F_4(q)$, где q нечетно, и $S<G\leqslant \operatorname{Aut}S$. В силу [68,69], если $\omega(G)=\omega(S)$, то G/S является $\{2,3\}$-группой. По [54, теорема 2.5.12] имеем $\operatorname{Aut}S=S\rtimes\langle\varphi\rangle$, а значит, $G=S\rtimes\langle\psi\rangle$ для некоторого $\psi\in\langle\varphi\rangle$. Пусть $|\psi|=k$. По лемме 1.3.3

$$\omega(G)=\bigcup_{r|k} r\omega(F_4(q^{\frac{1}{r}})).$$

Если k делится на 3, то $\omega(G)$ содержит подмножество $3\cdot\omega(F_4(q_0))$, где $q_0^3=q$. Отсюда легко получить, что $3(q_0^4+1)\in\omega(G)\backslash\omega(S)$.

Теперь предположим, что $k=2^t$. Если $p=3$, то $kp^3\in\omega(G)\backslash\omega(S)$, если $p=7$, то $2kp^2\in\omega(G)\backslash\omega(S)$, и если $p=11$, то $kp^2\in\omega(G)\backslash\omega(S)$. Докажем, что при $p=5$ или $p>11$ выполнено равенство $\omega(G)=\omega(S)$. Из теоремы 3.2.1 следует, что $\omega(S)$ состоит из всех делителей чисел q^4-q^2+1, q^4+1, $(q^2\pm q+1)(q^2-1)$, $\frac{q^4-1}{2}$, $p(q^3\pm1)$, $p(q^2+1)(q\pm1)$, $p(q^2-1)$ и $p^2(q\pm1)$ if $p=5$. С другой стороны,

$$\omega(G)=\bigcup_{0\leq l\leq t} 2^l\cdot\omega(F_4(q^{\frac{1}{2^t}})).$$

Поскольку множество $2^l\cdot\omega(F_4(q_0))$ состоит из всех делителей чисел $2^l(q_0^4-q_0^2+1)$, $2^l(q_0^4+1)$, $2^l(q_0^2\pm q_0+1)(q_0^2-1)$, $2^{l-1}(q_0^4-1)$, $2^lp(q_0^3\pm1)$, $2^lp(q_0^2+1)(q_0\pm1)$, $2^lp(q_0^2-1)$ и $2^lp^2(q_0\pm1)$ при $p=5$, мы применяем лемму 3.3.1 и получаем, что $2^l\cdot\omega(F_4(q_0))\subseteq\omega(S)$ для любого l, и значит, $\omega(G)\subseteq\omega(S)$. Тем самым $\omega(G)=\omega(S)$ и теорема 3 доказана. □

Доказательство теоремы 4. Пусть $S={}^3D_4(q)$ и $S<G\leqslant\operatorname{Aut}S$. Если $\omega(G)=\omega(S)$, то G/S — $\{2,3\}$-группа в силу [68, 69]. По [54, теорема

2.5.12] имеем $\operatorname{Aut} S = S \rtimes \langle\varphi\rangle$, а значит, $G = S \rtimes \langle\psi\rangle$ для некоторого $\psi \in \langle\varphi\rangle$. Пусть $|\psi| = k$.

Предположим, что k делится на 3. Тогда из равенства $\gamma = \varphi^{|\varphi|/3}$ следует, что $\gamma \in G$. Централизатор $C_S(\gamma)$ изоморфен группе $G_2(q)$ (см. (9-1) в [53]). Значит, $\omega(G) \supseteq 3 \cdot \omega_{3'}(G_2(q))$. По [11, лемма 1.4], спектр группы $G_2(q)$ состоит из всех делителей чисел $(q^2 \pm q + 1)$, $q^2 - 1$, $p(q \pm 1)$ и, вдобавок, делителей числа p^2, если $p \in \{3, 5\}$. Докажем, что для любого простого числа p существует число $r \in \omega_{3'}(G_2(q))$, такое что $3r \notin \omega(S)$. Действительно, если $p = 2$, то $r = p^3$, а если $p = 5$, то $r = p^2$. Если $p = 3$, то $r = q^2 - 1$ (это число удовлетворяет нашему условию на r, поскольку единственные числа в $\mu(S)$, кратные r, равны $(q^3 \pm 1)(q \mp 1)$). Теперь предположим, что $p \geq 7$ и $q \equiv \varepsilon \pmod 3$, $\varepsilon \in \{1, -1\}$. Тогда $r = p(q + \varepsilon)$. Поскольку $p(q^3 + \varepsilon)$ — единственное число в $\mu(S)$, кратное r, и $q^3 + \varepsilon$ не делится на 3, получаем, что $3r \notin \omega(S)$. Следовательно, $3 \cdot \omega_{3'}(G_2(q)) \not\subseteq \omega(S)$ и $\omega(G) \not\subseteq \omega(S)$. Значит, k не делится на 3, т.е. G/S является 2-группой.

Пусть $k = 2^t$. По лемме 1.3.3

$$\omega(G) = \bigcup_{k|2^t} k\omega({}^3D_4(q^{\frac{1}{k}})) = \bigcup_{0 \leq l \leq t} 2^l \cdot \omega({}^3D_4(q^{\frac{1}{2^l}})).$$

Если $p = 2$, то $2^4 \in \omega(G)$. Однако $2^3 \in \mu(S)$, а значит, $\omega(G) \neq \omega(S)$. Если $p \in \{3, 5\}$, то $2p^2 \in \omega(G)$, но $p^2 \in \mu(S)$, и снова $\omega(G) \neq \omega(S)$. Осталось показать, что при $p \geq 7$ выполнено равенство $\omega(G) = \omega(S)$. Теорема 3.2.2 влечет, что $\omega(S)$ состоит из всех делителей чисел $q^4 - q^2 + 1$, $(q^2 \pm q + 1)(q^2 - 1)$, $p(q^3 \pm 1)$. С другой стороны, $\omega(G)$ является объединением множеств $2^l \cdot \omega({}^3D_4(q_0))$, где $q_0^{2^l} = q$, для всех $0 \leq l \leq t$. Поскольку $2^l \cdot \omega({}^3D_4(q_0))$ состоит из всех делителей чисел $2^l(q_0^4 - q_0^2 + 1)$, $2^l(q_0^2 \pm q_0 + 1)(q_0^2 - 1)$, $2^l p(q_0^3 \pm 1)$, применяем лемму 3.3.1 и получаем $2^l \cdot \omega({}^3D_4(q_0)) \subseteq \omega(S)$ для любого l, тем самым $\omega(G) \subseteq \omega(S)$, а значит, $\omega(G) = \omega(S)$. Теорема 4 доказана. □

§ 3.4. Расширения групп $E_6(q)$ и ${}^2E_6(q)$

Пусть $S = E_6^{\varepsilon}(q)$, где $q = p^m$. Пусть φ и γ — соответственно полевой и графовый автоморфизмы группы S, определенные в параграфе 1.3. Тогда по [54, теорема 2.5.12] группа $\operatorname{Aut} S$ имеет следующее строение.

Если $\varepsilon = +$, то

$$\operatorname{Aut} S = \operatorname{Inndiag} S \rtimes (\langle\varphi\rangle \times \langle\gamma\rangle); \tag{3.18}$$

если $\varepsilon = -$, то

$$\operatorname{Aut} S = \operatorname{Inndiag} S \rtimes \langle\varphi\rangle \ u\ \varphi^m = \gamma. \tag{3.19}$$

Пусть β — элемент из $\langle\varphi\rangle$ порядка k, и если $\varepsilon = -$, предположим, что k нечетно. Обозначим через ε^l знак $+$, если l четно, и $-$, если l нечетно. Тогда из леммы 1.3.3 вытекают следующие равенства.

$$\omega(S \rtimes \langle\beta\rangle) = \bigcup_{r|k} r \cdot \omega(E_6^{\varepsilon}(q^{\frac{1}{r}})). \tag{3.20}$$

$$\omega(S \rtimes \langle\beta\gamma\rangle) = \bigcup_{r|k} r \cdot \omega(E_6^{\varepsilon^{k/r}}(q^{\frac{1}{r}})). \tag{3.21}$$

$$\omega(\operatorname{Inndiag} S\beta) = k \cdot \omega(\operatorname{Inndiag} E_6^{\varepsilon}(q^{\frac{1}{k}})). \tag{3.22}$$

Отметим, что группа $\operatorname{Inndiag} S$ двойственна группе $(E_6^{\varepsilon}(q))_u$ в смысле [45, с. 120]. В силу [45, предложения 4.4.1, 4.3.4] двойственные группы имеют изоморфные максимальные торы, поэтому $\omega_{p'}(\operatorname{Inndiag} S) = \omega_{p'}((E_6^{\varepsilon}(q))_u)$. Кроме того, индекс подгруппы $\operatorname{Inndiag} S$ в группе $\operatorname{Aut} S$ равен $(3, q - \varepsilon 1)$. Обозначим через δ диагональный автоморфизм группы S, порождающий $\operatorname{Inndiag} S$ по модулю S, и положим $d = (3, q - \varepsilon 1)$.

Доказательство теоремы 5. Пусть G — конечная группа, такая что $S < G \leqslant \operatorname{Aut} S$.

Предположим, что $\pi(G/S)$ содержит простое число r, не равное 2 и 3. Тогда G содержит полевой автоморфизм порядка r, и, согласно формуле (3.20), $\omega(G)$ содержит числа $2r$ и $r \cdot r_9(\varepsilon q_0)$, где $q = q_0^r$. Поскольку $(r, 6) = 1$, $r_9(\varepsilon q_0)$ также является примитивным простым делителем числа $q^9 - \varepsilon 1$, то есть $r_9(\varepsilon q_0) \in R_9(\varepsilon q) = \pi((q^6 + \varepsilon q^3 + 1)/d)$. По лемме 1.2.7 число 2 и числа из $R_9(\varepsilon q)$ лежат в разных компонентах связности графа $GK(S)$, поэтому $\omega(S) \neq \omega(G)$ (см. также [68, 69]).

Предположим, что $2 \in \pi(G/S)$. Если $\varepsilon = +$, то с точностью до сопряжения G содержит один из следующих элементов: автоморфизм $\beta \in \langle\varphi\rangle$ порядка 2, графовый автоморфизм γ или их произведение $\beta\gamma$. Если $\varepsilon = -$, то G содержит графовый автоморфизм γ.

Пусть $\varepsilon = +$. Если G содержит β, то, согласно формуле (3.20), $\omega(G)$ содержит множество $2 \cdot \omega(E_6(q_0))$, где $q = q_0^2$, а значит, содержит число $2 \cdot r_9(q_0)$. Однако $r_9(q_0) \in R_9(q)$ и, как уже было отмечено, числа 2 и $r_9(q)$ лежат в разных компонентах связности графа $GK(S)$. Если G содержит $\beta\gamma$, то, согласно формуле (3.21), $\omega(G)$ содержит множество $2 \cdot \omega({}^2E_6(q_0))$, где $q = q_0^2$, а значит, содержит число $2 \cdot r_{18}(q_0)$. Аналогично, $r_{18}(q_0) \in R_9(q)$, и мы опять приходим к тому, что $\omega(G) \neq \omega(S)$.

Пусть теперь $\varepsilon \in \{+, -\}$ и G содержит γ. Тогда $\omega(G)$ содержит число $2 \cdot r_{12}(q)$, поскольку $C_S(\gamma) \simeq F_4(q)$ и $\omega(F_4(q))$ содержит нечетное число $r_{12}(q)$. Но $2 \cdot r_{12}(q) \notin \omega(S)$ по [6, предложения 3.2 и 4.5] (см. также лемму 1.2.3).

Таким образом, осталось рассмотреть случай, когда G/S является 3-группой.

Пусть $d = 1$, то есть 3 не делит $q - \varepsilon 1$. Тогда G содержит полевой автоморфизм порядка 3, и по формуле (3.20) в $\omega(G)$ содержится множество $3 \cdot \omega(E_6^\varepsilon(q_0))$, где $q = q_0^3$. Если $p = 3$, то p-период группы G больше, чем p-период группы S (см. лемму 1.2.3). Пусть $p \neq 3$. Отметим, что $(3, q_0 - \varepsilon 1) = (3, q - \varepsilon 1) = 1$. В $\omega(G)$ содержится число $3 \cdot p \cdot r_5(\varepsilon q_0)$. Так как $q = q_0^3$ и $(3, 5) = 1$, примитивные простые делители числа $(\varepsilon q_0)^5 - 1$ также являются примитивными простыми делителями числа $(\varepsilon q)^5 - 1$, то есть $r_5(\varepsilon q_0) \in R_5(\varepsilon q)$. Поэтому, предположив, что $3 \cdot p \cdot r_5(\varepsilon q_0) \in \omega(S)$, получаем, что $3 \cdot p \cdot r_5(\varepsilon q_0)$ делит $p(q^5 - \varepsilon 1)$ (см. пункт 2 леммы 1.2.3). Поскольку $p \neq 3$ и 3 не делит $q^5 - \varepsilon 1$, мы пришли к противоречию, следовательно, $3 \cdot p \cdot r_5(\varepsilon q_0) \in \omega(G) \setminus \omega(S)$, и теорема 5 доказана в случае $d = 1$.

Пусть $d = 3$, то есть 3 делит $q - \varepsilon 1$. Тогда силовская 3-подгруппа группы $\mathrm{Out}(S) = \mathrm{Aut}\, S/S$ является произведением группы $\mathrm{Outdiag}\, S = \mathrm{Aut}\, S/\,\mathrm{Inndiag}\, S$ порядка 3 и образа циклической 3-группы полевых автоморфизмов группы S. Значит, с точностью до сопряжения либо $G = S \rtimes \langle\beta\rangle$, где $\beta \in \langle\varphi\rangle$ имеет порядок 3^t, либо G содержит $\delta\beta$, либо G содержит $\mathrm{Inndiag}\, S$.

Предложение 3.4.1. *Пусть $S = E_6^\varepsilon(q)$, q — степень простого числа p, 3 делит $q - \varepsilon 1$, и пусть $G = S \rtimes \langle\beta\rangle$, где β — полевой автоморфизм группы S порядка 3^t, $t > 0$. Тогда верны следующие утверждения.*

1) *Если $p = 2$, то $\mu(G) \setminus \mu(S) = \{3^t \cdot p^4\}$.*

2) *Если $p = 11$, то $\mu(G) \setminus \mu(S) = \{3^t \cdot p^2\}$.*

3) *Если* $p \notin \{2, 11\}$, *то* $\omega(G) = \omega(S)$.

Доказательство. По формуле (3.20) имеем

$$\omega(G) = \bigcup_{0 \leqslant n \leqslant t} 3^n \cdot \omega(E_6^\varepsilon(q^{\frac{1}{3^n}})). \tag{3.23}$$

Из (3.23) и леммы 1.2.3 следует, что $3^t \cdot p^4 \in \mu(G) \setminus \mu(S)$ при $p = 2$ и $3^t \cdot p^2 \in \mu(G) \setminus \mu(S)$ при $p = 11$.

Пусть $\nu(E_6^\varepsilon(q))$ — множество чисел, определенное в лемме 1.2.3. Определим $\tilde{\nu}(E_6^\varepsilon(q))$ как $\nu(E_6^\varepsilon(q))$ при $p \notin \{2, 11\}$, $\nu(E_6^\varepsilon(q)) \setminus \{p^4\}$ при $p = 2$ и $\nu(E_6^\varepsilon(q)) \setminus \{p^2\}$ при $p = 11$. В силу (3.23) предложение будет доказано, если показать, что $3^n \cdot \tilde{\nu}(E_6^\varepsilon(q^{\frac{1}{3^n}})) \subseteq \omega(S)$ для любого $0 < n \leqslant t$. Зафиксируем такое n и обозначим $q^{\frac{1}{3^n}}$ через q_0, а $E_6^\varepsilon(q_0)$ через S_0.

По лемме 1.2.3 множество $\tilde{\nu}(S_0)$ состоит из чисел вида $p^j \cdot X(q_0)$, где $j \geqslant 0$ и $X(q_0)$ — некоторый многочлен от q_0 ненулевой степени. Заметим, что $(3, q - \varepsilon 1) = (3, q_0 - \varepsilon 1)$, а значит, если $p^j \cdot X(q_0) \in \tilde{\nu}(S_0)$, то $p^j \cdot X(q) \in \nu'(S)$. Найдем для каждого числа $p^j \cdot X(q_0) \in \tilde{\nu}(S_0)$ число $p^j \cdot Y(q) \in \omega(S)$, такое что $3^n \cdot p^j \cdot X(q_0)$ делит $p^j \cdot Y(q)$.

(а) Пусть $X(q_0) = c \cdot (q_0^l - (\varepsilon 1)^l)\Pi_{i \in I}(q_0^i + (\varepsilon 1)^i)$, где $c \in \{1, \frac{1}{3}\}$. Тогда $Y(q) = X(q)$. Действительно, $q_0^l - (\varepsilon 1)^l$ делит $q^l - (\varepsilon 1)^l = q_0^{l \cdot 3^t} - (\varepsilon 1)^l$, а $q_0^i + (\varepsilon 1)^i$ делит $q^i + (\varepsilon 1)^i = q_0^{i \cdot 3^t} + (\varepsilon 1)^i$. При этом $q_0 \equiv \varepsilon 1 \pmod 3$, следовательно, $q_0^i \equiv (\varepsilon 1)^i \pmod 3$, откуда $q_0^i + (\varepsilon 1)^i \equiv \varepsilon 2 \pmod 3$. Из леммы 1.1.1 следует, что $(q^l - (\varepsilon 1)^l)_3 = (q_0^{3^n \cdot l} - (\varepsilon 1)^l)_3 = 3^n (q_0^l - (\varepsilon 1)^l)_3$. Следовательно, $3^n (X(q_0))_3 = (X(q))_3$.

(б) Пусть $X(q_0) = \frac{q_0^{2l} + (\varepsilon q_0)^l + 1}{3} = \frac{q_0^{3l} - (\varepsilon 1)^l}{3(q_0^l - (\varepsilon 1)^l)}$, где $l \in \{1, 2, 3\}$. Тогда $p^j \cdot \frac{q^l - (\varepsilon 1)^l}{3} \in \omega(S)$, и мы можем положить $Y(q) = \frac{q^l - (\varepsilon 1)^l}{3}$. По лемме 1.1.2 получаем, что $X(q_0)$ делит $Y(q)$. Из леммы 1.1.1 следует, что $3^n (X(q_0))_3 = 3^{n-1} \cdot \frac{3(l)_3 (q_0 - \varepsilon 1)_3}{(l)_3 (q_0 - \varepsilon 1)_3} = 3^n \leqslant (Y(q))_3 = (l)_3 \cdot 3^{n-1} \cdot (q_0 - \varepsilon 1)_3$.

(в) Пусть $X(q_0) = \frac{(q_0^2 + \varepsilon q_0 + 1)}{3} \cdot (q_0^4 - q_0^2 + 1)$. В **(б)** доказано, что $3^n \frac{(q_0^2 + \varepsilon q_0 + 1)}{3}$ делит $q - \varepsilon 1$. В то же время $q_0^4 - q_0^2 + 1 = \frac{q_0^6 + 1}{q_0^2 + 1}$ делит $q^2 + 1$ и $(q_0^4 - q_0^2 + 1, 3) = 1$. Следовательно, $3^n X(q_0)$ делит $Y(q) = (q - \varepsilon 1)(q^2 + 1)$.

(г) Пусть $X(q_0) = \frac{q_0^6 - 1}{3(q_0 - \varepsilon 1)} = \frac{q_0^3 - \varepsilon 1}{3(q_0 - \varepsilon 1)} \cdot (q_0^3 + \varepsilon 1)$. Мы показали, что $3^n \cdot \frac{q_0^3 - \varepsilon 1}{3(q_0 - \varepsilon 1)}$ делит $q - \varepsilon 1$. При этом $q_0^3 + \varepsilon 1$ делит $q + \varepsilon 1$ и $(q_0^3 + \varepsilon 1, 3) = 1$, а значит, $3^n \cdot X(q_0)$ делит $Y(q) = (q - \varepsilon 1)(q + \varepsilon 1) = q^2 - 1$.

Мы рассмотрели все возможности для $X(q_0)$, и предложение 3.4.1 доказано. $\square$

Вернемся к доказательству теоремы 5. Предположим, что G содержит $\operatorname{Inndiag} S$. Тогда $\omega_{p'}(G) \supseteq \omega_{p'}(\operatorname{Inndiag} S) = \omega_{p'}(E_6^\varepsilon(q)_u)$. По лемме 1.2.5 получаем, что $(q+\varepsilon 1)(q^5-\varepsilon 1) \in \omega_{p'}(\operatorname{Inndiag} S)$. Но из леммы 1.2.3 следует, что $(q+\varepsilon 1)(q^5-\varepsilon 1) \notin \omega(S)$, поскольку $d=3$. Имеем $(q+\varepsilon 1)(q^5-\varepsilon 1) \in \omega(G)\backslash\omega(S)$.

Предположим, что G содержит $\delta\beta$. Тогда $\omega(G)$ содержит множество $\omega(S\delta\beta)$. Поскольку $\operatorname{Inndiag} S\beta = S\beta \cup S\delta\beta \cup S\delta^2\beta$ и $(S\delta\beta)^\gamma = S\delta^2\beta$, имеем

$$\omega(\operatorname{Inndiag} S\beta) = \omega(S\beta) \cup \omega(S\delta\beta). \tag{3.24}$$

Из формулы (3.22) следует, что в $\omega(\operatorname{Inndiag} S\beta)$ содержится число $a = 3^t(q_0+\varepsilon 1)(q_0^5-\varepsilon 1)$. Покажем, что $a \notin \omega(S)$. Если $a \in \omega(S)$, то a делит $\frac{(q+\varepsilon 1)(q^5-\varepsilon 1)}{3}$, но по лемме 1.1.1

$$(a)_3 = 3^t(q_0-\varepsilon 1)_3 > 3^{t-1}(q_0-\varepsilon 1)_3 = \left(\frac{(q+\varepsilon 1)(q^5-\varepsilon 1)}{3}\right)_3.$$

Теперь покажем, что $a \in \omega(G)$. Поскольку $a \neq 3^t \cdot p^j$, из предложения 3.4.1 следует, что $a \notin \omega(S\beta)$. Значит в силу формулы (3.24) $a \in \omega(S\delta\beta) \subseteq \omega(G)$, и, следовательно, $a \in \omega(G) \setminus \omega(S)$.

Таким образом, если $\omega(S) = \omega(G)$, то $G = S \rtimes \langle\beta\rangle$, где β — полевой автоморфизм группы S порядка 3^t. Согласно предложению 3.4.1, если $p \notin \{2, 11\}$, то $\omega(G) = \omega(S)$, и если $p \in \{2, 11\}$, то $\omega(G) \neq \omega(S)$. Теорема 5 доказана. $\square$

§ 3.5. Расширения групп $E_7(q)$

Пусть $S = E_7(q)$, где $q = p^m$. Пусть φ — полевой автоморфизм группы S, определенный в параграфе 1.3. Тогда по [54, теорема 2.5.12] группа $\operatorname{Aut} S$ имеет следующее строение.

$$\operatorname{Aut} S = \operatorname{Inndiag} S \rtimes \langle\varphi\rangle. \tag{3.25}$$

Пусть β — элемент из $\langle\varphi\rangle$ порядка k. Тогда из леммы 1.3.3 вытекают следующие равенства.

$$\omega(S \rtimes \langle\beta\rangle) = \bigcup_{r|k} r \cdot \omega(E_7(q^{\frac{1}{r}})). \tag{3.26}$$

$$\omega(\operatorname{Inndiag} S\beta) = k \cdot \omega(\operatorname{Inndiag} E_7(q^{\frac{1}{k}})). \tag{3.27}$$

Отметим, что $\operatorname{Inndiag} S$ двойственна группе $(E_7(q))_u$ — универсальной группе типа E_7, поэтому $\omega_{p'}(\operatorname{Inndiag} S) = \omega_{p'}((E_7(q))_u)$. Кроме того, индекс подгруппы $\operatorname{Inndiag} S$ в группе $\operatorname{Aut} S$ равен $(2, q-1)$. Обозначим через δ диагональный автоморфизм группы S, порождающий $\operatorname{Inndiag} S$ по модулю S, и положим $d = (2, q-1)$.

Доказательство теоремы 6. Пусть G — конечная группа, такая что $S < G \leqslant \operatorname{Aut} S$.

Пусть $r \in \pi(G/S)$ и r нечетно. Тогда G содержит полевой автоморфизм порядка r. Обозначим $q^{\frac{1}{r}}$ через q_0. Согласно формуле (3.26), в $\omega(G)$ содержится множество $r \cdot \omega(E_7(q_0))$. Если $r \neq 7$, то $r_7(q_0) \in R_7(q)$ и $r_{14}(q_0) \in R_{14}(q)$, поскольку $(r, 14) = 1$. Тогда в $\omega(G)$ одновременно содержатся числа $r \cdot r_7(q_0)$ и $r \cdot r_{14}(q_0)$, где $r_7(q_0)$ и $r_{14}(q_0)$ также являются примитивными простыми делителями чисел $q^7 - 1$ и $q^{14} - 1$ соответственно. Но в $GK(S)$ не существует вершины, смежной одновременно с $r_7(q)$ и $r_{14}(q)$ (см. [7, рисунок 4]), следовательно, $\omega(G) \neq \omega(S)$. Если $r = 7$, то в $\omega(G)$ одновременно содержатся числа $r \cdot r_9(q_0)$ и $r \cdot r_{18}(q_0)$, где $r_9(q_0)$ и $r_{18}(q_0)$ также являются примитивными простыми делителями чисел $q^9 - 1$ и $q^{18} - 1$ соответственно, поскольку $(r, 18) = 1$. И снова в $GK(S)$ не существует вершины, смежной одновременно с $r_9(q)$ и $r_{18}(q)$, следовательно, $\omega(G) \neq \omega(S)$.

Осталось рассмотреть случай, когда G/S является 2-группой. Пусть $p = 2$. Тогда G содержит полевой автоморфизм порядка 2, и по формуле (3.26) в $\omega(G)$ содержится множество $2 \cdot \omega(E_7(q^{\frac{1}{2}}))$, и p-период группы G больше, чем p-период группы S (см. лемму 1.2.4). Таким образом, при $p = 2$ теорема 2 доказана. Теперь рассмотрим случай, когда p нечетно.

Предложение 3.5.1. *Пусть $S = E_7(q)$, q — степень нечетного простого числа p, и пусть $G = S \rtimes \langle\beta\rangle$, где β — полевой автоморфизм группы S порядка 2^t, $t > 0$. Тогда верны следующие утверждения.*

1) *Если $p \in \{13, 17\}$, то $\mu(G) \setminus \mu(S) = \{2^t \cdot p^2\}$.*

2) *Если $p \notin \{13, 17\}$, то $\omega(G) = \omega(S)$.*

Доказательство. По формуле (3.26) имеем

$$\omega(G) = \bigcup_{0 \leqslant n \leqslant t} 2^n \cdot \omega(E_7(q^{\frac{1}{2^n}})). \tag{3.28}$$

Из (3.28) и леммы 1.2.4 следует, что $2^t \cdot p^2 \in \mu(G) \setminus \mu(S)$ при $p \in \{13, 17\}$.

Пусть $\nu(E_7(q))$ — множество чисел, определенное в лемме 1.2.4. Определим $\tilde{\nu}(E_7(q))$ как $\nu(E_7(q))$, если $p \notin \{13, 17\}$, и $\nu(E_7(q)) \setminus \{2^t \cdot p^2\}$ в противном случае. В силу (3.28) предложение будет доказано, если показать, что $2^n \cdot \tilde{\nu}(E_7(q^{\frac{1}{2^n}})) \subseteq \omega(S)$ для любого $0 < n \leqslant t$. Зафиксируем такое n и обозначим $q^{\frac{1}{2^n}}$ через q_0, а $E_7(q_0)$ через S_0.

По лемме 1.2.4 множество $\tilde{\nu}(S_0)$ состоит из чисел вида $p^j \cdot X(q_0)$, где $j \geqslant 0$ и $X(q_0)$ — некоторый многочлен от q_0 ненулевой степени. Заметим, что если $p^j \cdot X(q_0) \in \tilde{\nu}(S_0)$, то $p^j \cdot X(q) \in \tilde{\nu}(S)$. Кроме того, $q_0^{2l} \pm q_0^l + 1$ делит $q^{2l} + q^l + 1$ и $q_0^l \pm 1$ делит $q^l - 1$ для любого натурального l, при этом из леммы 1.1.1 следует, что $2^n \cdot (q_0^l - (\varepsilon 1)^l)_2 \leqslant (q^l - 1)_2$. Найдем для каждого числа $p^j \cdot X(q_0) \in \tilde{\nu}(S_0)$ число $p^j \cdot Y(q) \in \omega(S)$, такое что $2^n \cdot p^j \cdot X(q_0)$ делит $p^j \cdot Y(q)$.

(а) Пусть $X(q_0) = c(q_0^l \pm 1)$, где $c \in \{1, \frac{1}{2}\}$. Положим $Y(q) = c(q^l - 1)$. Тогда $X(q_0)$ делит $Y(q)$, при этом $(Y(q))_2 = c \cdot (q^l - 1)_2 \geqslant c \cdot 2^n \cdot (q_0^l \pm 1)_2 = 2^n \cdot (X(q_0))_2$, поэтому $2^n \cdot X(q_0)$ делит $Y(q)$.

(б) Пусть $X(q_0) = c(q_0 \pm 1)(q_0^l \mp 1)$, где $c \in \{1, \frac{1}{2}\}$, $l \in \{3, 5\}$. Положим $Y(q) = c(q + 1)(q^l - 1)$. Тогда $X(q_0)$ делит $Y(q)$, а поскольку l нечетно, $(Y(q))_2 \geqslant c \cdot 2^n \cdot (q_0^l - 1)_2(q_0^l + 1)_2 = 2^n \cdot (X(q_0))_2$.

(в) Пусть $X(q_0) = c \cdot (q_0^{2l} + (\varepsilon q_0)^l + 1)(q_0^k - (\varepsilon 1)^k)$, где $\varepsilon \in \{+, -\}$, $c \in \{1, \frac{1}{2}\}$, $l \in \{1, 3\}$. Положим $Y(q) = c \cdot (q^{2l} + q^l + 1)(q^k - 1)$. Тогда $X(q_0)$ делит $Y(q)$, при этом $(Y(q))_2 = c \cdot (q^k - 1)_2 \geqslant c \cdot 2^n \cdot (q_0^k \pm 1)_2 = 2^n \cdot (X(q_0))_2$.

(г) Пусть $X(q_0) = q_0^4 - q_0^2 + 1$ или $X(q_0) = (q_0^4 - q_0^2 + 1) \cdot \frac{q_0^3 \pm 1}{2}$. Тогда $X(q_0)$ делит $(q_0^6 + 1) \cdot \frac{(q_0^3 \pm 1)}{2}$. Положим $Y(q) = \frac{q^6 - 1}{2}$. Тогда $X(q_0)$ делит $Y(q)$, при этом $(Y(q))_2 = \frac{1}{2} \cdot (q_0^{3 \cdot 2^{n+1}} - 1)_2 \geqslant 2^{n-1} \cdot (q_0^3 \pm 1)_2(q_0^6 + 1)_2 \geqslant 2^n \cdot (X(q_0))_2$.

(д) Пусть $X(q_0) = \frac{q_0^8 - 1}{(q_0 \pm 1)(4, q_0 \pm 1)}$. Положим $Y(q) = q^4 - 1$. Тогда $Y(q)$ делится на $q_0^8 - 1$, а значит, делится на $X(q_0)$, при этом $(Y(q))_2 = (q_0^{2^{n+2}} - 1)_2 \geqslant 2^{n-1} \cdot (q_0^8 - 1)_2 > 2^n \cdot (X(q_0))_2$.

(е) Пусть $X(q_0) = c \cdot (q_0^{2l} + 1)(q_0^l \pm 1)$, где $c \in \{1, \frac{1}{2}\}$, $l \in \{1, 2\}$. Тогда $p^j \cdot c \cdot (q^{2l} - 1) \in \omega(S)$. Положим $Y(q) = c \cdot (q^{2l} - 1)$. Тогда $X(q_0)$ делит $Y(q)$, при этом $(Y(q))_2 = c \cdot (q_0^{l \cdot 2^{n+1}} - 1)_2 \geqslant c \cdot 2^n \cdot (q_0^l \pm 1)_2(q_0^{2l} + 1)_2 = 2^n \cdot (X(q_0))_2$.

Мы рассмотрели все возможности для $X(q_0)$, и предложение 3.5.1 доказано. □

Вернемся к доказательству теоремы 6. Поскольку p нечетно, силовская 2-подгруппа группы $\operatorname{Out} S$ является произведением группы $\operatorname{Inndiag} S/S$ порядка 2 и образа циклической 2-группы полевых автоморфизмов группы S. Значит, либо $G = S \rtimes \langle\beta\rangle$, где $\beta \in \langle\varphi\rangle$ имеет порядок 2^t, либо G содержит $\delta\beta$, либо G содержит $\operatorname{Inndiag} S$.

Предположим, что G содержит $\operatorname{Inndiag} S$. Тогда $\omega_{p'}(G) \supseteq \omega_{p'}(\operatorname{Inndiag} S) = \omega_{p'}(E_7(q)_u)$. Из лемм 1.2.4 и 1.2.6 следует, что $q^7 - 1 \in \omega(G) \setminus \omega(S)$.

Предположим, что G содержит $\delta\beta$. Тогда $\omega(G)$ содержит множество $\omega(S\delta\beta)$. Поскольку $\operatorname{Inndiag} S\beta = S\beta \cup S\delta\beta$, имеем

$$\omega(\operatorname{Inndiag} S\beta) = \omega(S\beta) \cup \omega(S\delta\beta). \tag{3.29}$$

Положим $a = 2^t(q_0^7 + \varepsilon 1)$, если $q_0 - \varepsilon 1 \equiv 2 \pmod 4$. Из формулы (3.27) следует, что $a \in \omega(\operatorname{Inndiag} S\beta)$. Покажем, что $a \notin \omega(S)$. Если $a \in \omega(S)$, то a делит $\frac{q^7-1}{2}$, но по лемме 1.1.1

$$(a)_2 = 2^t(q_0 + \varepsilon 1)_2 > 2^{t-1}(q_0 + \varepsilon 1)_2 = \left(\frac{q^7 - 1}{2}\right)_2.$$

Теперь покажем, что $a \in \omega(G)$. Поскольку $a \neq 2^t p^2$, из предложения 3.5.1 следует, что $a \notin \omega(S\beta)$. Значит, в силу формулы (3.29), $a \in \omega(S\delta\beta) \subseteq \omega(G)$, и, следовательно, $a \in \omega(G) \setminus \omega(S)$.

Таким образом, если $\omega(G) = \omega(S)$, то $G = S \rtimes \langle\beta\rangle$, где β — полевой автоморфизм группы S порядка 2^t. Согласно предложению 3.5.1, если $p \notin \{13, 17\}$, то $\omega(G) = \omega(S)$, и если $p \in \{13, 17\}$, то $\omega(G) \neq \omega(S)$. Теорема 6 доказана. □

§ 3.6. Распознаваемость простых исключительных групп по спектру

Теорема В. *Пусть $S = {}^d\Phi(q)$ — простая исключительная группа лиева типа, где $q = p^m$, p — простое число. Тогда $h(S)$ указано в таблице 2. Если $1 < h(S) < \infty$, то конечная группа изоспектральна группе S тогда и*

только тогда, когда она изоморфна группе G такой, что $S \leq G \leq S \rtimes \langle\varphi\rangle$, где φ — полевой автоморфизм группы S порядка, указанного в таблице 2.

Таблица 2. Распознаваемость по спектру простых исключительных групп

S	Условия	$\lvert\varphi\rvert$	$h(S)$	Ссылки
${}^2B_2(q)$	нет	–	1	[78]
${}^2G_2(q)$	нет	–	1	[39]
${}^2F_4(q)$	нет	–	1	[47]
$G_2(q)$	нет	–	1	[11]
$E_8(q)$	нет	–	1	[23]
${}^3D_4(q)$	$q = 2$	–	∞	[30]
	$p \notin \{2,3,7,11\}$, $(m)_2 = 2^s > 1$	2^s	$s+1$	[95]
	$q \neq 2$ и либо $p \in \{2,3,7,11\}$, либо m нечетно	–	1	
$F_4(q)$	$p \notin \{2,3,7,11\}$, $(m)_2 = 2^s > 1$	2^s	$s+1$	[95]
	в противном случае	–	1	[95], [9]
$E_6^\varepsilon(q)$	$p \notin \{2,11\}$, $3 \mid q - \varepsilon 1$, $(m)_3 = 3^s > 1$	3^s	$s+1$	[22], [55], теор. 5
	в противном случае	–	1	
$E_7(q)$	$p \notin \{2,13,17\}$, $(m)_2 = 2^s > 1$	2^s	$s+1$	[1], [12], [55], теор. 6
	в противном случае	–	1	

Доказательство. Если S — исключительная группа, отличная от групп типов E_6 и E_7, то утверждение теоремы 3.6 для группы S доказано в работах, указанных в таблице 1. Пусть $S = E_6^\varepsilon(q)$ или $S = E_7(q)$ и G — конечная группа, такая что $\omega(G) = \omega(S)$. Тогда в силу [22] (для групп типа E_6) и [1], [12] (для групп типа E_7) группа G имеет единственный неабелев композиционный фактор, и этот фактор изоморфен S. Из [55] следует, что разрешимый радикал группы G тривиален, то есть с точностью до изоморфизма $S \leq G \leq \operatorname{Aut} S$. Теперь теоремы 5 и 6 завершают доказательство. □

4. Простые группы с графом простых чисел как у знакопеременной группы

Данная глава посвящена изучению случаев совпадения графа простых чисел конечной простой группы с графом простых чисел знакопеременной группы. Основным результатом главы является следующая теорема.

Теорема 7. *Пусть $S = A_m$, где $m \geq 5$, и G — конечная простая группа, не изоморфная S. Тогда верны следующие утверждения.*

1) *Если $m \geq 10$ и $GK(G) = GK(S)$, то G — знакопеременная группа.*

2) *Если $m \geq 10$, n нечетно и m, $m-4$ — составные числа, то $GK(A_{m-1}) = GK(A_m)$.*

3) *Если $m \leq 9$, то $GK(G) = GK(S)$ тогда и только тогда, когда $(S, G) \in \{(A_5, A_6), (A_7, L_2(49)), (A_7, U_4(3)), (A_9, J_2), (A_9, S_6(2)), (A_9, O_8^+(2))\}$.*

Замечание. В пунктах 2) и 3) теоремы 7 указаны некоторые случаи совпадения графов простых чисел двух различных знакопеременных групп. Доказательство того, что других случаев совпадения графов знакопеременных групп нет, можно провести лишь по модулю теоретико-числовой гипотезы, связанной с бинарной проблемой Гольдбаха. Общеизвестная формулировка проблемы Гольдбаха такова: верно ли, что любое четное число $n \geq 4$ представимо в виде суммы двух простых чисел? Нам потребуется следующая, более сильная, чем в проблеме Гольдбаха, гипотеза.

Гипотеза $(*)$. *Для любого четного числа $n > 6$ найдется пара различных простых чисел, сумма которых равна n.*

Более подробная информация о проблеме Гольдбаха и гипотезе $(*)$ приведена в параграфе 4.5.

Теорема 8. *Пусть $S = A_m$, где $m \geq 10$, и $G = A_n$, где $5 \leq n < m$. Если верна гипотеза $(*)$, то $GK(G) = GK(S)$ тогда и только тогда, когда $n = m - 1$, m нечетно и m, $m - 4$ — составные числа.*

В частности, если верна гипотеза $(*)$, то для произвольной знакопеременной группы $S = A_m$ степени $m \geq 5$ существует не более трех попарно неизоморфных неабелевых простых групп, отличных от S, граф простых чисел которых совпадает с $GK(S)$. Отметим связь этого результата со следующим вопросом [26, вопрос 16.26]: существует ли такое натуральное k (гипотетически, $k = 5$), что никакие k попарно неизоморфных конечных неабелевых простых групп не могут иметь один и тот же граф простых чисел?

§ 4.1. Свойства графа простых чисел знакопеременной группы

Вид графа простых чисел $GK(A_n)$ знакопеременной группы имеет специфические особенности, отличающие $GK(A_n)$ от графов неабелевых простых групп, отличных от знакопеременных.

Прежде всего, сформулируем критерий смежности вершин в $GK(A_n)$, который легко проверить.

Лемма 4.1.1. *Пусть $S = A_n$.*

1) *Если $r, s \in \pi(S)$ — нечетные числа, то r и s несмежны тогда и только тогда, когда $r + s > n$.*

2) *Если $r \in \pi(S)$ — нечетное число, то 2 и r несмежны тогда и только тогда, когда $r + 4 > n$.*

Этот критерий можно сделать более удобным с помощью функции $e(r)$, определенной на всех простых числах следующим образом: $e(r) = r$ для нечетного простого числа r, и $e(2) = 4$. Отметим, что по значению $e(r)$ однозначно восстанавливается число r, поэтому лемму 4.1.1 можно переписать в следующем виде.

Лемма 4.1.2. *Пусть $S = A_n$, и числа r, s содержатся в $\pi(S)$. Тогда r и s несмежны в том и только в том случае, если $e(r) + e(s) > n$.*

Из этой леммы вытекает, в частности, следующее свойство: если p и r — простые числа, $e(r) < e(p)$ и $p \in \pi(A_n)$, то $r \in \pi(A_n)$.

Множество вершин графа называется *кокликой*, если вершины, принадлежащие этому множеству, попарно несмежны. Мощность коклики с наибольшим числом вершин называется *неплотностью* графа. Обозначим через $t(S)$

неплотность графа $GK(S)$. Кроме того, для произвольной вершины r обозначим через $t(r, S)$ мощность наибольшей коклики, содержащей вершину r.

Опишем два множества $\Theta(S)$ и $\Theta'(S)$, элементами которых являются подмножества $\pi(S)$. Нужно выбрать такие множества, чтобы каждая коклика максимального размера в $GK(S)$ представлялась в виде $\rho(S) = \theta(S) \cup \theta'(S)$, где $\theta(S) \in \Theta(S)$ и $\theta'(S) \in \Theta'(S)$.

Обозначим через $\theta(S)$ пересечение всех коклик максимального размера в $GK(S)$. Тогда $\Theta(S) = \{\theta(S)\}$. Множество $\theta'(S)$, являющееся подмножеством $\pi(S) \setminus \theta(S)$, является элементом $\Theta'(S)$ тогда и только тогда, когда $\rho(S) = \theta(S) \cup \theta'(S)$ является кокликой максимального размера в $GK(S)$.

Пусть $S = A_n$, где $n \geq 5$. Обозначим через $\tau(n)$ множество простых чисел r таких, что $\frac{n}{2} \leq r \leq n$, а через s_n и s'_n — наименьшие элементы из $\tau(n)$ и $\tau(n) \setminus s_n$ соответственно. Пусть $\tau'(n)$ — множество простых чисел r таких, что $e(r) < \frac{n}{2}$ и $e(r) + e(s_n) > n$, а $\tau''(n)$ — множество простых чисел r таких, что $e(r) < \frac{n}{2}$ и $e(r) + e(s'_n) > n$.

Следующая лемма является несложным следствием леммы 4.1.1.

Лемма 4.1.3. *Пусть $S = A_n$, где $n \geq 5$.*

1) *Если $\tau'(n) = \tau''(n) = \varnothing$, то $\theta(S) = \tau(n)$ и $\Theta'(S) = \varnothing$.*

2) *Если $\tau'(n) = \varnothing$, $\tau''(n) \neq \varnothing$, то $\theta(S) = \tau(n) \setminus \{s_n\}$ и $\Theta'(S) = \{\{r\} | r \in \tau''(n) \cup \{s_n\}\}$.*

3) *Если $|\tau(n)| = 1$, то $\theta(S) = \tau(n) \cup \tau'(n)$ и $\Theta'(S) = \varnothing$.*

4) *Если $|\tau'(n)| \geq 2$, то $\theta(S) = \tau(n)$ и $\Theta'(S) = \{\{r\} | r \in \tau'(n)\}$.*

Лемма 4.1.4. *$t(A_n) > 3$ тогда и только тогда, когда $n = 17$ или $n \geq 19$.*

Доказательство. Легко убедиться, что при $n < 17$ или $n = 18$ размер максимальной коклики меньше четырех. Если $19 \leq n \leq 26$ или $29 \leq n \leq 37$, то в интервале $[\frac{n}{2}, n]$ находится не менее четырех простых чисел, которые входят в коклику максимального размера графа $GK(A_n)$, а значит, выполняется неравенство $t(A_n) \geq 4$. Если $n \in \{17, 27, 28\}$, то неплотность графа $GK(A_n)$ равна четырем. Если $n > 37$, то существует по меньшей мере 4 простых числа

p_i, таких что $\frac{n+1}{2} < p_i < n$ (этот факт сформулирован в [24, лемма 1], его доказательство опирается на результат, полученный в [74]). □

Лемма 4.1.5. *Для любого натурального n не существует таких различных четырех простых чисел $v_1, v_2, w_1, w_2 \in \pi(A_n)$, что в графе $GK(A_n)$ есть ребра (v_1, w_1) и (v_2, w_2) и нет ребер (v_1, w_2) и (v_2, w_1).*

Доказательство. Пусть в $GK(A_n)$ вершина v_1 смежна с w_1 и несмежна с w_2. Из критерия смежности следует, что $e(w_2) > e(w_1)$. Если при этом существует вершина v_2, смежная с w_2 и несмежная с w_1, то $e(w_1) > e(w_2)$; мы пришли к противоречию. □

Лемма 4.1.6. *Если G — простая группа лиева типа, $S = A_m$, где $m \geq 5$. Если у G и S один и тот же граф простых чисел, то этот граф несвязен.*

Доказательство. Согласно лемме 1.2.12, для любого числа $r \in \pi(G) = \pi(S)$ существует число $s \in \pi(S)$, такое что r и s несмежны в графе $GK(S)$. В частности, в $GK(S)$ найдется вершина r, не смежная с вершиной 3. Но тогда для любого числа $s \in \pi(S)$ числа r и s несмежны в графе $GK(S)$, т.е. r — изолированная вершина. Значит, граф $GK(S) = GK(G)$ является несвязным. □

§ 4.2. Линейные и унитарные группы

Пусть $G = L_n(q)$, где $n \geq 2$, или $G = U_n(q)$, где $n \geq 3$. Отметим, что группы $U_3(2)$, $L_2(2)$ и $L_2(3)$ не являются простыми; кроме того, имеют место изоморфизмы:

$$L_2(4) \cong L_2(5) \cong A_5;$$

$$L_2(9) \cong A_6;$$

$$L_4(2) \cong A_8;$$

$$L_2(q) \cong U_2(q).$$

Мы рассматриваем случаи совпадения графов простых чисел неизоморфных между собой групп.

Предложение 4.2.1. *Пусть $S = A_m$ — простая знакопеременная группа, $m \geq 5$, G — простая линейная или унитарная группа, не изоморф-*

ная G. Тогда $GK(G) = GK(S)$ в том и только в том случае, если $S = A_7$ и $G \in \{U_4(3), L_2(49)\}$.

Доказательство. Пусть $S = A_m$ и $t(S) \leq 3$. Тогда $m < 19$ (по лемме 4.1.4), и $\pi(S)$ содержится в множестве $\{2, 3, 5, 7, 11, 13, 17\}$. Нужно найти все такие простые линейные и унитарные группы G, что $\pi(G)$ содержится в множестве $\{2, 3, 5, 7, 11, 13, 17\}$ и, кроме того, если $r \in \pi(G)$, то любое простое число $r_1 < r$ также содержится в $\pi(G)$. В [90, табл. 1] приведены порядки всех неабелевых простых групп, наибольший простой делитель порядка которых не превышает 1000. Используя эти данные, получаем, что при выполнении указанных выше условий G изоморфна одной из следующих групп: $L_2(49)$, $L_3(4)$, $L_6(3)$, $U_3(5)$, $U_4(2)$, $U_4(3)$, $U_6(2)$. У двух из перечисленных групп граф простых чисел совпадает с графом знакопеременной группы: $GK(L_2(49)) = GK(U_4(3)) = GK(A_7)$. Это граф со множеством вершин $\{2, 3, 5, 7\}$ и ребром $(2, 3)$. Таким образом, если $t(G) \leq 3$, то $S = A_7$, а $G = L_2(49)$ или $G = U_4(3)$.

Пусть теперь $t(G) \geq 4$. Если G — линейная или унитарная группа, и $t(G) \geq 4$, то из [6, табл. 8] следуют ограничения на размерность группы G. Рассмотрим все возможные случаи.

Пусть $n = 3$ и $(q-\varepsilon 1)_3 = 3$, $q+\varepsilon 1 \neq 2^k$. В этом случае неплотность графа $GK(G)$ равна четырем и вершина 3 входит в коклику максимального размера $\rho(G)$. Но в этом случае $GK(G)$ не может совпадать с графом знакопеременной группы. Если в $GK(A_m)$ вершина 3 входит в коклику максимального размера, то размер этой коклики $t(A_m) \leq 3$, т.е. $t(3, A_m) \leq 3$. Действительно, если s_1 и s_2 — наибольшие простые числа в $\pi(A_m)$, и они оба входят в коклику максимального размера, содержащую при этом вершину 3, то $s_1 > m - 3$ и $s_2 > m - 3$. Это возможно лишь тогда, когда $s_1 = m$, $s_2 = m - 2$. Очевидно, что невозможно найти еще одну такую вершину $s_3 \in \pi(A_m)$, что $s_3 > m - 3$, а значит, размер коклики не превышает трех.

Пусть $n \geq 7$, $G \neq L_7(2)$, $G \neq L_8(2)$. Чтобы показать, что $GK(G)$ не может быть графом знакопеременной группы, воспользуемся леммой 4.1.5 и найдем такие вершины v_1, v_2, w_1, w_2, что в графе $GK(G)$ есть ребра (v_1, w_1), (v_2, w_2) и нет ребер (v_1, w_2), (v_2, w_1). Опираясь на критерий смежности вершин (леммы 1.2.8, 1.2.9), выбираем искомую четверку вершин следующим образом.

Если n — четное число, то

$$v_1 = p, v_2 \in R_{\frac{n}{2}}(\varepsilon q), w_2 \in R_n(\varepsilon q), w_1 \in R_{n-2}(\varepsilon q).$$

Если n — нечетное число, то

$$v_1 = p, v_2 \in R_{\frac{n-1}{2}}(\varepsilon q), w_2 \in R_{n-1}(\varepsilon q), w_1 \in R_{n-2}(\varepsilon q).$$

□

§ 4.3. Симплектические и ортогональные группы

Отметим, что при любых n и q выполнено равенство $GK(S_{2n}(q)) = GK(O_{2n+1}(q))$. Кроме того, имеют место изоморфизмы:

$$S_{2n}(2^k) \cong O_{2n+1}(2^k);$$

$$S_4(q) \cong O_5(q).$$

Пусть $S = A_m$, где $m \geq 5$, G — простая симплектическая или ортогональная группа. Предположим, что G и S неизоморфны и их графы простых чисел совпадают. По лемме 4.1.6 граф $GK(S) = GK(G)$ несвязен. Кроме того, $s(S)$ не превосходит 3. Все неабелевы простые группы с несвязным графом простых чисел были описаны в [21, 87]. В следующей лемме мы суммируем результаты этих работ для простых симплектических и ортогональных групп G, удовлетворяющих условию $s(G) \in \{2, 3\}$.

Лемма 4.3.1.([24]) *Все простые симплектические и ортогональные группы G, такие что $s(G) \in \{2, 3\}$, перечислены в таблице 3. Через t обозначено простое число.*

Предложение 4.3.2. *Пусть $S = A_m$, $m \geq 5$ — знакопеременная группа, G — простая симплектическая или ортогональная группа, не изоморфная S. Тогда $GK(G) = GK(S)$ в том и только в том случае, если $(S, G) \in \{(A_9, S_6(2)), (A_9, O_8^+(2))\}$.*

Доказательство. Прежде всего заметим, что если $GK(G) = GK(S)$, то G изоморфна одной из групп, перечисленных в таблице 3.

Далее в тексте доказательства цифра (цифры) в начале абзаца указывает на номер строки таблицы 3, группы из которой рассматриваются в этом абзаце.

Таблица 3

№	G	Ограничения на G	$s(G)$
1	$O^+_{2t}(q)$	$t \geqslant 5$, $q = 2, 3, 5$	2
2	$O^-_{2n}(2)$	$n = 2^k + 1 \geqslant 5$	2
3	$S_{2t}(q)$	$q = 2, 3$	2
4	$O_{2t+1}(3)$		2
5	$O^+_{2(t+1)}(q)$	$q = 2, 3$	2
6	$O^-_{2t}(3)$	$5 \leq t = 2^k + 1$	3
7	$O^-_{2n}(3)$	$n = 2^k + 1 \neq t$	2
8	$O^-_{2t}(3)$	$7 \leqslant t \neq 2^k + 1$	2
9	$O^-_{2n}(q)$	$n = 2^k \geqslant 4$	2
10	$S_{2n}(q)$	$n = 2^k \geqslant 2$	2
11	$O_{2n+1}(q)$	$n = 2^k \geqslant 4$, q нечетно	2

1–8. Сначала мы рассмотрим группы малых размерностей. Отметим, что для этих групп информация о графе простых чисел может быть получена из [46] или с помощью [52]. Непосредственная проверка графов простых чисел групп $S_{2t}(2)$ $(t = 3, 5)$, $S_{2t}(3)$ $(t = 2, 3, 5, 7)$, $O^+_{2l}(2)$ $(l = 4, 5, 6, 7)$, $O^+_{2l}(3)$ $(l \in \{4, 5, 6, 7, 8\})$, $O^-_{10}(2)$, $O^-_{2l}(3)$ $(l = 5, 7, 9)$ показывает, что они не могут совпадать с графом знакопеременной группы. Выполнено равенство $GK(S_6(2)) = GK(O^+_8(2)) = GK(A_9)$.

Теперь рассмотрим группы из пунктов 1–8 по отдельности, опуская случаи малых размерностей, перечисленные выше.

1. Пусть $q = 2$. Поскольку случаи $t = 5, 7$ уже были рассмотрены, мы можем считать, что $t > 7$. Тогда в графе $GK(G)$ вершина $r_{2(t-4)}(2)$ смежна с $r_8(2) = 17$ и не смежна с $r_{12}(2) = 13$. Из критерия смежности вершин в графе знакопеременной группы S (лемма 4.1.1) следует, что если для чисел $v, w_1, w_2 \in \pi(S)$ выполнено неравенство $w_1 > w_2$ и вершина v смежна с w_1 в графе $GK(S)$, то она смежна и с w_2. Ясно, что для $GK(G)$ это утверждение неверно, поэтому $GK(G)$ не может совпадать с графом знакопеременной группы. Далее в доказательстве аналогичное рассуждение не будет приводиться в развернутом виде.

Пусть $q = 3$. Поскольку $t \geq 11$, то из чисел $\{t - 8, t - 6\}$ можно выбрать

нечетное число, не кратное 11. Обозначим это число через s. Тогда в графе $GK(G)$ число $r_s(3)$ смежно с $r_8(3) = 41$ и не смежно с $r_{11}(3) = 23$.

Пусть $q = 5$. Здесь можно не рассматривать отдельно группы малых размерностей, т.к. рассуждение верно при $t \geq 5$. Множества $R_1(5)$ и $R_2(5)$ непусты. В графе $GK(G)$ есть ребра $(r_1(5), r_t(5))$, $(r_2(5), r_{2t}(5))$ и нет ребер $(r_1(5), r_{2t}(5))$, $(r_2(5), r_t(5))$. Это противоречит лемме 4.1.5, поэтому $GK(G)$ не может совпадать с графом знакопеременной группы.

2. Пусть $G = O^-_{2n}(2)$ и $(n = 2^k + 1 > 5)$. Тогда в графе $GK(G)$ вершина $r_{n-4}(2)$ смежна с $r_8(2) = 17$ и не смежна с $r_{12}(2) = 13$.

3. Пусть $G = S_{2t}(2)$ и $t > 5$. Тогда в графе $GK(G)$ вершина $r_{t-4}(2)$ смежна с $r_8(2) = 17$ и не смежна с $r_{10}(2) = 11$.

Пусть $G = S_{2t}(3)$ и $t > 7$. Тогда, если число $t-4$ не кратно 5, то в графе $GK(G)$ вершина $r_{t-4}(3)$ смежна с $r_3(3) = 13$ и не смежна с $r_5(3) = 11$. Если $t - 4$ делится на 5, то вершина $r_{t-3}(3)$ смежна с $r_3(3) = 13$ и не смежна с $r_5(3) = 11$.

4. Пусть $G = O_{2t+1}(3)$ и $t > 7$. Выполнено равенство $GK(O_{2t+1}(3)) = GK(S_{2t}(3)$. Эти симплектические группы рассмотрены в пункте 3.

5. Пусть $G = O^+_{2(t+1)}(2)$ и $t > 5$. Тогда в графе $GK(G)$ вершина $r_{t-4}(2)$ смежна с $r_5(2) = 31$ и не смежна с $r_{12}(2) = 13$.

Пусть $G = O^+_{2(t+1)}(3)$ и $t > 7$. Из чисел $\{t-6, t-4\}$ можно выбрать число s, не кратное 11. Тогда в графе $GK(G)$ вершина $r_s(3)$ смежна с $r_8(3) = 41$ и не смежна с $r_{11}(3) = 23$.

6,7,8. Эти пункты можно объединить, поскольку рассуждение верно для всех трех случаев. Пусть $G = O^-_{2k}(3)$, где k —нечетное число, не меньшее 11. Среди чисел $\{n - 6, n - 4\}$ можно выбрать число s, не кратное 11. Тогда в графе $GK(G)$ вершина $r_s(3)$ смежна с $r_8(3) = 41$ и не смежна с $r_{11}(3) = 23$.

Рассмотрим пункты **9–11** таблицы 3.

Пусть G — одна из групп $O_{2n+1}(q)$, $S_{2n}(q)$ $(n = 2^k \geq 2)$, $O^-_{2n}(q)$ $(n = 2^k \geq 4)$ над полем порядка $q = p^a$.

Рассмотрим сначала группы небольших размерностей.

Пусть $G = S_4(q)$. Тогда $t(G) = 2$. Среди неабелевых простых знакопеременных групп только для $S \in \{A_9, A_{10}, A_{12}\}$ выполнено $t(S) = 2$. Используя [90, табл. 1], несложно убедиться, что $GK(G)$ не может совпадать с графом знакопеременной группы.

Пусть $G \in \{S_8(q), O_9(q), O_8^-(q)\}$. Тогда $t(G) \leq 4$ и в графе $GK(G)$ существует изолированная вершина $r_8(q)$. Это число является простым делителем числа $\frac{q^4+1}{2}$. С другой стороны, если $GK(G)$ совпадает с графом знакопеременной группы S, то $t(S) \leq 4$, следовательно, $\pi(S) \subseteq \{2, 3, ..., 37\}$. Тогда $r_8(q) \leq \frac{q^4+1}{2} \leq 37$, значит, $q = 2$. Графы простых чисел групп $S_8(2)$, $O_9(2)$, $O_8^-(2)$ не могут совпадать с графом знакопеременной группы.

Осталось рассмотреть группы из пунктов 9–11 таблицы 3 при $n \geq 8$.

9. Пусть G — группа $O_{2n}^-(q)$ $(n = 2^k \geq 8)$, и ее граф простых чисел совпадает с графом знакопеременной группы. Поскольку $n - 5$ — нечетное число, не кратное пяти, в $GK(G)$ есть ребра $(r_5(q), r_{2(n-5)}(q))$, $(r_{10}(q), r_{n-5}(q))$ и нет ребер $(r_5(q), r_{n-5}(q))$, $(r_{10}(q), r_{2(n-5)}(q))$, что противоречит лемме 4.1.5.

10,11. Если число $q = p^a$ составное, то, обозначив через a' некоторый простой делитель числа a, получаем $q = p^a = q_0^{a'}$, где $q_0 = p^{\frac{a}{a'}}$ и a' — простое число. По лемме 1.1.4, $|R_i(q_0^{a'}| > 1$, если $(i, a') = 1$ и множества $R_i(q_0)$, $R_{ia'}(q_0)$ непусты. При $n \geq 8$ для любого $a \geq 2$ найдутся по крайней мере два различных множества $R_i(p^a)$, такие что $|R_i(p^a)| > 1$ и в графе $GK(G)$ вершины из одного множества смежны между собой и несмежны с вершинами из другого множества. Из леммы 4.1.5 следует, что такого не может быть в графе простых чисел знакопеременной группы S. Поэтому граф $GK(G)$ не может совпадать с графом $GK(S)$. Значит, при $n \geq 8$ осталось рассмотреть группы G над полем простого порядка.

Исключим случаи $q = 2, 3$.

Если $G = S_{2n}(2)$ или $G = O_{2n+1}(2)$ и $8 < n = 2^k$, то в графе $GK(G)$ вершина $r_{n-5}(2)$ смежна с $r_5(2) = 31$ и не смежна с $r_{12}(2) = 13$. Если $n = 8$, то непосредственная проверка показывает, что граф $GK(S_{16}(2)) = GK(O_{17}(2))$ не совпадает с графом знакопеременной группы.

Если $G = S_{2n}(3)$ или $G = O_{2n+1}(3)$ и $8 \leq n = 2^k$, то в графе $GK(G)$ вершина $r_{n-5}(3)$ смежна с $r_{10}(3) = 61$ и не смежна с $r_{16}(3) = 17$, поэтому $GK(G)$ не совпадает с графом знакопеременной группы.

Пусть $p \geq 5$ — простое число и G — группа $S_{2n}(p)$ или $O_{2n+1}(p)$, $n = 2^k \geq 8$, и ее граф простых чисел совпадает с графом знакопеременной группы.

Пусть k четно, тогда $n \equiv 1 \pmod 3$. В этом случае в $GK(G)$ есть ребра $(r_3(p), r_{n-1}(p))$, $(r_6(p), r_{2(n-1)}(p))$ и нет ребер $(r_3(p), r_{2(n-1)}(p))$, $(r_6(p), r_{n-1}(p))$, что противоречит лемме 4.1.5.

Если k нечетно, то $n \equiv -1 \pmod 3$. Обозначим через $r_0(p)$ число $r_3(p)$, если $p \equiv 1 \pmod 3$, и $r_6(p)$, если $p \equiv -1 \pmod 3$. Рассмотрим числа $r_4(p)$ и $r_0(p)$. Число $r_4(p)$ является делителем числа $k_4(p) = \frac{p^2+1}{2}$. Покажем, что при сделанных предположениях $k_4(p)$ — простое число. Если оно составное, то существует его простой делитель $r \in R_4(p)$, такой что $r \leq \sqrt{\frac{p^2+1}{2}} < p$. Но в $GK(G)$ вершина $s = r_{n-2}(p)$ смежна с p и не смежна с r. Это противоречит тому, что $GK(G)$ совпадает с графом знакопеременной группы. Значит, $r_4(p) = \frac{p^2+1}{2}$. Если $p \equiv 1 \pmod 3$, то $r_0(p) = r_3(p)$ — простой делитель числа $k_3(p) = \frac{p^2+p+1}{3}$; если $p \equiv -1 \pmod 3$, то $r_0(p) = r_6(p)$ — простой делитель числа $k_6(p) = \frac{p^2-p+1}{3}$. В любом случае $r_4(p) = \frac{p^2+1}{2} > \frac{p^2+p+1}{3} \geq r_0(p)$, но в графе $GK(G)$ вершина $r_4(p)$ смежна с $r_{2(n-2)}(p)$, а вершина $r_0(p)$ не смежна; противоречие. Значит, $GK(G)$ не может совпадать с графом знакопеременной группы. □

§ 4.4. Исключительные группы лиева типа и спорадические группы

Предложение 4.4.1. *Пусть $S = A_m$, где $m \geq 5$, G — исключительная группа лиева типа. Тогда $GK(G)$ не совпадает с $GK(S)$.*

Доказательство. Если $G \in \{G_2(q), {}^3D_4(q), {}^2F_4(2)'\}$, то $t(G) \leq 3$. Если $GK(G) = GK(A_m)$, то $\pi(G) \in \{2, 3, 5, 7, 11, 13, 17\}$. Из [90, табл. 1] следует, что в этом случае совпадений нет.

Рассмотрим теперь группы G, такие что $t(G) \geq 4$. Если $G \in \{E_6^\varepsilon(q), E_7(q), E_8(q)\}$, то по лемме 4.1.5 граф $GK(G)$ не совпадает с графом знакопеременной группы. Компактные формы графов простых чисел этих исключительных групп приведены в [7]. Укажем наборы вершин v_1, v_2, w_1, w_2, такие что в $GK(G)$ есть ребра (v_1, w_1), (v_2, w_2) и нет ребер (v_1, w_2), (v_2, w_1):

- если $G = E_6^\varepsilon(q)$, то $v_1 \in R_4, v_2 \in R_{12}, w_1 \in R_{\nu_\varepsilon(6)}, w_2 \in R_{\nu_\varepsilon(3)}$;
- если $S = E_7(q)$, то $v_1 \in R_8, v_2 \in R_{10}, w_1 \in R_4, w_2 \in R_6$;
- если $S = E_8(q)$, то $v_1 \in R_9, v_2 \in R_{10}, w_1 \in R_3, w_2 \in R_4$.

Пусть теперь $G = F_4(q)$. На рис. 3 приведена компактная форма для $GK(G)$ (см. [7]).

Пусть $p \neq 2$. Тогда либо $p = 3$, либо $3 \in R_1(q)$, либо $3 \in R_2(q)$. В

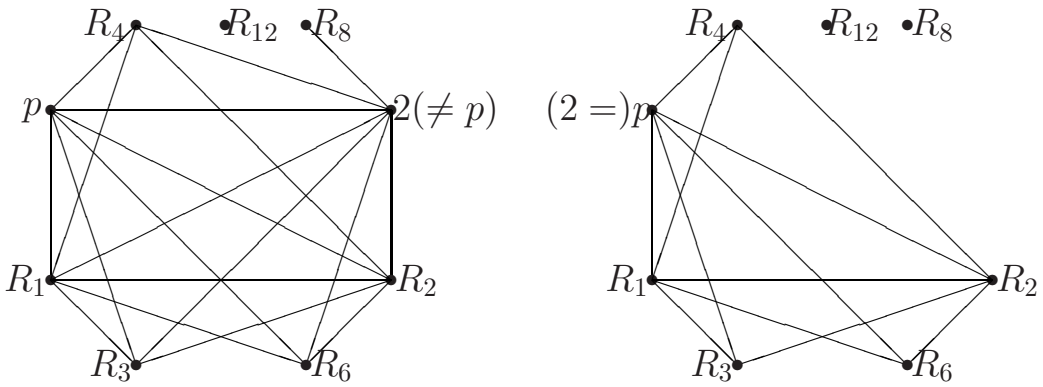

Рис. 3. Компактная форма графа $GK(F_4(q))$

любом случае вершина r_8 смежна с 2 и несмежна с 3, что невозможно в графе знакопеременной группы.

Пусть $p = 2$. Тогда $t(G) = 4$ и r_8, r_{12} — изолированные вершины. Если $GK(G) = GK(A_m)$, то $t(A_m) = 4$ и оба числа $m, m-2$ — простые. Единственная знакопеременная группа, удовлетворяющая этим условиям, — это группа A_{19}. Ее граф простых чисел не совпадает с $GK(G)$.

Осталось рассмотреть группы Сузуки и Ри. Поскольку порядки простых групп Сузуки $G = {}^2B_2(2^{2n+1})$ не делятся на 3, то $GK(G) \neq GK(S)$ в этом случае. Заметим, наконец, что если $S = A_m$ — знакопеременная группа, то $t(2, S) \leq 3$ и $t(3, S) \leq 3$. Это не так для простых групп Ри: в графе $GK({}^2G_2(3^{2n+1}))$ вершина 3 входит в коклику максимального размера 5; в графе $GK({}^2F_4(2^{2n+1}))$ вершина 2 входит в коклику максимального размера 4. □

Предложение 4.4.2. *Пусть $S = A_m$, где $m \geq 5$, G — спорадическая группа. Тогда $GK(G) = GK(S)$ в том и только в том случае, если $(S, G) = (A_9, J_2)$.*

Доказательство. В [46] указаны множества порядков элементов всех спорадических групп. Этого достаточно для того, чтобы в явном виде построить граф простых чисел любой из спорадических групп или проверить выполнение в этом графе условий, заведомо выполняющихся в графе знакопеременной группы. Из леммы 4.1.1 вытекает следующее свойство графа $GK(A_m)$: если p и q — простые числа, $q < p$ и $p \in \pi(A_m)$, то $q \in \pi(A_m)$. Указанным свойством не обладает множество $\pi(G)$, если G — одна из следующих групп: Co_1, Co_2, Co_3, F_1, F_2, F_3, Fi_{23}, Fi_{24}, He, HN, J_1, J_3, J_4,

Ly, M_{11}, M_{23}, M_{24}, $O'N$, Ru. Проверка показывает, что из оставшихся шести спорадических групп Fi_{22}, HS, J_2, M_{22}, McL, Suz только J_2 имеет граф простых чисел, совпадающий с графом знакопеременной группы $S = A_9$. А именно, $\{2, 3, 5, 7\} = \pi(A_9) = \pi(J_2)$ — множество вершин, $(2, 3), (2, 5), (3, 5)$ — множество ребер графов $GK(A_9)$ и $GK(J_2)$. □

§ 4.5. Знакопеременные группы

Предложение 4.5.1. *Пусть $n \geq 6$ — натуральное число, и либо $n = 6$, либо n нечетно и оба числа n, $n - 4$ являются составными. Тогда графы простых чисел знакопеременных групп A_n и A_{n-1} совпадают.*

Доказательство. Прямая проверка показывает, что выполнено равенство $GK(A_6) = GK(A_5)$. Предположим, что $n > 6$ и выполнено неравенство $GK(A_n) \neq GK(A_{n-1})$. Множества $\pi(A_n)$ и $\pi(A_{n-1})$ (т.е. множества вершин соответствующих графов простых чисел) различаются тогда и только тогда, когда n — простое число. Если n не является простым числом и $GK(A_n) \neq GK(A_{n-1})$, то множества ребер этих графов различны (в силу того, что множества их вершин $\pi(A_n)$ и $\pi(A_{n-1})$ совпадают). Следовательно, существуют простые числа $r, s \in \pi(A_n)$ такие, что $n - 1 < e(r) + e(s) \leq n$, т. е. $e(r) + e(s) = n$. Поскольку n нечетно, получаем, что одно из чисел r, s равно двум, а другое равно $n - 4$. Значит, $n - 4$ является простым числом. Следовательно, если n нечетно и оба числа n, $n-4$ являются составными, то $GK(A_n) = GK(A_{n-1})$ и предложение доказано. □

Доказательство теоремы 7 следует из предложений 4.2.1, 4.3.2, 4.4.1, 4.4.2 и 4.5.1. □

Прежде чем перейти к доказательству теоремы 8, напомним, что нам потребуется следующая гипотеза.

Гипотеза (∗). *Для любого четного числа $n > 6$ найдется пара различных простых чисел, сумма которых равна n.*

Широко известна бинарная гипотеза Гольдбаха о том, что любое четное число $n \geq 4$ представимо в виде суммы двух простых чисел. В 1930-х гг. было доказано, что доля непредставимых чисел, если они существуют, стремится к нулю с ростом n [51, 86]. На апрель 2012 г. бинарная гипотеза Гольдбаха

была проверена для всех четных чисел до $4 \cdot 10^{18}$ [72, 88]. Более сильная гипотеза $(*)$ верна для всех четных чисел, не превосходящих $4 \cdot 10^4$ (см. [84], последовательность A002375 в OEIS). Кроме того, утверждение гипотезы $(*)$ следует из асимптотической формулы количества различных представлений четного числа n в виде суммы двух простых чисел, проверенной для всех чисел, не превосходящих 2^{40}. Отметим, что оценивающая функция в этой формуле быстро растет с ростом n (см. более подробный обзор обеих гипотез в [32]).

Доказательство теоремы 8. Пусть $S = A_m$, $m \geq 10$, и G — знакопеременная группа. Если $G = A_{m-1}$, оба числа m, $m-4$ являются составными и m нечетно, то равенство $GK(G) = GK(S)$ доказано в предложении 4.5.1. Докажем утверждение в обратную сторону. Предположим, что верна гипотеза $(*)$. Сначала покажем, что $GK(A_n)$ и $GK(A_m)$ не могут совпадать, если $m-n > 1$. Пусть $n \leq m-2$. Одно из чисел m, $m-1$ является четным. В силу гипотезы $(*)$, найдутся два различных нечетных простых числа r и s, таких что $n \leq m-2 < r+s \leq m$, а значит, множества ребер рассматриваемых графов различны: $GK(A_n)$ не содержит ребро (r, s), а $GK(A_m)$ содержит. Пусть теперь $G = A_{m-1}$. Если m четно, то в силу гипотезы $(*)$ существуют различные простые числа r и s, такие что $m = r+s$. Тогда $GK(A_m)$ содержит ребро (r, s) и не совпадает с графом $GK(A_{m-1})$. Если m — нечетное простое число, то у графов $GK(S)$ и $GK(G)$ не совпадают множества вершин, а если $m-4$ является простым числом — множества ребер. Теорема 8 доказана. $\square$

Заключение

В диссертации изучался вопрос о совпадении спектра почти простого расширения группы лиева типа со спектром этой группы, а также вопрос о совпадении графов простых чисел различных неабелевых простых групп. Эти вопросы связаны с общими проблемами распознаваемости конечной простой группы по спектру и графу простых чисел. Были получены следующие результаты:

1) доказано, что нетривиальное почти простое расширение симплектической или ортогональной группы над полем характеристики 2 не изоспектрально этой группе;

2) получено точное описание почти простых расширений исключительных групп ${}^3D_4(q)$, $F_4(q)$, $E_6(q)$, ${}^2E_6(q)$ и $E_7(q)$, изоспектральных этим группам (результаты о группах $F_4(q)$ и ${}^3D_4(q)$ — совместно с М.А. Гречкосеевой);

3) показано, что за конечным числом явно описанных исключений конечная простая группа, имеющая такой же граф простых чисел, как знакопеременная группа, также является знакопеременной группой.

Полученные результаты завершают исследование распознаваемости по спектру конечных простых групп лиева типа над полями характеристики 2 и простых исключительных групп над полями произвольной характеристики, а также вносят вклад в доказательство гипотезы о том, что число попарно неизоморфных конечных неабелевых простых групп с одинаковым графом простых чисел ограничено константой. Разработанные методы могут быть использованы для дальнейших исследований спектров почти простых расширений групп лиева типа.

Список литературы

[1] Алексеева О. А., Кондратьев А. С. Квазираспознаваемость одного класса конечных простых групп по множеству порядков элементов // Сиб. матем. журн. — 2003. — Т. 44, № 2. — С. 241–255.

[2] Бутурлакин А. А. Спектры конечных простых групп $E_7(q)$ // Сиб. матем. журн. — 2016. — Т. 57, № 5. — С. 988–998.

[3] Бутурлакин А. А. Спектры конечных симплектических и ортогональных групп // Матем. тр. — 2010. — Т. 13, № 2. — С. 33–83.

[4] Бутурлакин А. А. Спектры конечных простых групп $E_6(q)$ и ${}^2E_6(q)$ // Алгебра и логика. — 2013. — Т. 52, № 3. — С. 284–304.

[5] Бутурлакин А. А., Гречкосеева М. А. Циклическое строение максимальных торов в конечных классических группах // Алгебра и логика. — 2007. — Т. 46, № 2. — С. 129–156.

[6] 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.

[7] 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.

[8] Васильев А. В., Гречкосеева М. Распознаваемость по спектру для простых классических групп в характеристике 2 // Сиб. матем. журн. — 2015. — Т. 56, № 6. — С. 1264–1276.

[9] Васильев А. В., Гречкосеева М. А., Мазуров В. Д. и др. Распознавание конечных простых групп $F_4(2^m)$ по спектру // Сиб. матем. журн. — 2004. — Т. 45, № 6. — С. 1256–1262.

[10] Васильев А. В., Гречкосеева М. А., Старолетов А. М. О конечных группах, изоспектральных простым линейным и унитарным группам // Сиб. матем. журн. — 2011. — Т. 52, № 1. — С. 39–53.

[11] Васильев А. В., Старолетов А. М. Распознаваемость групп $G_2(q)$ по спектру // Алгебра и логика. — 2013. — Т. 52, № 1. — С. 3–21.

[12] Васильев А. В., Старолетов А. М. Почти распознаваемость простых исключительных групп лиева типа // Алгебра и логика. — 2014. — Т. 53, № 6. — С. 669–692.

[13] Горшков И. Б. Распознавание по спектру конечных простых групп, простые делители порядков которых не превосходят 17 // Сиб. электрон. матем. изв. — 2010. — Т. 7. — С. 14–20.

[14] Горшков И. Б. Распознаваемость знакопеременных групп по спектру // Алгебра и логика. — 2013. — Т. 52, № 1. — С. 57–63.

[15] Гречкосеева М. А. Распознавание по спектру конечных простых линейных групп над полями характеристики 2 // Алгебра и логика. — 2008. — Т. 47, № 4. — С. 405–427.

[16] Гречкосеева М. А., Лыткин Д. В. Почти распознаваемость по спектру конечных простых линейных групп простой размерности // Сиб. матем. журн. — 2012. — Т. 53, № 4. — С. 805–818.

[17] Заварницин А. В. Распознавание по множеству порядков элементов знакопеременных групп степени $r+1$ и $r+2$ для простого r и группы степени 16 // Алгебра и логика. — 2000. — Т. 39, № 6. — С. 648–661.

[18] Заварницин А. В. О распознавании конечных групп по графу простых чисел // Алгебра и логика. — 2006. — Т. 45, № 4. — С. 390–408.

[19] Заварницин А. В. Распознавание простых групп $U_3(q)$ по порядкам элементов // Алгебра и логика. — 2006. — Т. 45, № 2. — С. 185–202.

[20] Заварницин А. В. Строение максимальных торов в спинорных группах // Сиб. матем. журн. — 2015. — Т. 56, № 3. — С. 537–548.

[21] Кондратьев А. С. О компонентах графа простых чисел конечных простых групп // Матем. сб. — 1989. — Т. 180, № 6. — С. 787–797.

[22] Кондратьев А. С. Квазираспознаваемость по множеству порядков элементов групп $E_6(q)$ и ${}^2E_6(q)$ // Сиб. матем. журн. — 2007. — Т. 48, № 6. — С. 1250–1271.

[23] Кондратьев А. С. Распознаваемость по спектру групп $E_8(q)$ // Тр. ИММ УрО РАН. — 2010. — Т. 16, № 3. — С. 146–149.

[24] 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.

[25] Кондратьев А. С., Храмцов И. В. О конечных четырехпримарных группах // Тр. ИММ УрО РАН. — 2011. — Vol. 17, no. 4. — P. 142–159.

[26] Коуровская тетрадь. Нерешенные вопросы теории групп / Под ред. В. Д. Мазуров, Е.И. Хухро. — 17 изд. — Новосибирск : Институт математики СО РАН, 2010. — С. 218.

[27] Мазуров В. Д. Характеризация конечных групп множествами порядков их элементов // Алгебра и логика. — 1997. — Т. 36, № 1. — С. 37–53.

[28] Мазуров В. Д. Распознавание конечных простых групп $S_4(q)$ по порядкам их элементов // Алгебра и логика. — 2002. — Т. 41, № 2. — С. 166–198.

[29] Мазуров В. Д. Группы с заданным спектром // Изв. Урал. гос. ун-та. Серия Математика и механика. — 2005. — Т. 36. — С. 119–138.

[30] Мазуров В. Д. Нераспознаваемость конечной простой группы ${}^3D_4(2)$ по спектру // Алгебра и логика. — 2013. — Т. 52, № 5. — С. 601–605.

[31] Мазуров В. Д., Су М., Чао Х. Распознавание конечных простых групп $L_3(2^m)$ и $U_3(2^m)$ по порядкам их элементов // Алгебра и логика. — 2000. — Т. 39, № 5. — С. 567–585.

[32] Маслова Н. В. О совпадении графов Грюнберга–Кегеля конечной простой группы и ее собственной подгруппы // Тр. ИММ УрО РАН. — 2014. — Т. 20, № 1. — С. 156–168.

[33] Махмудифар А., Хосрави Б. О характеризуемости знакопеременных групп порядком и графом простых чисел // Сиб. матем. журн. — 2015. — Т. 56, № 1. — С. 149–157.

[34] Старолетов А. М. Группы, изоспектральные знакопеременной группе степени 10 // Сиб. матем. ж. — 2010. — Т. 51, № 3. — С. 638–648.

[35] Старолетов А. М. О распознаваемости по спектру простых групп $B_3(q)$, $C_3(q)$ и $D_4(q)$ // Сиб. матем. журн. — 2012. — Т. 53, № 3. — С. 663–671.

[36] Хосрави А., Хосрави Б. Квазираспознавание простой группы ${}^2G_2(q)$ по графу простых чисел // Сиб. мат. журн. — 2007. — Vol. 48, no. 3. — P. 707–715.

[37] Хосрави А., Хосрави Б. 2-распознаваемость $PSL(2, p^2)$ по графу простых чисел // Сиб. мат. журн. — 2008. — Vol. 49, no. 4. — P. 934–944.

[38] Brandl R., Shi W. Finite groups whose element orders are consecutive integers // J. Algebra. — 1991. — Vol. 143, no. 2. — P. 388–400.

[39] Brandl R., Shi W. A characterization of finite simple groups with abelian Sylow 2-subgroups // Ricerche Mat. — 1993. — Vol. 42, no. 1. — P. 193–198.

[40] Brandl R., Shi W. The characterization of $PSL(2, q)$ by its element orders // J. Algebra. — 1994. — Vol. 163, no. 1. — P. 109–114.

[41] Burness T. C., Covato E. On the prime graph of simple groups // Bull. Aust. Math. Soc.. — 2015. — Vol. 91, no. 2. — P. 227–240.

[42] Burnside W. On a class of groups of finite order // Trans. Cambridge Phil. Soc. — 1900. — Vol. 18. — P. 269–276.

[43] Carter R. W. Simple groups of Lie type. — London etc. : John Wiley & Sons, 1972.

[44] Carter R. W. Centralizers of semisimple elements in finite groups of Lie type // Proc. Lond. Math. Soc. (3). — 1978. — Vol. 37. — P. 491–507.

[45] Carter R. W. Finite groups of Lie type. Conjugacy classes and complex characters. — Chichester-New York etc. : John Wiley & Sons, 1985.

[46] Conway J. H., Curtis R. T., Norton S. P. et al. Atlas of finite groups. — Oxford : Clarendon Press, 1985.

[47] Deng H., Shi W. The characterization of Ree groups ${}^2F_4(q)$ by their element orders // J. Algebra. — 1999. — Vol. 217, no. 1. — P. 180–187.

[48] Deriziotis D. I. Conjugacy classes of centralizers of semisimple elements in finite groups of Lie type. — Essen : Universität Essen Fachbereich Mathematik, 1984.

[49] 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.

[50] 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.

[51] Estermann T. On Goldbach's Problem: Proof that Almost All Even Positive Integers are Sums of Two Primes // Proc. London Math. Soc. Ser. 2. — 1938. — Vol. 44. — P. 307–314.

[52] The GAP Group. — GAP – Groups, Algorithms, and Programming, Version 4.7.5, 2014. — URL: `http://www.gap-system.org`.

[53] Gorenstein D., Lyons R. Local structure of finite groups of characteristic 2 type. — Providence, RI : Amer. Math. Soc., 1983.

[54] Gorenstein D., Lyons R., Solomon R. The classification of the finite simple groups. Number 3. — Providence, RI : Amer. Math. Soc., 1998.

[55] Grechkoseeva M. A. On element orders in covers of finite simple groups of Lie type // J. Algebra Appl. — 2015. — Vol. 14. — 1550056 [16 pages].

[56] Grechkoseeva M. A., Shi W., Vasil'ev A. V. Recognition by spectrum for finite simple groups of Lie type // Front. Math. China. — 2008. — Vol. 3, no. 2. — P. 275–285.

[57] Grechkoseeva M. A., Shi W. J. On finite groups isospectral to finite simple unitary groups over fields of characteristic 2 // Сиб. электрон. матем. изв. — 2013. — Т. 10. — С. 31–37.

[58] 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.

[59] Hagie M. The prime graph of a sporadic simple group // Comm. Algebra. — 2003. — Vol. 31, no. 9. — P. 4405–4424.

[60] Higman G. Finite groups in which every element has prime power order // J. London Math. Soc. — 1957. — Vol. 32. — P. 335–342.

[61] Khosravi B. n-recognition by prime graph of the simple group $PSL(2, q)$ // J. Algebra Appl. — 2008. — Vol. 7, no. 6. — P. 735–748.

[62] Khosravi B. On the prime graph of a finite group // London Mathematical Society Lecture Note Series. — 2009. — Vol. 388. — P. 424–428.

[63] Khosravi B., Amiri S. S. S. Groups with the same prime graph as $L_2(q)$ where $q = p^a < 100$ // Hadronic J. — 2007. — Vol. 30, no. 3. — P. 343–354.

[64] Khosravi B., Khosravi B., Khosravi B. Groups with the same prime graph as a CIT simple group // Houston J. Math. — 2007. — Vol. 33, no. 4. — P. 967–977.

[65] Khosravi B., Khosravi B., Khosravi B. On the prime graph of $PSL(2, p)$ where $p > 3$ is a prime number // Acta Math. Hungar. — 2007. — Vol. 116, no. 4. — P. 295–307.

[66] Khosravi B., Khosravi B., Khosravi B. A characterization of the finite simple group $L_{16}(2)$ by its prime graph // — 2008. — Vol. 126, no. 1. — P. 49–58.

[67] Lawther R. The action of $F_4(q)$ on cosets of $B_4(q)$ // — 1999. — Vol. 212, no. 1. — P. 79–118.

[68] Lucido M. S. Prime graph components of finite almost simple groups // Rend. Semin. Mat. Univ. Padova. — 1999. — Vol. 102. — P. 1–22.

[69] Lucido M. S. Addendum to "Prime graph components of finite almost simple groups" // Rend. Semin. Mat. Univ. Padova. — 2002. — Vol. 107. — P. 189–190.

[70] Lytkin Y. V. On groups critical with respect to a set of natural numbers // Сиб. электрон. матем. изв. — 2013. — Т. 10. — С. 666–675.

[71] Mazurov V. D., Shi W. A note to the characterization of sporadic simple groups // Algebra Colloq. — 1998. — Vol. 5, no. 3. — P. 285–288.

[72] Oliveira S. T. Goldbach conjecture verification. — URL: `http://sweet.ua.pt/tos/goldbach.html`.

[73] Praeger C. E., Shi W. A characterization of some alternating and symmetric groups // Commun. Algebra. — 1994. — Vol. 22, no. 5. — P. 1507–1530.

[74] Rohrbach H., Weis J. Zum finiten Fall des Bertrandschen Postulates // J. Reine Angew. Math. — 1964. — Vol. 214, no. 5. — P. 432–440.

[75] Shi W. A characteristic property of $PSL_2(7)$ // J. Aust. Math. Soc. Ser. A. — 1984. — Vol. 36. — P. 354–356.

[76] Shi W. A characteristic property of A_5 // J. Southwest-China Teach. Univ. — 1986. — Vol. 11. — P. 11–14.

[77] Shi W. A characterization of J_1 and $PSL_2(2^n)$ // Adv. in Math. (Beijing). — 1987. — Vol. 16. — P. 397–401.

[78] Shi W. A characterization of Suzuki's simple groups // Proc. Amer. Math. Soc. — 1992. — Vol. 114, no. 3. — P. 589–591.

[79] Shi W., Tang C. A characterization of some orthogonal groups // Progr. Natur. Sci. — 1997. — Vol. 7, no. 2. — P. 155–162.

[80] Shoji T. The conjugacy classes of Chevalley groups of type (F_4) over finite fields of characteristic $p \neq 2$ // J. Fac. Sci. Univ. Tokyo Sect. IA Math. — 1974. — Vol. 21. — P. 1–17.

[81] Steinberg R. Endomorphisms of linear algebraic groups. — Providence, RI : Amer. Math. Soc., 1968.

[82] Steinberg R. Lectures on Chevalley groups. — Yale University, New Haven, Conn., 1968. — P. iii+277.

[83] 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.

[84] The on-line encyclopedia of integer sequences. — URL: `https://oeis.org/A002375`.

[85] Vasil'ev A. V. On finite groups isospectral to simple classical groups // J. Algebra. — 2015. — Vol. 423. — P. 318–374.

[86] Vinogradov I. M. Some theorems concerning the theory of primes // Recueil Math. — 1937. — Vol. 2. — P. 179–195.

[87] Williams J. S. Prime graph components of finite groups // J. Algebra. — 1981. — Vol. 69. — P. 487–513.

[88] Weisstein E. W. Goldbach conjecture. — URL: `http://mathworld.wolfram.com/GoldbachConjecture.html`.

[89] Zavarnitsine A. V. Recognition of the simple groups $L_3(q)$ by element orders // J. Group Theory. — 2004. — Vol. 7, no. 1. — P. 81–97.

[90] Zavarnitsine A. V. Finite simple groups with narrow prime spectrum // Сиб. электрон. матем. изв. — 2009. — Т. 6. — С. 1–12.

[91] Zavarnitsine A. V. Uniqueness of the prime graph of $L_{16}(2)$ // Сиб. электрон. матем. изв. — 2010. — Т. 7. — С. 119–121.

[92] Zsigmondy K. Zur Theorie der Potenzreste // Monatsh. Math. Phys. — 1892. — Vol. 3. — P. 265–284.

Работы автора по теме диссертации

[93] 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.

[94] Zvezdina M. A. Spectra of automorphic extensions of finite simple symplectic and orthogonal groups over fields of characteristic 2 // Сиб. электрон. матем. изв. — 2014. — Т. 11. — С. 823–832.

[95] 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].

[96] Звездина М. А. О спектрах автоморфных расширений конечных простых исключительных групп лиева типа // Алгебра и логика. — 2016. — Т. 55, № 5. — С. 540–557.

[97] Звездина М. А. О простых группах с графом простых чисел, как у знакопеременной группы // Современные проблемы математики: тезисы Международной (43-й Всероссийской) молодежной школы-конференции. Екатеринбург, 29 января — 5 февраля 2012 г. — Екатеринбург: ИММ УрО РАН, 2012. — С. 39.

[98] Zvezdina M. A. Spectrum of automorphic extensions of simple symplectic groups over fields of characteristic 2 // Международная конференция «Мальцевские чтения», тезисы докладов. Новосибирск, 11–15 ноября 2013 г. (электронное издание). — Новосибирск, 2013. Режим доступа: http://www.math.nsc.ru/ conference / malmeet /13/maltsev13.pdf. — С. 127.

[99] Zvezdina M. A. On spectra of automorphic extensions of Steinberg's triality groups // Международная конференция «Мальцевские чтения», тезисы докладов. Новосибирск, 10–13 ноября 2014 г. (электронное издание). — Новосибирск, 2014. Режим доступа: http://math.nsc.ru/conference/malmeet/14/Malmeet2014.pdf. — С. 99.

[100] Grechkoseeva M. A., Zvezdina M. A. Spectra of automorphic extensions of finite simple groups $F_4(q)$ and ${}^3D_4(q)$ // Международная конференция «Мальцевские чтения», тезисы докладов. Новосибирск, 3–7 мая 2015 г. (электронное издание). — Новосибирск, 2015. Режим доступа: http://math.nsc.ru/conference/malmeet/15/malmeet15.pdf. — С. 139.

[101] Zvezdina M. A. On the spectra of automorphic extensions of finite simple exceptional groups of Lie type // Международная конференция «Группы и графы, спектры и симметрии», тезисы докладов. Новосибирск, 15-28 августа 2016 г. — Новосибирск: Новосиб. гос. ун-т., 2016. — С. 115.

[102] Zvezdina M. A. Spectra of automorphic extensions of finite simple groups $E_6(q)$, ${}^2E_6(q)$ and $E_7(q)$ // Международная конференция «Мальцевские чтения», тезисы докладов. Новосибирск, 21-25 ноября 2016 г. (электронное издание). — Новосибирск, 2016. Режим доступа: http://www.math.nsc.ru/conference/malmeet/16/malmeet16.pdf. — С. 134.