Московский государственный университет
имени М. В. Ломоносова
Механико-математический факультет

На правах рукописи

УДК 512.54+512.55+512.54.03

Бунина Елена Игоревна

Автоморфизмы и элементарная эквивалентность групп Шевалле и других производных структур

01.01.06 — математическая логика, алгебра и теория чисел

Диссертация на соискание ученой степени
доктора физико-математических наук

Научный консультант:
д. ф.-м. н., профессор
Михалев Александр Васильевич

Москва
2010

Оглавление

Введение

Работа посвящена автоморфизмам и изоморфизмам групп Шевалле над кольцами, а также элементарной эквивалентности различных производных структур (в том числе групп Шевалле).

Исторический обзор

Автоморфизмы и изоморфизмы линейных и классических групп

Линейные группы — традиционный объект исследования математиков. Различные вопросы, связанные с их структурой, изучались К. Жорданом, Л. Диксоном, Б. ван дер Варденом, Г. Вейлем, Ж. Дьедонне, Ж. Титсом и их многочисленными последователями в огромном количестве работ. Ко второй половине XX века сложилось несколько крупных направлений исследования линейных групп, среди которых изучение нормальных подгрупп, описание линейных групп с помощью образующих и определяющих соотношений, описание подгрупп, порожденных некоторыми специальными элементами, а также описание автоморфизмов и изоморфизмов между линейными группами.

Изучение автоморфизмов классических групп началось работой Шрайера и Ван-дер-Вардена [147] 1928 г., в которой были описаны автоморфизмы группы PSL_n $(n \geqslant 3)$ над произвольным полем. Затем Дьедонне [98] в 1951 г. и Рикарт [145] в 1950 г. ввели метод инволюций, с помощью которого были описаны автоморфизмы группы GL_n $(n \geqslant 3)$ над телом.

Первый шаг в построении теории автоморфизмов над кольцами, а именно для группы GL_n $(n \geqslant 3)$ над кольцом целых чисел, сделали Хуа Логен и Райнер[110] в 1951 г. В 1957 г. Лэндин и Райнер [124], а также Вань Чжесянь [175] обобщили результат Хуа Логена и Райнера на некоммутативные области главных идеалов.

Методы отмечавшихся выше работ основывались главным образом на изучении инволюций в рассматриваемых группах. В 1976 г. О'Мира [129] придумал совершенно новый так называемый метод вычетных пространств, не использующий инволюций, с помощью которого ему удалось описать автоморфизмы группы GL_n $(n \geqslant 3)$ над областями целостности. Независимо от О'Миры, опираясь на изучение инволюций, автоморфизмы группы

$E_n(R)$ ($n \geqslant 3$) над областями целостности характеристики $\neq 2$ описал Янь Шицзянь [151] (1965 г.).

Помфрэ и Макдональд [143] в 1972 г., используя теорема Капланского, утверждающую, что проективные модули над локальным кольцом свободны, определили автоморфизмы группы GL_n ($n \geqslant 3$) над коммутативным локальным кольцом, в котором двойка обратима. Обратимость в кольце двойки дает возможность привлекать к изучению автоморфизмов группы GL_n технику, опирающуюся на изучение инволюций. Г.А. Носков [45] и В.Я. Блошицын [2] в 1975 г. описали автоморфизмы группы $\mathrm{GL}_n(R)$ ($n \geqslant 3$), если R — коммутативное кольцо, которое не порождается делителями нуля, с обратимой двойкой. В.С. Дроботенко и Э.Я. Погориляк [18] в 1977 г. сделали то же для конечных сумм локальных колец, Макдональд [128] в 1978 г. — если коммутативное кольцо R содержит только нулевой и единичный идемпотенты.

Уотерхауз [177] в 1980 г. доказал стандартность автоморфизмов групп GL_n ($n \geqslant 3$) над произвольным коммутативным кольцом с обратимой двойкой. Если 2 — необратимый элемент коммутативного локального кольца R, то автоморфизмы групп $\mathrm{SL}_n(R)$, $\mathrm{GL}_n(R)$ были изучены В.М. Петечуком в 1980 г. при $n \geqslant 4$ ([47]) и в 1982 г. при $n = 3$ ([48]). Основываясь на результатах над локальными кольцами в 1982 г. В.М. Петечук [46] описал автоморфизмы линейных групп GL_n, SL_n ($n \geqslant 4$) над произвольными коммутативными кольцами.

В качестве результатов для некоммутативных колец в 1980-х годах в работе И.З. Голубчиком и А.В. Михалевым [16] было дано описание изоморфизмов групп $\mathrm{GL}_n(R)$ и $\mathrm{GL}_m(S)$ над ассоциативными кольцами R и S с $\frac{1}{2}$ при $n, m \geqslant 3$, и несколько иным способом в работе Е.И. Зельманова [24]. Затем, в 1997 году И.З. Голубчиком [15] описание изоморфизмов между общими линейными группами было продолжено на случай произвольных ассоциативных колец и $n, m \geqslant 4$.

Группы Шевалле, их автоморфизмы и изоморфизмы

С другой стороны, теория алгебраических групп также является одной из важнейших областей современной алгебры. Она возникла в середине XX века, на стыке алгебраической геометрии, теории групп и теории Ли, и в настоящее время имеет приложения как в этих, так и в других областях математики: теории конечных групп, теории чисел, теории инвариантов, теории дифференциальных уравнений и т. д. Центральное место в теории алгебраических групп занимают полупростые алгебраические группы и их непосредственное обобщение — группы Шевалле.

Основы теории групп Шевалле были заложены в 1950-х, 1960-х годах в работах К. Шевалле, Ж. Титса, А. Бореля, А. Вейля, А. Гротендика, М. Демазюра, Р. Стейнберга и др. В частности, в 1956–1958 годах К. Шевалле получил классификацию полупростых алгебраических групп над алгебраически замкнутым полем. Позднее Шевалле показал, что все полупростые группы над алгебраически замкнутым полем в действительности определены над $\mathbb{Z}$, или, иначе говоря, получаются в результате расширения базы из некоторых групповых схем над $\mathbb{Z}$, называемых схемами Шевалле–Демазюра. Группы точек схем Шевалле–Демазюра над коммутативными кольцами называются группами Шевалле.

Частными случаями групп Шевалле являются расщепимые классические группы матриц $\mathrm{SL}\,_n(R)$, $\mathrm{SO}\,_n(R)$, $\mathrm{Sp}\,_n(R)$ (над коммутативным кольцом R с единицей); конечные простые группы типа Ли $A_n(q)$–$G_2(q)$ являются центральными факторами групп Шевалле.

Таким образом, группы Шевалле являются естественным продолжением как алгебраических групп, так и классических линейных групп над коммутативными кольцами.

Изучением групп Шевалле занимались такие известные математики, как К. Шевалле, Э. Абе, Р. Стейнберг, Дж. Хамфри, Н.А. Вавилов, Е.Б. Плоткин, В.М. Левчук, С.Г. Колесников и многие другие. В том числе, изучались автоморфизмы и изоморфизмы групп Шевалле над полями и различными классами колец. Например, Р. Стейнберг и Дж. Хамфри описали изоморфизмы групп Шевалле над полями. Описанию автоморфизмов групп Шевалле над различными коммутативными кольцами были посвящены работы многих авторов, среди которых отметим работы Бореля–Титса [83], Картера–Ю Чена [86], Ю Чена [88]–[92], Э. Абе [69], А.А. Клячко [121].

Э. Абе [69] доказал стандартность автоморфизмов для нетеровых колец, что полностью могло бы закрыть вопрос об автоморфизмах групп Шевалле над произвольными коммутативными кольцами (для случая системы корней ранга $\geqslant 2$ и колец с обратимой двойкой), однако в рассмотрении случая присоединенных элементарных групп в работе [69] содержится ошибка, которую не удается устранить методами этой статьи. Именно, в доказательстве леммы 11 используется то, что $\mathrm{ad}\,(x_\alpha)^2 = 0$ для всех длинных корней, что неверно в присоединенном представлении. Главной проблемой здесь является случай групп типа E_8, так как во всех остальных случаях группы Шевалле допускают представление, обладающие свойством $\mathrm{ad}\,(x_\alpha)^2 = 0$ для всех длинных корней, а в случае E_8 таких представлений нет.

Случаи, когда кольцо содержит достаточно много обратимых целых чисел (например, все рациональные числа) полностью закрыт в работе А.А. Клячко [121]. Таким образом, наибольший интерес на данный момент представляют кольца, в которых мало обратимых целых элементов (например, обратимы только единица и двойка, либо только единица).

По этой причине особый интерес представляет рассмотрение групп Шевалле над локальными кольцами (с обратимой двойкой или без нее), так как появляется возможность перейти к описанию автоморфизмов (и изоморфизмов) групп Шевалле над всеми коммутативными кольцами с помощью метода локализации. В данной диссертационной работе описаны автоморфизмы групп Шевалле всех типов над локальными кольцами с обратимой двойкой, а также типов A_l, D_l, E_l над локальными кольцами с не обратимой двойкой.

Заметим, что случай A_l был полностью рассмотрен в работах В. Уотерхауза [176], В.М. Петечука [46], Ли Фу-аня и Ли-Дзун-сяна [114], причем даже без условия обратимости двойки в кольце. Статья И.З. Голубчика и А.В. Михалева [15] охватывает случай системы корней C_l, который в данной диссертационной работе не рассматривается.

Элементарная эквивалентность

Две модели $\mathcal{U}$ и $\mathcal{U}'$ одного языка первого порядка $\mathcal{L}$ (например, две группы или два кольца) называются *элементарно эквивалентными*, если любое предложение φ языка $\mathcal{L}$ истинно в модели $\mathcal{U}$ тогда и только тогда, когда оно истинно в модели $\mathcal{U}'$. Любые две конечные модели одного языка элементарно эквивалентны тогда и только тогда, когда они изоморфны.

Любые две изоморфные модели элементарно эквивалентны, однако для бесконечных моделей обратное неверно. Например, поле $\mathbb{C}$ комплексных чисел и поле $\overline{\mathbb{Q}}$ алгебраических чисел элементарно эквивалентны, но не изоморфны, так как имеют различную мощность (для более подробных примеров см. [28]).

Обзоры и книги по элементарной эквивалентности

Классической книгой по теории моделей (в том числе и по элементарной эквивалентности) является книга [28]. Подробным обзором 1984 года результатов по элементарной эквивалентности и смежным вопросам является обзор [52] В. Н. Ремесленникова и В. А. Романькова "Теоретико-модельные и алгоритмические вопросы теории групп". Более новые результаты включены в обзоры Е.И. Буниной и А.В. Михалева [199] и [200], а также в обзор В. Гоулда, А.В. Михалева, Е.А. Палютина, А.А. Степановой [17]. Справочным материалом по теории моделей могут служить книги [58], [22], [36], [54]. Испытательным полигоном для большинства результатов теории моделей служат алгебра, теория чисел и анализ. Среди многочисленных книг и обзоров по приложениям теории моделей можно выделить те, в которых затрагиваются приложения к теории групп. Основные методы доказательств разрешимости и неразрешимости элементарных теорий изложены в книгах Тарского, Мостовского, Робинсона [167] и Ю. Л. Ершова [22]. Кроме того, в книге Ю. Л. Ершова приведена классификация полных теорий абелевых групп и показано на примерах из алгебры, как работает метод модельной полноты и родственное понятие относительной алгебраической замкнутости. Результаты по проблеме разрешимости элементарных теорий до 1964 года с подробным изложением методов доказательств освещены в обзоре Ю. Л. Ершова, И. А. Лаврова, А. Д. Тайманова, М. А. Тайцлина [20]. Вопросы разрешимости расширенных теорий, особенно расширенных теорий абелевых групп, разобраны в обзоре А. И. Кокорина и А. Г. Пинуса [31].

Элементарная эквивалентность различных классов групп

Ряд интересных задач в теории групп возник в связи с применением в ней теоретико-модельных методов. К их числу относится проблема классификации групп с точностью до элементарной эквивалентности, или в другой формулировке — проблема классификации *полных теорий* групп.

Анализ решений проблемы элементарной классификации групп определенного класса позволяет выделить три основных метода доказательств: модельной полноты, перехода к насыщенным моделям и прямой, когда доказывается формульность характеристик, определяющих групповую структуру исследуемой группы. Наиболее полные результаты по проблеме элементарной эквивалентности были получены для абелевых и линейных групп.

Весьма прозрачная и полезная в приложениях классификация абелевых групп по элементарным свойствам получена в 1954 г. польским математиком Шмелевой [152]. В настоящее время известны несколько доказательств ее результатов, полученных либо методом модельной полноты [27], [29] (исправление в [30], [79]), либо переходом к насыщенным группам [100], либо комбинацией этих методов [22]. Одним из наиболее важных следствий теоремы Шмелевой является разрешимость элементарной теории класса абелевых групп.

Проблема классификации групп по элементарным свойствам, как правило, является трудной задачей. Удовлетворительные результаты по ее решению получены для свободных групп, для некоторых классов нильпотентных групп и для классических линейных групп.

Сформулируем результаты по элементарной эквивалентности для степенных нильпотентных групп:

Теорема (А. Г. Мясников, В. Н. Ремесленников [42], [43], [41]). *Пусть G и H — нильпотентные $\mathbb{Q}$-группы конечного ранга. Тогда группа G элементарно эквивалентна группе H тогда и только тогда, когда основы G и H изоморфны, причем G и H одновременно либо совпадают со своими основами, либо не равны им.*

По определению, подгруппа $\overline{G} \leqslant G$ называется *основой* группы G, если $Z(\overline{G}) \leqslant G'$ и $G = \overline{G} \times C$, где $Z(G)$ — центр G, G' — коммутант G и $C \leqslant Z(G)$. Основа по группе определяется единственным образом с точностью до изоморфизма.

Эта теорема резко контрастирует с соответствующим результатом для абелевых групп и сводит проблему элементарной эквивалентности к проблеме изоморфизма для нильпотентных $\mathbb{Q}$-групп конечного ранга. Последняя проблема алгоритмически разрешима ([55]). В [41] доказательство теоремы получено с помощью перехода к насыщенным группам и детального изучения связей между абстрактными и алгебраическими изоморфизмами унипотентных алгебраических k-групп, где k — поле нулевой характеристики. В [43] доказательство теоремы получено прямым методом.

Ситуация в случае нильпотентных групп, т. е. степенных групп над кольцом $\mathbb{Z}$, более сложная, чем в случае поля $\mathbb{Q}$. Б. И. Зильбер [25] построил пример двух неизоморфных элементарно эквивалентных конечно порожденных 2-нильпотентных групп.

Ряд результатов 1980–1998 гг., принадлежащих французскому математику Франсису Огеру (Francis Oger), посвящен элементарной эквивалентности различных (конечно порожденных, в основном почти абелевых или почти нильпотентных) групп ([138], [133], [132], [139], [130], [135], [137], [134], [136], [140]).

В районе 1945 года Тарский сформулировал два предположения об элементарных теориях свободных групп. Первое из них состояло в том, что две свободные неабелевы группы различных рангов элементарно эквивалентны. Второе состояло в том, что элементарная теория свободной неабелевой группы разрешима. Обе гипотезы были доказаны в окрестности 1999 года А. Мясниковым и О. Харлампович в работах [117]–[120].

Элементарная эквивалентность линейных групп

Впервые вопросы связи элементарных свойств некоторых моделей с элементарными свойствами производных моделей были рассмотрены в 1961 г. А.И. Мальцевым в работе [37]. Он доказал, что группы $G_n(K)$ и $G_m(L)$ ($G = \mathrm{GL}\,, \mathrm{SL}\,, \mathrm{PGL}\,, \mathrm{PSL}\,, n, m \geqslant 3$, K, L — поля характеристики 0) элементарно эквивалентны тогда и только тогда, когда $m = n$ и поля K и L элементарно эквивалентны.

Продолжение эта теория получила в 1992 году, когда с помощью конструкции ультрапроизведения и теоремы об изоморфизме [28] К.И. Бейдар и А.В. Михалев в работе [81] нашли общий подход к проблемам элементарной эквивалентности различных алгебраических структур и обобщили теорему Мальцева для случая, когда K и L являются телами и ассоциативными кольцами.

Продолжением исследований в этой области явились работы Е.И. Буниной 1998–2001 гг. (см. [181], [183], [192]), в которых результаты А.И. Мальцева была распространены на унитарные линейные группы над телами и ассоциативными кольцами с инволюцией, а также на группы Шевалле над алгебраически замкнутыми полями.

Тематика исследований А.И. Мальцева активно продолжается в данной диссертации. Во второй главе изучается элементарная эквивалентность групп Шевалле над полями и локальными кольцами (эти результаты опубликованы в работах [185], [189], [192], [197]).

В третьей главе изучены элементарные свойства полугрупп неотрицательных матриц над линейно упорядоченными кольцами (этот результат опубликован в работе [190]). Элементарные свойства полугрупп неотрицательных матриц над частично упорядоченными коммутативными кольцами были изучены Е.И. Буниной и П.П. Семеновым в работе [5], не вошедшей в данную диссертацию.

Элементарная эквивалентность колец инцидентности изучалась автором совместно с А.С. Доброхотовой–Майковой (см. [6]) и также не вошла в данную работу.

Структуры бесконечных рангов и логика второго порядка

В [102] Фелгнер предложил изучить проблему элементарной эквивалентности бесконечномерных общих линейных групп и других классических групп над полями. В [169] В. Толстых решает эту проблему для бесконечномерных групп типов GL, PGL, $\Gamma L, P\Gamma L$ для достаточно широкого класса тел. Предмет изучения статьи [169] может быть описан как исследование *выразительности* языка логики первого порядка для бесконечномерных классических групп и близких структур. Похожие проблемы изучались во многих статьях, например, в [149], [150] Шелахом для бесконечномерных симметрических групп, в его статье [169], посвященной полугруппам эндоморфизмов свободных алгебр, в серии статей об автоморфизмах групп булевых алгебр (Рубин и Шелах, [146]), в работе [125] Магидора, Розенталя, Рубина и Срура о решетках замкнутых подмножеств систем Штейница.

Другая работа В. Толстых [168] посвящена исследованию теории группы автоморфизмов бесконечно порожденной свободной группы. Пусть F_k — свободная группа бесконечного ранга k. В работе [168] доказано, что теория второго порядка множества k и элементарная теория группы $\mathrm{Aut}\, F_k$ интерпретируются друг в друге равномерно по F_k, а следовательно, группы автоморфизмов $\mathrm{Aut}\, F_k$ и $\mathrm{Aut}\, F_\lambda$ элементарно эквивалентны тогда и только тогда, когда k и λ эквивалентны в логике второго порядка.

Связь между совпадением теорий первого порядка одних структур и совпадением теорий второго порядка некоторых других структур была установлена в ряде работ А. Г. Пинусом. Например, работа [50] посвящена элементарной эквивалентности решеток разбиений. В ней показано, что выразительные возможности решеток разбиений в логике первого порядка совпадают с выразительными возможностями логики второго порядка. Именно, пусть $L(A)$ — решетка разбиений на множестве A, $Th(L(A))$ — теория первого порядка решетки $L(A)$, $Th_2(A)$ — теория множества A (с пустой сигнатурой) в полной логике второго порядка. Доказано, что для любых множеств A, B теории $Th(L(A))$ и $Th(L(B))$ совпадают тогда и только тогда, когда $Th_2(A) = Th_2(B)$.

Результаты, полученные в 2000 г. в [49] А. Г. Пинусом и Г. Роузом, посвящены элементарной эквивалентности решеток подалгебр свободных алгебр.

В силу элементарной эквивалентности любых двух бесконечно порожденных V-свободных алгебр понятен интерес к вопросу об элементарной эквивалентности производных структур от свободных алгебр многообразий, обзор по этому поводу см. [142]. В частности, там доказано, что для любого нормального многообразия V, решетка конгруэнций алгебры $F_V(\kappa)$ элементарно определима в классе всех подобных решеток тогда и только тогда, когда кардинал κ определим в полной логике второго порядка. Возникает вопрос об элементарной эквивалентности структур, связанных с понятием подалгебры, для V-свободных алгебр с различным числом порождающих.

В четвертой главе данной диссертации рассмотрена связь свойств второго порядка ассоциативных колец и свойств первого порядка категорий модулей, колец эндоморфизмов, групп автоморфизмов и проективных пространств модулей бесконечного ранга над этими кольцами (данные результаты опубликованы в [184]).

Также в четвертой главе доказываются теоремы, аналогичные теореме Бэра–Капланского о кольцах эндоморфизмов абелевых p-групп (абелева p-группа определяется своим кольцом эндоморфизмов), но для элементарной эквивалентности. Показано, что элементарная теория кольца эндоморфизмов абелевой p-группы определяет полную теорию второго порядка (в некоторых случаях ее счетное ограничение) самой абелевой группы. Данный результат опубликован в работе [186].

В работах [193] и [201] Е.И. Буниной и А.В. Михалева (не вошедших в данную диссертационную работу) рассматривались категории полигонов над моноидами, а также моноиды эндоморфизмов свободных полигонов над моноидами. Было показано, что при определенных условиях на исходные моноиды моноиды эндоморфизмов свободных полигонов над ними элементарно эквивалентны тогда и только тогда, когда сами моноиды эквивалентны в логике второго порядка.

Элементарная эквивалентность других структур и производных конструкций

В работе [99] приводится пример двух групп G и H, таких, что $G \equiv H$, но $G' \not\equiv H'$, где G', H' — коммутанты групп G и H.

Для модулей существует достаточно простой критерий элементарной эквивалентности. Именно: два модуля M и N над кольцом R элементарно эквивалентны тогда и только тогда, когда для любых двух 1-позитивно-примитивных формул (т. е. формул вида $\exists x \Theta$, где Θ — конъюнкция атомных формул) φ, ψ таких, что $\psi \to \varphi$, мощности абелевых групп $\varphi(M)/\psi(M)$ и $\varphi(N)/\psi(N)$ либо бесконечны, либо конечны и совпадают.

В ряде работ изучался вопрос о сохранении элементарной эквивалентности для различных теоретико-групповых конструкций. Например, в работе [80] доказано, что

1) для модулей над вполне приводимым кольцом тензорное произведение, рассматриваемое как абелева группа, сохраняет элементарную эквивалентность;

2) для счетного свободного булевого кольца R существуют R-модули A, B, C, D такие, что $A \equiv B$, $C \equiv D$, $A \otimes_R C \cong \langle 0 \rangle$ и $B \otimes_R D \cong \mathbb{Z}(2)$.

В [28] (стр. 392) доказано, что фильтрованные произведения, фильтрованные степени, прямые произведения сохраняют элементарную эквивалентность.

Проблема элементарной эквивалентности свободных произведений $H_1 * G_1$ и $H_2 * G_2$, где G_1, G_2, H_1, H_2 — группы и при этом $H_1 \equiv H_2$, $G_1 \equiv G_2$, остается открытой в настоящее время (сообщено автору В.Н. Ремесленниковым).

Не сохраняют элементарной эквивалентности: а) операция сплетения групп [59], [60], [61], б) нильпотентные произведения групп [141].

Работа [44] рассматривает элементарную эквивалентность свободных произведений групп.

Большое число работ посвящено проблеме элементарной эквивалентности расширенных теорий абелевых групп (см. библиографию и обзор [31]).

Уилер [180] установил, что кольца верхних треугольных матриц порядка ≥ 3 над полями P и P^* элементарно эквивалентны в том и только том случае, когда элементарно эквивалентны поля P и P^*.

Общая характеристика работы

Цель работы и основные задачи

Цель данной работы состоит в создании новых универсальных методов исследования автоморфизмов, изоморфизмов и элементарной эквивалентности различных важнейших производных алгебраических структур таких, как кольца эндоморфизмов, группы автоморфизмов, проективные геометрии, категории модулей, матричные группы (в первую очередь, группы Шевалле), в установлении связи между изоморфизмами или элементарной эквивалентностью производных структур и условиями, которым должны отвечать базисные структуры, в точном описании автоморфизмов различных алгебраических структур, таких, как группы Шевалле над коммутативными кольцами, полугруппы неотрицательных обратимых матриц над упорядоченными кольцами. Основными задачами диссертации являются: описание (доказательство стандартности) автоморфизмов групп Шевалле над локальными кольцами; нахождение необходимых и достаточных условий того, что (элементарные) группы Шевалле над полями или локальными кольцами элементарно эквивалентны; описание автоморфизмов и элементарной эквивалентности полугрупп неотрицательных обратимых матриц над линейно упорядоченными кольцами; нахождение необходимых и достаточных условий того, чтобы две категории модулей над кольцами, два кольца эндоморфизмов, две группы автоморфизмов, две проективные геометрии модулей бесконечного ранга над кольцами были элементарно эквивалентны; продолжение теоремы Бэра–Капланского об изоморфизмах колец эндоморфизмов абелевых p-групп на случай элементарной эквивалентности.

Основные методы исследования

В работе используются классические методы структурной теории колец, линейной алгебры, теории линейных групп, теории моделей и математической логики, в том числе методы А.И. Мальцева, К.И. Бейдара, А.В. Михалева, И.З. Голубчика, В.М. Петечука, метод инволюций, переработанный автором в кандидатской диссертации, а также новые методы, в том числе метод перевода задач об автоморфизмах матричных групп над локальными кольцами к системам целочисленных линейных уравнений, метод интерпретации теорий второго порядка алгебраических систем в их производных структурах.

Научная новизна

Основные результаты работы являются новыми. Среди них:

- Разработка новых методов описания автоморфизмов и изоморфизмов групп Шевалле с помощью линейных уравнений над локальными кольцами. Получение полного описания (доказательство стандартности) автоморфизмов групп Шевалле следующих типов:

  — типов A_l, D_l, E_l, B_l, C_l, F_4, $l > 1$, над локальными кольцами с обратимой двойкой;

  — типа G_2 над локальными кольцами с обратимыми двойкой и тройкой;

  — типов A_l, D_l, E_l, $l > 2$, над локальными кольцами с необратимой двойкой (теорема 1.1).

- Описание элементарных свойств и элементарной эквивалентности групп Шевалле над полями и локальными кольцами с обратимой двойкой с использованием метода инволюций (доработанного автором для случая групп Шевалле), методов А.И. Мальцева и метода ультрастепеней К.И. Бейдара и А.В. Михалева. Сведение элементарной эквивалентности групп Шевалле описанных типов к элементарной эквивалентности базисных полей или колец (теоремы 2.1 и 2.2).

- Описание автоморфизмов и элементарной эквивалентности полугруппы неотрицательных обратимых матриц над линейно упорядоченными кольцами с обратимой двойкой, что является продолжением описания аналогичных полугрупп над линейно упорядоченными телами, полученного А.В. Михалевым и А.М. Шаталовой (теоремы 3.1 и 3.2).

- Получение связи между элементарной эквивалентностью

  — категорий модулей над кольцами,

  — колец эндоморфизмов свободных модулей над кольцами бесконечных рангов,

  — групп автоморфизмов свободных модулей над кольцами бесконечных рангов,

  — проективных геометрий свободных модулей над кольцами

  и эквивалентности в логике второго порядка структур, связанных с кольцами (теоремы 4.7, 4.13, 4.15 и 4.19).

- Разработка методов работы с логикой второго порядка, построение интерпретации теории второго порядка кольца в теории первого порядка его производной структуры (категории модулей над ним, кольца эндоморфизмов, группы автоморфизмов, проективной геометрии модулей над ним).

- Получение в качестве следствий полного описания элементарной эквивалентности колец эндоморфизмов и групп автоморфизмов модулей бесконечного ранга над

  — телами;

  — областями главным идеалов;

  — коммутативными кольцами;

  — локальными кольцами;

  — артиновыми кольцами;

— полупростыми кольцами (следствия из теорем 4.13 и 4.19).

- Получение аналога теорема Бэра–Капланского об изоморфизме колец эндоморфизмов абелевых p-групп для элементарной эквивалентности. Интерпретация логики второго порядка абелевой p-группы в кольце ее эндоморфизмов, разработка методов кодирования элементов абелевой группы в кольце ее эндоморфизмов (теоремы 4.33, 4.34, 4.35).

Краткое содержание работы

Глава 1 посвящена изучению автоморфизмов групп Шевалле над локальными кольцами. Автоморфизмы групп Шевалле над полями были полностью описаны в 1970-е годы Стейнбергом и Хамфри, в 1993 году появилась работа Э. Абе, описывающая автоморфизмы групп Шевалле над нетеровыми кольцами с обратимой двойкой. В этой работе для случая системы корней E_8 имело место ошибка, неустранимая методами самой работы. В главе 1 данной диссертации проблема автоморфизмов групп Шевалле решена для групп Шевалле различных типов над локальными кольцами с обратимой двойкой, а также для групп Шевалле типов A_l, D_l, E_l, $l \geqslant 3$, над локальными кольцами с необратимой двойкой. Для доказательства объединены различные методы, использованные ранее для описания автоморфизмов групп GL и SL над локальными кольцами, методы линейной алгебры, а также их специфическое объединение, придуманное автором диссертации. Для доказательства приходилось проводить очень много различных матричных подсчетов, они выполнялись как вручную, так и на компьютере, не все из них приведены в тексте диссертации. Особенно сложными подсчетами отличается случай необратимой двойки, в процессе вычислений неоднократно возникали матрицы размера, большего чем 20×20.

Основными объектами, рассматриваемыми в первой главе, являются группа Шевалле $G_\pi(\Phi, R)$ с системой корней Φ ранга, большего единицы, над локальным кольцом R (с обратимой или необратимой двойкой) и ее элементарная подгруппа $E_\pi(\Phi, R)$, порожденная элементарными корневыми унипотентами $x_\alpha(t)$, $\alpha \in \Phi$, $t \in R$.

В первом параграфе приводятся основные определения групп Шевалле, их свойства, определяются четыре типа автоморфизмов группы Шевалле $G_\pi(\Phi, R)$, называемые *стандартными*:

Центральные автоморфизмы. Пусть $C_G(R)$ — центр группы $G_\pi(\Phi, R)$, $\tau : G_\pi(\Phi, R) \to C_G(R)$ — гомоморфизм групп. Тогда отображение $x \mapsto \tau(x)x$ из $G_\pi(\Phi, R)$ на себя является автоморфизмом группы $G_\pi(\Phi, R)$, который обозначается буквой τ и называется *центральным автоморфизмом* группы $G_\pi(\Phi, R)$.

Кольцевые автоморфизмы. Пусть $\rho : R \to R$ — автоморфизм кольца R. Отображение $(x_{i,j}) \mapsto (\rho(x_{i,j}))$ из $G_\pi(\Phi, R)$ на себя является автоморфизмом группы $G_\pi(\Phi, R)$, который обозначается той же буквой ρ и называется *кольцевым автоморфизмом* группы $G_\pi(\Phi, R)$. Заметим, что для всех $\alpha \in \Phi$ и $t \in R$ элемент $x_\alpha(t)$ отображается в $x_\alpha(\rho(t))$.

Внутренние автоморфизмы. Пусть S — некоторое кольцо, содержащее R, g — элемент группы $G_\pi(\Phi, S)$, нормализующий подгруппу $G_\pi(\Phi, R)$. Тогда отображение $x \mapsto gxg^{-1}$ является автоморфизмом группы $G_\pi(\Phi, R)$, который обозначается i_g и называется *внутренним автоморфизмом, индуцированным элементом* $g \in G_\pi(\Phi, S)$. Если $g \in$

$G_\pi(\Phi, R)$, то назовем i_g *строго внутренним* автоморфизмом.

Диаграммные (графовые) автоморфизмы. Пусть δ — автоморфизм системы корней Φ такой, что $\delta\Delta = \Delta$. Тогда существует единственный автоморфизм группы $G_\pi(\Phi, R)$ (будем обозначать его той же буквой δ) такой, что для любого $\alpha \in \Phi$ и $t \in R$ элемент $x_\alpha(t)$ переходит в $x_{\delta(\alpha)}(\varepsilon(\alpha)t)$, где $\varepsilon(\alpha) = \pm 1$ для всех $\alpha \in \Phi$ и $\varepsilon(\alpha) = 1$ для всех $\alpha \in \Delta$.

Автоморфизм σ группы $G_\pi(\Phi, R)$ (или $E_\pi(\Phi, R)$) называется *стандартным*, если он является композицией автоморфизмов введенных четырех типов.

Наряду со стандартными автоморфизмами автором вводится следующий "временный" тип автоморфизмов элементарной присоединенной группы Шевалле:

Автоморфизмы-сопряжения. Пусть V — пространство представления группы $E_{\mathrm{ad}}(\Phi, R)$, $C \in \mathrm{GL}(V)$ — матрица, оставляющая группу Шевалле на месте:

$$CE_{\mathrm{ad}}(\Phi, R)C^{-1} = E_{\mathrm{ad}}(\Phi, R).$$

Тогда отображение $x \mapsto CxC^{-1}$ из $E_\pi(\Phi, R)$ на себя является автоморфизмом группы Шевалле, который обозначается i и называется *автоморфизмом-сопряжением* группы $E(R)$, *индуцированным элементом* C группы $\mathrm{GL}(V)$.

Далее в первом параграфе формулируется следующая основная теорема:

Теорема 1 (теорема 1.1). *Пусть $G = G_\pi(\Phi, R)$ ($E_\pi(\Phi, R)$) — (элементарная) группа Шевалле со следующими условиями*:

1) *если рассматривается система корней A_l, D_l или E_l, $l \geqslant 3$, то R — произвольное локальное коммутативное кольцо*;

2) *если рассматривается система корней A_2, F_4, B_l, C_l, $l \geqslant 2$, то R — произвольное локальное коммутативное кольцо с* $1/2$;

3) *если рассматривается система корней G_2, то R — произвольное локальное коммутативное кольцо с $1/2$ и $1/3$.*

Тогда любой автоморфизм группы G стандартен. Если группа Шевалле при этом присоединенная, то внутренний автоморфизм в композиции является строго внутренним.

Этот основной результат получается с помощью применения двух следующих теорем:

Теорема 2 (теорема 1.2). *Каждый автоморфизм элементарной присоединенной группы Шевалле рассматриваемого выше типа является композицией кольцевого, диаграммного автоморфизмов и автоморфизма–сопряжения.*

Теорема 3 (теорема 1.3). *Каждый автоморфизм–сопряжение элементарной присоединенной группы Шевалле рассматриваемого типа является композицией строго внутреннего (сопряжения с помощью элемента соответствующей группы Шевалле) и диаграммного автоморфизмов.*

Во втором, третьем, четвертом и пятом параграфах доказывается теорема 2 для колец с обратимой двойкой: во втором параграфе по произвольному автоморфизмы элементарной присоединенной групп Шевалле G строится (с помощью замены базиса в пространстве представления группы G) изоморфизм группы G на некоторую подгруппу $\mathrm{GL}_n(R)$, с тем свойством, что ее образ при факторизации R по радикалу совпадает с кольцевым автоморфизмом. В третьем параграфе с помощью еще одной замены базиса мы приходим к изоморфизму G на подгруппу в $\mathrm{GL}_n(R)$ со всеми свойствами предыдущего и такому, что все элементы $w_\alpha(1)$ переходят сами в себя. В четвертом параграфе проводится еще одна дополнительная замена базиса такая, что рассматриваемый изоморфизм начинает обладать дополнительным свойством: все элементы $x_\alpha(1)$, $\alpha \in \Phi$, также переходят в себя. Доказано, что при этом элементы $h_\alpha(t)$ переходят в элементы $h_\alpha(s)$. В пятом параграфе показано, что соответствие $t \mapsto s$ продолжается до автоморфизма кольца R, после чего получается, что композиция изначального автоморфизма и некоторой замены базиса (т. е. внутреннего автоморфизма) является кольцевым автоморфизмом группы Шевалле G. Таким образом, в параграфе 5 теорема 2 доказана для локальных колец с обратимой двойкой.

В шестом и седьмом параграфах доказывается теорема 3. В шестом параграфе первой главы показано, как свести доказательство к линейным уравнениям над локальными кольцами, а в седьмом параграфе показано, как найти нужное решение этих уравнений для различных систем корней. В конце седьмого параграфа полностью доказывается теорема 3. Наконец, восьмой параграф первой главы посвящен доказательству теоремы 1. Для присоединенных элементарных групп Шевалле эта теорема является прямым следствием теорем 2 и 3, теорему 1 остается доказать для всех других элементарных групп Шевалле, а далее для самих групп Шевалле.

Девятый параграф посвящен рассмотрению групп Шевалле типов A_l, D_l, E_l над локальными кольцами с необратимой двойкой. Требуется только доказать теорему 2, так как теорема 3 доказывается сразу и для колец с обратимой двойкой, и для колец с необратимой двойкой. Для этого случая все основные идеи и методы остаются теми же, но приходится рассматривать более сложные матрицы (матрицы порядка три вида $w_\alpha(1) \cdot x_\alpha(1)$), которые требуется на первом этапе переводить в себя заменой базиса. Все вычисления усложняются из-за того, что нет возможности делить на два.

Глава 2 посвящена элементарной эквивалентности групп Шевалле над полями и локальными кольцами. Теоремы об элементарной эквивалентности линейных групп восходят к А.И. Мальцеву, доказавшему в 1961 году, что линейные (GL, SL) и проективные линейные (PGL, PSL) группы над полями элементарно эквивалентны тогда и только тогда, когда их размеры совпадают, а поля элементарно эквивалентны. Подобные теоремы получены и для групп Шевалле:

Теорема 4 (теорема 2.1). *Пусть $G = G_\pi(\Phi, K)$ и $G' = G_{\pi'}(\Phi', K')$ (или $E_\pi(\Phi, K)$ и $E_{\pi'}(\Phi', K')$) — две (элементарные) группы Шевалле над бесконечными полями K и K' характеристики, отличной от двух, с решетками весов Λ и Λ' соответственно. Тогда группы G и G' элементарно эквивалентны тогда и только тогда, когда системы корней Φ и Φ' изоморфны, поля K и K' элементарно эквивалентны, решетки Λ и Λ' совпадают.*

Теорема 5 (теорема 2.2). *Пусть $G = G_\pi(\Phi, R)$ и $G' = G_{\pi'}(\Phi', R')$ (или $E_\pi(\Phi, R)$ и $E_{\pi'}(\Phi', R')$) — две (элементарные) группы Шевалле над локальными кольцами R и R' с обратимой двойкой (в случае системы корней G_2 еще и с обратимой тройкой), в одной из систем корней Φ, Φ' присутствует простая подсистема корней, отличная от A_1. Пусть решетки весов групп G и G' обозначены через Λ и Λ' соответственно. Тогда группы G и G' элементарно эквивалентны тогда и только тогда, когда системы корней Φ и Φ' изоморфны, кольца R и R' элементарно эквивалентны, решетки Λ и Λ' совпадают.*

В первом параграфе доказываются более простые импликации, а именно, следующие две теоремы:

Теорема 6 (теорема 2.3). *Если две группы Шевалле $G = G_\pi(\Phi, R)$ и $G' = G_\pi(\Phi, R')$ построены с помощью одной и той же комплексной алгебры Ли типа Φ и одного и того же ее представления π, а также с помощью элементарно эквивалентных колец R и R', то $G \equiv G'$.*

Теорема 7 (теорема 2.4). *Если две элементарные группы Шевалле $E = E_\pi(R, \Phi)$ и $E' = E_\pi(R', \Phi)$ построены с помощью одной и той же комплексной алгебры Ли типа Φ и одного и того же ее представления π, а также с помощью элементарно эквивалентных полулокальных колец R и R' с $1/2$, то $E \equiv E'$.*

Во втором параграфе доказано, что если две (элементарные) группы Шевалле элементарно эквивалентны, то их системы корней совпадают, а исходные кольца элементарно эквивалентны, решетки весов изоморфны. Далее имея две элементарно эквивалентные элементарные группы Шевалле E и E', мы также имеем две элементарно эквивалентные элементарные присоединенные группы Шевалле E_{ad} и E'_{ad}, являющиеся факторами по центру исходных групп.

В параграфах 3–12 рассматриваются группы Шевалле над полями, доказывается теорема 4. Можно считать, что поле имеет характеристику, отличную от двух, и бесконечно (для конечных полей элементарная эквивалентность совпадает с изоморфизмом, поэтому результат будет следовать из теорем Стейнберга и Хамфриса).

В § 3 классические элементарные присоединенные группы Шевалле над полями отождествляются с некоторыми подгруппами группы $\mathrm{GL}_n(K)$.

В § 4 описывается, как устроены инволюции (элемента порядка два) в классических группах Шевалле над полями.

В пятом параграфе второй главы доказано, что для любых двух классических групп Шевалле с неизоморфными системами корней существует предложение первого порядка, истинное в одной группе и ложное во второй. Делается это с помощью рассмотрения инволюций, максимальных множеств коммутирующих инволюций, коммутантов централизаторов инволюций.

В параграфах 6–10 рассматриваются по отдельности исключительные системы корней. Например, в § 6 рассматриваются группы Шевалле типа G_2 и доказывается следующая лемма:

Лемма 8 (лемма 2.10). *Существует предложение φ_{G_2} первого порядка, истинное в любой присоединенной группе типа G_2 и ложное во всех классических присоединенных группах Шевалле.*

В § 7 рассматриваются группы Шевалле типа F_4, а в § 8,9,10 соответственно группы типа E_6, E_7, E_8. Наконец, в конце десятого параграфа доказано следующее

Предложение 9 (предложение 2.3). *Если две (элементарные) группы Шевалле над бесконечными полями характеристики, не равной 2, элементарно эквивалентны, то соответствующие системы корней совпадают.*

Параграф 11 посвящен доказательству того, что если две группы Шевалле одинакового типа элементарно эквивалентны, то поля, по которым они построены, элементарно эквивалентны. Для этого сначала данный результат доказывается для самой “маленькой” системы корней — A_1:

Лемма 10 (лемма 2.15). *Если группы* $\mathrm{PSL}_2(K)$ *и* $\mathrm{PSL}_2(K')$ (K, K' *— бесконечные поля характеристики* $\neq 2$) *элементарно эквивалентны, то поля* K, K' *элементарно эквивалентны.*

Этот результат, в том числе, является дополнением к теореме А.И. Мальцева об элементарной эквивалентности линейных групп над полями, так как в работе Мальцева для групп SL и PSL рассматривался размер, больший двух.

Далее в § 11 для произвольной системы корней Φ берется фактор по центру коммутанта централизатора подходящей инволюции, который является прямым произведением двух групп Шевалле, одна из них есть $\mathrm{PSL}_2(K)$ (в предыдущих параграфах показано, что такая инволюция всегда найдется). После этого достаточно воспользоваться леммой 10. В результате получается

Предложение 11 (предложение 2.4). *Если две присоединенные элементарные группы Шевалле* $G(\Phi, K)$ *и* $G(\Phi, K')$ (K, K' *— бесконечные поля характеристики, отличной от двух*) *элементарно эквивалентны, то поля* K, K' *элементарно эквивалентны.*

В § 12 остается рассмотреть решетки весов групп Шевалле. Доказывается

Предложение 12 (предложение 2.5). *Если две* (*элементарные*) *группы Шевалле элементарно эквивалентны, то их решетки весов совпадают.*

Таким образом, к концу § 12 полностью доказывается теорема 4. Остальные параграфы второй главы посвящены доказательству теоремы 5.

В § 13 сначала доказывается, что подгруппа $E_J = E_{\mathrm{ad}}(\Phi, R, J)$ определима в группе $E = E_{\mathrm{ad}}(\Phi, R)$, т. е. если две элементарные присоединенные группы Шевалле над локальными кольцами элементарно эквивалентны, то и соответствующие элементарные присоединенные группы Шевалле над вычетными полями элементарно эквивалентны. Таким образом, в § 12 доказано, что если две группы Шевалле над локальными кольцами элементарно эквивалентны, то их системы корней совпадают.

В § 14 второй главы доказывается, что известное разложение Гаусса для элементов групп Шевалле над локальными кольцами можно задавать в виде формул:

Предложение 13 (предложение 2.7). (1) *Любой элемент* x *группы Шевалле* G (E) *над локальным кольцом* R *представляется в виде*

$$x = utvu' \quad (x = uhvu'),$$

где $u, u' \in U(R)$, $v \in V(R)$, $t \in T(R)$, $h \in H(R)$;

(2) *Для разложений* $x_1 = u_1t_1v_1u_1'$ *и* $x_2 = u_2t_2v_2u_2'$, *где*

$$\begin{aligned}
u_i &= x_{\alpha_1}(t_1^{(i)}) \dots x_{\alpha_n}(t_n^{(i)}),\\
u_i' &= x_{\alpha_1}(s_1^{(i)}) \dots x_{\alpha_n}(s_n^{(i)}),\\
v_i &= x_{-\alpha_1}(r_1^{(i)}) \dots x_{-\alpha_n}(r_n^{(i)}),\\
t_i &= h_{\alpha_1}(\xi_1^{(i)}) \dots h_{\alpha_l}(\xi_l^{(i)}), \quad i = 1, 2,
\end{aligned}$$

существует формула первого порядка кольцевого языка

$$\varphi(t_1^{(1)},\dots,t_n^{(1)},t_1^{(2)},\dots,t_n^{(2)},s_1^{(1)},\dots,s_n^{(1)},s_1^{(2)},\dots,s_n^{(2)},\\ r_1^{(1)},\dots,r_n^{(1)},r_1^{(2)},\dots,r_n^{(2)},\xi_1^{(1)},\dots,\xi_n^{(1)},\xi_1^{(2)},\dots,\xi_n^{(2)}),$$

истинная тогда и только тогда, когда

$$x_1 = x_2;$$

(3) *Аналогично, для разложений* $x_1 = u_1t_1v_1u_1'$, $x_2 = u_2t_2v_2u_2'$ *и* $x_3 = u_3t_3v_3u_3'$, *где*

$$\begin{aligned} u_i &= x_{\alpha_1}(t_1^{(i)})\dots x_{\alpha_n}(t_n^{(i)}),\\ u_i' &= x_{\alpha_1}(s_1^{(i)})\dots x_{\alpha_n}(s_n^{(i)}),\\ v_i &= x_{-\alpha_1}(r_1^{(i)})\dots x_{-\alpha_n}(r_n^{(i)}),\\ t_i &= h_{\alpha_1}(\xi_1^{(i)})\dots h_{\alpha_l}(\xi_l^{(i)}),\quad i=1,2,3, \end{aligned}$$

существует формула первого порядка кольцевого языка

$$\psi(t_1^{(i)},\dots,t_n^{(i)},s_1^{(i)},\dots,s_n^{(i)},r_1^{(i)},\dots,r_n^{(i)},\xi_1^{(i)},\dots,\xi_n^{(i)}),$$

истинная тогда и только тогда, когда

$$x_3 = x_1\cdot x_2.$$

В параграфе § 14 с помощью перехода к ультрастепеням и теореме Кейслера-Шелаха об изоморфизме (методы, впервые использованные К.И. Бейдаром и А.В. Михалевым для линейных групп над кольцами показано, что если две рассматриваемые группы Шевалле элементарно эквивалентны, то элементарно эквивалентны и базисные кольца, по которым они построены.

В последнем параграфе все результаты сводятся воедино и доказывается теорема 5.

Третья глава диссертации посвящена автоморфизмам и элементарной эквивалентности полугрупп неотрицательных обратимых матриц над упорядоченными кольцами. В первом параграфе вводятся основные определения. Определяется полугруппа $G_n(R)$, состоящая из обратимых в группе $\mathrm{GL}_n(R)$ матриц, все коэффициенты которых неотрицательны. Далее вводятся следующие важные подполугруппы и подмножества полугруппы $G_n(R)$:

Определение 14 (определение 3.4). Пусть $I = I_n$, $\Gamma_n(R)$ — группа, состоящая из всех обратимых матриц из $G_n(R)$, Σ_n — симметрическая группа порядка n, S_σ — матрица перестановки $\sigma\in\Sigma_n$ (т. е. матрица $(\delta_{i\sigma(j)})$, где $\delta_{i\sigma(j)}$ — символ Кронекера), $S_n = \{S_\sigma|\sigma\in\Sigma_n\}$, $\mathrm{diag}\,[d_1,\dots,d_n]$ — диагональная матрица с элементами $d_1,\dots,d_n$ на диагонали, $d_1,\dots,d_n\in R_+^*$. Через $D_n(R)$ обозначим группу всех обратимых диагональных матриц из $G_n(R)$, через $D_n^Z(R)$ — центр группы $D_n(R)$.

Определение 15 (определение 3.8). Через $B_{ij}(x)$ обозначим матрицу $I + xE_{ij}$. Пусть $\mathbf{P}$ обозначает подполугруппу в $G_n(R)$, порожденную всеми матрицами S_σ $(\sigma \in \Sigma_n)$, $B_{ij}(x)$ $(x \in R_+, i \neq j)$ и $\mathrm{diag}\,[\alpha_1, \dots, \alpha_n] \in D_n(R)$.

Определение 16 (определение 3.9). Две матрицы $A, B \in G_n(R)$ называются $\mathcal{P}$-эквивалентными, если существуют матрицы $A_j \in G_n(R)$, $j = 0, \dots, k$, $A = A_0$, $B = A_k$, и матрицы $P_i, \widetilde{P}_i, Q_i, \widetilde{Q}_i \in \mathbf{P}$, $i = 0, \dots, k-1$ такие, что $P_i A_i \widetilde{P}_i = Q_i A_{i+1} \widetilde{Q}_i$.

Определение 17 (определение 3.10). Через $\mathrm{GE}_n^+(R)$ обозначим подполугруппу в $G_n(R)$, порожденную всеми матрицами, $\mathcal{P}$-эквивалентными матрицам из $\mathbf{P}$.

Второй параграф посвящен описанию автоморфизмов полугруппы неотрицательных обратимых матриц над линейно упорядоченными кольцами с обратимой двойкой. Основным результатом этого параграфа является следующая

Теорема 18 (определение 3.1). *Пусть Φ — автоморфизм полугруппы $G_n(R)$, $n \geqslant 3$, $1/2 \in R$, кольцо R линейно упорядочено. Тогда на полугруппе $\mathrm{GE}_n^+(R)$ $\Phi = \Phi_M \Phi^c \Omega$, где Φ_M — внутренний автоморфизм с помощью матрицы $M \in \Gamma_n(R)$, Φ^c — кольцевой автоморфизм при помощи автоморфизма $c(\cdot) \in \mathrm{Aut}\,(R_+)$, $\Omega(\cdot)$ — центральная гомотетия полугруппы $\mathrm{GE}_n^+(R)$.*

В третьем параграфе рассматривается элементарная эквивалентность полугрупп $G_n(R)$, автоморфизмы которых были найдены в §,2. Параграф посвящен доказательству следующей теоремы:

Теорема 19 (теорема 3.2). *Полугруппы $G_n(R)$, $G_m(S)$ ($n, m \geqslant 3$, $1/2 \in R$, $1/2 \in S$, кольца R и S линейно упорядочены) элементарно эквивалентны тогда и только тогда, когда $n = m$ и полукольца R_+ и S_+ элементарно эквивалентны.*

В четвертой главе диссертации рассматриваются элементарные свойства категорий модулей над кольцом, колец эндоморфизмов свободных модулей бесконечного ранга над кольцами и групп автоморфизмов свободных модулей бесконечного ранга над кольцами, а также колец эндоморфизмов абелевых p-групп. Выясняется, что элементарная эквивалентность таких структур равносильна эквивалентности базисных структур, по которым они строятся, в логике второго порядка (или какой-то ее части). Таким образом, требуются строгие определения логики второго порядка (языках и теориях второго порядка, их моделях, формулах, выполнимости), которые приводятся в первом параграфе.

Второй параграф посвящен элементарным свойствам и элементарной эквивалентности категорий модулей над кольцом.

В первом пункте второго параграфа приводятся некоторые дополнительные сведения о категории mod-R.

Во втором пункте показано, что в категории mod-R понятие прообразующего объекта определимо без параметров, т. е. существует формула в языке первого порядка теории категорий с одной свободной объектной переменной, истинная в категории mod-R для прообразующих модулей этой категории, и только для них.

В пункте 2.3 показано, что для данного прообразующего модуля P на полугруппе $Mor(P, P)$ можно ввести операции сложения и умножения так, чтобы эта полугруппа превратилась в кольцо, изоморфное кольцу $\mathrm{End}_R(P)$.

В пункте 2.4 рассматривается случай конечных колец и доказывается теорема о том, что *категории mod-R и mod-S, где R — конечное кольцо, элементарно эквивалентны тогда и только тогда, когда они Морита-эквивалентны.*

В пункте 2.5 мы формулируем, как распространить результаты С. Шелаха из работы [6] об интерпретации теории множеств в категории на случай категории mod-R.

В пункте 2.6 результаты п. 2.5 используются для того, чтобы в категории mod-R для некоторых фиксированных модулей X и Y выделить элементарными средствами множество линейно независимых проекторов из X на Y.

В пункте 2.7 описывается структура $\langle Cn, ring\rangle$, состоящая из класса **Cn** всех кардинальных чисел, который состоит из множеств мощности $\varkappa$ для каждого $\varkappa \in \mathbf{Cn}$, и кольца $ring$ с отношениями суммы и произведения, а также логика второго порядка такой структуры (мы обозначаем ее через $L_2(\langle Cn, ring\rangle)$), позволяющая в формулах использовать произвольные предикатные символы вида

$$P_{\lambda_1,\dots,\lambda_k}(c_1,\dots,c_k; v_1,\dots,v_n),$$

где $\lambda_1,\dots,\lambda_k$ — фиксированные кардинальные числа, $c_1,\dots c_k$ — переменные для элементов из $\lambda_1,\dots,\lambda_k$ соответственно, $v_1,\dots,v_n$ — переменные для элементов кольца. Кроме того, доказана следующая теорема

Теорема 20 (теорема 4.5). *Пусть даны кольца R и S и существует предложение ψ языка $L_2(\langle Cn, ring\rangle)$, истинное в кольце R и ложное во всех кольцах, ему подобных и не эквивалентных ему в языке $L_2(\langle Cn, ring\rangle)$. Пусть, кроме того, категории mod-R и mod-S элементарно эквивалентны. Тогда существует кольцо S', подобное кольцу S и такое, что структуры $\langle Cn, R\rangle$ и $\langle Cn, S'\rangle$ эквивалентны в логике L_2.*

Пункт 2.8 посвящен доказательству “обратной” теоремы:

Теорема 21 (теорема 4.6). *Для произвольных колец с единицей R и S если структуры $\langle Cn, R\rangle$ и $\langle Cn, S\rangle$ эквивалентны в логике второго порядка L_2, то категории mod-R и mod-S элементарно эквивалентны.*

В результате в п. 2.9 из двух предыдущих теорем выводится теорема, являющаяся аналогом теоремы Мориты для элементарной эквивалентности, и несколько полезных следствий из нее:

Теорема 22 (теорема 4.7). *Пусть даны кольца R и S и существует предложение ψ языка $L_2(\langle Cn, ring\rangle)$, истинное в кольце R и ложное во всех кольцах, ему подобных и не эквивалентных ему в языке $L_2(\langle Cn, ring\rangle)$. Тогда категории mod-$R$ и mod-S элементарно эквивалентны в том и только том случае, когда существует кольцо S', подобное кольцу S и такое, что структуры $\langle Cn, R\rangle$ и $\langle Cn, S'\rangle$ эквивалентны в логике L_2.*

Следствие 1. *Для произвольных тел F_1 и F_2 категории mod-F_1 и mod-F_2 элементарно эквивалентны тогда и только тогда, когда структуры $\langle Cn, F_1\rangle$ и $\langle Cn, F_2\rangle$ эквивалентны в логике второго порядка L_2.*

Следствие 2. *Для произвольных коммутативных колец R_1 и R_2 категории mod-R_1 и mod-R_2 элементарно эквивалентны тогда и только тогда, когда структуры $\langle Cn, R_1\rangle$ и $\langle Cn, R_2\rangle$ эквивалентны в логике второго порядка L_2.*

Следствие 3. *Для произвольных локальных колец R_1 и R_2 категории mod-R_1 и mod-R_2 элементарно эквивалентны тогда и только тогда, когда структуры $\langle Cn, R_1\rangle$ и $\langle Cn, R_2\rangle$ эквивалентны в логике второго порядка L_2.*

Следствие 4. *Для произвольных областей главных идеалов R_1 и R_2 категории mod-R_1 и mod-R_2 элементарно эквивалентны тогда и только тогда, когда структуры $\langle Cn, R_1\rangle$ и $\langle Cn, R_2\rangle$ эквивалентны в логике L_2.*

Следствие 5. *Для произвольных артиновых колец R_1 и R_2 категории mod-R_1 и mod-R_2 элементарно эквивалентны тогда и только тогда, когда существуют кольца S_1 и S_2, подобные кольцам R_1 и R_2 соответственно, такие, что структуры $\langle Cn, S_1\rangle$ и $\langle Cn, S_2\rangle$ эквивалентны в логике L_2.*

Третий параграф посвящен рассмотрению тех же вопросов для колец эндоморфизмов модулей бесконечных рангов.

На протяжении всего параграфа предполагается, что кольцо R и бесконечное кардинальное число $\varkappa$ таковы, что в кольце R существует максимальный идеал, порожденный не более чем $\varkappa$ элементами (например, это всегда так, когда $\varkappa \geqslant |R|$ или кольцо R полупросто или является кольцом главных идеалов).

В первом пункте этого параграфа для каждого свободного модуля V бесконечного ранга над кольцом вводится некоторая специальная категория $C_{M(V)}$ такая, что элементарная эквивалентность колец эндоморфизмов двух свободных модулей бесконечных рангов над кольцами равносильна элементарной эквивалентности соответствующих категорий.

Второй пункт третьего параграфа посвящен изучению элементарной эквивалентности категорий вида $C_{M(V)}$, в результате чего в третьем пункте доказаны следующая основная теорема и следствие из нее:

Теорема 23 (теорема 4.13). *Пусть V_1 и V_2 — свободные модули бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над кольцами R_1 и R_2 соответственно, и существует предложение $\psi \in T_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$, ложное во всех кольцах, подобных кольцу R_1 и имеющих другую теорию $Th_2^{\varkappa_1}$. Тогда кольца $\mathrm{End}_{R_1}(V_1)$ и $\mathrm{End}_{R_2}(V_2)$ элементарно эквивалентны в том и только в том случае, когда существует кольцо S, подобное кольцу R_2 и такое, что теории $Th_2^{\varkappa_1}\langle \varkappa_1, R_1\rangle$ и $Th_2^{\varkappa_2}\langle \varkappa_2, S\rangle$ совпадают.*

Следствие 1. *Для пространств V_1 и V_2 бесконечных размерностей $\varkappa_1$ и $\varkappa_2$ над произвольными телами (областями главных идеалов) F_1 и F_2 кольца $\mathrm{End}_{F_1} V_1$ и $\mathrm{End}_{F_2} V_2$ элементарно эквивалентны тогда и только тогда, когда теории $Th_2^{\varkappa_1}(\langle \varkappa_1, F_1\rangle)$ и $Th_2^{\varkappa_2}(\langle \varkappa_2, F_2\rangle)$ совпадают.*

Следствие 2. *Предположим, что $\varkappa_1$ и $\varkappa_2$ — бесконечные кардинальные числа, R_1 и R_2 — коммутативные (локальные) кольца, и каждый максимальный идеал кольца R_1 порожден не более, чем $\varkappa_1$ элементами кольца. Тогда для свободных модулей V_1 и V_2 рангов $\varkappa_1$ и $\varkappa_2$ над кольцами R_1 и R_2 соответственно, кольца $\mathrm{End}_{R_1} V_1$ и $\mathrm{End}_{R_2} V_2$ элементарно эквивалентны тогда и только тогда, когда теории $Th_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$ и $Th_2^{\varkappa_2}(\langle \varkappa_2, R_2\rangle)$ совпадают.*

Следствие 3. *Предположим, что $\varkappa_1$ и $\varkappa_2$ — бесконечные кардинальные числа, R_1 и R_2 — артиновы кольца, и каждый максимальный идеал кольца R_1 порожден не более,* *чем* $\varkappa_1$ *элементами кольца. Тогда для свободных модулей* V_1 *и* V_2 *рангов* $\varkappa_1$ *и* $\varkappa_2$ *над кольцами* R_1 *и* R_2 *соответственно, кольца* $\mathrm{End}_{R_1} V_1$ *и* $\mathrm{End}_{R_2} V_2$ *элементарно эквивалентны тогда и только тогда, когда существуют кольца* S_1 *и* S_2*, подобные кольцам* R_1 *и* R_2 *соответственно, такие, что теории* $Th_2^{\varkappa_1}(\langle \varkappa_1, S_1\rangle)$ *и* $Th_2^{\varkappa_2}(\langle \varkappa_2, S_2\rangle)$ *совпадают.*

Следствие 4. *Для свободных модулей* V_1 *и* V_2 *бесконечных рангов* $\varkappa_1$ *и* $\varkappa_2$ *над полупростыми кольцами* R_1 *и* R_2 *соответственно, кольца* $\mathrm{End}_{R_1}(V_1)$ *и* $\mathrm{End}_{R_2}(V_2)$ *элементарно эквивалентны тогда и только тогда, когда существуют кольца* S_1 *и* S_2*, подобные кольцам* R_1 *и* R_2 *соответственно, такие, что теории* $Th_2^{\varkappa_1}\langle \varkappa_1, S_1\rangle)$ *и* $Th_2^{\varkappa_2}(\langle \varkappa_2, S_2\rangle)$ *совпадают.*

В четвертом параграфе рассматриваются проективные пространства модулей бесконечных рангов.

В первом пункте этого параграфа описывается язык проективной геометрии над кольцом (т. е. решетки подмодулей модуля на кольцом) и основные понятия, выразимые в этом языке.

Во втором пункте показано, как в проективной геометрии модуля бесконечного ранга интерпретировать кольцо, изоморфное кольцу $\mathrm{End}_R P$ для некоторого прообразующего модуля P.

В третьем пункте четвертого параграфа показано, как в проективной геометрии модуля V интерпретировать кольцо $\mathrm{End}_R V$.

В результате в этом пункте доказана следующая теорема:

Теорема 24 (теорема 4.14). *Для свободных модулей* V_1 *и* V_2 *бесконечных рангов над произвольными кольцами* R_1 *и* R_2 *соответственно из элементарной эквивалентности решеток подмодулей* $P(V_1)$ *и* $P(V_2)$ *следует элементарная эквивалентность колец эндоморфизмов* $\mathrm{End}_{R_1}(V_1)$ *и* $\mathrm{End}_{R_2}(V_2)$.

В четвертом пункте доказывается “обратная” теорема:

Теорема 25 (теорема 4.15). *Предположим, что* V_1 *и* V_2 *— свободные модули бесконечных рангов* $\varkappa_1$ *и* $\varkappa_2$ *над кольцами* R_1 *и* R_2 *соответственно, и каждый подмодуль модуля* V_1 (V_2) *имеет не более* $\varkappa_1$ $(\varkappa_2)$ *порождающих элементов (например, это так, если* $\varkappa_1 \geqslant |R_1|$ *и* $\varkappa_2 \geqslant R_2$ *или если* R_1, R_2 *— полупростые кольца или кольца главных идеалов). Тогда из*

$$\mathrm{End}_{R_1}(V_1) \equiv \mathrm{End}_{R_2}(V_2)$$

следует

$$P(V_1) \equiv P(V_2).$$

В пятом параграфе рассматриваются группы автоморфизмов модулей бесконечных рангов над кольцами.

В пункте 5.1 по аналогии с работой [15] доказывается, что *если кольца* R *и* S *с* $1/2$ *не содержат центральных идемпотентов, отличных от* 0 *и* 1, V *и* V' *— свободные модули бесконечных рангов над кольцами* R *и* S *соответственно, то группы* $\mathrm{Aut}_R(V)$ *и* $\mathrm{Aut}_S(V')$ *изоморфны тогда и только тогда, когда* $\mathrm{End}_R(V) \cong \mathrm{End}_S(V')$.

В пункте 5.2 результаты п. 5.1 распространяются на элементарную эквивалентность. Это делается с помощью перехода к ультрастепеням, аналогично работе [81] К. И. Бейдара и А. В. Михалева. Доказана следующая теорема:

Теорема 26 (теорема 4.17). *Предположим, что кольца R, S содержат $1/2$ и не содержат центральных идемпотентов, отличных от 1 и 0. Тогда группы $\mathrm{Aut}_R(V)$ и $\mathrm{Aut}_S(V')$ элементарно эквивалентны тогда и только тогда, когда кольца $\mathrm{End}_R(V)$ и $\mathrm{End}_S(V')$ элементарно эквивалентны.*

В пункте 5.3 мы считаем, что кардинальное число $\varkappa_1$ таково, что существует максимальный идеал кольца R_1, порожденный не более чем $\varkappa_1$ элементами.

Доказана следующая теорема и следствия из нее:

Теорема 27. (теорема 4.19). *Предположим, что кольца R_1 и R_2 содержат $1/2$ и не содержат центральных идемпотентов, отличных от 1 и 0. Пусть, кроме того, V_1 и V_2 — свободные модули бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над кольцами R_1 и R_2 соответственно, и пусть существует предложение $\psi \in Th_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$, ложное во всех кольцах, подобных кольцу R_1 и имеющих другую теорию $Th_2^{\varkappa_1}$. Тогда группы $\mathrm{Aut}_{R_1}(V_1)$ и $\mathrm{Aut}_{R_2}(V_2)$ элементарно эквивалентны в том и только том случае, когда существует кольцо S, подобное кольцу R_2 и такое, что $Th_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle) = Th_2^{\varkappa_2}(\langle \varkappa_2, S\rangle)$.*

Следствие 1. *Для свободных модулей V_1 и V_2 бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над телами (коммутативными или локальными кольцами, не содержащими центральных идемпотентов, отличных от 1 или 0, областями целостности) F_1 и F_2, содержащими $1/2$, соответственно, группы $\mathrm{Aut}_{F_1}(V_1)$ и $\mathrm{Aut}_{F_2}(V_2)$ элементарно эквивалентны тогда и только тогда, когда $Th_2^{\varkappa_1}(\langle \varkappa_1, F_1\rangle) = Th_2^{\varkappa_2}(\langle \varkappa_2, F_2\rangle)$.*

Следствие 2. *Для свободных модулей V_1 и V_2 бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над артиновыми кольцами R_1 и R_2, не содержащими центральных идемпотентов, отличных от 0 или 1, содержащими $1/2$, соответственно, группы $\mathrm{Aut}_{R_1}(V_1)$ и $\mathrm{Aut}_{R_2}(V_2)$ элементарно эквивалентны тогда и только тогда, когда существуют кольца S_1 и S_2, подобные кольцам R_1 и R_2 соответственно, такие, что $Th_2^{\varkappa_1}(\langle \varkappa_1, S_1\rangle) = Th_2^{\varkappa_2}(\langle \varkappa_2, S_2\rangle)$.*

В шестом параграфе четвертой главы устанавливается связь между свойствами второго порядка абелевой p-группы и свойствами первого порядка ее кольца эндоморфизмов.

В первом пункте приведены все нужные н для дальнейших построений сведения об абелевых группах, взятые в основном из книги [63], а также сформулировано, как распространить результаты С. Шелаха из работы [148] об интерпретации теории множеств в категории на случай кольца эндоморфизмов специальной абелевой p-группы, являющейся прямой суммой циклических групп одного порядка.

В пункте 6.2 еще раз описан групповой язык второго порядка $\mathcal{L}_2$, а также его ограничение $\mathcal{L}_2^{\varkappa}$ некоторым кардинальным числом $\varkappa$, после чего в п. 4.2 вводим *выразимый ранг* r_{exp} абелевой группы A, представленной в виде прямой суммы $D \oplus G$ своих делимой и редуцированных частей как максимум мощностей группы D и базисной подгруппы B группы A. В п. 6.2 мы сформулирована основная теорема этого параграфа:

Если A_1 и A_2 — абелевы p-группы, $\varkappa_1 = r_{exp}(A_1)$, $\varkappa_2 = r_{exp}(A_2)$, то из элементарной эквивалентности колец эндоморфизмов $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$ следует

$$Th_2^{\varkappa_1}(A_1) = Th_2^{\varkappa_2}(A_2).$$

Заметим, что $r_{exp}(A) = |A|$ во всех случаях, кроме случая, когда $|D| < |G|$, базисная подгруппа группы A счетна, а группа G несчетна. В этом случае $r_{exp}(A) = \omega$.

В том же пункте мы доказываем две "обратных импликации" основной теоремы:

1. *Для любых абелевых групп A_1 и A_2 если группы A_1 и A_2 эквивалентны в логике второго порядка L_2, то кольца* $\mathrm{End}\,(A_1)$ *и* $\mathrm{End}\,(A_2)$ *элементарно эквивалентны.*

2. *Если абелевы группы A_1 и A_2 редуцированны и их базисные подгруппы счетны, то из $Th_2^{\omega}(A_1) = Th_2^{\omega}(A_2)$ следует* $\mathrm{End}\,(A_1) \equiv \mathrm{End}\,(A_2)$.

Таким образом, для всех абелевых групп, за исключением случая $A = D \oplus G$, $D \neq 0$, $|D| < |G|$, $|G| > \omega$, базисная подгруппа в A счетна, элементарная эквивалентность колец $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$ равносильна соотношению

$$Th_2^{\varkappa_1}(A_1) = Th_2^{\varkappa_2}(A_2).$$

В конце п. 6.2 доказательство основной теоремы разделено на три случая:

1) группы A_1 и A_2 ограниченны;

2) $A_1 = D_1 \oplus G_1$, $A_2 = D_2 \oplus G_2$, группы D_1 и D_2 делимы, группы G_1 и G_2 ограниченны;

3) группы A_1 и A_2 обладают неограниченными базисными подгруппами.

В следующих трех пунктах шестого параграфа эти три случая рассматриваются по отдельности. В последнем пункте шестого параграфе окончательно доказана основная теорему.

Основные результаты диссертации, выносимые на защиту

1. Доказано, что любой автоморфизм группы Шевалле ранга, большего одного, над локальным кольцом с обратимой двойкой (в случае системы корней G_2 — с обратимой тройкой) стандартен, т. е. является композицией диаграммного, кольцевого, внутреннего и центрального автоморфизмов. Таким образом, решена проблема описания автоморфизмов групп Шевалле над локальными кольцами с обратимой двойкой, что дает возможность с помощью методов локализации описать автоморфизмы групп Шевалле над произвольными кольцами с обратимой двойкой (теорема 1.1).

2. Доказано, что любой автоморфизм группы Шевалле ранга, большего двух, типов A_l, D_l, E_l, над локальным кольцом с необратимой двойкой стандартен, что открывает описание автоморфизмов и изоморфизмов групп Шевалле над коммутативными кольцами с необратимой двойкой (теоремы 1.3, 1.2, 1.1).

3. Доказано, что две (элементарные) группы Шевалле над бесконечными полями характеристики, не равной двум, элементарно эквивалентны тогда и только тогда, когда их системы корней и решетки весов совпадают, а поля элементарно эквивалентны. После этого показано, что (элементарные) группы Шевалле над локальными кольцами с обратимой двойкой (в случае системы корней G_2 еще и с обратимой тройкой) ранга, большего одного, элементарно эквивалентны тогда и только тогда, когда их системы корней и решетки весов совпадают, а кольца элементарно эквивалентны (теоремы 2.1 и 2.2).

4. Описаны все автоморфизмы полугрупп неотрицательных обратимых матриц размера, большего двух, над линейно упорядоченными кольцами с обратимой двойкой, доказано, что на специальной (достаточно большой) подполугруппе такие автоморфизмы

стандартны, т. е. являются композицией внутреннего, полукольцевого и центрального автоморфизмов (теорема 3.1).

5. Доказано, что полугруппы неотрицательных обратимых матриц размера, большего двух, над линейно упорядоченными кольцами с обратимой двойкой, элементарно эквивалентны тогда и только тогда, когда их размеры совпадают, а полукольца неотрицательных элементов элементарно эквивалентны (теорема 3.2).

6. Доказано, что две категории модулей над кольцами (при некоторых условиях на кольца) элементарно эквивалентны тогда и только тогда, когда специальные структуры, построенные на кольцах, эквивалентны в логике второго порядка (теоремы 4.5, 4.6, 4.7 и следствия из нее).

7. Доказано, что кольца эндоморфизмов модулей бесконечных рангов над кольцами (при некоторых условиях на кольца) элементарно эквивалентны тогда и только тогда, когда специальные структуры, построенные на кольцах, эквивалентны в логике второго порядка или ее ограничении на некоторое кардинальное число (теорема 4.13 и следствия из нее).

8. Доказано, что проективные пространства модулей бесконечных рангов над кольцами (с некоторым условием на кольца) элементарно эквивалентны тогда и только тогда, когда кольца эндоморфизмов этих модулей элементарно эквивалентны (теоремы 4.14 и 4.15).

9. Описана связь элементарной эквивалентности групп автоморфизмов модулей бесконечного ранга над кольцами с эквивалентностью в логике второго порядка этих колец (теоремы 4.18, 4.19 и следствия из нее).

10. Описана связь элементарной эквивалентности колец эндоморфизмов абелевых p-групп и эквивалентности в логике второго порядка этих абелевых групп, что продолжает известную теорему Бэра–Капланского об изоморфизмах периодических абелевых групп на случай элементарной эквивалентности (теоремы 4.33, 4.34 и 4.35).

Глава 1

Автоморфизмы групп Шевалле над локальными кольцами

Введение

Пусть G_π — это схема Шевалле-Демазюра, ассоциированная с неприводимой системой корней Φ ранга, большего одного, $G_\pi(\Phi, R)$ — множество точек G_π со значениями в R; $E_\pi(\Phi, R)$ — элементарная подгруппа в $G_\pi(\Phi, R)$, где R — коммутативное кольцо с единицей. В данной главе мы описываем автоморфизмы групп $E_\pi(\Phi, R)$ и $G_\pi(\Phi, R)$ над локальными коммутативными кольцами с $1/2$ для произвольных систем корней, а также над локальными кольцами с необратимой двойкой для систем корней с простыми связями. Подобные результаты для групп Шевалле над полями были доказаны Р. Стейнбергом [158] для конечного случая и Дж. Хамфри [111] для бесконечного. Описанию автоморфизмов групп Шевалле над различными коммутативными кольцами были посвящены работы многих авторов, среди которых стоит отметить работы Бореля–Титса [83], Картера–Ю Чена [86], Ю Чена [88]–[92], Э. Абе [69], А.Клячко [121].

Э. Абе [69] доказал стандартность автоморфизмов для нетеровых колец, что полностью могло бы закрыть вопрос об автоморфизмах групп Шевалле над произвольными коммутативными кольцами (для случая системы корней ранга ≥ 2 и колец с обратимой двойкой), однако в рассмотрении случая присоединенных элементарных групп в работе [69] содержится ошибка, которую не удается устранить методами этой статьи. Именно, в доказательстве леммы 11 используется то, что $\mathrm{ad}\,(x_\alpha)^2 = 0$ для всех длинных корней, что неверно в присоединенном представлении. Главной проблемой здесь является случай групп типа E_8, так как во всех остальных случаях группы Шевалле допускают представление, обладающие свойством $\mathrm{ad}\,(x_\alpha)^2 = 0$ для всех длинных корней, а в случае E_8 таких представлений нет.

Для доказательства основной теоремы обобщаются некоторые методы из работы В. М. Петечука [47].

Заметим, что случай A_l был полностью закрыт работами В. Уотерхауза [176], В.М. Петечука [46], Ли Фу-аня и Ли-Дзун-сяна [114], причем даже без условия обратимости двойки в кольце. Статья И.З. Голубчика и А.В. Михалева [15] охватывает случай системы корней C_l, который в этой работе не рассматривается.

Сначала будет показано, что автоморфизмы присоединенных элементарных групп Шевалле (с рассматриваемыми нами условиями и над локальными кольцами) представляются в виде композиции кольцевого автоморфизма и *автоморфизма–сопряжения*, где автоморфизмом–сопряжением мы называем сопряжение элементов группы Шевалле в присоединенном представлении с помощью некоторой матрицы из нормализатора этой группы в $\mathrm{GL}\,(V)$.

Далее, используя этот результат, мы сможем описать (доказать стандартность) автоморфизмы (элементарных) групп Шевалле ранга, большего одного, над произвольными коммутативными локальными кольцами с обратимой двойкой (и с необратимой двойкой для систем корней с простыми связями). Под стандартным автоморфизмом мы здесь будем иметь в виду композицию внутреннего, кольцевого, диаграммного и центрального автоморфизмов.

Для доказательства основной теоремы будут описаны нормализаторы присоединенных элементарных групп Шевалле в присоединенном представлении. Заметим, что нормализатор односвязанной группы Шевалле типа E_6 в 27-мерном представлении описан Вавиловым и Лузгаревым в [12].

Результаты для систем корней A_l, $l \geqslant 2$, D_l, $l \geqslant 4$, E_l, $l = 6, 7, 8$, над локальными кольцами с обратимой двойкой, опубликованы в работах [196] и [204]. Для систем корней F_4 теоремы полностью доказаны в работе [198]. Системы корней B_2 и G_2 рассматривались в работе [195], в ней была доказана промежуточная теорема о том, что любой автоморфизм группы Шевалле рассматриваемого типа (для системы корней B_2 над коммутативным кольцом с обратимой двойкой, для системы корней G_2 — с обратимыми двойкой и тройкой) есть композиция кольцевого автоморфизма и автоморфизма–сопряжения.

В работе [205] полностью описаны автоморфизмы групп Шевалле типов B_l, $l \geqslant 2$, над локальными кольцами с обратимой двойкой.

В работе [206] доказана стандартность автоморфизмов групп Шевалле в случае систем корней A_l, $l \geqslant 2$, D_l, $l \geqslant 4$, E_l, $l = 6, 7, 8$, над локальными кольцами с необратимой двойкой.

Окончательные результаты для системы корней G_2 (кольцо по-прежнему содержит $1/2$ и $1/3$) опубликованы в работе [**?**]. В этой работе рассматриваются не автоморфизмы одной группы Шевалле, а изоморфизмы между двумя группами Шевалле. Показано, что такая задача абсолютно аналогична задаче об автоморфизмах, нужно поменять только несколько объектов, поэтому можно считать, что все теоремы доказаны и для изоморфизмов групп Шевалле рассматриваемых типов.

1.1 Определения и формулировки основных теорем

Мы фиксируем систему корней Φ ранга, большего одного. Подробные сведения о системах корней и их свойствах можно найти в книгах [64], [8]. То, как выглядят корни в системах разных типов, мы будем выписывать непосредственно в тех параграфах, где будем вести подсчеты для них. Предположим теперь, что у нас имеется полупростая комплексная алгебра Ли $\mathcal{L}$ типа Φ с картановской подалгеброй $\mathcal{H}$ (подробную информацию о полупростых алгебрах Ли можно найти в книге [64]).

Можно выбрать базис $\{h_1, \dots, h_l\}$ в $\mathcal{H}$ и для каждого $\alpha \in \Phi$ элементы $x_\alpha \in \mathcal{L}_\alpha$ так, что $\{h_i; x_\alpha\}$ образуют базис в $\mathcal{L}$ и для любых двух элементов этого базиса их коммутатор является целочисленной линейной комбинацией элементов того же базиса.

Введем элементарные группы Шевалле (см., например, [56]).

Пусть $\mathcal{L}$ — полупростая алгебра Ли (над $\mathbb{C}$) с системой корней Φ, $\pi : \mathcal{L} \to gl(V)$ — ее конечномерное точное представление (размерности n). Если $\mathcal{H}$ — картановская подалгебра алгебры $\mathcal{L}$, то функционал $\lambda \in \mathcal{H}^*$ называется *весом* данного представления, если существует ненулевой вектор $v \in V$ (который называется *весовым вектором*) такой, что для любых $h \in \mathcal{H}$ $\pi(h)v = \lambda(h)v$.

В пространстве V существует базис из весовых векторов такой, что все операторы $\pi(x_\alpha)^k/k!$ для $k \in \mathbb{N}$ записываются целочисленными (нильпотентными) матрицами. Этот базис называется *базисом Шевалле*. Целочисленная матрица также может рассматриваться как матрица над произвольным коммутативным кольцом с единицей. Пусть R — такое кольцо. Рассмотрим матрицы размера $n \times n$ над R, матрицы $\pi(x_\alpha)^k/k!$ при $\alpha \in \Phi$, $k \in \mathbb{N}$ вложим в $M_n(R)$.

Теперь рассмотрим автоморфизмы свободного модуля R^n вида

$$\exp(tx_\alpha) = x_\alpha(t) = 1 + t\pi(x_\alpha) + t^2\pi(x_\alpha)^2/2 + \dots + t^k\pi(x_\alpha)^k/k! + \dots$$

Так как все матрицы $\pi(x_\alpha)$ нильпотентны, этот ряд конечен. Автоморфизмы $x_\alpha(t)$ называются *элементарными корневыми элементами*. Подгруппа в $\mathrm{Aut}\,(R^n)$, порожденная всеми автоморфизмами $x_\alpha(t)$, $\alpha \in \Phi$, $t \in R$, называется *элементарной группой Шевалле* (обозначение: $E_\pi(\Phi, R)$).

Действие элементов $x_\alpha(t)$ на базисе Шевалле описано в работах [85], [173].

Все веса данного представления (по сложению) порождают решетку (свободную абелеву группу, в которой любой $\mathbb{Z}$-базис также является $\mathbb{C}$-базисом в $\mathcal{H}^*$), называемую *решеткой весов* Λ_π.

Элементарные группы Шевалле определяются даже не представлением соответствующей алгебры Ли, а просто ее *решеткой весов*. Именно, с точностью до абстрактного изоморфизма элементарная группа Шевалле полностью определяется системой корней Φ, коммутативным кольцом R с единицей и решеткой весов Λ_π.

Среди всех решеток выделим решетку, соответствующую присоединенному представлению: она порождается всеми корнями (*решетка корней* Λ_{ad}). Соответствующая элементарная группа Шевалле называется *присоединенной*.

Введем теперь группы Шевалле (см. [56], [93], [3], [85], [96], [171], [173], а также дальнейшие ссылки в этих работах).

Рассмотрим полупростые алгебраические группы над алгебраически замкнутыми полями. Это в точности элементарные группы Шевалле $E_\pi(\Phi, K)$ (см. [56], § 5).

Все эти группы можно определить в группе $\mathrm{SL}_n(K)$ как множество общих нулей полиномов от матричных коэффициентов a_{ij} с целочисленными коэффициентами (например, в случае системы корней C_l и универсального представления имеем $n = 2l$ и полиномы, соответствующие условию $(a_{ij})Q(a_{ji}) - Q = 0$). Ясно, что умножение и взятие обратного элемента также описываются полиномами с целыми коэффициентами. Таким образом, эти полиномы можно рассматривать как полиномы над произвольным коммутативным кольцом с единицей. Пусть некоторая элементарная группа Шевалле E над $\mathbb{C}$ определена в $\mathrm{SL}_n(\mathbb{C})$ полиномами $p_1(a_{ij}),\dots,p_m(a_{ij})$. Для коммутативного кольца R с единицей рассмотрим группу

$$G(R)=\{(a_{ij})\in \mathrm{SL}_n(R)\mid \widetilde{p}_1(a_{ij})=0,\dots,\widetilde{p}_m(a_{ij})=0\},$$

где $\widetilde{p}_1(\dots),\dots\widetilde{p}_m(\dots)$ — полиномы, имеющие те же коэффициенты, что и $p_1(\dots),\dots,p_m(\dots)$, но рассматриваемые над R.

Эта группа называется *группой Шевалле* $G_\pi(\Phi,R)$ типа Φ над кольцом R, и для любого алгебраически замкнутого поля K она совпадает с элементарной группой Шевалле.

Подгруппа диагональных (в стандартном базисе из весовых векторов) матриц в группе Шевалле $G_\pi(\Phi,R)$ называется *стандартным максимальным тором* группы $G_\pi(\Phi,R)$ и обозначается через $T_\pi(\Phi,R)$. Эта группа изоморфна группе $\mathrm{Hom}\,(\Lambda_\pi,R^*)$.

Обозначим через $h(\chi)$ элементы тора $T_\pi(\Phi,R)$, соответствующие гомоморфизму $\chi\in \mathrm{Hom}\,(\Lambda_\pi,R^*)$.

В частности, $h_\alpha(u)=h(\chi_{\alpha,u})$ ($u\in R^*$, $\alpha\in\Phi$), где

$$\chi_{\alpha,u}:\lambda\mapsto u^{\langle\lambda,\alpha\rangle}\quad(\lambda\in\Lambda_\pi).$$

Заметим, что условие

$$G_\pi(\Phi,R)=E_\pi(\Phi,R)$$

не выполняется даже в случае полей, не являющихся алгебраически замкнутыми. Покажем различие между группами Шевалле и их элементарными подгруппами в случае, когда кольцо R полулокально. В этом случае $G_\pi(\Phi,R)=E_\pi(\Phi,R)T_\pi(\Phi,R)$ (см., например, [70]), а элементы $h(\chi)$ связаны с элементарными порождающими формулой

$$h(\chi)x_\beta(\xi)h(\chi)^{-1}=x_\beta(\chi(\beta)\xi). \tag{1.1}$$

В случае полулокальных колец из формулы (1.1) видно, что

$$[G(\Phi,R),G(\Phi,R)]\subseteq E(\Phi,R).$$

Если кольцо R содержит $1/2$, либо все корни имеют одинаковую длину $l\geqslant 2$, то легко показать, что

$$[G(\Phi,R),G(\Phi,R)]=[E(\Phi,R),E(\Phi,R)]=E(\Phi,R).$$

Определим четыре типа автоморфизмов группы Шевалле $G_\pi(\Phi,R)$, мы назовем их *стандартными.*

Центральные автоморфизмы. Пусть $C_G(R)$ — центр группы $G_\pi(\Phi,R)$, $\tau:G_\pi(\Phi,R)\to C_G(R)$ — гомоморфизм групп. Тогда отображение $x\mapsto\tau(x)x$ из $G_\pi(\Phi,R)$ на себя является автоморфизмом группы $G_\pi(\Phi,R)$, который обозначается буквой τ и называется *центральным автоморфизмом* группы $G_\pi(\Phi,R)$.

Кольцевые автоморфизмы. Пусть $\rho:R\to R$ — автоморфизм кольца R. Отображение $(x_{i,j})\mapsto(\rho(x_{i,j}))$ из $G_\pi(\Phi,R)$ на себя является автоморфизмом группы $G_\pi(\Phi,R)$, который обозначается той же буквой ρ и называется *кольцевым автоморфизмом* группы $G_\pi(\Phi,R)$. Заметим, что для всех $\alpha\in\Phi$ и $t\in R$ элемент $x_\alpha(t)$ отображается в $x_\alpha(\rho(t))$.

Внутренние автоморфизмы. Пусть S — некоторое кольцо, содержащее R, g — элемент группы $G_\pi(\Phi, S)$, нормализующий подгруппу $G_\pi(\Phi, R)$. Тогда отображение $x \mapsto gxg^{-1}$ является автоморфизмом группы $G_\pi(\Phi, R)$, который обозначается i_g и называется *внутренним автоморфизмом*, *индуцированным элементом* $g \in G_\pi(\Phi, S)$. Если $g \in G_\pi(\Phi, R)$, то назовем i_g *строго внутренним* автоморфизмом.

Диаграммные (графовые) автоморфизмы. Пусть δ — автоморфизм системы корней Φ такой, что $\delta\Delta = \Delta$. Тогда существует единственный автоморфизм группы $G_\pi(\Phi, R)$ (будем обозначать его той же буквой δ) такой, что для любого $\alpha \in \Phi$ и $t \in R$ элемент $x_\alpha(t)$ переходит в $x_{\delta(\alpha)}(\varepsilon(\alpha)t)$, где $\varepsilon(\alpha) = \pm 1$ для всех $\alpha \in \Phi$ и $\varepsilon(\alpha) = 1$ для всех $\alpha \in \Delta$.

Аналогично мы можем определить четыре типа автоморфизмов элементарной подгруппы $E(R)$. Автоморфизм σ группы $G_\pi(\Phi, R)$ (или $E_\pi(\Phi, R)$) называется *стандартным*, если он является композицией автоморфизмов введенных четырех типов.

Наряду со стандартными автоморфизмами мы будем использовать следующий "временный" тип автоморфизмов элементарной присоединенной группы Шевалле:

Автоморфизмы-сопряжения. Пусть V — пространство представления группы $E_{\mathrm{ad}}(\Phi, R)$, $C \in \mathrm{GL}(V)$ — матрица, оставляющая группу Шевалле на месте:

$$CE_{\mathrm{ad}}(\Phi, R)C^{-1} = E_{\mathrm{ad}}(\Phi, R).$$

Тогда отображение $x \mapsto CxC^{-1}$ из $E_\pi(\Phi, R)$ на себя является автоморфизмом группы Шевалле, который обозначается i и называется *автоморфизмом-сопряжением* группы $E(R)$, *индуцированным элементом* C группы $\mathrm{GL}(V)$.

Главная наша цель — доказательство следующей основной теоремы:

Теорема 1.1. *Пусть $G = G_\pi(\Phi, R)$ $(E_\pi(\Phi, R))$ — (элементарная) группа Шевалле со следующими условиями:*

1) *если рассматривается система корней A_l, D_l или E_l, $l \geqslant 3$, то R — произвольное локальное коммутативное кольцо*;

2) *если рассматривается система корней A_2, F_4, B_l, C_l, $l \geqslant 2$, то R — произвольное локальное коммутативное кольцо с $1/2$*;

3) *если рассматривается система корней G_2, то R — произвольное локальное коммутативное кольцо с $1/2$ и $1/3$.*

Тогда любой автоморфизм группы G стандартен. Если группа Шевалле при этом присоединенная, то внутренний автоморфизм в композиции является строго внутренним.

Основной результат будет непосредственно следовать из следующих двух следующих теорем, доказательству которых посвящены все оставшиеся параграфы этой главы. Случай колец с необратимой двойкой будет рассмотрен полностью отдельно, так как для него приходится строить другое доказательство.

Теорема 1.2. *Каждый автоморфизм элементарной присоединенной группы Шевалле рассматриваемого выше типа является композицией кольцевого, диаграммного автоморфизмов и автоморфизма–сопряжения.*

Теорема 1.3. *Каждый автоморфизм–сопряжение элементарной присоединенной группы Шевалле рассматриваемого типа является композицией строго внутреннего (сопряжения с помощью элемента соответствующей группы Шевалле) и диаграммного автоморфизмов.*

Пример группы Шевалле типа A_2 над локальными кольцами с необратимой двойкой, для которых существуют нестандартные автоморфизмы, можно найти в работе [48].

1.2 Замена изначального автоморфизма на специальный изоморфизм

Несколько ближайших параграфов посвящены доказательству теоремы 1.2 для локальных колец с обратимой двойкой.

В этом параграфе система корней произвольная. В этом параграфе мы используем некоторые соображения из работы [47].

Пусть J — максимальный идеал (радикал) кольца R, k — поле вычетов R/J. Тогда $E_J = E_{\mathrm{ad}}(\Phi, R, J)$ — наибольшая нормальная собственная подгруппа в $E_{\mathrm{ad}}(\Phi, R)$ (см. [70]). Таким образом, подгруппа E_J инвариантна относительно действия автоморфизма φ.

Значит, автоморфизм
$$\varphi : E_{\mathrm{ad}}(\Phi, R) \to E_{\mathrm{ad}}(\Phi, R)$$
индуцирует автоморфизм
$$\overline{\varphi} : E_{\mathrm{ad}}(\Phi, R)/E_J = E_{\mathrm{ad}}(\Phi, k) \to E_{\mathrm{ad}}(\Phi, k).$$
Группа $E_{\mathrm{ad}}(\Phi, k)$ является присоединенной группой Шевалле над полем, значит, автоморфизм $\overline{\varphi}$ стандартен (см. [56]), т. е. имеет вид
$$\overline{\varphi} = i_{\overline{g}}\overline{\rho}, \quad \overline{g} \in N(E_{\mathrm{ad}}(\Phi, k)),$$
где $\overline{\rho}$ — кольцевой автоморфизм, индуцированный некоторым автоморфизмом поля k.

Ясно, что существует матрица $g \in \mathrm{GL}_n(R)$ такая, что ее образ при факторизации R по J совпадает с $\overline{g}$. Мы не можем быть уверены, что $g \in N(E_{\mathrm{ad}}(\Phi, R))$.

Рассмотрим отображение $\varphi' = i_{g^{-1}}\varphi$. Это изоморфизм группы $E_{\mathrm{ad}}(\Phi, R) \subset \mathrm{GL}_n(R)$ на некоторую подгруппу $\mathrm{GL}_n(R)$, с тем свойством, что ее образ при факторизации R по J совпадает с автоморфизмом $\overline{\rho}$.

Проведенные рассуждения доказывают

Предложение 1.1. *Любая матрица $A \in E_{\mathrm{ad}}(\Phi, R)$ с элементами из подкольца R' в R, порожденного единицей, отображается при изоморфизме φ' в матрицу из множества*
$$A \cdot \mathrm{GL}_n(R, J) = \{B \in \mathrm{GL}_n(R) \mid A - B \in M_n(J)\}.$$

Пусть $a \in E_{\mathrm{ad}}(\Phi, R)$, $a^2 = 1$. Тогда элемент $e = \frac{1}{2}(1+a)$ является идемпотентом в кольце $M_n(R)$. Этот идемпотент e определяет разложение свободного R-модуля $V \cong R^n$:

$$V = eV \oplus (1-e)V = V_0 \oplus V_1$$

(модули V_0, V_1 свободны, так как любой проективный модуль над локальным кольцом свободен [128]). Пусть $\overline{V} = \overline{V}_0 \oplus \overline{V}_1$ — разложение k-модуля (линейного пространства) $\overline{V} \cong k^n$ по отношению к $\overline{a}$, и $\overline{e} = \frac{1}{2}(1+\overline{a})$.

Тогда имеем

Предложение 1.2. *Модули (подпространства) $\overline{V}_0$, $\overline{V}_1$ являются образами модулей V_0, V_1 при факторизации по J.*

Доказательство. Обозначим образы модулей V_0, V_1 при факторизации по J через $\widetilde{V}_0$, $\widetilde{V}_1$, соответственно. Так как $V_0 = \{x \in V | ex = x\}$, $V_1 = \{x \in V | ex = 0\}$, то $\overline{e}(\overline{x}) = \frac{1}{2}(1+\overline{a})(\overline{x}) = \frac{1}{2}(1+\overline{a}(\overline{x})) = \frac{1}{2}(1+\overline{a(x)}) = \overline{e(x)}$. Тогда $\widetilde{V}_0 \subseteq \overline{V}_0$, $\widetilde{V}_1 \subseteq \overline{V}_1$.

Пусть $x = x_0 + x_1$, $x_0 \in V_0$, $x_1 \in V_1$. Тогда $\overline{e}(\overline{x}) = \overline{e}(\overline{x}_0) + \overline{e}(\overline{x}_1) = \overline{x}_0$. Если $\overline{x} \in \widetilde{V}_0$, то $\overline{x} = \overline{x}_0$. □

Пусть $b = \varphi'(a)$. Тогда $b^2 = 1$ и b сравнимо с a по модулю J.

Предложение 1.3. *Предположим, что $a, b \in E_\pi(\Phi, R)$, $a^2 = b^2 = 1$, a — матрица с элементами из подкольца $R' \subset R$, порожденного единицей, b и a сравнимы по модулю J, $V = V_0 \oplus V_1$ — разложение V по отношению к a, $V = V_0' \oplus V_1'$ — разложение V по отношению к b. Тогда* $\dim V_0' = \dim V_0$, $\dim V_1' = \dim V_1$.

Доказательство. Мы имеем R-базис модуля V $\{e_1, \dots, e_n\}$ такой, что $\{e_1, \dots, e_k\} \subset V_0$, $\{e_{k+1}, \dots, e_n\} \subset V_1$. Ясно, что

$$\overline{a}\overline{e}_i = \overline{ae_i} = \overline{(\sum_{j=1}^{n} a_{ij}e_j)} = \sum_{j=1}^{n} \overline{a}_{ij}\overline{e}_j.$$

Пусть $\overline{V} = \overline{V}_0 \oplus \overline{V}_1$, $\overline{V} = \overline{V}'_0 \oplus \overline{V}'_1$ — разложения k-модуля (пространства) $\overline{V}$ по отношению к $\overline{a}$ и $\overline{b}$. Ясно, что $\overline{V}_0 = \overline{V}'_0$, $\overline{V}_1 = \overline{V}'_1$. Таким образом, по предложению 1.2 образы модулей V_0 и V_0', V_1 и V_1' при факторизации J совпадают. Возьмем такие $\{f_1, \dots, f_k\} \subset V_0'$, $\{f_{k+1}, \dots, f_n\} \subset V_1'$, что $\overline{f}_i = \overline{e}_i$, $i = 1, \dots, n$. Так как матрица перехода от $\{e_1, \dots, e_n\}$ к $\{f_1, \dots, f_n\}$ обратима (сравнима с единичной матрицей по модулю J), то $\{f_1, \dots, f_n\}$ — это R-базис в V. Ясно, что $\{f_1, \dots, f_k\}$ является R-базисом в V_0', $\{v_{k+1}, \dots, v_n\}$ — R-базисом в V_1'. □

1.3 Образы элементов w_{α_i}

Рассмотрим некоторую фиксированную присоединенную группу Шевалле $E = E_{\mathrm{ad}}(\Phi, R)$ с системой корней ранга, большего двух, ее присоединенное представление в группе $\mathrm{GL}_n(R)$

($n = l+2m$, где m — число положительных корней системы Φ), с базисом из весовых векторов $v_1 = x_{\alpha_1}, v_{-1} = x_{-\alpha_1}, \dots, v_n = x_{\alpha_n}, v_{-n} = x_{-\alpha_n}, V_1 = h_1, \dots, V_l = h_l$, соответствующему базису Шевалле системы Φ.

У нас также есть изоморфизм φ', описанный в параграфе 2.

Рассмотрим матрицы $h_{\alpha_1}(-1), \dots, h_{\alpha_l}(-1)$ в нашем базисе. Они имеют вид

$$h_{\alpha_i}(-1) = \operatorname{diag}[\pm 1, \dots, \pm 1, \underbrace{1, \dots, 1}_{l}],$$

на $(2j-1)$-м и $(2j)$-м местах стоят -1 тогда и только тогда, когда $\langle \alpha_i, \alpha_j \rangle = -1$. Как мы видим, для всех i $h_{\alpha_i}(-1)^2 = 1$.

В соответствии с предложением 1.3 мы знаем, что любая матрица $h_i = \varphi'(h_{\alpha_i}(-1))$ в некотором базисе диагональна с ± 1 на диагонали, и число 1 и -1 совпадает с их числом для матрицы $h_{\alpha_i}(-1)$. Так как все матрицы h_i коммутируют, то существует базис, в котором все h_i имеют тот же вид, что и $h_{\alpha_i}(-1)$ в изначальном базисе из весовых векторов. Предположим, что мы перешли к этому базису с помощью матрицы g_1. Ясно, что $g_1 \in \operatorname{GL}_n(R, J)$. Рассмотрим отображение $\varphi_1 = i_{g_1}^{-1}\varphi'$. Оно также является изоморфизмом группы E на некоторую подгруппу $\operatorname{GL}_n(R)$ таким, что его образ при факторизации R по J есть $\overline{\rho}$, и $\varphi_1(h_{\alpha_i}(-1)) = h_{\alpha_i}(-1)$ для всех $i = 1, \dots, l$.

Вместо изоморфизма φ' будем теперь рассматривать изоморфизм φ_1.

Любой элемент $w_i = w_{\alpha_i}(1)$ переводит сопряжением h_i друг в друга, поэтому его образ должен иметь блочно-мономиальный вид. В частности, этот образ можно записать как блочно-диагональную матрицу, где первый блок имеет размер $2m \times 2m$, а второй — $l \times l$.

Рассмотрим первый вектор базиса, к которому мы перешли в результате последней замены. Обозначим его через e. Группа Вейля W транзитивно действует на множестве корней одной длины, поэтому для каждого корня α_i той же длины, что и первый корень, существует такой $w^{(\alpha_i)} \in W$, что $w^{(\alpha_i)}\alpha_1 = \alpha_i$. Аналогично, все корни второй длины также сопряжены под действием группы Вейля. Пусть α_k — первый корень длины, отличной от длины корня α_1, и пусть f — k-ый вектор базиса, к которому мы перешли в результате последней замены. Если α_j — корень, сопряженный с α_k, то обозначим через $w_{(\alpha_j)}$ элемент группы Вейля такой, что $w_{(\alpha_j)}\alpha_k = \alpha_j$. Рассмотрим теперь базис $e_1, \dots, e_{2m}, e_{2m+1}, \dots, e_{2m+l}$, где $e_1 = e$, $e_k = f$, при $1 < i \leq 2m$ либо $e_i = \varphi_1(w^{(\alpha_i)})e$, либо $e_i = \varphi_1(w_{(\alpha_i)})f$ в зависимости от того, какую длину имеет корень α_k; при $2m < i \leq 2m+1$ оставим e_i прежним. Понятно, что матрица для такой замены базиса сравнима с единицей по модулю радикала. Отсюда следует, что полученный набор векторов снова будет базисом.

Очевидно, что матрица для $\varphi_1(w_i)$ $(i = 1, \dots, l)$ в части базиса $\{e_1, \dots, e_{2m}\}$ совпадает с матрицей для w_i в исходном базисе из весовых векторов. Так как $h_i(-1)$ — это квадраты w_i, то их образы также не изменяются в новом базисе.

Кроме того, мы знаем, что матрица $\varphi_1(w_i)$ блочно-диагональна относительно разделения базиса на первые $2m$ и последние l элементов. Таким образом, последнюю часть базиса, состоящую из l элементов, мы можем заменять независимо.

Будем обозначать сами элементы и их образы на этой части базиса через $\widetilde{w}_i$ и $\widetilde{w'_i}$, соответственно. Это матрицы размера $l \times l$. Значит, последнюю часть базиса, состоящую из l элементов, можно менять независимо.

Обозначим матрицы w_i и $\varphi_1(w_i)$ на этой части базиса через $\widetilde{w}_i$ и $\widetilde{\varphi_1(w_i)}$, соответственно. Все эти матрицы являются инволюциями, при этом у них ровно одна -1 в диагональной форме. Пусть $\widetilde{V} = \widetilde{V}_0^i \oplus \widetilde{V}_1^i$ — разложение матрицы $\widetilde{\varphi_1(w_i)}$.

Лемма 1.1. *Матрицы $\widetilde{\varphi_1(w_i)}$ и $\widetilde{\varphi_1(w_j)}$, при $i \neq j$, коммутируют тогда и только тогда, когда $\widetilde{V}_1^i \subseteq \widetilde{V}_0^j$ и $\widetilde{V}_1^j \subseteq \widetilde{V}_0^i$.*

Доказательство. Если $\widetilde{\varphi_1(w_i)}$ и $\widetilde{\varphi_1(w_j)}$ коммутируют, то (свободный одномерный) подмодуль $\widetilde{V}_1^i$ является собственным для $\widetilde{\varphi_1(w_j)}$ и (свободный одномерный) подмодуль $\widetilde{V}_1^j$ является собственным для $\widetilde{\varphi_1(w_i)}$. Таким образом, либо $\widetilde{V}_1^i \subset \widetilde{V}_1^j$, либо $\widetilde{V}_1^i \subset \widetilde{V}_0^j$. Если $\widetilde{V}_1^i \subset \widetilde{V}_1^j$, то $\widetilde{V}_1^i = \widetilde{V}_1^j$. Так как модуль V_0^i инвариантен для $\widetilde{\varphi}_1(w_j)$, то $\widetilde{V}_0^i \subset \widetilde{V}_0^j$, следовательно, $\widetilde{V}_0^i = \widetilde{V}_0^j$, и, значит, $\widetilde{\varphi}_1(w_i) = \widetilde{\varphi}_1(w_j)$ и мы приходим к противоречию. Следовательно, $\widetilde{V}_1^i \subset \widetilde{V}_0^j$, и, аналогично, $\widetilde{V}_1^j \subset \widetilde{V}_0^i$. □

Теперь по отдельности рассмотрим случаи различных систем корней.

1.3.1 Системы корней A_l, D_l, E_l

Лемма 1.2. *Для любой рассматриваемой системы корней Φ существует такой базис в $\widetilde{V}$, что матрица $\widetilde{\varphi}_1(w_1)$ в этом базисе имеет тот же вид, что и w_1, т.е. равна*

$$\begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & E_{l-2} \end{pmatrix}.$$

Доказательство. Так как $\widetilde{w}_1$ — инволюция, а $\widetilde{V}_1^1$ имеет размерность 1, то существует базис $\{e_1, e_2, \ldots, e_l\}$, в котором $\widetilde{\varphi}_1(w_1)$ имеет вид $\operatorname{diag}[-1, 1, \ldots, 1]$. В базисе $\{e_1, e_2 - 1/2e_1, e_3, \ldots, e_l\}$ матрица $\widetilde{\varphi}_1(w_1)$ имеет искомую форму. □

Лемма 1.3. *Для системы корней A_2 существует такой базис, что $\widetilde{\varphi}_1(w_1)$ и $\widetilde{\varphi}_1(w_2)$ в этом базисе имеют тот же вид, что w_1 и w_2, т.е. равны*

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

соответственно.

Доказательство. По лемме 1.2 можно найти базис в $\widetilde{V}$ такой, что матрица $\widetilde{\varphi}_1(w_1)$ в этом базисе имеет тот же вид, что и w_1. Пусть матрица $\widetilde{\varphi}_1(w_2)$ в этом базисе — это

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Произведем замену базису с помощью матрицы

$$\begin{pmatrix} c & (1-c)/2 \\ 0 & 1 \end{pmatrix}$$

(эта замена корректна, так как $c \equiv 1 \mod J$). При этой замене базиса матрица $\widetilde{\varphi}_1(w_1)$ не меняет вид, а матрица $\widetilde{\varphi}_1(w_2)$ становится

$$\begin{pmatrix} a' & b' \\ 1 & d' \end{pmatrix}.$$

Так как эта матрица имеет порядок два, то $a'+d'=0$, ${a'}^2+b'=1$. Значит, $d'=-a'$. Теперь используем условие

$$\left(\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a' & b' \\ 1 & -a' \end{pmatrix}\right)^2 = \begin{pmatrix} a' & b' \\ 1 & -a' \end{pmatrix}\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Это условие дает (вторая строка, первый столбец) $1-2a'=-1$, следовательно, $a'=1$. Из ${a'}^2+b'=1$ следует $b'=0$. □

Лемма 1.4. *Для любой системы корней $\Phi \neq A_2$ можно выбрать базис в $\widetilde{V}$ такой, что матрицы $\widetilde{\varphi}_1(w_1)$ и $\widetilde{\varphi}_1(w_2)$ в этом базисе имеют тот же вид, что и $\widetilde{w}_1$ и $\widetilde{w}_2$, соответственно.*

Доказательство. Пересечение модулей $\widetilde{V}_0^1$ и $\widetilde{V}_0^2$ — это свободный модуль размерности $\geq l-3$. Таким образом, мы можем считать, что $\widetilde{\varphi}_1(w_1)$ и $\widetilde{\varphi}_1(w_2)$ имеют вид $\begin{pmatrix} * & 0 \\ 0 & E_{l-3} \end{pmatrix}$. Кроме того, по лемме 1.2 мы можем считать, что $\widetilde{\varphi}_1(w_1)$ имеет тот же вид, что и $\widetilde{w}_1$. Мы теперь можем рассматривать не весь модуль $\widetilde{V}$, а его ограничение на первые три базисных вектора. Пусть

$$\widetilde{\varphi}_1(w_1) = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}.$$

Проведем замену базису с помощью матрицы

$$\begin{pmatrix} b_1 & (1-b_1)/2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

при этом не поменяется $\widetilde{\varphi}_1(w_1)$, но $\widetilde{\varphi}_1(w_2)$ перейдет в

$$\widetilde{\varphi}_1(w_1) = \begin{pmatrix} a_1' & a_2' & a_3' \\ 1 & b_2' & b_3' \\ c_1' & c_2' & c_3' \end{pmatrix}.$$

Теперь используем те же условия, что и в предыдущей лемме. Первое — это $\widetilde{\varphi}_1(w_2)^2 - 1 = 0$ (соотн. 1), второе — $(\widetilde{\varphi}_1(w_1)\widetilde{\varphi}_1(w_2))^2 - \widetilde{\varphi}_1(w_2)\widetilde{\varphi}_1(w_1) = 0$ (соотн. 2). Если вычесть соотношение 1 из соотношения 2, мы получим (строка 2, столбец 1) $a_1' = 1$, (строка 2, столбец 2) $a_2' = 0$, то из соотн. 1, строка 1, столбец 3, мы получим $a_3'(1 + c_3') = 0$. Так как $c_3' \equiv 1 \mod J$, то $a_3' = 0$. То же соотношение (строка 2, столбец 3) дает $b_3'(b_2' + c_3') = 0$, а так как $b_3' \in R^*$, то $c_3' = -b_2'$.

Снова взяв замену базиса, но с помощью матрицы

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -c_1' & 1 \end{pmatrix},$$

мы не меняем $\widetilde{\varphi}_1(w_1)$, а $\widetilde{\varphi}_1(w_2)$ переходит в

$$\widetilde{\varphi}_1(w_1) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & b_2'' & b_3'' \\ 0 & c_2'' & -b_2'' \end{pmatrix}.$$

Тогда прямо из соотношения 1 получаем $b_2'' = -1$, $c_2'' = 0$, и последняя замена базиса с помощью матрицы $\operatorname{diag}[1, 1, b_3'']$ дает нам требуемую форму для $\widetilde{\varphi}_1(w_1)$ и $\widetilde{\varphi}_1(w_2)$. □

Лемма 1.5. *Для системы корней D_4 существует такой базис, что $\widetilde{\varphi}_1(w_1)$, $\widetilde{\varphi}_1(w_2)$, $\widetilde{\varphi}_1(w_3)$ и $\widetilde{\varphi}_1(w_4)$ в этом базисе имеют тот же вид, что и $\widetilde{w}_1$, $\widetilde{w}_2$, $\widetilde{w}_3$, и $\widetilde{w}_4$, т.е. равны*

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

соответственно.

Доказательство. Сначала возьмем такой базис, что $\widetilde{\varphi}_1(w_1)$, $\widetilde{\varphi}_1(w_3)$, $\widetilde{\varphi}_1(w_4)$ имеют тот же вид, что и изначальные $\widetilde{w}_1$, $\widetilde{w}_3$, $\widetilde{w}_4$. Мы это можем сделать, так как w_1, w_3, w_4 являются коммутирующими инволюциями, существует базис, в котором $\widetilde{\varphi}_1(w_1)$, $\widetilde{\varphi}_1(w_3)$, $\widetilde{\varphi}_1(w_4)$ имеют вид $\operatorname{diag}[-1, 1, 1, 1]$, $\operatorname{diag}[1, 1, -1, 1]$, $\operatorname{diag}[1, 1, 1, -1]$, соответственно. Далее, сопрягая их матрицей

$$\begin{pmatrix} 1 & -1/2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -1/2 & 1 & 0 \\ 0 & -1/2 & 0 & 1 \end{pmatrix},$$

мы переходим к требуемому базису. Теперь посмотрим на $\widetilde{\varphi}_1(w_2)$. Имеем следующие соотношения: $\widetilde{w}_2^2 = 1$ (соотн. 1), $(\widetilde{w}_1\widetilde{w}_2)^2 = \widetilde{w}_2\widetilde{w}_1$ (соотн. 2), $(\widetilde{w}_3\widetilde{w}_2)^2 = \widetilde{w}_2\widetilde{w}_3$ (соотн. 3), $(\widetilde{w}_4\widetilde{w}_2)^2 = \widetilde{w}_2\widetilde{w}_4$ (соотн. 4). Пусть

$$\widetilde{\varphi}_1(w_2) = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{pmatrix}.$$

Рассмотрим теперь замену базиса с помощью матрицы

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & \frac{d_1}{2d_1-b_1} & 0 & \frac{b_1}{b_1-2d_1} \end{pmatrix},$$

мы тогда не поменяем $\widetilde{\varphi}_1(w_1)$, $\widetilde{\varphi}_1(w_3)$, $\widetilde{\varphi}_1(w_4)$, а $\widetilde{\varphi}_1(w_2)$ становится

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ 0 & d_2 & d_3 & d_4 \end{pmatrix}$$

(для краткости мы не ставим штрихи).

Теперь из 4-ой строки разности соотношений 1 и 2 следует $d_2 = d_3 = 0$, $d_4 = 1$.

Строка 2, столбец 4 разности соотношений 1 и 4 дает $b_4(b_4 - 1) = 0$. Так как $b_4 \in R^*$, получаем $b_4 = 1$.

Теперь, взяв замену базиса с помощью матрицы

$$\begin{pmatrix} \frac{b_3}{b_3-2a_3} & \frac{a_3}{2a_3-b_3} & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

мы не меняем $\widetilde{\varphi}_1(w_1)$, $\widetilde{\varphi}_1(w_3)$, $\widetilde{\varphi}_1(w_4)$, а $\widetilde{\varphi}_1(w_2)$ становится

$$\begin{pmatrix} a_1 & a_2 & 0 & a_4 \\ b_1 & b_2 & b_3 & 1 \\ c_1 & c_2 & c_3 & c_4 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

(мы снова не ставим штрихи для краткости).

Теперь строка 1, столбец 3 соотношения 1 дает $a_2 b_3 = 0 \Rightarrow a_2 = 0$, строка 1, столбец 1 соотношения 1 дает $a_1^2 = 1 \Rightarrow a_1 = 1$, строка 1, столбец 4 дает $2a_4 = 0 \Rightarrow a_4 = 0$. Строка 2, столбец 4 разности соотношений 1 и 2 дает $b_1 = 1$, строка 3, столбец 4 дает $c_4 = c_1$. Строка 2, столбец 3 соотношения 1 дает $c_3 = -b_2$.

Наконец, взяв замену базиса с помощью матрицы

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & \frac{1-b_3}{2} & b_3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

мы не поменяем $\widetilde{\varphi}_1(w_1)$, $\widetilde{\varphi}_1(w_3)$, $\widetilde{\varphi}_1(w_4)$, а $\widetilde{\varphi}_1(w_2)$ станет равной

$$\begin{pmatrix} 1 & 0 & 0 & a_4' \\ 1 & b_2' & 1 & 1 \\ c_1' & c_2' & -b_2' & c_1' \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

После этого строка 2, столбец 3 соотношения 3 дает $b_2' = -1$, и тогда соотн. 1 дает $c_1' = c_2' = 0$. □

Лемма 1.6. *Предположим, что у нас есть некоторая система корней Φ и элементы $\widetilde{\varphi}_1(w_{i_1}) = \widetilde{w}_{i_1}, \dots, \widetilde{\varphi}_1(w_{i_k}) = \widetilde{w}_{i_k}$, и также $\widetilde{\varphi}_1(w_{i_{k+1}})$, где выполнен один и следующих случаев:*

а) $\Phi = A_l$, $l \geq 3$, $i_1 = 1$, $i_2 = 2, \dots, i_k = k$, $i_{k+1} = k+1$, $k+1 < l$;

б) $\Phi = D_l$, $l > 4$, $i_1 = l$, $i_2 = l-1$, $i_3 = l-2$, $\dots$, $i_k = l-k+1$, $i_{k+1} = l-k$, $4 < k < l$;

в) $\Phi = E_6, E_7$ или E_8, $i_1 = 1$, $i_2 = 2, \dots, i_k = k$, $i_{k+1} = k+1$, $4 \leq k < l-1$.

Тогда можно выбрать такой базис в $\widetilde{V}$, что $\widetilde{\varphi}_1(w_{i_1}) = \widetilde{w}_{i_1}, \dots, \widetilde{\varphi}_1(w_{i_{k+1}}) = \widetilde{w}_{i_{k+1}}$.

Доказательство. Во всех случаях $\widetilde{\varphi}_1(w_{i_{k+1}})$ коммутирует со всеми $\widetilde{\varphi}_1(w_{i_1}) = \widetilde{w}_{i_1}, \dots, \widetilde{\varphi}_1(w_{i_{k-1}}) = \widetilde{w}_{i_{k-1}}$, следовательно (см. лемму 1.1), для всех $j = i_1, \dots, i_{k-1}$ $V_1^j \subset V_0^{i_{k+1}}$. Так как $V_1^{i_1} \oplus \dots \oplus V_1^{i_{k-1}} = \langle e_{i_1}, \dots, e_{i_{k-1}} \rangle$, мы получаем, что $\widetilde{\varphi}_1(w_{i_{k+1}})$ тождественна на первых $k-1$ базисных векторах. Как и в лемме 1.4, мы получаем, что $\widetilde{\varphi}_1(w_{i_{k+1}})$ тождественна на последних $l-k-2$ базисных векторах. Таким образом, мы можем ограничить $\widetilde{\varphi}_1(w_{i_{k+1}})$ на часть базиса $\{e_k, e_{k+1}, e_{k+2}\}$ (без потери общности). Теперь доказательство становится полностью аналогичным доказательству леммы 1.4. □

Предложение 1.4. *Для любой из систем корней $\Phi = A_l, D_l, E_l$ мы можем выбрать базис в $\widetilde{V}$ такой, что матрицы $\widetilde{\varphi}_1(w_1), \dots, \widetilde{\varphi}_1(w_l)$ в этом базисе имеют вид $\widetilde{w}_1, \dots, \widetilde{w}_l$, соответственно.*

Доказательство. В случае системы корней A_2 мы можем использовать лемму 1.3. Если $\Phi = A_l$, $l \geq 3$, то применим лемму 1.4, после этого лемму 1.6 $l-3$ раз, и, наконец, те же рассуждения, что и в лемме 1.3, для элемента $\widetilde{\varphi}_1(w_l)$.

Если $\Phi = D_l$, то применим лемму 1.5 для корней $\alpha_{l-3}, \dots, \alpha_l$, затем лемму 1.6 $l-5$ раз к корням $\alpha_{l-4}, \dots, \alpha_2$, и, наконец, те же аргументы, что и в лемме 1.3, для элемента $\widetilde{\varphi}_1(w_1)$.

Если $\Phi = E_l$, то применим лемму 1.5 к корням $\alpha_2, \dots, \alpha_5$, затем лемму 1.6 к корням $\alpha_6, \dots, \alpha_{l-1}$, и, наконец, те же рассуждения, что и в лемме 1.3, к элементам $\widetilde{\varphi}_1(w_1)$ и $\widetilde{\varphi}_1(w_l)$. □

1.3.2 Системы корней B_l

Матрица $\widetilde{w}_1$ единична на позициях $3, \dots, l$, на позициях $1, 2$ она имеет вид

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

Матрицы $\widetilde{w}_i$, $i = 2, \dots, l-1$, единичны на позициях $1, \dots, i-2, i+2, \dots, l$, а на позициях $i-1, i, i+1$ имеют вид

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

Матрица $\widetilde{w}_l$ единична на позициях $1, \ldots, l-2$, а на позициях $l-1, l$ имеет вид

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

Пусть $\widetilde{V} = \widetilde{V}_0^i \oplus \widetilde{V}_1^i$ — разложение матрицы $\widetilde{w}_i'$.

Лемма 1.7. *Для системы корней B_l существует такой базис в $\widetilde{V}$, что матрица $\widetilde{w_1'}$ в этом базисе имеет тот же вид, что и $\widetilde{w}_1$, т.е. равна*

$$\begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & E_{l-2} \end{pmatrix}.$$

Доказательство. Так как $\widetilde{w}_1$ — инволюция, а $\widetilde{V}_1^1$ имеет размерность 1, то существует базис $\{e_1, e_2, \ldots, e_l\}$, в котором $\widetilde{w_1'}$ имеет вид $\mathrm{diag}\,[-1, 1, \ldots, 1]$. В базисе $\{e_1, e_2 - 1/2e_1, e_3, \ldots, e_l\}$ матрица $\widetilde{w_1'}$ имеет искомую форму. $\square$

Лемма 1.8. *Для системы корней B_l, $l > 2$ если $\widetilde{w}_1 = \widetilde{w_1'}$, $\ldots$, $\widetilde{w}_{i-1} = \widetilde{w_{i-1}'}$, $i < l$, то можно выбрать базис в $\widetilde{V}$ такой, что в нем $\widetilde{w}_1 = \widetilde{w_1'}$, $\ldots$, $\widetilde{w}_{i-1} = \widetilde{w_{i-1}'}$, $\widetilde{w}_i' = \widetilde{w}_i$.*

Доказательство. Пересечение модулей $\widetilde{V}_0^1, \widetilde{V}_0^2, \ldots, \widetilde{V}_0^i$ — это свободный модуль размерности $\geq l-i-1$. Таким образом, мы можем считать, что $\widetilde{w_2'}$ имеет вид $\begin{pmatrix} * & 0 \\ 0 & E_{l-i-1} \end{pmatrix}$. Кроме того, так как $\widetilde{w}_i'$ коммутирует с $\widetilde{w}_1, \ldots, \widetilde{w}_{i-1}$ и является инволюцией, то матрица $\widetilde{w}_i'$ единична на первых $i-2$ векторах. Мы теперь можем рассматривать не весь модуль $\widetilde{V}$, а его ограничение на три базисных вектора с номерами $i-1, i, i+1$. Пусть

$$\widetilde{w_i'} = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}.$$

Проведем замену базису с помощью матрицы

$$\begin{pmatrix} E_{i-2} & 0 & 0 & 0 & 0 \\ 0 & b_1 & (1-b_1)/2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & E_{l-i-1} \end{pmatrix},$$

при этом не поменяются $\widetilde{w}_1, \ldots, \widetilde{w}_{i-1}$, но $\widetilde{w_2'}$ перейдет в

$$\widetilde{\varphi}_1(w_1) = \begin{pmatrix} a_1' & a_2' & a_3' \\ 1 & b_2' & b_3' \\ c_1' & c_2' & c_3' \end{pmatrix}.$$

Теперь используем следующие условия $\widetilde{w}_i'^2 = E$ (соотн. 1) и $\widetilde{w}_{i-1}\widetilde{w}_i'\widetilde{w}_{i-1} = \widetilde{w}_i'\widetilde{w}_{i-1}\widetilde{w}_i'$ (соотн. 2). Если сложить эти два соотношения, то вторая строка полученной суммы сразу дает $a_1 = 1$, $a_2 = a_3 = 0$.

Позиция $(2,3)$ первого соотношения дает $b_3(b_2+c_3)=0$, и так как b_2 обратим, то $c_3=-b_2$.

Дополнительно проведем замену базиса с помощью матрицы

$$\begin{pmatrix} E_{i-2} & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1+b_2 & b_3 & 0 \\ 0 & 0 & 0 & 0 & E_{l-i-1} \end{pmatrix},$$

при этом не поменяются $\widetilde{w}_1,\ldots,\widetilde{w}_{i-1}$, но $\widetilde{w'_2}$ перейдет в

$$\widetilde{\varphi}_1(w_1)=\begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 1 \\ x & y & 1 \end{pmatrix}.$$

Теперь из первого соотношения сразу $x=y=0$, что и требовалось. □

Лемма 1.9. *Для системы корней B_l если $\widetilde{w}_1=\widetilde{w'_1}$, ..., $\widetilde{w}_{l-1}=\widetilde{w'_{l-1}}$, то можно выбрать базис в $\widetilde{V}$ такой, что в нем $\widetilde{w}_1=\widetilde{w'_1}$, ..., $\widetilde{w}_{l-1}=\widetilde{w'_{l-1}}$, $\widetilde{w'_l}=\widetilde{w}_l$.*

Доказательство. Так как $\widetilde{w'_l}$ коммутирует со всеми $\widetilde{w}_1$, ..., $\widetilde{w}_{l-2}$ и имеет порядок два, то на элементах базиса $e_1,\ldots,e_{l-2}$ она единична. Таким образом, остается рассмотреть только последние два элемента базиса, рассматриваемую матрицу можно считать матрицей 2×2 вида

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Из того, что она имеет порядок два, сразу получаем $c(a+d)=0$, а так как $c\equiv 2 \mod J$, то $a+d=0$.

После замены базиса с помощью матрицы

$$\begin{pmatrix} E_{l-2} & 0 & 0 \\ 0 & 1 & (1-a)/c \\ 0 & 0 & 1+2(1-a)/c \end{pmatrix}$$

элементы $\widetilde{w}_1$, ..., $\widetilde{w}_{l-1}$ не поменяются, а $\widetilde{w'_l}$ примет вид

$$\begin{pmatrix} E_{l-2} & 0 & 0 \\ 0 & 1 & b \\ 0 & c & -1 \end{pmatrix}.$$

Снова из того, что матрица имеет порядок два, а c обратим, получаем $b=0$.

Осталось воспользоваться соотношением

$$\widetilde{w}_{l-1}\widetilde{w'_l}\widetilde{w}_{l-1}\widetilde{w'_l}=\widetilde{w'_l}\widetilde{w}_{l-1}\widetilde{w'_l}\widetilde{w}_{l-1},$$

которое сразу же дает $c=2$. □

Рассмотрение системы корней F_4 фактически является “склейкой” случаев, уже рассмотренных выше, поэтому мы не приводим доказательство для него в этой работе.

Таким образом, осталось рассмотреть систему корней G_2.

1.3.3 Система корней G_2

Лемма 1.10. *Для системы корней G_2 существует такой базис, что $\widetilde{\varphi_1(w_1)}$ и $\widetilde{\varphi_1(w_2)}$ в этом базисе имеют тот же вид, что и $\widetilde{w_1}$ и $\widetilde{w_2}$, с одним, может быть, отличием в матрице $\widetilde{w_2}$, а именно, равны*

$$\begin{pmatrix} -1 & 3 \\ 0 & 1 \end{pmatrix} \text{ и } \begin{pmatrix} 1 & 0 \\ 1+u & -1 \end{pmatrix}, \quad 3u = 0.$$

Доказательство. Так как $\widetilde{w}_1$ является инволюцией и $\widetilde{V}_1^1$ имеет размерность 1, то существует базис $\{e_1, e_2\}$, где $\widetilde{\varphi_1(w_1)}$ имеет вид $\operatorname{diag}[-1, 1]$. В базисе $\{e_1, e_2 - 3/2e_1\}$ матрица имеет требуемую форму для G_2.

Пусть матрица $\widetilde{\varphi_1(w_2)}$ в этом новом базисе есть

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Сделаем замену базиса с помощью матрицы

$$\begin{pmatrix} 1 & (1-a)/c \\ 0 & 1 + \frac{2(1-a)}{c} \end{pmatrix}$$

(это возможно, так как c сравним с единицей по модулю радикала). При такой замене базиса матрица $\widetilde{\varphi_1(w_1)}$ не изменится, а матрица $\widetilde{\varphi_1(w_2)}$ примет вид

$$\begin{pmatrix} 1 & b' \\ c' & d' \end{pmatrix}.$$

Так как эта матрица является инволюцией, то $c'(1+d') = 0$, $1 + b'c' = 1$. Таким образом, $d' = -1$, $b' = 0$.

Кроме того,

$$\left(\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c' & -1 \end{pmatrix} \right)^3 = \left(\begin{pmatrix} 1 & 0 \\ c' & -1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \right)^3,$$

откуда $3c'(3c'-1)(c'-1) = 0$. Так как $c' \equiv 1 \mod J$, $3c'-1 \equiv 2 \mod J$, то $3(c'-1) = 3u = 0$.

Понятно, что если тройка обратима в кольце S, то $u = 0$. Обозначим полученный образ матрицы w_2 за w_2'. □

Мы не рассматриваем здесь систему корней C_l, однако доказательство для нее совершенно аналогично доказательству для системы корней B_l.

Таким образом, Для всех существующих систем корней мы теперь можем перейти от рассматриваемого изоморфизма φ_1 к изоморфизму φ_2, обладающему теми свойствами, что и φ_1, и при этом такому, что $\varphi_2(w_i) = w_i$ для всех $i = 1, \ldots, l$.

Будем считать, что нам дан изоморфизм φ_2, обладающий этими свойствами.

Теперь мы хотим с помощью еще одной замены базиса перейти к новому изоморфизму φ_3, обладающему всеми свойствами изоморфизма φ_2, но еще и такому, что все элементы $x_{\alpha_i}(1)$, $\alpha_i \in \Phi$, переходят сами в себя.

1.4 Образы элементов $x_{\alpha_i}(1)$ и диагональных матриц

В этом параграфе нас будут интересовать образы матриц $x_{\alpha_i}(t)$. Мы будем считать попрежнему, что в кольце R обратима двойка, а если рассматривается система корней G_2, то также обратима и тройка.

Будем рассматривать типы систем корней по отдельности (отдельно системы корней A_l, D_l, E_l, отдельно B_l, отдельно F_4, отдельно G_2. Систему корней C_l мы исключим из рассмотрения, так как доказательство для нее очень похоже на доказательство для системы корней B_l.

1.4.1 Системы корней A_l, D_l, E_l

Пусть $\varphi_2(x_{\alpha_1}(1)) = x_1$. Так как x_1 коммутирует со всеми $h_{\alpha_i}(-1)$, $i = 1, 3, \dots, l$, то получаем, что x_1 можно разделить на блоки следующего вида: блоки 2×2 соответствуют части базиса $\{v_i, v_{-i}\}$, где $i > 1$ и $\langle \alpha_i, \alpha_1 \rangle \neq 0$; блоки 4×4 соответствуют частям базиса $\{v_i, v_{-i}, v_j, v_{-j}\}$, где $i > 1$, $\alpha_i = \alpha_j \pm \alpha_1$; кроме того, у нас есть часть $\{v_1, v_{-1}, V_1, \dots, V_l\}$.

Для $h_{\alpha_2}(-1)$ мы знаем, что $h_{\alpha_2}(-1) x_1 h_{\alpha_2}(-1) = x_1^{-1}$. Тогда на блоках 2×2, описанных выше, если x_1 имеет вид

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

то эта матрица в квадрате есть 1, поэтому $a^2 + bc = d^2 + bc = 1$, $b(a + d) = c(a + d) = 0$. Так как $a + d \equiv 2 \mod J$, имеем $a + d \in R^*$, т. е. $b = c = 0$. Так как $a^2 = d^2 = 1$ и $a, d \equiv 1 \mod J$, то $a = d = 1$. Значит, на блоках 2×2 матрица x_1 всегда единична (т.е. совпадает с $x_{\alpha_1}(1)$ на этих блоках), значит, мы можем даже не рассматривать базисные элементы такого вида.

Теперь используем соотношения $w_i x_1 w_i^{-1} = x_1$ для $i \geq 3$.

Для начала, все блоки 4×4 имеют одинаковый вид, так как любые два таких блока сопряжены относительно действия w_i, $i \geq 3$.

Соотношения $w_i x_1 w_i^{-1} = x_1$ для $i \geq 3$ для остальных элементов базиса вместе с соотношением $h_2 x_1 h_2^{-1} = x_1^{-1}$ утверждают, что наша матрица на подмножестве базиса

$$\{v_1, v_{-1}, V_1, V_2, V_3, \dots, V_l\}$$

имеет вид

$$\begin{pmatrix} * & * & * & * & 0 & \dots & 0 \\ * & * & * & * & 0 & \dots & 0 \\ * & * & * & * & 0 & \dots & 0 \\ * & * & * & * & 0 & \dots & 0 \\ * & * & * & * & 1 & \dots & 0 \\ \multicolumn{7}{c}{\dots\dots\dots\dots\dots\dots} \\ * & * & * & * & 0 & \dots & 1 \end{pmatrix},$$

а все строки $5, \dots, l$ выражаются через четвертую строку. Благодаря углу нулей для данной матрицы мы можем ограничить соотношения на ее левую верхнюю подматрицу размера 4×4.

Предположим, что на этой части базиса матрица x_1 имеет вид
$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{pmatrix},$$
а на части базиса $v_2, v_{-2}, v_{1+2}, v_{-1-2}$ — вид
$$\begin{pmatrix} e_1 & e_2 & e_3 & e_4 \\ f_1 & f_2 & f_3 & f_4 \\ g_1 & g_2 & g_3 & g_4 \\ h_1 & h_2 & h_3 & h_4 \end{pmatrix}.$$

Мы будем рассматривать часть базиса $\{v_1, v_{-1}, v_2, v_{-2}, v_{1+2}, v_{-1-2}, V_1, V_2\}$.

Возьмем замену базиса с помощью блочно-диагональной матрицы, которая имеет вид
$$\begin{pmatrix} 1 & -\frac{b_4}{a_4} \\ -\frac{b_4}{a_4} & 1 \end{pmatrix}$$

на каждом блоке $\{v_i, v_{-i}\}$ (это возможно, так как $b_4 \in J$), и тождественна на блоке $\{V_1, \dots, V_l\}$. Тогда элементы w_i, h_i не изменятся, а у x_1 теперь будет $b_4 = 0$. Значит, мы можем считать, что изоморфизм φ_2 таков, что $\varphi_2(x_{\alpha_1}(1))$ имеет $b_4 = 0$.

Теперь проделаем еще одну замену базиса с помощью диагональной матрицы, имеющей вид $\frac{1}{a_4} \cdot E$ на части $\{v_1, v_{-1}, \dots, v_m, v_{-m}\}$, и единичной на части $\{V_1, \dots, V_l\}$. Аналогично, элементы w_i, h_i не меняются, а a_4 становится равным 1.

Значит, мы можем считать, что $\varphi_2(x_{\alpha_1}(1))$ имеет $b_4 = 0$ и $a_4 = 1$.

На рассматриваемой части базиса
$$w_1 = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad w_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}.$$
Так как
$$x_{\alpha_1}(1) = \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 & -2 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$
получаем
$$x_1 = \varphi_2(x_1(1)) = \begin{pmatrix} a_1 & a_2 & 0 & 0 & 0 & 0 & a_3 & 1 \\ b_1 & b_2 & 0 & 0 & 0 & 0 & b_3 & 0 \\ 0 & 0 & e_1 & e_2 & e_3 & e_4 & 0 & 0 \\ 0 & 0 & f_1 & f_2 & f_3 & f_4 & 0 & 0 \\ 0 & 0 & g_1 & g_2 & g_3 & g_4 & 0 & 0 \\ 0 & 0 & h_1 & h_2 & h_3 & h_4 & 0 & 0 \\ c_1 & c_2 & 0 & 0 & 0 & 0 & c_3 & c_4 \\ d_1 & d_2 & 0 & 0 & 0 & 0 & d_3 & d_4 \end{pmatrix},$$

где $a_1, b_2, e_1, f_2, f_4, g_3, h_4, c_2, c_3, d_4 \equiv 1 \mod J$, $a_2, g_1 \equiv -1 \mod J$, $a_3 \equiv -2 \mod J$, остальные коэффициенты лежат в J.

Тогда

$$x_{1+2} = \varphi_2(x_{\alpha_1+\alpha_2}(1)) = w_2 x_1 w_2^{-1} = \begin{pmatrix} g_3 & g_4 & g_2 & g_1 & 0 & 0 & 0 & 0 \\ h_3 & h_4 & h_2 & h_1 & 0 & 0 & 0 & 0 \\ f_3 & f_4 & f_2 & f_1 & 0 & 0 & 0 & 0 \\ e_3 & e_4 & e_2 & e_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a_1 & a_2 & 1+a_3 & -1 \\ 0 & 0 & 0 & 0 & b_1 & b_2 & b_3 & 0 \\ 0 & 0 & 0 & 0 & c_1 & c_2 & c_3+c_4 & -c_4 \\ 0 & 0 & 0 & 0 & c_1-d_1 & c_2-d_2 & c_3-d_3+c_4-d_4 & -c_4+d_4 \end{pmatrix}$$

и

$$x_2 = \varphi_2(x_{\alpha_2}(1)) = w_1 x_{1+2} w_1^{-1} = \begin{pmatrix} h_4 & h_3 & 0 & 0 & h_2 & h_1 & 0 & 0 \\ g_4 & g_3 & 0 & 0 & g_2 & g_1 & 0 & 0 \\ 0 & 0 & a_1 & a_2 & 0 & 0 & -1-a_3 & a_3 \\ 0 & 0 & b_1 & b_2 & 0 & 0 & -b_3 & b_3 \\ f_4 & f_3 & 0 & 0 & f_2 & f_1 & 0 & 0 \\ e_4 & e_3 & 0 & 0 & e_2 & e_1 & 0 & 0 \\ 0 & 0 & -d_1 & -d_2 & 0 & 0 & d_3+d_4 & -d_3 \\ 0 & 0 & c_1-d_1 & c_2-d_2 & 0 & 0 & -c_3+d_3-c_4+d_4 & c_3-d_3 \end{pmatrix}.$$

Будем использовать следующие соотношения:

$$\mathrm{Con1} := (x_1 x_{1+2} - x_{1+2} x_1 = 0), \quad \mathrm{Con2} := (h_2 x_1 h_2 x_1 - 1 = 0).$$

Позиция (3,8) соотн. Con1 дает $f_3 = -e_3$, позиция (2,8) соотн. Con1 дает $h_3 = -b_3 c_4$, позиция (2,8) соотн. Con2 дает $b_1 = b_3 c_4$, таким образом, $h_3 = -b_1$. Из позиции (1,1) соотн. Con1 получаем $b_1(a_2 + g_4) = 0$, откуда $b_1 = 0$, так как $a_2 + g_4 \in R^*$.

Введем еще два соотношения:

$$\mathrm{Con3} := (x_1 w_1 x_1 w1^{-1} - w_1 h_2 x_1 h_2 = 0), \quad \mathrm{Con4} := (x_2 x_1 - x_{1+2} x_1 x_2 = 0).$$

Обозначим $y_1 = a_1 - 1, y_2 = a_2 + 1, y_3 = a_3 + 2, y_4 = b_2 - 1, y_5 = b_3, y_6 = c_1, y_7 = c_2 - 1, y_8 = c_3 - 1, y_9 = c_4, y_{10} = d_1, y_{11} = d_2, y_{12} = d_3, y_{13} = d_4 - 1, y_{14} = e_1 - 1, y_{15} = e_2, y_{16} = e_3$, $y_{17} = e_4, y_{18} = f_1, y_{19} = f_2 - 1, y_{20} = f_4 - 1, y_{21} = g_1 + 1, y_{22} = g_2, y_{23} = g_3 - 1, y_{24} = g_4, y_{25} = h_1, y_{26} = h_2, y_{27} = h_4 - 1$. Все эти элементы y_i лежат в J. Из соотношений 1–4 получаем следующие 27 уравнений (линейных относительно y_i):

$y_{23}(-a_2) + y_{24}(a_1 - b_2) + y_{27} a_2 = 0,$ Con1, поз. (1,2),
$y_{18}(-g_1) + y_{22}(a_1 - e_1) + y_{26}(a_2) = 0,$ Con1, поз. (1,3),
$y_1 g_1 + y_{15}(-g_2) + y_{19}(-g_1) + y_{25} a_2 = 0,$ Con1, поз. (1,4),
$y_6(a_3 + 1) + y_{10}(-1) + y_{16}(g_1 + g_2) = 0,$ Con1, поз. (1,5),
$y_3(c_2) + y_7(-1) + y_{11}(-1) + y_{20} + y_{21}(-f_4) + y_{22}(-e_4) = 0,$ Con1, поз. (1,6),

$$
\begin{array}{ll}
y_3(c_3+c_4-g_3)+y_8(-1)+y_9(-1)+y_{13}(-1)+y_{14}(-1)+y_{23}2+ & \\
\quad +y_{24}(-b_3)=0, & \text{Con1, поз. (1,7)},\\
y_9(-a_3-1)+y_{13}+y_{23}(-1)=0, & \text{Con1, поз. (1,8)},\\
y_5c_2+y_{25}(-f_4)+y_{26}(-e_4)=0, & \text{Con1, поз. (2,6)},\\
y_{16}a_2+y_{17}(b_2-f_2)+y_{18}(-f_4)=0, & \text{Con1, поз. (3,6)},\\
y_5(e_4-f_4)+y_{16}(1+2a_3)=0, & \text{Con1, поз. (3,7)},\\
y_{15}(-f_1f_4-f_2e_3)+y_{16}(a_1-a_2+a_1h_2+f_1f_2-f_2^2)+y_{22}(e_3a_2-f_4b_2)=0, & \text{Con4, поз. (3,5)},\\
y_{10}(-d_3-d_4)+y_{11}(a_1+1)+y_{12}c_1=0, & \text{Con3, поз. (8,2)},\\
y_1(-1)+y_2(a_1+b_2)+y_3(-c_2)+y_4(-1)+y_72+y_{11}(-1)=0, & \text{Con2, поз. (1,2)},\\
y_5(-c_2g_3)+y_{16}(b_2-b_2h_4)+y_{17}a_2=0, & \text{Con4, поз. (6,2)},\\
y_{14}g_3+y_{16}(e_4-e_3)+y_{21}+y_{23}=0, & \text{Con3, поз. (3,3)},\\
y_4(b_2+1)+y_5(-c_2)=0, & \text{Con2, поз. (2,2)},\\
y_{14}(e_1+1)+y_{15}f_1+y_{16}(-g_1)+y_{17}(-h_1)=0, & \text{Con2, поз. (3,3)},\\
y_{15}(e_1+f_2)+y_{16}(-g_2)+y_{17}(-h_2)=0, & \text{Con2, поз. (3,4)},\\
y_6(-g_1a_1)+y_9(c_3+c_4-d_4)(c_1-d_1)+y_{10}(c_3^2+c_3c_4-d_3c_4-e_1)+ & \\
\quad +y_{11}(-f_1)+y_{25}c_2a_1=0, & \text{Con4, поз. (7,3)},\\
y_{16}g_4+y_{18}e_4+y_{19}+y_{20}(f_2-h_4)+y_{27}(-1)=0, & \text{Con2, поз. (4,6)},\\
y_{14}+y_{21}(g_3-e_1)+y_{22}f_1+y_{23}(-1)+y_{24}h_1=0, & \text{Con2, поз. (5,3)},\\
y_{17}(-g_1)+y_{22}(-f_4)+y_{24}(g_3+h_4)=0, & \text{Con2, поз. (5,6)},\\
y_4(-c_2)+y_6(-a_2)+y_8c_2+y_9d_2=0, & \text{Con2, поз. (7,2)},\\
y_6(-1)+y_9(c_3+d_4)=0, & \text{Con2, поз. (7,8)},\\
y_1a_2+y_2+y_4+y_6a_3+y_{10}(-1-a_3)=0, & \text{Con3, поз. (1,2)},\\
y_{19}h_4+y_{20}(-1)+y_{25}(-g_2)+y_{26}(-h_2)+y_{27}=0, & \text{Con3, поз. (6,6)},\\
y_6(-g_3f_2)+y_{15}(-c_1g_4-c_2h_4)+y_{16}(d_2-d_1)+ & \\
\quad +y_{22}(c_4d_2-c_3c_2-c_2c_4)+y_{26}(c_4d_1-c_3c_1-c_4c_1)=0, & \text{Con4, поз. (7,5)}.
\end{array}
$$

Матрица полученной системы линейных уравнений по модулю радикала J имеет вид

$$
\left(\begin{array}{ccccccccccccccccccccccccccc}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&-1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&-1&0\\
-1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&-1&0&0\\
0&0&0&0&0&-1&0&0&0&-1&0&0&0&0&0&-1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&-1&0&0&0&-1&0&0&0&0&0&0&0&0&1&-1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&0&0&1&1&0&0&0&0&0&0&0&0&0&-2&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&-1&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&-1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&-1&0&0&0&0&0&0&0&0&0&0&-3&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&-1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&-1&2&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
-1&2&-1&-1&0&0&2&0&0&0&-1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&2&-1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&-1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&-1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&-1&0&2&0&0&0\\
0&0&0&-1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&-1&0&0&2&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
-1&1&0&1&0&-2&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&-1&0&0&0&0&0&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0
\end{array}\right).
$$

Определитель этой матрицы есть 2^8, то есть это элемент, обратимый в R. Таким образом, данная система имеет единственное решение $y_1 = \dots = y_{27} = 0$. Следовательно, $x_1 = x_{\alpha_1}(1)$ на рассматриваемой части базиса. Так как все корни сопряжены друг другу относительно действия группы W, получаем $x_1 = x_{\alpha_1}(1)$ на всем базисе. Ясно, что $x_2 = x_{\alpha_2}(1)$.

Теперь рассмотрим матрицу $d_t = \varphi_2(h_{\alpha_1}(t))$. Матрица $h_{\alpha_1}(t)$ — это $\operatorname{diag}[t^2, 1/t^2, 1/t, t, t, 1/t, 1, 1]$ на рассматриваемой части базиса.

Лемма 1.11. *Матрица d_t — это $h_{\alpha_1}(s)$ для некоторого $s \in R^*$.*

Доказательство. Для матрицы d_t имеем соотношения $d_t w_3 = w_3 d_t, \ldots, d_t w_l = w_l d_t$.

Пусть $l > 2$ и
$$d_t = \begin{pmatrix} \gamma_{11} & \gamma_{12} & \cdots & \gamma_{1l} \\ \gamma_{21} & \gamma_{22} & \cdots & \gamma_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_{l1} & \gamma_{l2} & \cdots & \gamma_{ll} \end{pmatrix}$$
на $\widetilde{V}$.

Каждое из соотношений $d_t w_i = w_i d_t$, $i > 2$, дает $\gamma_{1i} = \cdots = \gamma_{i-1,i} = \gamma_{i+1,i} = \cdots = \gamma_{li} = 0$. Из соотношения $d_t w_1 d_t w_1^{-1} = 1$ теперь сразу следует $\gamma_{33}^2 = \cdots = \gamma_{ll}^2 = 1 \Rightarrow \gamma_{33} = \cdots = \gamma_{ll} = 1$. Условие $d_t w_l = w_l d_t$ показывает, что $\gamma_{l-1,j}$ линейно выражается через $\gamma_{l,j}$, $j = 1, 2, \ldots$, условие $d_t w_3 = w_3 d_t$ показывает, что $\gamma_{2,j}$ линейно выражается через $\gamma_{l,j}$, $j = 1, 2$.

Благодаря углу нулей мы можем рассматривать соотношения для d_t на части базиса $v_1, v_{-1}, v_2, v_{-2}, v_{1+2}, v_{-1-2}, V_1, V_2$, как мы это делали для x_1.

Так как d_t коммутирует со всеми h_i, мы получаем, что на рассматриваемой части базиса
$$d_t = \begin{pmatrix} k_1 & k_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ k_3 & k_4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & l_1 & l_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & l_3 & l_4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & m_1 & m_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & m_3 & m_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & n_1 & n_2 \\ 0 & 0 & 0 & 0 & 0 & 0 & n_3 & n_4 \end{pmatrix}.$$

Мы знаем, что $x_2 = x_{\alpha_2}(1)$ и $x_2^t = \varphi_2(x_{\alpha_2}(t)) = d_t x_2 d_t^{-1} = d_t x_2 w_1 d_t w_1^{-1}$. Используя эти условия, получаем выражение x_2^t через коэффициенты d_t. Теперь мы можем использовать условие $\mathrm{Con5} := (x_2^t x_2 - x_2 x_2^t = 0)$. Его позиция (1,6) дает $k_1(k_2 + k_3) = 0 \Rightarrow k_2 = -k_3$, позиция (2,1) дает $k_4(l_3 - m_3) = 0 \Rightarrow m_3 = l_3$, поз. (2,5) дает $l_3(l_1 + m_4) = 0 \Rightarrow l_3 = 0$, поз. (5,6) дает $k_2(l_4 + m_1) = 0 \Rightarrow k_2 = 0$. Из $\mathrm{Con6} := (d_t w_1 d_t w_1^{-1} - 1 = 0)$ следует $k_1 k_4 = l_1 m_1 = l_4 m_4 = 1$. Используя соотношение $\mathrm{Con7} := (w_2 d_t w_2^{-1} - d_t w_1 w_2 d_t w_2^{-1} w_1^{-1} = 0)$, получаем $m_2 = l_2 = 0$ (позиции (1,2) и (4,3)) и $l_4 = l_1 k_1$ (поз. (1,1)). Позиция (7,7) соотношения Con6 дает $n_1^2 - (n_1 + n_2)n_3 = 1$, позиция (3,7) соотношения Con5 дает $n_1^2 - (3n_1 + n_2 - 2n_3 - n_4)n_3 = 1$. Таким образом, $n_3 = 0$, $n_1^2 = 1$. После этого мы очевидно получаем $n_1 = n_4 = 1$, $n_2 = 0$. Наконец, позиция (3,4) соотношения Con5 дает $k_1 = 1/l_1^2$. Обозначим $1/l_1$ через s.

Очевидно, что с помощью w_i, $i = 3, \ldots l$, мы можем однозначно определить все остальные диагональные элементы. Именно, если $\langle \alpha_1, \alpha_k \rangle = p$, то $\varphi(h_{\alpha_1}(t)) v_k = s^p \cdot v_k$, $\varphi(h_{\alpha_1}(t)) v_{-k} = s^{-p} \cdot v_{-k}$. Поэтому $\varphi(h_{\alpha_1}(t)) = h_{\alpha_1}(s)$. $\square$

1.4.2 Система корней B_l

Пусть $e_1, \dots, e_l$ — ортонормированный базис пространства $\mathbb{R}^l$. Тогда пронумеруем корни системы B_l следующим образом:

$$\alpha_1 = e_1 - e_2, \alpha_2 = e_2 - e_3, \alpha_{l-1} = e_{l-1} - e_l, \alpha_l = e_l$$

— простые корни;

$$e_i \pm e_j,\ e_i,\ i < j,$$

— остальные положительные корни.

К сожалению, не получается провести доказательство для всех систем B_l, $l \geqslant 2$, одновременно. Приходится отдельно рассматривать случаи $l = 2$, $l = 3$, $l = 4$, $l \geqslant 5$.

Самый простой случай B_2 разбирать не будем, доказательство для него можно найти в работе [195].

Случай B_3

В этом случае имеем следующие корни: $\alpha_1 = e_1 - e_2$, $\alpha_2 = e_2 - e_3$, $\alpha_3 = e_3$, $\alpha_4 = \alpha_1 + \alpha_2 = e_1 - e_3$, $\alpha_5 = \alpha_2 + \alpha_3 = e_2$, $\alpha_6 = \alpha_1 + \alpha_2 + \alpha_3 = e_1$, $\alpha_7 = \alpha_2 + 2\alpha_3 = e_2 + e_3$, $\alpha_8 = \alpha_1 + \alpha_2 + 2\alpha_3 = e_1 + e_3$, $\alpha_9 = \alpha_1 + 2\alpha_2 + 2\alpha_3 = e_1 + e_2$.

Пусть $x_1 = \varphi_2(x_{\alpha_1}(1))$, $x_3 = \varphi_2(x_{\alpha_3}(1))$.

Заметим, что

$$\begin{aligned}
h_{\alpha_1}(-1) = &\ \mathrm{diag}\,[1,1,-1,-1,1,1,-1,-1,-1,-1,-1,-1,-1,-1,-1,-1,1,1,1,1,1],\\
h_{\alpha_2}(-1) = &\ \mathrm{diag}\,[-1,-1,1,1,-1,-1,-1,-1,-1,-1,1,1,1,1,-1,-1,-1,-1,1,1,1].
\end{aligned}$$

Напомним для удобства, что

$$\begin{aligned}
w_1 = &-e_{\alpha_1,-\alpha_1} - e_{-\alpha_1,\alpha_1} + e_{\alpha_2,\alpha_4} + e_{-\alpha_2,-\alpha_4} - e_{\alpha_4,\alpha_2} - e_{-\alpha_4,\alpha_2} + e_{\alpha_3,\alpha_3} + e_{-\alpha_3,-\alpha_3} +\\
&+ e_{\alpha_5,\alpha_6} + e_{-\alpha_5,-\alpha_6} - e_{\alpha_6,\alpha_5} - e_{-\alpha_6,\alpha_5} + e_{\alpha_7,\alpha_8} + e_{-\alpha_7,-\alpha_8} - e_{\alpha_8,\alpha_7} - e_{-\alpha_8,-\alpha_7} +\\
&+ e_{\alpha_9,\alpha_9} + e_{-\alpha_9,-\alpha_9} - e_{h_1,h_1} + e_{h_1,h_2} + e_{h_2,h_2} + e_{h_3,h_3};\\
w_2 = &-e_{\alpha_2,-\alpha_2} - e_{-\alpha_2,\alpha_2} + e_{\alpha_1,\alpha_4} + e_{-\alpha_1,-\alpha_4} - e_{\alpha_4,\alpha_1} - e_{-\alpha_4,\alpha_1} +\\
&+ e_{\alpha_3,\alpha_5} + e_{-\alpha_3,-\alpha_5} - e_{\alpha_5,\alpha_3} - e_{-\alpha_5,\alpha_3} + e_{\alpha_6,\alpha_6} + e_{-\alpha_6,-\alpha_6} + e_{\alpha_7,\alpha_7} + e_{-\alpha_7,-\alpha_7} +\\
&+ e_{\alpha_8,\alpha_9} + e_{-\alpha_8,-\alpha_9} - e_{\alpha_9,\alpha_8} - e_{-\alpha_9,-\alpha_8} + e_{h_1,h_1} + e_{h_2,h_1} - e_{h_2,h_2} + e_{h_2,h_3} + e_{h_3,h_3};\\
w_3 = &\ e_{\alpha_1,\alpha_1} + e_{\alpha_1,\alpha_1} + e_{\alpha_2,\alpha_7} + e_{-\alpha_2,-\alpha_7} + e_{\alpha_7,\alpha_2} + e_{-\alpha_7,\alpha_2} - e_{\alpha_3,-\alpha_3} - e_{-\alpha_3,\alpha_3} +\\
&+ e_{\alpha_4,\alpha_8} + e_{-\alpha_4,-\alpha_8} + e_{\alpha_8,\alpha_4} + e_{-\alpha_8,\alpha_4} + e_{\alpha_5,\alpha_5} + e_{-\alpha_5,-\alpha_5} + e_{\alpha_6,\alpha_6} + e_{-\alpha_6,-\alpha_6} +\\
&+ e_{\alpha_9,\alpha_9} + e_{-\alpha_9,-\alpha_9} + e_{h_1,h_1} + e_{h_2,h_2} + 2e_{h_3,h_2} - e_{h_3,h_3};\\
X_1 = &-e_{h_1,-\alpha_1} + 2e_{\alpha_1,h_1} - e_{\alpha_1,h_2} + e_{\alpha_4,\alpha_2} - e_{-\alpha_2,-\alpha_4} + e_{\alpha_6,\alpha_5} - e_{-\alpha_5,-\alpha_6} +\\
&+ e_{\alpha_8,\alpha_7} - e_{-\alpha_7,-\alpha_8},\\
X_3 = &-e_{h_3,-\alpha_3} + 2e_{\alpha_3,h_3} - 2e_{\alpha_3,h_2} + 2e_{\alpha_5,\alpha_2} - e_{-\alpha_2,-\alpha_5} + 2e_{\alpha_6,\alpha_4} - e_{-\alpha_4,-\alpha_6} -\\
&- e_{\alpha_7,\alpha_5} + 2e_{-\alpha_5,-\alpha_7} - e_{\alpha_8,\alpha_6} + 2e_{-\alpha_6,-\alpha_8}.
\end{aligned}$$

Так как матрицы x_1 и x_3 коммутируют с $h_{\alpha_1}(-1)$, то они обе разбиваются на блоки, соответствующие частям базиса $\{v_1, v_{-1}, v_3, v_{-3}, v_9, v_{-9}, V_1, V_2, V_3\}$ и $\{v_2, v_{-2}, v_4, v_{-4}, v_5, v_{-5}, v_6, v_{-6}, v_7, v_{-7}, v_8, v_{-8}\}$.

Из того, что матрица x_1 коммутирует с w_3 и с $w_2 w_3 w_2 w_1 w_2^{-1} w_3^{-1} w_2^{-1}$, следует, что на первом блоке она имеет вид

$$\begin{pmatrix}
t_1 & t_2 & t_3 & -t_3 & t_4 & -t_4 & -2t_5 & t_5 & 0\\
t_6 & t_7 & t_8 & -t_8 & t_9 & -t_9 & -2t_{10} & t_{10} & 0\\
t_{11} & t_{12} & t_{13} & t_{14} & -t_{15} & t_{15} & -2t_{16}-2t_{17} & t_{16} & t_{17}\\
-t_{11} & -t_{12} & t_{14} & t_{13} & t_{15} & -t_{15} & 2t_{16}+2t_{17} & t_{16}-2t_{17} & t_{17}\\
t_{18} & t_{19} & -t_{20} & t_{20} & t_{21} & t_{22} & t_{23} & t_{24} & 0\\
-t_{18} & -t_{19} & t_{20} & -t_{20} & t_{22} & t_{21} & -t_{23} & t_{23}+t_{24} & 0\\
t_{25} & t_{26} & -t_{27} & t_{27} & t_{28} & t_{29} & t_{30} & t_{31} & 0\\
0 & 0 & 0 & 0 & t_{28}+t_{29} & t_{28}+t_{29} & 0 & 2t_{31}+t_{30} & 0\\
0 & 0 & t_{32} & t_{32} & t_{28}+t_{29} & t_{28}+t_{29} & 0 & t_{33} & 2t_{31}-t_{33}+t_{30}
\end{pmatrix};$$

а на втором блоке — вид

$$\begin{pmatrix}
t_{34} & t_{35} & t_{36} & t_{37} & t_{38} & t_{39} & t_{40} & t_{41} & t_{42} & t_{43} & t_{44} & t_{45}\\
t_{46} & t_{47} & t_{48} & t_{49} & t_{50} & t_{51} & t_{52} & t_{53} & t_{54} & t_{55} & t_{56} & t_{57}\\
-t_{49} & -t_{48} & t_{47} & t_{46} & -t_{53} & -t_{52} & t_{51} & t_{50} & -t_{57} & -t_{56} & t_{55} & t_{54}\\
-t_{37} & -t_{36} & t_{35} & t_{34} & -t_{41} & -t_{40} & t_{39} & t_{38} & -t_{45} & -t_{44} & t_{43} & t_{42}\\
t_{58} & t_{59} & t_{60} & t_{61} & t_{62} & t_{63} & t_{64} & t_{65} & t_{58} & t_{59} & t_{60} & t_{61}\\
t_{66} & t_{67} & t_{68} & t_{69} & t_{70} & t_{71} & t_{72} & t_{73} & t_{66} & t_{67} & t_{68} & t_{69}\\
-t_{69} & -t_{68} & t_{67} & t_{66} & -t_{73} & -t_{72} & t_{71} & t_{70} & -t_{69} & -t_{68} & t_{67} & t_{66}\\
-t_{61} & -t_{60} & t_{59} & t_{58} & -t_{65} & -t_{64} & t_{63} & t_{62} & -t_{61} & -t_{60} & t_{59} & t_{58}\\
t_{42} & t_{43} & t_{44} & t_{45} & t_{38} & t_{39} & t_{40} & t_{41} & t_{34} & t_{35} & t_{36} & t_{37}\\
t_{54} & t_{55} & t_{56} & t_{57} & t_{38} & t_{39} & t_{40} & t_{41} & t_{34} & t_{35} & t_{36} & t_{37}\\
-t_{57} & -t_{56} & t_{55} & t_{54} & -t_{53} & -t_{52} & t_{51} & t_{50} & -t_{49} & -t_{48} & t_{47} & t_{46}\\
-t_{45} & -t_{44} & t_{43} & t_{42} & -t_{41} & -t_{40} & t_{39} & t_{38} & -t_{37} & -t_{36} & t_{35} & t_{34}
\end{pmatrix}.$$

Аналогично, из того, что матрица x_3 коммутирует с w_1 и $w_2 w_3 w_2^{-1}$, следует, что на первом блоке она имеет вид

$$\begin{pmatrix}
u_1 & u_2 & u_3 & u_4 & u_5 & -u_5 & -2u_6-2u_7 & u_6 & u_7\\
u_2 & u_1 & -u_3 & -u_4 & -u_5 & u_5 & -2u_6-2u_7 & u_6+2u_7 & -u_7\\
-u_8 & u_8 & u_9 & u_{10} & u_8 & -u_8 & 0 & -u_{11} & u_{11}\\
u_{12} & -u_{12} & u_{13} & u_{14} & -u_{12} & u_{12} & 0 & -u_{15} & u_{15}\\
u_5 & -u_5 & -u_3 & -u_4 & u_1 & u_2 & 0 & u_6+2u_7 & -u_7\\
-u_5 & u_5 & u_3 & u_4 & u_2 & u_1 & 0 & u_6 & u_7\\
-u_{16} & -u_{16} & 0 & 0 & u_{16} & u_{16} & u_{20}+u_{21} & 0 & 0\\
0 & 0 & 0 & 0 & 2u_{16} & 2u_{16} & 0 & u_{20}+u_{21} & 0\\
-u_{17} & u_{17} & u_{18} & u_{19} & 2u_{16}+u_{17} & 2u_{16}+u_{17} & u_{20} & u_{21} &
\end{pmatrix};$$

а на втором блоке — вид

$$\begin{pmatrix}
u_{22} & u_{23} & -u_{24} & -u_{25} & u_{27} & u_{26} & -u_{28} & u_{28} & u_{29} & u_{30} & u_{25} & u_{24}\\
u_{31} & u_{32} & -u_{33} & -u_{34} & u_{36} & u_{35} & -u_{37} & u_{37} & u_{38} & u_{39} & u_{34} & u_{33}\\
u_{24} & u_{25} & u_{22} & u_{23} & u_{28} & -u_{28} & u_{27} & u_{26} & -u_{25} & -u_{24} & u_{29} & u_{30}\\
u_{33} & u_{34} & u_{31} & u_{32} & u_{37} & -u_{37} & u_{36} & u_{35} & -u_{34} & -u_{33} & u_{38} & u_{39}\\
u_{40} & u_{41} & -u_{42} & -u_{43} & u_{44} & u_{45} & -u_{46} & u_{46} & u_{47} & u_{48} & u_{43} & u_{42}\\
u_{48} & u_{47} & u_{42} & u_{43} & u_{45} & u_{44} & u_{46} & -u_{46} & u_{41} & u_{40} & -u_{43} & -u_{42}\\
u_{42} & u_{43} & u_{40} & u_{41} & u_{46} & -u_{46} & u_{44} & u_{45} & -u_{43} & -u_{42} & u_{47} & u_{48}\\
-u_{42} & -u_{43} & u_{48} & u_{47} & -u_{46} & u_{46} & u_{45} & u_{44} & u_{43} & u_{42} & u_{41} & u_{40}\\
u_{39} & u_{38} & u_{33} & u_{34} & u_{35} & u_{36} & u_{37} & -u_{37} & u_{32} & u_{31} & -u_{34} & -u_{33}\\
u_{30} & u_{29} & u_{24} & u_{25} & u_{26} & u_{27} & u_{28} & -u_{28} & u_{23} & u_{22} & -u_{25} & -u_{24}\\
-u_{33} & -u_{34} & u_{39} & u_{38} & -u_{37} & u_{37} & u_{35} & u_{36} & u_{34} & u_{33} & u_{32} & u_{31}\\
-u_{24} & -u_{25} & u_{30} & u_{29} & -u_{28} & u_{28} & u_{26} & u_{27} & u_{25} & u_{24} & u_{23} & u_{22}
\end{pmatrix}.$$

При этом $t_1, t_7, t_{13}, t_{21}, t_{30}, t_{34}, t_{47}, t_{62}, t_{71}, u_1, u_9, u_{14}, u_{21}, u_{22}, u_{32}, u_{44}$ сравнимы с единицей по модулю радикала, $t_2, t_5, t_{26}, t_{49}, t_{73}, u_{10}, u_{19}, u_{35}, u_{39}$ сравнимы с -1 по модулю радикала, u_{11}, u_{40} сравнимы с двойкой, все остальные элементы лежат в радикале. Всего мы имеем 121 переменную $t_1, \ldots, t_{73}, u_1, \ldots, u_{48}$.

Применим последовательно три замены базиса, коммутирующие друг с другом и со всеми матрицами w_i. Эти замены будут представлены матрицами C_1, C_2, C_3. Матрица C_1 блочно-диагональна с блоками размера 2×2. На всех блоках размера 2×2, соответствующих длинным и коротким корням, матрица C_1 имеет вид

$$\begin{pmatrix} 1 & -u_{18}/u_{19}\\ -u_{18}/u_{19} & 1 \end{pmatrix}.$$

На последнем блоке она единична.

Матрица C_2 диагональна, единична на последнем блоке, скалярна с множителем a на всех местах, соответствующих корням.

Матрица C_3 — это единичная, которой прибавлены блоки 2×2 в следующих местах: если по горизонтали часть базиса $\{v_\alpha, v_{-\alpha}\}$, $\alpha = e_1 - e_2, e_2 + e_3, e_1 - e_3$, то по вертикали соответственно $\{v_\beta, v_{-\beta}\}$, $\beta = e_3, e_1, e_2$, и матрица

$$\begin{pmatrix} t_3 & -t_3 \\ -t_3 & t_3 \end{pmatrix};$$

если же по горизонтали часть базиса $\{v_\alpha, v_{-\alpha}\}$, $\alpha = e_1 + e_2, e_2 - e_3, e_1 + e_3$, то по вертикали снова $\{v_\beta, v_{-\beta}\}$, $\beta = e_3, e_1, e_2$, и противоположная матрица.

Так как все три матрицы коммутируют со всеми w_i, то после замены базиса любой из этих матриц все соотношения на элементы матриц x_1 и x_3 будут выполнены.

Сначала применим замены с помощью матрицы C_1. После нее новая u_{18} в матрице x_3 станет равной нулю (для удобства обозначений не будем изменять названия переменных). Далее выберем $a = -1/u_{19}$ (где u_{19} — самое последнее). При этом u_{18} не изменится, а u_{19} станет равным -1. Наконец, применим последнюю замену и получим дополнительно $t_3 = 0$.

Теперь мы можем считать, что $u_{18} = 0, u_{19} = -1, t_3 = 0$, переменных стало 118.

Введем $x_4 = \varphi_2(x_{\alpha_4}(1)) = w_2 x_1 w_2^{-1}$, $x_2 = \varphi_2(x_{\alpha_2}(1)) = w_1 x_4 w_1^{-1}$, $x_7 = \varphi_2(x_{\alpha_7}(1)) = w_3 x_2 w_3^{-1}$, $x_5 = \varphi_2(x_{\alpha_5}(1)) = w_2 x_3 w_2^{-1}$.

Используем теперь следующие соотношения, которые должны выполняться для элементов w_i и x_i:

$$\begin{aligned}
Con1 &= (h_2 x_1 h_2 x_1 = E);\\
Con2 &= (x_1 x_4 = x_4 x_1);\\
Con3 &= (x_1 x_3 = x_3 x_1);\\
Con4 &= (x_1 x_2 = x_4 x_2 x_1);\\
Con5 &= (x_7 x_3 = x_3 x_7);\\
Con6 &= (h_2 x_3 h_2 x_3 = E);\\
Con7 &= (x_7^2 x_3 x_5 = x_5 x_3).
\end{aligned}$$

Заметим, что каждое из соотношений на матрицы является 441 полиномиальным тождеством, где все полиномы имеют целые коэффициенты и зависят от переменных t_i, u_j. Перенумеруем временно все переменные в $v_1, \dots, v_{118}$.

Предположим, что один из таких полиномов мы можем представить в виде

$$\begin{aligned}
&(v_{k_0} - \overline{v}_{k_0})A + (v_1 - \overline{v}_1)B_1 + \dots\\
&\qquad \dots + (v_{k_0-1} - \overline{v}_{k_0-1})B_{k_0-1} + (v_{k_0+1} - \overline{v}_{k_0+1})B_{k_0+1} + \dots + v_{118} - \overline{v}_{118})B_{118} = 0,
\end{aligned}$$

при этом $\overline{v}_i$ — это то целое число, с которым сравнимо v_i по модулю радикала, полином A обратим по модулю радикала, B_i — какие-то полиномы (во все эти полиномы, в том числе и в A может входить v_{k_0}). Тогда

$$
\begin{aligned}
&v_{k_0} - \overline{v}_{k_0} = \\
&= -\frac{(v_1 - \overline{v}_1)B_1 + \dots + (v_{k_0-1} - \overline{v}_{k_0-1})B_{k_0-1} + (v_{k_0+1} - \overline{v}_{k_0+1})B_{k_0+1} + \dots + v_{118} - \overline{v}_{118})B_{118}}{A},
\end{aligned}
$$

мы можем подставить выражение для v_{k_0} во все остальные полиномиальные соотношения. Если мы сможем выбрать последовательно 118 таких соотношений, что в процессе процедуры такой подстановки каждый раз сможем избавляться от какой-то очередной переменной, то к последнему соотношению мы будем иметь выражение

$$(v_{k_{118}} - \overline{v}_{k_{118}})C = 0,$$

где C — это некоторое рациональное выражение от переменных $v_1, \dots, v_{118}$, обратимое по модулю радикала. Таким образом, мы сможем сказать, что $v_{k_{118}} = \overline{v}_{k_{118}}$, а следовательно, все остальные переменные тоже равны тому, с чем они сравнимы по модулю радикала. Существование искомых 118 соотношений эквивалентно существованию таких 118 соотношений, что квадратная матрица, составленная из коэффициентов этих соотношений по модулю радикала, имеет обратимый определитель.

Так как выписывать матрицу 118×118 сложно и ненаглядно, то будем последовательно выписывать искомые соотношения, но для простоты писать коэффициенты A и B_i по модулю радикала (в результате эти коэффициенты будут иметь вид чисел 0, ± 1, ± 2).

Мы запишем ниже, каким образом выражаются переменные из соотношений (в скобках записываем номер соотношения и позицию в нем): $(Con1,1,1)$: $t_6 = 2(t_1-1)$; $(Con1,1,2)$: $t_7 = -t_1 - 2t_5$; $(Con1,1,5)$: $t_8 = 2t_{27}$; $(Con1,1,17)$: $t_{28} = 2t_4 - t_9 + t_{29}$; $(Con1,1,19)$: $t_{10} = t_{30} - t_1$; $(Con1,5,1)$: $t_{11} = 0$; $(Con1,5,2)$: $t_{12} = 2t_{16} + 2t_{17}$; $(Con1,5,5)$: $t_{13} = 1$; $(Con1,5,6)$: $t_{14} = 0$; $(Con1,5,17)$: $t_{15} = 0$; $(Con1,17,1)$: $t_{18} = 0$; $(Con1,17,2)$: $t_{23} = -t_{19}$; $(Con1,17,5)$: $t_{20} = 0$; $(Con1,19,5)$: $t_{27} = 0$; $(Con1,19,1)$: $t_1 = 1$; $(Con1,19,20)$: $t_{30} = 1-2t_{31}$; $(Con1,19,18)$: $t_9 = 0$; $(Con1,2,2)$: $t_{31} = 1 + t_5$; $(Con1,1,20)$: $t_5 = -1$; $(Con1,18,18)$: $t_{21} = 1$; $(Con1,6,2)$: $t_{17} = -t_{16}$; $(Con1,18,17)$: $t_{22} = 0$; $(Con1,21,21)$: $t_{33} = 0$; $(Con1,18,2)$: $t_{19} = 0$; $(Con1,2,1)$: $t_2 = -1$; $(Con2,2,2)$: $t_{35} = 0$; $(Con2,5,2)$: $t_{60} = 0$; $(Con2,1,19)$: $t_{47} = 1$; $(Con2,6,2)$: $t_{68} = 0$; $(Con2,7,15)$: $t_{43} = 0$; $(Con2,17,2)$: $t_{55} = 0$; $(Con2,19,18)$: $t_{42} = t_{29}$; $(Con2,7,8)$: $t_{34} = 1$; $(Con1,3,3)$: $t_{36} = 0$; $(Con1,3,4)$: $t_{37} = 0$; $(Con1,4,3)$: $t_{48} = 2t_{46}$; $(Con2,1,8)$: $t_{49} = -1$; $(Con2,4,5)$: $t_{52} = 0$; $(Con2,9,2)$: $t_{58} = t_{16}$; $(Con2,9,5)$: $t_{64} = 0$; $(Con2,15,4)$: $t_{29} = 0$; $(Con2,20,3)$: $t_{25} = 0$; $(Con1,10,3)$: $t_{61} = 0$; $(Con1,10,7)$: $t_{59} = 0$; $(Con2,1,11)$: $t_{39} = 0$; $(Con2,4,8)$: $t_{46} = 0$; $(Con2,16,2)$ $t_{45} = t_{24}$; $(Con2,7,2)$: $t_{26} = -1$; $(Con1,4,9)$: $t_{41} = 0$; $(Con1,9,12)$: $t_{63} = 0$; $(Con2,4,9)$: $t_{40} = 0$; $(Con1,13,8)$: $t_{44} = 0$; $(Con3,17,2)$: $u_5 = 0$; $(Con3,2,19)$: $u_2 = 0$; $(Con3,5,19)$: $u_8 = 0$; $(Con3,6,19)$: $u_{12} = 0$; $(Con3,5,5)$: $t_{32} = 0$; $(Con3,5,6)$: $t_{16} = 0$; $(Con3,21,2)$: $u_{17} = 0$; $(Con3,1,1)$: $u_{16} = 0$; $(Con2,14,2)$: $t_{56} = -t_{54}$; $(Con2,14,19)$ и $(Con2,14,21)$: $t_{54} = t_{24} = 0$; $(Con3,19,19)$: $u_7 = -u_6$; $(Con4,5,5)$: $t_{62} = 1$; $(Con4,5,10)$: $t_{65} = 0$; $(Con4,6,21)$: $t_{67} = 0$; $(Con4,9,20)$: $t_{66} = 0$; $(Con4,21,13)$: $t_4 = 0$; $(Con4,2,13)$: $t_{57} = 0$; $(Con4,6,18)$: $t_{69} = 0$; $(Con4,4,5)$: $t_{50} = 0$; $(Con4,6,6)$: $t_{71} = 1$; $(Con4,6,5)$: $t_{70} = 0$; $(Con4,17,5)$: $t_{53} = 0$; $(Con4,11,10)$: $t_{72} = 0$; $(Con4,11,5)$: $t_{73} = -1$; $(Con4,3,5)$: $t_{38} = 0$; $(Con4,3,6)$: $t_{51} = 0$; $(Con3,9,3)$: $u_{42} = 0$; $(Con3,16,3)$: $u_{30} = 0$; $(Con3,12,3)$: $u_{48} = 0$; $(Con3,11,4)$: $u_{41} = 0$; $(Con3,10,4)$: $u_{43} = 0$; $(Con3,4,7)$: $u_{31} = 0$;

$(Con3,3,8)$: $u_{23}=0$; $(Con3,9,12)$: $u_{45}=0$; $(Con3,8,13)$: $u_{38}=0$; $(Con3,9,3)$: $u_1=u_{20}+u_{21}$; $(Con3,14,4)$: $u_{25}=0$; $(Con3,4,4)$: $u_{34}=0$; $(Con3,4,11)$: $u_{36}=0$; $(Con3,7,7)$: $u_{24}=0$; $(Con3,1,20)$: $u_6=0$; $(Con5,2,8)$: $u_{29}=0$; $(Con5,9,5)$: $u_{13}=0$; $(Con5,5,4)$: $u_{47}=0$; $(Con5,3,6)$: $u_{27}=0$; $(Con5,9,20)$: $u_{15}=0$; $(Con5,13,20)$: $u_{20}=0$; $(Con5,13,19)$: $u_{32}=u_{21}$; $(Con6,8,8)$: $u_{21}=1$; $(Con6,17,20)$: $u_3=0$; $(Con6,5,20)$: $u_9=1$; $(Con6,12,9)$: $u_{28}=0$; $(Con6,6,6)$: $u_{14}=1$; $(Con6,2,6)$: $u_4=0$; $(Con6,3,3)$: $u_{22}=1$; $(Con6,10,14)$: $u_{44}=1$; $(Con5,5,14)$: $u_{40}=u_{11}$; $(Con5,13,9)$: $u_{26}=0$; $(Con6,5,6)$: $u_{11}=-2u_{10}$; $(Con6,12,3)$: $u_{46}=0$; $(Con7,13,14)$: $u_{10}=-1$; $(Con7,17,5)$: $u_{37}=0$; $(Con7,5,7)$: $u_{33}=0$; $(Con7,5,14)$: $u_{39}=-1$; $(Con7,2,16)$: $u_{35}=-1$.

Таким образом, оказывается, что $x_1=x_{\alpha_1}(1)$ и $x_3=x_{\alpha_3}(1)$. Из того, что все длинные (и все короткие) корни сопряжены относительно действия группы Вейля, сразу получаем, что $\varphi_2(x_\alpha(1))=x_\alpha(1)$ для всех $\alpha\in\Phi$.

Теперь рассмотрим $h_t=\varphi_2(h_{\alpha_1}(t))$. Из того, что h_t коммутирует с h_1, h_2, w_3, w_9, $x_{\alpha_3}(1)$, $x_{\alpha_9}(1)$, а также из соотношений $w_1h_tw_1^{-1}h_t=E$, $w_2h_tw_2^{-1}=w_1w_2h_tw_2^{-1}w_1^{-1}h_t$, напрямую следует, что $h_t=h_{\alpha_1}(s)$ для некоторого $s\in R^*$. Аналогично, $\varphi_2(h_{\alpha_3}(t))=h_{\alpha_3}(s)$.

Случай B_4

В этом случае мы имеем 32 корня

$$\pm e_1,\pm e_2,\pm e_3,\pm e_4,\pm e_i\pm e_j,\qquad 1\leqslant i<j\leqslant 4,$$

присоединенное представление 36-мерно. Точно так же, как в предыдущем пункте, мы будем рассматривать $x_1=\varphi_2(x_{\alpha_1}(1))$ и $x_4=\varphi_2(x_{\alpha_4}(1))$. Благодаря коммутированию с элементами h_1 и h_3 матрица x_1 разбивается на блоки

$$\begin{aligned}&\{v_{e_1-e_2},v_{e_2-e_1},v_{e_1+e_2},v_{-e_1-e_2},v_{e_3-e_4},v_{e_4-e_3},v_{e_3+e_4},v_{-e_3-e_4},V_1,V_2,V_3,V_4\},\\&\{v_{e_1-e_3},v_{e_3-e_1},v_{e_1+e_3},v_{-e_1-e_3},v_{e_1-e_4},v_{e_4-e_1},v_{e_1+e_4},v_{-e_1-e_4},\\&\qquad v_{e_2-e_3},v_{e_3-e_2},v_{e_2+e_3},v_{-e_2-e_3},v_{e_2-e_4},v_{e_4-e_2},v_{e_2+e_4},v_{-e_2-e_4}\},\\&\{v_{e_1},v_{-e_1},v_{e_2},v_{-e_2}\},\\&\{v_{e_3},v_{-e_3},v_{e_4},v_{-e_4}\},\end{aligned}$$

а матрица x_4 благодаря коммутированию с h_1 и h_2 — на блоки

$$\begin{aligned}&\{v_{e_4},v_{-e_4},V_1,V_2,V_3,V_4\},\\&\{v_{e_1-e_2},v_{e_2-e_1},v_{e_1+e_2},v_{-e_1-e_2},v_{e_3},v_{-e_3},v_{e_3-e_4},v_{e_4-e_3},v_{e_3+e_4},v_{-e_3-e_4}\},\\&\{v_{e_1},v_{-e_1},v_{e_1-e_4},v_{e_4-e_1},v_{e_1+e_4},v_{-e_1-e_4},v_{e_2-e_3},v_{e_3-e_2},v_{e_2+e_3},v_{-e_2-e_3}\},\\&\{v_{e_2},v_{-e_2},v_{e_2-e_4},v_{e_4-e_2},v_{e_2+e_4},v_{-e_2-e_4},v_{e_1-e_3},v_{e_3-e_1},v_{e_1+e_3},v_{-e_1-e_3}\}.\end{aligned}$$

Для начала рассмотрим матрицу x_1 на блоке $\{v_{e_3},v_{-e_3},v_{e_4},v_{-e_4}\}$, прообраз ее на этом блоке просто единичен. Мы знаем, что x_1 коммутирует с w_{e_3}, w_{e_4}, $w_{e_3-e_4}$. Это дает нам следующий вид матрицы на рассматриваемом блоке:

$$\begin{pmatrix}a_1&a_2&a_3&-a_3\\a_2&a_1&-a_3&a_3\\-a_3&a_3&a_1&a_2\\a_3&-a_3&a_2&a_1\end{pmatrix}.$$

Кроме того, из того, что $h_2x_1h_2x_1 = E$, мы получаем уравнения $a_1^2 + a_2^2 + 2a_3^2 = 1$ и $2a_1a_2 - 2a_3^2 = 0$. Сложив их, получим $(a_1 + a_2)^2 = 1$, откуда (так как $a_1 + a_2 \equiv 1 \mod J$) имеем $a_1 + a_2 = 1$, т. е. $a_1 = 1 - a_2$.

Теперь рассмотрим нашу матрицу на блоке $\{v_{e_1}, v_{-e_1}, v_{e_2}, v_{-e_2}\}$. Ее прообраз на этом блоке имеет вид

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

Из коммутирования с $w_{e_1+e_2}$ следует вид

$$\begin{pmatrix} b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ -c_4 & -c_3 & c_2 & c_1 \\ -b_4 & -b_3 & b_2 & b_1 \end{pmatrix}.$$

Теперь соединим эти базисы вместе, заметив, что для всех w_α, $\alpha \in \Phi$, и всех $x_\beta(1)$, β — длинный корень, эта часть базиса выделится инвариантным прямым слагаемым. В рассматриваемой сейчас матрице 11 неизвестных. Рассмотрим на этой части базиса матрицу $\varphi_2(x_{e_1-e_3}(1)) = w_{e_2-e_3}x_1w_{e_2-e_3}^{-1}$. Она имеет вид

$$\begin{pmatrix} b_1 & b_2 & 0 & 0 & -b_3 & -b_4 & 0 & 0 \\ c_1 & c_2 & 0 & 0 & -c_3 & -c_4 & 0 & 0 \\ 0 & 0 & 1-a_2 & a_2 & 0 & 0 & a_3 & -a_3 \\ 0 & 0 & a_2 & 1-a_2 & 0 & 0 & -a_3 & a_3 \\ c_4 & c_3 & 0 & 0 & c_2 & c_1 & 0 & 0 \\ b_4 & b_3 & 0 & 0 & b_2 & b_1 & 0 & 0 \\ 0 & 0 & -a_3 & a_3 & 0 & 0 & 1-a_2 & a_2 \\ 0 & 0 & a_3 & -a_3 & 0 & 0 & a_2 & 1-a_2 \end{pmatrix}$$

Мы знаем, что матрицы $\varphi_2(x_{e_1-e_3}(1))$ и x_1 коммутируют, откуда (позиция $(1,8)$) следует $2a_3(b_3 - b_4) = 0$. Так как $b_3 - b_4 \equiv 1 \mod J$, то $a_3 = 0$. Из уже выписанных выше уравнений получаем $2a_2(a_2 - 1) = 0$, откуда (так как $a_2 \in J$) $a_2 = 0$. Теперь воспользуемся соотношением $x_{e_1-e_2}(1)x_{e_2-e_3}(1) = x_{e_1-e_3}(1)x_{e_2-e_3}(1)x_{e_1-e_2}(1)$. Его позиция $(6,5)$ дает нам $b_2(1 - b_1 - c_2)$, откуда $b_2 = 0$. После этого позиция $(6,6)$ дает $b_1(b_1 - 1) = 0$, откуда $b_1 = 1$. Из позиции $(5,5)$ $c_2 = 1$, а из позиции $(5,6)$ $c_1 = 0$. Из того же соотношения получаем $b_4 = -c_3$, $c_4 = -b_4^2/b_3$. Таким образом, рассматриваемая матрица на данной части базиса имеет вид

$$\begin{pmatrix} 1 & 0 & b_3 & -c_3 & 0 & 0 & 0 & 0 \\ 0 & 1 & c_3 & -c_3^2/b_3 & 0 & 0 & 0 & 0 \\ c_3^2/b_3 & -c_3 & 1 & 0 & 0 & 0 & 0 & 0 \\ c_3 & -b_3 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Теперь возьмем немного другую часть базиса:

$$\{v_{e_1-e_2}, v_{e_2-e_1}, v_{e_1+e_2}, v_{-e_1-e_2}, v_{e_3-e_4}, v_{e_4-e_3}, v_{e_3+e_4}, v_{-e_3-e_4}, v_{e_3}, v_{-e_3}, v_{e_4}, v_{-e_4}, V_1, V_2, V_3, V_4\}.$$

Матрица x_1 коммутирует с $w_{e_1+e_2}$, w_{e_4}, $w_{e_3-e_4}$, откуда непосредственно получаем, что на неизвестной части базиса размера 12×12 матрица имеет вид

$$\begin{pmatrix}
b_{1,1} & b_{1,2} & b_{1,3} & -b_{1,3} & b_{1,5} & -b_{1,5} & b_{1,5} & -b_{1,5} & -2b_{1,14} & b_{1,14} & 0 & 0 \\
b_{2,1} & b_{2,2} & b_{2,3} & -b_{2,3} & b_{2,5} & -b_{2,5} & b_{2,5} & -b_{2,5} & -2b_{2,14} & b_{2,14} & 0 & 0 \\
b_{3,1} & b_{3,2} & b_{3,3} & b_{3,4} & b_{3,5} & -b_{3,5} & b_{3,5} & -b_{3,5} & b_{4,14}-b_{3,14} & b_{3,14} & 0 & 0 \\
-b_{3,1} & -b_{3,2} & b_{3,4} & b_{3,3} & -b_{3,5} & b_{3,5} & -b_{3,5} & b_{3,5} & b_{3,14}-b_{4,14} & b_{4,14} & 0 & 0 \\
b_{5,1} & b_{5,2} & b_{5,3} & -b_{5,3} & b_{5,5} & b_{5,6} & b_{5,7} & -b_{5,7} & 2(b_{8,14}-b_{6,16}) & 2b_{6,16}-b_{8,14} & -2b_{6,16} & b_{6,16} \\
-b_{5,1} & -b_{5,2} & -b_{5,3} & b_{5,3} & b_{5,6} & b_{5,5} & -b_{5,7} & b_{5,7} & 2(-b_{8,14}+b_{6,16}) & b_{8,14} & -2b_{6,16} & b_{6,16} \\
b_{5,1} & b_{5,2} & b_{5,3} & -b_{5,3} & b_{5,7} & -b_{5,7} & b_{5,5} & b_{5,6} & 2(b_{8,14}-b_{6,16}) & 2b_{6,16}-b_{8,14} & 0 & -b_{6,16} \\
-b_{5,1} & -b_{5,2} & -b_{5,3} & b_{5,3} & -b_{5,7} & b_{5,7} & b_{5,6} & b_{5,5} & 2(-b_{8,14}+b_{6,16}) & b_{8,14} & 0 & -b_{6,16} \\
b_{13,1} & b_{13,2} & b_{13,3} & b_{15,3}-b_{13,3} & b_{13,5} & -b_{13,5} & b_{13,5} & -b_{13,5} & b_{14,14}-2b_{13,14} & b_{13,14} & 0 & 0 \\
0 & 0 & b_{15,3} & b_{15,3} & 0 & 0 & 0 & 0 & 0 & b_{14,14} & 0 & 0 \\
0 & 0 & b_{15,3} & b_{15,3} & b_{15,5} & b_{15,5} & b_{15,5} & b_{15,5} & 0 & b_{8,14} & b_{14,14}-b_{8,14} & 0 \\
0 & 0 & b_{15,3} & b_{15,3} & 0 & 0 & 2b_{15,5} & 2b_{15,5} & 0 & b_{8,14} & 0 & b_{14,14}-b_{8,14}
\end{pmatrix}$$

Из того, что матрица x_4 коммутирует с $w_{e_1-e_2}$, $w_{e_1+e_2}$, w_{e_3}, мы получаем, что на части базиса $\{v_{e_1-e_2}, v_{e_2-e_1}, v_{e_1+e_2}, v_{-e_1-e_2}, v_{e_3-e_4}, v_{e_4-e_3}, v_{e_3+e_4}, v_{-e_3-e_4}, v_{e_3}, v_{-e_3}\}$ она равна

$$\begin{pmatrix}
a_{1,1} & a_{1,2} & a_{1,3} & -a_{1,3} & a_{1,5} & a_{1,6} & -a_{1,6} & -a_{1,5} & a_{1,9} & -a_{1,9} \\
a_{1,2} & a_{1,1} & -a_{1,3} & a_{1,3} & -a_{1,5} & -a_{1,6} & a_{1,6} & a_{1,5} & -a_{1,9} & a_{1,9} \\
a_{3,1} & -a_{3,1} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & -a_{3,6} & -a_{3,5} & a_{3,9} & -a_{3,9} \\
-a_{3,1} & a_{3,1} & a_{3,4} & a_{3,3} & -a_{3,5} & -a_{3,6} & a_{3,6} & a_{3,5} & -a_{3,9} & a_{3,9} \\
a_{5,1} & -a_{5,1} & a_{5,3} & -a_{5,3} & a_{5,5} & a_{5,6} & a_{5,7} & a_{5,8} & a_{5,9} & a_{5,10} \\
a_{6,1} & -a_{6,1} & a_{6,3} & -a_{6,3} & a_{6,5} & a_{6,6} & a_{6,7} & a_{6,8} & a_{6,9} & a_{6,10} \\
-a_{6,1} & a_{6,1} & -a_{6,3} & a_{6,3} & a_{6,8} & a_{6,7} & a_{6,6} & a_{6,5} & a_{6,10} & a_{6,9} \\
-a_{5,1} & a_{5,1} & -a_{5,3} & a_{5,3} & a_{5,8} & a_{5,7} & a_{5,6} & a_{5,5} & a_{5,10} & a_{5,9} \\
a_{9,1} & -a_{9,1} & a_{9,3} & -a_{9,3} & a_{9,5} & a_{9,6} & a_{9,7} & a_{9,8} & a_{9,9} & a_{9,10} \\
-a_{9,1} & a_{9,1} & -a_{9,3} & a_{9,3} & a_{9,8} & a_{9,7} & a_{9,6} & a_{9,5} & a_{9,10} & a_{9,9}
\end{pmatrix},$$

а на части базиса $\{v_{e_4}, v_{-e_4}, V_1, V_2, V_3, V_4\}$ (с учетом того, что $h_{e_3-e_4}(-1)x_4h_{e_3-e_4}(-1)x_4 = E$) —

$$\begin{pmatrix}
a_{11,11} & a_{11,12} & 0 & 0 & a_{11,15} & -a_{11,15} \\
a_{12,11} & a_{12,12} & 0 & 0 & a_{12,15} & -a_{12,15} \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
a_{16,11} & a_{16,12} & 0 & 0 & 1-a_{16,16} & a_{16,16}
\end{pmatrix}.$$

Как в предыдущем пункте, мы можем блочно-диагональной заменой базиса добиться того, что $a_{16,11} = 0$, $a_{16,12} = -1$.

Из позиции $(15, 14)$ соотношения

$$Con1 = (h_{e_3-e_4}(-1)x_4h_{e_3-e_4}(-1)x_4 = E)$$

следует $a_{16,14}(a_{16,14}+2)=0$, откуда $a_{16,14}=0$. Аналогично, из позиции $(13,14)$ получаем $a_{13,14}=0$, из позиции $(16,12)$ — $a_{16,16}=a_{12,12}$, из позиции $(16,11)$ — $a_{12,11}=0$, из позиции $(11,11)$ — $a_{11,11}=1$; из позиции $(16,16)$ — $a_{12,15}=-1+a_{12,12}^2$, из позиции $(11,12)$ — $a_{11,15}=a_{11,12}(1+a_{12,12})$.

Из коммутирования x_1 и x_4 следует: позиции $(16,12)$ — $b_{14,14}=1+b_{8,14}$; $(10,16)$ — $b_{6,16}(a_{9,8}+a_{9,7}-a_{9,6}-a_{9,5})\Rightarrow b_{6,16}=0$; $(16,9)$ — -$b_{15,5}(a_{6,10}+a_{5,10})=0\Rightarrow b_{15,5}=0$.

Теперь блочно-диагональными заменами базиса, нееденичными на длинных корнях, добьемся $b_{13,1}=0$, $b_{13,2}=-1$.

После этого рассмотрим позиции $(1,14)$ и $(2,14)$ соотношения коммутирования, суммируя их, получим $(a_{1,1}+a_{1,2}-1)(b_{1,14}+b_{2,14})=0$. Так как $b_{1,14}+b_{2,14}$ обратимо, то $a_{1,2}=1-a_{1,1}$.

Теперь, как и в предыдущем пункте, будем писать соотношения для простоты по модулю радикала, понемногу сокращая переменные.

Из соотношения коммутирования: позиция $(13,1)$ — $a_{1,1}=1$; $(13,3)$ — $a_{1,3}=1$; $(13,5)$ — $a_{1,5}=1$; $(13,6)$ — $a_{1,6}=1$. Из $Con1$: позиция $(2,5)$ — $a_{1,9}=0$; снова коммутирование: позиция $(2,9)$ — $b_{1,5}=0$; позиция $(3,9)$ — $b_{3,5}=0$; позиция $(5,9)$ — $b_{5,6}=0$; позиция $(6,9)$ — $b_{5,7}=0$; позиция $(3,14)$ — $a_{3,1}=0$; позиция $(5,14)$ — $a_{5,1}=0$; позиция $(6,14)$ — $a_{6,1}=0$; позиция $(9,14)$ — $a_{9,1}=b_{8,14}$; позиция $(13,10)$ — $b_{13,5}=0$; $Con1$: позиция $(3,3)$ — $a_{3,3}=1$; позиция $(3,5)$ — $a_{3,5}=a_{3,9}$; позиция $(3,6)$ — $a_{3,6}=0$; позиция $(10,9)$ — $a_{9,10}=-a_{9,6}$; соотношение $Con2=(h_{e_2-e_3}(-1)x_1h_{e_2-e_3}(-1)x_1=E)$: позиция $(13,6)$ — $b_{2,5}=0$; позиция $(5,5)$ — $b_{5,5}=1$; позиция $(1,2)$ — $b_{1,2}=b_{1,14}$; позиция $(15,14)$ — $b_{8,14}=0$; позиция $(8,14)$ — $b_{5,1}=0$; позиция $(4,14)$ — $b_{3,1}=0$; позиция $(2,1)$ — $b_{2,1}=0$; позиция $(1,1)$ — $b_{1,1}=1$; позиция $(1,2)$ — $b_{2,2}=1$.

Теперь введем новое соотношение. Заметим, что $[x_{e_3}(1),x_{e_4}(1)]=x_{e_3+e_4}(1)^2$, а элементы $x_{e_3+e_4}(1)^2$ и $x_{e_1-e_2}(1)^2$ сопряжены с помощью элемента группы Вейля. Значит, матрицы x_1^2 и $[x_4,w_{e_3-e_4}x_4w_{e_3-e_4}^{-1}]$ сопряжены с помощью элемента группы Вейля. В частности, этот элемент меняет местами корни $\{e_1,-e_1,e_2,-e_2\}$ и $\{-e_3,e_3,-e_4,e_4\}$, поэтому матрица $[x_4,w_{e_3-e_4}x_4w_{e_3-e_4}^{-1}]$ блочно-диагональна относительно разбиения на части базиса $\{-e_3,e_3,-e_4,e_4\}$ и все остальные.

Отсюда сразу $a_{9,6}=0$, $a_{9,9}=1$, $a_{9,8}=a_{5,9}$, $a_{5,10}=0$, $a_{5,9}=0$; $a_{5,6}=0$.

Снова из $Con1$ имеем $a_{6,6}=1$, $a_{9,7}=0$, $a_{5,7}=0$, $a_{6,7}=0$, $a_{5,8}=0$, $a_{5,3}=0$, $a_{5,5}=1$, $a_{3,9}=0$, $a_{3,4}=0$.

Из коммутирования $b_{5,2}=0$, $b_{5,3}=0$. Из $Con2$ $b_{2,14}=0$, $b_{3,4}=0$, $b_{2,3}=0$, $b_{3,3}=1$, $b_{13,14}=0$, $b_{3,14}=2b_{3,2}+b_{4,14}$, $b_{1,3}=-2b_{13,3}+2b_{15,3}$.

Опять из блочно-диагональности матрицы $[x_4,w_{e_3-e_4}x_4w_{e_3-e_4}^{-1}]$ получаем $a_{6,5}=0$, $a_{6,9}=0$, $a_{12,12}=1$, $a_{6,3}=0$, $a_{9,3}=0$, $a_{6,8}=a_{11,12}$, $a_{11,12}=a_{6,10}a_{9,5}/2$, $b_{3,2}=0$, $b_{13,3}=0$, $b_{15,3}=0$, $b_{4,14}=0$.

Из остальных соотношений $a_{6,10}=-2/a_{9,5}$, $a_{9,5}=-2$, $a_{1,14}=2$.

Таким образом, $\varphi_2(x_{\alpha_4}(1))=x_{\alpha_4}(1)$ и $\varphi_2(x_{\alpha_1}(1))=x_{\alpha_1}(1)$ на рассматриваемых частях базиса. Однако для $x_{\alpha_4}(1)$ оставшиеся (не рассмотренные нами еще) части базиса $\{v_{e_1},v_{-e_1},v_{e_1-e_4},v_{e_4-e_1},v_{e_1+e_4},v_{-e_1-e_4},v_{e_2-e_3},v_{e_3-e_2},v_{e_2+e_3},v_{-e_2-e_3}\}$ и $\{v_{e_2},v_{-e_2},v_{e_2-e_4},v_{e_4-e_2},v_{e_2+e_4},v_{-e_2-e_4},v_{e_1-e_3},v_{e_3-e_1},v_{e_1+e_3},v_{-e_1-e_3}\}$ сопряжены к части базиса $\{v_{e_1-e_2},v_{e_2-e_1},v_{e_1+e_2},v_{-e_1-e_2},v_{e_3},v_{-e_3},v_{e_3-e_4},v_{e_4-e_3},v_{e_3+e_4},v_{-e_3-e_4}\}$ с помощью элементов группы Вейля w_{α_2} и $w_{\alpha_1}w_{\alpha_2}$. Значит, x_4 совпадает с $x_{\alpha_4}(1)$ на всем 36-мерном пространстве. Понятно, что отсюда сразу следует $\varphi_2(x_\alpha(1)) = x_\alpha(1)$ для всех коротких корней $\alpha \in \Phi$. Кроме того, $\varphi_2(x_\alpha(2)) = x_\alpha(2)$ для всех длинных корней α.

Следовательно, если мы покажем, что при автоморфизме φ_2 диагональная матрица $h_{e_2-e_3}(2)$ перейдет сама в себя, то искомое утверждение будет доказано. Рассмотрим $d_t = \varphi_2(h_{\alpha_1}(t))$.

Так как d_t коммутирует с h_1, h_2, h_3, то она разбивается на диагональные блоки, соответствующие частям базиса $\{v_{e_i}, v_{-e_i}\}$, $i = 1, \dots, 4$, $\{V_1, V_2, V_3, V_4\}$ и $\{v_{e_i-e_j}, v_{e_j-e_i}, v_{e_i+e_j}, v_{-e_i-e_j}, v_{e_k-e_l}, v_{e_l-e_k}, v_{e_k+e_l}, v_{-e_k-e_l}\}$, где i, j, k, l — различные числа от 1 до 4. Так как d_t коммутирует еще и с w_{e_4}, $w_{e_3-e_4}$, $w_{e_1+e_2}$, то она, во-первых, имеет одинаковый вид на частях базиса $\{v_{e_1}, v_{-e_1}\}$ и $\{v_{-e_2}, v_{e_2}\}$, $\{v_{e_3}, v_{-e_3}\}$ и $\{v_{e_4}, v_{-e_4}\}$, $\{v_{e_1-e_3}, v_{e_3-e_1}, v_{e_1+e_3}, v_{-e_1-e_3}, v_{e_2-e_4}, v_{e_4-e_2}, v_{e_2+e_4}, v_{-e_2-e_4}\}$ и $\{v_{e_1-e_4}, v_{e_4-e_1}, v_{e_1+e_4}, v_{-e_1-e_4}, v_{e_2-e_3}, v_{e_3-e_2}, v_{e_2+e_3}, v_{-e_2-e_3}\}$. Во-вторых, если на части $\{v_{e_4}, v_{-e_4}\}$ матрица d_t имела вид

$$\begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix},$$

то из коммутирования с w_{e_4} сразу же $d_4 = d_1$, $d_3 = d_2$. Из соотношения $w_{\alpha_1} d_t w_{\alpha_1}^{-1} d_t = E$ получаем $2d_1d_2 = 0$ и $d_1^2 + d_2^2 = 1$, откуда сразу $d_1 = 1$, $d_2 = 0$, на данной части базиса получили искомый вид.

Кроме того, заметим, что d_t коммутирует с $x_{e_1+e_2}(2)$, $x_{e_4}(1)$, $x_{e_3-e_4}(2)$, или, что то же с самое, с $X_{e_1+e_2}$, X_{e_4}, $X_{e_3-e_4}$.

Рассмотрев часть базиса $\{v_{e_1}, v_{-e_1}, v_{e_2}, v_{-e_2}\}$, мы увидим, что из коммутирования с $w_{e_1+e_2}$ на ней матрица d_t имеет вид

$$\begin{pmatrix} d_{1,1} & d_{1,2} & 0 & 0 \\ d_{2,1} & d_{2,2} & 0 & 0 \\ 0 & 0 & d_{2,2} & d_{2,1} \\ 0 & 0 & d_{1,2} & d_{1,1} \end{pmatrix};$$

коммутирование с $X_{e_1+e_2}$, которая на этой части базиса есть $e_{v_{e_1}, v_{-e_2}} - e_{v_{e_2}, v_{-e_1}}$, дает $d_{1,2} = d_{2,1} = 0$, и, наконец, условие $w_{\alpha_1} d_t w_{\alpha_1}^{-1} d_t = E$ дает $d_{1,1}d_{2,2} = 1$.

Теперь перейдем к части базиса $\{V_1, V_2, V_3, V_4\}$. Сразу же из коммутирования с w_{e_4}, $w_{e_3-e_4}$, $w_{e_1+e_2}$ из из соотношения $w_{\alpha_1} d_t w_{\alpha_1}^{-1} d_t = E$ получаем, что на этой части базиса d_t единична.

Нам осталось рассмотреть части базиса размера 8×8. Во-первых, рассмотрим часть $\{v_{e_1-e_2}, v_{e_2-e_1}, v_{e_1+e_2}, v_{-e_1-e_2}, v_{e_3-e_4}, v_{e_4-e_3}, v_{e_3+e_4}, v_{-e_3-e_4}\}$. Объединим ее временно с предыдущей частью базиса, получим матрица размера 12×12, у которой последний блок размера 4×4 единичен.

Из того, что d_t на этой части базиса коммутирует с $X_{e_1+e_2} = 2e_{v_{e_1+e_2}, v_{h_2}} - e_{v_{h_2}, v_{-e_1-e_2}}$ и с $X_{-e_1-e_2} = 2e_{v_{-e_1-e_2}, v_{h_2}} - e_{v_{h_2}, v_{e_1+e_2}}$, сразу получаем, что матрица разбивается на диагональные блоки относительно частей базиса $\{v_{e_1-e_2}, v_{e_2-e_1}, v_{e_3-e_4}, v_{e_4-e_3}, v_{e_3+e_4}, v_{-e_3-e_4}\}$ и $v_{e_1+e_2}, v_{-e_1-e_2}$, а на последней она единична.

Аналогично, из того, что d_t коммутирует с $X_{e_3-e_4} = 2e_{v_{e_3-e_4}, v_{h_3}} - e_{v_{e_3-e_4}, v_{h_2}} - e_{v_{e_3-e_4}, v_{h_4}} - e_{v_{h_3}, v_{e_4-e_3}}$ и с $X_{e_4-e_3} = 2e_{v_{e_4-e_3}, v_{h_3}} - e_{v_{e_4-e_3}, v_{h_2}} - e_{v_{e_4-e_3}, v_{h_4}} - e_{v_{h_3}, v_{e_3-e_4}}$, получаем, что матрица разбивается еще и на диагональные блоки относительно частей базиса $\{v_{e_1-e_2}, v_{e_2-e_1}, v_{e_3+e_4}, v_{-e_3-e_4}\}$ и $v_{e_3-e_4}, v_{e_4-e_3}$, а на последней снова единична.

Теперь воспользуемся коммутированием нашей матрицы с w_{e_4}, которая меняет местами пары корней e_3-e_4 и e_3+e_4, e_4-e_3 и $-e_3-e_4$. Сразу получим, что матрица d_t единична везде, кроме блока $\{v_{e_1-e_2}, v_{e_2-e_1}\}$. Этот блок мы пока не будем трогать, перейдем к последних не рассмотренных еще частях базиса $\{v_{e_1-e_3}, v_{e_3-e_1}, v_{e_1+e_3}, v_{-e_1-e_3}, v_{e_2-e_4}, v_{e_4-e_2}, v_{e_2+e_4}, v_{-e_2-e_4}\}$ и $\{v_{e_1-e_4}, v_{e_4-e_1}, v_{e_1+e_4}, v_{-e_1-e_4}, v_{e_2-e_3}, v_{e_3-e_2}, v_{e_2+e_3}, v_{-e_2-e_3}\}$.

Для начала d_t коммутирует с $X_{e_1+e_2}$, $X_{-e_1-e_2}$, $X_{e_3+e_4}$, $X_{-e_3-e_4}$, $X_{e_3-e_4}$, $X_{e_4-e_3}$. Напрямую из этого получаем, что d_t диагональна и имеет вид

$$\mathrm{diag}\,[d_1, d_2, d_1, d_2, d_2, d_1, d_2, d_1, d_1, d_2, d_1, d_2, d_2, d_1, d_2, d_1].$$

Из того, что $w_{e_1-e_2} d_t w_{e_1-e_2}^{-1} d_t = E$, получаем $d_1 d_2 = 1$.

Теперь временно ограничимся частью базиса $\{v_{e_1-e_2}, v_{e_2-e_1}, v_{e_2-e_3}, v_{e_3-e_2}, v_{e_1-e_3}, v_{e_3-e_1}\}$. Имеем соотношение $w_{e_2-e_3} d_t w_{e_2-e_3}^{-1} = d_t w_{e_1-e_2} w_{e_2-e_3} d_t w_{e_2-e_3}^{-1} w_{e_1-e_2}^{-1}$. Из него сразу же получается, что на блоке $\{v_{e_1-e_2}, v_{e_2-e_1}\}$ матрица d_t диагональна с числами $d_1^2, 1/d_1^2$ на диагонали.

Далее воспользуемся коммутированием с матрицей X_{e_4} и получим $d_{1,1} = d_1$. Таким образом, $d_t = h_{\alpha_1}(d_1)$.

Заметим, что если $t = 2$, то появляется еще соотношение

$$d_2 x_{e_2}(1) d_2^{-1} = x_{e_2}(1)^2,$$

откуда $d_2 = h_{\alpha_1}(2)$. Это сразу же показывает, что $x_1 = x_{\alpha_1}(1)$.

Искомое утверждение доказано.

Случай B_l, $l \geqslant 5$

В этом случае нам удобно будет рассмотреть $x = \varphi_2(x_{e_1-e_2}(1))$ и $y = \varphi_2(x_{e_3}(1))$.

Матрица x коммутирует с $h_{\alpha_1}(-1)$, $h_{\alpha_3}(-1), h_{\alpha_4}(-1), \dots, h_{\alpha_{l-1}}(-1)$, откуда следует, что она разбивается на диагональные блоки, соответствующие следующим частям базиса:

1. $\{v_{e_1-e_2}, v_{e_2-e_1}, v_{e_1+e_2}, v_{-e_1-e_2}, V_{h_1}, \dots, V_{h_l}\}$;
2. $\{v_{e_i-e_j}, v_{e_j-e_i}, v_{e_i+e_j}, v_{-e_i-e_j}\}$, $2 < i < j \leqslant l$;
3. $\{v_{e_1-e_i}, v_{e_i-e_1}, v_{e_1+e_i}, v_{-e_1-e_i}, v_{e_2-e_i}, v_{e_i-e_2}, v_{e_2+e_i}, v_{-e_2-e_i}\}$, $2 < i \leqslant l$;
4. $\{v_{e_1}, v_{-e_1}, v_{e_2}, v_{-e_2}\}$;
5. $\{v_{e_i}, v_{-e_i}\}$, $2 < i \leqslant l$.

Если на части базиса последнего типа матрица x имеет вид

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

то из соотношения $h_{\alpha_2}(-1) x h_{\alpha_2}(-1) x = E$ получим $c(a+d) = b(a+d) = 0$, откуда (так как $a + d \equiv 2 \mod J$) получаем $b = c = 0$. Тогда $a^2 = d^2 = 1$, откуда $a = d = 1$. Значит, на всех частях базиса пятого типа матрица x единична.

Теперь рассмотрим часть базиса четвертого типа.

Благодаря коммутированию с матрицей $w_{e_1+e_2}$ мы сразу получаем, что на этой части матрица x имеет вид

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_5 & x_6 & x_7 & x_8 \\ -x_8 & -x_7 & x_6 & x_5 \\ -x_4 & -x_3 & x_2 & x_1 \end{pmatrix}.$$

Добавим сюда часть базиса $\{v_{e_3}, v_{-e_3}\}$, на которой матрица x, как мы уже знаем, единична. На этой части базиса рассмотрим соотношение

$$xw_{e_1-e_2}w_{e_2-e_3}xw_{e_2-e_3}^{-1}w_{e_1-e_2}^{-1} = w_{e_2-e_3}xw_{e_2-e_3}^{-1}w_{e_1-e_2}w_{e_2-e_3}xw_{e_2-e_3}^{-1}w_{e_1-e_2}^{-1}x.$$

Из его позиции $(6,5)$ следует $x_2(1-x_1-x_6)=0$. Так как $1-x_1-x_6\equiv -1 \mod J$, то $x_2=0$. Совершенно аналогично из позиции $(5,6)$ получаем $x_5=0$. После этого из позиций $(5,5)$ и $(6,6)$ $x_1=x_6=1$. Из позиции $(1,4)$ $x_3(x_4+x_7)=0$, а так как $x_3\equiv -1 \mod J$, то $x_7=-x_4$. Из позиций $(6,2)$ и $(5,1)$ получим $x_4^2=x_3+x_3^2$ и $x_4^2=x_8+x_8^2$, откуда $(x_3-x_8)(1+x_3+x_8)=0$. Так как $x_3-x_8\equiv -1 \mod J$, то $x_8=-1-x_3$.

Таким образом, пока мы получили, что на части базиса четвертого типа матрица x имеет вид

$$\begin{pmatrix} 1 & 0 & x_3 & x_4\\ 0 & 1 & -x_4 & -1-x_3\\ 1+x_3 & x_4 & 1 & 0\\ -x_4 & -x_3 & 0 & 1 \end{pmatrix}.$$

Благодаря тому, что элементы группы Вейля, оставляющие на месте α_1, транзитивно действуют на корнях одной длины, ортогональных α_1, мы получаем, что на всех частях базиса второго типа и на всех частях базиса третьего типа матрица x выглядит одинаково.

Рассмотрим какую-нибудь из частей базиса второго типа (например, $\{v_{e_3-e_4}, v_{e_4-e_3}, v_{e_3+e_4}, v_{-e_3-e_4}\}$). Из того, что матрица x коммутирует с w_{e_3}, w_{e_4}, $w_{e_3-e_4}$ (в общем случае — с w_{e_i}, w_{e_j}, $w_{e_i-e_j}$), следует, что x имеет вид

$$\begin{pmatrix} x_5 & x_6 & x_7 & -x_7\\ x_6 & x_5 & -x_7 & x_7\\ x_7 & -x_7 & x_5 & x_6\\ -x_7 & x_7 & x_6 & x_5 \end{pmatrix}.$$

Воспользуемся соотношением $h_{e_2-e_3}(-1)xh_{e_2-e_3}(-1)x=E$ и получим (на месте $(1,3)$) $2x_7(x_5-x_6)=0$, откуда, так как $x_5-x_6\equiv 1 \mod J$, следует $x_7=0$. После этого на месте $(1,2)$ получается $2x_5x_6=0$, откуда $x_6=0$, и далее, очевидно, $x_5=0$. Таким образом, мы уже получили, что на частях базиса второго типа матрица x единична.

Перейдем к части базиса третьего типа (аналогично, мы можем взять $i=3$).

Благодаря коммутированию матрицы x с $w_{e_1+e_2}$ и w_{e_i} мы получаем, что x на этой части базиса имеет вид

$$\begin{pmatrix} x_5 & x_6 & x_7 & x_8 & x_9 & x_{10} & x_{11} & x_{12}\\ x_{13} & x_{14} & x_{15} & x_{16} & x_{17} & x_{18} & x_{19} & x_{20}\\ x_7 & x_8 & x_5 & x_6 & x_{11} & x_{12} & x_9 & x_{10}\\ x_{15} & x_{16} & x_{13} & x_{14} & x_{19} & x_{20} & x_{17} & x_{18}\\ -x_{18} & -x_{17} & -x_{20} & -x_{19} & x_{14} & x_{13} & x_{16} & x_{15}\\ -x_{10} & -x_9 & -x_{12} & -x_{11} & x_6 & x_5 & x_8 & x_7\\ -x_{20} & -x_{19} & -x_{18} & -x_{17} & x_{16} & x_{15} & x_{14} & x_{13}\\ -x_{12} & -x_{11} & -x_{10} & -x_9 & x_8 & x_7 & x_6 & x_5 \end{pmatrix}.$$

Теперь рассмотрим оставшуюся часть базиса $\{v_{e_1-e_2}, v_{e_2-e_1}, v_{e_1+e_2}, v_{-e_1-e_2}, V_{h_1}, \dots, V_{h_l}\}$. Благодаря коммутированию с матрицами $w_{\alpha_3}, \dots, w_{\alpha_l}$ матрица x единична на части базиса

$\{V_{h_3}, \dots, V_{h_l}\}$. Таким образом, мы можем рассматривать в данном случае матрицу размера 6×6.

Коммутирование с матрицей $w_{e_1+e_2}$ даст нам следующий вид:

$$\begin{pmatrix} x_{21} & x_{22} & x_{23} & -x_{23} & -2x_{24} & x_{24} \\ x_{25} & x_{26} & x_{27} & -x_{27} & -2x_{28} & x_{28} \\ x_{29} & x_{30} & x_{31} & x_{32} & x_{33} & x_{34} \\ -x_{29} & -x_{30} & x_{32} & x_{31} & -x_{33} & x_{33}+x_{34} \\ x_{35} & x_{36} & x_{37} & x_{38} & x_{39} & x_{40} \\ 0 & 0 & x_{37}+x_{38} & x_{37}+x_{38} & 0 & 2x_{40}+x_{39} \end{pmatrix}.$$

Таким образом, для матрицы x мы пока имеем 40 неизвестных $x_1, \dots, x_{40}$.

Теперь рассмотрим матрицу y. Она коммутирует с $h_{\alpha_1}(-1)$, $h_{\alpha_2}(-1)h_{\alpha_3}(-1)$, $h_{\alpha_4}(-1)$, $h_{\alpha_5}(-1)$, $\dots$, $h_{\alpha_{l-1}}(-1)$ и разбивается на следующие блоки:

1. $\{v_{e_3}, v_{-e_3}, V_{h_1}, \dots, V_{h_l}\}$;
2. $\{v_{e_3-e_i}, v_{e_i-e_3}, v_{e_3+e_i}, v_{-e_3-e_i}, v_{e_i}, v_{-e_i}\}$, $i \neq 3$;
3. $\{v_{e_i-e_j}, v_{e_j-e_i}, v_{e_i+e_j}, v_{-e_i-e_j}\}$, $1 \leqslant i < j \leqslant l$; $i, j \neq 3$.

На частях базиса третьего типа матрица y единична (это доказывается точно так же, как и про матрицу x; мы здесь пользуемся коммутированием с w_{e_i}, w_{e_j}, $w_{e_i-e_j}$ и соотношением $h_{e_2-e_3}(-1)yh_{e_2-e_3}(-1)y = E$).

Понятно, что на всех частях базиса второго типа матрица y выглядит одинаково (благодаря тому, что элементы группы Вейля, не двигающие e_3, транзитивно действуют на корни e_i, $i \neq 3$).

Благодаря коммутированию y с w_{e_3} матрица на данной части базиса имеет вид

$$\begin{pmatrix} y_1 & y_2 & y_3 & y_4 & y_5 & y_6 \\ y_7 & y_8 & y_9 & y_{10} & y_{11} & y_{12} \\ y_3 & y_4 & y_1 & y_2 & -y_6 & -y_5 \\ y_9 & y_{10} & y_7 & y_8 & -y_{12} & -y_{11} \\ y_{13} & y_{14} & y_{15} & y_{16} & y_{17} & y_{18} \\ -y_{15} & -y_{16} & -y_{13} & -y_{14} & y_{18} & y_{17} \end{pmatrix}.$$

На части базиса первого типа, благодаря коммутированию матрицы y со всеми w_{α_j}, не сдвигающими e_3, на элементах базиса $V_{h_1}, V_{h_5}, \dots, V_{h_l}$ матрица y единична. На части базиса $\{v_{e_3}, v_{-e_3}, V_{h_2}, V_{h_3}, V_{h_4}\}$ воспользуемся дополнительно тем, что $h_{e_2-e_3}(-1)yh_{e_2-e_3}(-1)y = E$, $yw_{e_4}yw_{e_4}^{-1}y = w_{e_4}$, а также, как в предыдущем пункте, произведем замену базиса таким образом, чтобы на местах (V_{h_3}, v_{e_3}) и (V_{h_4}, v_{e_3}) стояли нули, на местах (V_{h_3}, v_{-e_3}), (V_{h_4}, v_{-e_3}) — -1. Тогда получим вид y:

$$\begin{pmatrix} 1 & y_{19} & y_{19}-y_{19}^2 & y_{19}^2-y_{19} & 0 \\ 0 & -y_{19} & y_{19}^2-1 & 1-y_{19}^2 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1+y_{19} & -y_{19} & 0 \\ 0 & -1 & 1+y_{19} & -1-y_{19} & 1 \end{pmatrix}.$$

Значит, для матрицы y мы имеем 19 переменных $y_1, \dots, y_{19}$.

С помощью дополнительной замены базиса из предыдущих пунктов добьемся $x_{35} = 0$, $x_{36} = -1$.

Теперь воспользуемся коммутированием матриц x и y. Во-первых, рассмотрим часть базиса $\{v_{e_1-e_2}, v_{e_2-e_1}, v_{e_1+e_2}, v_{-e_1-e_2}, v_{e_3}, v_{-e_3}, V_{h_1}, V_{h_2}, V_{h_3}, V_{h_4}\}$. На ней матрица y имеет только одно неизвестное $y_{19} \equiv -1 \mod J$. Благодаря данному соотношению $x_{37} + x_{38} = 0$ и $x_{39} + 2x_{40} = 1$.

Теперь рассмотрим часть базиса $v_{e_1-e_2}, v_{e_2-e_1}, v_{e_1+e_2}, v_{-e_1-e_2}, v_{e_1}, v_{-e_1}, v_{e_2}, v_{-e_2}, V_{h_1}, V_{h_2}$. Так как матрица $x_{e_1}(1)$ сопряжена к матрице $x_{e_3}(1)$ с помощью элемента группы Вейля, то мы легко можем рассмотреть $\varphi_2(x_{e_1}(1)) = y'$. Матрица y' имеет те же неизвестные, что и y. Матрицы x и y' тоже коммутируют. Рассмотрим это соотношение на выписанной части базиса.

Матрица x выглядит как

$$\begin{pmatrix} x_{21} & x_{22} & x_{23} & -x_{23} & 0 & 0 & 0 & 0 & -2x_{24} & x_{24} \\ x_{25} & x_{26} & x_{27} & -x_{27} & 0 & 0 & 0 & 0 & -2x_{28} & x_{28} \\ x_{29}x_{30} & x_{31} & x_{32} & 0 & 0 & 0 & 0 & x_{33} & x_{34} & \\ -x_{29} & -x_{30} & x_{32} & x_{31} & 0 & 0 & 0 & 0 & -x_{33} & x_{33}+x_{34} \\ 0 & 0 & 0 & 0 & 1 & 0 & x_3 & x_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -x_4 & 1-x_3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1+x_3 & x_4 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -x_4 & -x_3 & 0 & 1 & 0 & 0 \\ 0 & -1 & x_{37}-x_{37} & 0 & 0 & 0 & 0 & 1-2x_{40} & x_{40} & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

а матрица y' — как

$$\begin{pmatrix} y_1 & y_2 & y_3 & y_4 & 0 & 0 & y_5 & y_6 & 0 & 0 \\ y_7 & y_8 & y_9 & y_{10} & 0 & 0 & y_{11} & y_{12} & 0 & 0 \\ y_3 & y_4 & y_1 & y_2 & 0 & 0 & -y_6 & -y_5 & 0 & 0 \\ y_9 & y_{10} & y_7 & y_8 & 0 & 0 & -y_{12} & -y_{11} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & y_{19} & 0 & 0 & y_{19}^2-y_{19} & 0 \\ 0 & 0 & 0 & 0 & 0 & -y_{19} & 0 & 0 & y_{19}^2-1 & 0 \\ y_{13} & y_{14} & y_{15} & y_{16} & 0 & 0 & y_{17} & y_{18} & 0 & 0 \\ -y_{15} & -y_{16} & -y_{13} & -y_{14} & 0 & 0 & y_{18} & y_{17} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1+y_{19} & -y_{19} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Позиция $(5, 10)$ условия коммутирования этих матриц дает $x_{40}(y_{19} - y_{19}^2) = 0$, откуда $x_{40} = 0$. Позиция $(9, 6)$ дает $x_3(1+y_{19}) = 0$, откуда $y_{19} = -1$. Если рассмотреть соотношение $h_{e_2-e_3}(-1)xh_{e_2-e_3}(-1)x = E$, то сразу получим $x_4 = 0$, $x_3 = 1$. Теперь из коммутирования (пятая строка) $y_{13} = 0$, $y_{14} = -2$, $y_{15} = 2x_{37}$, $y_{16} = -2x_{37}$, $y_{17} = 1$, $y_{18} = 0$, (шестой столбец) $y_6 = -2x_{24}$, $y_{12} = -2x_{28}$, $y_5 = -x_{33}$, $y_{11} = x_{33}$. Из седьмой строки соотношения $h_{e_2-e_3}(-1)xh_{e_2-e_3}(-1)x = E$ получаем: $x_{25} = 2x_{37}x_{29}$, $x_{26} = 1+2x_{37}x_{30}$, $x_{27} = x_{37}(-1+x_{31} - x_{32})$, $x_{28} = -x_{33}x_{37}$, $x_{29}(-x_{21} - 2x_{30}x_{37} + x_{32} - x_{31}) = 0$, откуда $x_{29} = 0$, далее $x_{21} = 1$.

Из позиции $(2, 10)$ соотношения

$$Comm : (y'w_{e_1-e_2}y'w_{e_1-e_2}^{-1} = w_{e_2}x^2w_{e_2}^{-1}w_{e_1-e_2}y'w_{e_1-e_2}^{-1}y')$$

получаем $x_{34} = x_{33}$, а из позиции $(2,9)$ $x_{33}(-1-4x_{37}x_{30}-2x_{31}+2x_{32}) = 0$, откуда $x_{33} = 0$.

Теперь снова из соотношения коммутирования $y_9x_{24} = x_{32}x_{24} = x_{37}x_{24} = 0$, откуда $y_9 = x_{32} = x_{37} = 0$, далее $x_{31} = 1$, $y_7 = y_{10} = y_3 = x_{23} = x_{30} = 0$, $y_1 = y_8 = 1$. Из $h_{e_2-e_3}(-1)xh_{e_2-e_3}(-1)x = E$ получим $x_{24} = x_{22}$, а из $h_{e_1-e_2}(-1)y'h_{e_1-e_2}(-1)y' = E - y_2 = 0$, $y_4 = -2x_{22}$. Наконец, из соотношения $Comm$ увидим, что $x_{22} = -1$, и мы избавились от переменных.

Теперь матрица y' совпадает с $x_{e_1}(1)$ на рассматриваемой части базиса, а значит, и на всем базисе. Соответственно, матрица y совпадает с $x_{e_3}(1)$.

Осталось только найти вид матрицы x на частях базиса третьего типа, что легко получается из соотношений коммутирования и того, что матрица x^2 уже известна.

Аналогично предыдущим пунктам можно убедиться, что $\varphi_2(h_\alpha(t)) = h_\alpha(s)$ для каждого $t \in R^*$ и $\alpha \in \Phi$.

1.4.3 Система корней F_4

Выпишем матрицы w_i, $i = 1, \dots, 4$:

$$\begin{aligned}
w_1 = &-e_{\alpha_1,-\alpha_1} - e_{-\alpha_1,\alpha_1} + e_{\alpha_2,\alpha_5} + e_{-\alpha_2,-\alpha_5} - e_{\alpha_5,\alpha_2} - e_{-\alpha_5,\alpha_2} + \\
&+ e_{\alpha_3,\alpha_3} + e_{-\alpha_3,-\alpha_3} + e_{\alpha_4,\alpha_4} + e_{-\alpha_4,-\alpha_4} + e_{\alpha_6,\alpha_8} + e_{-\alpha_6,-\alpha_8} - e_{\alpha_8,\alpha_6} - e_{-\alpha_8,-\alpha_6} + \\
&+ e_{\alpha_7,\alpha_7} + e_{-\alpha_7,-\alpha_7} + e_{\alpha_9,\alpha_{11}} + e_{-\alpha_9,-\alpha_{11}} - e_{\alpha_{11},\alpha_9} - e_{-\alpha_{11},-\alpha_9} + \\
&+ e_{\alpha_{10},\alpha_{12}} + e_{-\alpha_{10},-\alpha_{12}} - e_{\alpha_{12},\alpha_{10}} - e_{-\alpha_{12},-\alpha_{10}} + e_{\alpha_{13},\alpha_{15}} + e_{-\alpha_{13},-\alpha_{15}} - e_{\alpha_{15},\alpha_{13}} - e_{-\alpha_{15},-\alpha_{13}} + \\
&+ e_{\alpha_{14},\alpha_{14}} + e_{-\alpha_{14},-\alpha_{14}} + e_{\alpha_{16},\alpha_{18}} + e_{-\alpha_{16},-\alpha_{18}} - e_{\alpha_{18},\alpha_{16}} - e_{-\alpha_{18},-\alpha_{16}} + \\
&+ e_{\alpha_{17},\alpha_{17}} + e_{-\alpha_{17},-\alpha_{17}} + e_{\alpha_{19},\alpha_{19}} + e_{-\alpha_{19},-\alpha_{19}} + e_{\alpha_{20},\alpha_{20}} + e_{-\alpha_{20},-\alpha_{20}} + \\
&+ e_{\alpha_{21},\alpha_{21}} + e_{-\alpha_{21},-\alpha_{21}} + e_{\alpha_{22},\alpha_{22}} + e_{-\alpha_{22},-\alpha_{22}} + +e_{\alpha_{23},\alpha_{24}} + e_{-\alpha_{23},-\alpha_{24}} - \\
&- e_{\alpha_{24},\alpha_{23}} - e_{-\alpha_{24},-\alpha_{23}} - e_{h_1,h_1} + e_{h_1,h_2} + e_{h_2,h_2} + e_{h_3,h_3} + e_{h_4,h_4};
\end{aligned}$$

$$\begin{aligned}
w_2 = &-e_{\alpha_2,-\alpha_2} - e_{-\alpha_2,\alpha_2} + e_{\alpha_1,\alpha_5} + e_{-\alpha_1,-\alpha_5} - e_{\alpha_5,\alpha_1} - e_{-\alpha_5,\alpha_1} + \\
&- e_{\alpha_3,\alpha_6} - e_{-\alpha_3,-\alpha_6} + e_{\alpha_6,\alpha_3} + e_{-\alpha_6,-\alpha_3} + e_{\alpha_4,\alpha_4} + e_{-\alpha_4,-\alpha_4} + \\
&+ e_{\alpha_7,\alpha_9} + e_{-\alpha_7,-\alpha_9} - e_{\alpha_9,\alpha_7} - e_{-\alpha_9,-\alpha_7} + e_{\alpha_8,\alpha_8} + e_{-\alpha_8,-\alpha_8} + e_{\alpha_{10},\alpha_{10}} + e_{-\alpha_{10},-\alpha_{10}} + e_{\alpha_{11},\alpha_{11}} + e_{-\alpha_{11},-\alpha_{11}} + \\
&+ e_{\alpha_{12},\alpha_{14}} + e_{-\alpha_{12},-\alpha_{14}} - e_{\alpha_{14},\alpha_{12}} - e_{-\alpha_{14},-\alpha_{12}} + e_{\alpha_{13},\alpha_{13}} + e_{-\alpha_{13},-\alpha_{13}} + \\
&+ e_{\alpha_{15},\alpha_{17}} + e_{-\alpha_{15},-\alpha_{17}} - e_{\alpha_{17},\alpha_{15}} - e_{-\alpha_{17},-\alpha_{15}} + e_{\alpha_{16},\alpha_{16}} + e_{-\alpha_{16},-\alpha_{16}} + \\
&+ e_{\alpha_{18},\alpha_{20}} + e_{-\alpha_{18},-\alpha_{20}} - e_{\alpha_{20},\alpha_{18}} - e_{-\alpha_{20},-\alpha_{18}} + e_{\alpha_{19},\alpha_{19}} + e_{-\alpha_{19},-\alpha_{19}} + \\
&+ e_{\alpha_{21},\alpha_{21}} + e_{-\alpha_{21},-\alpha_{21}} + e_{\alpha_{22},\alpha_{23}} + e_{-\alpha_{22},-\alpha_{23}} - e_{\alpha_{23},\alpha_{22}} - e_{-\alpha_{23},-\alpha_{22}} + \\
&+ e_{\alpha_{24},\alpha_{24}} + e_{-\alpha_{24},-\alpha_{24}} + e_{h_1,h_1} + e_{h_2,h_1} - e_{h_2,h_2} + e_{h_2,h_3} + e_{h_3,h_3} + e_{h_4,h_4};
\end{aligned}$$

$$\begin{aligned}
w_3 = &\ e_{\alpha_1,-\alpha_1} + e_{-\alpha_1,\alpha_1} + e_{\alpha_2,\alpha_{10}} + e_{-\alpha_2,-\alpha_{10}} + e_{\alpha_{10},\alpha_2} + e_{-\alpha_{10},\alpha_2} - \\
&- e_{\alpha_3,-\alpha_3} - e_{-\alpha_3,\alpha_3} + e_{\alpha_4,\alpha_7} + e_{-\alpha_4,-\alpha_7} - e_{\alpha_7,\alpha_4} - e_{-\alpha_7,-\alpha_4} + \\
&+ e_{\alpha_5,\alpha_{12}} + e_{-\alpha_5,-\alpha_{12}} + e_{\alpha_{12},\alpha_5} + e_{-\alpha_{12},-\alpha_5} - e_{\alpha_6,\alpha_6} - e_{-\alpha_6,-\alpha_6} - e_{\alpha_8,\alpha_8} - e_{-\alpha_8,-\alpha_8} + \\
&+ e_{\alpha_9,\alpha_{13}} + e_{-\alpha_9,-\alpha_{13}} - e_{\alpha_{13},\alpha_9} - e_{-\alpha_{13},-\alpha_9} + e_{\alpha_{11},\alpha_{15}} + e_{-\alpha_{11},-\alpha_{15}} - e_{\alpha_{15},\alpha_{11}} - e_{-\alpha_{15},-\alpha_{11}} + \\
&+ e_{\alpha_{14},\alpha_{14}} + e_{-\alpha_{14},-\alpha_{14}} + e_{\alpha_{16},\alpha_{16}} + e_{-\alpha_{16},-\alpha_{16}} + \\
&+ e_{\alpha_{17},\alpha_{19}} + e_{-\alpha_{17},-\alpha_{19}} - e_{\alpha_{19},\alpha_{17}} - e_{-\alpha_{19},-\alpha_{17}} + e_{\alpha_{18},\alpha_{18}} + e_{-\alpha_{18},-\alpha_{18}} + \\
&+ e_{\alpha_{20},\alpha_{22}} + e_{-\alpha_{20},-\alpha_{22}} + e_{\alpha_{22},\alpha_{20}} + e_{-\alpha_{22},-\alpha_{20}} - e_{\alpha_{21},\alpha_{21}} - e_{-\alpha_{21},-\alpha_{21}} + e_{\alpha_{23},\alpha_{23}} + e_{-\alpha_{23},-\alpha_{23}} + \\
&+ e_{\alpha_{24},\alpha_{24}} + e_{-\alpha_{24},-\alpha_{24}} + e_{h_1,h_1} + e_{h_2,h_2} + 2e_{h_3,h_2} - e_{h_3,h_3} + e_{h_3,h_4} + e_{h_4,h_4};
\end{aligned}$$

$$
\begin{aligned}
w_4 = e_{\alpha_1,-\alpha_1} + e_{-\alpha_1,\alpha_1} + e_{\alpha_2,-\alpha_2} + e_{-\alpha_2,\alpha_2} - e_{\alpha_3,\alpha_7} - e_{-\alpha_3,-\alpha_7} + e_{\alpha_7,\alpha_3} + e_{-\alpha_7,\alpha_3} - \\
- e_{\alpha_4,-\alpha_4} - e_{-\alpha_4,\alpha_4} + e_{\alpha_5,\alpha_5} + e_{-\alpha_5,-\alpha_5} + e_{\alpha_6,\alpha_9} + e_{-\alpha_6,-\alpha_9} - e_{\alpha_9,\alpha_6} - e_{-\alpha_9,-\alpha_6} + \\
+ e_{\alpha_8,\alpha_{11}} + e_{-\alpha_8,-\alpha_{11}} - e_{\alpha_{11},\alpha_8} - e_{-\alpha_{11},-\alpha_8} + e_{\alpha_{10},\alpha_{16}} + e_{-\alpha_{10},-\alpha_{16}} + e_{\alpha_{16},\alpha_{10}} + e_{-\alpha_{16},-\alpha_{10}} + \\
+ e_{\alpha_{12},\alpha_{18}} + e_{-\alpha_{12},-\alpha_{18}} + e_{\alpha_{18},\alpha_{12}} + e_{-\alpha_{18},-\alpha_{12}} - -e_{\alpha_{13},\alpha_{13}} - e_{-\alpha_{13},-\alpha_{13}} - e_{\alpha_{15},\alpha_{15}} - e_{-\alpha_{15},-\alpha_{15}} - \\
- e_{\alpha_{17},\alpha_{17}} - e_{-\alpha_{17},-\alpha_{17}} + e_{\alpha_{14},\alpha_{20}} + e_{-\alpha_{14},-\alpha_{20}} + e_{\alpha_{20},\alpha_{14}} + e_{-\alpha_{20},-\alpha_{14}} + \\
+ e_{\alpha_{19},\alpha_{21}} + e_{-\alpha_{19},-\alpha_{21}} - e_{\alpha_{21},\alpha_{19}} - e_{-\alpha_{21},-\alpha_{19}} + e_{\alpha_{22},\alpha_{22}} + e_{-\alpha_{22},-\alpha_{22}} + e_{\alpha_{23},\alpha_{23}} + e_{-\alpha_{23},-\alpha_{23}} + \\
+ e_{\alpha_{24},\alpha_{24}} + e_{-\alpha_{24},-\alpha_{24}} + e_{h_1,h_1} + e_{h_2,h_2} + e_{h_3,h_3} + e_{h_4,h_3} - e_{h_4,h_4}.
\end{aligned}
$$

Кроме того, $x_{\alpha_1}(t) = E + tX_1 + t^2X_1^2/2$, где

$$
\begin{aligned}
X_1 = 2e_{\alpha_1,h_1} - e_{\alpha_1,h_2} - e_{h_1,-\alpha_1} + e_{\alpha_5,\alpha_2} - e_{-\alpha_2,-\alpha_5} + e_{\alpha_8,\alpha_6} - e_{-\alpha_6,-\alpha_8} + \\
+ e_{\alpha_{11},\alpha_9} - e_{-\alpha_9,-\alpha_{11}} + e_{\alpha_{12},\alpha_{10}} - e_{-\alpha_{10},-\alpha_{12}} + e_{\alpha_{15},\alpha_{13}} - e_{-\alpha_{13},-\alpha_{15}} + \\
+ e_{\alpha_{18},\alpha_{16}} - e_{-\alpha_{16},-\alpha_{18}} + e_{\alpha_{24},\alpha_{23}} - e_{-\alpha_{23},-\alpha_{24}};
\end{aligned}
$$

$x_{\alpha_3}(t) = E + tX_3 + t^2X_3^2/2$, где

$$
\begin{aligned}
X_3 = -2e_{\alpha_3,h_2} + 2e_{\alpha_3,h_3} - e_{\alpha_3,h_4} - e_{h_3,-\alpha_3} + e_{\alpha_7,\alpha_4} - e_{-\alpha_4,-\alpha_7} + \\
+ e_{\alpha_{13},\alpha_9} - e_{-\alpha_9,-\alpha_{13}} + e_{\alpha_{15},\alpha_{11}} - e_{-\alpha_{11},-\alpha_{15}} + e_{\alpha_{19},\alpha_{17}} - e_{-\alpha_{17},-\alpha_{19}} - \\
- 2e_{\alpha_6,\alpha_2} + e_{-\alpha_2,-\alpha_6} - e_{\alpha_{10},\alpha_6} + 2e_{-\alpha_6,-\alpha_{10}} - 2e_{\alpha_8,\alpha_5} + e_{-\alpha_5,-\alpha_8} - \\
- e_{\alpha_{12},\alpha_8} + 2e_{-\alpha_8,\alpha_{12}} - 2e_{\alpha_{21},\alpha_{20}} + e_{-\alpha_{20},-\alpha_{21}} - e_{\alpha_{22},\alpha_{21}} + 2e_{-\alpha_{21},-\alpha_{22}}.
\end{aligned}
$$

Нам интересны образы элементов $x_{\alpha_i}(t)$. Пусть $\varphi_2(x_{\alpha_1}(1)) = x_1 = (y_{i,j})$. Так как x_1 коммутирует со всеми $h_{\alpha_i}(-1)$, $i = 1, 3, 4$, а также с w_3, w_4 и w_{14}, то с помощью прямых вычислений получим:

1. Матрица x_1 может быть разложена в следующие восемь диагональных блоков:

$$
\begin{aligned}
&B_1 = \{v_1, v_{-1}, v_{14}, v_{-14}, v_{20}, v_{-20}, v_{22}, v_{-22}, V_1, V_2, V_3, V_4\};\\
&B_2 = \{v_2, v_{-2}, v_5, v_{-5}, v_{10}, v_{-10}, v_{16}, v_{-16}, v_{18}, v_{-18}, v_{23}, v_{-23}, v_{24}, v_{-24}\};\\
&B_3 = \{v_3, v_{-3}, v_{21}, v_{-21}\};\\
&B_4 = \{v_4, v_{-4}, v_{17}, v_{-17}\};\\
&B_5 = \{v_6, v_{-6}, v_8, v_{-8}\};\\
&B_6 = \{v_7, v_{-7}, v_{19}, v_{-19}\};\\
&B_7 = \{v_9, v_{-9}, v_{11}, v_{-11}\};\\
&B_8 = \{v_{13}, v_{-13}, v_{15}, v_{-15}\}.
\end{aligned}
$$

2. На блоке B_1 матрица x_1 имеет вид

$$
\begin{pmatrix}
y_1 & y_2 & -y_3 & y_3 & -y_3 & y_3 & -y_3 & y_3 & -2y_4 & y_4 & 0 & 0\\
y_5 & y_6 & -y_7 & y_7 & -y_7 & y_7 & -y_7 & y_7 & -2y_8 & y_8 & 0 & 0\\
y_9 & y_{10} & y_{11} & y_{12} & -y_{13} & y_{13} & -y_{13} & y_{13} & -2y_{14}+2y_{15} & y_{14} & 0 & -y_{15}\\
-y_9 & -y_{10} & y_{12} & y_{11} & y_{13} & -y_{13} & y_{13} & -y_{13} & 2y_{14}-2y_{15} & -y_{14}+2y_{15} & 0 & y_{15}\\
y_9 & y_{10} & -y_{13} & y_{13} & y_{11} & y_{12} & -y_{13} & y_{13} & 2(-y_{14}+y_{15}) & y_{14} & -y_{15} & y_{15}\\
-y_9 & -y_{10} & y_{13} & -y_{13} & y_{12} & y_{11} & y_{13} & -y_{13} & 2(y_{14}-y_{15}) & -y_{14}+2y_{15} & -y_{15} & y_{15}\\
y_9 & y_{10} & -y_{13} & y_{13} & -y_{13} & y_{13} & y_{11} & y_{12} & 2(-y_{14}+y_{15}) & -y_{14}+2y_{15} & y_{15} & 0\\
-y_9 & -y_{10} & y_{13} & -y_{13} & y_{13} & -y_{13} & y_{12} & y_{11} & 2(y_{14}-y_{15}) & -y_{14} & y_{15} & 0\\
y_{16} & y_{17} & -y_{18} & y_{18} & -y_{18} & y_{18} & -y_{18} & y_{18} & y_{19}-2y_{20} & y_{20} & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & y_{20} & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & y_{20} & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & y_{20}
\end{pmatrix}.
$$

3. На блоке B_2 она имеет вид

$$
\left(\begin{array}{cccccccccccccccc}
y_{21} & y_{22} & -y_{23} & -y_{24} & -y_{25} & -y_{26} & y_{27} & y_{28} & -y_{25} & -y_{26} & y_{27} & y_{28} & y_{28} & y_{27} & y_{26} & y_{25}\\
y_{29} & y_{30} & -y_{31} & -y_{32} & -y_{25} & -y_{33} & y_{34} & y_{35} & -y_{25} & -y_{33} & y_{34} & y_{35} & y_{35} & y_{34} & y_{33} & y_{28}\\
y_{32} & y_{31} & y_{30} & y_{29} & -y_{35} & -y_{34} & -y_{33} & -y_{25} & -y_{35} & -y_{34} & -y_{33} & -y_{25} & -y_{25} & -y_{33} & y_{34} & y_{35}\\
y_{24} & y_{23} & y_{22} & y_{21} & -y_{28} & -y_{27} & -y_{26} & -y_{25} & -y_{28} & -y_{27} & -y_{26} & -y_{25} & -y_{25} & -y_{26} & y_{27} & y_{28}\\
-y_{25} & -y_{26} & y_{27} & y_{28} & y_{21} & y_{22} & -y_{23} & -y_{24} & -y_{25} & -y_{26} & y_{27} & y_{28} & y_{28} & y_{27} & y_{26} & y_{25}\\
-y_{25} & -y_{33} & y_{34} & y_{35} & y_{29} & y_{30} & -y_{31} & -y_{32} & -y_{25} & -y_{33} & y_{34} & y_{35} & y_{35} & y_{34} & y_{33} & y_{25}\\
-y_{35} & -y_{34} & -y_{33} & -y_{25} & y_{32} & y_{31} & y_{30} & y_{29} & -y_{35} & -y_{34} & -y_{33} & -y_{25} & -y_{25} & -y_{33} & y_{34} & y_{35}\\
-y_{28} & -y_{27} & -y_{26} & -y_{25} & y_{24} & y_{23} & y_{22} & y_{21} & -y_{28} & -y_{27} & -y_{26} & -y_{25} & -y_{25} & -y_{26} & y_{27} & y_{28}\\
-y_{25} & -y_{26} & y_{27} & y_{28} & -y_{25} & -y_{26} & y_{27} & y_{28} & y_{21} & y_{22} & -y_{23} & -y_{24} & y_{28} & y_{27} & y_{26} & y_{25}\\
-y_{25} & -y_{33} & y_{34} & y_{35} & -y_{25} & -y_{33} & y_{34} & y_{35} & y_{29} & y_{30} & -y_{31} & -y_{32} & y_{35} & y_{34} & y_{33} & y_{25}\\
-y_{35} & -y_{34} & -y_{33} & -y_{25} & -y_{35} & -y_{34} & -y_{33} & -y_{25} & y_{32} & y_{31} & y_{30} & y_{29} & -y_{25} & -y_{33} & y_{34} & y_{35}\\
-y_{28} & -y_{27} & -y_{26} & -y_{25} & -y_{28} & -y_{27} & -y_{26} & -y_{25} & y_{24} & y_{23} & y_{22} & y_{21} & -y_{25} & -y_{26} & y_{27} & y_{28}\\
-y_{28} & -y_{27} & -y_{26} & -y_{25} & -y_{28} & -y_{27} & -y_{26} & -y_{25} & -y_{28} & -y_{27} & -y_{26} & -y_{25} & y_{21} & y_{22} & -y_{23} & -y_{24}\\
-y_{35} & -y_{34} & -y_{33} & -y_{25} & -y_{35} & -y_{34} & -y_{33} & -y_{25} & -y_{35} & -y_{34} & -y_{33} & -y_{25} & y_{29} & y_{30} & -y_{31} & -y_{32}\\
y_{25} & y_{33} & -y_{34} & -y_{35} & y_{25} & y_{33} & -y_{34} & -y_{35} & y_{25} & y_{33} & -y_{34} & -y_{35} & y_{32} & y_{31} & y_{30} & y_{29}\\
y_{25} & y_{26} & -y_{27} & -y_{28} & y_{25} & y_{26} & -y_{27} & -y_{28} & y_{25} & y_{26} & -y_{27} & -y_{28} & y_{24} & y_{23} & y_{22} & y_{21}
\end{array}\right).
$$

4. На блоках B_3, B_4, B_6 —

$$
\begin{pmatrix}
y_{36} & y_{37} & y_{38} & y_{38}\\
y_{37} & y_{36} & y_{38} & y_{38}\\
-y_{38} & -y_{38} & y_{36} & y_{37}\\
-y_{38} & -y_{38} & y_{37} & y_{36}
\end{pmatrix}.
$$

5. Наконец, на блоках B_5, B_7, B_8 она имеет вид

$$
\begin{pmatrix}
y_{39} & y_{40} & y_{41} & y_{42}\\
y_{43} & y_{44} & y_{45} & y_{46}\\
-y_{46} & -y_{45} & y_{44} & y_{43}\\
-y_{42} & -y_{41} & y_{39} & y_{40}
\end{pmatrix}.
$$

Теперь пусть $\varphi_2(x_{\alpha_4}(1)) = x_4 = (z_{i,j})$. Так как x_4 коммутирует со всеми $h_{\alpha_i}(-1)$, $i = 1, 2, 4$, и w_1, w_2, а также для w_{13} имеет место $w_{13}x_4w_{13}^{-1} = x_4^{-1} = h_{\alpha_3}(-1)x_4h_{\alpha_3}(-1)$, то с помощью прямых вычислений получим:

1. Матрица x_4 может быть разложена в следующие восемь диагональных блоков:

$$
\begin{aligned}
B_1' &= \{v_4, v_{-4}, V_1, V_2, V_3, V_4\};\\
B_2' &= \{v_1, v_{-1}, v_{14}, v_{-14}, v_{17}, v_{-17}, v_{20}, v_{-20}, v_{22}, v_{-22}\};\\
B_3' &= \{v_2, v_{-2}, v_{10}, v_{-10}, v_{13}, v_{-13}, v_{16}, v_{-16}, v_{24}, v_{-24}\};\\
B_4' &= \{v_5, v_{-5}, v_{12}, v_{-12}, v_{15}, v_{-15}, v_{18}, v_{-18}, v_{23}, v_{-23}\};\\
B_5' &= \{v_6, v_{-6}, v_9, v_{-9}\};\\
B_6' &= \{v_3, v_{-3}, v_7, v_{-7}\};\\
B_7' &= \{v_8, v_{-8}, v_{11}, v_{-11}\};\\
B_8' &= \{v_{19}, v_{-19}, v_{21}, v_{-21}\}.
\end{aligned}
$$

2. На первом блоке x_4 имеет вид

$$
\begin{pmatrix}
z_1 & z_2 & 0 & 0 & z_3 & -2z_3\\
z_4 & z_5 & 0 & 0 & z_6 & -2z_6\\
0 & 0 & z_7 & 0 & 0 & 0\\
0 & 0 & 0 & z_7 & 0 & 0\\
0 & 0 & 0 & 0 & z_7 & 0\\
z_8 & z_9 & 0 & 0 & z_{10} & z_7 - 2z_{10}
\end{pmatrix}.
$$

3. На втором, третьем и четвертом блоках она есть

$$\begin{pmatrix}
z_{11} & z_{12} & -z_{13} & -z_{14} & z_{15} & z_{15} & z_{14} & z_{13} & -z_{16} & z_{16}\\
z_{12} & z_{11} & z_{13} & z_{14} & -z_{15} & -z_{15} & -z_{14} & -z_{13} & z_{16} & -z_{16}\\
-z_{17} & z_{17} & z_{18} & z_{19} & z_{20} & z_{21} & z_{22} & z_{23} & z_{17} & -z_{17}\\
z_{24} & -z_{24} & z_{25} & z_{26} & z_{27} & z_{28} & z_{29} & z_{30} & -z_{24} & z_{24}\\
-z_{31} & z_{31} & z_{32} & z_{33} & z_{34} & z_{35} & z_{36} & z_{37} & z_{31} & -z_{31}\\
-z_{31} & z_{31} & -z_{37} & -z_{36} & z_{35} & z_{34} & -z_{33} & -z_{32} & z_{31} & -z_{31}\\
-z_{24} & z_{24} & z_{30} & z_{29} & -z_{28} & -z_{27} & z_{26} & z_{25} & z_{24} & -z_{24}\\
z_{17} & -z_{17} & z_{23} & z_{22} & -z_{21} & -z_{20} & z_{19} & z_{18} & -z_{17} & z_{17}\\
-z_{16} & z_{16} & z_{13} & z_{14} & -z_{15} & -z_{15} & -z_{14} & -z_{13} & z_{11} & z_{12}\\
z_{16} & -z_{16} & -z_{13} & -z_{14} & z_{15} & z_{15} & z_{14} & z_{13} & z_{12} & z_{11}
\end{pmatrix}.$$

4. На всех остальных блоках x_4 имеет вид

$$\begin{pmatrix}
z_{38} & z_{39} & z_{40} & z_{41}\\
z_{42} & z_{43} & z_{44} & z_{45}\\
-z_{45} & -z_{44} & z_{43} & z_{42}\\
-z_{41} & -z_{40} & z_{39} & z_{38}
\end{pmatrix}.$$

Таким образом, у нас имеется 85 неизвестных $y_1, \dots, y_{40}, z_1, \dots, z_{45}$, где y_1, y_6, y_{11}, y_{20}, y_{21}, y_{30}, y_{32}, y_{36}, y_{39}, y_{44}, z_1, z_5, z_7, z_{11}, z_{18}, z_{26}, z_{28}, z_{30}, z_{38}, z_{34}, z_{43}, z_{45} сравнимы с 1 по модулю радикала, y_2, y_4, y_{17}, y_{46}, z_2, z_3, z_9 сравнимы с -1 по модулю радикала, z_{32} — с -2, остальные переменные лежат в радикале.

Мы применим поочередно четыре замены базиса, коммутирующие друг с другом и со всеми матрицами w_i. Эти замены представляются матрицами C_1, C_2, C_3, C_4. Матрицы C_1 и C_2 блочно-диагональны, где первые 24 блока имеют размер 2×2, последний блок — 4×4. На всех блоках размера 2×2, соответствующих коротким корням, матрица C_1 единична, на всех блоках размера 2×2, соответствующих длинным корням, она имеет вид

$$\begin{pmatrix} 1 & -y_{16}/y_{17}\\ -y_{16}/y_{17} & 1\end{pmatrix}.$$

На последнем блоке она единична.

Аналогично, C_2 единична на блоках, соответствующих длинным корням, а также на последнем блоке. На блоках, соответствующих коротким корням, она имеет вид

$$\begin{pmatrix} 1 & -z_8/z_9\\ -z_8/z_9 & 1\end{pmatrix}.$$

Матрицы C_3 и C_4 диагональны, единичны на последнем блоке размера 4×4, матрица C_3 единична на всех местах, соотвествующих коротким корням, скалярна с множителем a на всех местах, соответствующих длинным корням. Наоборот, матрица C_4 единична на всех местах, соответствующих длинным корням, скалярна с множителем b на всех местах, соответствующих коротким корням.

Так как все эти четыре матрицы коммутируют со всеми w_i, $i = 1, 2, 3, 4$, то после замены базиса любой из них все соотношения на элементы x_1 и x_4 по-прежнему выполняются.

Для начала применим замены базиса с помощью матриц C_1 и C_2. После этого новое y_{16} в матрице x_1 и новое z_8 в матрице x_4 станут равны нулю (для удобства обозначений мы не будем менять названия переменных). Теперь выберем $a = -1/y_{17}$ (для нового y_{17}) и применим третью замену базиса. После этого y_{17} в матрице x_1 станет равно -1. Ясно, что y_{16} по-прежнему является нулем.

Наконец, применим последнюю замену базиса с $b = -1/z_9$ (где z_9 — самое последнее, полученное после трех предыдущих замен). Увидим, что y_{16}, y_{17}, z_8 не поменяются, а z_9 станет равно -1.

Теперь мы модем считать, что $y_{16} = 0, y_{17} = -1, z_8 = 0, z_9 = -1$, теперь у нас осталось лишь 81 переменных.

Так как x_1 и x_4 коммутируют (Cond. 1), сразу получим $y_{37} = y_{38} = 0$, $y_{36} = y_{20}$. Из соотношения $h_{\alpha_2}(-1)x_1h_{\alpha_2}(-1)x1 = E$ (Cond. 2, позиция $(52, 52)$) следует $y_{20}^2 = 1$, откуда $y_{20} = 1$.

Из соотношения $w_2x_1w_2^{-1}x_1 = x_1w_2(1)x_1w_2(1)^{-1}$ (Cond. 3, позиция $(50, 10)$) следует $y_{21} = 1$, из позиции $(49, 10)$ следует $y_{19} = 0$.

Соотношение $w_2w_3w_2x_1w_2^{-1}w_3(1)w_2^{-1}x_1 = x_1w_2w_3w_2x_1w_2^{-1}w_3^{-1}w_2^{-1}$ (Cond. 4, позиция $(51, 52)$) влечет $y_{15} = 0$.

Снова из Cond. 3 (позиция $(18, 13)$) имеем $y_{46}(y_{45} + y_{42}) = 0$, поэтому $y_{45} = -y_{42}$. Из Cond. 2 (позиции $(11, 12)$ и $(12, 11)$) получаем $y_{40}(y_{39} + y_{44}) = 0$ и $y_{43}(y_{39} + y_{44}) = 0$, откуда $y_{40} = y_{43} = 0$. После этого то же соотношение на позиции $(12, 16)$ дает $y_{44} = y_{39}$. Позиция $(12, 16)$ соотношения Cond. 3 теперь дает нам $y_{46}(y_{39} - 1) = 0 \Rightarrow y_{39} = 1$.

В соотношении $h_{\alpha_3}(-1)x_4h_{\alpha_3}(-1)x_4 = E$ (Cond. 5) позиция $(8, 7)$ дает $z_4 = 0$, позиция $(7, 7)$ — $z_1 = 1$; $(51, 51)$ —$z_7 = 1$;

В соотношении $w_3x_4x_3^{-1}x_4 = x_4w_3x_4x_3^{-1}$ (Cond. 6) позиция $(51, 5)$ дает $z_{41} = 0$, позиция $(51, 6)$ дает $z_{40} = 0$, позиция $(52, 7)$ — $z_{39} = 0$, позиция $(51, 8)$ — $z_{10} = 0$, позиция $(52, 8)$ — $z_{38} = 1$.

Снова из Cond. 5 (позиции $(52, 52)$, $(52, 8)$, $(7, 8)$) получим $z_6 = 0$, $z_5 = 1$, $z_2 = z_3$.

Возвращаясь к Cond. 6, из $(13, 51)$ имеем $z_{43} = 1$, из $(5, 51)$ — $z_{44} = 0$, из $(5, 14)$ — $z_{42} = 0$, из $(12, 17)$ — $z_{35} = 0$, из $(12, 18)$ — $z_{34} = 1$, из $(12, 19)$ — $z_{37} = -z_{31}$, из $(12, 20)$ — $z_{36} = z_{31}$, из $(9, 15)$ — $z_{20} = -z_{15}$, а из $(10, 15)$ — $z_{27} = z_{15}$.

Позиция $(11, 22)$ соотношения Cond. 1 теперь дает нам $y_{42} = 0$, а позиция $(11, 11)$ в Cond. 2 — $y_{41} = 0$.

Рассматривая $x_{1+2} = \varphi_2(x_{\alpha_1+\alpha_2}(1)) = w_2x_1w_2^{-1}$, $x_2 = \varphi(x_{\alpha_2}(1)) = w_1x_{1+2}w_1$ и Cond. 7: $x_1x_2 = x_{1+2}x_2x_1$ (позиция $(6, 16)$), мы получим $y_{46} = -1$.

Аналогично, рассматривая $x_{3+4} = \varphi_2(x_{\alpha_3+\alpha_4}(1)) = w_3x_4w_3^{-1}$, $x_3 = \varphi(x_{\alpha_3}(1)) = w_4x_{3+4}w_4^{-1}$, и Cond. 8: $x_3x_4 = x_{3+4}x_4x_3$ (применяя позиции $(51, 14)$, $(13, 52)$, $(12, 11)$, $(29, 9)$, $(15, 35)$, $(15, 36)$, $(16, 36)$, $(12, 19)$, $(12, 20)$, $(11, 25)$, $(12, 26)$, $(10, 30)$, $(47, 11)$, $(1, 2)$, $(1, 1)$, $(4, 4)$, $(3, 4)$, $(3, 18)$, $(3, 17)$, $(4, 17)$, $(4, 3)$, $(3, 3)$, $(18, 3)$), получим $z_{45} = 1$, $z_3 = -1$, $z_{31} = 0$, $z_{32} = -2$, $z_{14} = 0$, $z_{13} = 0$, $z_{30} = 1$, $z_{25} = 0$, $z_{26} = 1$, $z_{15} = 0$, $z_{28} = 1$, $z_{24} = 0$, $z_{16} = 0$, $z_{12} = 0$, $z_{11} = 1$, $z_{17} = 0$, $z_{19} = 0$, $z_{21} = 0$, $z_{22} = 0$, $z_{29} = 0$, $z_{23} = 0$, $z_{18} = 1$, $z_{33} = 0$, соответственно.

Таким образом, мы получим, что $x_4 = x_{\alpha_4}(1)$.

Напрямую из первого соотношения теперь имеем $y_3 = y_7 = y_{27} = y_{25} = y_{34} = y_{26} =$

$y_{33} = y_{28} = y_{35} = y_{22} = y_{24} = y_{29} = y_{31} = y_{12} = y_{13} = y_9 = y_{10} = y_{23} = y_{18} = y_{14} = 0$, $y_{30} = y_{32} = y_{11} = 1$.

Наконец, из Cond. 3 получим $y_5 = 0$, $y_6 = 1$, $y_1 = 1$, $y_8 = 0$, $y_4 = -1$, а из Cond. 2 — $y_2 = -1$.

Теперь $x_1 = x_{\alpha_1}(1)$, что и требовалось.

Так как все длинные (и все короткие) корни сопряжены друг с другом под действием группы Вейля, то $\varphi_2(x_\alpha(1)) = x_\alpha(1)$ для всех $\alpha \in \Phi$.

Рассмотрим теперь матрицу $d_t = \varphi_2(h_{\alpha_4}(t))$.

Лемма 1.12. *Матрица d_t равна $h_{\alpha_4}(s)$ для некоторого $s \in R^*$.*

Доказательство. Так как матрица d_t коммутирует с $h_\alpha(-1)$ для всех $\alpha \in \Phi$, то d_t раскладывается в следующие диагональные блоки:

$$
\begin{aligned}
D_1 &= \{v_1, v_{-1}, v_{14}, v_{-14}, v_{20}, v_{-20}, v_{22}, v_{-22}\},\\
D_2 &= \{v_2, v_{-2}, v_{10}, v_{-10}, v_{16}, v_{-16}, v_{24}, v_{-24}\},\\
D_3 &= \{v_3, v_{-3}\}, \quad D_4 = \{v_4, v_{-4}\},\\
D_5 &= \{v_5, v_{-5}, v_{12}, v_{-12}, v_{18}, v_{-18}, v_{23}, v_{-23}\},\\
D_6 &= \{v_6, v_{-6}\}, \quad D_7 = \{v_7, v_{-7}\},\\
D_8 &= \{v_8, v_{-8}\}, \quad D_9 = \{v_9, v_{-9}\},\\
D_{10} &= \{v_{11}, v_{-11}\}, \quad D_{11} = \{v_{13}, v_{-13}\},\\
D_{12} &= \{v_{15}, v_{-15}\}, \quad D_{13} = \{v_{17}, v_{-17}\},\\
D_{14} &= \{v_{19}, v_{-19}\}, \quad D_{15} = \{v_{21}, v_{-21}\},\\
D_{16} &= \{V_1, V_2, V_3, V_4\}.
\end{aligned}
$$

Используя то, что d_t коммутирует с w_1, w_2, w_{13} и x_1, мы получим, что на блоках D_1, D_2, D_5 матрица d_t имеет вид

$$
\begin{pmatrix}
t_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & t_1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & t_8 & 0 & t_9 & 0 & 0 & 0\\
0 & 0 & 0 & t_{10} & 0 & t_{11} & 0 & 0\\
0 & 0 & t_{11} & 0 & t_{10} & 0 & 0 & 0\\
0 & 0 & 0 & t_9 & 0 & t_8 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & t_1 + 2t_{13} & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & t_1
\end{pmatrix};
$$

на блоках D_3, D_6, D_8, D_{14} — вид $\mathrm{diag}\,[t_2, t_3]$; на блоках D_7, D_9, D_{10}, D_{15} — $\mathrm{diag}\,[t_3, t_2]$, на блоке D_4 —

$$
\begin{pmatrix}
t_4 & t_5\\
t_6 & t_7
\end{pmatrix};
$$

на блоках D_{11}, D_{12}, D_{13} она имеет вид $\mathrm{diag}\,[t_{12}, t_{12}]$; а на последнем блоке —

$$
\begin{pmatrix}
t_1 & 0 & 0 & 0\\
0 & t_1 & 0 & 0\\
0 & 0 & t_1 & 0\\
0 & 0 & t_{13} & t_1 - 2t_{13}
\end{pmatrix}.
$$

Используя соотношение $w_4 d_t w_4^{-1} d_t = E$, получим: из позиции $(1,1)$ следует $t_1^2 = 1$, поэтому $t_1 = 1$, из $(52,52)$ следует $(1-2t_{13})^2 = 1$, откуда $t_{13} = 0$; $(5,5)$ влечет $t_3 = 1/t_2$; $(7,8)$ влечет $t_7(t_5+t_6) = 0$, поэтому $t_6 = -t_5$; из $(24,36)$ получим $t_8(t_9+t_{11}) = 0$, таким образом, $t_{11} = -t_9$; из $(26,26)$ имеем $t_{12}^2 = 1$, и тогда $t_{12} = 1$.

Теперь рассмотрим соотношение $w_3 d_t w_3^{-1} = d_t w_4 w_3 d_t w_3^{-1} w_4^{-1}$. Его позиция $(13,14)$ дает $t_5 = 0$, позиция $(5,5)$ — $t_4 = 1/t_2^2$, $(6,6)$ — $t_7 = t_2^2$; $(3,19)$ — $t_9 = 0$; $(19,19)$ — $t_{10} = 1/t_8$.

Наконец, введем $\varphi_2(h_{\alpha_3}(t)) = w_4 w_3 d_t w_3^{-1} w_3^{-1}$, $\varphi_2(h_{\alpha_6}(t)) = w_2 \varphi_2(h_{\alpha_3}(t)) w_2^{-1}$, $\varphi_2(h_{\alpha_{10}}(t)) = \varphi_2(h_{\alpha_6}(t))\varphi_2(h_{\alpha_3}(t))$. Так как $\varphi_2(h_{\alpha_{10}}(t))$ коммутирует с $x_{\alpha_8}(1)$, мы получим (позиция $(9,6)$) $t_8 = t_2^2$.

Таким образом, $\varphi_2(h_{\alpha_4}(t)) = h_{\alpha_4}(1/t_2)$, лемма доказана. $\square$

Ясно, что эта лемма также верна для образов всех $h_\alpha(t)$, $\alpha \in \Phi$.

1.4.4 Система корней G_2

Пусть e_1, e_2, e_3 — ортонормированный базис пространства $\mathbb{R}^3$. Тогда пронумеруем корни системы G_2 следующим образом: $\alpha_1 = e_1 - e_2, \alpha_2 = -2e_1 + e_2 + e_3$ — простые корни; $\alpha_3 = \alpha_1 + \alpha_2 = e_3 - e_1$, $\alpha_4 = 2\alpha_1 + \alpha_2 = e_3 - e_2$, $\alpha_5 = 3\alpha_1 + \alpha_2 = e_1 + e_3 - 2e_2$, $\alpha_6 = 3\alpha_1 + 2\alpha_2 = 2e_3 - e_1 - e_2$ — остальные положительные корни.

Напомним, что

$w_1 = -e_{1,2} - e_{2,1} + e_{3,9} + e_{4,10} - e_{9,3} - e_{10,4} + e_{5,7} + e_{6,8} - e_{7,5} - e_{8,6} + e_{11,,11} + e_{12,12} - e_{13,13} + e_{14,14} + 3e_{13,14}$;
$w_2 = -e_{3,4} - e_{4,3} + e_{1,5} + e_{2,6} - e_{5,1} - e_{6,2} + e_{7,7} + e_{8,8} + e_{9,11} + e_{10,12} - e_{11,9} - e_{12,10} + e_{13,13} - e_{14,14} + e_{14,13}$;
$x_{\alpha_1}(1) = E - e_{1,2} - 2e_{1,13} + 3e_{1,14} - e_{4,6} - e_{4,8} - e_{4,10} + 3e_{5,3} + 2e_{6,8} + 3e_{6,10} - 3e_{7,3} - 2e_{7,5} + 3e_{8,10} + e_{9,3} + e_{9,5} - e_{9,7} + e_{13,2}$;
$x_{\alpha_2}(1) = E + e_{2,6} - e_{3,4} + e_{3,13} - 2e_{3,14} - e_{5,1} + e_{10,12} - e_{11,9} + e_{14,4}$.

То, что $x_1 = \varphi_2(x_{\alpha_1}(1))$ коммутирует с $h_{\alpha_1}(-1)$ и с $w'_{3\alpha_1+2\alpha_2} = w'_2 w_1 w'_2 w_1^{-1} w_2^{-1\prime}$, дает разбиение матрицы x_1 на блоки $\{v_1, v_{-1}, v_6, v_{-6}, V_1, V_2\}$ и $\{v_2, v_{-2}, v_3, v_{-3}, v_4, v_{-4}, v_5, v_{-5}\}$; на первом блоке матрица имеет вид

$$\begin{pmatrix} y_1 & y_2 & y_3 & -y_3 & y_4 & -\frac{3y_4}{2} \\ y_5 & y_6 & y_7 & -y_7 & y_8 & -\frac{3y_8}{2} \\ y_9 & y_{10} & y_{11} & y_{12} & y_{13} & y_{14} \\ -y_9 & -y_{10} & y_{12} & y_{11} & -y_{13} & 3y_{13}+y_{14} \\ y_{15} & y_{16} & y_{17} & y_{17}+3y_{19} & y_{18} & \frac{3(y_{20}-y_{18})}{2} \\ 0 & 0 & y_{19} & y_{19} & 0 & y_{20} \end{pmatrix};$$

на втором блоке она имеет вид

$$\begin{pmatrix} y_{21} & y_{22} & y_{23} & y_{24} & -y_{25} & -y_{26} & -y_{27} & -y_{28} \\ y_{29} & y_{30} & y_{31} & y_{32} & -y_{33} & -y_{34} & -y_{35} & -y_{36} \\ y_{37} & y_{38} & y_{39} & y_{40} & -y_{41} & -y_{42} & -y_{43} & -y_{44} \\ y_{45} & y_{46} & y_{47} & y_{48} & -y_{49} & -y_{50} & -y_{51} & -y_{52} \\ y_{52} & y_{51} & y_{50} & y_{49} & y_{48} & y_{47} & y_{46} & y_{45} \\ y_{44} & y_{43} & y_{42} & y_{41} & y_{40} & y_{39} & y_{38} & y_{37} \\ y_{36} & y_{35} & y_{34} & y_{33} & y_{32} & y_{31} & y_{30} & y_{29} \\ y_{28} & y_{27} & y_{26} & y_{25} & y_{24} & y_{23} & y_{22} & y_{21} \end{pmatrix}.$$

Аналогично, так как $x_2 = \varphi_2(x_{\alpha_2}(1))$ коммутирует с $h_{\alpha_2}(-1)$ и $w_{2\alpha_1+\alpha_2} = w_1 w_2' w_1 w_2^{-1\prime} w_1^{-1}$, имеем разбиение на блоки $\{v_1, v_{-1}, v_3, v_{-3}, v_5, v_{-5}, v_6, v_{-6}\}$ и $\{v_2, v_{-2}, v_4, v_{-4}, V_1, V_2\}$; на первом блоке матрица равна

$$\begin{pmatrix} z_1 & z_2 & z_3 & z_4 & z_5 & z_6 & z_7 & z_8 \\ z_9 & z_{10} & z_{11} & z_{12} & z_{13} & z_{14} & z_{15} & z_{16} \\ -z_{12} & -z_{11} & z_{10} & z_9 & -z_{16} & -z_{15} & z_{13} & z_{14} \\ -z_4 & -z_3 & z_2 & z_1 & -z_8 & -z_7 & z_6 & z_5 \\ z_{17} & z_{18} & z_{19} & z_{20} & z_{21} & z_{22} & z_{23} & z_{24} \\ z_{25} & z_{26} & z_{27} & z_{28} & z_{29} & z_{30} & z_{31} & z_{32} \\ -z_{28} & -z_{27} & z_{26} & z_{25} & -z_{32} & -z_{31} & z_{30} & z_{29} \\ -z_{20} & -z_{19} & z_{18} & z_{17} & -z_{24} & -z_{23} & z_{22} & z_{21} \end{pmatrix};$$

на втором —

$$\begin{pmatrix} z_{33} & z_{34} & -z_{35} & z_{35} & z_{36} & -\frac{2z_{36}}{1+u} \\ z_{37} & z_{38} & -z_{39} & z_{39} & z_{40} & -\frac{2z_{40}}{1+u} \\ z_{41} & z_{42} & z_{43} & z_{44} & z_{45} & z_{46} \\ -z_{41} & -z_{42} & z_{44} & z_{43} & z_{45}+z_{46} & -z_{46} \\ 0 & 0 & \frac{z_{47}+z_{48}}{1+u} & \frac{z_{47}+z_{48}}{1+u} & \frac{2z_{49}}{1+u}+z_{50} & 0 \\ z_{51} & z_{52} & z_{47} & z_{48} & z_{49} & z_{50} \end{pmatrix}.$$

Таким образом, мы имеем 104 переменных $y_1, \dots, y_{52}, z_1, \dots, z_{52}$, из которых y_1, y_6, y_{11}, $y_{16}, y_{18}, y_{20}, y_{21}, y_{30}, y_{34}, y_{36}, y_{39}, y_{48}, z_1, z_{10}, z_{12}, z_{21}, z_{30}, z_{32}, z_{33}, z_{36}, z_{38}, z_{43}, z_{50}, z_{52}$ сравнимы с единицей по модулю радикала, y_2, y_{32}, z_{34} сравнимы с -1 по модулю радикала, y_4, y_{50}, — с -2, $y_{37}, -y_{52}$ — с тройкой, все остальные элементы лежат в радикале.

Применим последовательно четыре замены базиса, коммутирующие друг с другом и со всеми матрицами w_i. Эти замены будут представлены матрицами C_1, C_2, C_3, C_4. Матрицы C_1 и C_2 блочно-диагональны с блоками размера 2×2. На всех блоках размера 2×2, соответствующих коротким корням, матрица C_1 единична, а на всех блоках 2×2, соответствующих длинным корням, имеет вид

$$\begin{pmatrix} 1 & -z_{51}/z_{52} \\ -z_{51}/z_{52} & 1 \end{pmatrix}.$$

На последнем блоке она единична.

Аналогично, матрица C_2 единична на блоках, соответствующих длинным корням, и на последнем блоке, а на блоках, соответствующих коротким корням, имеет вид

$$\begin{pmatrix} 1 & -y_{15}/y_{16} \\ -y_{15}/y_{16} & 1 \end{pmatrix}.$$

Матрицы C_3 и C_4 диагональны, единичны на последнем блоке, матрица C_3 единична на всех местах, соответствующих коротким корням, скалярна с множителем a на всех местах, соответствующих длинным корням. Матрица C_4, напротив, единична на всех местах, соответствующих длинным корням, и скалярна с множителем b на всех местах, соответствующих коротким корням.

Так как все четыре матрицы коммутируют со всеми w_i, $i = 1, 2, 3, 4$, то после замены базиса любой из этих матриц все соотношения на элементы матриц x_1 и x_2 будут выполнены.

Сначала применим замены с помощью матриц C_1 и C_2. После них новые y_{15} в матрице x_1 и z_{51} в матрице x_2 станут равными нулю (для удобства обозначений не будем изменять названия переменных). Далее выберем $a = 1/z_{52}$ (новое z_{52}), применим вторую замену базиса. После этого z_{52} в матрице x_1 становится равным 1. Понятно, что z_{51} при этом останется нулевым.

Наконец, применим последнюю замену базиса с $b = 1/y_{16}$ (где y_{16} — самое последнее, полученное после предыдущих двух замен). При этом y_{15}, z_{51}, z_{52} не изменятся, а y_{16} станет равным 1.

Теперь мы можем считать, что $y_{15} = 0, y_{16} = 1, z_{51} = 0, z_{52} = 1$, переменных стало 100.

Введем $x_{1+2} = \varphi_2(x_{\alpha_1+\alpha_2}(1)) = w_2' x_1 w_2^{-1'}$, $x_{1+1+2} = \varphi_2(x_{2\alpha_1+\alpha_2}(1)) = w_1 x_{1+2} w_1^{-1}$, $x_{1+1+1+2} = \varphi_2(x_{3\alpha_1+\alpha_2}(1)) = w_1 x_2 w_1^{-1}$, $x_{1+1+1+2+2} = \varphi_2(x_{3\alpha_1+2\alpha_2}(1)) = w_2' x_{1+1+1+2} w_2^{-1'}$.

Используем теперь следующие соотношения, которые должны выполняться для элементов w_i и x_i:

$$
\begin{aligned}
&Con1 = (x_2 x_{1+2} = x_{1+2} x_2),\\
&Con2 = (h_1 x_2 h_1 x_2 = E);\\
&Con3 = (h_2 x_1 h_2 x_1 = E);\\
&Con4 = (x_2 x_{1+1+2} = x_{1+1+2} x_2);\\
&Con5 = (x_2 x_{1+1+1+2} = x_{1+1+1+2+2} x_{1+1+1+2} x_2);\\
&Con6 = (x_{1+1+1+2} x_1 = x_1 x_{1+1+1+2};\\
&Con7 = (x_1 x_{1+1+2} = x_{1+1+1+2}^3 x_{1+1+2} x_1);\\
&Con8 = (w_1^3 = x_1 w_1 x_1 w_1^3 x_1).
\end{aligned}
$$

Как и для системы корней B_l, будем последовательно выписывать соотношения и для простоты писать коэффициенты по модулю радикала (в результате эти коэффициенты будут иметь вид чисел 0, ± 1, ± 2, ± 3).

Мы запишем ниже, каким образом выражаются переменные из соотношений (в скобках записываем номер соотношения и позицию в нем): $(Con1, 14, 3)$: $y_{22} = 0$; $(Con1, 6, 10)$: $y_3 = 0$; $(Con1, 1, 1)$: $y_{47} = -z_7$; $(Con1, 1, 3)$: $y_{46} = 0$; $(Con1, 1, 6)$: $y_{40} = -z_3$; $(Con1, 1, 7)$ $y_{49} = -z_7 + 3z_{39}$; $(Con1, 1, 9)$: $y_{43} = 0$; $(Con1, 1, 11)$: $y_{51} = 0$; $(Con1, 2, 1)$: $z_{15} = -3z_{20}$; $(Con1, 2, 3)$: $y_{41} = 0$; $(Con1, 2, 5)$: $y_5 = -3z_{18}$; $(Con1, 2, 7)$: $z_{44} = -3/2z_{20}$; $Con1, 2, 9)$: $y_7 = -3z_{24}$; $(Con1, 3, 1)$: $z_{20} = y_{23} + 2z_{35} - z_9$; $(Con1, 3, 3)$: $z_{41} = 0$; $(Con1, 3, 5)$: $z_{18} = z_{11}$; $(Con1, 4, 1)$: $y_{23} = -2z_{39}$; $(Con1, 4, 2)$: $z_{37} = -y_{24}$; $(Con1, 5, 3)$: $y_{35} = 0$; $(Con1, 7, 5)$: $z_3 = 0$; $(Con1, 11, 5)$: $y_9 = 0$; $(Con1, 11, 3)$: $y_{24} = 0$; $(Con1, 10, 3)$: $y_{27} = 0$; $(Con1, 9, 3)$: $y_{38} = 0$; $(Con1, 4, 5)$: $z_{11} = 0$; $(Con1, 5, 5)$: $z_2 = 0$; $(Con2, 3, 3)$: $z_{33} = 1$; $(Con2, 14, 4)$: $z_{50} = z_{38}$; $(Con2, 11, 5)$: $z_{19} = 0$; $(Con2, 3, 13)$: $z_{38} = 1 - z_{40}$; $(Con2, 10, 5)$: $z_{27} = 0$; $(Con2, 5, 5)$: $z_{10} = 1$; $(Con2, 6, 6)$: $z_1 = 1$; $(Con2, 1, 9)$: $z_7 = 0$; $(Con1, 11, 6)$: $z_{26} = y_{10} + z_4 + y_{33}$; $(Con2, 7, 7)$: $z_{43} = 1$; $(Con2, 9, 9)$: $z_{23} = 2(z_{21} - 1)$; $(Con2, 11, 12)$: $z_{31} := -2z_{29} - z_{24}$; $(Con3, 1, 1)$: $y_1 = 1$; $(Con3, 1, 2)$: $y_4 = 1 + 2y_2 - y_6$; $(Con3, 2, 2)$: $y_8 = 2(y_6 - 1)$; $(Con3, 4, 4)$: $y_{30} = 1$; $(Con3, 14, 14)$: $y_{20} = 1$; $(Con3, 13, 13)$: $y_{18} = y_6$; $(Con3, 12, 12)$: $y_{11} = 1$; $(Con1, 13, 11)$: $z_6 = 0$; $(Con4, 2, 2)$: $y_{42} = 6z_{39} - 6z_{35} + 3z_9 + 3z_{10} + 3z_4 + 3y_{33}$; $(Con2, 5, 6)$: $z_4 = -2z_9$; $(Con2, 9, 11)$: $z_{21} = 1$; $(Con2, 12, 11)$:

$z_{22} = 0$; $(Con2, 10, 10)$: $z_{30} = 1$; $(Con2, 14, 7)$: $z_{39} = 0$; $(Con2, 11, 1)$: $y_{33} = 2y_{28} - y_{10} + 2z_9 - z_{17}$; $(Con3, 12, 2)$: $y_{13} = y_{10}$; $(Con3, 10, 6)$: $y_{25} = 0$; $(Con3, 10, 5)$: $y_{26} = 0$; $(Con3, 7, 7)$: $y_{48} = 1$; $(Con3, 3, 3)$ $y_{28} = 1$; $(Con3, 8, 3)$: $y_{44} = 0$; $(Con2, 5, 9)$: $z_5 = 2z_{16} - z_{14}$; $(Con4, 10, 5)$: $z_{24} = -2z_{29}$; $(Con3, 7, 5)$: $y_{39} = 1$; $(Con4, 5, 10)$: $y_{45} = 3z_{14}$; $(Con4, 11, 12)$: $z_{16} = -3z_{28} - 3z_{25} - z_{13}$; $(Con4, 9, 6)$: $y_{31} = -2z_9 + 3z_{17}$; $(Con4, 11, 2)$: $z_9 = 3z_{28}$; $(Con4, 5, 5)$: $z_{14} = 0$; $(Con2, 1, 12)$: $z_8 = 0$; $(Con4, 2, 1)$: $z_{13} = -3z_{25}$; $(Con4, 6, 10)$: $y_{52} = -y_{37} + 3y_{50}/2 + 3$; $(Con4, 10, 10)$: $y_{28} = -6z_{28} + 3z_{17}$; $(Con1, 13, 1)$: $z_{48} = -z_{47}$; $(Con1, 5, 4)$: $y_{37} = 3/2 + 3/2y_6 - 3z_{12} - 3y_2$; $(Con4, 13, 13)$: $y_{17} = 3/2y_{19} - z_{45} - z_{46}$; $(Con1, 14, 1)$: $z_{47} = 0$; $(Con2, 7, 4)$: $z_{46} = 2z_{42}$; $(Con4, 3, 3)$: $y_{19} = -y_{12}$; $(Con5, 3, 2)$: $z_{17} = z_{25} + z_{35} + 2z_{28}$; $(Con5, 3, 3)$: $z_{29} = 0$; $(Con5, 3, 4)$: $z_{40} = 0$; $(Con5, 3, 5)$: $z_{35} = -z_{25}$; $(Con5, 3, 6)$: $z_{25} = -3z_{28}$; $(Con5, 3, 13)$: $z_{49} = 0$; $(Con5, 14, 12)$: $z_{32} = 1$; $(Con5, 11, 4)$: $z_{36} = -z_{34}$; $(Con5, 9, 4)$: $z_{34} = -1$; $(Con5, 3, 10)$: $z_{45} = -1/2y_{12} - 2z_{42}$; $(Con5, 4, 10)$: $u = 0$ (таким образом, $w_2' = w_2$); $(Con1, 3, 9)$: $y_{12} = -9z_{28}$; $(Con3, 11, 2)$: $y_{10} = 0$; $(Con3, 7, 4)$: $z_{42} = 0$; $(Con4, 14, 14)$: $y_{14} = 0$; $(Con4, 11, 1)$: $z_{12} = 1 + 6z_{28}$; $(Con4, 11, 10)$: $y_{29} = -9z_{28}$; $(Con6, 7, 13)$: $y_6 = 1 - 9/2z_{28}$; $(Con6, 9, 2)$: $y_{32} = -1 + 4z_{28}$; $(Con3, 9, 5)$: $y_{50} = -2y_{34} - 8z_{28}$; $(Con7, 7, 2)$: $y_2 = -8y_{34} + 7 - 119/4z_{28}$; $(Con8, 13, 1)$: $y_{34} = 1 + 137/32z_{28}$; $(Con8, 3, 9)$: $y_{36} = 1$; $(Con8, 13, 2)$: $z_{28} = 0$.

Таким образом, $x_1 = x_{\alpha_1}(1)$, $x_2 = x_{\alpha_2}(1)$, откуда $\varphi_2(x_\alpha(1)) = x_\alpha(1)$ для любого корня α.

Теперь посмотрим на образы при изоморфизме φ_2 элементов $h_\alpha(t)$, $t \in R^*$.

Пусть $h_t = \varphi_2(h_{\alpha_1}(t))$. Из того, что h_t коммутирует с $h_1, h_2, w_{\alpha_6}(1)$ и $x_{\alpha_6}(1)$, сразу следует, что

$$h_t = \begin{pmatrix} d_1 & d_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ d_3 & d_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & d_5 & 0 & 0 & -d_6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & d_7 & 0 & 0 & -d_8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & d_9 & 0 & 0 & -d_{10} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & d_{11} & 0 & 0 & -d_{12} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & d_{12} & 0 & 0 & d_{11} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & d_{10} & 0 & 0 & d_9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & d_8 & 0 & 0 & d_7 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & d_6 & 0 & 0 & d_5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & d_{13} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & d_{13} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & d_{14} & \frac{3}{2}(d_{13} - d_{14}) \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & d_{13} \end{pmatrix}.$$

Воспользуемся теперь тем, что $h_{\alpha_1+\alpha_2}(t) = w_2 h_{\alpha_1}(t) w_2^{-1}$, $h_{2\alpha_1+\alpha_2}(t) = w_1 h_{\alpha_1+\alpha_2}(t) w_1^{-1}$ и $h_{\alpha_1}(t) h_{\alpha_1+\alpha_2}(t) = h_{2\alpha_1+\alpha_2}(t)$. Это даст нам соотношение $w_1 w_2 h_t w_2^{-1} w_1^{-1} = w_2 h_t w_2^{-1} h_t$, из которого $d_2 d_{11} = 0 \Rightarrow d_2 = 0$; $d_3 d_9 = 0 \Rightarrow d_3 = 0$; $d_5(1 - d_{13}) = 0 \Rightarrow d_{13} = 1$; $d_6 = d_8 = d_{10} = d_{12} = 0$; $d_7 = 1/d_5$; $d_1 = d_{11}^2$; $d_4 = d_9^2$; $d_{11} = 1/d_9$; $d_{14} = 1$.

Наконец, используем то, что $h_{3\alpha_1+2\alpha_2}(t) = h_{\alpha_1+\alpha_2}(t) h_{2\alpha_1+\alpha_2}(t)$ коммутирует с x_1. Это даст нам $d_5 = d_9^3$, откуда $h_t = h_{\alpha_1}(1/d_9)$.

Таким образом, для всех рассматриваемых систем корней мы показали, что существует еще одна замена базиса такая, что все $x_{\alpha_i}(1)$ перейдут при композиции изоморфизма φ_2 и этой замены базиса в себя, а элементы $h_{\alpha_i}(t)$ — в некоторые $h_{\alpha_i}(s)$.

1.5 Доказательство теоремы 2

Мы получили, что $\varphi_2(h_{\alpha_k}(t)) = h_{\alpha_k}(s)$, $k = 1, \dots, n$. Обозначим отображение $t \mapsto s$ через $\rho : R^* \to R^*$. Заметим, что для $t \in R^*$ $\varphi_2(x_1(t)) = \varphi_2(h_{\alpha_2}(t^{-1}) x_1(1) h_{\alpha_2}(t)) = h_{\alpha_2}(s^{-1}) x_1(1) h_{\alpha_2}(s) = x_1(s)$. Если $t \notin R^*$, то $t \in J$, т. е. $t = 1 + t_1$, где $t_1 \in R^*$. Тогда $\varphi_2(x_1(t)) = \varphi_2(x_1(1) x_1(t_1)) = x_1(1) x_1(\rho(t_1)) = x_1(1 + \rho(t_1))$. Таким образом, если мы продолжим отображение ρ на все кольцо R (по формуле $\rho(t) := 1 + \rho(t-1)$, $t \in R$), то получим

$\varphi_2(x_1(t)) = x_1(\rho(t))$ для всех $t \in R$. Ясно, что ρ инъективно, аддитивно, а также мультипликативно на всех обратимых элементах. Так как каждый элемент кольца R есть сумма двух обратимых, то получаем, что ρ — это изоморфизм из кольца R на некоторое его подкольцо R'. Заметим, что в данной ситуации $CE(\Phi, R)C^{-1} = E(\Phi, R')$ для некоторой матрицы $C \in \mathrm{GL}\,(V)$. Покажем, что $R' = R$.

Обозначим матричные единицы через E_{ij}.

Лемма 1.13. *Элементарная группа Шевалле $E(\Phi, R)$ порождает кольцо $M_n(R)$.*

Доказательство. Докажем это по отдельности для разных систем корней.

1. Системы корней A_l, D_l, E_l.

Матрица $(x_{\alpha_1}(1)-1)^2$ имеет единственный ненулевой элемент $-2\cdot E_{12}$. Умножая его на подходящие диагональные матрицы, мы можем получить произвольную матрицу вида $\lambda \cdot E_{12}$ (так как $-2 \in R^*$ и R^* порождает R). Так как группа Вейля транзитивно действует на системе корней Φ, т.е. для любого корня α_k существует такой элемент $w \in W$, что $w(\alpha_1) = \alpha_k$, то матрица $\lambda E_{12}\cdot w$ имеет вид $\lambda E_{1,2k}$, а матрица $w^{-1}\cdot \lambda E_{12}$ — вид $\lambda E_{2k-1,2}$. Кроме того, благодаря элементу группы Вейля, переводящему первый корень в противоположный, мы имеем элемент $E_{2,1}$. Беря различные комбинации полученных элементов, мы можем получить произвольный элемент λE_{ij}, $1 \le i,j \le 2m$. Таким образом, мы уже породили подкольцо $M_{2m}(R)$. Теперь вычтем из матрицы $x_{\alpha_1}(1)-1$ подходящие матричные единицы, получим матрицу $E_{2m+1,2} - 2E_{1,2m+1} + E_{1,2m+2}$. Умножая ее (справа) на $E_{2,i}$, $1 \le i \le 2m$, получаем все $E_{2m+1,i}$, $1 \le i \le 2m$. С помощью элементов группы Вейля получим все $E_{i,j}$, $2m < i \le 2m + l$, $1 \le j \le 2n$. Теперь мы имеем матрицу $-2E_{1,2m+1} + E_{1,2m+2}$. Умножая ее (слева) на $E_{2m+1,1}$, получим $E_{2m+1,2m+1}$. С помощью последних двух полученных матриц имеем $E_{1,2m+1}$, и, таким образом, все $E_{i,j}$, $1 \le i \le 2m$, $2m < j \le 2m + l$. Ясно, что теперь мы породили все матричные единицы, т.е. все матричное кольцо $M_n(R)$.

Продемонстрируем это подробнее на простейшем случае системы корней A_2. Имеем $(x_{\alpha_1}(1) - 1)^2 = -2E_{12}$, $h_{\alpha_2}(t)(-2E_{12}) = -2tE_{12}$, т.е. мы можем получить любой λE_{12}. Тогда $w_{\alpha_1}\lambda E_{12} w_{\alpha_1}(1)^{-1} = \lambda E_{21}$, $\lambda E_{12}E_{21} = \lambda E_{11}$, $\lambda E_{21}E_{12} = \lambda E_{22}$, $w_{\alpha_2}(1)\lambda E_{12} = \lambda E_{52}$, $w_{\alpha_2}(1)\lambda E_{21} = \lambda E_{61}$, $\lambda E_{52}E_{21} = \lambda E_{51}$, $\lambda E_{61}E_{12} = \lambda E_{62}$, $\lambda E_{12} w_{\alpha_2}(1) = \lambda E_{16}$, $\lambda E_{21} w_{\alpha_2}(1) = \lambda E_{25}$, $\lambda E_{21}E_{16} = \lambda E_{26}$, $\lambda E_{12}E_{25} = \lambda E_{15}$, $\lambda E_{51}E_{15} = \lambda E_{55}$, $\lambda E_{61}E_{16} = \lambda E_{66}$, $\lambda E_{51}E_{16} = E_{56}$, $\lambda E_{61}E_{15} = E_{65}$, $\lambda E_{i5} w_{\alpha_1}(1) = \lambda E_{i3}$, $i = 1,2,5,6$, $\lambda E_{i6} w_{\alpha_1}(1) = \lambda E_{i4}$, $i = 1,2,5,6$, $\lambda w_{\alpha_1}(1) E_{5i} = \lambda E_{3i}$, $i = 1,2,5,6$, $\lambda w_{\alpha_1}(1)E_{6i} = \lambda E_{4i}$, $i = 1,2,5,6$, $\lambda E_{41}E_{13} = \lambda E_{43}$, $\lambda E_{41}E_{14} = \lambda E_{44}$, $\lambda E_{31}E_{13} = \lambda E_{33}$, $\lambda E_{31}E_{14} = \lambda E_{34}$, таким образом, мы получили все матричные единицы подкольца $M_6(R)$.

Далее $y = x_{\alpha_1}(1) - 1 = -E_{12} - 2E_{17} + E_{18} + E_{46} - E_{53} + E_{73}$, $y' = y + E_{12} - E_{46} + E_{53} = E_{18} - 2E_{17} + E_{72}$, $(E_{18} - 2E_{17} + E_{72})\cdot \lambda E_{2i} = \lambda E_{7i}$, $i = 1,\dots,6$, $(w_{\alpha_2}(1) - 1)\lambda E_{7i} = \lambda E_{8i}$, $i = 1,\dots,6$, $y'' = y' - E_{72} = E_{18} - 2E_{17}$, $\lambda E_{81}y'' = \lambda E_{88}$, $\lambda E_{71}y'' = -2\lambda E_{77}$, $y''\lambda E_{88} = \lambda E_{18}$, $y''\lambda E_{77} = -2\lambda E_{17}$, $\lambda E_{i1}E_{17} = \lambda E_{i7}$, $\lambda E_{i1}E_{18} = \lambda E_{i8}$, и мы породили все кольцо $M_8(R)$.

Система корней B_l

Снова матрица $(x_{\alpha_1}(1)-1)^2$ содержит единственный ненулевой элемент $-2\cdot E_{12}$. Умножая его на подходящие диагональные матрицы, мы можем получить произвольную матрицу вида $\lambda\cdot E_{12}$ (так как $-2 \in R^*$ и R^* порождает R). Так как группа Вейля транзитивно действует на корнях одной длины, т.е. для любого длинного корня α_k существует такое $w \in W$, что $w(\alpha_1) = \alpha_k$, то матрица $\lambda E_{12}\cdot w$ имеет вид $\lambda E_{1,2k}$, а матрица $w^{-1}\cdot \lambda E_{12}$ — вид

$\lambda E_{2k-1,2}$. Кроме того, с помощью элемента группы Вейля, переводящего первый корень в противоположный, мы получаем матричную единицу $E_{2,1}$. Беря теперь различные комбинации полученных элементов, мы получаем произвольный элемент λE_{ij}, $1 \leqslant i,j \leqslant 2m$, индексы i,j соответствуют длинным корням.

Матрица $(x_{e_i}(1)-1)^2$ имеет вид

$$-2E_{v_{e_i},v_{-e_i}} + \sum_{j\neq i}(2E_{v_{e_i-e_j},v_{-e_i-e_j}} + 2E_{v_{e_i+e_j},v_{e_j-e_i}}).$$

Все матричные единицы, кроме первой, уже получены нами выше, поэтому мы можем вычесть их и получить $E_{v_{e_i},v_{-e_i}}$. Аналогично ситуации с длинными корнями, используя тот факт, что все короткие корни также сопряжены относительно действия группы Вейля, мы получим все λE_{ij}, $1 \leqslant i,j \leqslant 2m$, индексы i,j соответствуют коротким корням.

Теперь, вычитая из матрицы $x_{\alpha_1}(1)-1$ подходящие матричные единицы, мы сможем получить матрицу $E_{V_{h_1},v_{-\alpha_1}} - 2E_{v_{\alpha_1},V_{h_1}} + E_{v_{\alpha_1},V_{h_2}}$. Умножая эту матрицу (справа) на $E_{v_{-\alpha_1},i}$, $1 \leqslant i \leqslant 2m$, где i соответствует длинным корням, мы получим все $E_{V_{h_1},i}$, $1 \leqslant i \leqslant 2m$ для i, соответствующих длинным корням. Умножая эти последние элементы слева на w_{α_2}, мы получим $E_{V_{h_2},i}$, $1 \leqslant i \leqslant 2m$ для i, соответствующих длинным корням; далее, точно так же умножая полученные элементы слева на $w_{\alpha_3},\dots,w_{\alpha_l}$, мы получим все $E_{V_{h_j},i}$, $1 \leqslant j \leqslant l$, $1 \leqslant i \leqslant 2m$ для i, соответствующих длинным корням.

Далее,

$$\begin{aligned}
A &= 1/2^l(h_{\alpha_1}(-1)+E)\dots(h_{\alpha_l}(-1)+E) = E_{V_{h_1},V_{h_1}} + \dots + E_{V_{h_l},V_{h_l}},\\
B &= A(w_{\alpha_1}-A)(w_{\alpha_2}-A)\dots(w_{\alpha_{l-1}}-A)(w_{\alpha_l}-A)(w_{\alpha_{l-1}}-A)\dots\\
&\qquad \dots(w_{\alpha_2}-A)(w_{\alpha_1}-A)A = -4E_{V_{h_1},V_{h_1}} + 2E_{V_{h_1},V_{h_2}},\\
C_l &= A(w_{\alpha_1}-A)(w_{\alpha_2}-A)\dots(w_{\alpha_{l-1}}-A)(w_{\alpha_l}-A)A = 2E_{V_{h_1},V_{h_{l-1}}} - 2E_{V_{h_1},V_{h_l}},\\
C_{l-1} &= w_{\alpha_{l-1}}C_l w_{\alpha_{l-1}} = 2E_{V_{h_1},V_{h_{l-2}}} - 2E_{V_{h_1},V_{h_{l-1}}},\\
&\dots\dots\dots\dots\dots\\
C_3 &= w_{\alpha_3}C_4 w_{\alpha_3} = 2E_{V_{h_1},V_{h_2}} - 2E_{V_{h_1},V_{h_3}},\\
C_2 &= w_{\alpha_2}C_3 w_{\alpha_2} = 2E_{V_{h_1},V_{h_1}} + 2E_{V_{h_2},V_{h_1}} - 2E_{V_{h_1},V_{h_2}} - 2E_{V_{h_2},V_{h_2}}.
\end{aligned}$$

Теперь

$$\begin{aligned}
C &= B + C_2 = -2E_{V_{h_1},V_{h_1}} + 2E_{V_{h_2},V_{h_1}} - 2E_{V_{h_2},V_{h_2}},\\
C_1 &= w_{\alpha_1}Cw_{\alpha_1} = -4E_{V_{h_1},V_{h_1}} + 2E_{V_{h_1},V_{h_2}} - 2E_{V_{h_2},V_{h_1}},
\end{aligned}$$

наконец,

$$C_1 + B = -2E_{V_{h_2},V_{h_1}}.$$

Теперь с помощью элементов группы Вейля и умножения матричных единиц получаем все $E_{i,j}$, $2m < i,j \leqslant n$, и далее все $E_{i,j}$, $1 \leqslant i \leqslant n$, $2m < j \leqslant n$, где i соответствует длинным корням.

Теперь, взяв матрицу $x_{e_1}(t)$ и умножая ее справа и слева на подходящие матричные единицы $E_{i,i}$, мы можем получить $E_{i,j}$, где i соответствует длинному корню, а j — короткому.

После этого становиться ясным, как получить все матричные единицы $E_{i,j}$, $1 \leqslant i, j \leqslant 2m$ с помощью элементов группы Вейля. Наконец, как и выше, мы можем получить все $E_{i,j}$, $1 \leqslant i \leqslant 2m$, $2m < j \leqslant n$, где i соответствует коротким корням, а значит, вообще все матричные единицы.

Случай системы корней F_4 совершенно аналогичен случаю B_l.

Система корней G_2

Опять же матрица $\frac{1}{2}(x_{\alpha_2}(1)-1)^2$ есть $e_{3,4}$ ($e_{i,j}$ — матричная единица). Умножая ее на подходящую диагональную матрицу, мы получим произвольную матрицу вида $\alpha \cdot e_{3,4}$ (так как обратимые элементы кольца S порождают S).

Благодаря тому, что все длинные корни сопряжены относительно действия группы Вейля, умножая $e_{3,4}$ справа и слева на подходящие w_i, w_j, мы получим все $e_{k,l}$, $k, l = 3, 4, 9, 10, 11, 12$.

Далее, $e_{14,4} = (x_{\alpha_2}(1) - E) \cdot e_{4,4} + e_{3,4}$, снова с помощью домножения справа на различные элементы группы Вейля получим все $e_{14,l}$, $l = 3, 4, 9, 10, 11, 12$.

Теперь $e_{14,14} = -(e_{14,3}(x_{\alpha_2}(1) - E) + e_{14,4})(w_1 - E)$; $e_{3,14} = -1/2(x_{\alpha_2}(1) - E)e_{14,14}$. Аналогично предыдущему, получим все $e_{l,14}$, $l = 3, 4, 9, 10, 11, 12$.

Еще имеем $e_{14,13} = e_{14,3}(x_{\alpha_2}(1) - E) + e_{14,4} + 2e_{14,14}$; $e_{3,13} = e_{3,3}(x_{\alpha_2}(1) - E) + 2e_{3,14} + e_{3,4}$ (и сразу получим все $e_{l,13}$, $l = 3, 4, 9, 10, 11, 12$); $e_{3,2} = e_{3,13}(x_{\alpha_1}(1) - E)$. Теперь воспользуемся дополнительно тем, что все короткие корни сопряжены относительно действия группы Вейля и получим все $e_{k,l}$, $k = 3, 4, 9, 10, 11, 12$, $l = 1, 2, 5, 6, 7, 8$.

Так как $e_{13,13} = 1/4(h_1 + E)(h_2 + E) - e_{14,14}$, $e_{1,13} = -1/2(x_{\alpha_1} - E)e_{13,13}$, $e_{13,2} = e_{13,13}(x_{\alpha_1} - E)$, то мы имеем все $e_{l,13}, e_{13,l}$, $l = 1, 2, 5, 6, 7, 8$, и после этого умножением полученных матричных единиц получаются все $e_{l,k}$, $l, k = 1, \ldots, 14$, и, значит, все кольцо $M_{14}(S)$.

$\square$

Лемма 1.14. *Если для некоторого $C \in \mathrm{GL}(V)$ имеет место $CE(\Phi, R)C^{-1} = E(\Phi, R')$, где R' — это подкольцо в R, то $R' = R$.*

Доказательство. Предположим, что R' — это собственное подкольцо в R.

Тогда $CM_n(R)C^{-1} = M_n(R')$, так как группа $E(\Phi, R)$ порождает кольцо $M_n(R)$, а группа $E(\Phi, R') = CE(\Phi, R)C^{-1}$ порождает кольцо $M_n(R')$. Это невозможно, так как $C \in \mathrm{GL}_n(R)$. $\square$

Таким образом, мы доказали, что ρ — это автоморфизм кольца R. Следовательно, композиция изначального автоморфизма φ и некоторой замены базиса с помощью матрицы $C \in \mathrm{GL}_n(R)$, (переводящей $E(\Phi, R)$ в себя) — это кольцевой автоморфизм ρ. Это доказывает теорему 2. $\square$

В следующих параграфах мы будем доказывать теорему 3.

1.6 Сведение теоремы 3 к системам линейных уравнений над локальным кольцом

В этом параграфе мы будем рассматривать элементарную присоединенную группу Шевалле $E_{\mathrm{ad}}(\Phi, R)$ ранга, большего двух, в своем присоединенном n-мерном представлении, R — произвольное локальное кольцо.

Пусть $n = l+2m$, где m — число положительных корней системы Φ, базисные векторы пронумерованы как $v_1 = x_{\alpha_1}, v_{-1} = x_{-\alpha_1}, \dots, v_m = x_{\alpha_m}, v_{-m} = x_{-\alpha_m}, V_1 = h_1, \dots, V_l = h_l$, что соответствует базису Шевалле системы Φ. Для удобства мы будем нумеровать матричные единицы как $e_{\alpha,\beta}$, e_{α,h_i}, $e_{h_i,\alpha}$, e_{h_i,h_j}, $\alpha, \beta \in \Phi$, $1 \leqslant i, j \leqslant l$.

Пусть имеется некоторая матрица $C = (c_{i,j}) \in \mathrm{GL}_n(R)$ такая, что

$$C \cdot E_{\mathrm{ad}}(\Phi, R) \cdot C^{-1} = E_{\mathrm{ad}}(\Phi, R).$$

Если J — максимальный идеал (радикал) кольца R, то матрицы из $M_n(J)$ образуют радикал в кольце матриц $M_n(R)$, поэтому

$$C \cdot M_n(J) \cdot C^{-1} = M_n(J),$$

откуда

$$C \cdot (E + M_n(J)) \cdot C^{-1} = E + M_n(J),$$

то есть

$$C \cdot E_{\mathrm{ad}}(\Phi, R, J) \cdot C^{-1} = E_{\mathrm{ad}}(\Phi, R, J),$$

так как $E_{\mathrm{ad}}(\Phi, R, J) = E_{\mathrm{ad}}(\Phi, R) \cap (E + M_n(J))$.

Следовательно, образ $\overline{C}$ матрицы C при факторизации кольца R по радикалу J дает нам автоморфизм–сопряжение группы Шевалле $E_{\mathrm{ad}}(\Phi, k)$, где $k = R/J$ — поле вычетов кольца R.

Лемма 1.15. *Если $E_{\mathrm{ad}}(\Phi, k)$ — группа Шевалле, удовлетворяющая одному из следующих условий:*

1) *если ее тип — A_l, D_l или E_l, то поле может иметь любую характеристику, $l > 1$;*
2) *если ее тип — B_l, C_l или F_4, то характеристика поля k отлична от двух;*
3) *если ее тип — G_2, то характеристика поля отлична от трех.*

Тогда любой автоморфизм–сопряжение является композицией внутреннего и диаграммного автоморфизмов.

Доказательство. По теореме 30 из [56] любой автоморфизм группы Шевалле с рассматриваемой системой корней над полем k стандартен, т. е. является композицией внутреннего, кольцевого и диаграммного автоморфизмов. Предположим что некоторая матрица C лежит в нормализаторе группы $E_{\mathrm{ad}}(\Phi, k)$ в $\mathrm{GL}_n(k)$. Тогда сопряжение i_C является автоморфизмом группы $E_{\mathrm{ad}}(\Phi, k)$, поэтому получаем $i_C = i_g \circ \delta \circ \rho$, $g \in E_{\mathrm{ad}}(\Phi, k)$, δ — диаграммный автоморфизм, ρ — кольцевой автоморфизм. Взяв матрицу $A_\delta = \sum_{\alpha\in\Phi} \pm e_{\delta(\alpha),\alpha} + \sum_{\alpha\in\Delta} \pm e_{H_{\delta(\alpha)},H_\alpha}$, мы получим с помощью сопряжения ею диаграммный автоморфизм δ. Следовательно, $i_{A_\delta^{-1}} i_{g^{-1}} i_C = i_{C'} = \rho$ и некоторая матрица $C' \in \mathrm{GL}_n(k)$ определяет кольцевой автоморфизм ρ. Для любого корня $\alpha \in \Phi$ имеет место $\rho(x_\alpha(1)) = x_\alpha(1)$, откуда $C' x_\alpha(1) = x_\alpha(1) C'$ для всех $\alpha \in \Phi$. Значит, матрица C' скалярна, а автоморфизм i_C есть композиция внутреннего и диаграммного. □

По лемме 1.15
$$i_{\overline{C}} = i_{A_\delta} i_g, \quad g \in E_{\mathrm{ad}}(\Phi, k).$$

Матрица A_δ состоит из 0 и ± 1, поэтому ее можно рассматривать как матрицу из группы $\mathrm{GL}_n(R)$.

Так как над полем любой элемент группы Шевалле есть произведение элемента из элементарной подгруппы (которая порождается унипотентами $x_\alpha(t)$) и элемента тора, то матрицу g можно разложить в произведение $t_{\alpha_1}(X_1)\dots t_{\alpha_l}(X_l) x_{\alpha_{i_1}}(Y_1)\dots x_{i_N}(Y_N)$, где $X_1, \dots, X_l, Y_1, \dots, Y_N \in k$, $t_{\alpha_k}(X)$ — элемент тора, соответствующий гомоморфизму χ такому, что $\chi(\alpha_k) = X$, $\chi(\alpha_j) = 1$ при $j \neq k$, $1 \leqslant j \leqslant l$.

Так как каждый из элементов $X_1, \dots, X_l, Y_1, \dots, Y_N$ является классом вычетов в кольце R, то мы можем выбрать (произвольным образом) элементы $x_1 \in X_1, \dots, x_l \in X_l$, $y_1 \in Y_1, \dots, y_N \in Y_n$, и элемент
$$g' = t_{\alpha_1}(x_1)\dots t_{\alpha_l}(x_l) x_{\alpha_{i_1}}(y_1)\dots x_{i_N}(y_N)$$
будет удовлетворять условиям $g' \in G_{\mathrm{ad}}(\Phi, R)$ и $\overline{g'} = g$.

Рассмотрим матрицу $C' = {g'}^{-1} \circ d^{-1} \circ C$. Эта матрица также нормализует элементарную группу Шевалле $E_{\mathrm{ad}}(\Phi, R)$, при этом $\overline{C'} = E$. Таким образом, мы свели описание матриц из нормализатора группы $E_{\mathrm{ad}}(\Phi, R)$ к описанию матриц из нормализатора этой группы, сравнимых с единичной по модулю радикала J.

Поэтому будем считать, что данная нам изначально матрица C сравнима с единичной по модулю J.

Наша цель — показать, что $C \in \lambda G_{\mathrm{ad}}(\Phi, R)$.

Для начала докажем одну вспомогательную техническую лемму.

Лемма 1.16. *Пусть* $X = \lambda t_{\alpha_1}(s_1)\dots t_{\alpha_l}(s_l) x_{\alpha_1}(t_1)\dots x_{\alpha_m}(t_m) x_{-\alpha_1}(u_1)\dots x_{-\alpha_m}(u_m) \in \lambda E_{\mathrm{ad}}(\Phi, R, J)$. *Тогда у матрицы* X *существуют такие* $n+1$ *коэффициентов (точно описанные в доказательстве леммы), по которым однозначно восстанавливаются элементы* λ, s_1, s_2, $t_1, \dots, t_m$, $u_1, \dots, u_m$.

Доказательство. Для начала явно покажем, чему равна матрица X в случае системы корней A_2:
$$X = \lambda t_{\alpha_1}(s_1) t_{\alpha_2}(s_2) \times$$
$$\times x_{\alpha_1}(t_1) x_{\alpha_2}(t_2) x_{\alpha_1+\alpha_2}(t_3) x_{-\alpha_1}(u_1) x_{-\alpha_2}(u_2) x_{-\alpha_1-\alpha_2}(u_3) =$$
$$= \begin{pmatrix}
* & * & * & * & * & * & * & * \\
* & \frac{\lambda(1-t_2u_2)}{s_1} & * & * & * & \frac{\lambda t_2}{s_1} & * & * \\
* & * & * & * & * & * & * & * \\
* & * & * & \frac{\lambda(1-t_1u_1)}{s_2} & * & -\frac{\lambda t_1}{s_2} & * & * \\
* & * & * & * & * & * & * & * \\
* & -\frac{\lambda u_2}{s_1s_2} & * & \frac{\lambda u_1}{s_1s_2} & * & \frac{\lambda}{s_1s_2} & * & -\frac{\lambda(u_3+2u_1u_2)}{s_1s_2} \\
* & * & * & * & * & * & * & * \\
* & * & * & * & * & \lambda t_3 & * & *
\end{pmatrix}.$$

Понятно, что все числа $\lambda, s_1, s_2, t_1, t_2, t_3, u_1, u_2, u_3$ однозначно восстанавливаются по данной матрице X.

Теперь перейдем к произвольной системе корней. Для этого нам понадобится у каждой из рассматриваемых систем выделить специальные последовательности корней. Сначала мы покажем, что делать в общем случае для систем корней A_l, D_l, E_l, B_l, а потом явно проведем доказательство для систем G_2 и F_4.

Выделенные корни у системы A_l.

Пусть у системы корней A_l простые корни — $\alpha_1, \dots, \alpha_l$. Максимальный корень этой системы — $\beta_{1,l} = \alpha_1 + \dots + \alpha_l$, а любой корень имеет вид $\beta_{i,j} = \alpha_i + \alpha_{i+1} + \dots + \alpha_{j-1} + \alpha_j$, где $1 \leqslant i \leqslant j \leqslant l$. У данной системы мы будем рассматривать последовательность корней $\beta_{1,l}, \beta_{2,l}, \dots, \beta_{l-1,l}, \beta_l$. Любой корень системы A_l — это разность двух различных корней нашей последовательности (либо элемент этой последовательности).

Выделенные корни системы D_l.

Корни системы D_l имеют вид $\pm e_i \pm e_j$, $1 \leqslant i < j \leqslant l$, $\{e_1, \dots, e_l\}$ — ортонормированный базис пространства $\mathbb{R}^l$. Простые корни — это $\alpha_1 = e_1 - e_2, \alpha_2 = e_2 - e_3, \dots, \alpha_{l-2} = e_{l-2} - e_{l-1}, \alpha_{l-1} = e_{l-1} - e_l, \alpha_l = e_{l-1} - e_l$. Максимальный корень имеет вид $e_1 + e_2 = \alpha_1 + 2\alpha_2 + 2\alpha_3 + \dots + 2\alpha_{l-2} + \alpha_{l-1} + \alpha_l$. У данной системы корней мы будем рассматривать последовательность

$$\begin{aligned}
&e_1 + e_2 = \alpha_1 + 2\alpha_2 + 2\alpha_3 + \dots + 2\alpha_{l-2} + \alpha_{l-1} + \alpha_l,\\
&e_1 + e_3 = \alpha_1 + \alpha_2 + 2\alpha_3 + \dots + 2\alpha_{l-2} + \alpha_{l-1} + \alpha_l,\\
&e_2 + e_3 = \alpha_2 + 2\alpha_3 + \dots + 2\alpha_{l-2} + \alpha_{l-1} + \alpha_l,\\
&e_2 + e_4 = \alpha_2 + \alpha_3 + \dots + 2\alpha_{l-2} + \alpha_{l-1} + \alpha_l,\\
&\dots\dots\dots\dots\dots\dots,\\
&e_2 + e_{l-2} = \alpha_2 + \dots + \alpha_{l-3} + 2\alpha_{l-2} + \alpha_{l-1} + \alpha_l,\\
&e_2 + e_{l-1} = \alpha_2 + \dots + \alpha_{l-3} + \alpha_{l-2} + \alpha_{l-1} + \alpha_l,\\
&e_2 - e_l = \alpha_2 + \dots + \alpha_{l-2} + \alpha_{l-1},\\
&e_2 - e_{l-1} = \alpha_2 + \dots + \alpha_{l-2},\\
&\dots\dots\dots\dots\dots\dots,\\
&e_2 - e_3 = \alpha_2.
\end{aligned}$$

Каждый следующий элемент последовательности получается из предыдущего вычитанием простого корня. К тому же, любой корень системы D_l — это либо член последовательности, либо разность некоторых двух корней рассматриваемой последовательности $(e_i - e_j = (e_2 + e_i) - (e_2 + e_j),\ e_i + e_j = (e_2 + e_i) - (e_2 - e_j))$.

Выделенные корни системы E_l.

Так как системы корней E_6 и E_7 вложены в систему E_8, то для удобства будет рассматривать именно эту систему.

Корни системы E_8 имеют вид $\pm e_i \pm e_j$, $1 \leqslant i < j \leqslant 8$ и $\frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4 \pm e_5 \pm e_6 \pm e_7 \pm e_8)$, количество минусов нечетно. Простые корни: $\alpha_1 = e_1 - e_2$, $\alpha_2 = \frac{1}{2}(-e_1 - e_2 - e_3 + e_4 + e_5 + e_6 + e_7 + e_8)$, $\alpha_3 = e_2 - e_3$, $\alpha_4 = e_3 - e_4$, $\alpha_5 = e_4 - e_5$, $\alpha_6 = e_5 - e_6$, $\alpha_7 = e_6 - e_7$, $\alpha_8 = e_7 - e_8$. Максимальный корень имеет вид $\frac{1}{2}(e_1 + e_2 + e_3 + e_4 + e_5 + e_6 + e_7 - e_8) = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 5\alpha_5 + 4\alpha_6 + 3\alpha_7 + 2\alpha_8$. Мы будем рассматривать следующую последовательность:

$$
\begin{aligned}
&\frac{1}{2}(e_1+e_2+e_3+e_4+e_5+e_6+e_7-e_8)=2\alpha_1+3\alpha_2+4\alpha_3+6\alpha_4+5\alpha_5+4\alpha_6+3\alpha_7+2\alpha_8,\\
&\frac{1}{2}(e_1+e_2+e_3+e_4+e_5+e_6-e_7+e_8)=2\alpha_1+3\alpha_2+4\alpha_3+6\alpha_4+5\alpha_5+4\alpha_6+3\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1+e_2+e_3+e_4+e_5-e_6+e_7+e_8)=2\alpha_1+3\alpha_2+4\alpha_3+6\alpha_4+5\alpha_5+4\alpha_6+2\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1+e_2+e_3+e_4-e_5+e_6+e_7+e_8)=2\alpha_1+3\alpha_2+4\alpha_3+6\alpha_4+5\alpha_5+3\alpha_6+2\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1+e_2+e_3-e_4+e_5+e_6+e_7+e_8)=2\alpha_1+3\alpha_2+4\alpha_3+6\alpha_4+4\alpha_5+3\alpha_6+2\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1+e_2-e_3+e_4+e_5+e_6+e_7+e_8)=2\alpha_1+3\alpha_2+4\alpha_3+5\alpha_4+4\alpha_5+3\alpha_6+2\alpha_7+\alpha_8,\\
&e_1+e_2=2\alpha_1+2\alpha_2+4\alpha_3+5\alpha_4+4\alpha_5+3\alpha_6+2\alpha_7+\alpha_8,\\
&e_1+e_3=2\alpha_1+2\alpha_2+3\alpha_3+5\alpha_4+4\alpha_5+3\alpha_6+2\alpha_7+\alpha_8,\\
&e_2+e_3=\alpha_1+2\alpha_2+3\alpha_3+5\alpha_4+4\alpha_5+3\alpha_6+2\alpha_7+\alpha_8,\\
&e_2+e_4=\alpha_1+2\alpha_2+3\alpha_3+4\alpha_4+4\alpha_5+3\alpha_6+2\alpha_7+\alpha_8,\\
&e_2+e_5=\alpha_1+2\alpha_2+3\alpha_3+4\alpha_4+3\alpha_5+3\alpha_6+2\alpha_7+\alpha_8,\\
&e_3+e_5=\alpha_1+2\alpha_2+2\alpha_3+4\alpha_4+3\alpha_5+3\alpha_6+2\alpha_7+\alpha_8,\\
&e_4+e_5=\alpha_1+2\alpha_2+2\alpha_3+3\alpha_4+3\alpha_5+3\alpha_6+2\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1+e_2+e_3+e_4+e_5-e_6-e_7-e_8)=\alpha_1+\alpha_2+2\alpha_3+3\alpha_4+3\alpha_5+3\alpha_6+2\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1+e_2+e_3+e_4-e_5+e_6-e_7-e_8)=\alpha_1+\alpha_2+2\alpha_3+3\alpha_4+3\alpha_5+2\alpha_6+2\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1+e_2+e_3-e_4+e_5+e_6-e_7-e_8)=\alpha_1+\alpha_2+2\alpha_3+3\alpha_4+2\alpha_5+2\alpha_6+2\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1+e_2-e_3+e_4+e_5+e_6-e_7-e_8)=\alpha_1+\alpha_2+2\alpha_3+2\alpha_4+2\alpha_5+2\alpha_6+2\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1-e_2+e_3+e_4+e_5+e_6-e_7-e_8)=\alpha_1+\alpha_2+\alpha_3+2\alpha_4+2\alpha_5+2\alpha_6+2\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1-e_2+e_3+e_4+e_5-e_6+e_7-e_8)=\alpha_1+\alpha_2+\alpha_3+2\alpha_4+2\alpha_5+2\alpha_6+\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1-e_2+e_3+e_4-e_5+e_6+e_7-e_8)=\alpha_1+\alpha_2+\alpha_3+2\alpha_4+2\alpha_5+\alpha_6+\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1-e_2+e_3-e_4+e_5+e_6+e_7-e_8)=\alpha_1+\alpha_2+\alpha_3+2\alpha_4+\alpha_5+\alpha_6+\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1-e_2-e_3+e_4+e_5+e_6+e_7-e_8)=\alpha_1+\alpha_2+\alpha_3+\alpha_4+\alpha_5+\alpha_6+\alpha_7+\alpha_8,\\
&e_1-e_8=\alpha_1+\alpha_3+\alpha_4+\alpha_5+\alpha_6+\alpha_7+\alpha_8,\\
&e_1-e_7=\alpha_1+\alpha_3+\alpha_4+\alpha_5+\alpha_6+\alpha_7,\\
&e_1-e_6=\alpha_1+\alpha_3+\alpha_4+\alpha_5+\alpha_6,\\
&e_1-e_5=\alpha_1+\alpha_3+\alpha_4+\alpha_5,\\
&e_1-e_4=\alpha_1+\alpha_3+\alpha_4,\\
&e_1-e_3=\alpha_1+\alpha_3,\\
&e_1-e_2=\alpha_1.
\end{aligned}
$$

Любой корень системы E_8 — это либо член последовательности, либо разность некоторых двух корней рассматриваемой последовательности (проверяется непосредственным подсчетом), за исключением следующих корней:

$$
\begin{aligned}
&\frac{1}{2}(e_1-e_2-e_3+e_4+e_5+e_6-e_7+e_8)=\alpha_1+\alpha_2+\alpha_3+\alpha_4+\alpha_5+\alpha_6+\alpha_7,\\
&\frac{1}{2}(e_1-e_2+e_3-e_4+e_5+e_6-e_7+e_8)=\alpha_1+\alpha_2+\alpha_3+2\alpha_4+\alpha_5+\alpha_6+\alpha_7,\\
&\frac{1}{2}(e_1-e_2+e_3+e_4+e_5-e_6-e_7+e_8)=\alpha_1+\alpha_2+\alpha_3+2\alpha_4+2\alpha_5+2\alpha_6+\alpha_7,
\end{aligned}
$$

$$
\begin{aligned}
&\frac{1}{2}(e_1+e_2-e_3-e_4+e_5+e_6+e_7-e_8)=\alpha_1+\alpha_2+2\alpha_3+2\alpha_4+\alpha_5+\alpha_6+\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1+e_2-e_3+e_4+e_5-e_6+e_7-e_8)=\alpha_1+\alpha_2+2\alpha_3+2\alpha_4+2\alpha_5+2\alpha_6+\alpha_7+\alpha_8\\
&\frac{1}{2}(e_1+e_2+e_3-e_4+e_5-e_6+e_7-e_8)=\alpha_1+\alpha_2+2\alpha_3+3\alpha_4+2\alpha_5+2\alpha_6+\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1+e_2+e_3+e_4-e_5-e_6+e_7-e_8)=\alpha_1+\alpha_2+2\alpha_3+3\alpha_4+3\alpha_5+2\alpha_6+\alpha_7+\alpha_8,\\
&e_1+e_8=2\alpha_1+2\alpha_2+3\alpha_3+4\alpha_4+3\alpha_5+2\alpha_6+\alpha_7,\\
&e_1+e_7=2\alpha_1+2\alpha_2+3\alpha_3+4\alpha_4+3\alpha_5+2\alpha_6+\alpha_7+\alpha_8,\\
&e_1+e_6=2\alpha_1+2\alpha_2+3\alpha_3+4\alpha_4+3\alpha_5+2\alpha_6+2\alpha_7+\alpha_8,\\
&\frac{1}{2}(e_1-e_2+e_3+e_4+e_5+e_6+e_7+e_8)=2\alpha_1+3\alpha_2+3\alpha_3+5\alpha_4+4\alpha_5+3\alpha_6+2\alpha_7+\alpha_8.
\end{aligned}
$$

Выделенные корни системы B_l.

Как мы помним, любой корень системы B_l имеет вид $\pm e_i\pm e_j$, $i\neq j$, либо $\pm e_i$.

Рассмотрим последовательность

$$
\begin{aligned}
\gamma_1&=e_1+e_2=\alpha_1+2\alpha_2+\dots+2\alpha_l,\\
\gamma_2&=e_1+e_3=\alpha_1+\alpha_2+2\alpha_3+\dots+2\alpha_l,\\
&\dots\dots\dots\dots\\
\gamma_{l-1}&=e_1+e_l=\alpha_1+\alpha_2+\dots+\alpha_{l-1}+2\alpha_l,\\
\gamma_l&=e_2+e_l=\alpha_2+\dots+\alpha_{l-1}+2\alpha_l,\\
\gamma_{l+1}&=e_2=\alpha_2+\dots+\alpha_{l-1}+\alpha_l,\\
\gamma_{l+2}&=e_2-e_l=\alpha_2+\dots+\alpha_{l-1},\\
&\dots\dots\dots\dots\\
\gamma_{2l-2}&=e_2-e_4=\alpha_2+\alpha_3,\\
\gamma_{2l-1}&=e_2-e_3=\alpha_2.
\end{aligned}
$$

Таким образом, мы можем считать, что для всех рассматриваемых систем корней мы выделили последовательность $\gamma_1,\gamma_2,\dots\gamma_k$ положительных корней со следующими свойствами:

1. γ_1 — это максимальный корень системы.

2. γ_k — простой корень.

3. Каждый следующий корень последовательности получается из предыдущего вычитанием некоторого простого корня, при этом при первых l вычитаниях все вычитаемые корни различны.

4. Все корни в системах A_l, D_l — это либо элементы соответствующих последовательностей, либо разности каких-то двух корней из этих последовательностей. Для систем E_l, B_l это верно за несколькими исключениями, выписанными в отдельный список.

Рассмотрим в матрице X место (μ,ν), $\mu,\nu\in\Phi$.

Чтобы понять, что стоит в матрице на этом месте, надо найти все последовательности корней $\beta_1,\dots,\beta_p$, обладающие следующими двумя свойствами:

1. $\mu+\beta_1\in\Phi$, $\mu+\beta_1+\beta_2\in\Phi$, $\dots$, $\mu+\beta_1+\dots+\beta_i\in\Phi$, $\dots$, $\mu+\beta_1+\dots+\beta_p=\nu$.

2. В изначально пронумерованной последовательности $\alpha_1,\dots,\alpha_m,-\alpha_1,\dots,-\alpha_m$ корни $\beta_1,\dots,\beta_p$ расположены строго справа налево.

В результате в матрице X на месте (μ,ν) стоит сумма всех произведений $\pm\beta_1\cdot\beta_2\dots\beta_p$ по всем последовательностям корней с этими двумя свойствами, умноженная на $d_\mu=\lambda s_1^{\langle\alpha_1,\mu\rangle}\dots s_l^{\langle\alpha_l,\mu\rangle}$. Если $\mu=\nu$, то к сумме нужно добавить 1.

Будем находить искомые числа $\lambda,s_1,\dots,s_l,t_1,\dots,t_m,u_1,\dots,u_m$ по шагам.

Сначала рассмотрим в матрице X место $(-\gamma_1,-\gamma_1)$. К корню $-\gamma_1$ нельзя прибавить отрицательный корень так, чтобы в результате получился снова корень. Если же в последовательности $\beta_1,\dots,\beta_p$ первый корень положительный, то все остальные корни тоже должны быть положительны. Таким образом, на месте $(-\gamma_1,-\gamma_1)$ стоит просто $d_{-\gamma_1}$, которое мы сразу и найдем. Теперь рассмотрим место $(-\gamma_1,-\gamma_2)$. По тем же причинам, что и в предыдущем предложении, искомой последовательностью может быть только $\alpha_{k_1}=\gamma_1-\gamma_2$, т. е. некоторый простой корень α_{k_1}. Таким образом, на этом месте стоит $\pm d_{-\gamma_1}t_{k_1}$. Значит, мы нашли еще и t_{k_1}. Если мы рассмотрим места $(-\gamma_2,-\gamma_2)$ и $(-\gamma_2,-\gamma_1)$, то убедимся, что по аналогичным причинам на них стоят $d_{-\gamma_2}(1\pm u_{k_1}t_{k_1}$ и $\pm d_{-\gamma_2}u_{k_1}$ соответственно. Отсюда мы найдем $d_{-\gamma_2}$ и u_{k_1}.

Перейдем теперь ко второму шагу. Из описанных выше соображений в матрице X на месте $(-\gamma_2,-\gamma_3)$ стоит $d_{-\gamma_2}(\pm t_{k_2}\pm u_{k_1}t_{k_{1,2}})$, где $\alpha_{k_2}=\gamma_2-\gamma_3$, $\alpha_{k_{1,2}}=\alpha_{k_1}+\alpha_{k_2}$; на месте $(-\gamma_3,-\gamma_2)$ — $d_{-\gamma_3}(\pm u_{k_2}\pm u_{k_{1,2}}t_{k_1})$; на месте $(-\gamma_1,-\gamma_3)$ — $d_{-\gamma_1}(\pm t_{k_{1,2}}\pm t_{k_1}t_{k_2})$ (второго слагаемого может не быть, если $k_1<k_2$); на месте $(-\gamma_3,-\gamma_1)$ стоит $d_{-\gamma_3}(\pm u_{k_{1,2}}\pm u_{k_2}u_{k_1})$ (второго слагаемого может не быть, если $k_2<k_1$), и, наконец, на месте $(-\gamma_3,-\gamma_3)$ — $d_{-\gamma_3}(1\pm u_{k_{1,2}}t_{k_{1,2}}\pm u_{k_1}t_{k_1})$. Из полученных пяти уравнений с 5 неизвестными (лежащими в радикале) мы однозначно можем найти неизвестные, после чего считать, что нам известны $d_{-\gamma_1},d_{-\gamma_2},d_{-\gamma_3},t_1,t_2,t_{1,2},u_1,u_2,u_{1,2}$.

Пусть теперь нам известны числа t_i,u_j для всех индексов, соответствующих корням, равным разностям $\gamma_p-\gamma_q$, $1\leqslant p,q<s$, и все $d_{-\gamma_r}$, $1\leqslant r<s$, при этом $s\leqslant l+1$. Рассмотрим места $(-\gamma_1,-\gamma_s)$, $(-\gamma_s,-\gamma_1)$, $(-\gamma_2,-\gamma_s)$, $(-\gamma_s,-\gamma_2)$, $\dots$, $(-\gamma_{s-1},-\gamma_s)$, $(-\gamma_s,-\gamma_{s-1})$ и $(-\gamma_s,-\gamma_s)$ в матрице X. Очевидно, что на каждом месте вида $(-\gamma_i,-\gamma_s)$, $1\leqslant i<s$, стоит сумма числа t_p, где p — номер корня $\gamma_i-\gamma_s$ (если это корень), и произведений разных чисел t_a,u_b, из которых только одно число в произведении еще не является известным, а все остальные — это известные числа, и все они из радикала, умноженная на $d_{-\gamma_i}$. Ровно то же самое происходит на местах $(-\gamma_s,-\gamma_i)$, $1\leqslant i<s$, только там без множителей появляется не t_p, а u_p. На последнем месте находится $d_{-\gamma_s}(1+\Sigma)$, где Σ — это тоже сумма описанного выше вида. Таким образом, мы имеем ровно на одно больше (неоднородных) линейных уравнений, чем есть еще не полученных корней вида $\pm(\gamma_i-\gamma_s)$, с тем же количеством неизвестных, в каждом уравнении ровно у одного неизвестного стоит обратимый коэффициент, а остальные коэффициенты лежат в радикале, для разных уравнений такие неизвестные различны. Очевидно, что такая система уравнений имеет решение, и ровно одно. Следовательно, мы осуществили шаг индукции и теперь нам известны числа t_i,u_j для всех индексов, соответствующих корням, равным разностям $\gamma_p-\gamma_q$, $1\leqslant p,q\leqslant s$, а также число $d_{-\gamma_s}$.

После $l{+}1$-го шага ($s=l{+}1$) мы будем знать все $d_{-\gamma_1},\dots,d_{-\gamma_{l+1}}$, по которым однозначно восстановим $\lambda,s_1,\dots,s_l$. После этого нам станут известны все $d_{-\gamma_i}$, $l+1<i\leqslant\gamma_k$. На

последующих шагах не будем рассматривать последнюю позицию вида $(-\gamma_i, -\gamma_i)$, получим уравнений и неизвестных на одно меньше.

На самом последнем шаге нам уже известны числа t_i, u_j для всех индексов, соответствующих корням, равным разностям $\gamma_p - \gamma_q$, $1 \leqslant p, q \leqslant k$. Рассмотрим теперь в матрице X места $(-\gamma_1, h_{\gamma_1})$, $(h_{\gamma_1}, -\gamma_1)$, $(-\gamma_2, h_{\gamma_2})$, $(h_{\gamma_2}, -\gamma_2)$, ..., $(-\gamma_k, h_{\gamma_k})$, $(h_{\gamma_k}, -\gamma_k)$. Совершенно аналогично предыдущему рассуждению мы найдем все коэффициенты t и u, соответствующие корням $\pm\gamma_1, \dots, \pm\gamma_k$.

После этого в системах A_l и D_l мы будем знать все коэффициенты в произведении; кроме того, в доказательстве леммы описано, каким местам в матрице X они будут соответствовать.

В системах корней E_l, B_l окажется несколько корней, для которых мы не получили искомые коэффициенты. Посмотрим, что делать в этом случае на примере системы E_8. Упорядочим исключенные корни по высоте, назовем их $\beta_1, \dots, \beta_{11}$. Заметим, что: $\delta_1 := \gamma_2 - \beta_1 \in \Phi, \gamma_1 - \beta_1 \notin \Phi$, $\delta_2 := \gamma_2 - \beta_2 \in \Phi, \gamma_1 - \beta_2 \notin \Phi$, $\delta_3 := \gamma_2 - \beta_3 \in \Phi, \gamma_1 - \beta_3 \notin \Phi$, $\delta_4 := \gamma_1 - \beta_4 \in \Phi, \dots$, $\delta_7 := \gamma_1 - \beta_7 \in \Phi$, $\delta_8 := \gamma_2 - \beta_8 \in \Phi, \gamma_1 - \beta_8 \notin \Phi$, $\delta_9 := \gamma_1 - \beta_9 \in \Phi$, $\delta_{10} := \gamma_1 - \beta_{10} \in \Phi$, $\delta_{11} := \gamma_2 - \beta_{11} \in \Phi, \gamma_1 - \beta_{11} \notin \Phi$.

Начнем с корня β_1. Рассмотрим в матрице X место $(-\gamma_2, -\delta_1)$. На этом месте в матрице стоит (умноженная на известное число) сумма t_p, соответствующего корню β_1, и произведений чисел t_i, u_j, соответствующих корням меньшей высоты. Так как для всех высот, меньших высоты корня β_1, мы уже знаем коэффициенты t, u, то найдем искомый коэффициент t_p непосредственно. Аналогично мы найдем коэффициент u_p, рассмотрев место $(-\delta_1, -\gamma_2)$.

Теперь найдены все коэффициенты для всех корней высоты, меньшей высоты корня β_2. Благодаря этому мы полностью сможем повторить предыдущее рассуждение с местами в матрице $(-\gamma_2, -\delta_2)$ и $(-\delta_2, -\gamma_2)$. Далее будем действовать аналогично, но только для корней $\beta_4, \beta_5, \beta_6, \beta_7.\beta_9, \beta_{10}$ в матрице X будем рассматривать не места $(-\gamma_2, -\delta_i)$ и $(-\delta_i, -\gamma_2)$, а места $(-\gamma_1, -\delta_i)$ и $(-\delta_i, -\gamma_1)$.

Для серий корней A_l, B_l, D_l, E_l лемма доказана.

Перейдем теперь к конкретному доказательству для системы корней F_4.

Система корней F_4.

Рассмотрим явную последовательность корней: $\gamma_1 = \alpha_1$, $\gamma_2 = \alpha_5 = \alpha_1 + \alpha_2$, $\gamma_3 = \alpha_8 = \alpha_1+\alpha_2+\alpha_3$, $\gamma_4 = \alpha_{12} = \alpha_1+\alpha_2+2\alpha_3$, $\gamma_5 = \alpha_{15} = \alpha_1+\alpha_2+2\alpha_3+\alpha_4$, $\gamma_6 = \alpha_{17} = \alpha_1+2\alpha_2+2\alpha_3+\alpha_4$, $\gamma_7 = \alpha_{19} = \alpha_1+2\alpha_2+3\alpha_3+\alpha_4$, $\gamma_8 = \alpha_{21} = \alpha_1+2\alpha_2+3\alpha_3+2\alpha_4$, $\gamma_9 = \alpha_{22} = \alpha_1+2\alpha_2+4\alpha_3+2\alpha_4$, $\gamma_{10} = \alpha_{23} = \alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4$, $\gamma_{11} = \alpha_{24} = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4$.

Все корни в F_4, за исключением α_{14} и α_{18}, — это разности различных двух корней этой последовательности (или члены самой последовательности).

Кроме того, γ_1 — простой корень, γ_{11} — максимальный корень системы, любой корень последовательности получается из предыдущего прибавлением простого корня.

Как и выше, будем находить требуемые элементы $s_1, \dots, s_4, t_1, \dots, t_m, u_1, \dots, u_m$ по шагам.

Для начала рассмотрим в матрице X позицию $(-\gamma_{11}, -\gamma_{11})$. Из описанных выше соображений на ней стоит элемент $1 \cdot d_\nu$. Таким образом, мы знаем $d_{-\gamma_{11}}$. Аналогично, на позиции $(-\gamma_{11}, -\gamma_{10})$ стоит $d_{-\gamma_{11}} t_1$, то есть мы знаем $d_{-\gamma_{11}}$, элемент t_1 мы можем найти из позиции $(-\alpha_{24}, -\alpha_{23})$. Рассмотрев позиции $(-\gamma_{10}, -\gamma_{10})$ и $(-\gamma_{10}, -\gamma_{11})$, мы видим по тем же причинам $d_{-\gamma_{10}}(1 \pm u_1t_1)$ и $\pm d_{-\gamma_{10}}u_1$ на них. Таким образом, мы находим $d_{-\gamma_{10}}$ и u_1.

Перейдем к следующему шагу. У матрицы X на месте $(-\gamma_{10}, -\gamma_9)$ стоит $d_{-\gamma_{10}}(\pm t_2 \pm u_1t_5)$; на месте $(-\gamma_9, -\gamma_{10})$ — $d_{-\gamma_9}(\pm u_2 \pm u_5t_1)$; на месте $(-\gamma_{11}, -\gamma_9)$ — $\pm d_{-\gamma_{11}}t_5$ (второе слагаемое отсутствует, так как α_1 находится раньше, чем α_2); на месте $(-\gamma_9, -\gamma_{11})$ — $d_{-\gamma_9}(\pm u_5 \pm u_2u_1)$; наконец, на позиции $(-\gamma_9, -\gamma_9)$ стоит $d_{-\gamma_9}(1 + \pm u_5t_5 \pm u_2t_2)$. Из позиции $(-\gamma_{11}, -\gamma_9)$ мы находим t_5, далее из позиции $(-\gamma_{10}, -\gamma_9)$ находим t_2, из остальных трех позиций вместе мы можем узнать $u_2, u_5, d_{-\gamma_9}$. Таким образом, мы уже знаем $t_1, t_2, t_5, u_1, u_2, u_5, d_{-\gamma_9}, d_{-\gamma_{10}}, d_{-\gamma_{11}}$.

На третьем шаге мы рассмотрим места $(-\gamma_9, -\gamma_8)$ с $d_{-\gamma_9}(\pm t_3 \pm u_2t_6 \pm u_5t_8)$, $(-\gamma_8, -\gamma_9)$ с $d_{-\gamma_8}(\pm u_3 \pm t_2u_6 \pm t_5u_8)$, $(-\gamma_{10}, -\gamma_8)$ с $d_{-\gamma_{10}}(\pm t_6 \pm u_1t_8)$, $(-\gamma_8, -\gamma_{10})$ с $d_{-\gamma_8}(\pm u_6 \pm u_2u_3 \pm t_1u_8)$, $(-\gamma_{11}, -\gamma_8)$ с $d_{-\gamma_{11}}(\pm t_8 \pm t_5t_3)$, $(-\gamma_8, -\gamma_{11})$ с $d_{-\gamma_8}(\pm u_8 \pm u_3u_2u_1 \pm u_6u_1)$, и $(-\gamma_8, -\gamma_8)$ с $d_{-\gamma_8}(1 \pm u_3t_3 \pm u_5t_5 \pm u_8t_8 \pm u_8t_5t_3)$. Из полученных семи уравнений с семью неизвестными мы можем найти все $t_3, u_3, t_6, u_6, t_8, u_8$ и $d_{-\gamma_8}$.

Аналогично на следующем шаге рассмотрим позиции $(-\gamma_8, -\gamma_7)$, $(-\gamma_7, -\gamma_8)$, $(-\gamma_9, -\gamma_7)$, $(-\gamma_7, -\gamma_9)$, $(-\gamma_{10}, -\gamma_7)$, $(-\gamma_7, -\gamma_{10})$, $(-\gamma_{11}, -\gamma_7)$, $(-\gamma_7, -\gamma_{11})$, и $(-\gamma_7, -\gamma_7)$, и найдем t_4, u_4, t_7, u_7, t_9, u_9, t_{11}, u_{11}, $d_{-\gamma_7}$.

Теперь мы знаем $d_{-\gamma_7}, d_{-\gamma_8}, d_{-\gamma_9}, d_{-\gamma_{10}}$ and $d_{-\gamma_{11}}$, т. е. $\lambda s_4/s_3$, λ/s_4, $\lambda s_2/s_3$, $\lambda s_1/s_2$ and λ/s_1. Значит, мы знаем все s_i, $i = 1, \ldots, 4$, λ, и, следовательно, все $d_{-\gamma_i}$.

Предположим теперь, что нам известны все элементы t_i, u_j для всех индексов, соответствующих корням вида $\gamma_p - \gamma_q$, $11 \geqslant p, q > s$. Рассмотрим позиции $(-\gamma_{11}, -\gamma_s)$, $(-\gamma_s, -\gamma_{11})$, $(-\gamma_{10}, -\gamma_s)$, $(-\gamma_s, -\gamma_{10})$, $\ldots$, $(-\gamma_{s+1}, -\gamma_s)$, $(-\gamma_s, -\gamma_{s+1})$ в матрице X. Ясно, что на каждом месте $(-\gamma_i, -\gamma_s)$, $1 \geqslant i > s$, стоит сумма t_p, где p — это номер корня $\gamma_i - \gamma_s$ (если это корень), и произведения различных элементов t_a, u_b, где лишь один член произведения есть переменная, которую мы пока не вычислили, все остальные сомножители известны и лежат в радикале; и вся эта сумма еще умножается на некоторый известный элемент $d_{-\gamma_i}$. Точно та же ситуация происходит на позициях $(-\gamma_s, -\gamma_i)$, $1 \geqslant i > s$, но не с t_p, а с u_p без множителя. Таким образом, мы имеем то же число неоднородных линейных уравнений, что и число корней вида $\pm(\gamma_i - \gamma_s)$, с тем же числом неизвестных, в каждом уравнении ровно одно неизвестное имеет обратимый коэффициент, остальные коэффициенты из радикала, для различных уравнений такие переменные различны. Ясно, что такая система имеет решение, при том единственное. Следовательно, мы можем провести шаг индукции и считать, что теперь известны элементы t_i, u_j для всех индексов, соответствующих корням $\gamma_p - \gamma_q$, $11 \geqslant p, q \geqslant s$.

На последнем шаге мы знаем элементы t_i, u_j для всех индексов, соответствующих корням $\gamma_p - \gamma_q$, $11 \geqslant p, q \leqslant 1$. Теперь рассмотрим в матрице X позиции $(-\gamma_{11}, h_{\gamma_{11}})$, $(h_{\gamma_{11}}, -\gamma_{11})$, $(-\gamma_{10}, h_{\gamma_{10}})$, $(h_{\gamma_{10}}, -\gamma_{10})$, $\ldots$, $(-\gamma_1, h_{\gamma_1})$, $(h_{\gamma_1}, -\gamma_1)$. Аналогично предыдущим рассуждениям мы сможем найти все t и u, соответствующие корням $\pm\gamma_1, \ldots, \pm\gamma_k$.

Мы не нашли пока требуемые коэффициенты для двух пар корней: $\pm\alpha_{14}$ и $\pm\alpha_{18}$. Заметим, что $\alpha_{14} + \alpha_{18} = \alpha_{24}$.

Рассмотрим в X позиции $(-\alpha_{24}, -\alpha_{14})$, $(-\alpha_{14}, -\alpha_{24})$, $(-\alpha_{24}, -\alpha_{18})$, $(-\alpha_{18}, -\alpha_{24})$. На них стоят суммы t_{18} (соответственно, u_{18}, t_{14}, u_{14}), и произведений элементов t_i, u_j, соответствующих корням меньшего веса. Так как для всех весов, меньших веса α_{14}, мы знаем t, u, то мы можем напрямую найти искомые коэффициенты.

Таким образом, для системы корней F_4 лемма полностью доказана.

Прямое рассмотрение системы корней G_2.

Прямым подсчетом получаем, что в матрице X $x_{12,12} = \frac{\lambda}{s_1^3 s_2^2}$, $x_{12,10} = -\frac{\lambda u_2}{s_1^3 s_2^2}$, откуда мы находим u_2; $x_{12,8} = \frac{\lambda u_3}{s_1^3 s_2^2}$, откуда получим u_3; аналогично, из $x_{12,6} = \frac{\lambda u_4}{s_1^3 s_2^2}$, $x_{12,4} = -\frac{\lambda u_5}{s_1^3 s_2^2}$ и $x_{12,14} = -\frac{\lambda(u_6+u_2u_5)}{s_1^3 s_2^2}$ мы узнаем u_4, u_5, u_6. Кроме того, из $x_{10,12} = \frac{\lambda t_2}{s_1^3 s_2}$ и $x_{10,10} = \frac{\lambda(1-t_2u_2)}{s_1^3 s_2}$ мы находим t_2 и $\frac{\lambda}{s_1^3 s_2}$, а следовательно, нам становится известным s_2.

Из $x_{10,8} = -\frac{\lambda(u_1-t_2u_3}{s_1^3 s_2}$ найдем u_1. Из первого уравнения мы можем выразить λ через s_1. Таким образом, λ можно больше не считать неизвестным. Теперь из системы уравнений

$$\begin{aligned}
x_{14,12} &= \lambda(t_2t_5 + 3t_3t_4 + 2t_6);\\
x_{4,12} &= \frac{\lambda(t_5 + 3t_1t_4 + 3t_1^2t_3 - t_1^3t_2)}{s_2};\\
x_{4,6} &= \frac{-t_1 + 2t_1^2u_1 - t_1^3u_1^2 + u_4t_5 + 3u_4t_1t_4 + 3u_4t_1^2t_3 - u_4t_1^3t_2)}{s_2};\\
x_{8,8} &= \frac{\lambda(1 - 3t_1u_1 - 3u_3t_3 + 3u_3t_1t_2)}{s_1^2 s_2};\\
x_{14,6} &= \lambda(-t_3 - 2t_4u_1 - t_5u_1^2 + u_4t_2t_5 + 3u_4t_3t_4 + 2u_4t_6);\\
x_{14,8} &= \lambda(t_4 + t_5u_1 + u_3t_2t_5 + 3u_3t_3t_4 + 2u_3t_6),
\end{aligned}$$

в которой неизвестными являются $s_1, t_1, t_3, t_4, t_5, t_6$, в каждом уравнении ровно одно неизвестное имеет обратимый коэффициент, для всех уравнений эти неизвестные различны, мы можем найти все шесть неизвестных.

Теперь мы знаем все искомые элементы кольца.

Таким образом, лемма полностью доказана. $\square$

Теперь вернемся к нашему главному доказательству. Напомним, что мы работаем с матрицей C, сравнимой с единичной по модулю радикала, и переводящей элементарную группу Шевалле в себя.

Для каждого корня $\alpha \in \Phi$ имеет место равенство

$$Cx_\alpha(1)C^{-1} = x_\alpha(1) \cdot g_\alpha, \quad g_\alpha \in G_{\mathrm{ad}}(\Phi, R, J). \tag{1.2}$$

Любой элемент $g_\alpha \in G_{\mathrm{ad}}(\Phi, R, J)$ можно разложить в произведение

$$t_{\alpha_1}(1+a_1)\dots t_{\alpha_l}(1+a_l)x_{\alpha_1}(b_1)\dots x_{\alpha_m}(b_m)x_{\alpha_{-1}}(c_1)\dots x_{\alpha_{-m}}(c_m), \tag{1.3}$$

где $a_1, \dots, a_l, b_1, \dots, b_m, c_1, \dots, c_m \in J$ (см., например, [70]).

Пусть $C = E + X = E + (x_{i,j})$. Тогда для каждого корня $\alpha \in \Phi$ можно записать матричное равенство 1.2 с неизвестными $x_{i,j}, a_1, \dots, a_l, b_1, \dots, b_m, c_1, \dots, c_m$, каждое из которых должно лежать в радикале.

Изменим эти равенства. Рассмотрим матрицу C и "представим себе", что это была матрица из леммы 1.16. Тогда по некоторым ее конкретным $n+1$ позициям мы можем "восстановить" все коэффициенты $\lambda, s_1, \dots, s_l, t_1, \dots, t_m, u_1, \dots, u_m$ в разложении матрицы в произведение из леммы 1.16. В результате мы получим матрицу $D \in \lambda G_{\mathrm{ad}}(\Phi, R, J)$, в которой каждый матричный коэффициент есть некоторая (известная) функция от коэффициентов матрицы C. Заменим теперь уравнения (1.2) на уравнения

$$D^{-1}Cx_\alpha(1)C^{-1}D = x_\alpha(1)\cdot {g_\alpha}', \quad {g_\alpha}' \in G_{\,\mathrm{ad}}\,(\Phi, R, J). \tag{1.4}$$

Это снова матричные равенства, но уже с неизвестными $y_{i,j}, a'_1, \dots, a'_l, b'_1, \dots, b'_m, c'_1, \dots, c'_m$, каждое из которых по-прежнему лежит в радикале, при этом каждое $y_{p,q}$ есть известная функция от (всех) $x_{i,j}$. Матрицу $D^{-1}C$ обозначим через C'.

Нам нужно показать, что решение существует только при всех переменных со штрихом, равных нулю. Некоторые $x_{i,j}$ при этом тоже будут равны нулю, а другие сократятся в уравнениях. Так как уравнения очень сложные, то будем рассматривать линеаризованную систему уравнений. Нам достаточно будет показать, что все переменные, не сокращающиеся в линеаризованной системе (пусть их q штук) участвуют в системе из q линейных уравнений с обратимым в кольце R определителем.

Иначе говоря, нам надо постепенно из матричных равенств показывать, что все присутствующие в уравнениях переменные обнуляются.

Понятно, что линеаризация произведения $Y^{-1}(E+X)$ даст нам некоторую матрицу $E+(z_{i,j})$, у которой все позиции, описанные в лемме 1.16, — нулевые.

Чтобы найти вид окончательной линеаризованной системы, запишем последнюю в форме:

$$\begin{aligned}(E+Z)x_\alpha(1) = x_\alpha(1)(E+a_1T_1+a_1^2\dots)\dots(E+a_lT_l+a_1^2\dots)\cdot\\ \cdot(E+b_1X_{\alpha_1}+b_1^2X_{\alpha_1}^2/2)\dots(E+c_mX_{-\alpha_1}+c_m^2X_{-\alpha_m}^2/2)(E+Z),\end{aligned}$$

где X_α — соответствующий элемент алгебры Ли в присоединенном представлении, матрица T_i диагональна, имеет на диагонали p в месте, соответствующем вектору v_k тогда и только тогда, когда в разложении корня α_k в сумму простых корней простой корень α_i входит в это разложение ровно p раз (p может быть нулевым или отрицательным); в местах, соответствующих векторам V_j, матрица имеет нули на диагонали.

Тогда линеаризованная система будет иметь вид

$$Zx_\alpha(1) - x_\alpha(1)(Z + a_1T_1 + \dots + a_lT_l + b_1X_{\alpha_1} + \dots + c_mX_{\alpha_m}) = 0.$$

Ясно, что такое равенство можно написать для каждого $\alpha\in\Phi$ (естественно, с другими a_j, b_j, c_j), а можно только для тех корней, которые порождают остальные, — для $\alpha_1, \dots, \alpha_l, -\alpha_1, \dots, -\alpha_l$. При этом количество свободных переменных не изменится.

1.7 Доказательство теоремы 3

Снова разделим системы корней на разные случаи и будем показывать, что у выведенных выше линейных систем существует лишь нулевое решение.

1.7.1 Линейные системы в случае A_2

В этом случае мы имеем четыре соотношения:

$$
\begin{cases}
Zx_{\alpha_1}(1)-x_{\alpha_1}(1)(X+a_{1,1}T_1+a_{2,1}T_2+\\
\qquad +b_{1,1}X_{\alpha_1}+b_{2,1}X_{\alpha_2}+b_{3,1}X_{\alpha_1+\alpha_2}+c_{1,1}X_{-\alpha_1}+c_{2,1}X_{-\alpha_2}+c_{3,1}X_{-\alpha_1-\alpha_2})=0;\\
Zx_{\alpha_2}(1)-x_{\alpha_2}(1)(X+a_{1,2}T_1+a_{2,2}T_2+\\
\qquad +b_{1,2}X_{\alpha_1}+b_{2,2}X_{\alpha_2}+b_{3,2}X_{\alpha_1+\alpha_2}+c_{1,2}X_{-\alpha_1}+c_{2,2}X_{-\alpha_2}+c_{3,2}X_{-\alpha_1-\alpha_2})=0;\\
Xx_{-\alpha_1}(1)-x_{-\alpha_1}(1)(X+a_{1,3}T_1+a_{2,3}T_2+\\
\qquad +b_{1,3}X_{\alpha_1}+b_{2,3}X_{\alpha_2}+b_{3,3}X_{\alpha_1+\alpha_2}+c_{1,3}X_{-\alpha_1}+c_{2,3}X_{-\alpha_2}+c_{3,3}X_{-\alpha_1-\alpha_2})=0;\\
Xx_{-\alpha_2}(1)-x_{-\alpha_2}(1)(X+a_{1,4}T_1+a_{2,4}T_2+\\
\qquad +b_{1,4}X_{\alpha_1}+b_{2,4}X_{\alpha_2}+b_{3,4}X_{\alpha_1+\alpha_2}+c_{1,4}X_{-\alpha_1}+c_{2,4}X_{-\alpha_2}+c_{3,4}X_{-\alpha_1-\alpha_2})=0.
\end{cases}
$$

При этом

$$
\begin{cases}
T_1=e_{1,1}-e_{2,2}+e_{5,5}-e_{6,6};\\
T_2=e_{3,3}-e_{4,4}+e_{5,5}-e_{6,6};\\
X_{\alpha_1}=-2e_{1,7}+e_{1,8}+e_{4,6}-e_{3,5}+e_{7,2};\\
X_{\alpha_2}=e_{3,7}-2e_{3,8}+e_{2,6}-e_{5,1}+e_{8,4};\\
X_{\alpha_1+\alpha_2}=-e_{5,7}-e_{5,8}-e_{1,4}+e_{3,2}+e_{7,6}+e_{8,6};\\
X_{-\alpha_1}=-2e_{2,7}+e_{2,8}+e_{3,5}-e_{6,4}+e_{7,1};\\
X_{-\alpha_2}=e_{4,7}-2e_{4,8}-e_{1,5}+e_{6,2}+e_{8,3};\\
X_{-\alpha_1-\alpha_2}=-e_{6,7}-e_{6,8}-e_{2,3}+e_{4,1}+e_{7,5}+e_{8,5}.
\end{cases}
$$

Матрица Z имеет вид

$$
\begin{pmatrix}
z_{11} & z_{12} & z_{13} & z_{14} & z_{15} & z_{16} & z_{17} & z_{18}\\
z_{21} & 0 & z_{23} & z_{24} & z_{25} & 0 & z_{27} & z_{28}\\
z_{31} & z_{32} & z_{33} & z_{34} & z_{35} & z_{36} & z_{37} & z_{38}\\
z_{41} & z_{42} & z_{43} & 0 & z_{45} & 0 & z_{47} & z_{48}\\
z_{51} & z_{52} & z_{53} & z_{54} & z_{55} & z_{56} & z_{57} & z_{58}\\
z_{61} & 0 & z_{63} & 0 & z_{65} & 0 & z_{67} & 0\\
z_{71} & z_{72} & z_{73} & z_{74} & z_{75} & z_{76} & z_{77} & z_{78}\\
z_{81} & z_{82} & z_{83} & z_{84} & z_{85} & 0 & z_{87} & z_{88}
\end{pmatrix}.
$$

Напрямую выписывая все уравнения системы и последовательно решая их, мы получим, что все переменные типа a_i, b_i, c_i , и матрица Z — нулевые.

Значит, для системы корней A_2 утверждение доказано.

1.7.2 Линейные системы в случаях A_l, D_l, E_l, $l\geqslant 3$

Пусть теперь мы имеем дело с произвольной из систем с простыми связями корней ранга, большего двух. Соотношений в такой ситуации можно рассматривать ровно $2l$ (соотношения для простых корней и им противоположных):

$$\begin{cases} Zx_{\alpha_1}(1) - x_{\alpha_1}(1)(Z + a_{1,1}T_1 + \dots + a_{l,1}T_l + \\ \qquad +b_{1,1}X_{\alpha_1} + \dots + b_{m,1}X_{\alpha_m} + c_{1,1}X_{-\alpha_1} + \dots + c_{m,1}X_{-\alpha_m}) = 0; \\ \dots \\ Zx_{\alpha_l}(1) - x_{\alpha_l}(1)(Z + a_{1,l}T_1 + \dots + a_{l,l}T_l + \\ \qquad +b_{1,l}X_{\alpha_1} + \dots + X_{\alpha_m}b_{m,1}X_{\alpha_m} + c_{1,l}X_{-\alpha_1} + \dots + c_{m,l}X_{-\alpha_m}) = 0; \\ Zx_{-\alpha_1}(1) - x_{-\alpha_1}(1)(Z + a_{1,l+1}T_1 + \dots + a_{l,l+1}T_l + \\ \qquad +b_{1,l+1}X_{\alpha_1} + \dots + b_{m,l+1}X_{\alpha_m} + c_{1,l+1}X_{-\alpha_1} + \dots + c_{m,l+1}X_{-\alpha_m}) = 0; \\ \dots \\ Zx_{-\alpha_l}(1) - x_{-\alpha_l}(1)(Z + a_{1,2l}T_1 + \dots + a_{l,2l}T_l + \\ \qquad +b_{1,2l}X_{\alpha_1} + \dots + b_{m,2l}X_{\alpha_m} + c_{1,2l}X_{-\alpha_1} + \dots + c_{m,2l}X_{-\alpha_m}) = 0. \end{cases}$$

В случае рассматриваемых систем корней

$$T_i = e_{\alpha_i,\alpha_i} - e_{-\alpha_i,-\alpha_i} + \sum_{j\neq i} k_j(e_{\alpha_j,\alpha_j} - e_{-\alpha_j,-\alpha_j}),$$

где $\alpha_j = k_j\alpha_i + \alpha$, простой корень α_i не входит в разложение корня α в сумму простых;

$$X_{\alpha_p} = e_{h_p,-\alpha_p} - \sum_{q=1}^{l} \langle \alpha_p, \alpha_q \rangle e_{\alpha_p,h_q} + \sum_{s,t:\alpha_p+\alpha_s=\alpha_t} e_{-\alpha_s,-\alpha_t} - e_{\alpha_t,\alpha_s}$$

для всех $\alpha_p \in \Phi$.

Пусть мы фиксировали полученную линейную однородную систему уравнений с описанными $n+1$ нулевыми позициями. Напомним, что наша цель — показать, что все значения $z_{i,j}$, $a_{s,t}, b_{s,t}, c_{s,t}$ — нулевые.

Будем для начала рассматривать пару соотношений с первым и $l+1$-м номером. Понятно, что все остальные соответствующие пары соотношений устроены совершенно аналогично (так как перестановкой базиса можно перевести любой корень в любой).

Можно так переименовать базис, что матрицы $x_{\alpha_1}(1)$ и $x_{-\alpha_1}(1)$ разбиваются на три диагональных блока: первый блок соответствует векторам базиса $\{x_{\alpha_1}, x_{-\alpha_1}, h_1, h_2\}$, второй — векторам $\{x_\alpha \mid \langle \alpha_1, \alpha \rangle = \pm 1\}$, третий — векторам $\{x_\alpha \mid \langle \alpha_1, \alpha \rangle = 0; h_3, \dots, h_l\}$. При этом последний блок просто единичен. Пусть

$$x_{\alpha_1}(1) = \begin{pmatrix} A & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & E \end{pmatrix}, \quad x_{-\alpha_1}(1) = \begin{pmatrix} A' & 0 & 0 \\ 0 & B' & 0 \\ 0 & 0 & E \end{pmatrix}$$

и пусть все рассматриваемые нами матрицы Y также разделены на блоки соответствующим образом:

$$Y = \begin{pmatrix} Y_{11} & Y_{12} & Y_{13} \\ Y_{21} & Y_{22} & Y_{23} \\ Y_{31} & Y_{32} & Y_{33} \end{pmatrix}.$$

Обозначим матрицу $a_{1,1}T_1 + a_{2,1}T_2 + \dots + a_{l,1}T_l + b_{1,1}X_{\alpha_1} + \dots + b_{m,1}X_{\alpha_m} + c_{1,1}X_{-\alpha_1} + \dots + c_{m,1}X_{-\alpha_m}$ через D. Заметим, что из построения базиса $D_{1,3} = D_{3,1} = 0$. Тогда первое соотношение будет выглядеть как

$$\begin{pmatrix} Z_{11}A & Z_{12}B & Z_{13} \\ Z_{21}A & Z_{22}B & Z_{23} \\ Z_{31}A & Z_{32}B & Z_{33} \end{pmatrix} = \begin{pmatrix} AZ_{11} & AZ_{12} & AZ_{13} \\ BZ_{21} & BZ_{22} & BZ_{23} \\ Z_{31} & Z_{32} & Z_{33} \end{pmatrix} + \begin{pmatrix} AD_{11} & AD_{12} & 0 \\ BD_{21} & BD_{22} & BD_{23} \\ 0 & D_{32} & D_{33} \end{pmatrix}.$$

Из написанного равенства сразу следует, что $D_{33} = 0$. Следовательно, $a_{3,1} = \dots = a_{l,1} = 0$, $b_{k,1} = c_{k,1} = 0$ при $\langle \alpha_1, \alpha_k \rangle = 0$.

Теперь рассмотрим положительный корень α такой, что $\beta = \alpha + \alpha_1 \in \Phi$ и α, β являются одними из первых $l+1$ членов последовательности $\gamma_1, \dots, \gamma_k$. Для системы корней A_l это γ_2, для системы D_l — γ_3, для системы E_8 — γ_3 (аналогичные пары корней в последовательности $\gamma_1, \dots, \gamma_k$ можно найти и для $\alpha_2, \dots, \alpha_l$ благодаря свойству 3 последовательности $\gamma_1, \dots, \gamma_k$).

Рассмотрим часть базиса $\alpha, -\alpha, \beta, -\beta$. Для матриц $x_{\alpha_1}(1)$ и $x_{-\alpha_1}(1)$ эта часть базиса выделяется прямым слагаемым, поэтому можно рассмотреть ее независимо. По построению мы знаем, что $z_{-\alpha,-\alpha} = z_{-\beta,-\beta} = z_{-\alpha,-\beta} = z_{\beta,-\alpha} = 0$. Получим соотношение

$$\begin{pmatrix} z_{\alpha,\alpha} & z_{\alpha,-\alpha} & z_{\alpha,\beta} & z_{\alpha,-\beta} \\ z_{-\alpha,\alpha} & 0 & z_{-\alpha,\beta} & 0 \\ z_{\beta,\alpha} & z_{\beta,-\alpha} & z_{\beta,\beta} & z_{\beta,-\beta} \\ z_{-\beta,\alpha} & 0 & z_{-\beta,\beta} & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \left(\begin{pmatrix} z_{\alpha,\alpha} & z_{\alpha,-\alpha} & z_{\alpha,\beta} & z_{\alpha,-\beta} \\ z_{-\alpha,\alpha} & 0 & z_{-\alpha,\beta} & 0 \\ z_{\beta,\alpha} & z_{\beta,-\alpha} & z_{\beta,\beta} & z_{\beta,-\beta} \\ z_{-\beta,\alpha} & 0 & z_{-\beta,\beta} & 0 \end{pmatrix} + \begin{pmatrix} a_\alpha & 0 & -c_{1,1} & 0 & \\ 0 & -a_\alpha & 0 & -b_{1,1} & \\ b_{1,1} & 0 & a_\beta & 0 & 0 \\ 0 & c_{1,1} & 0 & -a_\beta & \end{pmatrix} \right).$$

В результате мы получим, что должна быть равна нулю матрица

$$\begin{pmatrix} z_{\alpha,\beta} - a_\alpha & 0 & c_{1,1} & z_{\alpha,-\alpha} \\ z_{-\alpha,\beta} + z_{-\beta,\alpha} & c_{1,1} + a_\alpha & z_{-\beta,\beta} & b_{1,1} - a_\beta \\ z_{\beta,\beta} - z_{\alpha,\alpha} - a_\alpha - b_{1,1} & -z_{\alpha,-\alpha} & -z_{\alpha,\beta} + c_{1,1} - a_\beta & -z_{\beta,-\alpha} - z_{\alpha,-\beta} \\ z_{-\beta,\beta} & -c_{1,1} & 0 & a_\beta \end{pmatrix}.$$

Отсюда сразу видно, что $a_\alpha = a_\beta = b_{1,1} = c_{1,1} = 0$. Так как мы уже знаем, что $a_{3,1} = \dots = a_{l,1} = 0$, то $a_{1,1} = a_{2,1} = 0$.

Теперь рассмотрим такой корень $\alpha \in \Phi^+$, что $\alpha + \alpha_1 \in \Phi^+$. В последовательности $\gamma_1, \dots, \gamma_k$ найдем такие корни γ_p и γ_q, что $\gamma_q - \gamma_p = \alpha$. Так как все корни наших систем имеют одинаковую длину, то коэффициенты отражения $\langle\ ,\ \rangle$ билинейны по отношению к корням. Мы знаем, что $\langle \alpha, \alpha_1 \rangle = -1$, а для чисел $\langle \gamma_p, \alpha_1 \rangle$ и $\langle \gamma_q, \alpha_1 \rangle$ есть только возможности $0, 1, -1$. Из билинейности остаются всего две возможности, рассматриваемые ниже:

1) корень γ_p ортогонален к корню α_1, а корень γ_q — не ортогонален. Тогда $\gamma' = \gamma_q + \alpha_1$ — тоже корень, мы можем рассмотреть часть базиса $\gamma_p, -\gamma_p, \gamma_q, -\gamma_q, \gamma', -\gamma'$, которая

выделяется инвариантным прямым слагаемым для $x_{\alpha_1}(1)$. На этой части базиса

$$x_{\alpha_1}(1) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

у матрицы Z равны нулю (по лемме 1.16) $z_{-\gamma_p,-\gamma_q}$ и $z_{-\gamma_q,-\gamma_p}$, матрица D равна

$$\begin{pmatrix} 0 & 0 & -c_{\alpha,1} & 0 & -c_{\alpha+\alpha_1,1} & 0 \\ 0 & 0 & 0 & -b_{\alpha,1} & 0 & -b_{\alpha+\alpha_1} \\ b_{\alpha,1} & 0 & 0 & 0 & 0 & 0 \\ 0 & c_{\alpha,1} & 0 & 0 & 0 & 0 \\ b_{\alpha+\alpha_1,1} & 0 & 0 & 0 & 0 & 0 \\ 0 & c_{\alpha+\alpha_1,1} & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Теперь из основного соотношения будет следовать равенство нулю матрицы

$$\begin{pmatrix} 0 & 0 & z_{\gamma_p,\gamma'} + c_{\alpha,1} & 0 & c_{\alpha+\alpha_1,1} & -z_{\gamma_p,-\gamma_q} \\ 0 & 0 & z_{-\gamma_p,\gamma'} & b_{\alpha,1} & 0 & b_{\alpha+\alpha_1,1} \\ -b_{\alpha,1} & 0 & z_{\gamma_q,\gamma'} & 0 & 0 & -z_{\gamma_q,-\gamma_q} \\ z_{-\gamma',\gamma_p} & z_{-\gamma',-\gamma_p} - c_{\alpha,1} + c_{\alpha+\alpha_1,1} & z_{-\gamma_q,\gamma'} + z_{-\gamma',\gamma_q} & z_{-\gamma',-\gamma_q} & z_{-\gamma',\gamma'} & z_{-\gamma',-\gamma'} - z_{-\gamma_q,-\gamma_q} \\ -z_{\gamma_q,\gamma_p} - b_{\alpha,1} - b_{\alpha+\alpha_1,1} & -z_{\gamma_q,-\gamma_p} & z_{\gamma',\gamma'} - z_{\gamma_q,\gamma_q} & -z_{\gamma_q,-\gamma_q} & -z_{\gamma_q,\gamma'} & -z_{\gamma',-\gamma_q} - z_{\gamma_q,-\gamma'} \\ 0 & -c_{\alpha+\alpha_1} & z_{-\gamma',\gamma'} & 0 & 0 & z_{-\gamma',-\gamma_q} \end{pmatrix}.$$

Легко видеть, что тогда $b_{\alpha,1} = b_{\alpha+\alpha_1,1} = c_{\alpha+\alpha_1,1} = 0$.

2) Во втором случае может быть $\gamma'' = \gamma_p - \alpha_1 \in \Phi^+$, $\langle \gamma_q, \alpha_1 \rangle = 0$. Этот случай очень похож на предыдущий, в результате на части базиса $\gamma_p, -\gamma_p, \gamma_q, -\gamma_q, \gamma'', -\gamma''$ получается равной нулю матрица

$$\begin{pmatrix} -z_{\gamma'',\gamma_p} & -z_{\gamma_p,-\gamma''} - z_{\gamma'',-\gamma_p} & -z_{\gamma'',\gamma_q} + c_{\alpha,1} + c_{\alpha+\alpha_1,1} & -z_{\gamma'',-\gamma_q} & z_{\gamma_p,\gamma_p} - z_{\gamma'',\gamma''} & -z_{\gamma'',-\gamma''} \\ 0 & -z_{-\gamma_p,-\gamma''} & 0 & b_{\alpha,1} & z_{-\gamma_p,\gamma_p} & 0 \\ -b_{\alpha,1} & -z_{\gamma_q,-\gamma''} & 0 & 0 & z_{\gamma_q,\gamma_p} - b_{\alpha+\alpha_1,1} & 0 \\ 0 & -z_{-\gamma+q,-\gamma''} - c_{\alpha,1} & 0 & 0 & z_{-\gamma_q,\gamma_p} & -c_{\alpha+\alpha_1,1} \\ 0 & -z_{\gamma'',-\gamma''} & c_{\alpha+\alpha_1,1} & 0 & z_{\gamma'',\gamma_p} & 0 \\ z_{-\gamma_p,\gamma_p} & -z_{-\gamma'',-\gamma''} + z_{-\gamma_p.-\gamma_p} & z_{-\gamma_p,\gamma_q} & b_{\alpha+\alpha_1,1} - b_{\alpha,1} & z_{-\gamma'',\gamma_p} + z_{-\gamma_p,\gamma''} & z_{-\gamma_p,-\gamma''} \end{pmatrix}.$$

Снова сразу получаем $b_{\alpha,1} = b_{\alpha+\alpha_1,1} = c_{\alpha+\alpha_1,1} = 0$.

При рассмотрении пары корней γ_s, γ_t, для которой $\gamma_t - \gamma_s = \alpha + \alpha_1$ мы аналогично получим два случая и $c_{\alpha,1} = 0$.

Таким образом, мы доказали, что $a_{i,1} = 0$ для любого $i = 1, \ldots, l$, $b_{\alpha,1} = c_{\alpha,1} = 0$ для любого $\alpha \in \Phi$. Значит, матрица Z должна коммутировать с $x_{\alpha_1}(1)$.

Точно так же из остальных соотношений получим, что матрица Z коммутирует со всеми $x_\alpha(1)$, $\alpha \in \Phi$, и поэтому является скалярной. Так как у рассматриваемой матрицы есть нули на диагонали (по построению), то она нулевая. Теорема 1.3 доказана для рассматриваемых систем корней.

1.7.3 Система корней F_4

Матрица T_1 имеет вид

$$\mathrm{diag}\,[2,-2,-1,1,0,0,0,0,1,-1,-1,1,0,0,1,-1,-1,1,-1,1,1,-1,\\ 1,-1,-1,1,0,0,1,-1,-1,1,0,0,1,-1,0,0,0,0,0,0,0,0,-1,1,1,-1,0,0,0,0];$$

T_2 есть $w_1w_2T_1w_2^{-1}w_1^{-1}$; T_3 есть

$$\mathrm{diag}\,[0,0,-2,2,2,-2,-1,1,-2,2,0,0,1,-1,0,0,-1,1,2,-2,-1,1,\\ 2,-2,1,-1,0,0,1,-1,0,0,-1,1,0,0,1,-1,-2,2,0,0,2,-2,0,0,0,0,0,0,0,0];$$

матрица T_4 — это $w_3w_4T_3w_4^{-1}w_3^{-1}$.

Матрицы $X_{\alpha_1}, X_{\alpha_3}$ выписывались выше. Кроме того, $X_{-\alpha_1}=w_1X_{\alpha_1}w_1^{-1}$, $X_{-\alpha_3}=w_3X_{\alpha_3}w_3^{-1}$. Другие матрицы X_α получаются следующим образом: $X_{\pm\alpha_5}=w_2X_{\pm\alpha_1}w_2^{-1}$, $X_{\pm\alpha_2}=w_1X_{\pm\alpha_5}w_1^{-1}$, $X_{\pm\alpha_{10}}=w_3X_{\pm\alpha_2}w_3^{-1}$, $X_{\pm\alpha_{12}}=w_1X_{\pm\alpha_{10}}w_1^{-1}$, $X_{\pm\alpha_{14}}=w_2X_{\pm\alpha_{12}}w_2^{-1}$, $X_{\pm\alpha_{16}}=w_4X_{\pm\alpha_{10}}w_4^{-1}$, $X_{\pm\alpha_{18}}=w_1X_{\pm\alpha_{16}}w_1^{-1}$, $X_{\pm\alpha_{20}}=w_2X_{\pm\alpha_{18}}w_2^{-1}$, $X_{\pm\alpha_{22}}=w_3X_{\pm\alpha_{20}}w_3^{-1}$, $X_{\pm\alpha_{23}}=w_2X_{\pm\alpha_{22}}w_2^{-1}$, $X_{\pm\alpha_{24}}=w_1X_{\pm\alpha_{23}}w_1^{-1}$, $X_{\pm\alpha_7}=w_4X_{\pm\alpha_3}w_4^{-1}$, $X_{\pm\alpha_4}=w_3X_{\pm\alpha_7}w_3^{-1}$, $X_{\pm\alpha_6}=w_2X_{\pm\alpha_3}w_2^{-1}$, $X_{\pm\alpha_8}=w_1X_{\pm\alpha_6}w_1^{-1}$, $X_{\pm\alpha_9}=w_4X_{\pm\alpha_6}w_4^{-1}$, $X_{\pm\alpha_{11}}=w_1X_{\pm\alpha_9}w_1^{-1}$, $X_{\pm\alpha_{13}}=w_3X_{\pm\alpha_9}w_3^{-1}$, $X_{\pm\alpha_{15}}=w_1X_{\pm\alpha_{13}}w_1^{-1}$, $X_{\pm\alpha_{17}}=w_2X_{\pm\alpha_{15}}w_2^{-1}$, $X_{\pm\alpha_{19}}=w_3X_{\pm\alpha_{17}}w_3^{-1}$, $X_{\pm\alpha_{21}}=w_4X_{\pm\alpha_{19}}w_4^{-1}$.

По лемме 1.16 мы знаем, что следующие позиции в Z являются нулями: $(48,48)$, $(48,46)$, $(46,46)$, $(46,48)$, $(46,44)$, $(44,44)$, $(44,46)$, $(44,42)$, $(42,42)$, $(42,44)$, $(42,38)$, $(38,38)$, $(38,42)$, $(48,44)$, $(44,48)$, $(46,42)$, $(42,46)$, $(44,38)$, $(38,44)$, $(48,42)$, $(42,48)$, $(46,38)$, $(38,46)$, $(24,2)$, $(2,24)$, $(48,38)$, $(38,48)$, $(24,49)$, $(49,24)$, $(46,34)$, $(34,46)$, $(48,36)$, $(36,48)$, $(48,34)$, $(34,48)$, $(44,24)$, $(24,44)$, $(48,30)$, $(30,48)$, $(48,28)$, $(28,48)$, $(38,51)$, $(51,38)$, $(48,24)$, $(24,48)$, $(48,16)$, $(16,48)$, $(48,10)$, $(10,48)$, $(48,2)$, $(2,48)$, $(48,49)$, $(49,48)$.

Предположим, что мы фиксировали полученную однородную линейную систему уравнений. Напомним, что наша цель — показать, что все значения $z_{i,j}$, $a_{s,t}, b_{s,t}, c_{s,t}$ равны нулю.

Рассмотрим первое соотношение. Она дает $a_{4,1}=0$ (поз. $(42,42)$); $a_{1,1}=0$ (поз. $(48,48)$); $a_{3,1}=0$ (поз. $(38,38)$); $a_{2,1}=0$ (поз. $(39,39)$). Таким образом, T_1,T_2,T_3,T_4 не входят в это соотношение. Далее, $c_{1,1}=0$ $(3,9)$; $b_{2,1}=0$ $(3,51)$; $c_{2,1}=0$ $(46,44)$; $b_{3,1}=0$ $(5,51)$; $c_{3,1}=0$ $(6,51)$; $b_{4,1}=0$ $(7,51)$; $c_{4,1}=0$ $(8,51)$; $b_{5,1}=0$ $(44,48)$; $c_{5,1}=0$ $(10,51)$; $b_{6,1}=0$ $(3,6)$; $c_{6,1}=0$ $(46,42)$; $b_{7,1}=0$ $(13,51)$; $c_{7,1}=0$ $(14,51)$; $b_{8,1}=0$ $(42,48)$; $c_{8,1}=0$ $(16,52)$; $b_{9,1}=0$ $(17,51)$; $c_{9,1}=0$ $(46,38)$; $b_{10,1}=0$ $(19,51)$; $b_{11,1}=0$ $(38,48)$; $c_{11,1}=0$ $(22,51)$; $c_{12,1}=0$ $(24,51)$; $b_{13,1}=0$ $(25,51)$; $c_{13,1}=0$ $(46,34)$; $b_{14,1}=0$ $(27,52)$; $c_{14,1}=0$ $(28,51)$; $b_{15,1}=0$ $(34,48)$; $c_{15,1}=0$ $(30,51)$; $b_{16,1}=0$ $(31,52)$; $c_{16,1}=0$ $(46,28)$; $b_{17,1}=0$ $(33,51)$; $c_{17,1}=0$ $(34,51)$; $b_{18,1}=0$ $(20,44)$; $c_{18,1}=0$ $(36,52)$; $b_{19,1}=0$ $(37,51)$; $c_{19,1}=0$ $(38,51)$; $b_{20,1}=0$ $(39,51)$; $c_{20,1}=0$ $(40,51)$; $b_{21,1}=0$ $(41,52)$; $c_{21,1}=0$ $(42,52)$; $b_{22,1}=0$ $(43,51)$; $c_{22,1}=0$ $(44,51)$; $b_{23,1}=0$ $(3,44)$; $c_{24,1}=0$ $(10,43)$.

Следовательно, правая часть соотношения содержит лишь $X_{\alpha_{12}}$, $X_{\alpha_{24}}$, $X_{-\alpha_{10}}$, $X_{-\alpha_{23}}$, само соотношение упрощается, многие элементы в Z равны нулю. Для начала, это элементы на позициях (i,j), $i=2,3,5,6,7,8,10,11,13,14,\ 16,17,19,22,24,\ 25,27,28,30,31,$ $33,36,37,38,\ 39,40,41,42,\ 43,44,45,48,50,51,52$, $j=1,4,9,12,15,\ 18,20,21,23,\ 26,29,32,$ $35,46,47,49$ (исключая $z_{6,15}=c_{10,1}$, $z_{5,12}=b_{12,1}$, $z_{7,29}=c_{10,1}$, $z_{8,26}=b_{12,1}$, $z_{24,49}=-c_{10,1}$,

$z_{28,35} = c_{23,1}$, $z_{27,32} = b_{24,1}$, $z_{33,26} = -b_{24,1}$, $z_{34,29} = -c_{23,1}$, $z_{37,18} = b_{24,1}$, $z_{38,21} = c_{23,1}$, $z_{38,18} = c_{10,1}$, $z_{39,47} = -c_{10,1}$, $z_{39,20} = b_{24,1}$, $z_{40,23} = c_{23,1}$, $z_{41,12} = -b_{24,1}$, $z_{42,15} = -c_{23,1}$, $z_{43,4} = b_{24,1}$, $z_{44,9} = c_{23,1}$, $z_{45,49} = -b_{24,1}$).

Сделав эти элементы равными нулю, мы видим, что $b_{12,1} = 0$ (поз. $(19, 2)$), $c_{10,1} = 0$ (поз. $(44, 36)$, $b_{24,1} = 0$ (поз. $(45, 2)$), $c_{23,1} = 0$ (поз. $(48, 2)$, т.е. соотношение теперь выглядит как $x_{\alpha_1}(1)Z = Zx_{\alpha_1}(1)$. Тем же способом для других соотношений получаем, что все они выглядят как $x_{\pm\alpha_p}(1)Z = Zx_{\pm\alpha_p}(1)$, $p = 1, \ldots, 4$. Так как централизатор данных восьми матриц состоит из скалярных матриц, а матрица Z имеет нулевой элемент $z_{52,52}$, получаем, что $Z = 0$, что и требовалось.

Теорема 3 доказана для системы корней F_4.

1.7.4 Система корней G_2

Для системы корней G_2

$$\begin{aligned} T_1 &= \operatorname{diag}[1, 1, 0, 0, 1, 1, 2, 2, 3, 3, 3, 3, 0, 0];\\ T_2 &= \operatorname{diag}[0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 0, 0]. \end{aligned}$$

Мы имеем четыре соотношения:

$$\begin{cases} Zx_{\alpha_1}(1) - x_{\alpha_1}(1)(X + a_{1,1}T_1 + a_{2,1}T_2 + \\ \qquad +b_{1,1}X_{\alpha_1} + \cdots + b_{6,1}X_{\alpha_6} + c_{1,1}X_{-\alpha_1} + \cdots + c_{6,1}X_{-\alpha_6}) = 0; \\ Zx_{\alpha_2}(1) - x_{\alpha_2}(1)(X + a_{1,2}T_1 + a_{2,2}T_2 + \\ \qquad +b_{1,2}X_{\alpha_1} + \cdots + b_{6,2}X_{\alpha_6} + c_{1,2}X_{-\alpha_1} + c_{6,2}X_{-\alpha_6}) = 0; \\ Xx_{-\alpha_1}(1) - x_{-\alpha_1}(1)(X + a_{1,3}T_1 + a_{2,3}T_2 + \\ \qquad +b_{1,3}X_{\alpha_1} + \cdots + b_{6,3}X_{\alpha_6} + c_{1,3}X_{-\alpha_1} + \cdots + c_{6,3}X_{-\alpha_6}) = 0; \\ Xx_{-\alpha_2}(1) - x_{-\alpha_2}(1)(X + a_{1,4}T_1 + a_{2,4}T_2 + \\ \qquad +b_{1,4}X_{\alpha_1} + \cdots + b_{6,4}X_{\alpha_6} + c_{1,4}X_{-\alpha_1} + \cdots + c_{6,4}X_{-\alpha_6}) = 0. \end{cases}$$

Матрица $Z = (z_{i,j})$ имеет равными нулю элементы $z_{4,6}$, $z_{4,12}$, $z_{8,8}$, $z_{10,8}$, $z_{10,10}$, $z_{10,12}$, $z_{12,4}$, $z_{12,6}$, $z_{12,8}$, $z_{12,10}$, $z_{12,12}$, $z_{12,14}$, $z_{14,6}$, $z_{14,8}$, $z_{14,12}$.

Из матрицы первого соотношения следует: позиция $(3, 6)$: $z_{3,4} = 0$; позиция $(3, 7)$: $z_{3,9} = 0$; позиция $(3, 11)$: $c_{5,1} = 0$; позиция $(10, 6)$: $z_{10,4} = 0$; позиция $(10, 7)$: $z_{10,9} = 0$; позиция $(10, 12)$: $b_{2,1} = 0$; позиция $(11, 6)$: $z_{11,4} = 0$; позиция $(11, 13)$: $z_{11,1} = 0$; позиция $(2, 6)$: $z_{2,4} = 0$; позиция $(2, 7)$: $z_{2,9} = 0$; позиция $(3, 8)$: $z_{3,6} = 0$; позиция $(3, 13)$: $z_{3,1} = 0$; позиция $(5, 6)$: $z_{5,4} = 0$; позиция $(6, 9)$: $z_{8,9} = 0$; позиция $(11, 8)$: $z_{11,6} = 0$; позиция $(11, 2)$: $z_{11,13} = 0$; позиция $(12, 8)$: $c_{3,1} = 0$; позиция $(12, 6)$: $c_{4,1} = 0$; позиция $(12, 10)$: $c_{2,1} = 0$; позиция $(14, 11)$: $c_{6,1} = 0$; позиция $(14, 12)$: $b_{6,1} = 0$; позиция $(10, 13)$: $z_{10,1} = 0$; позиция $(12, 7)$: $z_{12,9} = 0$; позиция $(11, 8)$: $z_{11,6} = 0$; позиция $(10, 2)$: $z_{10,13} = 0$; позиция $(13, 12)$: $z_{2,12} = 0$; позиция $(13, 11)$: $z_{2,11} = 0$; позиция $(12, 5)$: $z_{12,7} = 0$; позиция $(6, 1)$: $z_{8,1} = 0$; позиция $(14, 7)$: $z_{14,9} = 0$; позиция $(12, 13)$: $z_{12,1} = 0$; позиция $(14, 13)$: $z_{14,1} = 0$; позиция $(14, 5)$: $z_{14,7} = 0$; позиция $(12, 2)$: $z_{12,13} = 0$; позиция $(1, 9)$: $z_{13,9} = 0$; позиция $(4, 9)$: $z_{6,9} = 0$; позиция $(14, 2)$: $z_{14,13} = 0$; позиция $(2, 5)$: $z_{2,7} = 0$; позиция $(1, 12)$: $z_{13,12} = 0$; позиция $(10, 5)$: $z_{10,7} = 0$; позиция $(9, 4)$: $z_{7,4} = 0$.

Из матрицы второго соотношения следует: позиция $(9,6)$: $z_{9,2}=0$; $(13,13)$: $z_{13,3}=0$; $(12,13)$: $z_{12,3}=0$; $(12,14)$: $_{6,2}=0$; $(14,11)$: $z_{4,11}=0$; $(12,9)$: $z_{12,11}=0$; $(13,5)$: $_{3,2}=0$; $(11,10)$: $z_{9,10}=0$; $(8,9)$: $z_{8,11}=0$; $(11,8)$: $z_{9,8}=0$; $(10,9)$: $z_{10,11}=0$; $(6,9)$: $z_{6,11}=0$; $(2,3)$: $z_{6,3}=0$; $(4,1)$: $z_{4,5}=0$; $(10,1)$: $z_{10,5}=0$; $(10,5)$: $z_{12,5}=0$; $(7,12)$: $z_{7,10}=0$; $(5,10)$: $z_{1,10}=0$; $(7,5)$: $b_{1,2}=0$; $(12,10)$: $c_{2,2}=0$; $(5,3)$: $z_{1,3}=0$; $(13,7)$: $c_{4,2}=0$; $(13,8)$: $b_{4,2}=0$; $(10,8)$: $c_{1,2}=0$; $(12,4)$: $c_{5,2}=0$; $(7,2)$: $b_{5,2}=0$; $(1,6)$: $z_{1,2}=0$; $(4,12)$: $z_{4,10}=0$; $(5,11)$: $z_{1,11}=0$; $(13,9)$: $z_{13,11}=0$; $(4,6)$: $z_{4,2}=0$; $(7,9)$: $z_{7,11}=0$; $(10,6)$: $z_{10,2}=0$; $(14,8)$: $z_{4,8}=0$; $(4,13)$: $z_{4,3}=0$; $(7,13)$: $z_{7,3}=0$; $(8,13)$: $z_{8,3}=0$; $(9,13)$: $z_{9,3}=0$; $(10,13)$: $z_{10,3}=0$; $(6,1)$: $z_{6,5}=0$; $(8,1)$: $z_{8,5}=0$; $(9,1)$: $z_{9,5}=0$; $(13,1)$: $z_{13,5}=0$; $(10,2)$: $z_{12,2}=0$; $(6,4)$: $z_{6,14}=0$; $(7,4)$: $z_{7,14}=0$; $(8,4)$: $z_{8,14}=0$; $(10,4)$: $z_{10,14}=0$; $(13,4)$: $z_{13,14}=0$; $(4,5)$: $z_{14,5}=0$; $(8,6)$: $z_{8,2}=0$; $(2,7)$: $z_{6,7}=0$; $(5,7)$: $z_{1,7}=0$; $(14,7)$: $z_{4,7}=0$; $(3,7)$: $z_{13,7}=0$; $(3,8)$: $z_{13,8}=0$; $(8,8)$ и $(10,10)$: $a_{1,2}=0$ и $a_{2,2}=0$; $(1,1)$: $z_{1,5}=0$; $(2,2)$: $z_{6,2}=0$; $(3,3)$: $z_{14,3}=0$; $(4,4)$: $z_{4,14}=0$; $(9,9)$: $z_{9,11}=0$; $(10,12)$: $b_{2,2}=0$; $(3,11)$: $z_{14,11}=0$; $(2,10)$: $z_{6,10}=0$; $(2,14)$: $z_{2,3}=0$; $(2,13)$: $z_{6,13}=0$; $(14,13)$: $z_{4,13}=0$; $(14,1)$: $z_{4,1}=0$; $(14,9)$: $z_{4,9}=0$; $(14,4)$: $z_{14,14}=0$; $(3,9)$: $z_{3,11}=0$; $(3,14)$: $z_{13,13}=0$; $(3,13)$: $z_{3,3}=0$.

Снова вернемся к первому соотношению. Теперь обнуляются элементы $z_{1,9}$, $z_{2,5}$, $z_{6,1}$, $z_{8,7}$, $z_{8,13}$, $z_{5,6}$, $z_{5,11}$.

Если рассмотреть соотношение три, то сразу же из коэффициентов a_i, b_i, c_i остаются ненулевыми только $b_{2,3}, b_{3,3}, b_{4,3}, c_{1,3}, a_{1,3}$. Обнулятся следующие коэффициенты матрицы Z: $z_{5,3}$, $z_{5,10}$, $z_{1,12}$, $z_{7,8}$, $z_{11,2}$, $z_{11,10}$, $z_{11,8}$, $z_{14,2}$.

Теперь во втором соотношении позиция $(14,6)$ дает $b_{3,2}=0$, откуда обнуляются $z_{13,2}$, $z_{6,8}$, $z_{1,14}$, $z_{7,5}$, $z_{1,13}$, $z_{8,10}$, $z_{9,6}$, $z_{9,7}$, $z_{9,12}$.

Опять из третьего соотношения $a_{1,3}=0$, $z_{7,12}=0$.

Наконец, перейдем к последнему, четвертому соотношению. Так как корни α_2 и $-\alpha_2$ сопряжены с помощью элемента w_2, то сразу же ясно, что в четвертом соотношении из всех a_i, b_i, c_i ненулевым остается лишь $b_{5,4}$. Отсюда обнуляются следующие элементы матрицы Z: $z_{1,4}$, $z_{5,7}$, $z_{5,9}$, $z_{5,12}$, $z_{5,1}$, $z_{5,13}$, $z_{5,14}$, $z_{2,1}$, $z_{2,6}$, $z_{2,14}$, $z_{3,2}$, $z_{3,12}$, $z_{3,14}$, $z_{3,5}$, $z_{3,7}$, $z_{3,8}$, $z_{3,13}$, $z_{13,1}$, $z_{13,6}$, $z_{6,4}$, $z_{2,8}$, $z_{2,13}$, $z_{7,1}$, $z_{7,6}$, $z_{7,9}$, $z_{8,4}$, $z_{8,6}$, $z_{8,12}$, $z_{9,4}$, $z_{10,6}$, $z_{11,7}$, $z_{11,9}$, $z_{11,12}$, $z_{11,14}$, $z_{3,10}$, $z_{13,4}$, $z_{14,4}$, $z_{5,8}$.

Из первого соотношения теперь $z_{2,10}=z_{6,12}=z_{1,6}=0$, из второго — $z_{1,8}=z_{5,2}=z_{7,2}=z_{13,10}=z_{14,10}=z_{11,3}=z_{9,13}=z_{9,14}=0$, из третьего — $z_{9,1}=z_{11,5}=z_{7,13}=0$. Из второго соотношения $z_{6,6}=z_{2,2}$, $z_{5,5}=z_{1,1}$, $z_{11,11}=z_{9,9}$. Из первого соотношения $z_{4,4}=z_{1,1}=z_{2,2}=z_{7,7}=z_{9,9}=0$. Таким образом, $Z=0$, что и требовалось.

Теорема 3 доказана для системы корней G_2.

1.7.5 Системы корней B_l

Будем для начала рассматривать пару соотношений с первым и $l+1$-м номером. Понятно, что все остальные соответствующие пары соотношений длинных простых корней устроены совершенно аналогично (так как перестановкой базиса можно перевести любой длинный корень в любой другой длинный).

Можно так переименовать базис, что матрицы $x_{\alpha_1}(1)$ и $x_{-\alpha_1}(1)$ разбиваются на три диагональных блока: первый блок соответствует векторам базиса $\{x_{\alpha_1}, x_{-\alpha_1}, h_1, h_2\}$, второй — векторам $\{x_\alpha \mid \langle\alpha_1,\alpha\rangle = \pm 1\}$, третий — векторам $\{x_\alpha \mid \langle\alpha_1,\alpha\rangle = 0; h_3,\dots,h_l\}$. При этом последний блок просто единичен. Пусть

$$x_{\alpha_1}(1)=\begin{pmatrix}A&0&0\\0&B&0\\0&0&E\end{pmatrix},\quad x_{-\alpha_1}(1)=\begin{pmatrix}A'&0&0\\0&B'&0\\0&0&E\end{pmatrix}$$

и пусть все рассматриваемые нами матрицы Y также разделены на блоки соответствующим образом:

$$Y=\begin{pmatrix}Y_{11}&Y_{12}&Y_{13}\\Y_{21}&Y_{22}&Y_{23}\\Y_{31}&Y_{32}&Y_{33}\end{pmatrix}.$$

Обозначим матрицу $a_{1,1}T_1+a_{2,1}T_2+\dots+a_{l,1}T_l+b_{1,1}X_{\alpha_1}+\dots+b_{m,1}X_{\alpha_m}+c_{1,1}X_{-\alpha_1}+\dots+c_{m,1}X_{-\alpha_m}$ через D. Заметим, что из построения базиса $D_{1,3}=D_{3,1}=0$. Тогда первое соотношение будет выглядеть как

$$\begin{pmatrix}Z_{11}A&Z_{12}B&Z_{13}\\Z_{21}A&Z_{22}B&Z_{23}\\Z_{31}A&Z_{32}B&Z_{33}\end{pmatrix}=\begin{pmatrix}AZ_{11}&AZ_{12}&AZ_{13}\\BZ_{21}&BZ_{22}&BZ_{23}\\Z_{31}&Z_{32}&Z_{33}\end{pmatrix}+\begin{pmatrix}AD_{11}&AD_{12}&0\\BD_{21}&BD_{22}&BD_{23}\\0&D_{32}&D_{33}\end{pmatrix}.$$

Из написанного равенства сразу следует, что $D_{33}=0$. Следовательно, $a_{3,1}=\dots=a_{l,1}=0$, $b_{k,1}=c_{k,1}=0$ при $\langle\alpha_1,\alpha_k\rangle=0$.

Теперь рассмотрим положительный корень α такой, что $\beta=\alpha+\alpha_1\in\Phi$ и α,β являются одними из первых $l+1$ членов последовательности $\gamma_1,\dots,\gamma_k$, а именно, $\gamma_l=e_2+e_l$ (аналогичные пары корней в последовательности $\gamma_1,\dots,\gamma_k$ можно найти и для $\alpha_2,\dots,\alpha_l$ благодаря свойству 3 последовательности $\gamma_1,\dots,\gamma_k$).

Рассмотрим часть базиса $\alpha,-\alpha,\beta,-\beta$. Для матриц $x_{\alpha_1}(1)$ и $x_{-\alpha_1}(1)$ эта часть базиса выделяется прямым слагаемым, поэтому можно рассмотреть ее независимо. По построению мы знаем, что $z_{-\alpha,-\alpha}=z_{-\beta,-\beta}=z_{-\alpha,-\beta}=z_{\beta,-\alpha}=0$. Получим соотношение

$$\begin{pmatrix}z_{\alpha,\alpha}&z_{\alpha,-\alpha}&z_{\alpha,\beta}&z_{\alpha,-\beta}\\z_{-\alpha,\alpha}&0&z_{-\alpha,\beta}&0\\z_{\beta,\alpha}&z_{\beta,-\alpha}&z_{\beta,\beta}&z_{\beta,-\beta}\\z_{-\beta,\alpha}&0&z_{-\beta,\beta}&0\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&-1\\1&0&1&0\\0&0&0&1\end{pmatrix}=$$

$$=\begin{pmatrix}1&0&0&0\\0&1&0&-1\\1&0&1&0\\0&0&0&1\end{pmatrix}\left(\begin{pmatrix}z_{\alpha,\alpha}&z_{\alpha,-\alpha}&z_{\alpha,\beta}&z_{\alpha,-\beta}\\z_{-\alpha,\alpha}&0&z_{-\alpha,\beta}&0\\z_{\beta,\alpha}&z_{\beta,-\alpha}&z_{\beta,\beta}&z_{\beta,-\beta}\\z_{-\beta,\alpha}&0&z_{-\beta,\beta}&0\end{pmatrix}+\begin{pmatrix}a_\alpha&0&-c_{1,1}&0\\0&-a_\alpha&0&-b_{1,1}\\b_{1,1}&0&a_\beta&0&0\\0&c_{1,1}&0&-a_\beta\end{pmatrix}\right).$$

В результате мы получим, что должна быть равна нулю матрица

$$\begin{pmatrix}z_{\alpha,\beta}-a_\alpha&0&c_{1,1}&z_{\alpha,-\alpha}\\z_{-\alpha,\beta}+z_{-\beta,\alpha}&c_{1,1}+a_\alpha&z_{-\beta,\beta}&b_{1,1}-a_\beta\\z_{\beta,\beta}-z_{\alpha,\alpha}-a_\alpha-b_{1,1}&-z_{\alpha,-\alpha}&-z_{\alpha,\beta}+c_{1,1}-a_\beta&-z_{\beta,-\alpha}-z_{\alpha,-\beta}\\z_{-\beta,\beta}&-c_{1,1}&0&a_\beta\end{pmatrix}.$$

Отсюда сразу видно, что $a_\alpha=a_\beta=b_{1,1}=c_{1,1}=0$. Так как мы уже знаем, что $a_{3,1}=\dots=a_{l,1}=0$, то $a_{1,1}=a_{2,1}=0$.

Теперь рассмотрим такой корень $\alpha \in \Phi^+$, что $\alpha + \alpha_1 \in \Phi^+$. В последовательности $\gamma_1, \dots, \gamma_k$ найдем такие корни γ_p и γ_q, что $\gamma_q - \gamma_p = \alpha$. Рассматриваемые корни α могут иметь три вида: $\alpha = e_2 - e_i$, $3 \leqslant i \leqslant l$; $\alpha = e_2 + e_i$, $3 \leqslant i \leqslant l$; $\alpha = e_2$. Для всех трех случаев возможны только две ситуации:

1) корень γ_p ортогонален к корню α_1, а корень γ_q — не ортогонален. Тогда $\gamma' = \gamma_q + \alpha_1$ — тоже корень, мы можем рассмотреть часть базиса $\gamma_p, -\gamma_p, \gamma_q, -\gamma_q, \gamma', -\gamma'$, которая выделяется инвариантным прямым слагаемым для $x_{\alpha_1}(1)$. На этой части базиса

$$x_{\alpha_1}(1) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

у матрицы Z равны нулю (по лемме 1.16) $z_{-\gamma_p, -\gamma_q}$ и $z_{-\gamma_q, -\gamma_p}$, матрица D равна

$$\begin{pmatrix} 0 & 0 & -c_{\alpha,1} & 0 & -c_{\alpha+\alpha_1,1} & 0 \\ 0 & 0 & 0 & -b_{\alpha,1} & 0 & -b_{\alpha+\alpha_1} \\ b_{\alpha,1} & 0 & 0 & 0 & 0 & 0 \\ 0 & c_{\alpha,1} & 0 & 0 & 0 & 0 \\ b_{\alpha+\alpha_1,1} & 0 & 0 & 0 & 0 & 0 \\ 0 & c_{\alpha+\alpha_1,1} & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Теперь из основного соотношения будет следовать равенство нулю матрицы

$$\begin{pmatrix} 0 & 0 & z_{\gamma_p,\gamma'} + c_{\alpha,1} & 0 & c_{\alpha+\alpha_1,1} & -z_{\gamma_p,-\gamma_q} \\ 0 & 0 & z_{-\gamma_p,\gamma'} & b_{\alpha,1} & 0 & b_{\alpha+\alpha_1,1} \\ -b_{\alpha,1} & 0 & z_{\gamma_q,\gamma'} & 0 & 0 & -z_{\gamma_q,-\gamma_q} \\ z_{-\gamma',\gamma_p} & z_{-\gamma',-\gamma_p} - c_{\alpha,1} + c_{\alpha+\alpha_1,1} & z_{-\gamma_q,\gamma'} + z_{-\gamma',\gamma_q} & z_{-\gamma',-\gamma_q} & z_{-\gamma',\gamma'} & z_{-\gamma',-\gamma'} - z_{-\gamma_q,-\gamma_q} \\ -z_{\gamma_q,\gamma_p} - b_{\alpha,1} - b_{\alpha+\alpha_1,1} & -z_{\gamma_q,-\gamma_p} & z_{\gamma',\gamma'} - z_{\gamma_q,\gamma_q} & -z_{\gamma_q,-\gamma_q} & -z_{\gamma_q,\gamma'} & -z_{\gamma',-\gamma_q} - z_{\gamma_q,-\gamma'} \\ 0 & -c_{\alpha+\alpha_1} & z_{-\gamma',\gamma'} & 0 & 0 & z_{-\gamma',-\gamma_q} \end{pmatrix}.$$

Легко видеть, что тогда $b_{\alpha,1} = b_{\alpha+\alpha_1,1} = c_{\alpha+\alpha_1,1} = 0$.

2) Во втором случае может быть $\gamma'' = \gamma_p - \alpha_1 \in \Phi^+$, $\langle \gamma_q, \alpha_1 \rangle = 0$. Этот случай очень похож на предыдущий, в результате на части базиса $\gamma_p, -\gamma_p, \gamma_q, -\gamma_q, \gamma'', -\gamma''$ получается равной нулю матрица

$$\begin{pmatrix} -z_{\gamma'',\gamma_p} & -z_{\gamma_p,-\gamma''} - z_{\gamma'',-\gamma_p} & -z_{\gamma'',\gamma_q} + c_{\alpha,1} + c_{\alpha+\alpha_1,1} & -z_{\gamma'',-\gamma_q} & z_{\gamma_p,\gamma_p} - z_{\gamma'',\gamma''} & -z_{\gamma'',-\gamma''} \\ 0 & -z_{-\gamma_p,-\gamma''} & 0 & b_{\alpha,1} & z_{-\gamma_p,\gamma_p} & 0 \\ -b_{\alpha,1} & -z_{\gamma_q,-\gamma''} & 0 & 0 & z_{\gamma_q,\gamma_p} - b_{\alpha+\alpha_1,1} & 0 \\ 0 & -z_{-\gamma+q,-\gamma''} - c_{\alpha,1} & 0 & 0 & z_{-\gamma_q,\gamma_p} & -c_{\alpha+\alpha_1,1} \\ 0 & -z_{\gamma'',-\gamma''} & c_{\alpha+\alpha_1,1} & 0 & z_{\gamma'',\gamma_p} & 0 \\ z_{-\gamma_p,\gamma_p} & -z_{-\gamma'',-\gamma''} + z_{-\gamma_p.-\gamma_p} & z_{-\gamma_p,\gamma_q} & b_{\alpha+\alpha_1,1} - b_{\alpha,1} & z_{-\gamma'',\gamma_p} + z_{-\gamma_p,\gamma''} & z_{-\gamma_p,-\gamma''} \end{pmatrix}.$$

Снова сразу получаем $b_{\alpha,1} = b_{\alpha+\alpha_1,1} = c_{\alpha+\alpha_1,1} = 0$.

При рассмотрении пары корней γ_s, γ_t, для которой $\gamma_t - \gamma_s = \alpha + \alpha_1$ мы аналогично получим два случая и $c_{\alpha,1} = 0$.

Таким образом, мы доказали, что $a_{i,1} = 0$ для любого $i = 1, \dots, l$, $b_{\alpha,1} = c_{\alpha,1} = 0$ для любого $\alpha \in \Phi$. Значит, матрица Z должна коммутировать с $x_{\alpha_1}(1)$.

Точно так же из следующих $l-2$ соотношений получим, что матрица Z коммутирует со всеми $x_{\pm\alpha_i}(1)$, $i=1,\dots,l-1$.

Понятно, что это означает, что матрица Z коммутирует со всеми $X_{\pm\alpha_i}$, $i=1,\dots,l-1$.

Осталось последние два соотношения — для $x_{\pm e_l}(1)$.

Аналогично длинным корням, матрицы $x_{\pm e_l}(1)$ разбиваются на диагональные блоки. Как мы уже знаем из предыдущих параграфов, эти блоки соответствуют частям базиса $\{v_{\pm e_i\pm e_j} \mid 1\leqslant i<j<l\}\cup\{V_{h_1},\dots,V_{h_{l-2}}\}$ (на которой обе матрицы единичны), $\{v_{\pm e_i\pm e_l}, v_{\pm e_i}\}$, $1\leqslant i<l$, $\{v_{e_l}, v_{-e_l}, V_{h_{l-1}}, V_{h_l}\}$.

Аналогично ситуации с длинными корнями получим, что $D_{3,3}=0$, т. е. $a_{1,l}=\dots=a_{l-2,l}=0$, $b_{k,l}=c_{k,l}=0$ при $\alpha_k=\pm e_i\pm e_j$, $1\leqslant i<j<l$.

Теперь рассмотрим корни $\gamma_{l+1}=e_2$ и $\gamma_l=\gamma_{l+1}+\alpha_l=e_2+e_l$. Рассмотрим часть базиса $e_2-e_l, e_l-e_2, e_2+e_l, -e_2-e_l, e_2, -e_2$. Для матриц $x_{\alpha_l}(1)$ и $x_{-\alpha_l}(1)$ эта часть базиса выделяется прямым слагаемым, поэтому можно рассмотреть ее независимо. По построению мы знаем, что $z_{-e_2,-e_2}=z_{-e_2-e_l,-e_2-e_l}=z_{-e_2,-e_2-e_l}=z_{-e_2-e_l,-e_2}=0$.

Кроме того, если Z коммутирует со всеми $X_{\pm\alpha_1},\dots,X_{\pm\alpha_{l-1}}$, то Z коммутирует с $X_{e_2-e_l}$, $X_{e_l-e_2}$. Рассмотрев часть базиса $\{v_{e_2-e_l}, v_{e_l-e_2}, v_{e_2+e_l}, v_{-e_2-e_l}, V_{h_1},\dots,V_{h_l}\}$, мы увидим сразу, что $z_{\alpha,\beta}=0$ для всех пар $\langle\alpha,\beta\rangle$, где $\alpha=\pm(e_2-e_l)$, $\beta=\pm(e_2+e_l)$, либо $\alpha=\pm(e_2+e_l)$, $\beta=\pm(e_2-e_l)$.

Теперь получим соотношение

$$
\begin{pmatrix}
z_{e_2-e_l,e_2-e_l} & z_{e_2-e_l,e_l-e_2} & 0 & 0 & z_{e_2-e_l,e_2} & z_{e_2-e_l,-e_2}\\
z_{e_l-e_2,e_2-e_l} & z_{e_l-e_2,e_l-e_2} & 0 & 0 & z_{e_l-e_2,e_2} & z_{e_l-e_2,-e_2}\\
0 & 0 & z_{e_2+e_l,e_2+e_l} & z_{e_2+e_l,-e_2-e_l} & z_{e_2+e_l,e_2} & z_{e_2+e_l,-e_2}\\
0 & 0 & z_{-e_2-e_l,e_2+e_l} & 0 & z_{-e_2-e_l,e_2} & 0\\
z_{e_2,e_2-e_l} & z_{e_2,e_l-e_2} & z_{e_2,e_2+e_l} & z_{e_2,-e_2-e_l} & z_{e_2,e_2} & z_{e_2,-e_2}\\
z_{-e_2,e_2-e_l} & z_{-e_2,e_l-e_2} & z_{-e_2,e_2+e_l} & 0 & z_{-e_2,e_2} & 0
\end{pmatrix}
\begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 1\\
0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 1 & 0 & -1\\
0 & 0 & 0 & 1 & 0 & 0\\
0 & -2 & 0 & 0 & 1 & 0\\
0 & 0 & 0 & 2 & 0 & 1
\end{pmatrix}=
$$

$$
=\begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 1\\
0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 1 & 0 & -1\\
0 & 0 & 0 & 1 & 0 & 0\\
0 & -2 & 0 & 0 & 1 & 0\\
0 & 0 & 0 & 2 & 0 & 1
\end{pmatrix}
\left(
\begin{pmatrix}
z_{e_2-e_l,e_2-e_l} & z_{e_2-e_l,e_l-e_2} & 0 & 0 & z_{e_2-e_l,e_2} & z_{e_2-e_l,-e_2}\\
z_{e_l-e_2,e_2-e_l} & z_{e_l-e_2,e_l-e_2} & 0 & 0 & z_{e_l-e_2,e_2} & z_{e_l-e_2,-e_2}\\
0 & 0 & z_{e_2+e_l,e_2+e_l} & z_{e_2+e_l,-e_2-e_l} & z_{e_2+e_l,e_2} & z_{e_2+e_l,-e_2}\\
0 & 0 & z_{-e_2-e_l,e_2+e_l} & 0 & z_{-e_2-e_l,e_2} & 0\\
z_{e_2,e_2-e_l} & z_{e_2,e_l-e_2} & z_{e_2,e_2+e_l} & z_{e_2,-e_2-e_l} & z_{e_2,e_2} & z_{e_2,-e_2}\\
z_{-e_2,e_2-e_l} & z_{-e_2,e_l-e_2} & z_{-e_2,e_2+e_l} & 0 & z_{-e_2,e_2} & 0
\end{pmatrix}+\right.
$$

$$
\left.+\begin{pmatrix}
a_{l-1,l} & 0 & 0 & 0 & 0 & b_{l,l} & \\
0 & -a_{l-1,l} & 0 & 0 & 0 & c_{l,l} & 0\\
0 & 0 & 2a_{l,l}+a_{l-1,l} & 0 & -b_{l,l} & 0 & 0\\
0 & 0 & 0 & -2a_{l,l}-a_{l-1,l} & 0 & 0 & -c_{l,l}\\
0 & -2b_{l,l} & 2c_{l,l} & 0 & a_{l,l}+a_{l-1,l} & 0 & \\
-2c_{l,l} & 0 & 0 & 2b_{l,l} & 0 & -a_{l,l}-a_{l-1,l} &
\end{pmatrix}\right).
$$

Из него сразу же получается, что $a_{l-1,l}=a_{l,l}=b_{l,l}=c_{l,l}=0$.

Для корней e_i-e_l, e_i+e_l, e_i, $1\leqslant i<l$, поступим точно так же, как и выше, когда рассматривали самое первое соотношение, получим равенство нулю всех коэффициентов $b_{\alpha,l}$ и $c_{\alpha,l}$.

Аналогично рассматривается соотношение с $x_{-\alpha_l}(1)$.

Таким образом, матрица Z коммутирует со всеми $x_\alpha(1)$, $\alpha\in\Phi$, и поэтому является скалярной. Так как у рассматриваемой матрицы есть нули на диагонали (по построению), то она нулевая. Теорема доказана.

1.8 Доказательство основной теоремы (теоремы 1)

Лемма 1.17. *Если* $\overline{t}\in G_{\mathrm{ad}}(\Phi,R)$ — *элемент тора* (Φ — *одна из рассматриваемых систем корней,* R — *локальное коммутативное кольцо*), *то существует такой элемент тора*

$t \in G_\pi(\Phi, S)$, что кольцо S содержит R, t лежит в нормализаторе подгруппы $G_\pi(\Phi, R)$, при факторизации группы $G_\pi(\Phi, S)$ по центру t дает $\bar{t}$.

Доказательство. Понятно, что достаточно доказать утверждение леммы для базисных элементов тора $T_{\mathrm{ad}}(\Phi, R)$. Так как все корни в рассматриваемых системах сопряжены, то мы можем рассмотреть только один элемент тора — $\bar{t} = \chi_{\alpha_1}(r)$. Этот элемент действует на элементарную подгруппу следующим образом: $\bar{t}x_\alpha(s)\bar{t}^{-1} = x_\alpha(r^k s)$, где $\alpha = k\alpha_1 + \beta$, α_1 не входит в разложение β в сумму простых корней.

Понятно, что нам достаточно построить такое расширение S кольца R и элемент тора группы $G_\pi(\Phi, S)$ — t, что $tx_\alpha(s)t^{-1} = \bar{t}x_\alpha(s)\bar{t}^{-1}$ для всех $\alpha \in \Phi$, $s \in R$.

Ясно, что если построенный элемент тора будет правильно действовать на простых корнях, то он автоматически будет правильно действовать на всех корнях.

Для иллюстрации того, как построить такое расширение, разберем случай системы корней A_l.

Рассмотрим кольцо S, получающееся из кольца R добавлением корня $l+1$-й степени из элемента r (а именно, $S = R[x]/(x^{l+1} - r)$). Обозначим этот корень через s. Тогда нужным нам элементом будет
$$t = h_{\alpha_1}(s^l)h_{\alpha_2}(s^{l-1}) \dots h_{\alpha_{l-1}}(s^2)h_{\alpha_l}(s).$$

Именно,

$$\begin{aligned} tx_{\alpha_1}(u)t^{-1} = h_{\alpha_1}(s^l)h_{\alpha_2}(s^{l-1})x_{\alpha_1}(u)h_{\alpha_2}(s^{l-1})^{-1}h_{\alpha_1}(s^l)^{-1} = \\ = h_{\alpha_1}(s^l)x_{\alpha_1}(u/s^{l-1})h_{\alpha_1}(s^l)^{-1} = x_{\alpha_1}(u \cdot s^{2l}/s^{l-1}) = \\ = x_{\alpha_1}(us^{l+1}) = x_{\alpha_1}(ur), \end{aligned}$$

для любого простого корня α_i, $1 < i < l$,

$$\begin{aligned} tx_{\alpha_i}(u)t^{-1} = h_{\alpha_{i-1}}(s^{l-i+1})h_{\alpha_i}(s^{l-i})h_{\alpha_{i+1}}(s^{l-i-1})x_{\alpha_i}(u)h_{\alpha_{i+1}}(s^{l-i-1})^{-1}h_{\alpha_i}(s^{l-i})^{-1}h_{\alpha_{i-1}}(s^{l-i+1})^{-1} = \\ = x_{\alpha_i}(u \cdot s^{2l-2i}/(s^{l-i-1}s^{l-i+1})) = x_{\alpha_1}(u), \end{aligned}$$

наконец, для корня α_l

$$tx_{\alpha_l}(u)t^{-1} = h_{\alpha_{l-1}}(s^2)h_{\alpha_l}(s)x_{\alpha_i}(u)h_{\alpha_l}(s^2)^{-1}h_{\alpha_{l-1}}(s)^{-1} = x_{\alpha_i}(u \cdot s^2/s^2) = x_{\alpha_1}(u).$$

Таким образом ищутся нужные нам расширения кольца R и строятся элементы t. □

Докажем теперь основную теорему (теорема 1.1).

Доказательство. Случай, когда рассматриваемая группа Шевалле — элементарная и присоединенная, очевидно следует из теорем 1.2 и 1.3.

Пусть теперь у нас имеется любая другая элементарная группа Шевалле $E_\pi(\Phi, R)$ и ее автоморфизм φ. Ее фактор по центру изоморфен присоединенной элементарной группе $E_{\mathrm{ad}}(\Phi, R)$, соответственно строится автоморфизм $\overline{\varphi}$ группы $E_{\mathrm{ad}}(\Phi, R)$. Такой автоморфизм раскладывается в композицию

$$\overline{\varphi} = \overline{\rho} \circ \varphi_{\overline{g}},$$

где $\overline{\rho}$ — кольцевой автоморфизм, $\varphi_{\overline{g}}$ — сопряжение элементом $\overline{g} \in G_{\mathrm{ad}}(\Phi, R)$. Заметим, что автоморфизм $\overline{\rho}$ легко поднимается до кольцевого автоморфизма ρ группы $E_\pi(\Phi, R)$ такого, что ρ на смежных классах группы $E_\pi(\Phi, R)$ по ее центру действуют так же, как $\overline{\rho}$.

Теперь рассмотрим автоморфизм $\varphi_{\overline{g}}$. Заметим, что $\overline{g} = \overline{t}\overline{e}$, где $\overline{t} \in T_{\mathrm{ad}}(\Phi, R)$, $\overline{e} \in E_{\mathrm{ad}}(\Phi, R)$. Для элемента $\overline{e}$ мы можем найти такой $e \in E_\pi(\Phi, R)$, что образ e при факторизации по центру равен $\overline{e}$. У элемента $\overline{t}$ есть его прообраз $t \in T_\pi(\Phi, S)$, где S — кольцо, получающееся из кольца R добавлением некоторых скаляров (см. лемму 1.17). При этом t нормализует группу $E_\pi(\Phi, R)$. Рассмотрим теперь $g = te \in G_\pi(\Phi, S)$. Очевидно, что при факторизации группы $E_\pi(\Phi, R)$ по центру автоморфизм φ_g даст нам автоморфизм $\varphi_{\overline{g}}$.

Теперь рассмотрим автоморфизм

$$\psi = \varphi_{g^{-1}} \circ \rho^{-1} \circ \varphi.$$

Это автоморфизм группы $E_\pi(\Phi, R)$, при факторизации по центру дающий тождественный автоморфизм фактора. Значит, ψ — центральный автоморфизм.

Однако, так как элементарная группа Шевалле в рассматриваемом случае является собственным коммутантом, центральный автоморфизм тождественен.

Таким образом, мы уже доказали теорему для всех элементарных групп Шевалле рассматриваемого типа, а именно, доказали, что любой автоморфизм группы $E_\pi(\Phi, R)$ является композицией кольцевого и внутреннего (однако уже не строго внутреннего).

Теперь пусть нам даны группа Шевалле $G_\pi(\Phi, R)$ и ее автоморфизм φ. Так как элементарная подгруппа $E_\pi(\Phi, R)$ является характеристической (коммутантом) группы $G_\pi(\Phi, R)$, то φ одновременно является автоморфизмом элементарной подгруппы. На элементарной подгруппе он раскладывается в композицию $\rho \circ \varphi_g$, $g \in G_\pi(\Phi, S)$, при этом $g = te$, где $e \in E_\pi(\Phi, R)$, $t \in T_\pi(\Phi, S)$. Первый автоморфизм очевидным образом продолжается до автоморфизма всей группы $G_\pi(\Phi, R)$, а второй является автоморфизмом этой группы, так как элементы тора коммутируют. Тогда композиция $\psi = \varphi_{g^{-1}} \circ \rho^{-1} \circ \varphi$ является автоморфизмом группы $G_\pi(\Phi, R)$, тождественно действующим на элементарной подгруппе. Так как $G_\pi(\Phi, R) = T_\pi(\Phi, R) \cdot E_\pi(\Phi, R)$, то достаточно понять, как ψ действует на элементах тора. Элемент $t^{-1}\varphi(t) \in G_\pi(\Phi, R)$ лежит в центре группы $E_\pi(\Phi,)$, и, следовательно, в центре группы $G_\pi(\Phi, R)$. Значит, автоморфизм ψ является центральным.

Таким образом, теорема 1.1 доказана для всех рассматриваемых групп Шевалле. □

1.9 Автоморфизмы элементарных присоединенных групп Шевалле типов A_l, D_l, E_l над локальными кольцами с необратимой двойкой

Заметим, что в доказательстве теоремы 1.3 нигде не использовалось наличие обратимой двойке в кольце R для случая систем корней A_l, D_l, E_l. В доказательстве основной теоремы нам тоже требовалось лишь то, что выполняются теоремы 1.2, 1.3, а также элементарная группа Шевалле является коммутантом в самой группе Шевалле.

Значит, для того, чтобы доказать основную теорему для локальных колец с необратимой двойкой, для случая систем корней A_l, D_l, E_l, нам потребуется только доказать для них теорему 1.2.

Шаги доказательства будут похожими, но на каждом этапе придется рассматривать другие элементы (имеющие порядок три, а не два или четыре), а также другие соотношения.

1.9.1 Замена изначального автоморфизма на специальный изоморфизм

Начиная с этого параграфа, кольцо R будет предполагаться локальным кольцом с необратимой двойкой, группа Шевалле присоединенной, система корней — одна из рассматриваемых.

Как и выше, мы рассмотрим отображение $\varphi' = i_{g^{-1}}\varphi$, которое является изоморфизмом группы $E_{\mathrm{ad}}(\Phi, R) \subset \mathrm{GL}_n(R)$ на некоторую подгруппу $\mathrm{GL}_n(R)$, с тем свойством, что ее образ при факторизации R по J совпадает с автоморфизмом $\overline{\rho}$.

По-прежнему, очевидно

Предложение 1.5. *Любая матрица $A \in E_{\mathrm{ad}}(\Phi, R)$ с элементами из подкольца R' в R, порожденного единицей, отображается при изоморфизме φ' в матрицу из множества*

$$A \cdot \mathrm{GL}_n(R, J) = \{B \in \mathrm{GL}_n(R) \mid A - B \in M_n(J)\}.$$

Пусть $a \in E_{\mathrm{ad}}(\Phi, R)$, $a^3 = 1$. Тогда элемент $e = \frac{1}{3}(1 + a + a^2)$ является идемпотентом в кольце $M_n(R)$. Этот идемпотент e определяет разложение свободного R-модуля $V \cong R^n$:

$$V = eV \oplus (1 - e)V = V_0 \oplus V_1$$

(модули V_0, V_1 свободны, так как любой проективный модуль над локальным кольцом свободен [128]). Пусть $\overline{V} = \overline{V}_0 \oplus \overline{V}_1$ — разложение k-модуля (линейного пространства) $\overline{V} \cong k^n$ по отношению к $\overline{a}$, и $\overline{e} = \frac{1}{3}(1 + \overline{a} + \overline{a}^2)$.

Тогда имеем

Предложение 1.6. *Модули (подпространства) $\overline{V}_0$, $\overline{V}_1$ являются образами модулей V_0, V_1 при факторизации по J.*

Замечание.

Теперь предположим, что $a^3 = 1$. Посмотрим, как должна быть устроена эта матрица на подмодулях V_0 и V_1.

Пусть $x \in V_1$. Тогда $x = ex = \frac{1}{3}(a^2 + a + 1)(x)$, откуда $(a^2 + a - 2)(x) = 0$. Тем более имеем $(a - 1)(a^2 + a - 2)(x) = 0$, кроме того, так как $a^3 = 1$, то $(a - 1)(a^2 + a + 1)(x) = 0$. Взяв разность последних двух равенств, мы получим $3(a - 1)(x) = 0$ и, так как тройка обратима в кольце, то $a(x) = x$. Значит, на подмодуле V_1 отображение a тождественно.

Теперь пусть $x \in V_0$. Пусть $a(x) = \lambda x$. Тогда, очевидно, $\lambda^2 + \lambda + 1 = 0$. Так как $\lambda \neq 1$, то λ должно быть неединичным корнем из единицы третьей степени (их всего два, так как тройка обратима). Если $y = a(x) \neq \lambda x$, то векторы x и y линейно независимы, при этом $a(y) = a^2(x) = -x - a(x) = -x - y$. Таким образом, на подмодуле $\langle x, y\rangle$ матрица a действует инвариантно и имеет вид

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}. \tag{1.5}$$

Таким образом, модуль V_0 распадается прямую сумму инвариантных подмодулей размерностей один или два, при этом на одномерных подмодулях действие a на векторы x есть умножение на ξ или ξ^2 ($\xi^3 = 1$).

Понятно, что если изначальная матрица a имеет "целые" коэффициенты, то ее матричные инварианты (след, определитель, и т. д.) также являются целыми числами, откуда следует, что они должны быть целыми в любом базисе. Пусть одномерных подмодулей для ξ было p штук, а для ξ^2 — q штук. Пусть для определенности $p \geqslant q$. Тогда определитель на части базиса, порожденной этими одномерными подмодулями, равен ξ^{p-q}. Для того, чтобы это число было целым, необходимо, чтобы $p - q$ было кратно трем. След матрицы на данной части базиса есть $-q + (p - q)\xi$, т. е. $p - q$ должно быть равно нулю в кольце R. Из того, что остальные матричные инварианты также должны быть целыми числами, и, кроме того, из того, что все нечетные числа в кольце R обратимы, следует, что $p - q = 0$. Таким образом, если матрица a имела целые коэффициенты, то в некотором базисе она будет состоять из единичного блока размерности $\dim V_1$ и из блоков размера 2×2 вида (1.5) суммарного размера $\dim V_0$.

Пусть теперь для матрицы a с целыми коэффициентами $b = \varphi'(a)$. Тогда $b^3 = 1$ и b сравнимо с a по модулю J.

Предложение 1.7. *Предположим, что $a, b \in E_\pi(\Phi, R)$, $a^3 = b^3 = 1$, a — матрица с элементами из подкольца $R' \subset R$, порожденного единицей, b и a сравнимы по модулю J, $V = V_0 \oplus V_1$ — разложение V по отношению к a, $V = V_0' \oplus V_1'$ — разложение V по отношению к b. Тогда $\dim V_0' = \dim V_0$, $\dim V_1' = \dim V_1$.*

Доказательство. Мы имеем R-базис модуля V $\{e_1, \dots, e_n\}$ такой, что $\{e_1, \dots, e_k\} \subset V_0$, $\{e_{k+1}, \dots, e_n\} \subset V_1$. Ясно, что

$$\overline{a}\overline{e}_i = \overline{ae_i} = \overline{(\sum_{j=1}^n a_{ij} e_j)} = \sum_{j=1}^n \overline{a}_{ij} \overline{e}_j.$$

Пусть $\overline{V} = \overline{V}_0 \oplus \overline{V}_1$, $\overline{V} = \overline{V}'_0 \oplus \overline{V}'_1$ — разложения k-модуля (пространства) $\overline{V}$ по отношению к $\overline{a}$ и $\overline{b}$. Ясно, что $\overline{V}_0 = \overline{V}'_0$, $\overline{V}_1 = \overline{V}'_1$. Таким образом, по предложению 1.2 образы модулей V_0 и V_0', V_1 и V_1' при факторизации J совпадают. Возьмем такие $\{f_1, \dots, f_k\} \subset V_0'$, $\{f_{k+1}, \dots, f_n\} \subset V_1'$, что $\overline{f}_i = \overline{e}_i$, $i = 1, \dots, n$. Так как матрица перехода от $\{e_1, \dots, e_n\}$ к $\{f_1, \dots, f_n\}$ обратима (сравнима с единичной матрицей по модулю J), то $\{f_1, \dots, f_n\}$ — это R-базис в V. Ясно, что $\{f_1, \dots, f_k\}$ является R-базисом в V_0', $\{v_{k+1}, \dots, v_n\}$ — R-базисом в V_1'. $\square$

Из этого предложения, замечания выше и сравнимости матриц a и b очевидно следует, что для b существует некоторый базис модуля V, в котором b имеет тот же вид, что и a в изначальном базисе. Таким образом, a и b сопряжены.

1.9.2 Образы элементов $w_{\alpha_i} x_{\alpha_i}(1)$ и некоторых элементов группы Вейля

Рассмотрим некоторую фиксированную элементарную присоединенную группу Шевалле $E = E_{\mathrm{ad}}(\Phi, R)$ с системой корней A_l $(l \geqslant 3)$, D_l $(l \geqslant 4)$, E_6, E_7 или E_8, ее присоединенное представление в группе $\mathrm{GL}_n(R)$ $(n = l + 2m$, где m — число положительных корней системы $\Phi)$, с базисом из весовых векторов $v_1 = x_{\alpha_1}, v_{-1} = x_{-\alpha_1}, \dots, v_n = x_{\alpha_n}, v_{-n} = x_{-\alpha_n}, V_1 = h_1, \dots, V_l = h_l$, соответствующим базису Шевалле системы Φ.

У нас также есть изоморфизм φ', описанный в предыдущем пункте.

Для начала рассмотрим матрицу $Q_1 = w_{\alpha_1} x_{\alpha_1}(1)$ в нашем базисе. Заметим, что $Q_1^3 = E$.

На части базиса, образованной $\{v_1, v_{-1}, V_1, V_2\}$, эта матрица инвариантна и имеет вид

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ -1 & 1 & 2 & -1 \\ 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

на части базиса, образованной всеми v_j, v_{-j}, где $\langle \alpha_1, \alpha_j \rangle = 0$, а также всеми соответствующими V_i, $i > 2$, она тождественна; на части базиса $\{v_j, v_{-j}, v_k, v_{-k}\}$, где $\langle \alpha_1, \alpha_j \rangle = -1$, $\alpha_k = \alpha_1 + \alpha_j$, она имеет вид

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

Заметим, что данная матрица имеет только целые коэффициенты, поэтому ее образ при изоморфизме сопряжен ей.

Теперь присоединим (временно и если его нет) к кольцу R элемент ξ такой, что $\xi^3 = 1$. То есть введем такой внешний элемент и рассмотрим кольцо $\overline{R}$, порожденное кольцом R и элементом ξ.

Тогда в некотором базисе матрица Q_1 имеет диагональный вид с $1, \xi, \xi^2$ на диагонали. Именно, часть базиса третьего первого типа перейдет в $\mathrm{diag}\,[\xi, \xi^2, 1, 1]$, часть базиса второго типа — в $\mathrm{diag}\,[1, 1]$, часть базиса третьего типа — в $\mathrm{diag}\,[\xi, \xi, \xi^2, \xi^2]$. Понятно, что аналогичными свойствами будут обладать и другие элементы $Q_i = w_{\alpha_i} x_{\alpha_i}(1)$.

Для различных систем корней из рассматриваемого списка возьмем теперь следующие множества корней:

— для системы корней A_l рассмотрим множество $\alpha_1 = e_1 - e_2$, $\alpha_3 = e_3 - e_4$, $\dots$, $\alpha_{l-1} = e_{l-1} - e_l$ или $\alpha_l = e_l - e_{l+1}$ в зависимости от четности l, т. е. просто возьмем простые корни через один;

— для системы корней D_l рассмотрим множество $\alpha_1 = e_1 - e_2$, $\alpha_3 = e_3 - e_4$, $\dots$, $\alpha_{l-1} = e_{l-1} - e_l$, $e_1 + e_2$, $e_3 + e_4$, $\dots$, $e_{l-1} + e_l$;

— для системы E_8 (E_6, E_7 аналогичны) рассмотрим множество $\alpha_1 = e_1 - e_2$, $\alpha_4 = e_3 - e_4$, $\alpha_6 = e_5 - e_6$, $\alpha_8 = e_7 - e_8$, $\frac{1}{2}(e_1 + e_2 - e_3 - e_4 - e_5 - e_6 - e_7 - e_8)$, $\frac{1}{2}(e_1 + e_2 + e_3 + e_4 - e_5 - e_6 - e_7 - e_8)$, $\frac{1}{2}(e_1 + e_2 + e_3 + e_4 + e_5 + e_6 - e_7 - e_8)$, $\frac{1}{2}(e_1 + e_2 + e_3 + e_4 + e_5 + e_6 + e_7 + e_8)$.

Обозначим полученное множество (последовательность) корней через $\gamma_1, \dots, \gamma_k$.

Заметим, что все корни $\gamma_1, \dots, \gamma_k$ попарно ортогональны. Это означает, что все матрицы $Q_{\gamma_1}, \dots, Q_{\gamma_k}$ попарно коммутируют, и, конечно же, коммутируют их образы $P_{\gamma_i} = \varphi'(Q_{\gamma_i})$. Значит, их можно в одном базисе записать в диагональном виде с теми же (и тем же количеством и расположением) $1, \xi, \xi^2$ на диагонали. Временно перейдем к этому базису.

Опишем матрицу перехода к рассматриваемому базису.

На части базиса $\{\gamma_i, -\gamma_i, h_{\gamma_i}, h_\alpha\}$, где $\langle \alpha, \gamma_i \rangle = -1$, матрица перехода имеет вид

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

Если взять такой корень α, что $\langle \alpha, \gamma_i \rangle = \langle \alpha, \gamma_j \rangle = -1$, то на части базиса, образованной корнями

$$\{\alpha, -\alpha, \alpha + \gamma_i, -\alpha - \gamma_i, \alpha + \gamma_j, -\alpha - \gamma_j, \alpha + \gamma_i + \gamma_j, -\alpha - \gamma_i - \gamma_j\},$$

матрица перехода имеет вид

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

Заметим при этом, что для любой пары корней γ_i, γ_j, $1 \leqslant i, j \leqslant k$, существует корень $\gamma_{i,j}$ такой, что $\langle \gamma_i, \gamma_{i,j} \rangle = \langle \gamma_j, \gamma_{i,j} \rangle = -1$ (для пары корней $e_p - e_{p+1}$ и $e_q \pm e_{q+1}$ это корень $e_{p+1} - e_q$; для пары корней $e_p + e_{p+1}$ и $e_q \pm e_{q+1}$ это корень $-e_{p+1} - e_q$; для пары корней $e_p - e_{p+1}$ и $e_p + e_{p+1}$ это корень $-e_p + e_q$, $q \neq p, p+1$; для пары корней $e_p - e_{p+1}$ и $\frac{1}{2}(e_1 + e_2 \pm \dots \pm (e_p + e_{e_{p+1}}) \pm \dots)$ — это корень $e_1 \mp e_p$ или $e_1 \mp e_{p+1}$; наконец, для пары $\frac{1}{2}(e_1 + e_2 - e_3 - e_4 - e_5 - e_6 - e_7 - e_8)$ и $\frac{1}{2}(e_1 + e_2 + e_3 + e_4 - e_5 - e_6 - e_7 - e_8)$ — это $e_1 - e_5$).

Рассмотрим элемент группы Вейля $w_{i,j} = w_{\gamma_{i,j}}(1) w_{\gamma_i}(1) w_{\gamma_j}(1) w_{\gamma_{i,j}}(1)$. Легко показать, что $w_{i,j}^2 = E$ и $w_{i,j} Q_{\gamma_i} w_{i,j} = Q_{\gamma_j}$.

Рассмотренная замена базиса не меняет элементы $w_{i,j}$.

Посмотрим на $W_{i,j} = \varphi_1(w_{i,j})$. Понятно, что это тоже элемент порядка два, переводящий P_{γ_i} в P_{γ_j} сопряжением (сейчас мы находимся в базисе, в котором все P_q диагональны и совпадают с диагональным видом Q_q). При этом $W_{i,j}$ коммутирует со всеми P_{γ_k}, $k \neq i, j$.

Рассмотрим некоторые корни α, β и место (α, β) в матрице $W_{i,j}$.

Пусть корни α и β ортогональны γ_i и γ_j. Тогда они обязательно не ортогональны каким-то γ_k, $k \neq i, j$. Ясно, что чтобы на месте (α, β) стоял не ноль, нужно, чтобы для всякого γ_k, $k \neq i, j$, $\langle \alpha, \gamma_k \rangle = \langle \beta, \gamma_k \rangle$.

Для системы корней A_l можно для удобства считать, что $\gamma_i = \alpha_1$, $\gamma_j = \alpha_3$, $\alpha = e_p - e_q$, $\beta = e_t - e_s$. Сразу получаем, что $p, q, t, s > 4$. Пусть $p \neq t$, $q \neq s$. Рассмотрим $\gamma_k = e_p - e_{p+1}$ или $e_{p-1} - e_p$. Понятно, что, исходя из предположения, в первом случае $s = p+1$, во втором — $s = p - 1$. Аналогично, $t = q + 1$ или $q - 1$. Ясно, что не может быть ситуации, когда $p \neq t$, $q = s$, или $p = t$, $q \neq s$. Таким образом, чтобы на месте (α, β) в рассматриваемом случае стоял не ноль, нужно, чтобы $\alpha = \beta$ или $\alpha = -\beta \pm \gamma_l \pm \gamma_k$ (для каждого α существует не более одного такого β).

Для систем корней D_l, E_l ситуация еще лучше, так как в последовательности $\gamma_1, \dots, \gamma_k$ есть дополнительные корни, чтобы различить α и β. Поэтому в этом случае обязательно $\alpha = \beta$.

Теперь пусть корень α ортогонален γ_i и γ_j, а корень β — нет (и пусть он не ортогонален по крайней мере γ_j). Мы знаем, что выполняется соотношение $P_{\gamma_i} W_{i,j} = W_{i,j} P_{\gamma_j}$. Пусть на месте (α, β) в матрице $W_{i,j}$ стоит a, тогда в соотношении в левой матрице на этом место будет стоять по-прежнему a, а в правой — $a\xi$ или $a\xi^2$. Отсюда следует, что $a = 0$.

Остается рассмотреть случаи, когда оба корня α, β не ортогональны каким-то из корней γ_i, γ_j. Из тех же рассуждений, что и в предыдущем абзаце, следует, что если и α, и β ортогональны одному из γ_i, γ_j и не ортогональны второму, что на месте (α, β) стоит ноль.

Теперь пусть, для определенности, $\alpha \perp \gamma_j$, $\beta \perp \gamma_i$. В этом случае возможны снова два варианта: либо $\alpha = \pm\gamma_i$, либо существует еще какие-то γ_t, $t \neq i, j$, которым α не ортогонален. В первом случае понятно, что коэффициент будет ненулевым, только если $\beta = \pm\gamma_j$ (с тем же знаком). Во втором случае снова рассмотрим систему корней A_l, для удобства предположим, что $\gamma_i = \alpha_1$, $\gamma_j = \alpha_3$, тогда $\alpha = \pm e_1 \pm e_p$ или $\pm e_2 \pm e_p$, $p > 4$, сразу видно, что для β есть две возможности: либо это корень $w_{i,j}(\alpha) = \pm e_3 \pm e_p$ или $\pm e_4 \pm e_p$, либо это корень $-w_{i,j}(\alpha) \pm \gamma_j \pm \gamma_t$, $\gamma_t = e_p - e_{p+1}$ или $e_{p-1} - e_p$. Для других систем корней снова ситуация может быть только еще однозначнее.

В последнем из случаев для рассмотрения α и β не ортогональны ни γ_i, ни γ_j. Рассмотрим снова системы корней по отдельности.

Для системы корней A_l в предположении, что $\gamma_i = \alpha_1$, $\gamma_j = \alpha_3$, должно быть $\alpha = \pm e_p \pm e_q$, где $p = 1, 2$, $q = 3, 4$. Без ограничения общности можем считать, что $\alpha = e_1 - e_3$, тогда $\beta = e_3 - e_1$ или $\beta = e_2 - e_4$. Так для каждого из возможных корней α есть две возможности корня β.

Для системы корней D_l если $\gamma_i = e_1 - e_2$, $\gamma_j = e_3 - e_4$, $\alpha = e_1 - e_3$, $\beta = e_3 - e_1$, то $\langle \alpha, e_1 + e_2 \rangle \neq \langle \beta, e_1 + e_2 \rangle$, откуда снова получим, что на месте (α, β) стоит ноль. Значит, остается только возможность $\beta = e_2 - e_4$. Аналогично получаем единственную возможность $\beta = w_{i,j}(\alpha)$ для других выборов α. Если $\gamma_i = e_1 - e_2$, $\gamma_j = e_1 + e_2$, то α обязательно должно быть или $\pm e_1 \pm e_p$, или $\pm e_2 \pm e_p$, $p > 2$. Пусть, например, $\alpha = e_1 - e_3$. Тогда сразу видно, что $\beta = e_1 - e_3$, всего одна возможность.

Для системы корней E_l ситуация совершенно аналогична системе D_l.

На части базиса, образованной векторами $h_{\alpha_1}, \dots, h_{\alpha_l}$, пока матрица $W_{i,j}$ может быть произвольной.

Заметим, что для систем корней D_l, E_l элементы $W_{i,j}$ сразу же (просто после рассмотрения соотношений) близки к их прообразам $w_{i,j}$, поэтому мы рассмотрим замены базиса для систем корней A_l как для случая, где $W_{i,j}$ наиболее далеки от $w_{i,j}$. Для удобства рассмотрим систему корней A_5. Понятно, что для всех остальных рассматриваемых систем корней замены будут производиться аналогично.

В системе корней A_5 упорядочим корни таким образом: $\pm(e_1-e_2), \pm(e_2-e_3), \pm(e_3-e_4), \pm(e_4-e_5), \pm(e_5-e_6),\ \pm(e_1-e_3), \pm(e_2-e_4), \pm(e_3-e_5), \pm(e_4-e_6),\ \pm(e_1-e_4), \pm(e_2-e_5), \pm(e_2-e_6),\ \pm(e_1-e_5), \pm(e_2-e_6), \pm(e_1-e_6)$.

Нас будут интересовать $W_{1,3}$ и $W_{3,5}$ (так как $W_{1,5}$ ими порождается). Рассмотрим по отдельности части базиса, инвариантные одновременно относительно $W_{1,3}$ и $W_{3,5}$.

Инвариантна относительно обеих матриц часть базиса $\{\pm(e_1-e_2), \pm(e_3-e_4), \pm(e_5-e_6)\}$, на которой

$$W_{1,3} = \begin{pmatrix} 0 & 0 & a_{1,5} & 0 & 0 & 0 \\ 0 & 0 & 0 & a_{2,6} & 0 & 0 \\ a_{5,1} & 0 & 0 & 0 & 0 & 0 \\ 0 & a_{6,2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a_{9,9} & 0 \\ 0 & 0 & 0 & 0 & 0 & a_{10,10} \end{pmatrix}, \quad W_{3,5} = \begin{pmatrix} b_{1,1} & 0 & 0 & 0 & 0 & 0 \\ 0 & b_{2,2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & b_{5,9} & 0 \\ 0 & 0 & 0 & 0 & 0 & b_{6,10} \\ 0 & 0 & b_{9,5} & 0 & 0 & 0 \\ 0 & 0 & 0 & b_{10,6} & 0 & 0 \end{pmatrix}.$$

Произведем замену базиса (коммутирующую со всеми $P_{\alpha_1}, P_{\alpha_3}, P_{\alpha_5}$) следующим образом: $v_1' = v_1, v_2' = v_2, v_5' = a_{1,5}v_5, v_6' = a_{2,6}v_6, v_9' = b_{5,9}a_{1,5}v_9, v_{10}' = b_{6,10}a_{1,6}v_{10}$. Тогда матрицы $W_{1,3}, W_{3,5}$ На этих частях базиса примут вид

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ a_{5,1}' & 0 & 0 & 0 & 0 & 0 \\ 0 & a_{6,2}' & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a_{9,9} & 0 \\ 0 & 0 & 0 & 0 & 0 & a_{10,10} \end{pmatrix} \text{ и } \begin{pmatrix} b_{1,1} & 0 & 0 & 0 & 0 & 0 \\ 0 & b_{2,2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & b_{9,5}' & 0 & 0 & 0 \\ 0 & 0 & 0 & b_{10,6}' & 0 & 0 \end{pmatrix},$$

а так как $W_{1,3}^2 = W_{3,5}^2 = E$, то $a_{5,1}' = a_{6,2}' = b_{9,5}' = b_{10,6}' = 1$. Кроме того,

$$W_{1,3}W_{3,5} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ b_{1,1} & 0 & 0 & 0 & 0 & 0 \\ 0 & b_{2,2} & 0 & 0 & 0 & 0 \\ 0 & 0 & a_{9,9} & 0 & 0 & 0 \\ 0 & 0 & 0 & a_{10,10} & 0 & 0 \end{pmatrix}$$

— это элемент порядка три, то $b_{1,1} = a_{9,9}$, $b_{2,2} = a_{10,10}$, все эти элементы имеют порядок 2.

Следующая часть базиса —

$$\pm(e_2-e_3), \pm(e_4-e_5), \pm(e_1-e_4), \pm(e_2-e_5), \pm(e_3-e_6), \pm(e_1-e_6).$$

На ней матрица $W_{1,3}$ равна

$$\begin{pmatrix}
a_{3,3} & 0 & 0 & 0 & 0 & a_{3,20} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & a_{4,4} & 0 & 0 & a_{4,19} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & a_{7,21} & 0 & 0 & 0 & 0 & a_{7,30} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & a_{8,22} & 0 & 0 & a_{8,29} & 0 \\
0 & a_{19,4} & 0 & 0 & a_{19,19} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
a_{20,3} & 0 & 0 & 0 & 0 & a_{20,20} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & a_{21,7} & 0 & 0 & 0 & 0 & 0 & 0 & a_{21,24} & 0 & 0 \\
0 & 0 & 0 & a_{22,8} & 0 & 0 & 0 & 0 & a_{22,23} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & a_{23,22} & 0 & 0 & a_{23,29} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & a_{24,21} & 0 & 0 & 0 & 0 & a_{24,30} \\
0 & 0 & 0 & a_{29,8} & 0 & 0 & 0 & 0 & a_{29,23} & 0 & 0 & 0 \\
0 & 0 & a_{30,7} & 0 & 0 & 0 & 0 & 0 & 0 & a_{30,24} & 0 & 0
\end{pmatrix},$$

а матрица $W_{3,5}$ равна

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & b_{3,21} & 0 & 0 & 0 & 0 & b_{3,30}\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & b_{4,22} & 0 & 0 & b_{4,29} & 0\\
0 & 0 & b_{7,7} & 0 & 0 & 0 & 0 & 0 & 0 & b_{7,24} & 0 & 0\\
0 & 0 & 0 & b_{8,8} & 0 & 0 & 0 & 0 & b_{8,23} & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & b_{19,22} & 0 & 0 & b_{19,29} & 0\\
0 & 0 & 0 & 0 & 0 & 0 & b_{20,21} & 0 & 0 & 0 & 0 & b_{20,30}\\
b_{21,3} & 0 & 0 & 0 & 0 & b_{21,20} & 0 & 0 & 0 & 0 & 0 & 0\\
0 & b_{22,4} & 0 & 0 & b_{22,19} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & b_{23,8} & 0 & 0 & 0 & 0 & b_{23,23} & 0 & 0 & 0\\
0 & 0 & b_{24,7} & 0 & 0 & 0 & 0 & 0 & 0 & b_{24,24} & 0 & 0\\
0 & b_{29,4} & 0 & 0 & b_{29,19} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
b_{30,3} & 0 & 0 & 0 & 0 & b_{30,20} & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.$$

Опишем на этой части нужную нам замену базиса (естественно, коммутирующую со всеми $P_{\alpha_1}, P_{\alpha_3}, P_{\alpha_5}$). Замену базиса будем производить постепенно, по шагам.

1. Все векторы базиса остаются неизменными, кроме векторов v_{19} и v_{20}. Именно, $v_{19}' = a_{4,4}v_4 + a_{19,4}v_{19}$, $v_{20}' = a_{3,3}v_3 + a_{20,3}v_{20}$. После таких преобразований в матрице $W_{3,5}$ структура не изменится (только поменяются ненулевые элементы $b_{i,j}$, но мы для простоты не будем писать штрихи), а у матрицы $W_{1,3}$ (в том числе благодаря тому, что она имеет порядок два) будет вид

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & a_{7,21} & 0 & 0 & 0 & 0 & a_{7,30}\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & a_{8,22} & 0 & 0 & a_{8,29} & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & a_{21,7} & 0 & 0 & 0 & 0 & 0 & 0 & a_{21,24} & 0 & 0\\
0 & 0 & 0 & a_{22,8} & 0 & 0 & 0 & 0 & a_{22,23} & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & a_{23,22} & 0 & 0 & a_{23,29} & 0\\
0 & 0 & 0 & 0 & 0 & 0 & a_{24,21} & 0 & 0 & 0 & 0 & a_{24,30}\\
0 & 0 & 0 & a_{29,8} & 0 & 0 & 0 & 0 & a_{29,23} & 0 & 0 & 0\\
0 & 0 & a_{30,7} & 0 & 0 & 0 & 0 & 0 & 0 & a_{30,24} & 0 & 0
\end{pmatrix}.$$

Далее применим следующую замену.

2. Все векторы базиса остаются неизменными, кроме векторов v_{21} и v_{22}. Именно, $v_{21}' = b_{21,3}v_{21} + b_{30,3}v_{30}$, $v_{22}' = b_{22,4}v_{22} + b_{29,4}v_{29}$. После таких преобразований в матрице $W_{1,3}$ структура не изменится, а матрица $W_{3,5}$ примет вид

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & b_{7,7} & 0 & 0 & 0 & 0 & 0 & 0 & b_{7,24} & 0 & 0\\
0 & 0 & 0 & b_{8,8} & 0 & 0 & 0 & 0 & b_{8,23} & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & b_{19,22} & 0 & 0 & b_{19,29} & 0\\
0 & 0 & 0 & 0 & 0 & 0 & b_{20,21} & 0 & 0 & 0 & 0 & b_{20,30}\\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & b_{23,8} & 0 & 0 & 0 & 0 & b_{23,23} & 0 & 0 & 0\\
0 & 0 & b_{24,7} & 0 & 0 & 0 & 0 & 0 & 0 & b_{24,24} & 0 & 0\\
0 & 0 & 0 & 0 & b_{29,19} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & b_{30,20} & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.$$

3. Все векторы базиса остаются неизменными, кроме векторов v_7 и v_8. Именно, $v_7' = a_{7,21}v_7 + a_{24,21}v_{24}$, $v_8' = a_{8,22}v_8 + a_{23,22}v_{23}$. После таких преобразований в матрице $W_{3,5}$ структура не изменится, а матрица $W_{1,3}$ примет вид

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & a_{7,30}\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & a_{8,29} & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & a_{21,24} & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & a_{22,23} & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a_{23,29} & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a_{24,30}\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a_{29,23} & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a_{30,24} & 0 & 0
\end{pmatrix}.$$

Мы знаем, что $W_{3,5}^2 = E$. У матрицы $W_{3,5}^2$ на месте $(5,2)$ стоит $b_{19,22}$, а на месте $(6,1)$ — $b_{20,21}$. Значит, $b_{19,22} = b_{20,21} = 0$.

Будем теперь производить дальнейшие замены.

4. Все векторы базиса остаются неизменными, кроме векторов v_{23} и v_{24}. Именно, $v'_{23} = b_{7,7}v_7 + b_{24,7}v_{24}$, $v'_{24} = b_{8,8}v_8 + b_{23,8}v_{24}$. После таких преобразований в матрице $W_{1,3}$ структура не изменится, а матрица $W_{3,5}$ примет вид

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & b_{19,29} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & b_{20,30} \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & b_{29,19} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & b_{30,20} & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.$$

Из того, что матрица $W_{1,3}W_{3,5}$ имеет порядок три, сразу получаем $a_{22,23} = a_{21,24} = 0$. Из того, что $W_{1,3}$ имеет порядок два, следует, что $a_{7,30} = a_{8,29} = 0$.

5. Теперь рассмотрим последнюю замену базиса, в которой $v'_{29} = b_{29,19}v_{29}$, $v'_{30} = b_{30,20}v_{30}$, $v'_{23} = a_{23,29}v_{23}$, $v'_{24} = a_{24,30}v_{30}$. После этой замены мы будем иметь $W_{1,3} = w_{1,3}$, $W_{3,5} = w_{3,5}$ на рассматриваемой части базиса.

На части базиса $\pm(e_1 - e_3), \pm(e_2 - e_4), \pm(e_3 - e_5), \pm(e_4 - e_6), \pm(e_1 - e_5), \pm(e_2 - e_6)$ все рассуждения аналогичны предыдущей части.

Осталось рассмотреть часть базиса $h_{\alpha_1}, h_{\alpha_2}, h_{\alpha_3}, h_{\alpha_4}, h_{\alpha_5}$. На ней можно производить любую замену базиса, так как все $P_{\alpha_1}, P_{\alpha_3}, P_{\alpha_5}$ на этой части базиса единичны.

Пусть на этой части

$$W_{1,3} = \begin{pmatrix}
a_{31,31} & a_{31,32} & a_{31,33} & a_{31,34} & a_{31,35} \\
a_{32,31} & a_{32,32} & a_{32,33} & a_{32,34} & a_{32,35} \\
a_{33,31} & a_{33,32} & a_{33,33} & a_{33,34} & a_{33,35} \\
a_{34,31} & a_{34,32} & a_{34,33} & a_{34,34} & a_{34,35} \\
a_{35,31} & a_{35,32} & a_{35,33} & a_{35,34} & a_{35,35}
\end{pmatrix}, \quad W_{3,5} = \begin{pmatrix}
b_{31,31} & b_{31,32} & b_{31,33} & b_{31,34} & b_{31,35} \\
b_{32,31} & b_{32,32} & b_{32,33} & b_{32,34} & b_{32,35} \\
b_{33,31} & b_{33,32} & b_{33,33} & b_{33,34} & b_{33,35} \\
b_{34,31} & b_{34,32} & b_{34,33} & b_{34,34} & b_{34,35} \\
b_{35,31} & b_{35,32} & b_{35,33} & b_{35,34} & b_{35,35}
\end{pmatrix}.$$

Произведем сначала такую замену базиса. Все элементы базиса остаются неизменными, только $v'_{33} = a_{31,33}v_{31} + a_{32,33}v_{32} + a_{33,33}v_{33} + a_{34,33}v_{34} + a_{35,33}v_{35}$. После такой замены матрица $W_{1,3}$ примет вид

$$W_{1,3} = \begin{pmatrix}
0 & a_{31,32} & 1 & a_{31,34} & a_{31,35} \\
0 & a_{32,32} & 0 & a_{32,34} & a_{32,35} \\
1 & a_{33,32} & 0 & a_{33,34} & a_{33,35} \\
0 & a_{34,32} & 0 & a_{34,34} & a_{34,35} \\
0 & a_{35,32} & 0 & a_{35,34} & a_{35,35}
\end{pmatrix}.$$

Следующей заменой базиса будем менять только v_{32}. Именно, $v'_{32} = (a_{31,34}v_{31} + a_{32,34}v_{32} + a_{33,34}v_{33} + a_{34,34}v_{34} + a_{35,34}v_{35}) - v_{34} - v_{33}$. Тогда матрица $W_{1,3}$ будет иметь вид (пользуемся заодно тем, что $W_{1,3}^2 = E$)

$$W_{1,3} = \begin{pmatrix}
0 & -1 & 1 & 0 & a_{31,35} \\
0 & -1 & 0 & 1 & a_{32,35} \\
1 & -1 & 0 & 1 & a_{33,35} \\
0 & 0 & 0 & 1 & a_{34,35} \\
0 & 0 & 0 & 0 & a_{35,35}
\end{pmatrix}.$$

Аналогичными заменами для матрицы $W_{3,5}$ (менять нужно элементы базиса v_{34} и v_{35}) мы можем добиться

$$W_{3,5} = \begin{pmatrix} b_{31,31} & 0 & 0 & 0 & 0 \\ b_{32,31} & 1 & 0 & 0 & 0 \\ b_{33,31} & 1 & 0 & -1 & 0 \\ b_{34,31} & 1 & 0 & -1 & 0 \\ b_{35,31} & 0 & 1 & -1 & 1 \end{pmatrix}.$$

Далее мы имеем неизвестные $a_{31,35}, a_{32,35}, a_{33,35}, a_{34,35}, a_{35,35}, b_{31,31}, b_{32,31}, b_{33,31}, b_{34,31}, b_{35,31}$, из которых $a_{35,35}$ и $b_{31,31}$ сравнимы с единицей по модулю радикала, остальные переменные лежат в радикале.

Кроме того, у нас есть три матричных соотношения:

1) $W_{1,3}^2 = E$;

2) $W_{3,5}^2 = E$;

3) $(W_{1,3}W_{3,5})^3 = E$.

Из них мы получаем некоторое количество полиномиальных соотношений на переменные.

Будем постепенно избавляться от переменных, считая их коэффициенты по модулю радикала. Если в конце мы придем к тому, что последняя переменная равна нулю, то и все переменные равны тому, с чем они сравнимы по модулю радикала.

Из позиции $(1,5)$ соотношения 1) следует $a_{32,35} = a_{33,35} + a_{31,35}$; из позиции $(3,5)$ — $a_{34,35} = 0$. Аналогично, из позиции $(5,1)$ соотношения 2) следует $b_{34,31} = b_{35,31} + b_{33,31}$; из позиции $(33,31)$ — $b_{32,31} = 0$. Из позиции $(2,2)$ соотношения 3) следует $b_{35,31} = -b_{33,31}$; из позиции $(1,3)$ — $a_{31,35} = 0$; из позиции $(1,4)$ — $b_{33,31} = 0$; из позиции $(1,2)$ — $a_{35,35} = 1$; из позиции $(1,1)$ — $b_{31,31} = 1$, и, наконец, из позиции $(2,3)$ — $a_{33,35} = 0$. Таким образом, на этой части базиса также $W_{1,3}$ и $W_{3,5}$ совпали с $w_{1,3}$ и $w_{3,5}$, соответственно.

В совокупности у нас получилось, что $W_{1,3}$ отличается от $w_{1,3}$ только в позициях $(9,9)$ и $(10,10)$, где матрица диагональна, но на диагонали имеет не единицы, а некоторые элементы порядка два, сравнимые с единицей. Из того, что $W_{1,3}$ имеет единичный определитель (так как является произведением коммутаторов), то эти элементы на диагонали равны. Аналогичны равны друг другу (и множителям для $W_{1,3}$) элементы на позициях $(1,1)$ и $(2,2)$ у матрицы $W_{3,5}$. Обозначим их через μ. Понятно, как диагональной заменой базиса во всех рассмотренных его частях добиться того, что $W_{1,3} = \mu w_{1,3}$, $W_{3,5} = \mu w_{3,5}$.

Теперь заменой базиса, обратной к исходной, вернем Q_{γ_i} из диагонального вида в нормальный, в котором в матрице уже не встречаются элементы ξ и ξ^2. Как мы знаем, $W_{i,j}$ при этом не поменяются.

Таким образом, мы теперь можем считать, что нам дан изоморфизм φ_2 со всеми свойствами изоморфизма φ_1, и еще такой, что $\varphi_2(Q_{\gamma_i}) = Q_{\gamma_i}$ для всех $i = 1, \ldots, k$; $\varphi_2(w_{i,j}) = \mu w_{i,j}$ для всех $i, j = 1, \ldots, k$, $i \neq j$, $\mu^2 = 1$.

Будем далее предполагать, что мы рассматриваем изоморфизм φ_2 с этими свойствами.

1.9.3 Ограничение рассмотрения образов элементов $x_\alpha(1)$ и $w_\alpha(1)$ на различные части базиса

Предположим теперь, что $\varphi_2(x_{\alpha_i}(1)) = x_i$, $\varphi_2(w_{\alpha_i}(1)) = W_i$.

Для начала рассмотрим x_1 (мы сейчас считаем, что корни в любом случае пронумерованы так, чтобы $\gamma_1 = \alpha_1$). Мы знаем, что x_1 коммутирует со всеми Q_{γ_i}, $i > 1$. Понятно, что благодаря этому x_1 распадается на некоторые блоки. Посмотрим, на какие именно.

Для начала предположим, что мы имеем дело с системой корней A_l, l нечетно.

Рассмотрим корень $\alpha = e_i - e_j$, $i < j$. Если $\alpha = \alpha_1 = e_1 - e_2$, то α ортогонален всем γ_j, $j > 1$. Понятно, что при этом если взять произвольный другой корень β, не коллинеарный корню α, то будет существовать какое-то γ_j, не ортогональное β. Значит, на месте (α, β) в матрице x_1 должен стоять ноль. Получается, что корни $\pm\alpha_1$ вместе с базисными элементами $h_1, \dots, h_l$ дают нам отдельную инвариантную часть базиса. Пусть теперь $\alpha = e_1 - e_i$, $i > 2$ (аналогично можно будет рассмотреть корни вида $e_2 - e_i$, $i > 2$). Такой корень не ортогонален ровно одному корню из последовательности $\gamma_2, \dots, \gamma_k$, например, γ_j (это либо $e_i - e_{i+1}$, либо $e_{i-1} - e_i$). Тем же свойством будут обладать корни $\pm(e_1 - e_i), \pm(e_2 - e_i)$ и либо $\pm(e_1 - e_{i-1}), \pm(e_2 - e_{i-1}), \pm(e_{i-1} - e_i)$, либо $\pm(e_1 - e_{i+1}), \pm(e_2 - e_{i+1}), \pm(e_i - e_{i+1})$. Именно такое множество корней образует часть базиса, инвариантную относительно матрицы x_1. Осталось рассмотреть корень $e_i - e_j$, не ортогональный сразу к двум γ_p, γ_q. Без ограничения общности предположим, что i, j оба нечетны. Тогда инвариантна часть базиса $\pm(e_i - e_j), \pm(e_i - e_{j+1}), \pm(e_{i+1} - e_j), \pm(e_{i+1} - e_{j+1})$.

Теперь предположим, что мы система корней снова A_l, но l четно.

Аналогичными рассуждениями увидим, что части базиса, на которые будет распадаться матрица x_1, будут иметь один из следующих видов:

1) $\pm(e_1 - e_2), \pm(e_1 - e_{l+1}), \pm(e_2 - e_{l+1}), h_1, \dots;$

2) $\pm(e_1 - e_{2i-1}), \pm(e_1 - e_{2i}), \pm(e_2 - e_{2i-1}), \pm(e_2 - e_{2i}), \pm(e_{2i-1} - e_{2i}), \pm(e_{2i-1} - e_{l+1}), \pm(e_{2i} - e_{l+1})$, $i > 1$;

3) $\pm(e_{2i-1} - e_{2j-1}), \pm(e_{2i-1} - e_{2j}), \pm(e_{2i} - e_{2j-1}), \pm(e_{2i} - e_{2j})$, $i \neq j$, $i, j, > 1$.

Пусть мы имеем дело с системой корней D_l. Части базиса, на которые будет распадаться матрица x_1, будут иметь один из следующих видов:

1) $\pm(e_1 - e_2), h_1, \dots;$

2) $\pm(e_1 + e_2)$;

3) $\pm(e_1 - e_i), \pm(e_2 - e_i)$, $i > 2$;

4) $\pm(e_1 + e_i), \pm(e_2 + e_i)$, $i > 2$;

5) $\pm(e_i - e_j)$, $i, j > 2$;

6) $\pm(e_i + e_j)$, $i, j > 2$.

Видно, что они будут заведомо мельче, чем части базиса для систем корней A_l.

Теперь пусть рассматривается система E_8. В этом случае получатся такие части базиса:

1) $\pm(e_1 - e_2), h_1, \dots;$

2) $\pm(e_1 + e_2)$;

3) $\pm(e_1 - e_i), \pm(e_2 - e_i)$, $i > 2$;

4) $\pm(e_1 + e_i), \pm(e_2 + e_i)$, $i > 2$;

5) $\pm(e_i - e_j)$, $i, j > 2$;

6) $\pm(e_i + e_j)$, $i, j > 2$;

7) $\pm\frac{1}{2}(-e_1 + e_2 \pm e_3 \pm e_4 \pm e_5 \pm e_6 \pm e_7 \pm e_8), \pm\frac{1}{2}(e_1 - e_2 \pm e_3 \pm e_4 \pm e_5 \pm e_6 \pm e_7 \pm e_8)$;

8) $\pm\frac{1}{2}(e_1 + e_2 \pm e_3 \pm e_4 \pm e_5 \pm e_6 \pm e_7 \pm e_8)$.

Для таких систем корней тоже части базиса строго являются разбиениями частей базиса для системы корней A_l.

Благодаря этому мы можем ограничиться рассмотрением системы A_l, $l \geqslant 3$.

Теперь посмотрим на элемент x_2. Он коммутирует с элементами Q_i нашей последовательности, только начиная с ее третьего члена, поэтому будет распадаться изначально на более крупные части базиса.

Как мы уже видели, можно не рассматривать системы корней D_l, E_l, а рассмотреть только систему корней A_l, $l \geqslant 3$.

Для этой системы если l нечетно, то матрица x_2 разбивается на следующие части:

1) $\pm(e_1-e_2), \pm(e_1-e_3), \pm(e_1-e_4), \pm(e_2-e_3), \pm(e_2-e_4), \pm(e_3-e_4), h_1, \dots;$

2) $\pm(e_1-e_i), \pm(e_2-e_i), \pm(e_3-e_i), \pm(e_4-e_i), \pm(e_1-e_{i+1}), \pm(e_2-e_{i+1}), \pm(e_3-e_{i+1}), \pm(e_4-e_{i+1})$, $i > 4$, i нечетно;

3) $\pm(e_i-e_j), \pm(e_i-e_{j+1}), \pm(e_{i+1}-e_j), \pm(e_{i+1}-e_{j+1})$, $i, j > 4$, i, j нечетны;

4) $\pm(e_i-e_{i+1})$, $i > 4$, i нечетно.

Если l четно, то части будут иметь вот такой вид:

1) $\pm(e_1-e_2), \pm(e_1-e_3), \pm(e_1-e_4), \pm(e_2-e_3), \pm(e_2-e_4), \pm(e_3-e_4), \pm(e_1-e_{l+1}), \pm(e_2-e_{l+1}), \pm(e_3-e_{l+1}), \pm(e_4-e_{l+1}), h_1, \dots;$

2) $\pm(e_1-e_i), \pm(e_2-e_i), \pm(e_3-e_i), \pm(e_4-e_i), \pm(e_1-e_{i+1}), \pm(e_2-e_{i+1}), \pm(e_3-e_{i+1}), \pm(e_4-e_{i+1}), \pm(e_i-e_{l+1}), \pm(e_{i+1}-e_{l+1})$, $i > 4$, i нечетно;

3) $\pm(e_i-e_j), \pm(e_i-e_{j+1}), \pm(e_{i+1}-e_j), \pm(e_{i+1}-e_{j+1})$, $i, j > 4$, i, j нечетны;

4) $\pm(e_i-e_{i+1}), \pm(e_i-e_{l+1}), \pm(e_{i+1}-e_{l+1})$, $i > 4$, i нечетно.

Таким образом, в совокупности (для x_1 и x_2) наши матрицы разбиваются на те же части базиса, которые перечислены выше для матрицы x_2.

Ясно, что случаи четного и нечетного l нужно рассматривать по отдельности, но не нужно рассматривать никакие системы корней, кроме A_l.

1.9.4 Образы элементов w_{α_i} и $x_{\alpha_i}(1)$

Заметим, что на каждой части базиса и в каждом из рассматриваемых случаев ситуация такова: имеется несколько известных матриц (например, Q_{α_1}, Q_{α_3}, $w_{1,3}$) и несколько неизвестных (например, образы матриц $w_{\alpha_1}(1)$ и $w_{\alpha_2}(1)$, которые мы обозначим через $w_{\alpha_1}(1)+W_1$ и $w_{\alpha_2}(1)+W_2$). Понятно, что обе матрицы W_1 и W_2 лежат в идеале $M_N(J)$. Все остальные неизвестные матрицы каким-то образом выражаются через известные и введенные неизвестные матрицы (например, $\varphi_2(x_{\alpha_1}(1)) = Q_{\alpha_1}\cdot(w_{\alpha_1}(1)+W_1)^3$). Кроме того, имеется некоторый набор соотношений (например, $(w_{\alpha_1}(1)+W_1)Q_{\alpha_3} = Q_{\alpha_3}(w_{\alpha_1}(1)+W_1)$), которым удовлетворяют неизвестные матрицы W_1 и W_2. Мы хотим показать, что можно, сделав еще несколько замен базиса, коммутирующих с уже известными матрицами, добиться того, что всем выписанным соотношениям могут удовлетворять только нулевые матрицы W_1 и W_2. Это будет означать, что матрицы $w_{\alpha_1}(1)$ и $w_{\alpha_2}(1)$ при полученном изоморфизме переходят в себя, что нам и требуется.

Пусть элементы матриц W_1 и W_2 обозначены через $z_1, \dots, z_p$. Заметим, что каждое матричное соотношение дает N^2 полиномиальных уравнений от переменных $z_1, \dots, z_p$ с целыми коэффициентами.

Как и выше, мы можем последовательно выписывать искомые соотношения, но для простоты писать все коэффициенты по модулю радикала (в результате эти коэффициенты будут иметь вид чисел 0 и 1).

Понятно, что такая процедура эквивалентна "линеаризации" всех соотношений относительно переменных матриц W_1 и W_2. Именно, если при раскрытии скобок в соотношении где-то стоит выражение W_iW_jA, где $i, j \in \{1, 2\}$, A — любая матрица, то такое выражение мы можем считать нулевым. В результате соотношения станут иметь линейный вид относительно W_1 и W_2.

Нам нужно будет в результате показать, что после выражения одних неизвестных через другие в этих соотношениях все неизвестные оказываются нулевыми.

Сначала покажем это на простых частях базиса — на третьей и четвертой.

Части базиса четвертого типа

Это самая простая часть базиса, имеющая вид $\pm(e_i - e_{i+1})$, $i > 4$, i нечетно. На этой части базиса все интересующие нас матрицы ($w_{\alpha_1}(1)$, $w_{\alpha_2}(1)$, $x_{\alpha_1}(1)$, $x_{\alpha_2}(1)$, $x_{\alpha_1+\alpha_2}(1)$) единичны.

Мы знаем, что элемент $(w_{\alpha_1}(1) + W_1)(w_{\alpha_2}(1) + W_2) = (E + W_1)(E + W_2)$ имеет порядок три. Линеаризуя это соотношение, получаем:

$$(E + W_1 + W_2)^3 = E \Longleftrightarrow 3W_1 = -3W_2 \Longleftrightarrow W_2 = W_1.$$

Таким образом, мы можем считать, что $W_2 = W_1$.

Теперь вспомним, что $\varphi(x_{\alpha_1}(1)) = x_{\alpha_1}(1)+X_1 = E+X_1 = Q_1\cdot(w_{\alpha_1}(1)+W_1)^3 = (E+W_1)^3$, откуда после линеаризации $X_1 = 3W_1 = W_1$. Кроме того $E + X_{1+2} = \varphi_2(x_{\alpha_1+\alpha_2}(1)) = (E + W_2)\cdot(E + X_1)\cdot(E + W_2)^3 = E + X_1 + 4W_1 = E + X_1$, т. е. $X_{1+2} = X_1$. Аналогично, $E + X_2 = \varphi_2(x_{\alpha_2}(1) = (E + W_1)\cdot(E + X_{1+2})\cdot(E + W_1)^3$, откуда $X_2 = X_{1+2} = X_1 = W_1$.

Теперь воспользуемся соотношением $x_{\alpha_1+\alpha_2}(1)x_{\alpha_1}(1)x_{\alpha_2}(1) = x_{\alpha_2}(1)x_{\alpha_1}(1)$, которое для образов даст нам

$$(E + W_1)(E + W_1)(E + W_1) = (E + W_1)(E + W_1).$$

Очевидно, что это дает нам $W_1 = 0$, что и требовалось.

Части базиса третьего вида

Теперь рассмотрим часть базиса третьего типа, а именно, $\pm(e_i - e_j), \pm(e_i - e_{j+1}), \pm(e_{i+1} - e_j), \pm(e_{i+1} - e_{j+1})$, $i, j > 4$, i, j нечетны.

Заметим, что на этой части, как и на предыдущей, единичны матрицы $w_{\alpha_1}(1)$, $w_{\alpha_2}(1)$, $x_{\alpha_1}(1)$, $x_{\alpha_2}(1)$, $x_{\alpha_1+\alpha_2}(1)$.

Значит, рассуждения абсолютно аналогичны предыдущему пункту, так как в нем мы пользовались только видом выписанных выше матриц и двумя соотношениями, которые будут выполняться и на этой части базиса.

Части базиса второго вида

Перейдем теперь к части базиса второго вида, а именно, вида $\pm(e_1 - e_i), \pm(e_2 - e_i), \pm(e_3 - e_i), \pm(e_4 - e_i), \pm(e_1 - e_{i+1}), \pm(e_2 - e_{i+1}), \pm(e_3 - e_{i+1}), \pm(e_4 - e_{i+1})$, $i > 4$, i нечетно. Матрица W_1 раскладывается в прямую сумму на частях базиса $\pm(e_1 - e_i), \pm(e_2 - e_i), \pm(e_1 -$

$e_{i+1}), \pm(e_2 - e_{i+1})$ и $\pm(e_3 - e_i), \pm(e_4 - e_i), \pm(e_3 - e_{i+1}), \pm(e_4 - e_{i+1})$, поэтому про половину ее коэффициентов мы знаем, что они равны нулю.

Матрица для Q_{α_i} имеет вид

$$Q_i = \begin{pmatrix}
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1
\end{pmatrix};$$

матрица для Q_{α_1} —

$$Q_1 = \begin{pmatrix}
-1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix};$$

матрица для $w_{1,3}$ —

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

матрица для $w_{\alpha_1}(1)$ —

$$
w_1 = \begin{pmatrix}
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix};
$$

матрица для $w_{\alpha_2}(1)$ —

$$
w_2 = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.
$$

Кроме того, $x_1 = x_{\alpha_1}(1) = Q_1 \cdot w_1^{-1}$, $w_3 = w_{\alpha_3}(1) = w_{1,3}w_1w_{1,3}$, $Q_3 = Q_{\alpha_3} = w_{1,3}Q_1w_{1,3}$, $x_{1+2} = x_{\alpha_1+\alpha_2}(1) = w_2x_1w_2^{-1}$, $x_2 = x_{\alpha_2}(1) = w_1x_{1+2}w_1^{-1}$.

Пусть $W_1 = (a_{i,j})$, $W_2 = (b_{i,j})$. Из того, что W_1 коммутирует с Q_{α_3} и с Q_{α_i}, следует, что W_1 на первой части базиса — это

$$
\begin{pmatrix}
a_1 & a_2 & a_3 & a_4 & a_5 - a_1 & a_2 - a_6 & -a_7 & a_4 - a_8\\
a_9 & a_{10} & a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & -a_{16}\\
a_{17} & a_{18} & a_{19} & a_{20} & -a_{21} & a_{18} - a_{22} & a_{23} - a_{19} & a_{20} - a_{24}\\
a_{25} & a_{26} & a_{27} & a_{28} & a_{29} & a_{30} & a_{31} & a_{32}\\
a_1 - a_5 & a_6 & a_7 & a_8 & a_5 & a_2 & a_3 - a_7 & a_4\\
-a_{13} - a_9 & -a_{14} & -a_{15} - a_{11} & a_{16} & a_9 & a_{10} - a_{14} & a_{11} & a_{12} + a_{16}\\
a_{21} & a_{22} & a_{19} - a_{23} & a_{24} & a_{17} - a_{21} & a_{18} & a_{23} & a_{20}\\
-a_{29} - a_{25} & -a_{30} & -a_{31} - a_{27} & -a_{32} & a_{25} & a_{26} - a_{30} & a_{27} & a_{28} - a_{32}
\end{pmatrix},
$$

на второй —

$$
\begin{pmatrix}
-a_{33} + a_{34} & a_{35} + a_{36} & a_{33} & a_{35} & a_{37} & a_{35} + a_{36} - a_{38} & a_{39} & a_{35} + a_{40} - a_{38}\\
-a_{41} - a_{42} & a_{43} + a_{44} & a_{42} & a_{43} & a_{44} & a_{45} & -a_{47} - a_{45} & a_{46} + a_{48}\\
-a_{33} & a_{36} & a_{34} & a_{35} + a_{36} & a_{39} & a_{36} - a_{40} & a_{37} + a_{39} & a_{35} + a_{36} - a_{38}\\
a_{41} & -a_{43} & -a_{41} - a_{42} & a_{44} & a_{47} & -a_{48} - a_{46} & a_{45} & a_{47}\\
-a_{37} & a_{38} & a_{33} - a_{39} & a_{48} & a_{34} + a_{37} - a_{33} & a_{35} + a_{36} & a_{39} & a_{35}\\
a_{41} + a_{42} - a_{45} & -a_{46} & a_{47} + a_{45} - a_{42} & -a_{48} - a_{46} & -a_{41} - a_{42} & a_{44} - a_{46} & a_{42} & a_{43} - a_{46} - a_{48}\\
a_{39} - a_{33} & a_{40} & a_{33} - a_{37} - a_{39} & a_{38} & -a_{39} & a_{36} & a_{34} + a_{37} + a_{39} - a_{33} & a_{35} + a_{36}\\
-a_{41} - a_{47} & a_{46} + a_{48} & a_{41} + a_{42} - a_{45} & a_{48} & a_{41} & a_{46} + a_{48} - a_{43} & -a_{41} - a_{42} & a_{44} + a_{48}
\end{pmatrix}.
$$

Пусть при этом $W_2 = (b_{i,j})$, $1 \leqslant i, j \leqslant 16$.

Рассмотрим замену базиса с помощью матрицы C, которая на первой части базиса имеет вид

$$\begin{pmatrix} 1 & 0 & a_{1,3} & -a_{5,8} & 0 & a_{1,10} & a_{1,11} & b_{1,12} \\ a_{1,2} & 1 & a_{6,7} & 0 & a_{2,9} & 0 & a_{6,15} & a_{2,12} \\ -a_{1,3} & a_{5,8} & 1+a_{1,3} & 0 & -a_{1,11} & a_{1,10}-b_{1,12} & a_{1,11} & a_{1,10} \\ a_{6,7}-a_{1,2} & 0 & a_{1,2} & 1 & a_{2,9}+a_{6,15} & a_{2,12} & a_{2,9} & a_{2,12} \\ 0 & a_{1,10} & a_{1,11} & a_{5,8}+b_{1,12} & 1 & -a_{1,3}-a_{1,11} & a_{5,8} & 0 \\ a_{1,2}+a_{2,9} & 0 & -a_{6,7}+a_{6,15} & a_{2,12} & -a_{1,2} & 1 & a_{6,7} & a_{2,12} \\ -a_{1,11} & 0 & a_{1,11} & a_{1,10} & a_{1,3}+a_{1,11} & 0 & 1 & 0 \\ 0 & -a_{2,12} & a_{1,2}+a_{2,9} & -a_{2,12} & 0 & -a_{2,12} & -a_{1,2} & 1 \end{pmatrix},$$

на второй части —

$$\begin{pmatrix} 1 & 0 & -a_{1,3} & a_{5,8} & 0 & -a_{1,10} & -a_{1,11} & -b_{1,12} \\ -a_{1,2} & 1 & a_{6,7} & 0 & -a_{2,9} & 0 & -a_{6,15} & -a_{2,12} \\ a_{1,3} & -a_{5,8} & 1-a_{1,3} & 0 & a_{1,11} & -a_{1,10}+b_{1,12} & -a_{1,11} & 0 \\ a_{1,2}-a_{6,7} & 0 & a_{1,2} & 1 & a_{2,9}+a_{6,15} & a_{2,12} & -a_{2,9} & a_{2,12} \\ 0 & a_{1,12} & 0 & a_{5,8}+b_{1,12} & 1 & 0 & -a_{1,3}-a_{1,11} & a_{5,8} \\ 0 & a_{1,2}+a_{2,9} & 0 & -a_{6,7}+a_{6,15} & -a_{1,2} & 1 & a_{6,7} & a_{2,12} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Эта матрица коммутирует с Q_1, Q_3, Q_i и со всеми остальными полученными матрицами, поэтому замена базиса с помощью нее не изменит уже зафиксированные нами матрицы. С другой стороны, в линеаризованном виде в матрицах W_1 и W_2 обнулятся следующие элементы: $a_{1,3}$, $a_{1,10}$, $a_{1,11}$, $a_{2,12}$, $b_{1,12}$, $a_{1,2}$, $a_{6,7}$, $a_{2,9}$, $a_{6,15}$, $a_{5,8}$.

Введем выражение неизвестных матриц X_1, X_{1+2}, X_2 через W_1, W_2:

$$\begin{aligned} X_1 &= Q_1W_1w_1^2 + Q_1w_1W_1w_1 + Q_1w_1^2W_1; \\ X_{1+2} &= W_2x_1w_2^3 + w_2X_1w_2^3 + w_2x_1W_2w_2^2 + w_2x_1w_2W_2w_2 + w_2x_1w_2^2W_2; \\ X_2 &= W_1x_{1+2}w_1^3 + w_1X_{1+2}w_1^3 + w_1x_{1+2}W_1w_1^2 + w_1x_{1+2}w_1W_1w_1 + w_1x_{1+2}w_1^2W_1. \end{aligned}$$

Теперь выпишем список соотношений после линеаризации:

$$\begin{cases} W_2Q_i - Q_iW_2 = 0; \\ W_1w_2(w_1w_2)^2 + w_1W_2(w_1w_2)^2 + w_1w_2W_1w_2w_1w_2 + w_1w_2w_1W_2w_1w_2 + \\ \qquad +(w_1w_2)^2W_1w_2 + (w_1w_2)^2w_1W_2 = 0; \\ w_{1,3}W_1w_{1,3}w_1 + w_3W_1 - w_1w_{1,3}W_1w_{1,3} - W_1w_3 = 0; \\ w_2w_1w_3W_2 + w_2w_1w_{1,3}W_1w_{1,3}w_2 + w_2W_1w_3w_2 + W_2w_1w_3w_2 = 0; \\ x_1X_{1+2} + X_1x_{1+2} - X_{1+2}x_1 - x_{1+2}X_1 = 0; \\ X_1x_2x_{1+2} + x_1X_2x_{1+2} + x_1x_2X_{1+2} - X_2x_1 - x_2X_1 = 0. \end{cases}$$

После этого прямым подсчетом получаем, что матрицы W_1 и W_2 — нулевые. Таким образом, $\varphi_2(w_{\alpha_1}(1)) = w_{\alpha_1}(1)$ и $\varphi_2(w_{\alpha_2}(1)) = w_{\alpha_2}(1)$, что и требуется.

Части базиса первого вида

Заметим, что часть базиса первого типа для системы корней A_l с нечетным l — это просто базис системы корней типа A_3. Поэтому рассмотрим данную систему с условием, что матрицы Q_1, Q_3, $w_{1,3}$ переходят в себя.

Соответственно, мы можем считать, что нам даны три простых корня $\alpha_1, \alpha_2, \alpha_3$, порождающие систему корней A_3, базис из весовых векторов пронумерован так:

$$v_1 = v_{\alpha_1}, v_2 = v_{-\alpha_1}, v_3 = v_{\alpha_2}, v_4 = v_{-\alpha_2}, v_5 = v_{\alpha_3}, v_6 = v_{-\alpha_3},$$
$$v_7 = v_{\alpha_1+\alpha_2}, v_8 = v_{-\alpha_1-\alpha_2}, v_9 = v_{\alpha_2+\alpha_3}, v_{10} = v_{-\alpha_2-\alpha_3},$$
$$v_{11} = v_{\alpha_1+\alpha_2+\alpha_3}, v_{12} = v_{-\alpha_1-\alpha_2-\alpha_3}, v_{13} = h_{\alpha_1}, v_{14} = h_{\alpha_2}, v_{15} = h_{\alpha_3}.$$

В этом базисе матрицы, представляющие элементы $w_{\alpha_1}(1)$ и $w_{\alpha_2}(1)$, имеют соответственно вид

$$w_1 = \begin{pmatrix}
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix},$$

и

$$w_2 = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.$$

Кроме того, $x_{\alpha_1}(1)$ имеет вид

$$x_1 = \begin{pmatrix}
1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix};$$

матрица $w_{1,3}$ имеет вид

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

Рассмотрим теперь общий вид матрицы с коэффициентами из радикала, коммутирующей с матрицами Q_1, Q_3 и $w_{1,3}$. Прямым подсчетом получим, что такая матрица C разбивается на два диагональных блока относительно частей базиса $\{v_{\pm 1}, v_{\pm 3}, V_1, V_2, V_3\}$ и $\{v_{\pm 2}, v_{\pm 4}, v_{\pm 5}, v_{\pm 6}\}$; на первой части базиса имеет вид (мы не выписываем удвоенные коэффициенты, потому что они исчезают в линеаризованной форме)

$$\begin{pmatrix}
c_{1,1} & c_{1,2} & c_{1,5} & -c_{1,5} & -c_{1,5} & c_{1,14} & c_{1,5}\\
c_{1,2} & c_{1,1}-c_{1,2}+c_{1,5} & -c_{1,5} & c_{1,5} & -c_{1,5} & -c_{1,2}+c_{1,5}-c_{1,14} & -c_{1,5}\\
c_{1,5} & -c_{1,5} & c_{1,1} & c_{1,2} & c_{1,5} & -c_{1,14} & -c_{1,5}\\
-c_{1,5} & c_{1,5} & c_{1,2} & c_{1,1}-c_{1,2}+c_{1,5} & -c_{1,5} & c_{1,5}-c_{1,2}+c_{1,14} & -c_{1,5}\\
c_{13,1} & -c_{1,2}+c_{13,1}+c_{1,5} & c_{13,5} & -c_{13,5} & c_{1,1}+c_{1,2}+c_{13,1} & c_{13,14} & c_{13,5}\\
-c_{1,5} & c_{1,5} & c_{1,5} & -c1_5 & -c_{1,5} & c_{1,1}+c_{1,2}+c_{1,14} & c_{1,5}\\
-c_{1,5}-c_{13,5} & c_{13,5}+c_{1,5} & c_{1,5}+c_{13,1} & -c_{1,2}+c_{13,1} & -c_{1,5}-c_{13,5} & c_{15,14} & c_{15,15}
\end{pmatrix};$$

на второй части —

$$\begin{pmatrix}
c_{3,3} & c_{3,4} & c_{3,7} & c_{3,8} & c_{3,9} & c_{3,10} & c_{3,11} & c_{3,12}\\
c_{3,4} & c_{3,9}+c_{3,11}+c_{3,3}+c_{3,7} & c_{3,10}-c_{3,4} & c_{3,9}+c_{3,11} & c_{3,8}-c_{3,4} & c_{3,11}+c_{3,7} & c_{4,10} & c_{3,11}\\
-c_{3,7} & c_{3,4}-c_{3,8} & c_{3,3}+c_{3,7} & c_{3,4} & -c_{3,11} & c_{3,10}-c_{3,12} & c_{3,9}+c_{3,11} & c_{3,10}\\
-c_{3,10} & -c_{3,9}-c_{3,11} & c_{3,4} & c_{3,3}+c_{3,7} & c_{3,10}-c_{3,12} & -c_{3,11} & c_{3,8}-c_{3,4} & c_{3,7}\\
-c_{3,9} & c_{3,4}-c_{3,10} & -c_{3,11} & c_{3,8}-c_{3,12} & c_{3,3}+c_{3,9} & c_{3,4} & c_{3,7}+c_{3,11} & c_{3,8}\\
-c_{3,8} & -c_{3,7}-c_{3,11} & c_{3,8}-c_{3,12} & -c_{3,11} & c_{3,4} & c_{3,3}+c_{3,9} & c_{3,10}-c_{3,4} & c_{3,9}\\
c_{3,11} & c_{3,4}-c_{3,8}+c_{3,12}-c_{3,10} & -c_{3,9}-c_{3,11} & c_{3,4}-c_{3,10} & -c_{3,7}-c_{3,11} & c_{3,4}-c_{3,8} & c_{11,11} & c_{3,4}\\
c_{3,12} & c_{3,11} & -c_{3,8} & -c_{3,7} & -c_{3,10} & -c_{3,9} & c_{3,4} & c_{3,3}
\end{pmatrix}.$$

Пусть $W_1 = \varphi_2(w_{\alpha_1}(1)) - w_{\alpha_1}(1) = (x_{i,j})$, $W_2 = \varphi_2(w_{\alpha_2}(1)) - w_{\alpha_2}(1) = (y_{i,j})$.
Выражение других неизвестных через W_1 и W_2 такое же, как в прошлом пункте.
Соотношения после линеаризации имеют такой вид:

$$\begin{cases}
W_1Q_3 - Q_3W_1 = 0;\\
W_1w_{\alpha_2}(1)(w_{\alpha_1}(1)w_{\alpha_2}(1))^2 + w_{\alpha_1}(1)W_2(w_{\alpha_1}(1)w_{\alpha_2}(1))^2+\\
\qquad +w_{\alpha_1}(1)w_{\alpha_2}(1)W_1w_{\alpha_2}(1)w_{\alpha_1}(1)w_{\alpha_2}(1) + w_{\alpha_1}(1)w_{\alpha_2}(1)w_{\alpha_1}(1)W_2w_{\alpha_1}(1)w_{\alpha_2}(1)+\\
\qquad +(w_{\alpha_1}(1)w_{\alpha_2}(1))^2W_1w_{\alpha_2}(1) + (w_{\alpha_1}(1)w_{\alpha_2}(1))^2w_{\alpha_1}(1)W_2 = 0;\\
w_{1,3}W_1w_{1,3}w_{\alpha_1}(1) + w_{\alpha_3}(1)W_1 - w_{\alpha_1}(1)w_{1,3}W_1w_{1,3} - W_1w_3 = 0;\\
w_2w_1w_3W_2 + w_2w_1w_{1,3}W_1w_{1,3}w_2 + w_2W_1w_3w_2 + W_2w_1w_3w_2 = 0;\\
x_1X_{1+2} + X_1x_{1+2} - X_{1+2}x_1 - x_{1+2}X_1 = 0;\\
X_1x_2x_{1+2} + x_1X_2x_{1+2} + x_1x_2X_{1+2} - X_2x_1 - x_2X_1 = 0.
\end{cases}$$

Выберем в матрице C такие элементы: $c_{3,3} = -y_{1,7}$; $c_{1,1} = 0$; $c_{13,14} = y_{13,13}$; $c_{3,12} = y_{1,10}$; $c_{13,1} = x_{13,14}$; $c_{13,5} = -x_{15,14}$; $c_{1,5} = -x_{13,5}$; $c_{3,11} = -x_{5,5}$; $c_{3,9} = x_{4,8}$; $c_{3,7} = -x_{3,7}$; $c_{1,2} = -x_{1,14}$;

$c_{3,10} = -x_{3,10}$; $c_{3,4} = -x_{3,4}$, после этого сопряжем наши матрицы $w_1 + W_1$ и $w_2 + W_2$ рассматриваемой матрицей $E + C$. В линеаризованном виде получим

$$(E + C)(w_i + W_i)(E - C) \sim w_i + W_i + Cw_i - w_i C.$$

Таким образом, увидим, что у матриц W_1 и W_2 следующие элементы (в линеаризованном смысле) стали равны нулю: $y_{5,9}$, $y_{1,7}$, $y_{13,13}$, $y_{1,10}$, $x_{13,14}$, $x_{15,14}$, $x_{13,5}$, $x_{5,5}$, $x_{4,8}$, $x_{3,7}$, $x_{1,14}$, $x_{3,10}$, $x_{3,4}$.

После этого применим напрямую все выписанные соотношения, получим, что матрицы W_1 и W_2 полностью равны нулю. Таким образом, $\varphi_2(w_{\alpha_1}(1)) = w_{\alpha_1}(1)$ и $\varphi_2(w_{\alpha_2}(1)) = w_{\alpha_2}(1)$, что и требуется.

1.9.5 Образы элементов $x_{\alpha_i}(t)$

Теперь нас будут интересовать образы матриц $x_{\alpha_i}(t)$.

Так как все части базиса рассматриваются похожим образом, то посмотрим только на часть базиса второго типа.

Так как все элементы группы Вейля переходят в себя под действием φ, то достаточно проследить за образами элементов $x_{\alpha_1}(t)$. Фиксируем произвольный элемент $t \in R$ и рассмотрим образ $\varphi(x_{\alpha_1}(t)) = X_t$. Из того, что матрица X_t коммутирует с матрицами w_{α_3}, $x_{\alpha_1}(1)$, $x_{\alpha_3}(1)$, $x_{\alpha_i}(1)$, Q_i, Q_3, $x_{\alpha_1+\alpha_2}(1)$ и и $x_{-\alpha_2}(1)$, непосредственно получаем, что матрица X_t имеет вид

$$\begin{pmatrix}
x_{1,1} & 0 & x_{1,3} & 0 & 0 & 0 & 0 & 0 & 0 & x_{1,10} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & x_{2,2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & x_{1,1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & x_{4,2} & 0 & x_{2,2} & 0 & 0 & 0 & 0 & 0 & 0 & x_{4,11} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & x_{1,1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & x_{2,2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & x_{1,1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & x_{2,2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -x_{1,10} & 0 & 0 & 0 & 0 & 0 & 0 & x_{1,1} & 0 & x_{1,3} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_{2,2} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_{1,1} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -x_{4,11} & 0 & 0 & 0 & 0 & 0 & 0 & x_{4,2} & 0 & x_{2,2} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_{1,1} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_{2,2} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_{1,1} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_{2,2}
\end{pmatrix}.$$

Теперь введем $X_t^{1+2} = \varphi_2(x_{\alpha_1+\alpha_2}(t)) = w_2 X_t w_2^{-1}$ и рассмотрим соотношение $X_t^{1+2} x_{\alpha_2}(1) X_t = X_t x_{\alpha_2}(1)$.

Из его позиций $(1,1)$ и $(2,2)$ следует $x_{1,1}(x_{1,1} - 1) = 0$ и $x_{2,2}(x_{2,2} - 1) = 0$, откуда $x_{1,1} = x_{2,2} = 1$. Из позиции $(1,10)$ следует $x_{1,10} = 0$, из позиции $(4,13)$ — $x_{4,11} = 0$. Кроме того, коммутирование с другими элементами группы Вейля дает $x_{4_2} = -x_{1,3}$, откуда $X_t = x_{\alpha_1}(s)$ для некоторого $s \in R^*$.

Если ввести образ элемента $h_{\alpha_1}(t)$, то из аналогичных соотношений получим, что он есть $h_{\alpha_1}(s)$.

Рассмотрением остальных типов частей базиса можно легко убедиться, что для каждого элемента $t \in R^*$ соответствующий $s \in R^*$ един для всего базиса.

1.9.6 Доказательство основной теоремы

Ясно, что $\varphi_2(h_{\alpha_k}(t)) = h_{\alpha_k}(s)$, $k = 1, \dots, n$. Обозначим отображение $t \mapsto s$ через $\rho : R^* \to R^*$. Заметим, что для $t \in R^*$ $\varphi_2(x_1(t)) = \varphi_2(h_{\alpha_2}(t^{-1}) x_1(1) h_{\alpha_2}(t)) = h_{\alpha_2}(s^{-1}) x_1(1) h_{\alpha_2}(s) =$

$x_1(s)$. Если $t \notin R^*$, то $t \in J$, т.е. $t = 1 + t_1$, где $t_1 \in R^*$. Тогда $\varphi_2(x_1(t)) = \varphi_2(x_1(1)x_1(t_1)) = x_1(1)x_1(\rho(t_1)) = x_1(1 + \rho(t_1))$. Таким образом, если мы продолжим отображение ρ на все кольцо R (по формуле $\rho(t) := 1 + \rho(t-1)$, $t \in R$), то получим $\varphi_2(x_1(t)) = x_1(\rho(t))$ для всех $t \in R$. Ясно, что ρ инъективно, аддитивно, а также мультипликативно на всех обратимых элементах. Так как каждый элемент кольца R есть сумма двух обратимых, то получаем, что ρ — это изоморфизм из кольца R на некоторое его подкольцо R'. Заметим, что в данной ситуации $CE(\Phi, R)C^{-1} = E(\Phi, R')$ для некоторой матрицы $C \in \mathrm{GL}\,(V)$. Покажем, что $R' = R$.

Обозначим матричные единицы через E_{ij}.

Лемма 1.18. *Если для некоторого $C \in \mathrm{GL}\,(V)$ имеет место $CE(\Phi, R)C^{-1} = E(\Phi, R')$, где R' — это подкольцо в R, то $R' = R$.*

Доказательство. Покажем, что с помощью группы $E_{\mathrm{ad}}\,(\Phi, R)$ в нашем случае сложением и умножением матриц можно получить любую матрицу $aE_{1,1}$, $a \in R$.

Матрица $((x_{\alpha_1}(1) - 1)(x_{\alpha_2} - 1))^2$ имеет единственный ненулевой элемент $\cdot E_{7,8}$. Аналогично, $E_{8,7} = ((x_{-\alpha_1} - 1)(x_{-\alpha_2} - 1))^2$. Таким образом, сразу получаем матричные единицы $E_{7,7}, E_{7,8}, E_{8,7}$, $E_{8,8}$. Благодаря транзитивности действия группы Вейля на корнях, сопрягая данные матричные единицы с помощью различных элементов группы Вейля, получаем $E_{i,j}$, $i, j \in \{1, 2\}$, $\{3, 4\}$, $\{5, 6\}$, $\{9, 10\}$ или $\{11, 12\}$. Значит, имеем $E_{1,1}$. Далее с помощью элемента $E_{1,1}h_{\alpha_2}(t)E_{1,1}$ имеем $tE_{1,1}$ для всех обратимых $t \in R$. Так как любой элемент кольца R представляется как сумма двух обратимых, то получаем искомые $aE_{1,1}$, $a \in R$.

Предположим теперь, что R' — это собственное подкольцо в R.

Так как $CE(\Phi, R)C^{-1} = E(\Phi, R')$, то подкольцо кольца $M_n(R)$, порожденное всеми элементами группы $E(\Phi, R)$, должно переходить в подкольцо кольца $M_n(R')$, порожденное всеми элементами группы $E(\Phi, R')$. Значит, все коэффициенты матриц $G_a = C(aE_{1,1})C^{-1}$ должны лежать в подкольце R'.

Пусть $C = (c_{k,l})$, $C^{-1} = (c'_{k,l})$. Заметим, что (i, j)-ый коэффициент матрицы G_a равен $ac_{i,1}c_{1,j}$. У любой обратимой матрицы над локальным кольцом в каждом столбце и в каждой строке есть обратимый элемент, поэтому существуют такие i_0 и j_0, для которых $c_{i_0,1}c_{1,j_0}$ обратим. На соответствующем месте в матрице G_a тогда будет стоять любой наперед заданный элемент кольца R.

Полученное противоречие показывает, что $R' = R$. □

Таким образом, мы доказали, что ρ — это автоморфизм кольца R. Следовательно, композиция изначального автоморфизма φ и некоторой замены базиса с помощью матрицы $C \in \mathrm{GL}_n(R)$, (переводящей $E(\Phi, R)$ в себя) — это кольцевой автоморфизм ρ. Это доказывает теорему 1.2. □

Глава 2

Элементарная эквивалентность групп Шевалле над полями и локальными кольцами

Введение

Две модели $\mathcal{U}$ и $\mathcal{U}'$ одного языка первого порядка $\mathcal{L}$ (например, две группы или два кольца) называются *элементарно эквивалентными*, если любое предложение φ языка $\mathcal{L}$ истинно в модели $\mathcal{U}$ тогда и только тогда, когда оно истинно в модели $\mathcal{U}'$. Любые две конечные модели одного языка элементарно эквивалентны тогда и только тогда, когда они изоморфны. Любые две изоморфные модели элементарно эквивалентны, однако для бесконечных моделей обратное неверно. Например, поле $\mathbb{C}$ комплексных чисел и поле $\overline{\mathbb{Q}}$ алгебраических чисел элементарно эквивалентны, но не изоморфны, так как имеют различную мощность (для более подробных примеров см. [28]).

Первые результаты о связи элементарных свойств некоторых моделей с элементарными свойствами производных моделей были получены А.И. Мальцевым в 1961 году в работе [37]. Он доказал, что группы $G_n(K)$ и $G_m(L)$ (где $G = \mathrm{GL}\,, \mathrm{SL}\,, \mathrm{PGL}\,, \mathrm{PSL}\,$, $n, m \geqslant 3$, K, L — поля характеристики 0) элементарно эквивалентны тогда и только тогда, когда $m = n$ и поля K и L элементарно эквивалентны.

Изучение этих вопросов было продолжено в 1992 году, когда с помощью конструкции ультрастепени и теоремы об изоморфизме [28] К.И. Бейдар и А.В. Михалев [81] сформулировали общий подход к проблемам элементарной эквивалентности различных алгебраических структур, и обобщили теорему Мальцева на случай, когда K и L — тела и ассоциативные кольца.

В 1998–2004 Е.И. Бунина продолжила изучать некоторые проблемы этого типа. (см. [181]–[187]). Результаты А.И. Мальцева были обобщены для унитарных линейных групп над телами и ассоциативными кольцами с инволюциями, а также для групп Шевалле над алгебраически замкнутыми полями.

В этой главе мы доказываем следующие две *основные теоремы для полей и локальных колец*:

Теорема 2.1. *Пусть $G = G_\pi(\Phi, K)$ и $G' = G_{\pi'}(\Phi', K')$ (или $E_\pi(\Phi, K)$ и $E_{\pi'}(\Phi', K')$) — две (элементарные) группы Шевалле над бесконечными полями K и K' характеристики, отличной от двух, с решетками весов Λ и Λ' соответственно. Тогда группы G и G' элементарно эквивалентны тогда и только тогда, когда системы корней Φ и Φ' изоморфны, поля K и K' элементарно эквивалентны, решетки Λ и Λ' совпадают.*

Теорема 2.2. *Пусть $G = G_\pi(\Phi, R)$ и $G' = G_{\pi'}(\Phi', R')$ (или $E_\pi(\Phi, R)$ и $E_{\pi'}(\Phi', R')$) — две (элементарные) группы Шевалле над локальными кольцами R и R' с обратимой двойкой (в случае системы корней G_2 еще и с обратимой тройкой), в одной из систем корней Φ, Φ' присутствует простая подсистема корней, отличная от A_1. Пусть решетки весов групп G и G' обозначены через Λ и Λ' соответственно. Тогда группы G и G' элементарно эквивалентны тогда и только тогда, когда системы корней Φ и Φ' изоморфны, кольца R и R' элементарно эквивалентны, решетки Λ и Λ' совпадают.*

2.1 Обратная импликация (для произвольных коммутативных колец)

Мы хотим доказать следующую теорему:

Теорема. *Пусть $G = G_\pi(\Phi, R)$ и $G' = G_{\pi'}(\Phi, R')$ (или $E_\pi(\Phi, R)$ и $E_{\pi'}(\Phi, R')$) — две (элементарные) группы Шевалле над элементарно эквивалентными локальными кольцами R и R', где представления π и π' имеют изоморфные решетки весов. Тогда группы G и G' элементарно эквивалентны.*

В книге [28] (стр. 395) доказано, что элементарная эквивалентность сохраняется при взятии прямых произведений, откуда немедленно следует

Предложение 2.1. *Если полупростая алгебра Ли $\mathcal{L} = \mathcal{L}_1 \oplus \dots \oplus \mathcal{L}_k$, где алгебры $\mathcal{L}_1, \dots, \mathcal{L}_k$ просты, R, R' — кольца, то из попарной эквивалентности (элементарных) групп Шевалле $G_{\pi|_{\mathcal{L}_1}}(\mathcal{L}_1, R)$ и $G_{\pi'|_{\mathcal{L}_1}}(\mathcal{L}_1, R')$, ..., $G_{\pi|_{\mathcal{L}_k}}(\mathcal{L}_k, R)$ и $G_{\pi'|_{\mathcal{L}_k}}(\mathcal{L}_k, R')$ следует элементарная эквивалентность (элементарных) групп Шевалле $G_\pi(\mathcal{L}, R)$ и $G_{\pi'}(\mathcal{L}, R')$.*

Таким образом, нам достаточно доказать теорему для простых алгебр Ли.

Следующая теорема верна для произвольных коммутативных колец с единицей R и R'.

Теорема 2.3. *Если две группы Шевалле $G = G_\pi(\Phi, R)$ и $G' = G_\pi(\Phi, R')$ построены с помощью одной и той же комплексной алгебры Ли типа Φ и одного и того же ее представления π, а также с помощью элементарно эквивалентных колец R и R', то $G \equiv G'$.*

Доказательство. Как мы знаем из определения группы Шевалле,

$$G = \{(a_{ij}) \in M_N(R) \mid p_1(a_{ij}) = p_2(a_{ij}) = \dots = p_m(a_{ij}) = 0\},$$
$$G' = \{(a_{ij}) \in M_N(R') \mid p_1(a_{ij}) = p_2(a_{ij}) = \dots = p_m(a_{ij}) = 0\},$$

где $p_1, p_2, \dots, p_m$ — некоторые заранее известные полиномы с целыми коэффициентами, N — некоторое заранее известное целое число.

Предположим, что мы имеем некоторое предложение φ группового языка, которое будем рассматривать на группах G и G'. Переведем его в предложение $\widetilde{\varphi}$ кольцевого языка следующим образом:

— подформула $\forall g\ \psi(g)$ переходит в подформулу

$$\forall a^g_{1,1},\dots,a^g_{N,N}(p_1(a^g_{1,1},\dots,a^g_{N,N})=0\wedge\dots\wedge p_m(a^g_{1,1},\dots,a^g_{N,N})=0\Rightarrow\widetilde{\psi}(a^g_{1,1},\dots,a^g_{N,N}));$$

— подформула $\exists g\ \psi(g)$ переходит в подформулу

$$\exists a^g_{1,1},\dots,a^g_{N,N}(p_1(a^g_{1,1},\dots,a^g_{N,N})=0\wedge\dots\wedge p_m(a^g_{1,1},\dots,a^g_{N,N})=0\wedge\widetilde{\psi}(a^g_{1,1},\dots,a^g_{N,N}));$$

— подформула $g=h$ переходит в подформулу

$$a^g_{1,1}=a^h_{1,1}\wedge\dots\wedge a^g_{N,N}=a^h_{N,N};$$

— подформула $g=h\cdot f$ переходит в подформулу

$$\bigwedge_{i,j=1}^{N}\left(a^g_{i,j}=\sum_{k=1}^{n}a^h_{i,k}\cdot a^f_{k,j}\right).$$

Очевидно, что $G(R)\vDash\varphi$ тогда и только тогда, когда $R\vDash\widetilde{\varphi}$.

Таким образом, если кольца R и R' элементарно эквивалентны, то для любого предложения φ группового языка

$$G\vDash\varphi\Leftrightarrow R\vDash\widetilde{\varphi}\Leftrightarrow R'\vDash\widetilde{\varphi}\Leftrightarrow G'\vDash\varphi.$$

Значит, $G\equiv G'$. □

Следующая теорема верна для локальных и полулокальных колец R и R' с $1/2$.

Теорема 2.4. *Если две элементарные группы Шевалле $E=E_\pi(R,\Phi)$ и $E'=E_\pi(R',\Phi)$ построены с помощью одной и той же комплексной алгебры Ли типа Φ и одного и того же ее представления π, а также с помощью элементарно эквивалентных полулокальных колец R и R' с $1/2$, то $E\equiv E'$.*

Эта теорема очевидно следует из предыдущей теоремы и предложения 2.2 следующего параграфа.

2.2 Переход к элементарной присоединенной группе

Теперь мы хотим доказать, что если две (элементарные) группы Шевалле элементарно эквивалентны, то их системы корней совпадают, а исходные кольца элементарно эквивалентны, решетки весов изоморфны.

Для удобства мы будем считать кольца бесконечными. Заметим, что это предположение ни в какой степени не ограничивает общность результата, так как в случае двух конечных колец R и R' (элементарные) группы Шевалле $G(R)$ и $G(R')$ ($E(R)$ и $E(R')$) конечны, т. е.

$$G(R) \equiv G(R') \Rightarrow G(R) \cong G(R').$$

Таким образом, мы можем сослаться на доказанные ранее результаты, которые показывают, что в этом случае $\Phi \cong \Phi'$, $R \cong R'$, т. е. $\Phi \cong \Phi'$, $R \equiv R'$.

Для начала покажем, что

Предложение 2.2. *Если две группы Шевалле G и G' элементарно эквивалентны, то их элементарные подгруппы E и E' также элементарно эквивалентны.*

Лемма 2.1. *Пусть $G = G_\pi(\Phi, R)$ — группа Шевалле, $E = E_\pi(\Phi, R)$ — ее элементарная подгруппа, R — полулокальное кольцо с $1/2$ (и $1/3$, если $\Phi \cong G_2$). Тогда $E = [G, G]$ и существует такое число N, зависящее от Φ, но не зависящее от R (и даже от представления π), что любой элемент группы E есть произведение не более чем N коммутаторов группы G.*

Доказательство. Пусть система корней Φ имеет ранг l.

Если R — это (полу)локальное кольцо, то для любого элемента $g \in E$ имеет место *разложение Гаусса* (см. [70]) $g = uhvu'$, $u, u' \in U$, $v \in V$, $h \in H$. Известно (см. [56]), что элементы u, u', v представляются в виде произведения не более чем n (количество положительных корней системы Φ) элементов $x_\alpha(t)$, а элемент h есть произведение не более чем l элементов вида $h_\alpha(t)$, которые, в свою очередь, являются произведениями не более шести элементов $x_\alpha(t)$.

Значит, каждый элемент группы $E_\pi(\Phi, R)$ есть произведение не более чем $6l + 3n$ элементов $x_\alpha(t)$, где n — количество положительных корней, зависящее от l следующим образом:

тип системы корней	ранг	n
A_l	l	$(l^2+l)/2$
B_l	l	l^2
C_l	l	l^2
D_l	l	$l^2 - l$
E_6	6	36
E_7	7	63
E_8	8	120
F_4	4	24
G_2	2	6

Осталось показать, что каждое $x_\alpha(t)$ является произведением некоторого ограниченного сверху числа коммутаторов.

Для этого следует рассмотреть типы корней по отдельности.

Именно, если рассмотреть любую систему корней $A_l, l \geqslant 2$, $D_l, l \geqslant 4$, $E_l, l = 6, 7, 8$, то в ней каждый корень входит в какую-то систему типа A_2, то есть можно считать, что $\alpha =$

$\alpha_i + \alpha_j$ для некоторых корней α_i, α_j, эти три корня образуют множество положительных корней системы A_2. В этом случае

$$[x_{\alpha_i}(t), x_{\alpha_j}(s)] = x_\alpha(\pm ts),$$

откуда любой $x_\alpha(t)$ является коммутатором.

Для систем корней $B_l, l \geqslant 2$, $C_l, l \geqslant 3$, F_4 каждый корень может рассматриваться как длинный или короткий корень системы B_2. В этой системе любой корень имеет вид

$$\pm e_1, \pm e_2 \text{ или } \pm e_1 \pm e_2.$$

Заметим, что:

1) $\pm e_1 \pm e_2 = (\pm e_1) + (\pm e_2)$ и никакая линейная комбинация корней $\pm e_1$ и $\pm e_2$ с натуральными коэффициентами, отличная от $(\pm e_1) + (\pm e_2)$, не является корнем, откуда

$$[x_{\pm e_1}(t), x_{\pm e_2}(s)] = x_{\pm e_1 \pm e_2}(\pm 2ts),$$

то есть $x_{\pm e_1 \pm e_2}(t)$ является коммутатором (так как $1/2 \in R$).

2) Имеем $\pm e_1 = (\pm e_1 - e_2) + e_2$, откуда

$$[x_{\pm e_1 - e_2}(t), x_{e_2}(s)] = x_{\pm e_1}(\pm 2ts) x_{\pm e_1 + e_2}(cts^2),$$

поэтому $x_{\pm e_1}(t)$ является произведением двух коммутаторов.

Значит, любой элемент $x_\alpha(t)$ является произведением не более чем 2 коммутаторов.

Для системы G_2 любой корень имеет вид

$$\pm(e_1 - e_2),\ \pm(e_1 - e_3),\ \pm(e_2 - e_3),$$
$$\pm(2e_1 - e_2 - e_3),\ \pm(2e_2 - e_1 - e_3),\ \pm(2e_3 - e_1 - e_2).$$

Имеем соотношения:

$$\pm(2e_1 - e_2 - e_3) = \pm(2e_2 - e_1 - e_3) + (\mp(2e_3 - e_1 - e_2)),$$
$$\pm(2e_2 - e_1 - e_3) = \pm(2e_3 - e_1 - e_2) + (\pm(2e_1 - e_2 - e_3)),$$
$$\pm(2e_3 - e_1 - e_2) = \pm(2e_1 - e_2 - e_3) + (\mp(2e_2 - e_1 - e_3)).$$

Следовательно, для любого длинного корня α элемент $x_\alpha(t)$ является коммутатором.

Далее имеем:

$$e_1 - e_2 = (e_1 - e_3) + (e_3 - e_2),$$

откуда

$$[x_{e_1 - e_3}(t), x_{e_3 - e_2}(s)] = x_{e_1 - e_2}(\pm 3ts) x_{-2e_2 + e_1 + e_3}(c_1 ts^2) x_{2e_1 - e_2 - e_3}(c_2 t^2 s).$$

Значит, при $1/3 \in R$ любой элемент $x_{e_i - e_j}(t)$ является произведением трех коммутаторов. Следовательно, любой элемент $x_\alpha(t)$ является произведением не более чем трех коммутаторов.

Отсюда мы видим, что любой элемент элементарной группы Шевалле $E_\pi(\Phi, R)$ есть произведение не более чем M коммутаторов группы $G_\pi(\Phi, R)$, где число M зависит только от системы корней Φ. $\square$

Доказательство предложения 2.

Рассмотрим множество предложений

$$Define_M := \forall x_1, \dots, x_M, y_1, \dots, y_M, z_1, \dots, z_M, t_1, \dots, t_M \\ \exists v_1, \dots, v_M, u_1, \dots, u_M \\ (([x_1, y_1] \cdot \dots \cdot [x_M, y_M]) \cdot ([z_1, t_1] \cdot \dots \cdot [z_M, t_M]) = [u_1, v_1] \cdot \dots \cdot [u_M, v_M]).$$

Каждое такое предложение утверждает, что каждый элемент коммутанта группы, на которой оно рассматривается, есть произведение не более чем M коммутаторов. Мы знаем, что для групп G и G' существует (одно и то же, так как они элементарно эквивалентны) такое M, что предложение $Define_M$ выполняется в обеих группах. В этом случае формула

$$Commut_M(x) := \exists u_1, \dots, u_M, v_1, \dots v_M (x = [u_1, v_1] \cdot \dots \cdot [u_M, v_M])$$

определяет в обеих группах G и G' подгруппы E и E' соответственно, откуда следует, что эти подгруппы элементарно эквивалентны. □

Естественно, имея две элементарно эквивалентные группы Шевалле E и E', мы также имеем две элементарно эквивалентные элементарные присоединенные группы Шевалле E_{ad} и E'_{ad}, являющиеся факторами по центру исходных групп.

В следующих параграфах мы будем рассматривать группы Шевалле над полями, доказывая теорему 2.1. Мы будем считать, что поле имеет характеристику, отличную от двух, и бесконечно (для конечных полей элементарная эквивалентность совпадает с изоморфизмом, поэтому результат будет следовать из теорем Стейнберга и Хамфриса).

2.3 Идентификация в классических случаях

Теперь мы хотим отождествить классические элементарные присоединенные группы Шевалле над полями с некоторыми подгруппами группы $\mathrm{GL}_n(K)$.

$\mathbf{A_l}$. Очевидно, что $G_{sc}(A_l, K) \cong \mathrm{SL}_{l+1}(K)$, поэтому

$$E_{sc}(A_l, K) = [G_{sc}(A_l, K), G_{sc}(A_l, K)] \cong [\mathrm{SL}_{l+1}(K), \mathrm{SL}_{l+1}(K)] = \mathrm{SL}_{l+1}(K),$$

откуда следует

$$E_{ad}(A_l, K) \cong \mathrm{PSL}_{l+1}(K).$$

$\mathbf{C_l}$. Аналогично, $G_{sc}(C_l, K) \cong \mathrm{Sp}_{2l}(K)$, $E_{sc}(C_l, K) \cong [\mathrm{Sp}_{2l}(K), \mathrm{Sp}_{2l}(K)] = \mathrm{Sp}_{2l}(K)$, откуда

$$E_{ad}(C_l, K) \cong \mathrm{PSp}_{2l}(K).$$

$\mathbf{D_l}$. Для группы $G(D_l, K)$ есть промежуточное представление π, для которого $G_\pi(D_l, K) \cong \mathrm{SO}_{2l}(K)$. При этом группа $E_\pi(D_l, K)$ порождается матрицами $E + tE_{i,j} - tE_{l+j,l+i}$ и $E + tE_{l+i,l+j} - tE_{l+j,l+i}$, где $1 \leqslant i, j \leqslant l$.

С другой стороны, мы знаем, что группы $G_\pi(D_l,K)$ и $E_\pi(D_l,K)$ "отличаются на тор", т. е. в их разложениях Брюа T меняется на H, поэтому следует изучить возможные различия мемжду ними. Группа T есть просто группа всех диагональных матриц $D = \mathrm{diag}\,[d_1,\dots,d_{2n}]$, удовлетворяющих условию $DQD^T = Q$, т. е. T состоит из матриц

$$\mathrm{diag}\,[d_1,\dots,d_l,1/d_l,\dots,1/d_1].$$

Группу H можно вычислить с помощью элементов $h_\alpha(t)$. Эти элементы имеют вид:

$$\begin{aligned}
&\mathrm{diag}\,[t_1,1/t_1,1,\dots,1,t_1,1/t_1],\\
&\mathrm{diag}\,[s_1,s_1,1,\dots,1,1/s_1,1/s_1],\\
&\mathrm{diag}\,[1,t_2,1/t_2,1,\dots,1,t_2,1/t_2],\\
&\mathrm{diag}\,[1,s_2,s_2,1,\dots,1,1/s_2,1/s_2,1],\\
&\dots,\\
&\mathrm{diag}\,[1,\dots,1,t_{n-1},1/t_{n-1},t_{n-1},1/t_{n-1},1,\dots,1],\\
&\mathrm{diag}\,[1,\dots,1,s_{n-1},s_{n-1},1/s_{n-1},1/s_{n-1},1,\dots,1].
\end{aligned}$$

Заметим, что мы можем породить $\mathrm{diag}\,[d_1,1,\dots,1,1/d_1]$ только как

$$\mathrm{diag}\,[t_1s_1,s_1/t_1,1,\dots,1,t_1/s_1,1/(t_1s_1)],$$

откуда $d_1 = t_1^2$, т. е. все зависит от того, как устроены квадраты в поле K.

Мы получаем, что группа H состоит из всех диагональных матриц

$$\mathrm{diag}\,[d_1,\dots,d_l,1/d_l,\dots,1/d_1],$$

для которых элемент $(d_1\dots d_l)$ является квадратом в K, следовательно, инволюции в группе $E_\pi(D_l,K)$ совпадают с инволюциями в $G_\pi(D_l,K)$ при $i\in K$, а при $i\notin K$ инволюции с нечетным числом -1 среди первых l элементов диагонали в этой группе отсутствуют.

Чтобы получить после этого нужную нам группу $E_{ad}(D_l,K)$, остается профакторизовать найденную $E_\pi(D_l,K)$ по центру, являющемуся тривиальным при $i\notin K$ и нечетном l, и состоящему из $\pm E_{2l}$ в остальных случаях.

$\mathbf{B_l}$. Совершенно аналогично случаю D_l в данном случае группа $E_{ad}(B_l,K)$ совпадает с $\mathrm{SO}_{2l+1}(K)$, если любой элемент в K является квадратом, и отличается на ту часть тора, которая состоит из элементов

$$\mathrm{diag}\,[d_1,\dots,d_l,1,1/d_l,\dots,1/d_1],$$

где $(d_1\dots d_l)$ не является квадратом. Соответственно, при $i\notin K$ пропадают инволюции с нечетным числом -1 среди первых l элементов.

2.4 Изучение инволюций для классических групп Шевалле

Нас будет интересовать, как устроены инволюции (элемента порядка два) в рассматриваемых группах Шевалле. Сначала мы рассмотрим классические группы Шевалле.

2.4.1 Изучение инволюций для группы $PSL_n(K)$

Естественно, любая инволюция в группе $PSL_n(K)$ либо происходит из инволюции $SL_n(K)$ (*инволюция первого рода*), либо происходит из такой матрицы $A \in SL_n(K)$, что $A^2 = \lambda E$ (*инволюция второго рода*).

Сначала рассмотрим инволюции первого рода. Инволюции из $SL_n(K)$ имеют в некотором базисе вид

$$\operatorname{diag}[\underbrace{-1,\dots,-1}_{k},\underbrace{1,\dots,1}_{n-k}],$$

k четно. При четном n инволюции

$$\operatorname{diag}[\underbrace{-1,\dots,-1}_{k},\underbrace{1,\dots,1}_{n-k}]$$

и

$$\operatorname{diag}[\underbrace{-1,\dots,-1}_{n-k},\underbrace{1,\dots,1}_{k}]$$

равны в группе $PSL_n(K)$.

Для каждого четного k любые инволюции с одинаковым k сопряжены, т.е. для четного n существует $[n/4]$ классов сопряженности инволюций первого рода, а для нечетного n — $[n/2]$ классов сопряженности.

Централизатор инволюции первого рода (при $2k \neq n$) состоит из блоков

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, \quad A \in GL_k(K),\ B \in GL_{n-k}(K),\ \det A \cdot \det B = 1.$$

Его центр состоит из матриц вида

$$\operatorname{diag}[\underbrace{a,\dots,a}_{k}\underbrace{b,\dots,b}_{n-k}], \quad a^k \cdot b^{n-k} = 1.$$

Покажем, что таких матриц бесконечно много. Если НОД$(k, n-k) \neq 1$, то заменим k и $n-k$ на $k' = k/$НОД$(k, n-k)$ и $l = (n-k)' = (n-k)/$НОД$(k, n-k)$. Тогда нам нужно будет доказать, что решений равенства $a^{k'}b^l = 1$ бесконечно много. Для любого $\xi \in K^*$ элементы $a = \xi^{ml}$ и $b = \frac{1}{\xi^{mk'}}$ при $m > 0$ удовлетворяют условию, поэтому нужно только убедиться, что получается бесконечно много пар (a, b). Для $\operatorname{char} K = 0$ это очевидно. Пусть $\operatorname{char} K \neq 0$. В любом случае либо l, либо k взаимно просто с $p = \operatorname{char} K$. Пусть это l. Очевидно, что, варьируя ξ и m (причем ξ бесконечно много), мы получим бесконечно много различных a.

Значит, если $2k \neq n$, то центр централизатора инволюции первого рода обязательно бесконечен. Его коммутант состоит из матриц

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, \quad A \in \mathrm{SL}_k(K), B \in \mathrm{SL}_{n-k}(K),$$

профакторизованных по центру, а фактор этого коммутанта по центру есть прямое произведение

$$\mathrm{PSL}_k(K)\times \mathrm{PSL}_{n-k}(K).$$

Пусть теперь $2k=n$, т.е. наша инволюция в некотором базисе имеет вид $\mathrm{diag}\,[-E_k,E_k]$. Естественно, в этом случае k четно.

Централизатор этой инволюции состоит из матриц вида

$$\begin{pmatrix} A & 0\\ 0 & B\end{pmatrix}\quad A,B\in \mathrm{GL}_k(K), \det A\cdot\det B=1,$$

а также из матриц

$$\begin{pmatrix} 0 & C\\ D & 0\end{pmatrix},\quad C,D\in \mathrm{GL}_k(K),\ \det C\cdot\det D=1.$$

У этого централизатора центр конечен и имеет порядок 2. Его коммутант состоит из матриц

$$\begin{pmatrix} A & 0\\ 0 & B\end{pmatrix}\quad A,B\in \mathrm{SL}_k(K),$$

а фактор коммутанта по центру есть

$$\mathrm{PSL}_k(K)\times \mathrm{PSL}_k(K).$$

Теперь перейдем к инволюциям второго рода.

Пусть мы имеем некоторую полуинволюцию в группе $\mathrm{SL}_n(K)$, т.е. матрицу A, для которой $A^2=\lambda E$. Так как $\mathrm{char}\, K\neq 2$, то матрица A должна быть диагонализируема (в $\overline{K}$), а значит, ее собственные значения равны $\pm\sqrt{\lambda}$. При этом $\lambda^n=1$.

Здесь могут появиться различные случаи:

1) $\sqrt{\lambda}\in K$ и $\sqrt{\lambda}^n=1$. Такая полуинволюция совпадает с обычной инволюцией в $\mathrm{PSL}_n(K)$.

2) $\sqrt{\lambda}\in K$ и $\sqrt{\lambda}^n=-1$. Если n нечетно, то мы можем положить $\lambda'=\sqrt{\lambda}$ и прийти к случаю 1). Поэтому будем считать, что n четно. В этом случае появляются инволюции вида

$$\mathrm{diag}\,[\underbrace{-\sqrt{\lambda},\dots,-\sqrt{\lambda}}_{k},\underbrace{\sqrt{\lambda},\dots,\sqrt{\lambda}}_{n-k}],$$

k нечетно. Классов сопряженности таких инволюций появляется еще $[n/4]$.

Централизатор такой $(k,n-k)$-инволюции состоит из матриц

$$\begin{pmatrix} A & 0\\ 0 & B\end{pmatrix}\quad A\in \mathrm{GL}_k(K), B\in \mathrm{GL}_{n-k}(K), \det A\cdot\det B=1,$$

а при нечетном $k=n/2$ еще добавляются матрицы

$$\begin{pmatrix} 0 & C\\ D & 0\end{pmatrix}\quad C,D\in \mathrm{GL}_k(K), \det C\cdot\det D=-1.$$

Во всех случаях, кроме последнего, центр централизатора бесконечен, фактор коммутанта централизатора по центру есть

$$\mathrm{PSL}_k(K) \times \mathrm{PSL}_{n-k}(K),$$

если $k = 1$, то это просто $\mathrm{PSL}_{n-1}(K)$.

3) $\sqrt{\lambda} \notin K$, но при этом $\lambda \in K$. Заметим, что тогда собственных значений $+\sqrt{\lambda}$ и $-\sqrt{\lambda}$ должно быть поровну, так как $tr\, A \in K$. При этом $(-\lambda)^{n/2} = 1$.

Матрица

$$\begin{pmatrix} 0 & \lambda & & & & & \\ 1 & 0 & & & & & \\ & & 0 & \lambda & & & \\ & & 1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & \lambda \\ & & & & & 1 & 0 \end{pmatrix}$$

представляет такую инволюцию. Еще ее можно записать в виде

$$\begin{pmatrix} 0 & \lambda E \\ E & 0 \end{pmatrix}.$$

2.4.2 Изучение инволюций для групп типа C_l

Так как центр группы $\mathrm{Sp}_{2l}(K)$ состоит из двух элементов $\pm E$, то инволюции группы $\mathrm{PSp}_{2l}(K)$ — это элементы $\widetilde{A}$ такие, что $A^2 = E$ (первый тип) и элементы $\widetilde{A}$ такие, что $A^2 = -E$ (второй тип).

Сначала рассмотрим инволюции первого типа: в некотором базисе инволюция A имеет вид

$$\begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix},$$

в этом базисе форма Q принимает вид

$$Q_A = \begin{pmatrix} Q_1 & Q_2 \\ -Q_2^T & Q_3 \end{pmatrix}$$

Тогда из соотношения $AQ_AA^T = Q_A$ следует

$$\begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix} \begin{pmatrix} Q_1 & Q_2 \\ -Q_2^T & Q_3 \end{pmatrix} \begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix} = \begin{pmatrix} Q_1 & Q_2 \\ -Q_2^T & Q_3 \end{pmatrix} \Rightarrow$$

$$\begin{pmatrix} Q_1 & -Q_2 \\ Q_2^T & Q_3 \end{pmatrix} = \begin{pmatrix} Q_1 & Q_2 \\ -Q_2^T & Q_3 \end{pmatrix} \Rightarrow Q_2 = 0.$$

Значит, Q_1 и Q_3 — невырожденные кососимметрические матрицы, т.е. имеют четную размерность.

Очевидно, что для любого четного $k \leqslant l$ $(2k, 2(l-k))$-инволюции первого типа присутствуют в группе $\mathrm{PSp}_{2l}(K)$, так как можно взять матрицы

$$\mathrm{diag}\,[\underbrace{-1,\dots,-1}_{k},\underbrace{1,\dots,1}_{2(l-k)},\underbrace{-1,\dots,-1}_{k}].$$

Централизатор такой инволюции состоит из матриц

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, \quad A \in \mathrm{Sp}_{2k}(K), B \in \mathrm{Sp}_{2(l-k)}(K), \text{ или } A \in \mathrm{Sp}^-_{2k}(K), B \in \mathrm{Sp}^-_{2(l-k)}(K)$$

при $2k \neq l$.

Его центр конечен и состоит из двух элементов.

Коммутант централизатора состоит из матриц

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \quad A \in \mathrm{Sp}_{2k}(K), B \in \mathrm{Sp}_{2(l-k)}(K),$$

а фактор по центру коммутанта централизатора есть

$$\mathrm{PSp}_{2k}(K) \times \mathrm{PSp}_{2(l-k)}(K).$$

Исключение могут составить случаи малых k: при $k = 1$

$$\mathrm{Sp}_2(K) \cong \mathrm{SL}_2(K),$$

т.е. получается группа

$$\mathrm{PSL}_2(K) \times \mathrm{PSp}_{2l-2}(K).$$

Теперь посмотрим, что происходит при $2k = l$.

Пусть $Q_{2l} = \mathrm{diag}\,[Q_l, Q_l]$, $I = \mathrm{diag}\,[E_l, -E_l]$. Может появиться соотношение

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} E_l & 0 \\ 0 & -E_l \end{pmatrix} = \begin{pmatrix} -E_l & 0 \\ 0 & E_l \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

откуда $A = D = 0$, т.е. централизатор состоит из матриц

$$\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}, \quad A, D \in \mathrm{Sp}_{l=2k}(K)$$

и

$$\begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix}, \quad B, C, \in \mathrm{Sp}_{2k}(K).$$

Его центр состоит из двух элементов, а коммутант состоит из матриц

$$\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}, \quad A, D \in \mathrm{Sp}_{2k}(K).$$

Перейдем к инволюциям второго типа. Так как $A^2 = -E$, то в поле $\overline{K}$ инволюция A диагонализируема с собственными значениями $\pm i$:

$$\widetilde{A} = \begin{pmatrix} iE_k & 0 \\ 0 & -iE_{2l-k} \end{pmatrix},$$

при этом форма Q имеет в этом базисе вид

$$Q_A = \begin{pmatrix} Q_1 & Q_2 \\ -Q_2^T & Q_3 \end{pmatrix}.$$

Из соотношения

$$\begin{pmatrix} iE_k & 0 \\ 0 & -iE_{2l-k} \end{pmatrix} \begin{pmatrix} Q_1 & Q_2 \\ -Q_2^T & Q_3 \end{pmatrix} \begin{pmatrix} iE_k & 0 \\ 0 & -iE_{2l-k} \end{pmatrix} = \begin{pmatrix} Q_1 & Q_2 \\ -Q_2^T & Q_3 \end{pmatrix}$$

следует $Q_1 = Q_3 = 0$, откуда $k = l$.

Значит,

$$\widetilde{A} = \begin{pmatrix} iE_l & 0 \\ 0 & -iE_l \end{pmatrix}, \; Q_A = \begin{pmatrix} 0 & Q_2 \\ -Q_2^T & 0 \end{pmatrix}.$$

Независимо от того, $i \in K$ или нет, такие инволюции есть в группе $\mathrm{PSp}_{2l}(K)$, именно, это, например, инволюция

$$A = Q = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}.$$

Чтобы легко найти централизатор такой инволюции, рассмотрим (если понадобится, то в $\overline{K}$) сопряженную инволюцию

$$I = \begin{pmatrix} iE & 0 \\ 0 & -iE \end{pmatrix},$$

форма Q имеет вид

$$\begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}.$$

Пусть мы имеем матрицу

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Тогда возможно два варианта:

1) $MI = IM$ в $\mathrm{Sp}_{2l}(K)$, откуда $B = C = 0$, следовательно, $AD^T = E$. Значит,

$$M = \begin{pmatrix} A & 0 \\ 0 & (A^T)^{-1} \end{pmatrix}, \quad A \in \mathrm{GL}_l(K).$$

2) $MI = -IM$ в $\mathrm{Sp}_{2l}(K)$, откуда $A = D = 0$, следовательно, $BC^T = -E$. Значит,

$$M = \begin{pmatrix} 0 & B \\ -(B^T)^{-1} & 0 \end{pmatrix}, \quad B \in \mathrm{GL}_l(K).$$

Если l нечетно, то матрицы второго вида имеют определитель 1, т.е. лежат в нашей группе, откуда следует, что центр централизатора в этом случае состоит из двух элементов. Если l четно, то матрицы второго вида имеют определитель -1, т.е. не лежат в нашей группе, откуда следует, что центр централизатора бесконечен.

Коммутант в обоих случаях имеет вид

$$\begin{pmatrix} A & 0 \\ 0 & (A^T)^{-1} \end{pmatrix}, \quad A \in \mathrm{SL}_l(K).$$

Фактор по центру коммутанта изоморфен $\mathrm{PSL}_l(K)$.

2.4.3 Изучение инволюций в группах типа B_l

Как мы уже показали, для случая $E_{\mathrm{ad}}(B_l, K)$ существенно различными являются ситуации $i \in K$ и $i \notin K$. Рассмотрим их по отдельности.

1) $i \in K$. Так как $E_{\mathrm{ad}}(B_l, K)$ является подгруппой $\mathrm{SO}_{2l+1}(K)$, то все инволюции в $E_{\mathrm{ad}}(B_l, K)$ являются инволюциями первого рода. Если $i \in K$, то все инволюции группы $\mathrm{SO}_{2l+1}(K)$ содержатся в $E_{\mathrm{ad}}(B_l, K)$, поэтому нам надо изучить именно эти инволюции. Инволюции группы $\mathrm{SO}_{2l+1}(K)$, очевидно, имеют в некотором базисе вид

$$\mathrm{diag}\,[\underbrace{-1, \dots, -1}_{2k}, \underbrace{1, \dots, 1}_{2l-2k+1}],$$

их ровно l классов сопряженности. Централизатор такой инволюции состоит из матриц

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, \quad A \in \mathrm{EO}_{2k}(K), B \in \mathrm{EO}_{2l-2k+1}(K)$$

или

$$A \in \mathrm{O}^-_{2k}(K), B \in \mathrm{O}^-_{2l-2k+1}(K).$$

Если $2k = 2l$, то мы имеем матрицы

$$\begin{pmatrix} A & 0 \\ 0 & \pm 1 \end{pmatrix}, \quad A \in \mathrm{O}_{2l}(K).$$

Если $k = 1$, то получаем матрицы

$$\begin{pmatrix} a & 0 & 0 \\ 0 & 1/a & 0 \\ 0 & 0 & B \end{pmatrix}, \quad B \in \mathrm{SO}_{2l-1}(K)$$

и

$$\begin{pmatrix} 0 & a & 0 \\ 1/a & 0 & 0 \\ 0 & 0 & B \end{pmatrix}, \quad B \in \mathrm{O}^-_{2l-1}(K).$$

Центр этого централизатора имеет порядок два, как и все остальные центры централизаторов. Факторы по центру коммутантов централизаторов изоморфны

$$\mathrm{EO}_{2l-1}(K),\ \mathrm{PEO}_4(K)\times \mathrm{EO}_{2l-3}(K)\ldots,\ \mathrm{PEO}_{2l-2}(K)\times \mathrm{EO}_3(K),\ \mathrm{PEO}_{2l}(K).$$

2) $i\notin K$. Как мы уже показывали, из $E_{\mathrm{ad}}(B_l,K)$ исчезнут те инволюции $\mathrm{SO}_{2l+1}(K)$, у которых $2(2i+1)$ минус единиц на диагонали. Таким образом, останутся инволюции

$$\mathrm{diag}\,[-1,-1,-1,-1,1,\ldots,1],\ldots,\ \mathrm{diag}\,[\underbrace{-1,\ldots,-1}_{4k},1,\ldots,1],\ldots.$$

Очевидно, что центры их централизаторов будут также состоять из 2 элементов, а факторы по центру коммутантов централизаторов имеют вид

$$\mathrm{PEO}_4(K)\times \mathrm{EO}_{2l-3}(K),\ldots,\ \mathrm{PEO}_{2l-2}(K)\times \mathrm{EO}_3(K)\text{ либо }\mathrm{PEO}_{2l}(K).$$

2.4.4 Изучение инволюций для групп типа D_l $(l\geqslant 4)$

В данном случае, как и в предыдущем, различными являются ситуации $i\in K$ и $i\notin K$.

1) $i\in K$. Сначала рассмотрим инволюции первого рода. Это инволюции группы $\mathrm{PSO}_{2l}(K)$, прообразы которых являются инволюциями в $\mathrm{SO}_{2l}(K)$. Если $i\in K$, то все инволюции группы $\mathrm{SO}_{2l}(K)$ содержатся в $\mathrm{EO}_{2l}(K)$, поэтому все инволюции первого рода группы содержатся в $\mathrm{PEO}_{2l}(K)$. Очевидно, что инволюции группы $\mathrm{SO}_{2l}(K)$ в некотором базисе имеют вид

$$\mathrm{diag}\,[\underbrace{-1,\ldots,-1}_{2k},\underbrace{1,\ldots,1}_{2(l-k)}],$$

их $[l/2]$ классов сопряженности.

При $2k=l$ централизатор такой инволюции состоит из матриц

$$\begin{pmatrix}A&0\\0&B\end{pmatrix},\quad A\in \mathrm{EO}_{2k}(K),\ B\in \mathrm{EO}_{2(l-k)}(K).$$

Его центр состоит из 2 элементов: $-E$ и самой инволюции. Фактор по центру коммутанта централизатора есть

$$\mathrm{PEO}_{2k}(K)\times \mathrm{PEO}_{2(l-k)}(K).$$

Исключение могут составить случаи малых k: при $k=1$

$$\mathrm{PEO}_2(K)\times \mathrm{PEO}_{2(l-1)}(K)\cong \mathrm{PEO}_{2(l-1)}(K).$$

Заметим, кроме того, что тип D_2 совпадает с $A_1\times A_1$, а тип D_3 — с A_3.

Теперь посмотрим, что происходит при $2k=l$. Естественно, k четно. Пусть

$$Q_{2l}=\begin{pmatrix}Q_l&0\\0&Q_l\end{pmatrix},\quad I=\begin{pmatrix}E_l&0\\0&-E_l\end{pmatrix}.$$

Тогда может добавиться соотношение

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} E_l & 0 \\ 0 & -E_l \end{pmatrix} = \begin{pmatrix} -E_l & 0 \\ 0 & E_l \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \Rightarrow A = D = 0,$$

т.е. весь централизатор состоит из матриц

$$\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}, \quad A, D \in \mathrm{SO}_k(K) \text{ или } A, D \in \mathrm{O}^-(K)$$
$$\begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix} \quad B, C \in \mathrm{SO}_k(K) \text{ или } B, C \in \mathrm{O}_k^-(K).$$

Его центр состоит из двух элементов, а коммутант состоит из матриц

$$\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}, \quad A, D \in \mathrm{EO}_k(K).$$

Теперь перейдем к инволюциям второго типа. Так как $A^2 = -E$, то в поле K $(i \in K)$ инволюция A диагонализируется с собственными значениями $\pm i$, матрица A приводится к виду

$$\widetilde{A} = \begin{pmatrix} iE_k & 0 \\ 0 & -iE_{2l-k} \end{pmatrix},$$

при этом форма Q имеет в этом базисе вид

$$Q_A = \begin{pmatrix} Q_1 & Q_2 \\ Q_2^T & Q_3 \end{pmatrix}.$$

Имеем

$$\begin{pmatrix} iE_k & 0 \\ 0 & -iE_{2l-k} \end{pmatrix} \begin{pmatrix} Q_1 & Q_2 \\ Q_2^T & Q_3 \end{pmatrix} \begin{pmatrix} iE_k & 0 \\ 0 & -iE_{2l-k} \end{pmatrix} = \begin{pmatrix} Q_1 & Q_2 \\ Q_2^T & Q_3 \end{pmatrix},$$

откуда $Q_1 = Q_3 = 0$, т.е. $k = l$. Значит,

$$\widetilde{A} = \begin{pmatrix} iE_l & 0 \\ 0 & -iE_l \end{pmatrix}, \quad Q_A = \begin{pmatrix} 0 & Q_2 \\ Q_2^T & 0 \end{pmatrix}.$$

Например,

$$Q_A = \begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix}.$$

Централизатор матрицы $\widetilde{A}$ состоит из двух множеств:

1)

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} iE & 0 \\ 0 & -iE \end{pmatrix} = \begin{pmatrix} iE & 0 \\ 0 & -iE \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \Rightarrow B = C = 0 \Rightarrow$$
$$\Rightarrow AD^T = E \Rightarrow D = (A^T)^{-1}, A \in \mathrm{GL}_l(K).$$

2)

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} iE & 0 \\ 0 & -iE \end{pmatrix} = -\begin{pmatrix} iE & 0 \\ 0 & -iE \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \Rightarrow A = D = 0 \Rightarrow$$
$$\Rightarrow CB^T = E \Rightarrow C = (B^T)^{-1}, B \in \mathrm{GL}_l(K).$$

Если l четно, то матрицы второго вида имеют определитель 1, откуда следует, что они лежат в нашей группе, то есть центр централизатора состоит их двух элементов. Если l нечетно, то матрицы второго вида имеют определитель -1, то есть не лежат в нашей группе, откуда следует, что центр централизатора бесконечен.

Фактор по центру коммутанта централизатора в любом случае есть группа $\mathrm{PSL}_l(K)$.

2) $i \notin K$. Как мы помним, в этом случае количество несопряженных между собой инволюций первого рода в группе резко уменьшается. Именно, из $E_{\mathrm{ad}}(D_l, K)$ исчезнут те инволюции $\mathrm{SO}_{2l}(K)$, у которых $2(2j+1)$ минус единиц на диагонали. Таким образом, останутся инволюции

$$\mathrm{diag}\,[-1,-1,-1,-1,1,\dots,1],\dots,\ \mathrm{diag}\,[\underbrace{-1,\dots,-1}_{4k},1,\dots,1],\dots$$

Очевидно, что центры их централизаторов будут также состоять из двух элементов, а факторы по центру коммутантов централизаторов будут иметь вид

$$\mathrm{PEO}_4(K) \times \mathrm{PEO}_{2l-4}(K),\dots,$$
$$\mathrm{PEO}_{2l-2}(K) \times \mathrm{PEO}_2(K) \text{ либо } \mathrm{PEO}_{2l-4}(K) \times \mathrm{PEO}_4(K).$$

В случае нечетного l все инволюции первого рода остаются, а в случае четного l половина классов инволюций пропадает.

Если l нечетно, то пропадает инволюция второго рода, сопряженная к

$$\begin{pmatrix} iE_l & 0 \\ 0 & -iE_l \end{pmatrix}.$$

Если l четно, то такая инволюция есть, например, это

$$A = \begin{pmatrix} 0 & 1 & & & \\ -1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 \\ & & & -1 & 0 \end{pmatrix}$$

при

$$Q_A = \begin{pmatrix} 0 & E_l \\ E_l & 0 \end{pmatrix}.$$

2.5 Формулы, различающие разные классические группы Шевалле

В этом параграфе мы покажем, что для любых двух классических групп Шевалле с неизоморфными системами корней существует предложение первого порядка, истинное в одной группе и ложное во второй.

Лемма 2.2. *Существует предложение φ_{A_1} первого порядка, истинное в любой присоединенной группе типа A_1 и ложное во всех присоединенных группах Шевалле других классических типов.*

Доказательство. В группе $\mathrm{PSL}_2(K)$ есть всего 1 класс сопряженности инволюций: это инволюции, сопряженные к матрице
$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Централизатор такой инволюции состоит из матриц
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \quad a^2+b^2=1,$$
и
$$\begin{pmatrix} a & b \\ b & -a \end{pmatrix}, \quad -a^2-b^2=1.$$
Коммутант централизатора состоит из матриц
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \quad a^2+b^2=1,$$
то есть коммутативен.

Посмотрим, существуют ли другие группы Шевалле, удовлетворяющие этому условию: так как у нас всего один класс сопряженности инволюций, то нужно рассматривать лишь малые размерности.

A_2 — это группа $\mathrm{PSL}_3(K)$, в которой имеется инволюция
$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$
ее централизатор изоморфен $\mathrm{GL}_2(K)$, то есть не удовлетворяет тому условию, что его коммутант коммутативен.

A_3 — это группа $\mathrm{PSL}_4(K)$, в ней по крайней имеется инволюция $\mathrm{diag}\,[-1,-1,1,1]$, коммутант централизатора которой есть центральное произведение $\mathrm{SL}_2(K)$ на $\mathrm{SL}_2(K)$. Естественно, он также не коммутативен.

В группах A_l при $l \geqslant 4$ есть по крайней мере два класса сопряженности инволюций, поэтому эти случаи нам не нужно рассматривать.

C_3 — это группа $\mathrm{PSp}_6(K)$. Для инволюции $\mathrm{diag}\,[-1,-1,1,1,1,1]$ коммутант централизатора точно не коммутативен.

Для групп типа C_l при $l \geqslant 4$ точно есть по крайнем мере две несопряженные инволюции, поэтому эти типы мы тоже не будем рассматривать.

B_2 — это группа $\mathrm{EO}_5(K)$, в ней точно имеется инволюция

$$\mathrm{diag}\,[-1,-1,-1,-1,1],$$

коммутант централизатора которой есть $\mathrm{EO}_4(K)$, эта группа не коммутативна. Тем более не коммутативен коммутант централизатора инволюции в группах типа B_l при $l \geqslant 3$.

D_4 — это группа $\mathrm{PEO}_8(K)$, в которой точно имеется инволюция $\mathrm{diag}\,[-1,-1,-1,-1,1,1,1,1]$, ее коммутант централизатора также не коммутативен.

Значит, мы можем предъявить предложение, отличающее группу $\mathrm{PSL}_2(K)$ от всех других классических групп:

$$\begin{gathered}\varphi_{A_1} := \forall M_1 \forall M_2 (M_1^2 = M^2 = 1 \wedge M_1 \neq 1 \wedge M_2 \neq 1 \Rightarrow \\ \Rightarrow \exists X (X M_1 X^{-1} = M_2)) \wedge \forall X_1 \forall X_2 (\exists Y_1 \exists Y_2 \exists Z_1 \exists Z_2 \exists M (M^2 = 1 \wedge \\ M \neq 1 \wedge Y_1 M = M Y_1 \wedge Y_2 M = M Y_2 \wedge Z_1 M = M Z_1 \wedge Z_2 M = M Z_2 \wedge \\ X_1 = Y_1 Z_1 Y_1^{-1} Z_1^{-1} \wedge X_2 = Y_2 Z_2 Y_2^{-1} Z_2^{-1}) \Rightarrow X_1 X_2 = X_2 X_1).\end{gathered}$$

□

Заметим, что если в некоторой группе Шевалле есть формульное подмножество $\mathcal{N}$, само являющееся классической группой Шевалле, то можно написать формулу, утверждающую, что оно изоморфно группе $\mathrm{PSL}_2(K)$.

Эта формула выглядит следующим образом:

$$\begin{gathered}\varphi_{A_1}^{\mathcal{N}} := \forall M_1 \in \mathcal{N} \forall M_2 \in \mathcal{N} (M_1^2 = M^2 = 1 \wedge M_1 \neq 1 \wedge M_2 \neq 1 \Rightarrow \\ \Rightarrow \exists X \in \mathcal{N} (X M_1 X^{-1} = M_2)) \wedge \\ \wedge \forall X_1 \in \mathcal{N} \forall X_2 \in \mathcal{N} (\exists Y_1 \in \mathcal{N} \exists Y_2 \in \mathcal{N} \exists Z_1 \in \mathcal{N} \exists Z_2 \in \mathcal{N} \exists M \in \mathcal{N} (M^2 = 1 \wedge \\ M \neq 1 \wedge Y_1 M = M Y_1 \wedge Y_2 M = M Y_2 \wedge Z_1 M = M Z_1 \wedge Z_2 M = M Z_2 \wedge \\ X_1 = Y_1 Z_1 Y_1^{-1} Z_1^{-1} \wedge X_2 = Y_2 Z_2 Y_2^{-1} Z_2^{-1}) \Rightarrow \\ \Rightarrow X_1 X_2 = X_2 X_1).\end{gathered}$$

Лемма 2.3. *Существует предложение φ_{A_2} первого порядка, истинное в любой присоединенной группе типа A_2 и ложное во всех присоединенных группах Шевалле других классических типов.*

Доказательство. Эта группа характеризуется тем, что

1) у нее есть всего один класс сопряженности инволюций;

2) централизатор любой инволюции имеет бесконечный центр;

3) фактор по центру коммутанта централизатора любой инволюции есть группа $\mathrm{PSL}_2(K)$, т.е. группа, удовлетворяющая предложению φ_{A_1}.

Очевидно, что эти три условия полностью характеризуют группу $\mathrm{PSL}_3(K)$. □

Лемма 2.4. *Существует предложение φ_{A_3} первого порядка, истинное в любой присоединенной группе типа A_3 и ложное во всех присоединенных группах Шевалле других классических типов, исключая тип B_2.*

Доказательство. Мы имеем группу $\mathrm{PSL}_4(K)$.

В этом случае количество классов сопряженности инволюций зависит от базисного поля, но точно существует инволюция, фактор по центру коммутанта централизатора которой есть группа $\mathrm{PSL}_2(K)\times \mathrm{PSL}_2(K)$, т.е. такая группа, что существуют матрицы X_1, X_2, Y_1, Y_2 (например,

$$\left(\begin{pmatrix}1&1&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}, \begin{pmatrix}2&0&0&0\\0&1/2&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}, \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&1\\0&0&0&1\end{pmatrix}, \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&2&0\\0&0&0&1/2\end{pmatrix}\right),$$

что $X_1Y_1 = Y_1X_1$, $X_1Y_2 = Y_2X_1$, $X_2Y_1 = Y_1X_2$, $X_2Y_2 = Y_2X_2$, централизатор множества $\{X_1, X_2\}$ удовлетворяет формуле φ_{A_1}, централизатор множества $\{Y_1, Y_2\}$ удовлетворяет формуле φ_{A_1}, эти централизаторы коммутируют, любой элемент фактора по центру коммутанта централизатора инволюции представляется в виде произведения элемента из первого централизатора на элемент второго.

Очевидно, что у групп типа A_l нет больше представителей, у которых фактор по центру коммутанта централизатора какой-то инволюции есть $\mathrm{PSL}_2(K)\times \mathrm{PSL}_2(K)$.

В случае типа C_l у группы типа C_3, т.е. группы $\mathrm{PSp}_6(K)$ у инволюции $\mathrm{diag}\,[-1,-1,1,\dots,1]$ фактор по центру коммутанта централизатора изоморфен $\mathrm{PSL}_2(K)\times \mathrm{PSp}_4(K)$, что не элементарно эквивалентно $\mathrm{PSL}_2(K)\times \mathrm{PSL}_2(K)$, а у инволюции $\mathrm{diag}\,[i,i,i,-i,-i,-i]$ фактор по центру коммутанта централизатора есть $\mathrm{PSL}_3(K)$, что тоже не может быть элементарно эквивалентно $\mathrm{PSL}_2(K)\times \mathrm{PSL}_2(K)$.

Очевидно, что ситуацию $l > 3$ можно даже не рассматривать, так как там будут получаться произведения групп бóльших размерностей.

В случае типа D_l стоит рассмотреть только группу типа D_4 — $\mathrm{PEO}_8(K)$.

У инволюции $\mathrm{diag}\,[-1,-1,1,\dots,1]$ этой группы фактор по центру коммутанта централизатора есть $\mathrm{PEO}_6(K)$ что не элементарно эквивалентно $\mathrm{PSL}_2(K)\times \mathrm{PSL}_2(K)$. У инволюции $\mathrm{diag}\,[-1,-1,-1,-1,1,1,1,1]$ фактор по центру коммутанта централизатора есть $\mathrm{PEO}_4(K)\times \mathrm{PEO}_4(K)$, что не может быть элементарно эквивалентно $\mathrm{PSL}_2(K)\times \mathrm{PSL}_2(K)$. У инволюции $\mathrm{diag}\,[i,i,i,i,-i,-i,-i,-i]$ фактор по центру коммутанта централизатора есть $\mathrm{PSL}_4(K)$, что тоже нам не подходит.

Очевидно, что для группы типа B_l, $l \geqslant 3$, т.е. группы $\mathrm{EO}_{2l+1}(K)$, ни для какой инволюции фактор по центру коммутанта ее централизатора не может быть элементарно эквивалентен $\mathrm{PSL}_2(K)\times \mathrm{PSL}_2(K)$. □

Нам осталось рассмотреть группу типа B_2, т.е. группу $\mathrm{EO}_5(K)$, в которой точно есть только инволюция $\mathrm{diag}\,[-1,-1,-1,-1,1]$, фактор по центру коммутанта централизатора которой есть группа $\mathrm{PEO}_4(K)$, которая в принципе может быть элементарно эквивалентна $\mathrm{PSL}_2(K)\times \mathrm{PSL}_2(K)$, поэтому группы типов A_3 и B_2 нужно различать дополнительными предложениями.

Лемма 2.5. *Существует предложение $\varphi_{A_3-B_2}$ первого порядка, истинное в любой присоединенной группе типа A_3 и ложное во всех присоединенных группах Шевалле типа B_2.*

Доказательство. Очевидно, что если инволюции, на которых группы $G(A_3)$ и $G(B_2)$ не различаются, — это не единственные инволюции в этих группах, то мы легко можем различить эти группы. Поэтому нам нужно только рассмотреть тот случай, когда это единственные (с точностью до сопряжения) инволюции.

Рассмотрим матрицу M, удовлетворяющую следующей формуле:

$$\begin{aligned}DDiag_2(M) := \exists I(I^2 = 1 \land I \neq 1 \land \exists M_1 \exists M_2(M_1 I = I M_1 \land \\ \land M_2 I = I M_2 \land M = M_1 M_2 M_1^{-1} M_2^{-1} \land \\ \land \forall X \forall Y (XM = MY \land YM = MY \Rightarrow XY = YX) \land \\ \land \forall N \forall X (NI = IN \land NM = MN \land (XI = IX \land M = XNX^{-1}) \Rightarrow X^2 M = M X^2)).\end{aligned}$$

Эта формула утверждает, что существует инволюция I такая, что

1) M лежит в коммутанте ее централизатора;

2) любые матрицы, коммутирующие с M, коммутируют друг с другом;

3) для любой матрицы N, коммутирующей с M и I и сопряженной к M с помощью матрицы X, коммутирующей с I, выполняется условие $X^2 M = M X^2$.

Посмотрим, какие матрицы удовлетворяют формуле $DDiag_2(M)$ в группе $G(A_3) = \mathrm{PSL}_4(K)$.

Инволюция I имеет в некотором базисе вид $\mathrm{diag}\,[\xi, \xi, -\xi, -\xi]$, $\xi^4 = 1$. Значит, в этом базисе матрица M имеет вид

$$M = \begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & f & e \\ 0 & 0 & g & h \end{pmatrix}.$$

Вторая часть формула в данном случае означает всего лишь, что у матрицы M нет жордановых клеток с совпадающими собственными значениями. Значит, каждая из клеток

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ и } \begin{pmatrix} f & e \\ g & h \end{pmatrix}$$

либо диагонализируема в K^* с разными собственными значениями, либо есть жорданова клетка размера 2×2.

Пусть $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ — это жорданова клетка $\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$. Выберем

$$N = \begin{pmatrix} \alpha & 2 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Эти матрицы противоречат третьей части формулы $DDiag_2(M)$.

Значит, обе клетки должны быть диагонализируемы. При этом все собственные значения различны. Значит, в группе $\mathrm{PSL}_4(K)$ формула $DDiag_2(M)$ выделяет диагонализируемые в $\overline{K}$ матрицы с разными элементами на диагонали, и только их.

Теперь посмотрим, какие матрицы удовлетворяют этой формуле в группе $G(B_2) = \mathrm{EO}_5(K)$. Инволюция I должна иметь вид $\mathrm{diag}\,[-1,-1,-1,-1,1]$ в базисе, в котором форма имеет вид

$$\begin{pmatrix} Q_1 & 0 \\ 0 & q_2 \end{pmatrix}, \quad Q_1 \in \mathrm{GL}_4(K),\ Q_1^T = Q_1,\ q_2 \in K^*.$$

Значит, матрица M имеет вид

$$\begin{pmatrix} M_1 & 0 \\ 0 & 1 \end{pmatrix}, \quad M_1 \in \mathrm{SO}_4(K).$$

Приведем ее к жордановой форме:

$$\widetilde{M} = \begin{pmatrix} \widetilde{M_1} & 0 \\ 0 & 1 \end{pmatrix}, \quad \widetilde{Q} = \begin{pmatrix} \widetilde{Q_1} & 0 \\ 0 & 1 \end{pmatrix}.$$

Рассмотрим различные варианты:

1) если матрица $\widetilde{M}$ диагональна с различными элементами на диагонали, то легко проверить, что она удовлетворяет формуле $DDiag_2(M)$.

2) Матрица $\widetilde{M} = \mathrm{diag}\,[\alpha,\alpha,\beta,\gamma,\delta]$ в любом случае не может удовлетворять формуле $DDiag_2(M)$.

3) Если

$$\widetilde{M} = \begin{pmatrix} \alpha & 1 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 & 0 \\ 0 & 0 & \beta & 0 & 0 \\ 0 & 0 & 0 & \gamma & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

то имеем соотношения

$$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix} \begin{pmatrix} q_1 & q_2 & q_3 & q_4 \\ q_2 & q_5 & q_6 & q_7 \\ q_3 & q_6 & q_8 & q_9 \\ q_4 & q_7 & q_9 & q_{10} \end{pmatrix} \begin{pmatrix} \alpha & 0 & 0 & 0 \\ 1 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix} = \begin{pmatrix} q_1 & q_2 & q_3 & q_4 \\ q_2 & q_5 & q_6 & q_7 \\ q_3 & q_6 & q_8 & q_9 \\ q_4 & q_7 & q_9 & q_{10} \end{pmatrix}.$$

Получаем систему уравнений

$$\begin{cases} \alpha^2 q_1 + \alpha q_2 + \alpha q_2 + q_5 = q_1, \\ \alpha^2 q_2 + \alpha q_5 = q_2, \\ \alpha\beta q_3 + \beta q_6 = q_3 \\ \alpha\gamma q_4 + \gamma q_7 = q_4, \\ \alpha^2 q_5 = q_5, \\ \alpha\beta q_6 = q_6, \\ \alpha\gamma q_7 = q_7, \\ \beta^2 q_8 = q_8, \\ \gamma\beta q_9 = q_9, \\ \gamma^2 q_{10} = q_{10}. \end{cases}$$

Здесь также нужно рассмотреть разные случаи при разных α, β, γ.

a) $\alpha = \pm 1$, откуда $q_5 = 0 \Rightarrow q_2 = 0 \Rightarrow (q_6 \neq 0 \vee q_7 \neq 0) \Rightarrow \beta = \alpha \vee \gamma = \alpha$. Если $\beta = \alpha = \pm 1$, $\gamma \neq \alpha$, то $q_6 = q_7 = 0$, что невозможно. Если $\gamma = \beta = \pm 1$, то матрица не удовлетворяет формуле $DDiag_2(M)$.

b) если $\alpha \neq \pm 1$, то $q_1 = q_2 = q_5 = 0$. Значит, или $q_6 \neq 0$, или $q_7 \neq 0$. Это означает, что или $\beta = 1/\alpha$, или $\gamma = 1/\alpha$. Пусть $\beta = 1/\alpha$, $\gamma \neq 1/\alpha$. Тогда $q_7 = 0$, $q_6 = 0$, что невозможно.

Значит, матрица $\widetilde{M}$ не может иметь указанный вид.

4) Пусть

$$\widetilde{M} = \begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 1 \\ 0 & 0 & 0 & \beta \end{pmatrix}.$$

Получаем соотношения

$$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 1 \\ 0 & 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} q_1 & q_2 & q_3 & q_4 \\ q_2 & q_5 & q_6 & q_7 \\ q_3 & q_6 & q_8 & q_9 \\ q_4 & q_7 & q_9 & q_{10} \end{pmatrix} \begin{pmatrix} \alpha & 0 & 0 & 0 \\ 1 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 1 & \beta \end{pmatrix} = \begin{pmatrix} q_1 & q_2 & q_3 & q_4 \\ q_2 & q_5 & q_6 & q_7 \\ q_3 & q_6 & q_8 & q_9 \\ q_4 & q_7 & q_9 & q_{10} \end{pmatrix}.$$

Получаем систему уравнений

$$\begin{cases} \alpha^2 q_1 + \alpha q_2 + \alpha q_2 + q_5 = q_1, \\ \alpha^2 q_2 + \alpha q_5 = q_2, \\ \alpha\beta q_3 + \beta q_6 + \alpha q_4 + q_7 = q_3 \\ \alpha\beta q_4 + \beta q_7 = q_4, \\ \alpha^2 q_5 = q_5, \\ \alpha\beta q_6 + \alpha q_7 = q_6, \\ \alpha\beta q_7 = q_7, \\ \beta^2 q_8 + 2\beta q_9 + q_{10} = q_8, \\ \beta^2 q_9 + \beta q_{10} = q_9, \\ \beta^2 q_{10} = q_{10}. \end{cases}$$

a) $\alpha, \beta \neq \pm 1$, $\alpha\beta \neq 1 \Rightarrow q_7 = q_{10} = 0$, откуда $q_2 = 0 \Rightarrow q_6 = 0$, что невозможно.

b) $\alpha, \beta \neq \pm 1$, $\alpha\beta = 1$. Тогда $q_5 = q_{10} = 0 \Rightarrow q_9 = q_2 = q_7 = q_1 = q_8 = 0$, поэтому

$$\widetilde{Q} = \begin{pmatrix} 0 & 0 & q & \beta \\ 0 & 0 & \alpha & 0 \\ q & \alpha & 0 & 0 \\ \beta & 0 & 0 & 0 \end{pmatrix}.$$

Матрицы в этом базисе должны удовлетворять соотношению

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \widetilde{Q} \begin{pmatrix} A^T & C^T \\ B^T & D^T \end{pmatrix} = Q.$$

Значит, в этом базисе имеются матрицы

$$\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}, \quad D = \begin{pmatrix} q & \alpha \\ \beta & 0 \end{pmatrix} (A^T)^{-1} \begin{pmatrix} q & \alpha \\ \beta & 0 \end{pmatrix}^{-1},$$

A произвольна.

Отсюда следует, что матрица $\widetilde{M}$ не удовлетворяет последней части условия $DDiag_2(M)$.

в) $\alpha = \pm 1$, $\beta \neq \pm 1$. Тогда $q_7 = q_{10} = q_9 = q_4 = 0$, что невозможно.

г) $\alpha, \beta = \pm 1$, $\alpha\beta = -1$. тогда $q_7 = q_4 = q_6 = q_3 = q_5 = q_2 = 0$, что невозможно.

д) $\alpha, \beta = \pm 1$, $\alpha\beta = 1$. Тогда имеем следующую систему уравнений:

$$\begin{cases} q_1 \pm 2q_2 + q_5 = q_1, \\ q_2 \pm q_5 = q_2, \\ q_3 \pm q_6 \pm q_4 + q_7 = q_3 \\ q_4 \pm q_7 = q_4, \\ q_5 = q_5, \\ q_6 \pm q_7 = q_6, \\ q_7 = q_7, \\ q_8 \pm 2q_9 + q_{10} = q_8, \\ q_9 \pm q_{10} = q_9, \\ q_{10} = q_{10}. \end{cases}$$

Таким образом, $q_5 = q_7 = q_{10} = q_2 = q_9 = 0$, $q_6 = -q_4$, т. е.

$$\widetilde{Q} = \begin{pmatrix} q_1 & 0 & q_3 & q_4 \\ 0 & 0 & -q_4 & 0 \\ q_3 & -q_4 & q_8 & 0 \\ q_4 & 0 & 0 & 0 \end{pmatrix}.$$

Можно напрямую проверить, что матрицы

$$\begin{pmatrix} 0 & b & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & f & 0 & h \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad b = \frac{q_8 - q_1}{2q_4},\ f = \frac{-2q_3}{q_4},\ h = \frac{q_1 - q_8}{2q_4}$$

и

$$\begin{pmatrix} 0 & b' & -1/2 & d \\ 0 & 0 & 0 & -1/2 \\ 2 & 0 & 0 & h' \\ 0 & 2 & 0 & 0 \end{pmatrix}, \quad b' = \frac{q_1 - q_8/4}{q_4},\ h' = \frac{q_8 - 4q_1}{4q_4},\ d = \frac{q_4}{q_3}$$

лежат в нашей группе, не коммутируют друг с другом, но при этом коммутируют с матрицей $\widetilde{M}$. Значит, матрица $\widetilde{M}$ не удовлетворяет нашей формуле.

Таким образом, мы показали, что в обеих группах формула $DDiag_2(M)$ выделяет диагонализируемые в $\overline{K}$ матрицы с различными элементами на диагонали. Матрицы, перестановочные с M, образуют в нашей группе подгруппу диагонализируемых в одном базисе матриц, а фактор нормализатора этой группы по ней самой изоморфен группе Вейля W группы G. В первом случае это группа S_4, а во втором — произведение групп S_2 и $(\mathbb{Z}_2)^2$. Значит, можно написать предложение, различающее группы типов A_3 и B_2. $\square$

Таким образом, благодаря леммам 2.4 и 2.5, мы нашли предложения, отделяющие присоединенные группы типа A_3 от других классических групп.

Лемма 2.6. *Для каждого $l \geqslant 4$ существует предложение φ_{A_l} первого порядка, истинное в любой присоединенной группе типа A_l и ложное во всех присоединенных группах Шевалле других классических типов.*

Доказательство. Все группы Шевалле типа A_l, $l \geqslant 4$ характеризуются тем, что в них существует по крайней мере две несопряженных инволюции, у которых центры централизаторов бесконечны (имеют порядок, бо́льший 2).

Далее можно легко отделить их друг от друга с помощью групп меньших размерностей (фактор по центру коммутанта централизатора инволюции есть либо $\mathrm{PSL}_k(K) \times \mathrm{PSL}_{m-k}(K)$, либо $\mathrm{PSL}_{m-1}(K)$). $\square$

Лемма 2.7. *Для каждого $l \geqslant 2$ существует предложение φ_{B_l} первого порядка, истинное в любой присоединенной группе типа B_l и ложное во всех присоединенных группах Шевалле других классических типов.*

Доказательство. Группу $\mathrm{EO}_5(K)$ (т. е. присоединенную группу типа B_2) мы уже отличили от всех остальных, когда занимались группой $\mathrm{PSL}_4(K)$ (лемма 2.5).

Рассмотрим группу $\mathrm{EO}_7(K)$ (тип B_3). Если в данной группе существует инволюция $\mathrm{diag}\,[-1,-1,1,\dots,1]$, то группа однозначно характеризуется тем, что в ней есть инволюция, для которой фактор по центру коммутанта ее централизатора есть $\mathrm{EO}_5(K)$.

Если такой инволюции нет, то в этой группе есть только один класс сопряженности инволюций: $\mathrm{diag}\,[-1,-1,-1,-1,1,1,1]$. При этом данная группа точно не имеет ни тип A_l (благодаря леммам 2.2–2.6), ни B_2. Она не может иметь тип B_l ($l > 3$), так как тогда будет больше одного класса сопряженности инволюций. Это не может быть и тип C_l ($l \geqslant 3$) или D_l ($l \geqslant 4$). Таким образом, остается только сам тип B_3.

Теперь рассмотрим $l > 3$.

В таких группах уже существуют инволюции (вида $\mathrm{diag}\,[-1,-1,-1,-1,1,\dots,1]$), для которых фактор по центру коммутанта централизатора есть $\mathrm{EO}_{2l-3}(K) \times \mathrm{EO}_4(K)$. Предложение, характеризующее $\mathrm{EO}_{2l-3}(K)$, у нас уже есть. Так как больше ни с каких случаях эта группа появляться не может, то тип B_l можно считать выделенным. $\square$

Лемма 2.8. *Для каждого $l \geqslant 3$ существует предложение φ_{C_l} первого порядка, истинное в любой присоединенной группе типа C_l и ложное во всех присоединенных группах Шевалле других классических типов.*

Доказательство. Сначала надо рассмотреть группы $\mathrm{PSp}_6(K)$ (т. е. группы типа C_3).

Благодаря леммам 2.2–2.7 нам остается только отличить группу типа C_3 от групп типов C_l или D_l, $l \geqslant 4$. В ней существует инволюция, для которой фактор по центру коммутанта централизатора есть $\mathrm{PSL}_3(K)$. Остальные рассматриваемые группы таким свойством обладать не могут.

Теперь рассмотрим общий случай групп $\mathrm{PSp}_{2l}(K)$ $(l \geqslant 4)$.

Здесь уже можно действовать рекурсивно: существует инволюция, для которой фактор по центру коммутанта централизатора есть $\mathrm{PSp}_{2(l-1)}(K) \times \mathrm{PSL}_2(K)$. $\square$

Лемма 2.9. *Для каждого $l \geqslant 4$ существует предложение φ_{D_l} первого порядка, истинное в любой присоединенной группе типа D_l и ложное во всех присоединенных группах Шевалле других классических типов.*

Доказательство. Благодаря леммам 2.2–2.8 нам остается только различить группы типов D_l и D_m для $l \neq m$.

Для четных l есть инволюция, у которой фактор по центру коммутанта централизатора есть $\mathrm{PSL}_l(K)$, а для нечетных l — $PEO_{2(l-1)}(K)$.

Таким образом, мы можем различить все группы типа D_l. $\square$

Из лемм 2.2–2.9 следует, что никакие две присоединенные элементарные группы Шевалле с различными системами корней не могут быть элементарно эквивалентны.

В следующих параграфах мы установим этот результат для исключительных систем корней.

2.6 Группа Шевалле типа G_2

Существует точное представление алгебры Ли типа G_2 в $\mathrm{SL}_7(\mathbb{C})$, которое мы сейчас приведем. Для этого нам достаточно привести матрицы, соответствующие элементам X_α для корней α системы G_2. Мы будем обозначать через X_i матрицу, соответствующую элементу X_{α_i} для положительного корня α_i, а через X_{-i} — матрицу, соответствующую отрицательному корню $-\alpha_i$. Вот эти 12 матриц: $X_1 = -ie_{13} + 2ie_{21} + ie_{46} - ie_{75}$, $X_{-1} = -ie_{12} + 2ie_{31} - ie_{57} + ie_{64}$, $X_2 = e_{37} - e_{62}$, $X_{-2} = -e_{26} + e_{73}$, $X_3 = ie_{17} - ie_{35} + ie_{42} - 2ie_{61}$, $X_{-3} = -ie_{16} - ie_{24} + ie_{53} + 2ie_{71}$, $X_4 = -ie_{15} + i2_{27} + 2ie_{41} - ie_{63}$, $X_{-4} = -ie_{14} - ie_{36} + 2ie_{51} + ie_{72}$, $X_5 = -e_{27} + e_{43}$, $X_{-5} = e_{34} - e_{72}$, $X_6 = -e_{47} + e_{65}$, $X_{-6} = e_{56} - e_{74}$.

По этой алгебре Ли можно построить группу Шевалле типа G_2. В случае, когда $i \in K$, существует представление этой группы в группе $\mathrm{GL}_7(K)$, в ином случае — в группе $\mathrm{GL}_{14}(K)$.

С помощью элементов $x_1(t), \dots, x_6(t), x_{-1}(t), \dots, x_{-6}(t)$ найдем матрицы, соответствующие $w_1(t), \dots, w_6(t)$ и $h_1(t), \dots, h_6(t)$:

$w_1(t) = -e_{11} + t^2 e_{23} + t^{-2} e_{32} + ite_{46} - it^{-1} e_{57} + it^{-1} e_{64} - ite_{75}$, $h_1(t) = [1, t^2, 1/t^2, t, 1/t, 1/t, t]$, $w_2(t) = e_{11} + t^{-1} e_{26} + t3_{37} + e_{44} + e_{55} - te_{62} - t^{-1} e_{73}$, $h_2(t) = [1, 1/t, t, 1, 1, t, 1/t]$, $w_3(t) = -e_{11} - it^{-1} e_{24} + ite_{35} - ite_{42} + it^{-1} e_{53} + t^2 e_{67} + t^{-2} e_{76}$, $h_3(t) = [1, 1/t, t, 1/t, t, t^2, 1/t^2]$, $w_4(t) = -e_{11} - ite_{27} + it^{-1} e_{36} + t^2 e_{45} + t^{-2} e_{54} + ite_{63} - it^{-1} e_{72}$, $h_4(t) = [1, t, 1/t, t^2, 1/t^2, t, 1/t]$, $w_5(t) = e_{11} - te_{25} - t^{-1} e_{34} + te_{43} + t^{-1} e_{52} + e_{66} + e_{77}$, $h_5(t) = [1, t, 1/t, t, 1/t, 1, 1]$, $w_6(t) = e_{11} + e_{22} + e_{33} - te_{47} - t^{-1} e_{56} + te_{65} + t^{-1} e_{74}$, $h_6(t) = [1, 1, 1, t, 1/t, t, 1/t]$.

Таким образом, подгруппа H группы G (совпадающая с тором T, так как G односвязна) состоит из диагональных матриц, имеющих на диагонали собственные значения $[1, u, u^{-1}, uv, u^{-1}v^{-1}, v, v^{-1}]$. В этой группе есть только три неединичных инволюции, имеющие вид $[1, 1, 1, -1, -1, -1, -1]$, $[1, -1, -1, -1, -1, 1, 1]$ и $[1, -1, -1, 1, 1, -1, -1]$.

Группа Вейля этой группы Шевалле изоморфна диэдральной группе порядка 12. Ее представляют матрицы e, $w_1(1)$, $w_2(1)$, $w_3(1)$, $w_4(1)$, $w_5(1)$, $w_6(1)$, $w_1(1)w_2(1) = -e_{11}+e_{27}-e_{36}-ie_{42}+ie_{53}+ie_{64}-ie_{75}$, $w_1(1)w_3(1) = e_{11}+ie_{25}-ie_{34}+ie_{47}-ie_{56}+e_{62}+e_{73}$, $w_1(1)w_4(1) = e_{11}+ie_{26}-ie_{37}-e_{43}-e_{52}+ie_{65}-ie_{74}$, $w_1(1)w_5(1) = -e_{11}-e_{24}-e_{35}-ie_{46}+ie_{57}-ie_{63}+ie_{72}$, $w_1(1)w_6(1) = -e_{11}+e_{23}+e_{32}-ie_{45}+ie_{54}+ie_{67}-ie_{76}$.

Лемма 2.10. *Существует предложение φ_{G_2} первого порядка, истинное в любой присоединенной группе типа G_2 и ложное во всех классических присоединенных группах Шевалле.*

Доказательство. Из представления группы Вейля мы сразу же видим, что ее элемент $w_1(1)w_6(1)$ является инволюцией и коммутирует со всеми инволюциями группы H, и что такой элемент группы Вейля единственен. Также очевидно, что его произведения с инволюциями группы H тоже коммутируют со всеми перечисленными выше элементами и являются инволюциями.

Покажем, что элементы $h_2(-1)$ и $w_1(1)w_6(1)h_2(-1)$ сопряжены.

Действительно,

$$
\begin{gathered}
x_{-6}(-1/2)h_2(-1)x_{-6}(1/2) = x_{-6}(-1)h_2(-1),\\
x_6(1)x_{-6}(-1)h_2(-1)x_6(-1) =\\
= (x_6(1)x_{-6}(-1)x_6(-1))(x_6(1)h_2(-1)x_6(-1))x_6(1)x_{-6}(-1)x_6(-1)x_6(2)h_2(-1) =\\
= x_6(1)x_{-6}(-1)x_6(1)h_2(-1) = w_6(1)h_2(-1),\\
x_{-1}(-1/2)w_6(1)h_2(-1)x_{-1}(1/2) = x_{-1}(-1)w_6(1)h_2(-1),\\
x_1(1)x_{-1}(-1)w_6(1)h_2(-1)x_1(-1) = w_1(1)w_6(1)h_2(-1).
\end{gathered}
$$

Таким образом, как легко видеть, элементы $h_1(-1)$, $h_2(-1)$, $h_3(-1)$, $w_1(1)w_6(1)h_1(-1)$, $w_1(1)w_6(1)h_2(-1)$ и $w_1(1)w_6(1)h_3(-1)$ сопряжены.

Кроме того, в случае, когда $i \in K$, с помощью $h_1(i)$ сопряжены элементы $w_1(1)w_6(1)$ и $w_1(1)w_6(1)h_1(-1)$, то есть все перечисленные инволюции.

Отсюда мы видим, что имеется множество из семи коммутирующих друг с другом инволюций, из которых либо все семь, либо шесть сопряжены. Очевидно, что все централизаторы этих инволюций изоморфны между собой. Посмотрим, чему равен централизатор инволюции $h_1(-1)$.

Пусть $x \in G$ лежит в централизаторе элемента $h_1 = h_1(-1)$.

Из разложения Брюа (см. [56]) следует, что любой элемент группы G можно однозначно представить в виде

$$x_1(t_1)x_2(t_2)x_3(t_3)x_4(t_4)x_5(t_5)x_6(t_6)hwx_1(u_1)x_2(u_2)x_3(u_3)x_4(u_4)x_5(u_5)x_6(u_6),$$

где $h \in H$, w — один из 12 перечисленных элементов группы Вейля, $u_i = 0$ для всех i, для которых $w(\alpha_i) \in \Phi^+$. Так как $h_1 x h_1^{-1} = x$, то

$$\begin{aligned} x_1(t_1)x_2(-t_2)x_3(-t_3)x_4(-t_4)x_5(-t_5)x_6(t_6)h(h_1(-1)wh_1(-1))\times \\ \times x_1(u_1)x_2(-u_2)x_3(-u_3)x_4(-u_4)x_5(-u_5)x_6(u_6) = \\ = x_1(t_1)x_2(-t_2)x_3(-t_3)x_4(-t_4)x_5(-t_5)x_6(t_6)hh'w\times \\ \times x_1(u_1)x_2(-u_2)x_3(-u_3)x_4(-u_4)x_5(-u_5)x_6(u_6) = \\ = x_1(t_1)x_2(t_2)x_3(t_3)x_4(t_4)x_5(t_5)x_6(t_6)hw\times \\ \times x_1(u_1)x_2(u_2)x_3(u_3)x_4(u_4)x_5(u_5)x_6(u_6), \end{aligned}$$

где h' — некоторый элемент группы H. Из единственности разложения Брюа следует, что $t_2 = t_3 = t_4 = t_5 = u_2 = u_3 = u_4 = u_5 = 0$, $h' = 1$, т. е. $h_1(-1)wh_1(-1) = w$. Простой проверкой получаем, что либо $w = 1$, либо $w = w_1(1)$, либо $w = w_6(1)$, либо $w = w_1(1)w_6(1)$. Таким образом, централизатор инволюции $h_1(-1)$ есть произведение группы H, группы X_1, порожденной элементами $x_1(t)$ и $x_{-1}(t)$, и группы X_6, порожденной элементами $x_6(t)$ и $x_{-6}(t)$. Коммутант рассматриваемой группы порождается группами X_1 и X_6. Взяв фактор этого коммутанта по его центру, мы получим прямое произведение двух экземпляров группы $\mathrm{PSL}_2(K)$.

Как мы помним, кроме группы типа G_2 этому свойству могут удовлетворять только группы $\mathrm{PSL}_4(K)$ и $\mathrm{EO}_5(K)$.

Мы уже показали, что коммутант централизатора инволюции $h_1(-1)$ порожден группами X_1 и X_6. Аналогично, коммутант централизатора инволюции $h_2(-1)$ порожден группами X_2 и X_4, а коммутант централизатора инволюции $h_3(-1) = h_1(-1)h_2(-1)$ порожден группами X_3 и X_5. Заметим, что пары групп X_1 и X_2, X_1 и X_3, X_1 и X_4, X_1 и X_5, X_2 и X_3, X_3 и X_4, X_3 и X_6, X_4 и X_5, X_4 и X_6 порождают всю группу G, а пары групп X_2 и X_5, X_2 и X_6, X_5 и X_6 порождают лишь собственную подгруппу группы G, являющуюся группой Шевалле типа A_2.

Ни группа $\mathrm{PSL}_4(K)$, ни группа $\mathrm{EO}_5(K)$ не удовлетворяют этом свойству. Понятно, что это свойство можно записать в виде предложения первого порядка, поэтому группа Шевалле типа G_2 не может быть элементарно эквивалентна никакой классической группе Шевалле. $\square$

2.7 Группы Шевалле типа F_4

Напомним, что в системе корней F_4 имеется 48 корней, из которых 24 корня положительны. Эти положительные корни порождены четырьмя простыми корнями $\alpha_1 = e_2 - e_3$, $\alpha_2 = e_3 - e_4$, $\alpha_3 = e_4$ и $\alpha_4 = \frac{1}{2}(e_1 - e_2 - e_3 - e_4)$. Первые два корня являются длинными, последние два — короткими. Перечислим остальные положительные корни: $\alpha_5 = \alpha_1 + \alpha_2$, $\alpha_6 = \alpha_2 + \alpha_3$, $\alpha_7 = \alpha_3 + \alpha_4$, $\alpha_8 = \alpha_1 + \alpha_2 + \alpha_3$, $\alpha_9 = \alpha_2 + \alpha_3 + \alpha_3$, $\alpha_{10} = \alpha_2 + \alpha_3 + \alpha_4$, $\alpha_{11} = \alpha_1+\alpha_2+\alpha_3+\alpha_4$, $\alpha_{12} = \alpha_2+\alpha_3+\alpha_3+\alpha_4$, $\alpha_{13} = \alpha_1+\alpha_2+\alpha_3+\alpha_3$, $\alpha_{14} = \alpha_1+\alpha_2+\alpha_2+\alpha_3+\alpha_3$, $\alpha_{15} = \alpha_1+\alpha_2+\alpha_3+\alpha_3+\alpha_4$, $\alpha_{16} = \alpha_2+\alpha_3+\alpha_3+\alpha_4+\alpha_4$, $\alpha_{17} = \alpha_1+\alpha_2+\alpha_2+\alpha_3+\alpha_3+\alpha_4$, $\alpha_{18} = \alpha_1+\alpha_2+\alpha_2+\alpha_3+\alpha_3+\alpha_3+\alpha_4$, $\alpha_{19} = \alpha_1+\alpha_2+\alpha_2+\alpha_3+\alpha_4+\alpha_4$, $\alpha_{20} = \alpha_1+\alpha_2+\alpha_2+\alpha_3+\alpha_3+\alpha_3+\alpha_4+\alpha_4$,

$\alpha_{21} = \alpha_1 + \alpha_1 + \alpha_2 + \alpha_2 + \alpha + 2 + \alpha_3 + \alpha_3 + \alpha_3 + \alpha_4 + \alpha_4$, $\alpha_{22} = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_3 + \alpha_4 + \alpha_4$, $\alpha_{23} = \alpha_1 + \alpha_2 + \alpha_2 + \alpha_2 + \alpha_3 + \alpha_3 + \alpha_3 + \alpha_3 + \alpha_4 + \alpha_4$, $\alpha_{24} = \alpha_1 + \alpha_2 + \alpha_2 + \alpha_3 + \alpha_3 + \alpha_3 + \alpha_3 + \alpha_4 + \alpha_4$.

Лемма 2.11. *Существует предложение φ_{F_4} первого порядка, истинное в любой присоединенной группе типа F_4 и ложное во всех классических присоединенных группах Шевалле, а также в группах Шевалле типа G_2.*

Доказательство. Найдем централизатор инволюции $h_1(-1)$.

Пусть
$$Z(h_1) \ni x = x_1(t_1) \dots x_{24}(t_{24}) hw x_1(u_1) \dots x_{24}(u_{24}),$$
где $h \in H$, w — произведение некоторого количества элементов $w_i(1)$. Тогда
$$h_1(-1) x h_1(-1) = x_1(\pm t_1) \dots x_{24}(\pm t_{24}) hh'w x_1(\pm u_1) \dots x_{24}(\pm u_{24}),$$
причем $h_1(-1)x_i(s)h_1(-1) = x_i(s)$ тогда и только тогда, когда $i = 1, 3, 4, 7, 14, 17, 18, 19, 20, 24$. Значит,
$$\begin{gathered} x = x_{\alpha_1}(t_1)x_{\alpha_3}(t_3)x_{\alpha_4}(t_4)x_{\alpha_3+\alpha_4}(t_7)x_{\alpha_{14}}(t_{14})\times \\ x_{\alpha_{14}+\alpha_4}(t_{17})x_{\alpha_{14}+\alpha_3+\alpha_4}(t_{18})x_{\alpha_{14}+x_{\alpha_4}+x_{\alpha_4}}(t_{19})x_{\alpha_{14}+\alpha_3+\alpha_4+\alpha_4}(t_{20})\times \\ \times x_{\alpha_{14}+\alpha_3+\alpha_3+\alpha_4+\alpha_4}(t_{24})hwx_1(u_1)\times \\ \times x_3(u_3)x_4(u_4)x_7(u_7)x_{14}(u_{14})x_{17}(u_{17})x_{18}(u_{18})x_{19}(u_{19})x_{20}(u_{20})x_{24}(u_{24}). \end{gathered}$$

Отсюда следует, что $h_1(-1)$ должен коммутировать с w. Вспомним, что $w_\alpha(1)h_\beta(-1)w_\alpha(1)^{-1} = h_{w_\alpha(\beta)}(-1)$. Таким образом, чтобы $w_{i_1}(1)\dots w_{i_m}(1)$ коммутировало с $h_1(-1)$, необходимо и достаточно, чтобы $w_{\alpha_{i_1}}\dots w_{\alpha_{i_m}}(\alpha_1) = \pm\alpha_1$.

Очевидно, для любое произведение элементов $w_1(1)$, $w_3(1)$, $w_4(1)$ и $w_{14}(1)$ коммутирует с $h_1(-1)$. Легко показать, что другие представители группы Вейля не коммутируют с инволюцией $h_1(-1)$. Отсюда следует, что централизатор инволюции $h_1(-1)$ есть произведение группы H и подгруппы в G, порожденной X_1, X_3, X_4 и X_{14}, т. е. есть произведение группы H, группы Шевалле типа A_1 и группы Шевалле типа C_3. Как и выше, можно показать, что его коммутант есть центральное произведение группы Шевалле типа A_1 на группу Шевалле типа C_3, т. е. групп $\mathrm{SL}_2(K)$ и $\mathrm{Sp}_6(K)$, а фактор по центру этого коммутанта изоморфен $\mathrm{PSL}_2(K) \times \mathrm{PSp}_6(K)$.

Аналогично, централизатор инволюции $h_3(-1)$ порожден группой H и подгруппами X_1, X_2, X_3, X_{16}, т. е. есть произведение группы H и группы Шевалле типа B_4, а фактор по центру коммутанта изоморфен $\mathrm{EO}_9(K)$.

Чтобы написать предложение, отличающее группу Шевалле типа F_4 от всех рассмотренных нами групп Шевалле, теперь достаточно заметить, что мы не встречали еще группы Шевалле, у которой для одной инволюции фактор по центру коммутанта централизатора изоморфен $\mathrm{PSL}_2(K) \times \mathrm{PSp}_6(K)$, а для другой — $\mathrm{EO}_9(K)$. □

2.8 Группа Шевалле типа E_6

В системе корней E_6 имеется 72 корня, из которых 36 корней положительны. Эти положительные корни порождены шестью простыми корнями $\alpha_1 = \frac{1}{2}(e_1 + e_8 - e_2 - e_3 - e_4 - e_5 - e_6 - e_7)$, $\alpha_2 = e_1 + e_2$, $\alpha_3 = e_2 - e_1$, $\alpha_4 = e_3 - e_2$, $\alpha_5 = e_4 - e_3$ и $\alpha_6 = e_5 - e_4$. Перечислим остальные положительные корни, для простоты вместо α_i записывая просто число i: $\alpha_7 = 1+3$, $\alpha_8 = 3+4$, $\alpha_9 = 4+5$, $\alpha_{10} = 5+6$, $\alpha_{11} = 1+3+4$, $\alpha_{12} = 3+4+5$, $\alpha_{13} = 2+4$, $\alpha_{14} = 2+3+4$, $\alpha_{15} = 2+4+5$, $\alpha_{16} = 1+2+3+4$, $\alpha_{17} = 2+3+4+5$, $\alpha_{18} = 1+3+4+5$, $\alpha_{19} = 3+4+5+6$, $\alpha_{20} = 2+4+5+6$, $\alpha_{21} = 2+3+4+4+5$, $\alpha_{22} = 2+3+4+5+6$, $\alpha_{23} = 1+2+3+4+5$, $\alpha_{24} = 1+3+4+5+6$, $\alpha_{25} = 1+2+3+4+4+5$, $\alpha_{26} = 1+2+3+3+4+4+5$, $\alpha_{27} = 2+3+4+4+5+6$, $\alpha_{28} = 2+3+4+4+5+5+6$, $\alpha_{29} = 1+2+3+3+4+4+5+6$, $\alpha_{30} = 1+2+3+4+5+6$, $\alpha_{31} = 1+2+3+4+4+5+6$, $\alpha_{32} = 1+2+3+4+4+5+5+6$, $\alpha_{33} = 4+5+6$, $\alpha_{34} = 1+2+3+3+4+4+5+5+6$, $\alpha_{35} = 1+2+3+3+4+4+4+5+5+6$, $\alpha_{36} = 1+2+2+3+3+4+4+4+5+5+6$.

Лемма 2.12. *Существует предложение φ_{E_6} первого порядка, истинное в любой присоединенной группе типа E_6 и ложное во всех классических присоединенных группах Шевалле, а также в группах Шевалле типов G_2 и F_4.*

Доказательство. Найдем централизатор инволюции h_1.

Пусть $Z(h_1) \ni x = x_1(t_1)\dots x_{36}(t_{36})hwx_1(u_1)\dots x_{36}(u_{36})$, где $h \in H$, w — произведение некоторого количества элементов $w_i(1)$. Тогда

$$h_1xh_1 = x_1(\pm t_1)\dots x_{36}(\pm t_{36})hh'wx_1(\pm u_1)\dots x_{36}(\pm u_{36}),$$

причем $h_1(-1)x_i(s)h_1(-1) = x_i(s)$ тогда и только тогда, когда $i = 1, 2, 4, 5, 6, 9, 10, 13, 15, 20, 26, 29, 33, 34, 35, 36$.

Кроме того, $h_1(-1)$ должен коммутировать с w. Как мы помним из предыдущего параграфа, чтобы $w_{i_1}(1)\dots w_{i_m}(1)$ коммутировало с $h_1(-1)$, необходимо и достаточно, чтобы $w_{\alpha_{i_1}}\dots w_{\alpha_{i_m}}(\alpha_1) = \pm\alpha_1$.

Очевидно, что любое произведение элементов $w_1(1)$, $w_2(1)$, $w_4(1)$ $w_5(1)$, $w_6(1)$ и $w_{26}(1)$ коммутирует с $h_1(-1)$. Несложно показать, что другие представители группы Вейля не коммутируют с инволюцией $h_1(-1)$. Отсюда следует, что централизатор инволюции $h_1(-1)$ есть произведение группы H и подгруппы в G, порожденной X_1, X_2, X_4, X_5, X_6 и X_{26}. Группа X_1 коммутирует со всеми остальными порождающими подгруппами, а подгруппы X_2, X_4, X_5, X_6 и X_{26} порождают группу Шевалле типа A_5. Таким образом, централизатор инволюции h_1 есть произведение групп H и центрального произведения групп Шевалле типов A_1 и A_5, а коммутант этого централизатора есть просто центральное произведение групп Шевалле типов A_1 и A_5. Следовательно, фактор по центру коммутанта централизатора инволюции h_1 есть группа $\mathrm{PSL}_2(K) \times \mathrm{PSL}_6(K)$.

Централизатор инволюции h_1h_2 порожден группой H и группой, порожденной подгруппами X_1, X_2, X_5, X_6 и X_8, которая имеет тип D_5, а фактор по центру этого коммутанта изоморфен группе $\mathrm{PEO}_{10}(K)$.

Теперь нам требуется научиться отличать группу Шевалле типа E_6 от всех классических групп Шевалле. Это очень просто, если заметить, что не бывает классических групп Шевалле, для которых для некоторой одной инволюции фактор по центру коммутанта централизатора этой инволюции есть группа, элементарно эквивалентная группе

$\mathrm{PSL}_2(K) \times \mathrm{PSL}_6(K)$, а для некоторой другой инволюции фактор по центру коммутанта ее централизатора есть группа, элементарно эквивалентная группе $\mathrm{PEO}_{10}(K)$. Это же не может выполняться и для групп типов G_2 и F_4. $\square$

2.9 Группа Шевалле типа E_7

В системе корней E_7 имеется 126 корней, из которых 63 корня положительны. Эти положительные корни порождены семью простыми корнями $\alpha_1 = \frac{1}{2}(e_1 + e_8 - e_2 - e_3 - e_4 - e_5 - e_6 - e_7)$, $\alpha_2 = e_1 + e_2$, $\alpha_3 = e_2 - e_1$, $\alpha_4 = e_3 - e_2$, $\alpha_5 = e_4 - e_3$, $\alpha_6 = e_5 - e_4$ и $\alpha_7 = e_6 - e_5$. Перечислим остальные положительные корни: $\alpha_8 = 1+3$, $\alpha_9 = 3+4$, $\alpha_{10} = 4+5$, $\alpha_{11} = 5+6$, $\alpha_{12} = 6+7$, $\alpha_{13} = 1+3+4$, $\alpha_{14} = 2+4$, $\alpha_{15} = 3+4+5$, $\alpha_{16} = 2+3+4$, $\alpha_{17} = 2+4+5$, $\alpha_{18} = 4+5+6$, $\alpha_{19} = 5+6+7$, $\alpha_{20} = 4+5+6+7$, $\alpha_{21} = 1+2+3+4$, $\alpha_{22} = 2+3+4+5$, $\alpha_{23} = 3+4+5+6+7$, $\alpha_{24} = 2+4+5+6+7$, $\alpha_{25} = 2+3+4+5+6+7$, $\alpha_{26} = 1+3+4+5$, $\alpha_{27} = 3+4+5+6$, $\alpha_{28} = 2+4+5+6$, $\alpha_{29} = 2+3+4+4+5$, $\alpha_{30} = 2+3+4+5+6$, $\alpha_{31} = 1+2+3+4+5$, $\alpha_{32} = 1+3+4+5+6$, $\alpha_{33} = 1+2+3+4+4+5$, $\alpha_{34} = 1+2+3+3+4+4+5$, $\alpha_{35} = 2+3+4+4+5+6$, $\alpha_{36} = 2+3+4+4+5+5+6$, $\alpha_{37} = 1+2+3+3+4+4+5+6$, $\alpha_{38} = 1+2+3+4+5+6$, $\alpha_{39} = 1+2+3+4+4+5+6$, $\alpha_{40} = 1+2+3+4+4+5+5+6$, $\alpha_{41} = 1+2+3+3+4+4+5+5+6$, $\alpha_{42} = 1+2+3+3+4+4+4+5+5+6$, $\alpha_{43} = 1+2+2+3+3+4+4+4+5+5+6$, $\alpha_{44} = 1+1+2+2+3+3+3+4+4+4+4+5+5+5+6+6+7$, $\alpha_{45} = 1+3+4+5+6+7$, $\alpha_{46} = 2+3+4+4+5+6+7$, $\alpha_{47} = 2+3+4+4+5+5+6+7$, $\alpha_{48} = 1+2+3+3+4+4+5+6+7$, $\alpha_{49} = 1+2+3+4+5+6+7$, $\alpha_{50} = 1+2+3+4+4+5+6+7$, $\alpha_{51} = 1+2+3+4+4+5+5+6+7$, $\alpha_{52} = 1+2+3+3+4+4+5+5+6+7$, $\alpha_{53} = 1+2+3+3+4+4+4+5+5+6+7$, $\alpha_{54} = 1+2+2+3+3+4+4+4+5+5+6+7$, $\alpha_{55} = 1+2+3+4+4+5+5+6+6+7$, $\alpha_{56} = 1+2+3+3+4+4+5+5+6+6+7$, $\alpha_{57} = 1+2+3+3+4+4+4+5+5+6+6+7$, $\alpha_{58} = 1+2+2+3+3+4+4+4+5+5+6+6+7$, $\alpha_{59} = 2+3+4+4+5+5+6+6+7$, $\alpha_{60} = 1+2+3+3+4+4+4+5+5+5+6+6+7$, $\alpha_{61} = 1+2+2+3+3+4+4+4+5+5+5+6+6+7$, $\alpha_{62} = 1+2+2+3+3+4+4+4+4+5+5+5+6+6+7$, $\alpha_{63} = 1+2+2+3+3+3+4+4+4+4+5+5+5+6+6+7$.

Лемма 2.13. *Существует предложение φ_{E_7} первого порядка, истинное в любой присоединенной группе типа E_7 и ложное во всех классических присоединенных группах Шевалле, а также в присоединенных группах Шевалле типов G_2, F_2, E_6.*

Доказательство. Пусть $Z(h_1) \ni x = x_1(t_1)\dots x_{63}(t_{63})hwx_1(u_1)\dots x_{63}(u_{63})$, где $h \in H$, w — произведение некоторого количества элементов $w_i(1)$. Тогда

$$h_1 x h_1 = x_1(\pm t_1)\dots x_{63}(\pm t_{63})hh'wx_1(\pm u_1)\dots x_{63}(\pm u_{63}),$$

причем $h_1(-1)x_i(s)h_1(-1) = x_i(s)$ тогда и только тогда, когда $i = 1, 2, 4, 5, 6, 7, 10, 11, 12, 14, 17, 18, 19, 20, 24, 28, 34, 37, 41, 42, 43, 48, 52, 53, 54, 56, 57, 58, 60, 61, 62$. Кроме того, $h_1(-1)$ должен коммутировать с w. Чтобы $w_{i_1}(1)\dots w_{i_m}(1)$ коммутировало с $h_1(-1)$, нужно, чтобы $w_{\alpha_{i_1}}\dots w_{\alpha_{i_m}}(\alpha_1) = \pm\alpha_1$.

Очевидно, для любое произведение элементов $w_1(1)$, $w_2(1)$, $w_4(1)$ $w_5(1)$, $w_6(1)$, $w_7(1)$ и $w_{34}(1)$ коммутирует с $h_1(-1)$, а другие представители группы Вейля не коммутируют с инволюцией $h_1(-1)$. Отсюда следует, что централизатор инволюции $h_1(-1)$ есть произведение группы H и подгруппы в G, порожденной X_1, X_2, X_4, X_5, X_6, X_7 и X_{34}, откуда следует, что фактор по центру коммутанта централизатора $h_1(-1)$ изоморфен группе $\mathrm{PSL}_2(K) \times \mathrm{PEO}_{12}(K)$. Посмотрим, существует ли еще какая-то группа Шевалле, для которой фактор по центру коммутанта централизатора некоторой инволюции также изоморфен этой группе.

Очевидно, что такое невозможно ни для групп G_2, F_4, E_6, ни для групп типов A_l, C_l или D_l. Единственным возможным вариантом является группа $\mathrm{EO}_{15}(K)$ — группа типа B_7. Однако в этой группе существует инволюция

$$\mathrm{diag}\,[\underbrace{-1,\dots,-1}_{8},\underbrace{1,\dots,1}_{7}],$$

у которой фактор по центру коммутанта централизатора изоморфен $\mathrm{PEO}_8(K) \times \mathrm{EO}_7(K)$, что никак не может быть возможно для группы Шевалле типа E_7, так как в ней не содержится подгруппы $\mathrm{EO}_7(K)$ (так как никакие корни системы E_7 не образуют подсистему B_3).

Таким образом, группа Шевалле типа E_7 не может быть элементарно эквивалентна группе Шевалле типа B_7, а значит, никакой из рассмотренных групп. $\square$

2.10 Группа Шевалле типа E_8

В системе корней E_8 имеется 240 корня, из которых 120 корней положительны. Эти положительные корни порождены восемью простыми корнями $\alpha_1 = \frac{1}{2}(e_1+e_8-e_2-e_3-e_4-e_5-e_6-e_7)$, $\alpha_2 = e_1+e_2$, $\alpha_3 = e_2-e_1$, $\alpha_4 = e_3-e_2$, $\alpha_5 = e_4-e_3$, $\alpha_6 = e_5-e_4$, $\alpha_7 = e_6-e_5$ и $\alpha_8 = e_7-e_6$. Перечислим остальные положительные корни (для краткости пропуская знаки “+”): $\alpha_9 = 13$, $\alpha_{10} = 24$, $\alpha_{11} = 34$, $\alpha_{12} = 45$, $\alpha_{13} = 56$, $\alpha_{14} = 67$, $\alpha_{15} = 78$, $\alpha_{16} = 134$, $\alpha_{17} = 234$, $\alpha_{18} = 245$, $\alpha_{19} = 1234$, $\alpha_{20} = 345$, $\alpha_{21} = 456$, $\alpha_{22} = 1345$, $\alpha_{23} = 567$, $\alpha_{24} = 2456$, $\alpha_{25} = 3456$, $\alpha_{26} = 678$, $\alpha_{27} = 4567$, $\alpha_{28} = 13456$, $\alpha_{29} = 2345$, $\alpha_{30} = 23445$, $\alpha_{31} = 23456$, $\alpha_{32} = 12345$, $\alpha_{33} = 23567$, $\alpha_{34} = 123445$, $\alpha_{35} = 123456$, $\alpha_{36} = 34567$, $\alpha_{37} = 1233445$, $\alpha_{38} = 45678$, $\alpha_{39} = 234456$, $\alpha_{40} = 1234456$, $\alpha_{41} = 134567$, $\alpha_{42} = 5678$, $\alpha_{43} = 234567$, $\alpha_{44} = 1234567$, $\alpha_{45} = 245678$, $\alpha_{46} = 2344556$, $\alpha_{47} = 12344556$, $\alpha_{48} = 345678$, $\alpha_{49} = 12334456$, $\alpha_{50} = 1345678$, $\alpha_{51} = 2344567$, $\alpha_{52} = 12344567$, $\alpha_{53} = 2345678$, $\alpha_{54} = 23445567$, $\alpha_{55} = 123344556$, $\alpha_{56} = 23445566778$, $\alpha_{57} = 23445678$, $\alpha_{58} = 1233444556$, $\alpha_{59} = 234455667$, $\alpha_{60} = 12345678$, $\alpha_{61} = 123445567$, $\alpha_{62} = 1234455667$, $\alpha_{63} = 123445678$, $\alpha_{64} = 12233444556$, $\alpha_{65} = 123344567$, $\alpha_{66} = 1233445567$, $\alpha_{67} = 12334445567$, $\alpha_{68} = 12334455667$, $\alpha_{69} = 1233445678$, $\alpha_{70} = 122334445567$, $\alpha_{71} = 234455678$, $\alpha_{72} = 2344556678$, $\alpha_{73} = 1234455678$, $\alpha_{74} = 12344556678$, $\alpha_{75} = 123344455678$, $\alpha_{76} = 123344455667$, $\alpha_{77} = 12334455678$, $\alpha_{78} = 123445566778$, $\alpha_{79} = 123344556678$, $\alpha_{80} = 1233445566778$, $\alpha_{81} = 1233444556678$, $\alpha_{82} = 12334445566778$, $\alpha_{83} = 1233444555667$, $\alpha_{84} = 12334445556678$, $\alpha_{85} = 123344455566778$, $\alpha_{86} = 1233444555666778$, $\alpha_{87} = 1223344455678$, $\alpha_{88} = 1223344455667$, $\alpha_{89} = 12233444556678$, $\alpha_{90} = 122334445566778$, $\alpha_{91} = 12233444555667$, $\alpha_{92} = 1223344455566778$, $\alpha_{93} = 1223344455566778$, $\alpha_{94} = 12233444555666778$, $\alpha_{95} = 122334444555667$, $\alpha_{96} = 12233444455566677 8$, $\alpha_{97} = 12233444455566778$, $\alpha_{98} = 122334444555666778$, $\alpha_{99} = 1223344445555666778$, $\alpha_{100} = 1223334444555667$, $\alpha_{101} = 12233344445556678$, $\alpha_{102} = 122333444455566778$, $\alpha_{103} = 1223334444555666778$, $\alpha_{104} = 12233344445555666778$, $\alpha_{105} = 122333444445555666778$, $\alpha_{106} = 1222333444445555666778$, $\alpha_{107} =$

11223334444555667, $\alpha_{108} = 112233344445556678$, $\alpha_{109} = 1122333444455566778$, $\alpha_{110} = 11223334444555666778$, $\alpha_{111} = 112233344445555666778$, $\alpha_{112} = 1122333444445555666778$, $\alpha_{113} = 11223333444445555666778$, $\alpha_{114} = 112223333444445555666778$, $\alpha_{115} = 1122233334444455555666778$, $\alpha_{116} = 11222333344444455555666778$, $\alpha_{117} = 112223333444444555556666778$, $\alpha_{118} = 1122233334444445555566666778$, $\alpha_{119} = 11222333344444455555666667778$, $\alpha_{120} = 112223333444444555556666677788$.

Лемма 2.14. *Существует предложение φ_{E_8} первого порядка, истинное в любой присоединенной группе типа E_8 и ложное во всех присоединенных группах Шевалле других типов.*

Доказательство. Рассмотрим централизатор инволюции h_1.

Пусть $Z(h_1) \ni x = x_1(t_1) \dots x_{120}(t_{63}) h w x_1(u_1) \dots x_{120}(u_{120})$, где $h \in H$, w — произведение некоторого количества элементов $w_i(1)$. Тогда

$$h_1 x h_1 = x_1(\pm t_1) \dots x_{120}(\pm t_{120}) h h' w x_1(\pm u_1) \dots x_{120}(\pm u_{120}),$$

причем $h_1(-1) x_i(s) h_1(-1) = x_i(s)$ тогда и только тогда, когда $i = 1, 2, 4,\ 5, 6, 7,\ 8, 10, 11, 12,\ 13, 14,\ 15, 18,\ 19, 21,\ 23, 24,\ 26, 27,\ 33, 37, 38,\ 42, 45, 49,\ 55, 58,\ 64, 65, 66,\ 67, 68, 69, 70, 75, 76, 77, 79, 80,\ 81, 82, 83, 84,\ 85, 86, 87,\ 88, 89, 90,\ 91, 92, 93,\ 94, 95, 96,\ 97, 98, 99,\ 113, 115, 116, 117, 118, 119, 120$.

Очевидно, для любое произведение элементов $w_1(1)$, $w_2(1)$, $w_4(1)$ $w_5(1)$, $w_6(1)$, $w_7(1)$, $w_8(1)$ и $w_{37}(1)$ коммутирует с $h_1(-1)$, а другие представители группы Вейля не коммутируют, поэтому централизатор инволюции $h_1(-1)$ есть произведение группы H и подгруппы в G, порожденной X_1, X_2, X_4, X_5, X_6, X_7, X_8 и X_{37}.

Фактор по центру коммутанта централизатора этой инволюции изоморфен группе $\mathrm{PSL}_2(K) \times G(E_7, K)$, откуда сразу следует, что группа типа E_8 не может быть элементарно эквивалентна никакой другой группе Шевалле. $\square$

Из лемм 2.2–2.14 следует

Предложение 2.3. *Если две (элементарные) группы Шевалле над бесконечными полями характеристики, не равной 2, элементарно эквивалентны, то соответствующие системы корней совпадают.*

2.11 Определимость поля в группах Шевалле

Чтобы доказать, что в каждой из групп Шевалле определимо поле, нам достаточно доказать определимость поля в присоединенной группе Шевалле типа A_1 (т.е. в $\mathrm{PSL}_2(K)$).

Лемма 2.15. *Если группы $\mathrm{PSL}_2(K)$ и $\mathrm{PSL}_2(K')$ (K, K' — бесконечные поля характеристики $\neq 2$) элементарно эквивалентны, то поля K, K' элементарно эквивалентны.*

Доказательство. Пусть мы имеем группу $\mathrm{PSL}_2(K)$.

Рассмотрим матрицы, удовлетворяющие формуле

$$Cell(M) := M^2 \neq 1 \wedge \exists X((XMX^{-1})M = M(XMX^{-1}) \wedge X^2 M \neq MX^2).$$

Покажем, что эти матрицы имеют в некотором базисе вид

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

Пусть матрица M диагонализируема в поле $\overline{K}$, тогда в некотором базисе она имеет вид

$$A = \begin{pmatrix} \alpha & 0 \\ 0 & 1/\alpha \end{pmatrix}.$$

Матрица такого вида может коммутировать либо с диагональной матрицей, либо может быть ситуация $AB = -BA$ в группе $\mathrm{SL}_2(K)$, т.е.

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

но в этом случае $A^2 = 1$ в группе $\mathrm{PSL}_2(K)$, откуда следует, что $M^2 = 1$, а это противоречит первому условию формулы $Cell$.

Любая матрица M, сопряженная к матрице вида

$$A = \pm \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix},$$

удовлетворяет формуле $Cell$ (можно выбрать матрицу X диагональной с разными элементами на диагонали, при этом не равными в квадрате ± 1).

Фиксируем некоторую матрицу A, удовлетворяющую формуле $Cell$. Рассмотрим все матрицы, коммутирующие с A. Пусть для данной A этой множество обозначается через $\mathcal{X}_A$. Это матрицы, которые в одном и том же базисе приводятся к виду

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \quad t \in K.$$

Нормализатор $N(\mathcal{X}_A)$ множества $\mathcal{X}_A$ состоит из матриц, имеющих в данном базисе вид

$$\begin{pmatrix} \alpha & \beta \\ 0 & 1/\alpha \end{pmatrix}.$$

Выберем одну матрицу B из $N(\mathcal{X}_A) \setminus \mathcal{X}_A$ и все коммутирующие с ней матрицы. Обозначим выбранное множество через $\mathcal{D}_{A,B}$. Можно выбрать базис, в котором матрицы из $\mathcal{D}_{A,B}$ имеют вид

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

а матрицы из $\mathcal{X}_A$ имеют вид

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

Кроме того, рассмотрим множество $\mathcal{E}_{A,B}$ матриц, нормализующих $\mathcal{D}_{A,B}$, но не принадлежащих $\mathcal{D}_{A,B}$. Они имеют вид
$$\begin{pmatrix} 0 & \gamma \\ -1/\gamma & 0 \end{pmatrix}.$$

Через $\mathcal{Y}_{A,B}$ обозначим матрицы, сопряженные матрицам из $\mathcal{X}_A$ с помощью матриц из $\mathcal{E}_{A,B}$. Они имеют вид
$$\pm \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}.$$

Теперь введем формулу
$$\varphi(M,N) := (M \in \mathcal{X}_A) \wedge (N \in \mathcal{Y}_{A,B}) \wedge (MNM \in \mathcal{E}_{A,B}).$$

Если для матрицы
$$M = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$
выполнено $\varphi(M,N)$ для некоторой N, то
$$N = M^{\varphi} = \begin{pmatrix} 1 & 0 \\ -1/t & 1 \end{pmatrix}.$$

Будем писать
$$E_t := \mathcal{E}(A_t) = A_t A_t^{\varphi} A_t = \begin{pmatrix} 0 & t \\ -1/t & 0 \end{pmatrix}.$$

Фиксируем
$$A_u = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}.$$

Так как
$$E_t E_u^{-1} = \begin{pmatrix} 0 & t \\ -1/t & 0 \end{pmatrix} \begin{pmatrix} 0 & -u \\ 1/u & 0 \end{pmatrix} = \begin{pmatrix} t/u & 0 \\ 0 & u/t \end{pmatrix},$$
то
$$E_{ts/u} = E_t E_u^{-1} E_s.$$

Заметим, что так как мы имеем дело с группой $\mathrm{PSL}_2(K)$, то отображение $\mathcal{E} : \mathcal{X}_A \to \mathcal{E}_{A,B}$, $\mathcal{X}_A \mapsto \mathcal{E}(\mathcal{X}_A)$, необратимо (а именно, не мономорфно), так как $\mathcal{E}(A_t) = \mathcal{E}(A_{-t})$ в группе $\mathrm{PSL}_2(K)$.

Предположим, что мы имеем A_t и A_s и хотим найти $A_t \otimes A_s = A_{ts/u}$. В этом случае отображение $A_t \mapsto t/u$ будет изоморфизмом между множеством $\mathcal{X}_A$ (с операцией сложения $A_t \oplus A_s = A_t A_s$ и операцией умножения $\otimes$) и полем K. Так как $E_{ts/u} = \mathcal{E}(A_t)\mathcal{E}(A_u)^{-1}\mathcal{E}(A_s)$, то нам остается только восстановить $A_{ts/u}$ по $E_{ts/u}$. Имеется два кандидата: $A_{ts/u}$ и $A_{-ts/u}$, и нам нужно выбрать из них правильного.

Мы имеем следующее соотношение:
$$A_t A_{ts/u} = A_{t(1+s/u)} = A_{t/u(s+u)} = A_t \otimes (A_s A_u),$$

откуда

$$\mathcal{E}(A_t A_{ts/u}) = \mathcal{E}(A_t)\mathcal{E}(A_u)^{-1}\mathcal{E}(A_s A_u)$$

при $t, s \neq 0$.

При этом имеем

$$A_t A_{-ts/u} = A_{t/u(u-s)}.$$

Соотношение

$$\mathcal{E}(A_t A_{-ts/u}) = \mathcal{E}(A_t)\mathcal{E}(A_u)^{-1}\mathcal{E}(A_s A_u)$$

при $t, s \neq 0$, как легко проверить, выполняться не может, поэтому искомую формулу умножения можно написать в следующем виде:

$$\begin{aligned} &A_w = A_t \otimes A_s \Longleftrightarrow (A_t = 1 \wedge A_w = 1) \vee (A_s = 1 \wedge A_w = 1) \vee \\ &\vee (A_s \neq 1 \wedge A_t \neq 1 \wedge \mathcal{E}(A_w) = \mathcal{E}(A_t)\mathcal{E}(A_u)^{-1}\mathcal{E}(A_s) \wedge \mathcal{E}(A_t A_w) = \mathcal{E}(A_t)\mathcal{E}(A_u)^{-1}\mathcal{E}(A_s A_u)). \end{aligned}$$

Таким образом, искомый изоморфизм построен, откуда видно, что поле K определимо в группе $\mathrm{PSL}_2(K)$, т.е. существуют формулы $\varphi(X_1, X_2, \dots, X_l; Y)$, $\psi(X_1, \dots, X_l)$, $Add(Y_1, Y_2, Y_3)$, $Mult(Y_1, Y_2, Y_3)$ такие, что для любых $X_1, \dots, X_l$, удовлетворяющих формуле $\psi(\dots)$, все Y такие, что $\varphi(X_1, \dots, X_l; Y)$, с операциями сложения и умножения, заданными формулами $Add(\dots)$ и $Mult(\dots)$, образуют поле, изоморфное полю K.

Следовательно, если группы $\mathrm{PSL}_2(K)$ и $\mathrm{PSL}_2(K')$ элементарно эквивалентны, то поля K, K' элементарно эквивалентны. □

Предложение 2.4. *Если две присоединенные элементарные группы Шевалле $G(\Phi, K)$ и $G(\Phi, K')$ (K, K' — бесконечные поля характеристики, отличной от двух) элементарно эквивалентны, то поля K, K' элементарно эквивалентны.*

Доказательство. Для данной системы корней Φ рассмотрим фактор по центру коммутанта централизатора подходящей инволюции (см. леммы 2.2–2.14) выберем в нем ту из компонент прямого произведения, которая изоморфна $\mathrm{PSL}_2(K)$. После этого воспользуемся леммой 2.15. □

2.12 Изоморфизм решеток весов

Нам осталось доказать, что

Предложение 2.5. *Если две (элементарные) группы Шевалле элементарно эквивалентны, то их решетки весов совпадают.*

Доказательство. Сразу перейдем к элементарным группам Шевалле.

Заметим, что если две группы Шевалле элементарно эквивалентны, то их центры изоморфны, так как конечны. Центр группы Шевалле является факторгруппой ее решетки весов по решетке корней. Мы уже знаем, что две элементарные группы Шевалле имеют один и тот же тип. Тогда фактор решетки весов по решетке корней полностью определяет саму решетку весов, за исключением единственного случая: когда мы имеем дело с группой Шевалле типа D_{2m}, $m \geqslant 3$, и промежуточной решеткой такой, что порядок фактора решетки весов по решетке корней равен 2. В этом случае могут возникать две неизоморфные группы Шевалле — одна из них $\mathrm{SO}_{4m}(K)$ (коммутант этой группы в элементарном случае), а другая — так называемая "полуспинорная группа".

Напомним (см. [8]), что корни системы D_{2m} — это векторы $\pm e_i \pm e_j$, $i \neq j$ в ортонормированном базисе $e_1, \dots, e_{2m}$ $2m$-мерного евклидова пространства, решетка весов этой системы состоит из векторов с четной суммой целочисленной координат, универсальная решетка имеет вид

$$\oplus_{i=1}^{2m} \mathbb{Z} e_i + \mathbb{Z} \left(\frac{1}{2} \sum_{i=1}^{2m} e_i \right),$$

первая ("ортогональная") промежуточная решетка Λ_1 имеет вид

$$\oplus_{i=1}^{2m} \mathbb{Z} e_i,$$

вторая ("полуспинорная") Λ_2 — вид

$$\oplus_{i=1}^{2m-1} \mathbb{Z}(e_i - e_{i+1}) \oplus \mathbb{Z}(e_{2m-1} + e_{2m}) + \mathbb{Z} \left(\frac{1}{2} \sum_{i=1}^{2m} e_i \right).$$

Предположим сначала, что мы имеем дело с группой типа D_{2m}, $m \geqslant 4$. Тогда мы можем рассмотреть (выделить формулой) такую инволюцию j, у которой фактор по центру коммутанта централизатора имеет тип $D_6 \times D_{2m-6}$ (например, это инволюция $h_{\alpha_1}(-1) h_{\alpha_3}(-1) h_{\alpha_5}(-1)$). Коммутант централизатора инволюции j есть центральное произведение группы типа D_6 на группу типа D_{2m-6}, при этом тип весовой решетки у подгруппы типа D_6 будет тем же, что и у изначальной группы (если изначально была ортогональная группа, то и подгруппа будет ортогональной, если изначально была полуспинорная группа, то и подгруппа будет полуспинорной). Поэтому перейдем к подгруппе типа D_6, будем определять ее тип решетки.

Пусть нам изначально дана группа G типа D_6 с промежуточной решеткой. Будем считать, что либо $G = G_1 = \mathrm{SO}_{12}(K)'$, либо $G = G_2$ — полуспинорная группа (которая есть фактор группы $Spin_{12}(K)$ по центральной подгруппе из 2 элементов).

У каждой из групп G_1, G_2 центр состоит из двух элементов и факторизация по центру дает присоединенную группу $\mathrm{PSO}_{12}(K)'$, уже изученную нами.

Подгруппа $H_1 = H(G_1)$ порождается элементами $h_{\alpha_1}(t_1), h_{\alpha_2}(t_2), h_{\alpha_3}(t_3), h_{\alpha_4}(t_4), h_{\alpha_5}(t_5)$, $h_{\alpha_6}(t_6)$ с соотношением $h_{\alpha_5}(-1) h_{\alpha_6}(-1) = 1$, а подгруппа $H_2 = H(G_2)$ порождается теми же элементами с соотношением

$$h_{\alpha_1}(-1) h_{\alpha_3}(-1) h_{\alpha_5}(-1) = 1.$$

В группе $\mathrm{PSO}_{12}(K)$ при $i \notin K$ в подгруппе H имеется 16 инволюций, которые порождаются элементами $h_{\alpha_1}(-1), h_{\alpha_2}(-1), h_{\alpha_3}(-1), h_{\alpha_4}(-1)$. Максимальное же множество коммутирующих между собой инволюций состоит из 2^9 инволюций, которые порождаются перечисленными элементами, а также элементами $w_{e_1-e_2} w_{e_1+e_2}$, $w_{e_2-e_3} w_{e_2+e_3}$, $w_{e_3-e_4} w_{e_3+e_4}$,

$w_{e_4-e_5}w_{e_4+e_5}$, $w_{e_5-e_6}w_{e_5+e_6} = w_{\alpha_5}w_{\alpha_6}$. Если к тому же $i \in K$, то добавляется еще коммутирующая со всеми перечисленными элементами инволюция $h_{\alpha_5}(i)h_{\alpha_6}(i)$, и становится множество из 2^{10} (больше в группе $\mathrm{PSO}_{12}(K)$ никак не может быть!) инволюций.

Теперь заметим, что в группе $G_1 = \mathrm{SO}_{12}(K)$ прообразы этих инволюций также остаются инволюциями, так как в этой группе по-прежнему выполняется соотношение $h_{e_i-e_{i+1}}(-1) = h_{e_i+e_{i+1}}(-1)$, $i = 1, \ldots, 5$. Кроме того, добавляется центральная инволюция

$$-1 = h_{\alpha_1}(-1)h_{\alpha_3}(-1)h_{\alpha_5}(-1).$$

В полуспинорной группе G_2 соотношение $h_{e_i-e_{i+1}}(-1) = h_{e_i+e_{i+1}}(-1)$ перестает выполняться, поэтому $(w_{e_i-e_{i+1}}w_{e_i+e_{i+1}})^2 = h_{e_i-e_{i+1}}(-1)h_{e_i+e_{i+1}}(-1) \neq 1$. Аналогично, $(h_{\alpha_5}(i)h_{\alpha_6}(i))^2 = h_{\alpha_5}(-1)h_{\alpha_6}(-1) \neq 1$. Таким образом, прообразы только 16 инволюций из присоединенной группы являются инволюциями в полуспинорной группе.

Таким образом, легко пишется предложение, различающее группы G_1 и G_2, то есть они не являются элементарно эквивалентными.

Значит, у элементарно эквивалентных групп Шевалле решетки весов совпадают. □

Из теоремы 2.4 и предложений 2.2, 2.3, 2.4, 2.5 следует основная теорема для полей:

Теорема 2.5. *Пусть $G = G_\pi(\Phi, K)$ и $G' = G_{\pi'}(\Phi', K')$ (или $E_\pi(\Phi, K)$ и $E_{\pi'}(\Phi', K')$) — две (элементарные) группы Шевалле над бесконечными полями K и K' характеристики, отличной от двух, с решетками весов Λ и Λ' соответственно. Тогда группы G и G' элементарно эквивалентны тогда и только тогда, когда системы корней Φ и Φ' изоморфны, поля K и K' элементарно эквивалентны, решетки Λ и Λ' совпадают.*

Теперь, когда теорема для полей доказана, с помощью нее докажем основную теорему для локальных колец (теорему 2.2).

2.13 Факторизация для локальных колец

Так как радикал J является единственным максимальным (т.е. наибольшим собственным) идеалом кольца R, то подгруппа $E_J = E_{\mathrm{ad}}(\Phi, R, J)$, порожденная элементами $x_\alpha(t)$, $t \in J$, является наибольшей собственной нормальной подгруппой группы $E = E_{\mathrm{ad}}(\Phi, R)$ (см. [70]).

Таким образом, если мы сможем показать, что подгруппа E_J определима в группе E, то, профакторизовав E по E_J, мы получим группу $\widetilde{E} \cong E_{\mathrm{ad}}(R/J)$, т.е. группу Шевалле над полем, и после этого сможем сослаться на доказанные в предыдущем параграфе результаты по элементарной эквивалентности групп Шевалле над полями.

Предложение 2.6. *Подгруппа $E_J = E_{\mathrm{ad}}(\Phi, R, J)$ определима в группе $E = E_{\mathrm{ad}}(\Phi, R)$.*

Доказательство. Рассмотрим в группе E элементы A, удовлетворяющие формуле

$$NoInv_N(A) := \bigwedge_{i,j=0}^{N} \forall X_1 \dots \forall X_i \forall Y_1 \dots \forall Y_j$$

$$(\bigvee_{k=0}^{N} \exists Z_1 \dots \exists Z_k ((1 \cdot X_1 A X_1^{-1} \dots X_i A X_i^{-1}) \cdot (1 \cdot Y_1 A Y_1^{-1} \dots Y_j A Y_j^{-1}) = (1 \cdot Z_1 A Z_1^{-1} \dots Z_k A Z_k^{-1})) \wedge$$

$$(\text{элементы } X_1 A X_1^{-1} \dots X_k A X_k^{-1} \text{ для } k \leqslant N \text{ образуют подгруппу в } E) \wedge$$

$$\wedge \bigwedge_{i=0}^{N} \forall X_1 \dots \forall X_i \forall X (\bigvee_{k=0}^{N} \exists Z_1 \dots \exists Z_k (X(X_1 A X_1^{-1} \dots$$

$$\dots X_i A X_i^{-1}) X^{-1} = Z_1 A Z_1^{-1} \dots Z_k A Z_k^{-1}) \wedge$$

$$\wedge \exists X (\bigwedge_{i=0}^{N} \forall X_1 \dots \forall X_i (X \neq X_1 A X_1^{-1} \dots X_i A X_i^{-1}))$$

$$(\text{эта подгруппа нормальна и не совпадает со всей группой } E).$$

Если для данного элемента A и некоторого N эта формула истинна, то это означает, что минимальная нормальная подгруппа группы E, содержащая элемент A, является собственной подгруппой в E. Как мы знаем, любая собственная нормальная подгруппа в E содержится в E_J, откуда следует, что $A \in E_J$.

С другой стороны, для любого $A = x_\alpha(u), u \in J$, $\alpha \in \Phi$, формула $NoInv_N(A)$ истинна для некоторого достаточно большого N (которое можно выбрать единым для данной системы корней).

Зафиксируем такое минимальное натуральное число N, что если для некоторого A не выполняется предложение $NoInv_N(A)$, то для этого A не будет выполнено и никакое предложение $NoInv_p(A)$, $p > N$.

Теперь рассмотрим M такое, что в нашей группе истинно предложение

$$Norm_{M,N} := \bigwedge_{i,j=0}^{M} \forall X_1 \dots \forall X_i \forall Y_1 \dots \forall Y_j \ (Noinv_N(X_1) \wedge \dots \wedge Noinv_N(X_i) \wedge$$

$$\wedge Noinv_N(Y_1) \wedge \dots \wedge Noinv_N(Y_j) \Rightarrow \bigvee_{k=0}^{M} \exists Z_1 \dots \exists Z_k (NoInv_N(Z_1) \wedge \dots \wedge$$

$$\wedge NoInv_N(Z_k) \wedge X_1 \dots X_i Y_1 \dots Y_j = Z_1 \dots Z_k)) \wedge$$

$$(\text{произведения } X_1 \dots X_k,\ k \leqslant M \text{ элементов группы } E,$$

$$\text{удовлетворяющие формуле } NoInv_N(X), \text{ образуют подгруппу в } E)$$

$$\wedge \bigwedge_{i=0}^{M} \forall X_1 \dots \forall X_i \forall X (NoInv_N(X_1) \wedge \dots \wedge NoInv_N(X_i) \Rightarrow$$
$$\Rightarrow \bigvee_{j=0}^{M} \exists Y_1 \dots \exists Y_j (NoInv_N(Y_1) \wedge \dots \wedge NoInv_N(Y_j) \wedge$$
$$\wedge X(X_1 \dots X_i)X^{-1} = Y_1 \dots Y_j))$$

(эта подгруппа нормальна)

$$\wedge \exists X_1 \exists X_2 (NoInv_N(X_1) \wedge NoInv_N(X_2) \wedge X_1 \neq X_2)$$

(эта подгруппа нетривиальна)

$$\wedge \exists X (\bigwedge_{i=0}^{M} \forall X_1 \dots \forall X_i (NoInv_N(X_1) \wedge \dots \wedge NoInv_N(X_i) \Rightarrow X \neq X_1 \dots X_i))$$

(эта подгруппа не совпадает со всей группой).

С помощью этой формулы мы находим число M такое, что каждый элемент группы E_J порождается не более чем M элементами $x_\alpha(u)$, $u \in J$.

Теперь формула

$$Normal_{M,N}(X) := \bigwedge_{i=0}^{M} \exists X_1 \dots \exists X_i (NoInv_N(X_1) \wedge \dots \wedge NoInv_N(X_i) \wedge X = X_1 \dots X_i)$$

выделяет в группе E подгруппу E_J. □

На данный момент мы получаем следующую импликацию:

$$G_\pi(\Phi, R) \equiv G_{\pi'}(\Phi', R') \Longrightarrow E_\pi(\Phi, R) \equiv E_{\pi'}(\Phi', R') \Longrightarrow$$
$$\Longrightarrow E_{\mathrm{ad}}(\Phi, R) \equiv E_{\mathrm{ad}}(\Phi', R') \Longrightarrow E_{\mathrm{ad}}(\Phi, R/J) \equiv E_{\mathrm{ad}}(\Phi', R'/J') \Longrightarrow \Phi \equiv \Phi'.$$

Последняя импликация следует из основной теоремы для полей.

Теперь мы можем всегда считать, что система корней группы Шевалле известна.

2.14 Формулы для разложения Гаусса групп Шевалле

Напомним, что мы имеем систему корней Φ ранга, большего единицы. Множество простых корней будем обозначать через Δ, положительных — через Φ^+. Подгруппа $U = U(R)$ группы Шевалле G (E) порождается элементами $x_\alpha(t)$, $\alpha \in \Phi^+$, $t \in R$, подгруппа $V = V(R)$ — элементами $x_{-\alpha}(t)$, $\alpha \in \Phi^+$ $t \in R$.

Для обратимых $t \in R^*$ через $w_\alpha(t)$ обозначается элемент $x_\alpha(t)x_{-\alpha}(-t^{-1})x_\alpha(t)$, через $h_\alpha(t)$ — элемент $w_\alpha(t)w_\alpha(1)^{-1}$.

Группа $H = H(R)$ порождается всеми $h_\alpha(t)$, $\alpha \in \Phi$, $t \in R^*$.

Предложение 2.7. (1) *Любой элемент x группы Шевалле $G\ (E)$ над локальным кольцом R представляется в виде*

$$x = utvu' \quad (x = uhvu'),$$

где $u, u' \in U(R)$, $v \in V(R)$, $t \in T(R)$, $h \in H(R)$;

(2) *Для разложений $x_1 = u_1t_1v_1u_1'$ и $x_2 = u_2t_2v_2u_2'$, где*

$$\begin{aligned}
u_i &= x_{\alpha_1}(t_1^{(i)}) \dots x_{\alpha_n}(t_n^{(i)}),\\
u_i' &= x_{\alpha_1}(s_1^{(i)}) \dots x_{\alpha_n}(s_n^{(i)}),\\
v_i &= x_{-\alpha_1}(r_1^{(i)}) \dots x_{-\alpha_n}(r_n^{(i)}),\\
t_i &= h_{\alpha_1}(\xi_1^{(i)}) \dots h_{\alpha_l}(\xi_l^{(i)}), \quad i = 1, 2,
\end{aligned}$$

существует формула первого порядка кольцевого языка

$$\varphi(t_1^{(1)}, \dots, t_n^{(1)}, t_1^{(2)}, \dots, t_n^{(2)}, s_1^{(1)}, \dots, s_n^{(1)}, s_1^{(2)}, \dots, s_n^{(2)},\\
r_1^{(1)}, \dots, r_n^{(1)}, r_1^{(2)}, \dots, r_n^{(2)}, \xi_1^{(1)}, \dots, \xi_n^{(1)}, \xi_1^{(2)}, \dots, \xi_n^{(2)}),$$

истинная тогда и только тогда, когда

$$x_1 = x_2;$$

(3) *Аналогично, для разложений $x_1 = u_1t_1v_1u_1'$, $x_2 = u_2t_2v_2u_2'$ и $x_3 = u_3t_3v_3u_3'$, где*

$$\begin{aligned}
u_i &= x_{\alpha_1}(t_1^{(i)}) \dots x_{\alpha_n}(t_n^{(i)}),\\
u_i' &= x_{\alpha_1}(s_1^{(i)}) \dots x_{\alpha_n}(s_n^{(i)}),\\
v_i &= x_{-\alpha_1}(r_1^{(i)}) \dots x_{-\alpha_n}(r_n^{(i)}),\\
t_i &= h_{\alpha_1}(\xi_1^{(i)}) \dots h_{\alpha_l}(\xi_l^{(i)}), \quad i = 1, 2, 3,
\end{aligned}$$

существует формула первого порядка кольцевого языка

$$\psi(t_1^{(i)}, \dots, t_n^{(i)}, s_1^{(i)}, \dots, s_n^{(i)}, r_1^{(i)}, \dots, r_n^{(i)}, \xi_1^{(i)}, \dots, \xi_n^{(i)}),$$

истинная тогда и только тогда, когда

$$x_3 = x_1 \cdot x_2.$$

Доказательство. (1) Нам достаточно доказать, что

$$TUVUx_\alpha(t) \in TUVU \quad \forall \alpha \in \Phi^*, \forall t \in R, \tag{2.1}$$

$$TUVUh(\chi) \in TUVU \quad \forall h(\chi) \in T, \tag{2.2}$$

$$TUVUx_{-\alpha}(\pm 1) \in TUVU \quad \forall \alpha \in \Delta, \tag{2.3}$$

так как

$$x_{-\alpha}(t) = w_\alpha(\pm 1)x_\alpha(t)w_\alpha(\pm 1)^{-1} = x_\alpha(\pm 1)x_{-\alpha}(\mp 1)x_\alpha(\pm 1)x_\alpha(t)x_\alpha(\mp 1)x_{-\alpha}(\pm 1)x_\alpha(\mp 1),$$

и при этом $w_\alpha(1) = w_{\alpha_{i_1}}(1)\dots w_{\alpha_{i_k}}(1)$, где $\alpha_{i_1},\dots,\alpha_{i_k} \in \Delta$.

Равенство (2.1) совершенно очевидно следует из того, что $Ux_\alpha(t) \subset U$, $\forall \alpha \in \Phi^+$, $\forall t \in R$.

Равенство (2.2) следует из того, что

$$h(\chi)x_\alpha(t)h(\chi)^{-1} = x_\alpha(\chi(\alpha)t).$$

Остается доказать равенство (2.3).

Без ограничения общности мы можем считать, что $\alpha = \alpha_1 \in \Delta = \{\alpha_1,\dots,\alpha_l\}$. Тогда

$$\begin{aligned}h(\chi)x_{\alpha_1}(t_1)\dots x_{\alpha_n}(t_n)x_{-\alpha_1}(r_1)\dots x_{-\alpha_n}(r_n)x_{\alpha_1}(s_1)\dots x_{\alpha_n}(s_n)x_{-\alpha_1}(1) =\\ = h(\chi)x_{\alpha_1}(t_1)\dots x_{\alpha_n}(t_n)x_{-\alpha_1}(r_1)\dots x_{-\alpha_n}(r_n)x_{\alpha_1}(s_1)x_{-\alpha_1}(1)x_{\alpha_2}(s_2')\dots x_{\alpha_n}(s_n'),\end{aligned}$$

где $s_2',\dots,s_n'$ — это многочлены с целыми коэффициентами от $s_2,\dots,s_n$.

Если $1+s_1 \in R^*$, то равенство продолжается так:

$$\begin{aligned}&= h(\chi)x_{\alpha_1}(t_1)\dots x_{\alpha_n}(t_n)x_{-\alpha_1}(r_1)\dots x_{-\alpha_n}(r_n)x_{-\alpha_1}(\mu)h_{\alpha_1}(\eta)x_{\alpha_1}(s_1')\dots\dots x_{\alpha_n}(s_n') =\\ &(\mu,\eta,s_1' \text{ — многочлены Лорана от } s_1) =\\ &= h'(\chi)x_{\alpha_1}(t_1')\dots x_{\alpha_n}(t_n')x_{-\alpha_1}(r_1')\dots x_{-\alpha_n}(r_n')x_{\alpha_1}(s_1')\dots x_{\alpha_n}(s_n'),\end{aligned}$$

где все элементы в скобках являются многочленами Лорана (с целыми коэффициентами) от старых.

Если $1+s_1 \notin R^*$, то $s_1 \in R^*$,

$$\begin{aligned}x_{\alpha_1}(s_1)x_{-\alpha_1}(1) = x_{\alpha_1}(1+s_1)x_{\alpha_1}(-1)x_{-\alpha_1}(1)x_{\alpha_1}(-1)x_{\alpha_1}(1) =\\ = x_{\alpha_1}(1+s_1)w_{\alpha_1}(-1)x_{\alpha_1}(1) = w_{\alpha_1}(-1)x_{-\alpha_1}(-1-s_1)x_{\alpha_1}(1).\end{aligned}$$

Тогда наше равенство продолжается так:

$$\begin{aligned}h(\chi)x_{\alpha_1}(t_1)\dots x_{\alpha_n}(t_n)x_{-\alpha_1}(r_1)\dots x_{-\alpha_n}(r_n)w_{\alpha_1}(-1)x_{-\alpha_1}(-1-s_1)x_{\alpha_1}(1)x_{\alpha_2}(s_2')\dots x_{\alpha_n}(s_n') =\\ = h(\chi)x_{\alpha_2}(t_2')\dots x_{\alpha_n}(t_n')x_{\alpha_1}(t_1)x_{-\alpha_1}(r_1)\dots x_{-\alpha_n}(r_n)w_{\alpha_1}(-1)x_{-\alpha_1}(1)x_{\alpha_2}(s_2')\dots x_{\alpha_n}(s_n').\end{aligned}$$

Теперь воспользуемся равенством

$$x_{\alpha_1}(t_1)x_{-\alpha_1}(r_1) = x_{\alpha_1}(1+t_1)x_{-\alpha_1}(1)x_{\alpha_1}(1-r_1)w_{\alpha_1}(1).$$

Получим продолжение

$$\begin{aligned}&= h(\chi)x_{\alpha_2}(t_2')\dots x_{\alpha_n}(t_n')x_{\alpha_1}(1+t_1)x_{-\alpha_1}(1)x_{\alpha_1}(1-r_1)w_{\alpha_1}(1)x_{-\alpha_2}(r_2)\dots x_{-\alpha_n}(r_n)\cdot\\ &\cdot w_{\alpha_1}(-1)x_{-\alpha_1}(-1-s_1)x_{\alpha_1}(1)x_{\alpha_2}(s_2')\dots x_{\alpha_n}(s_n') =\\ &= h(\chi)x_{\alpha_1}(t_1'')\dots x_{\alpha_n}(t_n'')x_{-\alpha_1}(1)x_{\alpha_1}(1-r_1)x_{-\alpha_2}(r_2')\dots x_{-\alpha_n}(r_n')\cdot\\ &\cdot x_{-\alpha_1}(-1-s_1)x_{\alpha_1}(1)x_{\alpha_2}(s_2')\dots x_{\alpha_n}(s_n') =\\ &h'(\chi)x_{\alpha_1}(\bar t_1)\dots x_{\alpha_n}(\bar t_n)x_{-\alpha_1}(\bar r_1)\dots x_{-\alpha_n}(\bar r_n)x_{\alpha_1}(\bar s_1)\dots x_{\alpha_n}(\bar s_n),\end{aligned}$$

где все новые параметры являются рациональными функциями с целыми коэффициентами от старых параметров.

Таким образом, пункт (1) доказан.

(2) и (3). Пусть для $\alpha \in \Phi^+$, $\alpha = \alpha_i$

$$\psi^{\alpha,+}(t_1, \dots, t_n, r_1, \dots, r_n, s_1, \dots, s_n, \xi_1, \dots, \xi_n; \bar{t}_1, \dots, \bar{t}_n, \bar{r}_1, \dots, \bar{r}_n, \bar{s}_1, \dots, \bar{s}_n, \bar{\xi}_1, \dots, \bar{\xi}_l; t)$$

— это формула

$$t_1 = \bar{t}_1 \wedge \dots \wedge t_n = \bar{t}_n \wedge r_1 = \bar{r}_1 \wedge \dots \wedge r_n = \bar{r}_n \wedge \\ \wedge \xi_1 = \bar{\xi}_1 \wedge \dots \wedge \xi_l = \bar{\xi}_l \wedge \eta^{\alpha,+}(s_1, \dots, s_n; \bar{s}_1, \dots, \bar{s}_n; t),$$

где формула

$$\eta^{\alpha,+}(\dots) = \eta_1^{\alpha,+}(s_1, \dots, s_n, \bar{s}_1, t) \wedge \dots \wedge \eta_n^{\alpha,+}(s_1, \dots, s_n, \bar{s}_n, t),$$

формула $\eta_j^{\alpha_i,+}(s_1, \dots, s_n, \bar{s}_j, t)$ имеет вид $s_j = p(s_1, \dots, s_n, t)$, p — многочлен от $n+1$ переменной с целыми коэффициентами такой, что эта формула истинна тогда и только тогда, когда

$$x_{\alpha_1}(s_1) \dots x_{\alpha_n}(s_n) x_{\alpha_i}(t) = x_{\alpha_1}(\dots) x_{\alpha_2}(\dots) \dots x_{\alpha_{j-1}}(\dots) x_{\alpha_j}(\bar{s}_j) x_{\alpha_{j+1}}(\dots) \dots x_{\alpha_n}(\dots).$$

Отсюда видно, что формула $\psi^{\alpha,+}(\dots)$ истинна тогда и только тогда, когда для

$$\bar{x} = h_{\bar{\xi}_1 \dots \bar{\xi}_l}(\chi) x_{\alpha_1}(\bar{t}_1) \dots x_{\alpha_n}(\bar{t}_n) x_{-\alpha_1}(\bar{r}_1) \dots x_{-\alpha_n}(\bar{r}_n) x_{\alpha_1}(\bar{s}_1) \dots x_{\alpha_n}(\bar{s}_n)$$

и для

$$x = h_{\xi_1 \dots \xi_l}(\chi) x_{\alpha_1}(t_1) \dots x_{\alpha_n}(t_n) x_{-\alpha_1}(r_1) \dots x_{-\alpha_n}(r_n) x_{\alpha_1}(s_1) \dots x_{\alpha_n}(s_n)$$

имеет место равенство

$$\bar{x} = x \cdot x_\alpha(t).$$

Теперь пусть мы имеем

$$h(\chi_{\lambda_1 \dots \lambda_l}) \in T(R).$$

Пусть формула

$$\psi^T(t_1, \dots, t_n, r_1, \dots, r_n, s_1, \dots, s_n, \xi_1, \dots, \xi_n; \\ \bar{t}_1, \dots, \bar{t}_n, \bar{r}_1, \dots, \bar{r}_n, \bar{s}_1, \dots, \bar{s}_n, \bar{\xi}_1, \dots, \bar{\xi}_l; \lambda_1, \dots, \lambda_l)$$

истинна для

$$\bar{x} = x \cdot h(\chi_{\lambda_1, \dots, \lambda_l}).$$

Она имеет вид

$$\bar{\xi}_1 = \xi_1 \cdot \lambda_1 \wedge \dots \wedge \bar{\xi}_l = \xi_l \cdot \lambda_l \wedge \\ \wedge \bar{t}_1 = \psi_{1,1}^T(t_1, \lambda_1, \dots, \lambda_l) \wedge \dots \bar{t}_n = \psi_{1,n}^T(t_n, \lambda_1, \dots, \lambda_l) \wedge \\ \wedge \bar{r}_1 = \psi_{2,1}^T(r_1, \lambda_1, \dots, \lambda_l) \wedge \dots \wedge \bar{r}_n = \psi_{2,n}^T(r_n, \lambda_1, \dots, \lambda_l) \wedge \\ \wedge \bar{s}_1 = \psi_{3,1}^T(s_1, \lambda_1, \dots, \lambda_l) \wedge \dots \wedge \psi_{3,n}^T(s_n, \lambda_1, \dots, \lambda_l),$$

где $\psi^T_{i,j}$ — многочлен (точнее, одночлен) Лорана с целыми коэффициентами от своих аргументов.

Наконец, для $x_{-\alpha_i}(1)$ и $x_{-\alpha_i}(-1)$ при $\alpha_i \in \Delta$ в доказательстве п. (1) мы показали, что существуют формулы $\psi^{i,1}(\dots)$ и $\psi^{i,-1}(\dots)$ от переменных

$$t_1,\dots,t_n,r_1,\dots,r_n,s_1,\dots,s_n,\xi_1,\dots,\xi_l,\overline{t}_1,\dots,\overline{t}_n,\overline{r}_1,\dots,\overline{r}_n,\overline{s}_1,\dots,\overline{s}_n,\overline{\xi}_1,\dots,\overline{\xi}_l,$$

истинные в случаях $\overline{x}=x\cdot x_{-\alpha_i}(1)$ и $\overline{x}=x\cdot x_{-\alpha_i}(-1)$ соответственно.

Построим теперь формулу $\psi^{w_i}(\dots)$, истинную при $\overline{x}=x\cdot w_{\alpha_i}$, $\alpha_i\in\Delta$.

Она строится так:

$$\begin{gathered}\psi^{w_i}(t_1,\dots,t_n,r_1,\dots,r_n,s_1,\dots,s_n,\xi_1,\dots,\xi_l,\\ \overline{t}_1,\dots,\overline{t}_n,\overline{r}_1,\dots,\overline{r}_n,\overline{s}_1,\dots,\overline{s}_n,\overline{\xi}_1,\dots,\xi_l)=\\ =\exists t'_1\dots t'_n,t''_1,\dots,t''_n,r'_1,\dots,r'_n,r''_1,\dots,r''_n,s'_1,\dots,s'_n,s''_1,\dots,s''_n\in R\\ \exists\xi'_1,\dots,\xi'_l,\xi''_1,\dots\xi''_l\in R^*\\ \psi^{\alpha_i,+}(t_1,\dots,t_n,r_1,\dots,r_n,s_1,\dots,s_n,\xi_1,\dots,\xi_l,\\ t'_1,\dots,t'_n,r'_1,\dots,r'_n,s'_1,\dots,s'_n,\xi'_1,\dots,\xi_l;1)\wedge\\ \wedge\,\psi^{i,-1}(t'_1,\dots,t'_n,r'_1,\dots,r'_n,s'_1,\dots,s'_n,\xi'_1,\dots,\xi'_l,t''_1,\dots,t''_n,r_1,\dots,r''_n,\\ \xi''_1,\dots,\xi''_l)\wedge\\ \wedge\,\psi^{\alpha_i,+}(t''_1,\dots,t''_n,r''_1,\dots,r''_n,s''_1,\dots,s''_n,\xi''_1,\dots,\xi''_l,\\ \overline{t}_1,\dots,\overline{t}_n,\overline{r}_1,\dots,\overline{r}_n,\overline{s}_1,\dots,\overline{s}_n,\overline{\xi}_1,\dots,\overline{\xi}_n;1).\end{gathered}$$

На групповом языке она утверждает

$$\exists x'\exists x''\ x'=x\cdot x_{\alpha_i}(1)\wedge x''=x'\cdot x_{-\alpha_i}(-1)\wedge\overline{x}=x''\cdot x_{\alpha_i}(1).$$

Если $\alpha\in\Phi^+\setminus\Delta$, то для того, чтобы построить формулу $\psi^{w_\alpha}(\dots)$, истинную при $\overline{x}=x\cdot w_\alpha$, разложим w_α в произведение простых отражений $w_\alpha=w_{i_1}\dots w_{i_k}$ и применим последовательно умножения на $w_{i_1},\dots,w_{i_k}$.

Теперь напишем формулу

$$\psi^{\alpha,-}(t_1,\dots,t_n,r_1,\dots,r_n,s_1,\dots,s_n,\xi_1,\dots,\xi_l,\overline{t}_1,\dots,\overline{t}_n,\overline{r}_1,\dots,\overline{r}_n,\overline{s}_1,\dots,\overline{s}_n,\overline{\xi}_1,\dots,\overline{\xi}_l;t),$$

истинную при

$$\overline{x}=x\cdot x_{-\alpha}(t).$$

Она имеет вид

$$\exists t'_1,\dots,t'_n,t''_1,\dots,t''_n,r'_1,\dots,r'_n,r''_1,\dots,r''_n,s'_1,\dots,s'_n,s''_1,\dots,s''_n\in R$$
$$\exists \xi'_1,\dots,\xi'_l,\xi''_1,\dots,\xi''_l\in R^*$$
$$\psi^{w_\alpha}(t_1,\dots,t_n,r_1,\dots,r_n,s_1,\dots,s_n,\xi_1,\dots,\xi_l,$$
$$t'_1,\dots,t'_n,r'_1,\dots,r'_n,s'_1,\dots,s'_n,\xi'_1,\dots,\xi'_l)\wedge$$
$$\wedge\,\psi^{\alpha,+}(t'_1,\dots,t'_n,r'_1,\dots,r'_n,s'_1,\dots,s'_n,\xi'_1,\dots,\xi'_l,$$
$$t''_1,\dots,t''_n,r''_1,\dots,r''_n,s''_1,\dots,s''_n,\xi''_1,\dots,\xi''_l;-t)\wedge$$
$$\psi^{w_\alpha}(t''_1,\dots,t''_n,r''_1,\dots,r''_n,s''_1,\dots,s''_n,\xi''_1,\dots,\xi''_l,$$
$$\bar t_1,\dots,\bar t_n,\bar r_1,\dots,\bar r_n,\bar s_1,\dots,\bar s_n,\bar\xi_1,\dots,\bar\xi_l).$$

Теперь мы легко можем написать формулу

$$\psi^{\otimes}(t_1,\dots,t_n,r_1,\dots,r_n,s_1,\dots,s_n,\xi_1,\dots,\xi_l,$$
$$\bar t_1,\dots,\bar t_n,\bar r_1,\dots,\bar r_n,\bar s_1,\dots,\bar s_n,\bar\xi_1,\dots,\bar\xi_l;t'_1,\dots,t'_n,r'_1,\dots,r'_n,s'_1,\dots,s'_n,\xi'_1,\dots,\xi'_l),$$

истинную при $\overline{x}=x\cdot x'$, в виде композиции полученных выше формул $\psi^{\alpha,+}$, $\psi^{\alpha,-}$, ψ^T.

Однако, так как запись элемента $x\in G$ в виде $x=tuvu'$ не единственна, мы получили формулу, которая будет истинна при $x_3=x_1{\cdot}x_2$ только для каких-то определенных записей для x_1,x_2,x_3.

Нам же требуется, чтобы параметры удовлетворяли формуле $\widetilde{\psi}^{\otimes}(\dots)$ тогда и только тогда, когда они определяли элементы $x_1,x_2,x_3\in G$ такие, что $x_3=x_1\cdot x_2$, то есть когда существуют параметры, определяющие x'_3 такое, что записи для x_3 и x'_3 определяют одни и те же элементы, и при этом

$$\psi^{\otimes}(x_1,x_2,x_3).$$

То, что два элемента x_1 и x_2 равны, означает, что $x_1\cdot x_2^{-1}=1$. Найдем формулу, выражающую

$$x=x_{\alpha_1}(t_1)\dots x_{\alpha_n}(t_n)h(\chi_{\xi_1\dots\xi_l})x_{-\alpha_1}(r_1)\dots x_{-\alpha_n}(r_n)x_{\alpha_1}(s_1)\dots x_{\alpha_n}(s_n)=1.$$

Пусть $utvu'=1$, где $u,u'\in U$, $t\in T$, $v\in V$.

Тогда $TV\ni tv=u^{-1}u'^{-1}\in U$. Так как $TV\cap U=1$, то $tv=1\wedge u'u=1$.

Пусть $\psi^U(t_1,\dots,t_n,t'_1,\dots,t'_n,\bar t_1,\dots\bar t_n)$ — это формула, истинная тогда и только тогда, когда

$$x_{\alpha_1}(\bar t_1)\dots x_{\alpha_n}(\bar t_n)=x_{\alpha_1}(t_1)\dots x_{\alpha_n}(t_n)x_{\alpha_1}(t'_1)\dots x_{\alpha_n}(t'_n).$$

Тогда формула, выражающая равенство x единице, имеет вид

$$\psi^{(1)}(t_1,\dots,t_n,\xi_1,\dots,\xi_l,r_1,\dots,r_n,s_1,\dots,s_n)=$$
$$=(\xi_1=1)\wedge\dots\wedge(\xi_l=1)\wedge r_1=1\wedge\dots\wedge r_n=1\wedge$$
$$\wedge\,\psi^u(t_1,\dots,t_n,s_1,\dots,s_n,1,\dots,1).$$

Чтобы найти обратный элемент к

$$x=x_{\alpha_1}(t_1)\dots x_{\alpha_n}(t_n)h(\chi_{\xi_1\dots\xi_l})x_{-\alpha_1}(r_1)\dots x_{-\alpha_n}(r_n)x_{\alpha_1}(s_1)\dots x_{\alpha_n}(s_n),$$

выразим в виде $UTVU$ элемент

$$
\begin{aligned}
x^{-1} = x_{\alpha_n}(-s_n)\dots x_{\alpha_1}(-s_1)x_{-\alpha_n}(-r_n)\dots x_{-\alpha_1}(-r_1)h(\chi_{\xi_1^{-1}\dots\xi_l^{-1}})\\
x_{\alpha_n}(-t_n)\dots x_{\alpha_1}(-t_1) =\\
= x_{\alpha_n}(-s_n)\dots x_{\alpha_1}(-s_1)h(\chi_{\xi_1^{-1}\dots\xi_l^{-1}})\\
x_{-\alpha_n}(-q_n(\xi_1,\dots,\xi_l)r_n)\dots x_{-\alpha_1}(-q_1(\xi_1\dots\xi_l)r_1)x_{\alpha_n}(-t_n)\dots x_{\alpha_1}(-t_1) =\\
= x_{\alpha_1}(p_1^+(-s_n,\dots,-s_1))\dots x_{\alpha_n}(p_n^+(-s_n,\dots,-s_1))h(\chi_{\xi_1^{-1},\dots,\xi_l^{-1}})\\
x_{-\alpha_1}(p_1^-(-q_n(\xi_1,\dots,\xi_l)r_n,\dots,-q_1(\xi_1,\dots,\xi_l)r_1)\dots\\
\dots x_{-\alpha_n}(p_n^-(-q_n(\xi_1,\dots,\xi_l)r_n,\dots,-q_1(\xi_1,\dots,\xi_l)r_1)\\
x_{\alpha_1}(p_1^+(-t_n,\dots,t_1))\dots x_{\alpha_n}(p_n^+(-t_n,\dots,-t_1)),
\end{aligned}
$$

где $p_1^+(\dots)$, $\dots$, $p_n^+(\dots)$, $p_1^-(\dots)$, $\dots$, $p_n^-(\dots)$ — многочлены от n переменных с целыми коэффициентами, $q_1(\dots),\dots,q_n(\dots)$ — одночлены Лорана от l переменных.

Таким образом, формула

$$
\begin{aligned}
\psi^{(-1)}(t_1,\dots,t_n,\xi_1,\dots,\xi_l,r_1,\dots,r_n,s_1,\dots,s_n,\\
t_1',\dots,t_n',\xi_1',\dots,\xi_l',r_1',\dots,r_n',s_1',\dots,s_n) :=\\
= (t_1' = p_1^+(-t_n,\dots,-t_1))\wedge\dots\wedge(t_n' = p_n^+(-t_n,\dots,-t_1))\wedge\\
\wedge(\xi_1' = \xi_1^{-1})\wedge\dots\wedge(\xi_l' = \xi_l^{-1})\wedge\\
\wedge(r_1' = p_1^-(-q_1(\xi_1,\dots,\xi_l)r_1,\dots,-q_n(\xi_1,\dots,\xi_l)r_n)\wedge\\
\wedge\dots\wedge(r_n' = p_n^-(-q_1(\xi_1,\dots,\xi_l)r_1,\dots,-q_n(\xi_1,\dots,\xi_l)r_n)\wedge\\
\wedge(s_1' = p_1^+(-s_n,\dots,-s_1)\wedge\dots\wedge s_n' = p_n^+(-s_n,\dots,-s_1)
\end{aligned}
$$

истинна тогда и только тогда, когда $x' = x^{-1}$.

Значит, искомая формула $\psi^{(=)}(\dots)$, истинная тогда и только тогда, когда $x = x'$, имеет вид

$$
\begin{aligned}
\psi^{(=)}(t_1,\dots,t_n,\xi_1,\dots,\xi_l,r_1,\dots,r_n,s_1,\dots,s_n,t_1',\dots,t_n',\xi_1',\dots,\xi_l',r_1',\dots,r_n',s_1',\dots,s_n') =\\
= \exists t_1'',\dots,t_n'',\bar t_1,\dots,\bar t_n,r_1'',\dots,r_n'',\bar r_1,\dots,\bar r_n,s_1'',\dots s_n'',\bar s_1,\dots,\bar s_n\in R\\
\exists\xi_1'',\dots,\xi_l'',\bar\xi_1,\dots,\bar\xi_l\in R^*\\
\psi^{(-1)}(t_1',\dots,t_n',\xi_1',\dots,\xi_l',r_1',\dots,r_n',s_1',\dots,s_n',t_1'',\dots,t_n'',\xi_1'',\dots,\xi_l'',r_1'',\dots,r_n'',s_1'',\dots,s_n'')\wedge\\
\wedge\psi^{\oplus}(t_1,\dots,t_n,\xi_1,\dots,\xi_l,r_1,\dots,r_n,s_1,\dots,s_n,\\
t_1',\dots,t_n',\xi_1',\dots\xi_l',r_1',\dots,r_n',s_1',\dots,s_n',\bar t_1,\dots,\bar t_n,\bar\xi_1,\dots,\bar\xi_l,\bar r_1,\dots,\bar r_n,\bar s_1,\dots,\bar s_n)\wedge\\
\wedge\psi^{(1)}(\bar t_1,\dots\bar t_n,\bar\xi_1,\dots,\bar\xi_l,\bar r_1,\dots,\bar r_n,\bar s_1,\dots\bar s_n).
\end{aligned}
$$

Таким образом, мы получим формулу для п. (2).

Теперь мы можем написать формулу для п. (3):

$$\begin{gathered}
\psi^{(\otimes)}(t_1,\dots,t_n,\xi_1,\dots,\xi_l,r_1,\dots,r_n,s_1,\dots,s_n,t'_1,\dots,t'_n,\xi'_1,\dots,\xi'_l,r'_1,\dots,r'_n,s'_1,\dots,s'_n\\
\bar t_1,\dots,\bar t_n,\bar\xi_1,\dots,\bar\xi_l,\bar r_1,\dots,\bar r_n,\bar s_1,\dots,\bar s_n)=\\
=\exists t''_1,\dots,t''_n,r''_1,\dots,r''_n,s''_1,\dots s''_n\in R\exists\xi''_1,\dots,\xi''_l\in R^*\\
\psi^{\otimes}(t_1,\dots,t_n,\xi_1,\dots,\xi_l,r_1,\dots,r_n,s_1,\dots,s_n,t'_1,\dots,t'_n,\xi'_1,\dots,\xi'_l,r'_1,\dots,r'_n,s'_1,\dots,s'_n,\\
t''_1,\dots,t''_n,\xi''_1,\dots,\xi''_l,r''_1,\dots,r''_n,s''_1,\dots,s''_n)\wedge\\
\wedge\,\psi^{(=)}(t''_1,\dots,t''_n,\xi''_1,\dots,\xi''_l,r''_1,\dots,r''_n,s''_1,\dots,s''_n,\\
\bar t_1,\dots,\bar t_n,\bar\xi_1,\dots,\bar\xi_l,\bar r_1,\dots,\bar r_n,\bar s_1,\dots,\bar s_n).
\end{gathered}$$

□

2.15 Элементарная эквивалентность базисных колец и окончание доказательства теоремы

Предположим, что мы имеем две элементарно эквивалентные элементарные присоединенные группы Шевалле E и E' одного и того же типа Φ (ранга, большего единицы) над локальными кольцами R и R' с обратимой двойкой (если $\Phi=G_2$, то еще и с обратимой тройкой).

Из результатов предыдущей главы следует, что если две такие группы изоморфны, то кольца R и R' изоморфны.

Если группы E и E' элементарно эквивалентны, то по теореме Кейслера–Шелаха (см. [28]) существует такой ультрафильтр D, что $\prod\limits_D E\cong\prod\limits_D E'$. Из предложения 2.7 следует, что $\prod\limits_D E_{\mathrm{ad}}(\Phi,R)\cong E_{\mathrm{ad}}(\Phi,\prod\limits_D R)$.

Таким образом, $E_{\mathrm{ad}}(\Phi,\prod\limits_D R)\cong E_{\mathrm{ad}}(\Phi,\prod\limits_D R')$. Значит, $\prod\limits_D R\cong\prod\limits_D R'$, откуда следует, что $R\equiv R'$.

Теперь соберем воедино все, что мы доказали, и получим наконец-то доказательство основной теоремы.

(1) Обратная импликация теоремы полностью доказана в § 1, даже для более общего класса колец.

Теперь пускай у нас имеется две элементарно эквивалентных группы Шевалле, удовлетворяющих всем перечисленным в теореме условиям. (2) То, что в этом случае системы корней изоморфны, доказано в § 13. (3) То, что в этом случае базисные кольца элементарно эквивалентны, доказано только что выше. (4) Изоморфизм весовых решеток следует из того, что по нашим группам над локальными кольцами мы можем с помощью факторизации по наибольшей нормальной подгруппе получить группы Шевалле над вычетными полями с теми же самыми весовыми решетками, что и изначальные группы. Тогда нужный нам результат будет следовать из аналогичного результата параграфа 12.

Основная теорема для локальных колец полностью доказана. □

Глава 3

Автоморфизмы и элементарная эквивалентность полугруппы обратимых матриц с неотрицательными элементами

В этой главе мы описываем автоморфизмы и элементарную эквивалентность полугрупп обратимых неотрицательных матриц над упорядоченными кольцами. Автоморфизмы такой полугруппы для линейно упорядоченного тела характеристики, отличной от двух, были описаны в работе [40] А.В. Михалевым и М.А. Шаталовой.

Во втором параграфе доказывается стандартность автоморфизмов для полугруппы обратимых неотрицательных матриц в случае, когда R — линейно упорядоченное ассоциативное кольцо с обратимой двойкой, размер матриц больше двух. Данный результат является совместным с А.В. Михалевым, он опубликован в работе [188].

В третьем параграфе показано, что две полугруппы неотрицательных обратимых матриц над линейно упорядоченным ассоциативным кольцом с обратимой двойкой элементарно эквивалентны тогда и только тогда, когда их размерности равны, а полукольца неотрицательных элементов исходных колец элементарно эквивалентны. Показана связь этой задачи с задачей описания автоморфизмов и изоморфизмов. Этот результат также является совместным с А.В. Михалевым, он опубликован в работе [190].

Автором совместно с П.П. Семеновым было получено описание автоморфизмов и элементарной эквивалентности для полугруппы неотрицательных обратимых матриц над частично упорядоченными коммутативными кольцами с обратимой двойкой и размерностью матриц, большей двух. Из-за того, что в частично упорядоченном кольце могут появляться делители нуля, сильно усложняется вид обратимых в рассматриваемой полугруппе матриц, поэтому доказательство становится существенно длиннее. Мы не помещаем доказательство этих результатов в данную работу, они опубликованы в работах [4] и [5].

3.1 Необходимые определения и понятия

Пусть R — ассоциативное кольцо с 1.

Определение 3.1. Кольцо R называется *частично упорядоченным* (*линейно упорядоченным*), если на нем задано отношение частичного (линейного) порядка $\leqslant$, удовлетворяющее следующим условиям:

1) $\forall x, y, z \in R (x \leqslant y \Rightarrow x + z \leqslant y + z)$;

2) $\forall x, y \in R (0 \leqslant x \wedge 0 \leqslant y \Rightarrow 0 \leqslant xy)$.

Мы будем рассматривать такие частично (линейно) упорядоченные кольца, в которых $1/2, 1/3 \geqslant 0$.

Множество ненулевых элементов x таких, что $x \geqslant 0$, обозначается через R_+.

В линейно упорядоченном кольце всегда $1 \in R_+$, так как в противном случае $-1 \in R_+ \Rightarrow 1 = (-1)(-1) \in R_+$, что невозможно.

Легко доказать по индукции, что в линейно упорядоченном кольце R имеет место $\operatorname{char} R = 0$.

Элементы множества R_+ называются *положительными*, а элементы множества $R_+ \cup \{0\}$ — *неотрицательными*.

Определение 3.2. Пусть R — частично (линейно) упорядоченное кольцо. Через $G_n(R)$ обозначается подполугруппа группы $\mathrm{GL}_n(R)$, состоящая из всех матриц с неотрицательными элементами.

Множество всех обратимых элементов кольца R обозначается через R^*. Если $1/2 \in R$, то множество R^* бесконечно, так как оно содержит все $1/2^n$ для $n \in \mathbb{N}$. Множество $R_+ \cap R^*$ обозначается через R_+^*. Если $1/2 \in R$, то оно также бесконечно.

Определение 3.3. Предположим, что R — частично (линейно) упорядоченное кольцо, $T \subset R$. Тогда $Z(T)$ обозначает центр множества T, $Z^*(T) = Z(T) \cap R^*$, $Z_+(T) = Z(T) \cap R_+$, $Z_+^*(T) = Z(T) \cap R_+^*$.

Ясно, что $Z_+^*(R) \subseteq Z_+^*(R^*)$. Если $1/2 \in R$, то все эти множества бесконечны для $T = R$.

Определение 3.4. Пусть $I = I_n$, $\Gamma_n(R)$ — группа, состоящая из всех обратимых матриц из $G_n(R)$, Σ_n — симметрическая группа порядка n, S_σ — матрица перестановки $\sigma \in \Sigma_n$ (т. е. матрица $(\delta_{i\sigma(j)})$, где $\delta_{i\sigma(j)}$ — символ Кронекера), $S_n = \{S_\sigma | \sigma \in \Sigma_n\}$, $\operatorname{diag}[d_1, \ldots, d_n]$ — диагональная матрица с элементами $d_1, \ldots, d_n$ на диагонали, $d_1, \ldots, d_n \in R_+^*$.

Определение 3.5. Через $D_n(R)$ обозначим группу всех обратимых диагональных матриц из $G_n(R)$, через $D_n^Z(R)$ — центр группы $D_n(R)$.

Ясно, что группа $D_n^Z(R)$ состоит из всех матриц $\operatorname{diag}[d_1, \ldots, d_n]$, $d_1, \ldots, d_n \in Z_+^*(R^*)$.

Определение 3.6. Если $\mathcal{A}, \mathcal{B}$ — подмножества в $G_n(R)$, то положим

$$C_{\mathcal{A}}(\mathcal{B}) = \{a \in \mathcal{A} | \forall b \in \mathcal{B}\ (ab = ba)\}.$$

Матрица $A \in \Gamma_n(R)$, удовлетворяющая условию $A^2 = I$, называется *инволюцией*.

Определение 3.7. Через $K_n(R)$ обозначим подполугруппу в $G_n(R)$, состоящую из всех матриц

$$\begin{pmatrix} X_{n-1} & 0 \\ 0 & x \end{pmatrix}, \quad X_{n-1} \in G_{n-1}(R),\ x \in R_+^*.$$

Пусть E_{ij} — матрица с единственным ненулевым элементом $e_{ij} = 1$.

Определение 3.8. Через $B_{ij}(x)$ обозначим матрицу $I + xE_{ij}$. Пусть $\mathbf{P}$ обозначает подполугруппу в $G_n(R)$, порожденную всеми матрицами S_σ $(\sigma \in \Sigma_n)$, $B_{ij}(x)$ $(x \in R_+, i \neq j)$ и $\mathrm{diag}\,[\alpha_1, \ldots, \alpha_n] \in D_n(R)$.

Определение 3.9. Две матрицы $A, B \in G_n(R)$ называются $\mathcal{P}$-эквивалентными, если существуют матрицы $A_j \in G_n(R)$, $j = 0, \ldots, k$, $A = A_0, B = A_k$, и матрицы $P_i, \widetilde{P}_i, Q_i, \widetilde{Q}_i \in \mathbf{P}$, $i = 0, \ldots, k-1$ такие, что $P_i A_i \widetilde{P}_i = Q_i A_{i+1} \widetilde{Q}_i$.

Определение 3.10. Через $\mathrm{GE}_n^+(R)$ обозначим подполугруппу в $G_n(R)$, порожденную всеми матрицами, $\mathcal{P}$-эквивалентными матрицам из $\mathbf{P}$.

Заметим, что если R — тело, то $\mathrm{GE}_n^+(R) = G_n(R)$.

Определение 3.11. Если G — некоторая полугруппа (например, $G = R_+^*, G_n(R)$, $\mathrm{GE}_n^+(R)$), то гомоморфизм $\lambda(\cdot) : G \to G$ называется центральным гомоморфизмом G, если $\lambda(G) \subset Z(G)$. Отображение $\Omega(\cdot) : G \to G$ такое, что $\forall X \in G$

$$\Omega(X) = \lambda(X) \cdot X,$$

где $\lambda(\cdot)$ — центральный гомоморфизм, называется центральной гомотетией.

Например, если $R = \mathbb{R}$ (поле действительных чисел), то гомоморфизм $\lambda(\cdot) : G_n(\mathbb{R}) \to G_n(\mathbb{R})$ такой, что $\forall A \in G_n(\mathbb{R})$ $\lambda(A) = |det\, A| \cdot I$, является центральной гомотетией, а отображение $\Omega(\cdot) : G_n(\mathbb{R}) \to G_n(\mathbb{R})$ такое, что $\forall A \in G_n(\mathbb{R})$ $\Omega(A) = |\det A| \cdot A$, является центральной гомотетией. Заметим, что центральная гомотетия $\Omega(\cdot)$ всегда является эндоморфизмом полугруппы G: $\forall X, Y \in G$ $\Omega(X)\Omega(Y) = \lambda(X)X \cdot \lambda(Y)Y = \lambda(X)\lambda(Y)X \cdot Y = \lambda(XY)XY = \Omega(XY)$.

Для каждой матрицы $M \in \Gamma_n(R)$ пусть Φ_M обозначает автоморфизм полугруппы $G_n(R)$ такой, что $\forall X \in G_n(R)$ $\Phi_M(X) = MXM^{-1}$.

Для каждого $y(\cdot) \in \mathrm{Aut}\,(R_+)$ через Φ^y обозначим автоморфизм полугруппы $G_n(R)$ такой, что $\forall X = (x_{ij}) \in G_n(R)$ $\Phi^y(X) = \Phi^y((x_{ij})) = (y(x_{ij}))$.

3.2 Автоморфизмы полугруппы неотрицательных обратимых матриц над линейно упорядоченными кольцами

Основным результатом этого параграфа является следующая

Теорема 3.1. *Пусть Φ — автоморфизм полугруппы $G_n(R)$, $n \geqslant 3$, $1/2 \in R$, кольцо R линейно упорядочено. Тогда на полугруппе $\mathrm{GE}_n^+(R)$ $\Phi = \Phi_M \Phi^c \Omega$, где $M \in \Gamma_n(R)$, $c(\cdot) \in \mathrm{Aut}\,(R_+)$, $\Omega(\cdot)$ — центральная гомотетия полугруппы $\mathrm{GE}_n^+(R)$.*

3.2.1 Построение автоморфизма Φ'

В этом параграфе мы предполагаем, что фиксирован некоторый автоморфизм $\Phi \in \mathrm{Aut}\,(G_n(R))$, где $n \geqslant 3$, $1/2 \in R$, и с помощью него мы строим новый автоморфизм $\Phi' \in \mathrm{Aut}\,(G_n(R))$ такой, что $\Phi' = \Phi_{M'}\Phi$ для некоторой матрицы $M' \in \Gamma_n(R)$ и для всех $\sigma \in \Sigma_n$ выполнено условие $\Phi'(S_\sigma) = S_\sigma$.

Следующая лемма (в бо́льшей общности) доказана в [40].

Лемма 3.1. $\Gamma_n(R) = D_n(R) \cdot S_n$, *т.е. группа* $\Gamma_n(R)$ *состоит из всех мономиальных матриц.*

Доказательство. Очевидно, что любая мономиальная матрица обратима, т.е. $D_n(R)S_n \subset \Gamma_n(R)$.

Теперь рассмотрим некоторую матрицу $A = (a_{ij}) \in \Gamma_n(R)$. Нам требуется показать, что в каждой ее строке (столбце) содержится ровно один ненулевой элемент. Предположим, что это не так, и i-я строка матрицы A содержит по крайней мере два ненулевых (т. е. положительных) элемента $a_{i,k}$ и $a_{i,j}$. Рассмотрим обратную матрицу $B = (b_{l,m})$. Ее k-ая строка — ненулевая, поэтому существует l такое, что $b_{k,l} > 0$. Значит,

$$\delta_{il} = a_{i,1}b_{1,l} + \cdots + a_{i,n}b_{n,l} \geqslant a_{i,k}b_{k,l} > 0,$$

и поэтому $i = l$.

Аналогично существует m такое, что $b_{j,m} > 0$, т. е. $i = m$. Таким образом, $l = m = i$. Значит, $b_{j,i} > 0$, $b_{k,i} > 0$.

Условие $I = BA$ влечет

$$\delta_{j,k} = b_{j,1}a_{1,k} + \cdots + b_{j,n}a_{n,k} \geq b_{j,i}a_{i,k} > 0.$$

Следовательно, $j = k$, что противоречит предположению о том, что i-ая строка содержит два ненулевых элемента. □

Заметим, что представление матрицы $A \in \Gamma_n(R)$ в виде $A = DS_\sigma$, $D \in D_n(R)$, $\sigma \in \Sigma_n$, единственно.

Лемма 3.2. *Если* $r \in R_+$ *и* $r^k = 1$ *для некоторого* $k \geqslant 1$, *то* $r = 1$.

Доказательство. Нам нужно показать, что из $x > 1$ следует $x^k > 1$, а из $0 < x < 1$ следует $0 < x^k < 1$.

1) Докажем по индукции, что

$$x > 1 \Rightarrow x^k > 1.$$

Если $k = 1$, то соотношение очевидно. Предположим, что наше соотношение доказано для некоторого k, т. е. $x > 1$, $x^k > 1$, откуда $x - 1 \in R_+$, $x^k - 1 \in R_+$, следовательно, $x^{k+1} - x \in R_+ \Rightarrow (x^{k+1} - x) + (x - 1) \in R_+ \Rightarrow x^{k+1} - 1 \in R_+ \Rightarrow x^{k+1} > 1$.

2) Аналогично докажем по индукции, что

$$0 < x < 1 \Rightarrow 0 < x^k < 1.$$

Если $k = 1$, то соотношение очевидно выполнено. Предположим, что наше соотношение доказано для некоторого k, т. е. $0 < x < 1 \Rightarrow 0 < x^k < 1$. Значит, $x, x^k, 1-x, 1-x^k \in R_+$, откуда $x(1-x^k) = x - x^{k+1} \in R_+ \Rightarrow (1-x) + (x - x^{k+1}) = 1 - x^{k+1} \in R_+$, т. е. $0 < x^{k+1} < 1$.

Таким образом, соотношение доказано. $\square$

Ясно, что в кольце R нет делителей нуля.

Доказательство следующей леммы можно найти в [40].

Лемма 3.3. *Если A — инволюция в полугруппе $G_n(R)$, то $A = diag[t_1, \ldots, t_n]S_\sigma$, где $\sigma^2 = 1$, и для любого $i = 1, \ldots, n$ выполнено $t_i \cdot t_{\sigma(i)} = 1$.*

Доказательство. По лемме 1 имеем $A = dS_\sigma$, где $d = \operatorname{diag}[d_1, \ldots, d_n]$. Так как $A^2 = I$, то $dS_\sigma dS_\sigma = I \Rightarrow dS_\sigma = S_\sigma^{-1} d^{-1} S_\sigma S_\sigma^{-1}$. Так как представление матрицы A в виде dS_σ единственно и $S_\sigma^{-1} d^{-1} S_\sigma \in D_n(R)$, то $d = S_\sigma^{-1} d^{-1} S_\sigma$ и $S_\sigma = S_\sigma^{-1}$.

Значит, $\sigma^2 = 1$ и $\operatorname{diag}[d_1, \ldots, d_n] = \operatorname{diag}[d_{\sigma(1)}^{-1}, \ldots, d_{\sigma(n)}^{-1}]$, т. е. $t_i = t_{\sigma(i)}^{-1}$. $\square$

Лемма 3.4. *Если Φ — автоморфизм полугруппы $G_n(R)$, где $n \geqslant 3$, $1/2 \in R$, то*

1) $\Phi(\Gamma_n(R)) = \Gamma_n(R)$,

2) $\Phi(D_n(R)) = D_n(R)$,

3) $\Phi(D_n^Z(R)) = D_n^Z(R)$.

Доказательство. 1) Так как $\Gamma_n(R)$ является подгруппой всех обратимых матриц полугруппы $G_n(R)$, то $\Phi(\Gamma_n(R)) = \Gamma_n(R)$.

2) Рассмотрим множество $\mathcal{F}$ всех матриц $A \in \Gamma_n(R)$, коммутирующих со всеми матрицами, сопряженными к A.

Рассмотрим

$$A = \operatorname{diag}[\alpha_1, \ldots, \alpha_n] \in D_n^Z(R),$$

тогда любая матрица, сопряженная к A, имеет вид

$$S_{\sigma^{-1}} \operatorname{diag}[d_1^{-1}, \ldots, d_n^{-1}] \operatorname{diag}[\alpha_1, \ldots, \alpha_n] \operatorname{diag}[d_1, \ldots, d_n] S_\sigma = \\ = S_{\sigma^{-1}} \operatorname{diag}[\alpha_1, \ldots, \alpha_n] S_\sigma = \operatorname{diag}[\alpha_{\sigma^{-1}(1)}, \ldots, \alpha_{\sigma^{-1}(n)}],$$

т. е. коммутирует с $A = \operatorname{diag}[\alpha_1, \ldots, \alpha_n]$.

Если мы рассмотрим

$$A = \operatorname{diag}[\alpha_1, \ldots, \alpha_n] \in D_n(R) \setminus D_n^Z(R),$$

то матрица, сопряженная к A, также диагональна, но невозможно сказать, коммутирует ли она с $A = \operatorname{diag}[\alpha_1, \ldots, \alpha_n]$.

Теперь рассмотрим

$$A = \operatorname{diag}[\alpha_1, \ldots, \alpha_n] S_\rho, \quad \rho \neq e, \ \alpha_1, \ldots, \alpha_n \in R_+^*.$$

Рассмотрим некоторую матрицу

$$M = \operatorname{diag}[d_1, \ldots, d_n] \in D_n^Z(R),$$

чтобы получить матрицу, сопряженную с A.

Имеем

$$\begin{aligned}M^{-1}AM =& \operatorname{diag}[d_1^{-1},\dots,d_n^{-1}]\operatorname{diag}[\alpha_1,\dots,\alpha_n]S_\rho \operatorname{diag}[d_1,\dots,d_n] = \\ &= \operatorname{diag}[d_{\rho^{-1}(1)}d_1^{-1}\alpha_1,\dots,d_{\rho^{-1}(n)}d_n^{-1}\alpha_n]S_\rho = \operatorname{diag}[\gamma_1\alpha_1,\dots,\gamma_n\alpha_n]S_\rho,\end{aligned}$$

где $\gamma_1,\dots,\gamma_n \in Z_+^*(R^*)$.

Имеем соотношения

$$\begin{aligned}A(M^{-1}AM) &= \operatorname{diag}[\gamma_{\rho^{-1}(1)}\alpha_1\alpha_{\rho^{-1}(1)},\dots,\gamma_{\rho^{-1}(n)}\alpha_n\alpha_{\rho^{-1}(n)}]S_{\rho^2},\\ (M^{-1}AM)A &= \operatorname{diag}[\gamma_1\alpha_1\alpha_{\rho^{-1}(1)},\dots,\gamma_n\alpha_n\alpha_{\rho^{-1}(1)}]S_{\rho^2}.\end{aligned}$$

Так как $\rho \neq e$, то существует такое $i \in \{1,\dots,n\}$, что $j = \rho^{-1}(i) \neq i$. В этом случае возьмем

$$d_k = \begin{cases} 2, & \text{если } k = j,\\ 1, & \text{если } k \neq j.\end{cases}$$

Таким образом, имеем

$$\gamma_k = \begin{cases} 2 & \text{если } k = i,\\ 1/2, & \text{если } k = j,\\ 1, & \text{если } k \neq i \text{ и } k \neq j.\end{cases}$$

Значит,

$$A(M^{-1}AM) \neq (M^{-1}AM)A.$$

Поэтому соотношение

$$(A \in \Gamma_n(R)) \wedge (\forall M \in \Gamma_n(R)\ (M^{-1}AM)A = A(M^{-1}AM))$$

выполняется для всех элементов из $D_n^Z(R)$, может выполняться для некоторых элементов из $D_n(R) \setminus D_n^Z(R)$ и никогда не выполняется для элементов из $\Gamma_n(R) \setminus D_n(R)$.

Ясно, что $\Phi(\mathcal{F}) = \mathcal{F}$.

Введем на множестве $\mathcal{F}$ дополнительное условие

$$(A \in \mathcal{F}) \wedge (\forall M \in \Gamma_n(R)\ (M \neq I \wedge M^{n!} = I \Rightarrow AM \neq MA)), \tag{3.1}$$

т.е. "A не коммутирует ни с одной неединичной матрицей конечного порядка".

Ясно, что если матрица $A \in D_n(R)$ содержит два ненулевых элемента на i-ом и j-ом местах диагонали, то она коммутирует с $S_{(i,j)}$.

Если $A \in D_n^Z(R)$ имеет различные собственные значения, то она удовлетворяет условию (1).

Кроме того, это условие может выполняться для некоторых матриц из $D_n(R) \setminus D_n^Z(R)$, но они также должны содержать различные собственные значения. Обозначим множество всех матриц, удовлетворяющих условию (1), через $\mathcal{L}$. Ясно, что $\Phi(\mathcal{L}) = \mathcal{L}$.

Рассмотрим множество

$$\mathcal{X} = \bigcup_{M \in \mathcal{L}} C_{\Gamma_n(R)}(M),$$

т. е. множество всех обратимых матриц, коммутирующих с некоторой матрицей из $\mathcal{L}$.

Покажем, что $\mathcal{X} = D_n(R)$.

Для того, чтобы доказать, что $\mathcal{X} \subset D_n(R)$, заметим, что каждая матрица $M \in \mathcal{L}$ имеет различные собственные значения, поэтому если $AM = MA$, то $A \in D_n(R)$.

Чтобы доказать $D_n(R) \subset \mathcal{X}$, рассмотрим матрицу

$$M = \operatorname{diag}[2, 2^2, \ldots, 2^n] \in D_n^Z(R).$$

Очевидно, что $M \in \mathcal{L}$ и $C_{\Gamma_n(R)}(M) = D_n(R)$. Так как $C_{\Gamma_n(R)}(M) \subset \mathcal{X}$, имеем $D_n(\mathcal{X}) \subset \mathcal{X}$.

Следовательно, $\mathcal{X} = D_n(R)$.

Ясно, что $\Phi(\mathcal{X}) = \mathcal{X}$. Значит, $\Phi(D_n(R)) = D_n(R)$.

3) Так как $C_{\Gamma_n(R)}(D_n(R)) = D_n^Z(R)$ и $\Phi(D_n(R)) = D_n(R)$, то имеем $\Phi(D_n^Z(R)) = D_n^Z(R)$. □

Лемма 3.5. *Если Φ является автоморфизмом полугруппы $G_n(R)$, $n \geqslant 3$, $1/2 \in R$, то существует матрица $M \in \Gamma_n(R)$ такая, что $\Phi_M \Phi(K_n(R)) = K_n(R)$, где для всех $X \in G_n(R)$*

$$\Phi_M(X) = MXM^{-1}.$$

Доказательство. Рассмотрим матрицу

$$A = \operatorname{diag}[\alpha, \ldots, \alpha, \beta] \in D_n^Z(R), \quad \alpha \neq \beta.$$

Предположим, что

$$B = \Phi(A) = \operatorname{diag}[\gamma_1, \ldots, \gamma_n] \in D_n^Z(R).$$

Ясно, что

$$C_{\Gamma_n(R)}(A)/D_n(R) \cong \Sigma_{n-1},$$

поэтому

$$\Phi(C_{\Gamma_n(R)}(A))/\Phi(D_n(R)) = C_{\Gamma_n(R)}(B)/D_n(R) \cong \Sigma_{n-1}.$$

Значит,

$$B = \operatorname{diag}[\gamma, \ldots, \gamma, \delta, \gamma, \ldots, \gamma], \quad \gamma \neq \delta.$$

Таким образом, существует перестановка $\sigma \in \Sigma_n$ такая, что

$$\widetilde{B} = S_\sigma B S_{\sigma^{-1}} = [\gamma, \ldots, \gamma, \delta].$$

Имеем $C_{G_n(R)}(A) \subseteq K$ и $C_{G_n(R)}(\widetilde{B}) \subseteq K$. Кроме того, существует такая матрица A (например, $\operatorname{diag}[1, \ldots, 1, 2]$), что $C_{G_n(R)}(A) = K_n(R)$, т. е.

$$K_n(R) = \bigcup_{A = \operatorname{diag}[\alpha,\ldots,\alpha,\beta] \in D_n^Z(R), \alpha \neq \beta} C_{G_n(R)}(A),$$

$$K_n(R) = \bigcup_{A = \operatorname{diag}[\alpha,\ldots,\alpha,\beta] \in D_n^Z(R), \alpha \neq \beta} C_{G_n(R)}(S_\sigma \Phi(A) S_\sigma^{-1}),$$

так как Φ — автоморфизм.

Рассмотрим $M = S_\sigma$, $\Phi' = \Phi_M \circ \Phi$. Для каждой матрицы $A = \operatorname{diag}[\alpha, \ldots, \alpha, \beta] \in D_n^Z(R)$, $\alpha \neq \beta$, имеем $\Phi'(A) = \operatorname{diag}[\gamma, \ldots, \gamma, \delta] \in D_n^Z(R)$, $\gamma \neq \delta$, и

$$\Phi'(K_n(R)) = \Phi'\left(\bigcup_{A=\operatorname{diag}[\alpha,\ldots,\alpha,\beta]\in D_n^Z(R),\alpha\neq\beta} C_{G_n(R)}(A)\right) =$$
$$= \bigcup_{A=\operatorname{diag}[\alpha,\ldots,\alpha,\beta]\in D_n^Z(R),\alpha\neq\beta} \Phi'(C_{G_n(R)}(A)) = \bigcup_{A=diag[\alpha,\ldots,\alpha,\beta]\in D_n^Z(R),\alpha\neq\beta} C_{G_n(R)}(\Phi'(A)) = K_n(R).$$

Значит, $\Phi_M\Phi(K_n(R)) = K_n(R)$. □

Лемма 3.6. *Если Φ является автоморфизмом группы $G_n(R)$, то по лемме 3.4, так как $\Phi(\Gamma_n(R)) = \Gamma_n(R)$, то для каждого $\sigma \in \Sigma_n$ мы имеем*

$$\Phi(S_\sigma) = D_\sigma S_{\varphi(\sigma)},$$

где $D_\sigma \in D_n(R)$. Полученное отображение $\varphi : \Sigma_n \to \Sigma_n$ является эндоморфизмом группы Σ_n.

Доказательство. Для всех $\sigma_1, \sigma_2 \in \Sigma_n$

$$\begin{aligned} \Phi(S_{\sigma_1} \cdot S_{\sigma_2}) &= \Phi(S_{\sigma_1\cdot\sigma_2}) = D_{\sigma_1\sigma_2} \cdot S_{\varphi(\sigma_1\sigma_2)}, \\ \Phi(S_{\sigma_1}) \cdot \Phi(S_{\sigma_2}) &= D_{\sigma_1} S_{\varphi(\sigma_1)} D_{\sigma_2} S_{\varphi(\sigma_2)} = D_{\sigma_1} \cdot D'_{\sigma_2} S_{\varphi(\sigma_1)\varphi(\sigma_2)}, \\ \Phi(S_{\sigma_1} \cdot S_{\sigma_2}) &= \Phi(S_{\sigma_1}) \cdot \Phi(S_{\sigma_2}), \end{aligned}$$

поэтому

$$\varphi(\sigma_1\sigma_2) = \varphi(\sigma_1)\varphi(\sigma_2).$$

Так как $\Phi(D_n(R)) = D_n(R)$ (см. лемму 4(2)), то имеем $\varphi \in Aut(\Sigma_n)$. Действительно, если $\sigma_1, \sigma_2 \in \Sigma_n$, $\sigma_1 \neq \sigma_2$, $\sigma = \varphi(\sigma_1) = \varphi(\sigma_2)$, то

$$\Phi(S_{\sigma_1}) = D_{\sigma_1} S_\sigma,\ \Phi(S_{\sigma_2}) = D_{\sigma_2} S_\sigma \Rightarrow \Phi(S_{\sigma_1} \cdot S_{\sigma_2^{-1}}) = D_{\sigma_1} S_\sigma S_{\sigma^{-1}} D_{\sigma_2}^{-1} \in D_n(R).$$

Таким образом, для некоторого $\rho \neq e$ имеем

$$\Phi(S_\rho) \in D_n(R),$$

но это невозможно. □

Доказательство следующей леммы совершенно аналогично доказательству предложения 10 из [40], поэтому мы не приводим его здесь.

Лемма 3.7. *Если Φ — автоморфизм полугруппы $G_n(R)$, $1/2 \in R$, $n \geq 3$, то существует матрица $M \in \Gamma_n(R)$ такая, что $\Phi_M\Phi(S_\sigma) = S_\sigma$ для всех $\sigma \in \Sigma_n$.*

3.2.2 Действие автоморфизма Φ' на диагональных матрицах

В предыдущем пункте по нашему автоморфизму Φ мы построили новый автоморфизм $\Phi' = \Phi_M \Phi$ такой, что $\Phi'(S_\sigma) = S_\sigma$ для всех $\sigma \in \Sigma_n$. Мы предположим, что такой автоморфизм Φ' фиксирован.

Лемма 3.8. *Если $n \geqslant 3$, $1/2 \in R$, автоморфизм $\Phi' \in \mathrm{Aut}\,(G_n(R))$ таков, что $\forall \sigma \in \Sigma_n$ $\Phi'(S_\sigma) = S_\sigma$, то для всех $\alpha, \beta \in R_+^*$ мы имеем*

$$\Phi'(\,\mathrm{diag}\,[\alpha, \beta, \dots, \beta]) = \,\mathrm{diag}\,[\gamma, \delta, \dots, \delta], \quad \gamma, \delta \in R_+^*.$$

Если $\alpha \neq \beta$, то $\gamma \neq \delta$. Если $\alpha, \beta \in Z_+^*(R^*)$, то $\gamma, \delta \in Z_+^*(R^*)$.

Доказательство. По лемме 3.4

$$\Phi'(\,\mathrm{diag}\,[\alpha, \beta, \dots, \beta]) = \,\mathrm{diag}\,[\gamma_1, \dots, \gamma_n].$$

Так как $\Phi'(S_{(i,i+1)}) = S_{(i,i+1)}$ для всех $i = 2, \dots, n-1$, то для всех $i = 2, \dots, n-1$ имеем

$$\Phi'(\,\mathrm{diag}\,[\alpha, \beta, \dots, \beta])\Phi'(S_{(i,i+1)}) = \Phi'(S_{(i,i+1)})\Phi'(\,\mathrm{diag}\,[\alpha, \beta, \dots, \beta]) \Rightarrow \\ \mathrm{diag}\,[\gamma_1, \dots, \gamma_n]S_{(i,i+1)} = S_{(i,i+1)}\,\mathrm{diag}\,[\gamma_1, \dots, \gamma_n] \Rightarrow \gamma_i = \gamma_{i+1}.$$

Таким образом, $\gamma_2 = \gamma_3 = \dots = \gamma_{n-1} = \gamma_n$ и мы можем считать, что

$$\Phi'(\,\mathrm{diag}\,[\alpha, \beta, \dots, \beta]) = \,\mathrm{diag}\,[\gamma, \delta, \dots, \delta].$$

Если $\alpha \neq \beta$, то

$$\mathrm{diag}\,[\alpha, \beta, \dots, \beta]S_{(1,2)} \neq S_{(1,2)}\,\mathrm{diag}\,[\alpha, \beta, \dots, \beta] \Rightarrow \\ \Rightarrow \,\mathrm{diag}\,[\gamma, \delta, \dots, \delta]S_{(1,2)} \neq S_{(1,2)}\,\mathrm{diag}\,[\gamma, \delta, \dots, \delta] \Rightarrow \gamma \neq \delta.$$

Если $\alpha, \beta \in Z^*(R^*)$, то $\mathrm{diag}\,[\alpha, \beta, \dots, \beta] \in D_n^Z(R)$, и по лемме 3.4(3) $\mathrm{diag}\,[\gamma, \delta, \dots, \delta] \in D_n^Z(R^*)$, откуда $\gamma, \delta \in Z^*(R^*)$. □

Лемма 3.9. *Если $n \geqslant 3$, $1/2 \in R$, автоморфизм $\Phi' \in \mathrm{Aut}\,(G_n(R)$ таков, что $\forall \sigma \in \Sigma_n$ $\Phi'(S_\sigma) = S_\sigma$, то для всех $X \in G_2(R)$ имеет место*

$$\Phi' \begin{pmatrix} X & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots\dots & & \ddots & \dots \\ 0 & \dots\dots & & 1 \end{pmatrix} = \begin{pmatrix} Y & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \dots\dots & & \ddots & \dots \\ 0 & \dots\dots & & a \end{pmatrix}, \qquad \text{где } Y \in G_2(R), a \in Z_+^*(R^*).$$

Доказательство. Аналогично доказательству леммы 3.8 можно доказать, что для любой матрицы

$$A = \,\mathrm{diag}\,[\alpha, \alpha, \beta, \dots, \beta] \in D_n(R), \quad \alpha \neq \beta,$$

имеет место
$$\Phi'(A) = \operatorname{diag}[\gamma, \gamma, \delta, \dots, \delta] \in D_n(R), \quad \gamma \neq \delta.$$
Рассмотрим теперь множество $\mathcal{L}$ всех инволюций вида
$$\operatorname{diag}[\xi, \xi^{-1}, 1, \dots, 1]S_{(1,2)}, \quad \xi \in R_+^*.$$
Для любой такой инволюции M имеем
$$N = \Phi'(M) = \Phi'(\operatorname{diag}[\xi, \xi^{-1}, 1, \dots, 1])S_{(1,2)}$$
и N является инволюцией. По лемме 3.3
$$N = \operatorname{diag}[\eta, \eta^{-1}, 1, \dots, 1]S_{(1,2)}.$$
Если $\xi \in Z_+^*(R^*)$, то $\eta \in Z_+^*(R^*)$, если $\xi \notin Z_+^*(R^*)$, то $\eta \notin Z_+^*(R^*)$. Мы видим, что $\Phi'(\mathcal{L}) = \mathcal{L}$.

Множество матриц вида
$$\operatorname{diag}[\alpha, \alpha, \beta, \dots, \beta], \quad \alpha, \beta \in R_+^*, \ \alpha \neq \beta$$
обозначается через $\mathcal{M}$. Мы знаем, что $\Phi'(\mathcal{M}) = \mathcal{M}$. Таким образом,
$$\Phi'(C_{\mathcal{M}}\mathcal{L}) = C_{\mathcal{M}}\mathcal{L},$$
т.е. для любого $\mu \in Z_+^*(R^*)$, $\eta \in R_+^*$ имеем
$$\Phi'(\operatorname{diag}[\mu, \mu, \eta, \dots, \eta]) = \operatorname{diag}[\mu', \mu', \eta', \dots, \eta'],$$
где $\mu' \in Z_+^*(R^*)$, $\eta' \in R_+^*$ и если $\eta \in R_+^* \setminus Z_+^*(R^*)$, то $\eta' \in R_+^* \setminus Z_+^*(R^*)$.

Через $\mathcal{Z}$ мы обозначим множество всех матриц
$$\alpha I = \operatorname{diag}[\alpha, \dots, \alpha], \quad \alpha \in Z_+^*(R^*).$$

Ясно, что $\Phi'(\mathcal{Z}) = \mathcal{Z}$.

Рассмотрим некоторую матрицу
$$A = \begin{pmatrix} X & 0 & & \\ 0 & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}, \quad X \in G_2(R), a \in Z_+^*(R^*).$$
Эта матрица удовлетворяет условию
$$\forall M \in C_{\mathcal{M}}\mathcal{L} \ \exists N \in \mathcal{Z} \ A(MN) = (MN)A \wedge \\ \wedge AS_{(3,4)} = S_{(3,4)}A \wedge \dots \wedge AS_{(n-1,n)} = S_{(n-1,n)}A. \quad (3.2)$$
Действительно, любая матрица $M \in C_{\mathcal{M}}\mathcal{L}$ имеет вид
$$M = \operatorname{diag}[\mu, \mu, \eta, \dots, \eta], \quad \mu \in Z_+^*(R^*), \eta \in R_+^*.$$

Если $MA = AM$, то мы можем взять $N = I$. Если $MA \neq AM$, т.е. $\mu \in Z_+^*(R^*) \setminus Z_+^*(R)$ и $X \operatorname{diag}[\mu, \mu] \neq \operatorname{diag}[\mu, \mu]X$, то мы можем взять

$$N = \operatorname{diag}[\mu^{-1}, \dots, \mu^{-1}] \in \mathcal{Z}.$$

Тогда $MN = \operatorname{diag}[1, 1, \eta\mu^{-1}, \dots, \eta\mu^{-1}]$ и $A(MN) = (MN)A$.

Если некоторая матрица A удовлетворяет условию (2), то часть

$$AS_{(3,4)} = S_{(3,4)}A \wedge \dots \wedge AS_{(n-1,n)} = S_{(n-1,n)}A$$

влечет

$$A = \begin{pmatrix} X & 0 & & \\ 0 & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}, \quad X \in G_2(R), a \in R_+^*.$$

Если $a \in R_+^* \setminus Z_+^*(R^*)$, то существует элемент $b \in R_+^*$ такой, что $ab \neq ba$, значит, для

$$M = \operatorname{diag}[1, 1, b, \dots, b] \in C_{\mathcal{M}}\mathcal{L}$$

имеем $MA \neq AM$. Для каждой матрицы $N = \operatorname{diag}[\alpha, \dots, \alpha] \in \mathcal{Z}$ имеем $A(MN) \neq (MN)A$, так как $ab\alpha \neq b\alpha a$. Значит, матрица

$$A = \begin{pmatrix} X & 0 & & \\ 0 & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}$$

с $a \in R_+^* \setminus Z_+^*(R^*)$ не может удовлетворять условию (2). Значит, мы имеем $a \in Z_+^*(R^*)$.

Таким образом, мы видим, что матрица A имеет вид

$$A = \begin{pmatrix} X & 0 & & \\ 0 & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}, \quad X \in G_2(R), a \in Z_+^*(R^*)$$

тогда и только тогда, когда она удовлетворяет условию (2).

Так как $\Phi'(S_{(i,i+1)}) = S_{(i,i+1)}$ для всех $i = 3, \dots, n-1$, $\Phi'(\mathcal{Z}) = \mathcal{Z}$, $\Phi'(C_{\mathcal{M}}\mathcal{L}) = C_{\mathcal{M}}\mathcal{M}$, мы получаем, что если матрица A удовлетворяет (2), то и матрица $\Phi'(A)$ удовлетворяет (2).

Следовательно, для $X \in G_2(R)$, $a \in Z_+^*(R^*)$ имеем

$$\Phi' \begin{pmatrix} X & 0 & & \\ 0 & a & & \\ & & \ddots & \\ & & & a \end{pmatrix} = \begin{pmatrix} Y & 0 & & \\ 0 & b & & \\ & & \ddots & \\ & & & b \end{pmatrix}, \quad Y \in G_2(R), b \in Z_+^*(R^*).$$

$\square$

Лемма 3.10. *Если $n \geqslant 3$, $1/2 \in R$, автоморфизм $\Phi' \in \mathrm{Aut}\,(G_n(R))$ таков, что $\forall \sigma \in \Sigma_n$ $\Phi'(S_\sigma) = S_\sigma$, то для всех $x \in Z_+^*(R)$*

$$\Phi'(\,\mathrm{diag}\,[x, 1, \ldots, 1]) = \,\mathrm{diag}\,[\xi, \eta, \ldots, \eta], \quad \xi, \eta \in Z_+^*(R).$$

Доказательство. Так как $x \in Z_+^*(R)$, то $x \in Z_+^*(R^*)$, откуда $A = \,\mathrm{diag}\,[x, 1, \ldots, 1] \in D_n^Z(R)$, поэтому по лемме 8 $A' = \Phi'(A) = \,\mathrm{diag}\,[\xi, \eta, \ldots, \eta]$, где $\xi, \eta \in Z_+^*(R^*)$.

Пусть $\mathcal{Y}$ обозначает множество всех матриц вида

$$\begin{pmatrix} a & 0 & \ldots & 0 \\ 0 & \ddots & \ldots\ldots & \\ \ldots\ldots & & a & 0 \\ \ldots\ldots & & 0 & X \end{pmatrix}, \quad X \in G_2(R), a \in Z_+^*(R^*).$$

Ясно, что $\Phi'(\mathcal{Y}) = \mathcal{Y}$ (доказательство полностью аналогично доказательству леммы 3.9).

Пусть $\overline{\mathcal{Z}}$ обозначает центр полугруппы $G_n(R)$. Ясно, что

$$\overline{\mathcal{Z}} = \{\alpha I | \alpha \in Z_+^*(R)\}.$$

Имеем $\Phi'(\overline{\mathcal{Z}}) = \overline{\mathcal{Z}}$.

Любая матрица $A = \,\mathrm{diag}\,[x, 1, \ldots, 1]$, $x \in Z_+^*(R)$ удовлетворяет условию

$$\forall M \in \mathcal{Y}\ MA = AM. \tag{3.3}$$

Матрица $A' = \Phi'(A)$ также удовлетворяет условию (3), поэтому

$$\forall M \in \mathcal{Y} \quad M \cdot \,\mathrm{diag}\,[\xi, \eta, \ldots, \eta] = \,\mathrm{diag}\,[\xi, \eta, \ldots, \eta] \cdot M,$$

или

$$\forall X \in G_2(R) \quad X \circ \,\mathrm{diag}\,[\eta, \eta] = \,\mathrm{diag}\,[\eta, \eta] \circ X,$$

откуда $\eta \in Z_+^*(R)$.

Теперь нам нужно доказать, что $\xi \in Z_+^*(R)$.

Имеем

$$\begin{aligned} \Phi'(\,\mathrm{diag}\,[1, x, 1, \ldots, 1]) &= \Phi'(S_{(1,2)}\,\mathrm{diag}\,[x, 1, \ldots, 1] S_{(1,2)}) = \\ &= S_{(1,2)}\,\mathrm{diag}\,[\xi, \eta, \ldots, \eta] S_{(1,2)} = \,\mathrm{diag}\,[\eta, \xi, \eta, \ldots, \eta] \end{aligned}$$

и, аналогично,

$$\begin{aligned} &\Phi'(\,\mathrm{diag}\,[1, 1, x, 1, \ldots, 1]) = \,\mathrm{diag}\,[\eta, \eta, \xi, \eta, \ldots, \eta], \ldots \\ &\qquad \ldots, \Phi'(\,\mathrm{diag}\,[1, \ldots, 1, x]) = \,\mathrm{diag}\,[\eta, \ldots, \eta, \xi]. \end{aligned}$$

Следовательно,

$$\Phi'(x \cdot I) = \Phi'(\,\mathrm{diag}\,[x, 1, \ldots, 1] \cdot \,\mathrm{diag}\,[1, x, \ldots, 1] \ldots \,\mathrm{diag}\,[1, \ldots, 1, x]) = \xi\eta^{n-1} \cdot I.$$

Так как $x \in Z_+^*(R)$, то $\xi\eta^{n-1} \in Z_+^*(R)$. Так как (как мы только что доказали) $\eta \in Z_+^*(R)$, то $\eta^{n-1} \in Z_+^*(R)$, откуда $\xi \in Z_+^*(R)$, что нам и нужно было доказать. □

Лемма 3.11. *Если $n \geqslant 3$, $1/2 \in R$, автоморфизм $\Phi' \in \mathrm{Aut}\,(G_n(R))$ таков, что $\forall \sigma \in \Sigma_n$ $\Phi'(S_\sigma) = S_\sigma$, то для любого $x_1, x_2 \in Z_+^*(R)$ такого, что $x_1 \neq x_2$,*

$$\Phi'(A_1) = \Phi'(\,\mathrm{diag}\,[x_1, 1, \ldots, 1]) = \,\mathrm{diag}\,[\xi_1, \eta_1, \ldots, \eta_1],$$
$$\Phi'(A_2) = \Phi'(\,\mathrm{diag}\,[x_2, 1, \ldots, 1]) = \,\mathrm{diag}\,[\xi_2, \eta_2, \ldots, \eta_2]$$

имеем $\xi_1\eta_1^{-1} \neq \xi_2\eta_2^{-1}$.

Доказательство. Предположим, что для некоторых различных $x_1, x_2 \in Z_+^*(R)$ имеет место $\xi_1\eta_1^{-1} = \xi_2\eta_2^{-1}$, т.е.

$$\Phi'(A_1) = \Phi'(\,\mathrm{diag}\,[x_1, 1, \ldots, 1]) = \,\mathrm{diag}\,[\xi, \eta, \ldots, \eta] = A_1',$$
$$\Phi'(A_2) = \Phi'(\,\mathrm{diag}\,[x_2, 1, \ldots, 1]) = \alpha \cdot \,\mathrm{diag}\,[\xi, \eta, \ldots, \eta] = A_2',$$

где $\xi, \eta, \alpha \in Z_+^*(R)$ (см. лемму 3.10). Значит, $\Phi'^{-1}(\alpha I) = \Phi'^{-1}(A_1' {A_2'}^{-1}) = \,\mathrm{diag}\,[x_1 x_2^{-1}, 1, \ldots, 1]) = \mathrm{diag}\,[\beta, 1, \ldots, 1]$, где $1 \neq \beta \in Z_+^*(R)$, что невозможно, так как $\Phi'^{-1}(\overline{\mathcal{Z}}) = \overline{\mathcal{Z}}$ (см. доказательство леммы 3.10). Таким образом, $\xi_1\eta_1^{-1} \neq \xi_2\eta_2^{-1}$. $\square$

3.2.3 Основная теорема

В этом пункте мы докажем основную теорему параграфа.

Напомним (см. определение 3.9), что для $x \in R_+$

$$B_{12}(x) = \begin{pmatrix} 1 & x & & & \\ 0 & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \quad B_{21}(x) = \begin{pmatrix} 1 & 0 & & & \\ x & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}.$$

Лемма 3.12. *Если $n \geqslant 3$, $1/2 \in R$, автоморфизм $\Phi' \in \mathrm{Aut}\,(G_n(R))$ таков, что $\forall \sigma \in \Sigma_n$ $\Phi'(S_\sigma) = S_\sigma$, то существуют две возможности:*

1) *существует некоторое отображение $c(\cdot) : R_+ \to R_+$ такое, что для всех $x \in R_+$ $\Phi'(B_{12}(x)) = B_{12}(c(x))$;*

2) *существует некоторое отображение $b(\cdot) : R_+ \to R_+$ такое, что для всех $x \in R_+$ $\Phi'(B_{12}(x)) = B_{21}(b(x))$.*

Доказательство. По лемме 3.9 имеем

$$\Phi'(B_{12}(1)) = \begin{pmatrix} \alpha & \beta & & & \\ \gamma & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix}, \quad a \in Z_+^*(R^*), \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G_2(R)$$

(см. лемму 3.9).

Пусть для каждого $x \in R_+^*$

$$\Phi'(\operatorname{diag}[x, 1, \dots, 1)] = \operatorname{diag}[\xi(x), \gamma(x), \dots, \gamma(x)], \quad \xi(x), \eta(x) \in R_+^*$$

(см. лемму 3.8).

Тогда для любого $x \in Z_+^*(R)$

$$\Phi'(B_{12}(x)) = \Phi'(\operatorname{diag}[x, 1, \dots, 1] B_{12}(1) \operatorname{diag}[x^{-1}, 1, \dots, 1]) =$$

$$= \operatorname{diag}[\xi(x), \eta(x), \dots, \eta(x)] \begin{pmatrix} \alpha & \beta & & & \\ \gamma & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix} \operatorname{diag}[\xi(x)^{-1}, \eta(x)^{-1}, \dots, \eta(x)^{-1}] =$$

$$= \begin{pmatrix} \xi(x)\alpha\xi(x)^{-1} & \xi(x)\beta\eta(x)^{-1} & & & \\ \eta(x)\gamma\xi(x)^{-1} & \eta(x)\delta\eta(x)^{-1} & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix}.$$

Так как по лемме 3.10 $\xi(x), \eta(x) \in Z_+^*(R)$, то $\xi(x)\alpha\xi(x)^{-1} = \alpha$, $\xi(x)\beta\eta(x)^{-1} = \xi(x)\eta(x)^{-1}\beta$, $\eta(x)\gamma\xi(x)^{-1} = \eta(x)\xi(x)^{-1}\gamma$, $\eta(x)\delta\eta(x)^{-1} = \delta$, поэтому

$$\Phi'(B_{12}(x)) = \begin{pmatrix} \alpha & \nu(x)\beta & & & \\ \nu(x)^{-1}\gamma & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix}$$

для $\nu(x) = \xi(x)\eta(x)^{-1}$.

По лемме 3.11 для $x_1 \neq x_2$ имеем $\nu(x_1) \neq \nu(x_2)$.

Для каждого $x \in R_+$ $\Phi'(B_{12}(1))$ и $\Phi'(B_{12}(x))$ коммутируют. Напишем это условие в матричной форме для $x \in Z_+^*(R)$ (напомним, что в этом случае $\nu(x) \in Z_+^*(R)$ по лемме 3.10):

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha & \nu(x)\beta \\ \nu(x)^{-1}\gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & \nu(x)\beta \\ \nu(x)^{-1}\gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \Rightarrow$$

$$\Rightarrow \begin{pmatrix} \alpha^2 + \nu(x)^{-1}\beta\gamma & \nu(x)\alpha\beta + \beta\delta \\ \gamma\alpha + \nu(x)^{-1}\delta\gamma & \nu(x)\gamma\beta + \delta^2 \end{pmatrix} = \begin{pmatrix} \alpha^2 + \nu(x)\beta\gamma & \alpha\beta + \nu(x)\beta\delta \\ \nu(x)^{-1}\gamma\alpha + \delta\gamma & \nu(x)^{-1}\gamma\beta + \delta^2 \end{pmatrix}.$$

Следовательно, $\nu(x)^{-1}\beta\gamma = \nu(x)\beta\gamma$ для различных $x \in Z_+^*(R)$ (например, для $x = 2, 2^2, \dots$). По лемме 3.11 $\nu(x) \neq 1$ для $x \neq 1$, откуда $\nu(x) \neq \nu(x)^{-1}$ для $x \neq 1$ и $\beta\gamma = 0$, т.е. либо $\beta = 0$, либо $\gamma = 0$.

Предположим, что $\gamma = 0$ (случай $\beta = 0$ аналогичен).

Тогда

$$\Phi'(B_{12}(1)) = \begin{pmatrix} \alpha & \beta & & & \\ 0 & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix}, \quad a \in Z_+^*(R^*),\ \alpha, \delta \in R_+^*, \beta \in R_+ \cup \{0\}.$$

Используем условие $(B_{12}(1))^2 = \operatorname{diag}[2, 1, \ldots, 1] B_{12}(1) \cdot \operatorname{diag}[1/2, 1, \ldots, 1]$:

$$\begin{pmatrix} \alpha^2 & \alpha\beta + \beta\delta & & & \\ 0 & \delta^2 & & & \\ & & a^2 & & \\ & & & \ddots & \\ & & & & a^2 \end{pmatrix} = \begin{pmatrix} \alpha & \nu(2)\beta & & & \\ 0 & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix},$$

из которого следует $\alpha = \delta = a = 1$, $\nu(2) = 2$. Значит, имеем $\Phi'(B_{12}(1)) = B_{12}(\beta)$ для некоторого $\beta \in R_+$.

Аналогично, если $\beta = 0$, то $\Phi'(B_{12}(1)) = B_{21}(\gamma)$ для некоторого $\gamma \in R_+$.

Рассмотрим случай $\gamma = 0$ (случай $\beta = 0$ аналогичен). Так как для любого $x \in R_+$ $\Phi'(B_{12}(x))$ коммутирует с $\Phi(B_{12}(1))$, с $S_{(i,i+1)}$ для $i = 3, \ldots, n-1$, и с $\operatorname{diag}[1, 1, \mu_3, \ldots, \mu_n]$ для $\mu_3, \ldots, \mu_n \in R_+^*$, то

$$\Phi'(B_{12}(x)) = \begin{pmatrix} a(x) & b(x) & & & \\ 0 & a(x) & & & \\ & & d(x) & & \\ & & & \ddots & \\ & & & & d(x) \end{pmatrix}, \text{ где } a(x), b(x) \in R_+, d(x) \in Z_+^*(R^*).$$

Теперь используем условие

$$(B_{12}(x))^2 = \operatorname{diag}[2, 1, \ldots, 1] B_{12}(x) \operatorname{diag}[1/2, 1, \ldots, 1] \Rightarrow$$
$$\begin{pmatrix} a(x)^2 & a(x)b(x) + b(x)a(x) & & & \\ 0 & a(x)^2 & & & \\ & & d(x)^2 & & \\ & & & \ddots & \\ & & & & d(x)^2 \end{pmatrix} = \begin{pmatrix} a(x) & 2b(x) & & & \\ 0 & a(x) & & & \\ & & d(x) & & \\ & & & \ddots & \\ & & & & d(x) \end{pmatrix}.$$

Следовательно, $a(x) = d(x) = 1$ для любого $x \in R_+$. Значит, если $\gamma = 0$, то $\Phi'(B_{12}(x)) = B_{12}(b(x))$ для любого $x \in R_+$. Аналогично, в случае $\beta = 0$ имеем $\Phi'(B_{12}(x)) = B_{21}(c(x))$ для любого $x \in R_+$. □

Теперь рассмотрим случаи $\gamma = 0$ и $\beta = 0$ по отдельности. В следующей лемме мы докажем, что случай $\beta = 0$ невозможен.

Лемма 3.13. *Если $n \geqslant 3$, $1/2 \in R$, автоморфизм $\Phi' \in \mathrm{Aut}\,(G_n(R))$ таков, что $\forall \sigma \in \Sigma_n$ $\Phi'(S_\sigma) = S_\sigma$, то условие*

$$\Phi'(B_{12}(1)) = B_{21}(c(1)) \quad (= B_{21}(\gamma))$$

невозможно.

Доказательство. Если $\Phi'(B_{12}(1)) = B_{21}(\gamma) = B_{21}(c(1))$ для некоторого $\gamma = c(1) \in R_+$, то по предыдущей лемме существует такое отображение $c(\cdot) : R_+ \to R_+$, что для каждого $x \in R_+$ мы имеем $\Phi'(B_{12}(x)) = B_{21}(c(x))$. Так как $n \geqslant 3$ и $\forall \sigma \in \Sigma_n$ $\Phi'(S_\sigma) = S_\sigma$, то

$$\Phi'(B_{13}(x)) = \Phi'(S_{(2,3)}B_{12}(x)S_{(2,3)}) = S_{(2,3)}B_{21}(c(x))S_{(2,3)} = B_{31}(c(x)).$$

Аналогично, $\Phi'(B_{32}(x)) = B_{23}(c(x))$.

Используем условие

$$\forall x_1, x_2 \in R_+ \quad B_{13}(x_1)B_{32}(x_2) = B_{32}(x_2)B_{13}(x_1)B_{12}(x_1x_2).$$

Из него следует

$$\begin{aligned}
&\Phi'(B_{13}(x_1)B_{32}(x_2)) = \Phi'(B_{32}(x_2)B_{13}(x_1)B_{12}(x_1x_2)) \Rightarrow \\
&\Rightarrow B_{31}(c(x_1))B_{23}(c(x_2)) = B_{23}(c(x_2))B_{31}(c(x_1))B_{21}(c(x_1x_2)) \Rightarrow \\
&\Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & c(x_2) \\ c(x_1) & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ c(x_2)c(x_1) + c(x_1x_2) & 1 & c(x_2) \\ c(x_1) & 0 & 1 \end{pmatrix} \Rightarrow \\
&\Rightarrow \forall x_1, x_2 \in R_+ \quad c(x_2)c(x_1) + c(x_1x_2) = 0 \Rightarrow \\
&\Rightarrow \forall x \in R_+ \quad c(x)^2 + c(x^2) = 0 \Rightarrow c(x) = 0,
\end{aligned}$$

но это невозможно, так как Φ' является автоморфизмом. □

Напомним, что если G — полугруппа, то гомоморфизм $\lambda(\cdot) : G \to G$ называется *центральным гомоморфизмом* полугруппы G, если $\lambda(G) \subset Z(G)$. Отображение $\Omega(\cdot) : G \to G$ такое, что $\forall X \in G$

$$\Omega(X) = \lambda(X) \cdot X,$$

где $\lambda(\cdot)$ — центральный гомоморфизм, называется *центральной гомотетией.*

Напомним, что для любого $y(\cdot) \in \mathrm{Aut}\,(R_+)$ через Φ^y мы обозначаем автоморфизм полугруппы $G_n(R)$ такой, что $\forall X = (x_{ij}) \in G_n(R)$ $\Phi^y(X) = \Phi^y((x_{ij})) = (y(x_{ij}))$.

Докажем теперь основную теорему параграфа (теорему 3.1).

Доказательство. По лемме 3.6 существует такая матрица $M' \in \Gamma_n(R)$, что для любой перестановки $\sigma \in \Sigma_n$

$$\Phi'(S_\sigma) = \Phi_{M'}\Phi(S_\sigma) = S_\sigma.$$

Теперь рассмотрим автоморфизм Φ'.

По леммам 3.12 и 3.13 существует отображение $c(\cdot) : R_+ \to R_+$ такое, что для любого элемента $x \in R_+$

$$\Phi'(B_{12}(x)) = B_{12}(c(x)).$$

Рассмотрим это отображение. Так как Φ — автоморфизм полугруппы $G_n(R)$, то $c(\cdot) : R_+ \to R_+$ биективно.

Так как для всех $x_1, x_2 \in R_+$ $B_{12}(x_1 + x_2) = B_{12}(x_1)B_{12}(x_2)$, то $B_{12}(c(x_1 + x_2)) = \Phi'(B_{12}(x_1 + x_2)) = \Phi'(B_{12}(x_1)B_{12}(x_2)) = \Phi'(B_{12}(x_1))\Phi'(B_{12}(x_2)) = B_{12}(c(x_1)) \cdot B_{12}(c(x_2)) = B_{12}(c(x_1) + c(x_2))$, откуда для всех $x_1, x_2 \in R_+$ $c(x_1 + x_2) = c(x_1) + c(x_2)$, поэтому $c(\cdot)$ аддитивно.

Для того, чтобы доказать мультипликативность отображения $c(\cdot)$, используем следующее:

1) $\Phi'(B_{13}(x)) = \Phi'(S_{(2,3)}B_{12}(x)S_{(2,3)}) = S_{(2,3)}) = S_{(2,3)}B_{12}(c(x))S_{(2,3)} = B_{13}(c(x))$;

2) аналогично, $\Phi'(B_{32}(x)) = B_{32}(c(x))$;

3) (сравните с доказательством леммы 3.13)

$$\begin{aligned}
B_{13}(x_1)B_{32}(x_2) = B_{32}(x_2)B_{13}(x_1)B_{12}(x_1x_2) \Rightarrow \\
\Rightarrow \Phi'(B_{13}(x_1))\Phi'(B_{32}(x_2)) = \Phi'(B_{32}(x_2))\Phi'(B_{13}(x_1))\Phi'(B_{12}(x_1x_2)) \Rightarrow \\
\Rightarrow B_{13}(c(x_1))B_{32}(c(x_2)) = B_{32}(c(x_2))B_{13}(c(x_1))B_{12}(c(x_1x_2)) \Rightarrow \\
\Rightarrow \forall x_1, x_2 \in R_+ \ \begin{pmatrix} 1 & c(x_1)c(x_2) & c(x_1) \\ 0 & 1 & 0 \\ 0 & c(x_2) & 1 \end{pmatrix} = \begin{pmatrix} 1 & c(x_1x_2) & c(x_1) \\ 0 & 1 & 0 \\ 0 & c(x_2) & 1 \end{pmatrix} \Rightarrow \\
\Rightarrow \forall x_1, x_2 \in R_+ \ c(x_1x_2) = c(x_1)c(x_2).
\end{aligned}$$

Значит, $c(\cdot)$ является мультипликативным отображением.

Так как $c(\cdot)$ биективно, аддитивно и мультипликативно, то $c(\cdot)$ является автоморфизмом полукольца R_+, или, другими словами, $c(\cdot)$ может быть продолжено до автоморфизма кольца R, сохраняющего порядок.

Рассмотрим теперь отображение $\Phi^{c^{-1}}$, которое переводит каждую матрицу $A = (a_{ij})$ в матрицу $\Phi^{c^{-1}}(A) = (c^{-1}(a_{ij}))$. Это отображение является автоморфизмом полукольца $G_n(R)$. Тогда $\Phi'' = \Phi^{c^{-1}} \circ \Phi' = \Phi^{c^{-1}} \circ \Phi_{M'} \circ \Phi$ является автоморфизмом полугруппы $G_n(R)$, оставляющим на месте все матрицы S_σ ($\sigma \in \Sigma_n$) и $B_{ij}(x)$ ($x \in R_+$, $i, j = 1, \ldots, n$, $i \neq j$). Именно, $\Phi''(S_\sigma) = \Phi^{c^{-1}}(\Phi'(S_\sigma)) = \Phi^{c^{-1}}(S_\sigma) = S_\sigma$, так как матрица S_σ содержит только 0 и 1; для $i = 3, \ldots, n$

$$\begin{aligned}
\Phi''(B_{i2}(x)) = \Phi''(S_{(1,i)}B_{12}(x)S_{(1,i)}) = S_{(1,i)}\Phi''(B_{12}(x)))S_{(1,i)} = \\
= S_{(1,i)}\Phi^{c^{-1}}(B_{12}(c(x)))S_{(1,i)} = S_{(1,i)}B_{12}(x)S_{(1,i)} = B_{i,2}(x);
\end{aligned}$$

для $j = 3, \ldots, n$

$$\Phi''(B_{1j}(x)) = \Phi''(S_{(2,j)}B_{12}(x)S_{(2,j)}) = S_{(2,j)}B_{12}(x)S_{(2,j)} = B_{1j}(x);$$

для $i, j = 3, \ldots, n$

$$\Phi''(B_{ij}(x)) = \Phi''(S_{(i,1)}B_{1j}(x)S_{(1,i)}) = S_{(1,i)}B_{1j}(x)S_{(1,i)} = B_{ij}(x).$$

Как мы знаем (см. лемму 3.8), для всех $\alpha \in R_+^*$

$$\Phi''(\operatorname{diag}[\alpha, 1, \ldots, 1]) = \operatorname{diag}[\beta(\alpha), \gamma(\alpha), \ldots, \gamma(\alpha)], \quad \beta, \gamma \in R_+^*.$$

Используем соотношение

$$\operatorname{diag}[\alpha,1,\ldots,1]B_{12}(1)\operatorname{diag}[\alpha^{-1},1,\ldots,1]=B_{12}(\alpha)\Rightarrow$$
$$\Phi''(\operatorname{diag}[\alpha,1,\ldots,1])\Phi''(B_{12}(1))\Phi''(\operatorname{diag}[\alpha^{-1},1,\ldots,1])=\Phi''(B_{12}(\alpha))\Rightarrow$$
$$\Rightarrow \operatorname{diag}[\beta(\alpha),\gamma(\alpha),\ldots,\gamma(\alpha)]B_{12}(1)\operatorname{diag}[\beta(\alpha)^{-1},\gamma(\alpha)^{-1},\ldots,\gamma(\alpha)^{-1}]=B_{12}(\alpha)\Rightarrow$$
$$\Rightarrow \beta(\alpha)\gamma(\alpha)^{-1}=\alpha\Rightarrow\beta(\alpha)=\alpha\gamma(\alpha)\Rightarrow$$
$$\forall\alpha\in R_+^*\ \Phi''(\operatorname{diag}[\alpha,1,\ldots,1])=\operatorname{diag}[\alpha\gamma(\alpha),\gamma(\alpha),\ldots,\gamma(\alpha)].$$

Так как $\operatorname{diag}[\alpha,1,\ldots,1]$ коммутирует с любой матрицей вида

$$\begin{pmatrix}1&0\\0&X\end{pmatrix},\quad X\in G_{n-1}(R),$$

и $n\geqslant 3$, то для всех $\alpha\in R_+^*$ $\gamma(\alpha)\in Z_+^*(R)$.

Так как для всех $\alpha_1,\alpha_2\in R_+^*$

$$\operatorname{diag}[\alpha_1\alpha_2\gamma(\alpha_1\alpha_2),\gamma(\alpha_1\alpha_2),\ldots,\gamma(\alpha_1\alpha_2)]=\Phi''(\operatorname{diag}[\alpha_1\alpha_2,1,\ldots,1])=$$
$$=\Phi''(\operatorname{diag}[\alpha_1,1,\ldots,1])\Phi''(\operatorname{diag}[\alpha_2,1,\ldots,1])=$$
$$=\operatorname{diag}[\alpha_1\gamma(\alpha_1),\gamma(\alpha_1),\ldots,\gamma(\alpha_1)]\operatorname{diag}[\alpha_2\gamma(\alpha_2),\gamma(\alpha_2),\ldots,\gamma(\alpha_2)]=$$
$$=\operatorname{diag}[\alpha_1\alpha_2\gamma(\alpha_1)\gamma(\alpha_2),\gamma(\alpha_1)\gamma(\alpha_2),\ldots,\gamma(\alpha_1)\gamma(\alpha_2)]\Rightarrow$$
$$\Rightarrow\forall\alpha_1,\alpha_2\in R_+^*\ \gamma(\alpha_1\alpha_2)=\gamma(\alpha_1)\gamma(\alpha_2),$$

то отображение $\gamma(\cdot)$ является центральным гомоморфизмом $\gamma(\cdot):R_+^*\to Z_+^*(R)$.

Если $A=\operatorname{diag}[\alpha_1,\ldots,\alpha_n]\in D_n(R)$, то

$$\Phi''(A)=\Phi''(\operatorname{diag}[\alpha_1,1,\ldots,1]S_{1,2}\operatorname{diag}[\alpha_2,1,\ldots,1]S_{(1,2)}S_{(1,3)}\operatorname{diag}[\alpha_3,1,\ldots,1]S_{(1,3)}\ldots$$
$$\ldots S_{(1,n)}\operatorname{diag}[\alpha_n,1,\ldots,1]S_{(1,n)})=\gamma(\alpha_1)\operatorname{diag}[\alpha_1,1,\ldots,1]S_{(1,2)}\gamma(\alpha_2)\operatorname{diag}[\alpha_2,1,\ldots,1]S_{(1,2)}\ldots$$
$$\ldots S_{(1,n)}\gamma(\alpha_n)\operatorname{diag}[\alpha_n,1,\ldots,1]\gamma(\alpha_n)=$$
$$=\gamma(\alpha_1)\ldots\gamma(\alpha_n)A=\gamma(\alpha_1\ldots\alpha_n)A.$$

Напомним (см. определение 3.9), что $\mathbf{P}$ является подполугруппой в $G_n(R)$, порожденной матрицами S_σ ($\sigma\in\Sigma_n$), $B_{ij}(x)$ ($x\in R_+,\ i,j=1,\ldots,n,\ i\neq j$), и $\operatorname{diag}[\alpha_1,\ldots,\alpha_n]$ ($\alpha_1,\ldots,\alpha_n\in R_+^*$).

Ясно, что любая матрица $A\in\mathbf{P}$ может быть представлена в виде

$$A=\operatorname{diag}[\alpha_1,\ldots,\alpha_n]A_1\ldots A_k,$$

где $\alpha_1,\ldots,\alpha_n\in R_+^*$, $A_1,\ldots,A_k\in\{S_\sigma,B_{ij}(x)|\sigma\in\Sigma_n,x\in R_+,i,j=1,\ldots,n,i\neq j\}$. Тогда

$$\Phi''(A)=\Phi''(\operatorname{diag}[\alpha_1,\ldots,\alpha_n]A_1\ldots A_k)=$$
$$=\gamma(\alpha_1\ldots\alpha_n)\operatorname{diag}[\alpha_1,\ldots,\alpha_n]A_1\ldots A_k=\gamma(\alpha_1\ldots\alpha_n)A.$$

Теперь введем отображение $\overline{\gamma}(\cdot):\mathbf{P}\to Z_+^*(R)$ с помощью следующего правила: если $A\in\mathbf{P}$ и $A=\operatorname{diag}[\alpha_1,\ldots,\alpha_n]A_1\ldots A_k$, где $A_1,\ldots,A_k\in\{S_\sigma,B_{ij}(x)|\sigma\in\Sigma_n,x\in R_+,i,j=1,\ldots,n,i\neq j\}$, то $\overline{\gamma}(A)=\gamma(\alpha_1,\ldots,\alpha_n)$.

Отображение $\overline{\lambda}(\cdot)$ однозначно определено, так как если $A = \operatorname{diag}[\alpha_1, \ldots, \alpha_n]A_1 \ldots A_k = \operatorname{diag}[\alpha_1', \ldots, \alpha_n']A_1' \ldots A_m'$, то $\Phi''(A) = \gamma(\alpha_1 \ldots \alpha_n)A$ and $\Phi''(A) = \gamma(\alpha_1' \ldots \alpha_n')A$ и поэтому $\gamma(\alpha_1 \ldots \alpha_n) = \gamma(\alpha_1' \ldots \alpha_n')$.

Так как $\overline{\gamma}(AA')AA' = \Phi''(AA') = \Phi''(A)\Phi''(A') = \overline{\gamma}(A)A \cdot \overline{\gamma}(A')A' = \overline{\gamma}(A)\overline{\gamma}(A')AA'$, то $\overline{\gamma}$ является гомоморфизмом $\mathbf{P} \to Z_+^*(R)$.

Теперь мы видим, что на полугруппе $\mathbf{P}$ автоморфизм Φ'' совпадает с центральной гомотетией $\Omega(\cdot) : \mathbf{P} \to \mathbf{P}$, где для всех $a \in \mathbf{P}$ $\Omega(A) = \overline{\gamma}(A) \cdot A$.

Пусть $B \in \mathrm{GE}_n^+(R)$. Тогда (см. определения 3.10, 3.11) матрица B $\mathcal{P}$-эквивалентна некоторой матрице $A \in \mathbf{P}$, т.е. существуют матрицы $A_0, \ldots, A_k \in G_n(R)$, $A_0 = A \in \mathbf{P}$, $A_k = B$ и матрицы $P_i, \widetilde{P}_i, Q_i, \widetilde{Q}_i \in \mathbf{P}$, $i = 0, \ldots, k-1$ такие, что для всех $i = 0, \ldots, k-1$

$$P_i A_i \widetilde{P}_i = Q_i A_{i+1} \widetilde{Q}_i.$$

Тогда

$$\begin{aligned}
&\Phi''(P_0 A_0 \widetilde{P}_0) = \Phi''(Q_0 A_1 \widetilde{Q}_0) \Rightarrow \\
&\qquad \Rightarrow \overline{\gamma}(P_0)P_0\overline{\gamma}(A_0)A_0\overline{\gamma}(\widetilde{P}_0)\widetilde{P}_0 = \overline{\gamma}(Q_0)Q_0\Phi''(A_1)\overline{\gamma}(\widetilde{Q}_0)\widetilde{Q}_0 \Rightarrow \\
&\qquad \overline{\gamma}(P_0A_0\widetilde{P}_0)P_0A_0\widetilde{P}_0 = \overline{\gamma}(Q_0\widetilde{Q}_0)Q_0\Phi''(A_1)\widetilde{Q}_0 \Rightarrow \\
&\qquad \Rightarrow \overline{\gamma}(P_0A_0\widetilde{P}_0)\overline{\gamma}(Q_0\widetilde{Q}_0)^{-1}Q_0A_1\widetilde{Q}_0 = Q_0\Phi''(A_1)\widetilde{Q}_0 \Rightarrow \\
&\qquad \Rightarrow \Phi''(A_1) = \overline{\gamma}(P_0A_0\widetilde{P}_0)\overline{\gamma}(Q_0\widetilde{Q}_0)^{-1}A_1, \ldots, \\
&\qquad \ldots, \Phi''(B) = \Phi''(A_n) = \overline{\gamma}(P_{n-1})\overline{\gamma}(A_{n-1})\overline{\gamma}(\widetilde{P}_{n-1})\overline{\gamma}(Q_{n-1})^{-1}\overline{\gamma}(\widetilde{Q}_{n-1}).
\end{aligned}$$

Значит, мы можем продолжить отображение $\overline{\gamma}(\cdot) : \mathbf{P} \to Z_+^*(R)$ до некоторого отображения $\lambda(\cdot) : \mathrm{GE}_n^+(R) \to Z_+^*(R)$ такого, что для каждого $B \in \mathrm{GE}_n^+(R)$

$$\Phi''(B) = \lambda(B) \cdot B.$$

Так как Φ'' является автоморфизмом полугруппы $\mathrm{GE}_n^+(R)$, то $\lambda(\cdot)$ является центральным гомоморфизмом $\lambda(\cdot) : \mathrm{GE}_n^+(R) \to Z_+^*(R)$ и, значит, автоморфизм $\Phi'' : \mathrm{GE}_n^+(R) \to \mathrm{GE}_n^+(R)$ является центральной гомотетией $\Omega(\cdot) : \mathrm{GE}_n^+(R) \to \mathrm{GE}_n^+(R)$, где $\forall X \in \mathrm{GE}_n^+(R)$ $\Omega(X) = \lambda(X) \cdot X$.

Так как $\Phi'' = \Omega$ на $\mathrm{GE}_n^+(R)$ и $\Phi'' = \Phi^{c^{-1}} \circ \Phi_{M'} \circ \Phi$ на $G_n(R)$, то $\Phi = \Phi_M \circ \Phi^c \circ \Omega$ на $\mathrm{GE}_n^+(R)$, где $M = M'^{-1}$. □

3.3 Элементарная эквивалентность полугруппы обратимых матриц с неотрицательными элементами над линейно упорядоченными кольцами

Целью данного параграфа вляется доказательство следующей теоремы:

Теорема 3.2. *Полугруппы $G_n(R)$, $G_m(S)$ ($n, m \geqslant 3$, $1/2 \in R$, $1/2 \in S$, кольца R и S линейно упорядочены) элементарно эквивалентны тогда и только тогда, когда $n = m$ и полукольца R_+ и S_+ элементарно эквивалентны.*

Лемма 3.14. *Формула*

$$Invert(M) := \exists X(MX = XM = 1)$$

истинна в полугруппе $G_n(R)$ для элементов группы $\Gamma_n(R)$, и только для них.

Доказательство. Очевидно. □

Лемма 3.15. *Формула*

$$Inv(M) := \big((M^2 = 1) \wedge M \neq 1\big)$$

истинна в полугруппе $G_n(R)$ для инволюций, и только для них. Эти инволюции имеют вид $\mathrm{diag}\,[t_1, \ldots, t_n]S_\sigma$, где $\sigma^2 = 1$, $t_i \cdot t_{\sigma(i)} = 1$ для всех $i = 1, \ldots, n$.

Доказательство. Первая часть очевидна, а вторая следует из леммы 3.3. □

Лемма 3.16. 1) *Существует формула $Diag(M)$, истинная в полугруппе $G_n(R)$ для матриц $M \in D_n(R)$, и только для них.*

2) *Существует формула $CDiag(M)$, истинная в полугруппе $G_n(R)$ для матриц $M \in D_n^Z(R)$, и только для них.*

Доказательство. Рассмотрим формулу

$$ComCon(A) := \big(Invert(A) \wedge \forall M(\exists N(M = NAN^{-1}) \Rightarrow AM = MA)\big).$$

Эта формула утверждает, что матрица A обратима и коммутирует со всеми матрицами, с ней сопряженными. По лемме 3.4 формула $ComCon(A)$ выполняется для всех $A \in D_n^Z(R)$, может выполняться для некоторых элементов из $D_n(R) \setminus D_n^Z(R)$, и никогда не выполняется для элементов из $\Gamma_n(R) \setminus D_n(R)$.

Введем теперь новую формулу:

$$NComInv(A) := \big(ComCon(A) \wedge \forall M(Inv(M) \Rightarrow AM \neq MA)\big).$$

Этой формулой мы вводим дополнительное условие "матрица A не коммутирует ни с одной инволюцией". Как следует из доказательства леммы 3.4, эта формула всегда истинна для матриц $M \in D_n^Z(R)$, имеющих различные собственные значения, может быть истинна для некоторых матриц $M \in D_n(R) \setminus D_n^Z(R)$, имеющих различные собственные значения, и не может быть истинна ни для каких других матриц.

Рассмотрим теперь формулу

$$Diag(M) := \exists A(NComInv(A) \wedge MA = AM \wedge Invert(M)).$$

Формула $Diag(M)$ истинна для матриц из множества $\mathcal{X} = D_n(R)$ (см. доказательство леммы 3.4), т. е. удовлетворяет условию 1) леммы.

Формула

$$CDiag(M) := \big(Invert(M) \wedge \forall A(Diag(A) \Rightarrow AM = MA)\big)$$

является искомой для второго пункта леммы. □

Лемма 3.17. *Для любого $n \geqslant 2$ существует предложение $Size_n$, истинное во всех полугруппах $G_n(R)$, $1/2 \in R$, и ложное во всех полугруппах $G_m(S)$, $m \neq n$, $1/2 \in S$.*

Доказательство. Рассмотрим предложение

$$Size_n := \exists X_1 \dots \exists X_{n!} (\forall M (Diag(M) \Rightarrow \bigwedge_{i,j=1; i \neq j}^{n!} X_i \neq M X_j) \wedge \\ \wedge \forall X (Invert(X) \Rightarrow \exists M (Diag(M) \wedge \bigvee_{i=1}^{n!} (X = M X_i)))).$$

Очевидно, что оно является искомым. □

Теперь мы можем считать, что размерность n полугруппы $G_n(R)$ нам известна, т. е. можем использовать ее в формулах.

Лемма 3.18. *Существует формула $CDOneMany_n(M)$, истинная для всех матриц*

$$\operatorname{diag}[\alpha, \dots, \alpha, \beta, \alpha, \dots, \alpha] \in D_n^Z(R), \quad \alpha \neq \beta,$$

и только для них.

Доказательство. Из леммы 3.5 следует, что искомые матрицы M характеризуются тем условием, что

$$C_{\Gamma_n(R)}(M)/D_n(R) \cong \Sigma_{n-1}.$$

Пусть элементы $\sigma_1, \dots, \sigma_N$ ($N = (n-1)!$) группы Σ_{n-1} некоторым определенным фиксированным образом пронумерованы, причем $\sigma_i \cdot \sigma_j = \sigma_{\gamma(i,j)}$. Тогда искомая формула:

$$CDOneMany_n(M) := \exists X_1 \dots \exists X_N \left(\left(\bigwedge_{i=1}^{N} X_i M = M X_i \right) \wedge \right. \\ \wedge \left(\bigwedge_{i \neq j, i,j=1}^{N} \forall A (Diag(A) \Rightarrow X_i \neq X_j A) \right) \wedge \left(\bigwedge_{i=1}^{N} Invert(X_i) \right) \wedge \\ \wedge \forall X \left(Invert(X) \wedge XM = MX \Rightarrow \exists A \left(Diag(A) \wedge \bigvee_{i=1}^{N} (X = A X_i) \right) \right) \wedge \\ \left. \wedge \left(\bigwedge_{i,j=1}^{N} \exists A (Diag(A) \wedge X_i \cdot X_j = A X_{\gamma(i,j)}) \right) \right).$$

□

Аналогично можно ввести формулу $CDAll_n(M)$, характеризующую матрицы $\alpha I \in D_n^Z(R)$.

Лемма 3.19. *Для любой матрицы*

$$M = \operatorname{diag}[\alpha, \ldots, \alpha, \underbrace{\beta}_{i}, \alpha, \ldots, \alpha] \in D_n^Z(R), \quad \alpha \neq \beta,$$

формула

$$\begin{aligned} &DSame_{1,n-1}(A, M) := CDOneMany_n(A) \wedge CDOneMany_n(M) \wedge \\ &\quad \wedge (CDOneMany_n(AM) \vee CDAll_n(AM)) \wedge (CDOneMany_n(AM^{-1}) \vee CDAll_n(AM^{-1})) \end{aligned}$$

характеризует матрицы

$$A = \operatorname{diag}[\gamma, \ldots, \gamma, \underbrace{\delta}_{i}, \gamma, \ldots, \gamma] \in D_n^Z(R), \quad \gamma \neq \delta.$$

Доказательство. Если

$$A = \operatorname{diag}[\gamma, \ldots, \gamma, \underbrace{\delta}_{i}, \gamma, \ldots, \gamma] \in D_n^Z(R), \quad \gamma \neq \delta,$$

то по лемме 3.18 выполняется подформула $DOneMany_n(A)$,

$$AM = \operatorname{diag}[\alpha\gamma, \ldots, \alpha\gamma, \beta\delta, \alpha\gamma, \ldots, \alpha\gamma] \in D_n^Z(R),$$

и, если $\alpha\gamma = \beta\delta$, то выполняется подформула $CDAll_n(AM)$, а если $\alpha\gamma \neq \beta\delta$, то выполняется подформула $CDOneMany_n(AM)$, аналогично для AM^{-1}.

Обратно, пусть для $M = \operatorname{diag}[\alpha, \ldots, \alpha, \beta, \alpha, \ldots, \alpha]$ и для некоторой A выполняется формула $DSame_{1,n-1}(A, M)$. Так как в этом случае выполняется подформула $CDOneMany_n(A)$, то $A = \operatorname{diag}[\gamma, \ldots, \gamma, \delta, \gamma, \ldots, \gamma] \in D_n^Z(R)$, $\delta \neq \gamma$. Если β и δ находятся на одном и том же i-ом месте, то все доказано. Пусть это не так. Тогда без ограничения общности можно считать, что $M = \operatorname{diag}[\beta, \alpha, \ldots, \alpha]$, а $A = \operatorname{diag}[\gamma, \delta, \gamma, \ldots, \gamma]$. В этом случае $MA = \operatorname{diag}[\beta\gamma, \alpha\delta, \gamma\alpha, \ldots, \gamma\alpha]$. Очевидно. что $\beta\gamma \neq \alpha\gamma$ и $\alpha\delta \neq \alpha\gamma$. Если $n > 3$, то мы сразу получаем $\neg(CDOneMany_n(AM) \vee CDAll_n(AM))$ и приходим к противоречию. Если $n = 3$, то может оказаться, что $\beta\gamma = \alpha\delta$, и тогда выполняется формула $CDOneMany_n(AM)$. В этом случае рассмотрим матрицу $AM^{-1} = \operatorname{diag}[\beta\gamma^{-1}, \alpha\delta^{-1}, \alpha\gamma^{-1}]$. Так как $\beta\gamma^{-1} \neq \alpha\gamma^{-1}$ и $\alpha\delta^{-1} \neq \alpha\gamma^{-1}$, то должно быть $\beta\gamma^{-1} = \alpha\delta^{-1}$. Следовательно,

$$\begin{cases} \beta\gamma = \alpha\delta \\ \beta\gamma^{-1} = \alpha\delta^{-1} \end{cases} \Rightarrow \alpha = \beta,$$

получаем противоречие. □

Лемма 3.20. *Существует формула $KOneMany_n(X, M)$ от двух переменных такая, что для любой матрицы A, удовлетворяющей формуле $CDOneMany_n(A)$, множество матриц M, удовлетворяющих формуле $KOneMany_n(A, M)$, есть группа $\Phi_N(K_n(R)) = N(K_n(R))N^{-1}$ для некоторой матрицы $N \in \Gamma_n(R)$.*

Доказательство. Рассмотрим следующую формулу:

$$KOneMany_n(X, M) := \exists M'(XM' = M'X \wedge DSame_{1,n-1}(M', M)).$$

Эта формула утверждает, что

$$X \in \bigcup_{A = diag[\alpha,\ldots,\alpha,\beta,\alpha,\ldots,\alpha] \in D_n^Z(R), \alpha \neq \beta} C_{G_n(R)}(A),$$

откуда по лемме 3.5 мы получаем наше утверждение. □

Лемма 3.21. *Существуют формулы $Cycle_n(X)$, $Trans_n(X, Y)$ и $Perm_n(X, Y, Z)$ такие, что для любых матриц M_1, M_2, M_3, для которых выполняются формулы $Cycle_n(M_1)$, $Trans_n(M_1, M_2)$ и $Perm_n(M_1, M_2, M_3)$, существует матрица $N \in \Gamma_n(R)$ такая, что $M_1 = \Phi_N(S_{(1,2,\ldots,n)})$, $M_2 = \Phi_N(S_{(1,2)})$, $M_3 = \Phi_N(S_\sigma)$ для некоторой $\sigma \in \Sigma_n$.*

Доказательство. Рассмотрим матрицу M, удовлетворяющую формуле

$$Cycle_n(M) := (M^n = 1) \wedge \forall X(CDiag(X) \wedge MX = XM \Rightarrow CDAll_n(X)).$$

Эта формула утверждает, что матрица M имеет порядок n и коммутирует только со скалярными матрицами из $D_n^Z(R)$. Отсюда следует, что матрица $M = D_\rho S_\rho$, где ρ есть цикл длины n. Без ограничения общности можно считать, что $\rho = (1, 2, \ldots, n)$. Из леммы 3.7 тогда следует, что $M = \Phi_{N'}(S_\rho)$ для некоторого $N' \in \Gamma_n(R)$.

Фиксируем матрицу M, удовлетворяющую формуле $Cycle_n(M)$ (таким образом, матрица N' будет выбрана с точностью до умножения на матрицы, коммутирующие с S_ρ).

Рассмотрим теперь матрицу M', удовлетворяющую следующей формуле (относительно M):

$$\begin{aligned} Trans_n(M, M') := (M'^2 = 1) \wedge ((MM')^{n-1} = 1) \wedge \\ \wedge \exists X(CDOneMany_n(X) \wedge KOneMany_n(X, MM')). \end{aligned}$$

Рассмотрим матрицу $\Phi_{N'}^{-1}(M') = D_\sigma S_\sigma$.

Из того, что она удовлетворяет условию $(D_\sigma S_\sigma)^2 = 1$, следует $\sigma^2 = 1 \Rightarrow \sigma = (i, j)$, $D_\sigma = \operatorname{diag}[d_1, \ldots, d_n]$, $d_k = 1$ при $k \neq i$, $k \neq j$, $d_i d_j = 1$. Из остальных условий следует, что элемент $\sigma\rho$ является циклом длины $n-1$. С другой стороны, $\sigma\rho = (i, j)(1, 2, , \ldots, n) = (1, 2, \ldots, i-1, j, j+1, \ldots, n)(i, i+1, \ldots, j-1)$, следовательно, $j = i+1$. Значит, $S_\sigma = S_{(i,i+1)}$, $\sigma\rho = (1, 2, \ldots, i-1, i+1, \ldots, n)$. Из условия $(MM')^{n-1} = 1$ получаем

$$(\operatorname{diag}[d_1, \ldots, d_n] S_{(1,2,\ldots,i-1,i+1,\ldots,n)})^{n-1} = 1,$$

откуда $d_i^{n-1} = 1 \Rightarrow d_i = 1$. Таким образом, $\Phi_{N'}^{-1}(M') = S_{(i,i+1)}$ для некоторого $i = 1, \ldots, n$.

Рассмотрим тогда матрицу $N'' = S_{\rho'}$, где $\rho' = \rho^{i-1}$. Очевидно, что $\Phi_{N''}(S_\rho) = S_\rho$. При этом $\Phi_{N''}(S_{(i,i+1)}) = S_{(1,2)}$. Таким образом, мы получили матрицы M_1 и M_2, для которых существует матрица $N = N''N'$ такая, что $M_1 = \Phi_N(S_{(1,2,\ldots,n)})$, $M_2 = \Phi_N(S_{(1,2)})$.

Матрица M_1 — это любая матрица, удовлетворяющая формуле $Cycle_n(M)$.

Матрица M_2 — это любая матрица, удовлетворяющая формуле $Trans_n(M_1, M)$.

Формула $Perm_n(M_1, M_2, M)$ строится следующим образом: для данной группы Σ_n для каждого ее элемента σ считаем разложение $\sigma = (1,2)^{i_1}(1,2,\ldots,n)^{j_1}\ldots(1,2)^{i_k}(1,2,\ldots,n)^{j_k}$. Пусть элементы группы Σ_n — это $\sigma_1, \ldots, \sigma_N$,

$$\sigma_l = (1,2)^{i_1^l}(1,\ldots,n)^{j_1^l}\ldots(1,2)^{i_{k(l)}^l}(1,\ldots,n)^{j_{k(l)}^l}.$$

Тогда

$$Perm_n(M_1, M_2, M) := \bigvee_{l=1}^{N}(M = M_2^{i_1^l} M_1^{j_1^l}\ldots M_2^{i_{k(l)}^l} M_1^{j_{k(l)}^l}).$$

Например, для $n = 3$ имеем $\sigma_1 = 1$, $\sigma_2 = (1,2,3)$, $\sigma_3 = (1,2)$, $\sigma_4 = (3,2,1) = (1,2,3)^2$, $\sigma_5 = (1,3) = (1,2,3)(1,2)$, $\sigma_6 = (2,3) = (1,2)(1,2,3)$,

$$Perm_3(M_1, M_2, M) := (M = 1) \vee (M = M_1) \vee (M = M_2) \vee (M = M_1^2) \vee \\ \vee (M = M_1M_2) \vee (M = M_2M_1).$$

□

Теперь предположим, что матрицы M_1 и M_2 фиксированы. Таким образом, с точностью до умножения на матрицу $\alpha I \in D_n^Z(R)$ фиксирована и матрица N.

Лемма 3.22. *Существуют формулы $GDOneMany_n(M_1, M_2, M)$ и $DOneMany_n(M_1, M_2, M)$, истинные в полугруппе $G_n(R)$ для тех и только тех матриц M, которые имеют вид $\Phi_N(\operatorname{diag}[\alpha, \beta, \ldots, \beta])$, $\alpha, \beta \in R_+^*$ и $\Phi_N(\operatorname{diag}[\alpha, \beta, \ldots, \beta])$, $\alpha, \beta \in R_+^*$, $\alpha \neq \beta$, соответственно.*

Доказательство. Очевидно, что формулы

$$GDOneMany_n(M_1, M_2, M) := ((M_2M_1) \cdot M = M \cdot (M_2M_1)) \wedge Diag(M)$$

и

$$DOneMany_n(M_1, M_2, M) := GDOneMany_n(M_1, M_2, M) \wedge (M_2M \neq MM_2)$$

(см. лемму 3.8) являются искомыми. □

Лемма 3.23. *Существует формула $G_2CD_{n-2}(M_1, M_2, M)$, истинная в полгруппе $G_n(R)$ для тех и только и тех матриц M, которые имеют вид $\Phi_N(\operatorname{diag}[X, a, \ldots, a])$, где $X \in G_2(R)$, $a \in Z_+^*(R^*)$.*

Доказательство. Аналогично предыдущей лемме мы можем написать формулу

$$DTwoMany_n(M_1, M_2, M),$$

истинную в полугруппе $G_n(R)$ для тех и только тех матриц M, которые имеют вид

$$\Phi_N(\operatorname{diag}[\alpha, \alpha, \beta, \ldots, \beta]) \in D_n(R), \quad \alpha \neq \beta.$$

Формула

$$DTransp_{1,2}(M_1, M_2, M) := (M^2 = 1) \wedge \exists(Diag(X) \wedge M = XM_2)$$

выделяет инволюции вида

$$\Phi_N(\operatorname{diag}[\xi, \xi^{-1}, 1, \dots, 1]S_{(1,2)}), \quad \xi \in R_+^*$$

(см. начало доказательства леммы 3.9).

Аналогично, формула

$$CDTransp_{1,2}(M_1, M_2, M) := (M^2 = 1) \wedge \exists X(CDiad(X) \wedge M = XM_2)$$

выделяет инволюции

$$\Phi_N(\operatorname{diag}[\xi, \xi^{-1}, 1, \dots, 1]S_{(1,2)}), \quad \xi \in Z_+^*(R^*).$$

Формула

$$CD_2D_{n-2}(M_1, M_2, M) := DTwoMany(M_1, M_2, M) \wedge \\ \wedge \forall X(DTransp_{1,2}(M_1, M_2, X) \Rightarrow XM = MX)$$

выделяет множество матриц вида

$$\Phi_N(\operatorname{diag}[\mu, \mu, \eta, \dots, \eta]), \quad \mu \in Z_+^*(R^*), \eta \in R^*.$$

Как мы помним, формула $CDAll(M)$ выделяет матрицы αI, $\alpha \in Z_+^*(R^*)$.

Выпишем теперь формулу

$$G_2CD_{n-2}(M_1, M_2, M) := \forall X(CD_2D_{n-2}(M_1, M_2, X) \Rightarrow \\ \Rightarrow \exists Y(CDAll(Y) \wedge MXY = XYM \wedge \\ \wedge (M_1^{i_1} M_2^{j_2} \dots M_1^{i_k} M_2^{j_k})M = M(M_1^{i_1} M_2^{j_1} \dots M_1^{i_k} M_2^{j_k}))),$$

где

$$(1, 2, \dots, n)^{i_1}(1, 2)^{j_1} \dots (1, 2, \dots, n)^{i_k}(1, 2)^{j_k} = (3, \dots, n)$$

(при $n = 3$ это последнее условие не нужно).

Эта формула равносильна условию (2) из доказательства леммы 3.9. В предыдущем параграфе доказано, что в этом случае

$$M = \Phi_N(\operatorname{diag}[X, a, \dots, a]), \quad X \in G_2(R),\ a \in Z_+^*(R^*),$$

что и требовалось доказать. □

Лемма 3.24. *Существует формула $ZDOneMany_n(M_1, M_2, M)$, истинная в полугруппе $G_n(R)$ для тех и только тех матриц M, которые имеют вид*

$$\Phi_N(\operatorname{diag}[\xi, \eta, \dots, \eta]), \quad \xi, \eta \in Z_+^*(R).$$

Доказательство. Аналогично формуле $G_2CD_{n-2}(M_1, M_2, M)$ можно написать формулу $CD_{n-2}G_2(M_1, M_2, M)$, истинную для тех и только тех матриц M, которые имеют вид

$$\Phi_N(\operatorname{diag}[a, \ldots, a, X]), \quad X \in G_2(R),\ a \in Z_+^*(R).$$

Формула

$$ZDAll(M) := \forall X(XM = MX)$$

выделяет центр полугруппы $G_n(R)$, состоящий из матриц αI, $\alpha \in Z_+^*(R)$.

Пусть для $n \geqslant l \geqslant 2$

$$(1, l) = (1, 2, \ldots, n)^{i_1^l}(1, 2)^{j_1^l} \ldots (1, 2, \ldots, n)^{i_{k(l)}^l}(1, 2)^{j_{k(l)}^l}.$$

Тогда формула

$$\begin{aligned} ZDOneMany_n(M_1, M_2, M) &:= DOneMany_n(M_1, M_2, M)\wedge \\ &\wedge \forall X(CD_{n-2}G_2(M_1, M_2, X) \Rightarrow MX = XM)\wedge \\ \wedge\, ZDAll_n(M \cdot (M_1^{i_1^2} M_2^{j_1^2} &\ldots M_1^{i_{k(2)}^2} M_2^{j_{k(2)}^2} \cdot M M_2^{-j_{k(2)}^2} M_1^{-i_{k(2)}^2} \ldots M_2^{-j_1^2} M_1^{-i_1^2}) \ldots \\ &\ldots (M_1^{i_1^n} M_2^{j_1^n} \ldots M_1^{i_{k(n)}^n} M_2^{j_{k(n)}^n} M M_2^{-j_{k(n)}^n} M_1^{-j_{k(n)}^n} \ldots M_2^{-j_1^n} M_1^{-i_1^n})) \end{aligned}$$

удовлетворяет условию (см. доказательство леммы 3.10). □

Лемма 3.25. *Существует формула $Main(M_1, M_2, M)$, истинная для тех и только тех матриц M, которые имеют вид либо*

$$\Phi_N B_{12}(x) = N B_{12}(x) N^{-1},$$

либо

$$\Phi_N B_{21}(x) = N B_{21}(x) N^{-1}$$

для некоторого $x \in R_+$.

Доказательство. Рассмотрим формулу

$$\begin{aligned} Main(M_1, M_2, M) &:= G_2CD_{n-2}(M_1, M_2, M)\wedge \\ &\wedge \exists X(ZDOneMany(M_1, M_2, X) \wedge M^2 = XMX^{-1})\wedge \\ &\wedge \forall X(ZDOneMany(M_1, M_2, X) \Rightarrow M(XMX^{-1}) = (XMX^{-1})M). \end{aligned}$$

Матрица M удовлетворяет формуле $G_2CD_{n-2}(M_1, M_2, M)$, откуда следует

$$M = \Phi_N \begin{pmatrix} \alpha & \beta & & & \\ \gamma & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix}, \quad a \in Z_+^*(R^*),\ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G_2(R).$$

То, что матрица M удовлетворяет подформуле $\forall X(ZDOneMany(M_1, M_2, X) \Rightarrow M(XMX^{-1}) = (XMX^{-1})M)$, влечет соотношение

$$\begin{pmatrix} \alpha & \beta & & & \\ \gamma & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix} \begin{pmatrix} \alpha & \xi\eta^{-1}\beta & & & \\ \eta\xi^{-1}\gamma & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha & \xi\eta^{-1}\beta & & & \\ \eta\xi^{-1}\gamma & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix} \begin{pmatrix} \alpha & \beta & & & \\ \gamma & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix}$$

для всех $\eta, \xi \in Z_+^*(R)$, откуда следует соотношение

$$\eta\xi^{-1}\beta\gamma = \xi\eta^{-1}\beta\gamma$$

для любых $\eta, \xi \in Z_+^*(R)$, в том числе и для $\eta = 2$, $\xi = 1$. Отсюда получаем

$$2\beta\gamma = \frac{1}{2}\beta\gamma \Rightarrow \left(2 - \frac{1}{2}\right)\beta\gamma = 0.$$

Значит, либо $\beta = 0$, либо $\gamma = 0$.

Условие $\exists X(ZDOneMany(M_1, M_2, X) \wedge M^2 = XMX^{-1})$, $X = diag[\xi, \eta, \ldots, \eta]$, дает либо соотношение

$$\begin{pmatrix} \alpha^2 & \alpha\beta + \beta\delta & & & \\ 0 & \delta^2 & & & \\ & & a^2 & & \\ & & & \ddots & \\ & & & & a^2 \end{pmatrix} = \begin{pmatrix} \alpha & \xi\eta^{-1}\beta & & & \\ 0 & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix},$$

откуда $\alpha = \delta = a = 1$, либо соотношение

$$\begin{pmatrix} \alpha^2 & 0 & & & \\ \alpha\gamma + \gamma\delta & \delta^2 & & & \\ & & a^2 & & \\ & & & \ddots & \\ & & & & a^2 \end{pmatrix} \begin{pmatrix} \alpha & 0 & & & \\ \eta\xi^{-1}\gamma & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix},$$

откуда $\alpha = \delta = a = 1$, и, следовательно, либо $M = B_{12}(\beta)$, либо $M = B_{21}(\gamma)$. □

Лемма 3.26. *Существует формула*

$$MainUnit_{1,2}(M_1, M_2, M),$$

истинная только лишь для матрицы $M = \Phi_N B_{12}(1)$.

Доказательство. Рассмотрим формулу

$$
\begin{aligned}
MainUnit_{1,2}(M_1, M_2, M) = Main(M_1, M_2, M) \wedge (M \neq 1) \wedge \\
\wedge \big((M_1^{i_1^1} M_2^{j_1^1} \dots M_1^{i_{k(1)}^1} M_2^{j_{k(1)}^1}) \cdot M \cdot (M_2^{-j_{k(1)}^1} M_1^{-i_{k(1)}^1} \dots M_2^{-j_1^1} M_1^{-i_1^1}) \cdot \\
\cdot (M_1^{i_1^2} M_2^{j_1^2} \dots M_1^{i_{k(2)}^2} M_2^{j_{k(2)}^2}) \cdot M \cdot (M_1^{i_1^2} M_2^{j_1^2} \dots M_1^{i_{k(2)}^2} M_2^{j_{k(2)}^2}) = \\
= (M_1^{i_1^2} M_2^{j_1^2} \dots M_1^{i_{k(2)}^2} M_2^{j_{k(2)}^2}) \cdot M \cdot \\
\cdot (M_1^{i_1^2} M_2^{j_1^2} \dots M_1^{i_{k(2)}^2} M_2^{j_{k(2)}^2})(M_1^{i_1^1} M_2^{j_1^1} \dots M_1^{i_{k(1)}^1} M_2^{j_{k(1)}^1}) \cdot M \cdot \\
\cdot (M_1^{i_1^1} M_2^{j_1^1} \dots M_1^{i_{k(1)}^1} M_2^{j_{k(1)}^1}) \cdot M \big),
\end{aligned}
$$

где

$$
\begin{aligned}
(2,3) = (1,2,\dots,n)^{i_1^1}(1,2)^{j_1^1} \dots (1,2,\dots,n)^{i_{k(1)}^1}(1,2)^{j_{k(1)}^1}, \\
(1,3) = (1,2,\dots,n)^{i_1^2}(1,2)^{j_1^2} \dots (1,2,\dots,n)^{i_{k(2)}^2}(1,2)^{j_{k(2)}^2}.
\end{aligned}
$$

Так как любая матрица, удовлетворяющая формуле $Main(M_1, M_2, M)$, может иметь либо вид $\Phi_N B_{12}(x)$, либо $\Phi_N B_{21}(x)$, то мы получаем одно из двух соотношений: либо

$$
\begin{aligned}
S_{(2,3)}\Phi_N^{-1}(M)S_{(2,3)}S_{(1,3)}\Phi_N^{-1}(M)S_{(1,3)} = S_{(1,3)}\Phi_N^{-1}(M)S_{(1,3)}S_{(2,3)}\Phi_N^{-1}(M)S_{(2,3)}\Phi_N^{-1}(M) \Rightarrow \\
\Rightarrow \begin{pmatrix} 1 & x^2 & x \\ 0 & 1 & 0 \\ 0 & x & 1 \end{pmatrix} = \begin{pmatrix} 1 & x & x \\ 0 & 1 & 0 \\ 0 & x & 1 \end{pmatrix} \Rightarrow \\
x^2 = x \Rightarrow x = 1 \Rightarrow M = \Phi_N B_{12}(1),
\end{aligned}
$$

либо

$$
\begin{aligned}
S_{(2,3)}\Phi_N^{-1}(M)S_{(2,3)}S_{(1,3)}\Phi_N^{-1}(M)S_{(1,3)} = S_{(1,3)}\Phi_N^{-1}(M)S_{(1,3)}S_{(2,3)}\Phi_N^{-1}(M)S_{(2,3)}\Phi_N^{-1}(M) \Rightarrow \\
\Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & x \\ x & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ x^2 + x & 1 & x \\ x & 0 & 1 \end{pmatrix} \Rightarrow x^2 + x = 0,
\end{aligned}
$$

что невозможно. □

Лемма 3.27. *Существует формула $Main_{1,2}(M_1, M_2, M)$, истинная в полугруппе $G_n(R)$ для матриц $\Phi_N(B_{12}(x))$, $x \in R \cup \{0\}$, и только для них.*

Доказательство. Рассмотрим формулу

$$
Main_{1,2}(M_1, M_2, M) := Main(M_1, M_2, M) \wedge \forall X (MainUnit_{1,2}(X) \Rightarrow XM = MX).
$$

Из того, что матрица M удовлетворяет формуле $Main(M_1, M_2, M)$, следует, что $M = \Phi_N(B_{12}(x))$ или $\Phi_N(B_{21}(x))$ для некоторого $x \in R$. Во втором случае вторая часть формулы влечет

$$
\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1+x & 1 \\ x & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ x & 1+x \end{pmatrix} \Rightarrow x = 0.
$$

□

Лемма 3.28. *Существуют формулы*

$$Addit_n(M_1, M_2, X_1, X_2, X_3) \text{ и } Multipl_n(M_1, M_2, X_1, X_2, X_3),$$

истинные в полгруппе $G_n(R)$ для тех и только тех матриц X_1, X_2, X_3, которые имеют вид $X_1 = \Phi_N(B_{12}(x_1))$, $X_2 = \Phi_N(B_{12}(x_2))$, $X_3 = \Phi_N(B_{12}(x_3))$, где $x_1, x_2, x_3 \in R_+ \cup \{0\}$, и, соответственно, либо $x_3 = x_1 + x_2$, либо $x_3 = x_1 \cdot x_2$.

Доказательство. Искомые формулы имеют вид

$$\begin{aligned} Addit_n(M_1, M_2, X_1, X_2, X_3) &:= Main_{1,2}(M_1, M_2, X_1)\wedge \\ &\wedge Main_{1,2}(M_1, M_2, X_2) \wedge Main_{1,2}(M_1, M_2, X_3) \wedge X_3 = X_1 \cdot X_2 \end{aligned}$$

и

$$\begin{aligned} Multipl_n(M_1, M_2, X_1, X_2, X_3) &:= Main_{1,2}(M_1, M_2, X_1)\wedge \\ &\wedge Main_{1,2}(M_1, M_2, X_2) \wedge Main_{1,2}(M_1, M_2, X_3)\wedge \\ &\wedge (M_1^{i_1^1} M_2^{j_1^1} \dots M_1^{i_{k(1)}^1} M_2^{j_{k(1)}^1}) \cdot X_1 \ \cdot (M_1^{i_1^1} M_2^{j_1^1} \dots M_1^{i_{k(1)}^1} M_2^{j_{k(1)}^1})\times \\ &\times (M_1^{i_1^2} M_2^{j_1^2} \dots M_1^{i_{k(2)}^2} M_2^{j_{k(2)}^2}) \cdot X_2 \cdot (M_1^{i_1^2} M_2^{j_1^2} \dots M_1^{i_{k(2)}^2} M_2^{j_{k(2)}^2}) = \\ &= (M_1^{i_1^2} M_2^{j_1^2} \dots M_1^{i_{k(2)}^2} M_2^{j_{k(2)}^2}) \cdot X_2 \cdot (M_1^{i_1^2} M_2^{j_1^2} \dots M_1^{i_{k(2)}^2} M_2^{j_{k(2)}^2})\times \\ &\times (M_1^{i_1^1} M_2^{j_1^1} \dots M_1^{i_{k(1)}^1} M_2^{j_{k(1)}^1}) \cdot X_1 \cdot (M_1^{i_1^1} M_2^{j_1^1} \dots M_1^{i_{k(1)}^1} M_2^{j_{k(1)}^1}) \cdot X_3, \end{aligned}$$

где

$$\begin{aligned} (2,3) &= (1,2,\dots,n)^{i_1^1}(1,2)^{j_1^1} \dots (1,2,\dots,n)^{i_{k(1)}^1}(1,2)^{j_{k(1)}^1}, \\ (1,3) &= (1,2,\dots,n)^{i_1^2}(1,2)^{j_1^2} \dots (1,2,\dots,n)^{i_{k(2)}^2}(1,2)^{j_{k(2)}^2}. \end{aligned}$$

Первая формула совершенно очевидна, а вторая следует из соотношения

$$B_{13}(x_1)B_{32}(x_2) = B_{32}(x_2)B_{13}(x_1)B_{12}(x_1x_2).$$

□

Докажем теперь теорему 3.2.

Доказательство. 1. Пусть $R_+ \equiv S_+$. Покажем, что $G_n(R) \equiv G_n(S)$.

Действительно, пусть рассматривается полугруппа $G_n(R)$ ($n \geqslant 3$) и какое-нибудь предложение группового языка

$$\mathcal{U} = (Q_1 X_1) \dots (Q_r X_r) \mathcal{B}(X_1, \dots, X_r) \ (Q_i = \exists, \forall).$$

Матрица $X \in G_n(R)$ есть набор из n^2 элементов полукольца $R_+ \cup \{0\}$ $\{x_{ij}\}$ с условием существования в $\mathrm{GL}_n(R)$ обратной матрицы. Это условие можно выразить следующим образом. Пусть $\mathcal{J}_n$ — это множество $\{1, \dots, n\}$. Тогда получим

$$\exists y_{11}, \dots, \exists y_{nn} : \bigvee_{S \subseteq \mathcal{J}_n \times \mathcal{J}_n} \bigwedge_{i,k \in \mathcal{J}_n \times \mathcal{J}_n} \Big(\delta_{ik} + \sum_{\langle j,k \rangle \in S} x_{ij} y_{jk} = \sum_{\langle j,k \rangle \notin S} x_{ij} y_{jk} \bigwedge \\ \bigwedge \delta_{ik} + \sum_{\langle i,j \rangle \in S} y_{ij} x_{ij} = \sum_{\langle i,j \rangle \notin S} y_{ij} x_{jk} \Big).$$

Обозначим это условие на матрицу X через $\mathbf{G}(X)$.

Тогда истинность $\mathcal{U}$ на $G_n(R)$ очевидно, равносильна истинности на R_+ предложения $\mathcal{U}_R$, получающегося из $\mathcal{U}$ следующим процессом (ср. [3]):

а) в формуле $\mathcal{B}(X_1, \dots, X_r)$ отношения вида $X_i = X_j$ и $X_i = X_j X_k$ заменяем соответственно формулами

$$\bigwedge_{\lambda,\mu} (x_{i\lambda\mu} = x_{j\lambda\mu}) \text{ и } \bigwedge_{\lambda,\mu} (x_{i\lambda\mu} = x_{j\lambda 1} x_{k1\mu} + \dots + x_{j\lambda n} x_{kn\mu}).$$

б) Если формула $\mathcal{B}_{i+1} = (Q_{i+1} X_{i+1}) \dots (Q_r X_r) \mathcal{B}$ преобразовывается в формулу $\mathcal{Q}_{i+1}$, то формула $\mathcal{B}_i = (\forall X_i) \mathcal{B}_{i+1}$ преобразовывается в формулу

$$\forall x_{i11} \dots \forall x_{inn} (\mathbf{G}(x_{i11}, \dots, x_{inn}) \Rightarrow \mathcal{Q}_{i+1}),$$

а формула $\mathcal{B}_i = (\exists X_i) \mathcal{B}_{i+1}$ преобразовывается в формулу

$$\exists x_{i11} \dots \exists x_{inn} (\mathbf{G}(x_{i11}, \dots, x_{inn}) \wedge \mathcal{Q}_{i+1}).$$

Следовательно, каждое предложение $\mathcal{U}$ группового языка можно указанным выше способом преобразовать в предложение $\mathcal{U}_R$ кольцевого языка. Вид предложения $\mathcal{U}_R$ не зависит от базисного кольца. Таким образом, истинность $\mathcal{U}$ на $G_n(R)$ равносильна истинности $\mathcal{U}_R$ на R. Истинность же $\mathcal{U}_R$ на R равносильна истинности $\mathcal{U}_R$ на S, так как $R \equiv S$. Поэтому истинность $\mathcal{U}$ на $G_n(R)$ равносильна истинности $\mathcal{U}$ на $G_n(S)$, и, следовательно, $G_n(R) \equiv G_n(S)$.

2. Теперь докажем обратную импликацию. Пусть полугруппы $G_n(R)$ и $G_m(S)$ элементарно эквивалентны. Из леммы 3.17 тогда следует, что $m = n$, поэтому мы можем считать, что имеем дело с полугруппами $G_n(R)$ и $G_n(S)$.

Теперь докажем, что $R_+ \equiv S_+$. Пусть мы имеем некоторое предложение φ кольцевого языка. Переведем его в предложение $\overline{\varphi}$ группового языка по следующему алгоритму:

предложение $\overline{\varphi}$ имеет вид

$$\exists M_1 \exists M_2 (Cycle_n(M_1) \wedge Transp_n(M_1, M_2) \wedge \varphi'(M_1, M_2)),$$

где формула φ получается из предложения φ следующими заменами подформул, входящих в φ:

1) подформула $\forall x \psi$ переводится в подформулу $\forall X (Main_{1,2}(M_1, M_2, X) \Rightarrow \psi')$;

2) подформула $\exists x \psi$ переводится в подформулу $\exists X (Main_{1,2}(M_1, M_2, X) \wedge \psi')$;

3) подформула $x = y$ переводится в подформулу $X = Y$;

4) подформула $x = y + z$ переводится в подформулу $Addit_n(M_1, M_2, X, Y, Z)$;

5) подформула $x = yz$ переводится в подформулу $Multipl_n(M_1, M_2, X, Y, Z)$.

Очевидно, что предложение φ истинно в полукольце R_+ тогда и только тогда, когда предложение $\overline{\varphi}$ истинно в полугруппе $G_n(R)$. Так как полугруппы $G_n(R)$ и $G_n(S)$ элементарно эквивалентны, то истинность предложения $\overline{\varphi}$ в полугруппе $G_n(R)$ равносильна его истинности в полугруппе $G_n(S)$, что в свою очередь равносильно истинности предложения φ в полукольце S_+. Значит, полукольца R_+ и S_+ элементарно эквивалентны.

$\square$

Глава 4

Связь элементарной эквивалентности производных структур с эквивалентностью в логике второго порядка исходных структур

Введение

В этой главе мы рассматриваем элементарные свойства категорий модулей над кольцом, колец эндоморфизмов почти свободных модулей бесконечного ранга над кольцами и групп автоморфизмов свободных модулей бесконечного ранга над кольцами, а также колец эндоморфизмов абелевых p-групп.

Впервые вопросы связи элементарных свойств некоторых моделей с элементарными свойствами производных моделей были рассмотрены в 1961 г. А.И. Мальцевым в работе [37]. Он доказал, что группы $G_n(K)$ и $G_m(L)$ ($G = \mathrm{GL}, \mathrm{SL}, \mathrm{PGL}, \mathrm{PSL}$, $n, m \geqslant 3$, K, L — поля характеристики 0) элементарно эквивалентны тогда и только тогда, когда $m = n$ и поля K и L элементарно эквивалентны.

Продолжение эта теория получила в 1992 году, когда с помощью конструкции ультарпроизведения и теоремы об изоморфизме [28] К.И. Бейдар и А.В. Михалев в работе [81] нашли общий подход к проблемам элементарной эквивалентности различных алгебраических структур и обобщили теорему Мальцева для случая, когда K и L Являются телами и ассоциативными кольцами.

Продолжением исследований в этой области явились работы Е.И. Буниной 1998–2001 гг. (см. [181], [183], [192]), в которых результаты А.И. Мальцева была распространены на унитарные линейные группы над телами и ассоциативными кольцами с инволюцией, а также на группы Шевалле над полями.

В 2000 г. В. Толстых в работе [169] рассмотрел связь свойств второго порядка для тел и свойств первого порядка групп автоморфизмов бесконечномерных пространств над этими телами.

В этой главе мы рассматриваем связь свойств второго порядка ассоциативных колец и свойств первого порядка категорий модулей, колец эндоморфизмов, групп автоморфизмов и проективных пространств модулей бесконечного ранга над этими кольцами, а также находим необходимые и достаточные условия элементарной эквивалентности колец эндоморфизмов абелевых p-групп.

4.1 Языки и модели второго порядка

В этой главе помимо языков первого порядка мы будем вынуждены рассматривать языки второго порядка, в которых можно также навешивать кванторы на предикатные символы, то есть использовать предикатные символы как переменные. Такие языки будут описаны ниже. Мы будем говорить, что две модели одного языка (например, второго порядка) $\mathcal{L}$ эквивалентны в этом языке, если для любого предложения языка $\mathcal{L}$ его истинность в первой модели равносильна его истинности во второй модели.

Мы считаем известными основные понятия теории моделей — понятия языка первого порядка, формул первого порядка, теории, модели теории, выполнимости формулы в модели.

Так как описание понятий, связанных с языками и теориями второго порядка, встречается редко, то мы приведем его здесь.

Язык $\mathcal{L}_2$ второго порядка — это совокупность символов, состоящая из 1) скобок (,); 2) связок $\wedge$ ("и") и $\neg$ ("не"); 3) квантора $\forall$ (для всех); 4) символа равенства $=$; 5) счетного множества предметных переменных x_i; 6) счетного множества предикатных переменных P_i^l; 7) не более чем счетного множества предикатных символов Q_i^n $(n \geqslant 1)$; 8) не более чем счетного множества функциональных символов F_i^n $(n \geqslant 1)$; 9) не более чем счетного множества константных символов c_i.

Термы языка $\mathcal{L}_2$ определяются следующим образом:

1) предметная переменная есть *терм*;

2) константный символ есть *терм*;

3) если F^n — некоторый функциональный символ, а $t_1, \dots, t_n$ — термы, то $F^n(t_1, \dots, t_n)$ — *терм*;

4) Знакосочетание является *термом* в том и только том случае, если это можно показать с помощью конечного числа применений правил 1)–3).

Таким образом, термы языка $\mathcal{L}_2$ совпадают с термами языка $\mathcal{L}$.

Элементарные формулы языка $\mathcal{L}_2$ определяются так:

1) если t_1 и t_2 — термы языка $\mathcal{L}_2$, то $t_1 = t_2$ — элементарная формула;

2) если P^l — предикатная переменная, $t_1, \dots, t_l$ — термы, то знакосочетание $P^l(t_1, \dots, t_l)$ является элементарной формулой;

2) Если Q^n — некоторый предикатный символ, а $t_1, \dots, t_n$ — термы, то знакосочетание $Q^n(t_1, \dots, t_n)$ — это элементарная формула.

Например элементарные формулы группового языка второго порядка имеют вид $x_i = x_j$, $x_i = x_j \cdot x_k$ и $P^l(x_{i_1}, \dots, x_{i_l})$, $l \geqslant 1$.

Формулы языка $\mathcal{L}_2$ определяются следующим образом:

1) всякая элементарная формула есть *формула*;

2) если φ и ψ — формулы, x — предметная переменная, то каждое из знакосочетаний $(\neg\varphi)$, $(\varphi \wedge \psi)$, $(\forall x\, \varphi)$ есть *формула*;

3) если P^l — предикатная переменная, φ — формула, то знакосочетание

$$(\forall P^l(v_1, \dots, v_l)\varphi)$$

является формулой.

4) знакосочетание является *формулой* только в том случае, если это можно показать с помощью конечного числа применений правил 1)–3).

Договоримся о сокращениях (дополнительных к обычным сокращениям для языка первого порядка):

$\exists P^l(v_1, \dots, v_l)\varphi$ есть сокращение для $\neg(\forall P^l(v_1, \dots, v_l)(\neg\varphi))$;

$\forall P_1^{l_1}(v_1, \dots, v_{l_1}) \dots \forall P_n^{l_n}(v_1, \dots, v_{l_n})\varphi$ есть сокращение для $(\forall P_1^{l_1}(v_1, \dots, v_{l_1})) \dots (\forall P_n^{l_n}(v_1, \dots, v_{l_n}))\varphi$;

$\exists P_1^{l_1}(v_1, \dots, v_{l_1}) \dots \exists P_n^{l_n}(v_1, \dots, v_{l_n})\varphi$ есть сокращение для $(\exists P_1^{l_1}(v_1, \dots, v_{l_1})) \dots (\exists P_n^{l_n}(v_1, \dots, v_{l_n}))\varphi$.

Введем понятие *свободного* и *связанного* вхождения предикатной переменной в формулу языка $\mathcal{L}_2$.

1) Все вхождения всех предикатных переменных элементарной формулы являются свободными вхождениями.

2) Всякое свободное (связанное) вхождение переменной P^l в формулу φ является свободным (связанным) вхождением переменной P^l в формулы $(\neg\varphi)$, $(\varphi \wedge \psi)$ и $(\psi \wedge \varphi)$.

3) Каково бы ни было вхождение переменной P^l в формулу φ, вхождение переменной P^l в формулу $\forall P^l(v_1, \dots, v_l)\varphi$ является связанным. Если вхождение переменной P_1^l в формулу φ свободно (связанно), то таковым же является вхождение переменной P_1^l в формулы $\forall x\varphi$ и $\forall P_2^m(v_1, \dots, v_m)\varphi$.

Всякую формулу, *свободные* предметные и предикатные переменные которой образуют подмножество множества

$$\{x_1, \dots, x_n, P_1^{l_1}, \dots, P_k^{l_k}\},$$

будем обозначать через $\varphi(x_1, \dots, x_n, P_1^{l_1}, \dots, P_k^{l_k})$.

К обычным логическим аксиомам языка первого порядка добавляется еще одна чисто логическая аксиома:

6. $(\forall P^n(v_1, \dots, v_n)(\psi \Rightarrow \varphi) \Rightarrow (\psi \Rightarrow (\forall P^n(v_1, \dots, v_n)\varphi))$, если ψ не содержит свободных вхождений переменной P^n.

К аксиомам равенства тоже добавляется новая аксиома:

4. $\forall P^n(v_1, \dots, v_n)(y = z \Rightarrow (P^n(x_1, \dots, x_{i-1}, y, x_{i+1}, \dots, x_n) \Leftrightarrow P^n(x_1, \dots, x_{i-1}, z, x_{i+1}, \dots, x_n))$.

Кроме того, правило вывода по обобщению можно заменить на "из формулы φ выводится $\forall x\varphi$ и $\forall P^n(v_1, \dots, v_n)\varphi$".

Моделью языка второго порядка $\mathcal{L}_2$ называется пара $\mathcal{U} = \langle A, I\rangle$, состоящая из объекта A (т. е. класса или множества) и какого-либо соответствия I, относящего каждому предикатному символу Q^n некоторое n-местное отношение в A, каждому функциональному символу F^n — некоторую n-местную операцию в A, а каждой константе c — некоторый элемент из A.

Теперь дадим определение выполнимости. Пусть φ — произвольная формула языка $\mathcal{L}_2$, все переменные которой, свободные и связанные, содержатся среди $x_1, \dots, x_q, P_1^{l_1}, \dots, P_s^{l_s}$, и пусть $a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}$ — произвольная последовательность, где $a_1, \dots, a_q$ — элементы множества A, $b_i^{l_i} \subset A^{l_i}$. Мы определяем предикат φ *выполняется на последовательности* $a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}$ *в модели* $\mathcal{U}$.

1. Значение терма $t(x_1, \dots, x_q, P_1^{l_1}, \dots, P_s^{l_s})$ на последовательности $a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}$ определяется следующим образом (мы обозначаем это значение через $t[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}]$):

1) если t — это переменная x_i, то $t[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}] = a_i$;

2) если t — это символ константы c, то $t[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}] = I(c)$.

3) если t — это $F^m(t_1, \dots, t_m)$, где $t_1(x_1, \dots, x_q, P_1^{l_1}, \dots, P_s^{l_s}), \dots, t_m(x_1, \dots, x_q, P_1^{l_1}, \dots, P_s^{l_s})$ — термы, то

$$t[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}] = \\ = I(F^m)(\langle t_1[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}], \dots, t_m[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}]\rangle).$$

2. 1) Пусть
$$\varphi(x_1, \dots, x_q, P_1^{l_1}, \dots, P_s^{l_s})$$
— элементарная формула вида $t_1 = t_2$, где $t_1(x_1, \dots, x_q, P_1^{l_1}, \dots, P_s^{l_s})$ и $t_2(x_1, \dots, x_q, P_1^{l_1}, \dots, P_s^{l_s})$ — термы. Формула φ *выполняется* на элементах $a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}$, если

$$t_1[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}] = t_2[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}].$$

2) Пусть $\varphi(x_1, \dots, x_q, P_1^{l_1}, \dots, P_s^{l_s})$ — элементарная формула вида $Q^n(t_1, \dots, t_n)$, где Q^n — n-местный предикатный символ, а $t_1(x_1, \dots, x_q, P_1^{l_1}, \dots P_s^{l_s}), \dots, t_n(x_1, \dots, x_q, P_1^{l_1}, \dots, P_s^{l_s})$ — термы. Формула φ *выполняется* на элементах $a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}$, если

$$\langle t_1[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}], \dots, t_n[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}]\rangle \in I(Q^n).$$

3) Пусть $\varphi(x_1, \dots, x_q, P_1^{l_1}, \dots, P_s^{l_s})$ — элементарная формула вида $P_i^{l_i}(t_1, \dots, t_{l_i})$, где $t_1(x_1, \dots, x_q, P_1^{l_1}, \dots P_s^{l_s}), \dots, t_n(x_1, \dots, x_q, P_1^{l_1}, \dots, P_s^{l_s})$ — термы. Формула φ *выполняется* на элементах $a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}$, если

$$\langle t_1[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}], \dots, t_n[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}]\rangle \in b_i^{l_i}.$$

3. Пусть φ — формула языка $\mathcal{L}_2$, все свободные и связанные переменные которой содержатся среди $x_1, \dots, x_q, P_1^{l_1}, \dots, P_s^{l_s}$.

1) Если φ имеют вид $\theta_1 \wedge \theta_2$, то

$$\mathcal{U} \vDash \varphi[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}] \text{ тогда и только тогда, когда} \\ \mathcal{U} \vDash \Theta_1[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}] \text{ и } \mathcal{U} \vDash \Theta_2[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}].$$

2) Если φ имеет вид $\neg\Theta$, то

$$\mathcal{U} \vDash \varphi[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}] \text{ тогда и только тогда, когда} \\ \text{неверно, что } \mathcal{U} \vDash \Theta[a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s}].$$

3) Если φ имеет вид $\forall x_i \psi$, где $i \leqslant q$, то

$\mathcal{U} \vDash \varphi[a_1, \ldots, a_q, b_1^{l_1}, \ldots, b_s^{l_s}]$ тогда и только тогда, когда
$\mathcal{U} \vDash \psi[a_1, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_q, b_1^{l_1}, \ldots, b_s^{l_s}]$ для любого $a \in A$.

4) Если φ имеет вид $\forall P_i^{l_i}(v_1, \ldots v_{l_i})\psi$, где $i \leqslant s$, то

$\mathcal{U} \vDash \varphi[a_1, \ldots, a_q, b_1^{l_1}, \ldots, b_s^{l_s}]$ тогда и только тогда, когда
$\mathcal{U} \vDash \psi[a_1, \ldots, a_q, b_1^{l_1}, \ldots, b_{i-1}^{l_{i-1}}, b, b_{i+1}^{l_{i+1}}, \ldots, b_s^{l_s}]$ для любого $b \subset A^{l_i}$.

Утверждение о том, что

$$\mathcal{U} \models \varphi(x_1, \ldots, x_p, P_1^{l_1}, \ldots, P_t^{l_t})[a_1, \ldots, a_q, b_1^{l_1}, \ldots, b_s^{l_s}]$$

зависит только от значений $a_1, \ldots, a_p, b_1^{l_1}, \ldots, b_t^{l_t}$, где $p < q$, $s < t$, звучит совершенно так же, как и это утверждение для языков и теорий первого порядка.

Мы будем говорить, что две модели языка второго порядка эквивалентны в языке второго порядка, если для любого предложения этого языка его истинность в первой модели равносильна его истинности во второй модели.

4.2 Элементарная эквивалентность категорий модулей над кольцами

4.2.1 Некоторые сведения о категории модулей над кольцами

Для удобства приведем некоторые факты о категории $\mathrm{mod} - R$ (см. [62]).

Основные определения и понятия теории категорий можно найти в книге [62].

Для объектов категории mod-R всех модулей над фиксированным кольцом R (категория, которая будет нас интересовать) следующие понятия являются определимыми в языке первого порядка:

Модули X и Y изоморфны;
Модуль X вложим в модуль Y;
Модуль X наложим на модуль Y;
Модуль X изоморфен прямому слагаемому модуля Y;
Модуль X изоморфен прямой сумме модулей Y и Z;
Модуль X — проективный;
Модуль X — инъективный;
Модуль X — образующий;
Модуль X — кообразующий;

В общем случае формульными не являются следующие свойства модулей категории mod-R:

$$\text{Модуль } X \text{ свободен;}$$
$$\text{Модуль } X \text{ равен } A^I \text{ для некоторого множества } A;$$
$$\text{Модуль } X \text{ равен } A^{(I)} \text{ для некоторого множества } A.$$

Фактормодулем модуля M по подмодулю N называется модуль, состоящий из классов эквивалентности $a \sim b \Leftrightarrow a - b \in N$ и такой, что $(a + N)r = ar + N$. Свойство модуля L быть изоморфным фактормодулю модуля M является свойством первого порядка:

$\exists f \in Mor(M, L)(f$ — эпиморфизм).

Пусть $\mathbf{C}$ — конкретная категория. Если B и A — ее объекты и $B \subseteq A$, то B — *подобъект* в A. Если A — подмножество, а N — подобъект в A, то S *порождает* N, если N является пересечением всех подобъектов объекта A, содержащих S. В этом случае употребляется обозначение $N = (S)$. Подобъект M объекта A называется *конечно порожденным*, *счетно порожденным* или *порожденным* a *элементами*, если $M = (T)$, где $|T| < \omega_0$, $|T| \leqslant \omega_0$ или $|T| \leqslant a$ соответственно. Эти свойства в общем случае не являются элементарными.

Семейство $\{x_i\}_{i \in I}$, которое порождает подмодуль N модуля M, называется *системой образующих* подмодуля N. Если же каждый элемент модуля лишь одним способом раскладывается в линейную комбинацию образующих, то $\{x_i\}_{i \in I}$ называют *базисом* модуля N, а мощность множества I — *базисным числом* этого модуля. Семейство $\{x_i\}_{i \in I}$ называется *линейно независимым над* R.

Модуль $R^{(I)}$ является свободным модулем над множеством I.

Предложение 4.1. 1) *Если R — кольцо, а X — объект категории mod-R, то существует множество индексов I и некоторый эпиморфизм ${}^R(I) \to X$, т. е. любой R-модуль изоморфен фактормодулю свободного R-модуля.*

2) *Если $\{u_i : R \to R^{(I)}\}_{i \in I}$ — инъекции в прямую сумму, то $\{u_i(1)\}_{i \in I}$ — базис свободного модуля $R^{(I)}$.*

3) *Объект R является образующим в категории mod-R.*

Базисное число, вообще говоря, зависит от выбора базиса и, следовательно, не может служить инвариантом модуля $F = R^{(I)}$. Однако оно не зависит от выбора базиса, если F — свободный модуль над бесконечным множеством I.

Предложение 4.2. 1. *R-модуль P проективен тогда и только тогда, когда модуль P изоморфен прямому слагаемому свободного модуля.*

2. *Модуль P конечно порожден и проективен тогда и только тогда, когда $R^{(n)} \cong P \oplus X$ для некоторого целого числа $n > 0$ и модуля X.*

Предложение 4.3. *Модуль $M \in$ mod-R является образующим тогда и только тогда, когда любой R-модуль X является фактормодулем модуля $M^{(I)}$ для некоторого множества I.*

Предложение 4.4. *Объект G категории mod-R является образующим тогда и только тогда, когда существуют целое число $n > 0$ и изоморфизм $G^{(n)} \cong R \oplus X$ для некоторого объекта $X \in$ mod-R.*

Модуль M называется *простым*, если он имеет ровно два подмодуля — 0 и M. Если M — некоторый модуль, а S — его подмодуль, то M/S прост тогда и только тогда, когда S — максимальный подмодуль. Любой конечно порожденный модуль M имеет максимальные подмодули. Таким образом, для любого кольца R в категории mod-R содержатся какие-то простые модули (в принципе, они все могут быть между собой изоморфны). Очевидно, что свойство модуля быть простым определимо в языке первого порядка.

Предложение 4.5. *Для любого простого модуля M, любой подмодуль P модуля $M^{(I)}$ изоморфен $M^{(J)}$ для некоторого множества J, мощность которого не превосходит мощность множества I.*

Модуль $P \in$ mod-R называется *прообразующим* модулем, если он является образующим конечно порожденным проективным модулем.

Кольца R и S называются *подобными* (обозначается через $R \sim S$), если существует прообразующий модуль $P \in$ mod-R и изоморфизм колец $S \cong \mathrm{End}\,_R P$.

.

Теорема 4.1. (Теорема Мориты, [62], теорема 4.29) *Следующие условия эквивалентны*:

1) *категории mod-Rmod-S эквивалентны*;

2) *кольца R и S подобны.*

Кроме того, в дальнейшем нам потребуется следующая теорема из книги [62] (см. п. 4.35).

Теорема 4.2. *Если A — коммутативное кольцо и кольцо B подобно кольцу A, то A изоморфно центру кольца B. Таким образом, два коммутативных кольца подобны тогда и только тогда, когда они изоморфны.*

4.2.2 Выделение прообразующего объекта в категории mod-R

Пусть формула $Simp(M)$ выделяет в категории mod-R простые модули. Рассмотрим объект X, удовлетворяющий формуле

$$\begin{aligned} Sum^{\omega}(X, M) := Simp(M) \wedge (X \oplus M \cong X) \wedge \\ \wedge\, (\forall Y \in Obj(Y \oplus M \cong Y \Rightarrow \exists Q \in Obj(Y \cong X \oplus Q)). \end{aligned}$$

Свойство $Y \oplus M \cong Y$ означает, что $Y \cong M^{(\omega)} \oplus Z$ для некоторого объекта $Z \in$ mod-R. Следовательно, X — это модуль, содержащий $M^{(\omega)}$ в виде прямого слагаемого и являющийся прямым слагаемым в $M^{(\omega)}$. Из предложения 4.5 видно, что в этом случае $X \cong M^{(\omega)}$. Таким образом, для любого простого модуля M формула $Sum^{\omega}_M(X) := Sum^{\omega}(X, M)$ выделяет модуль $M^{(\omega)}$.

Формула

$$\begin{aligned} Sum^{Fin}(X, M) := Sum^{Fin}_M(X) := \\ = Simp(M) \wedge \exists Y \in Obj(Sum^{\omega}_M(Y) \wedge \exists Q \in Obj(Y \cong X \oplus Q) \wedge X \ncong Y) \end{aligned}$$

истинна для всех конечных прямых сумм простого модуля M, и только для них.

Формула

$$Sum(X,M) := Sum_M(X) := Simp(M) \wedge \forall Y(Y \subset X \wedge Y \neq 0 \Rightarrow \exists P(Y \cong P \oplus M))$$

выделяет класс Sum_M всех прямых сумм модуля M. Введем на этом классе отношение

$$(X \leqslant Y) := \exists f \in Mor(X,Y)(f \text{ — мономорфизм}).$$

Класс Sum_M вполне упорядочен относительно $\leqslant$ и существует естественная биекция (отождествление) класса Sum_M с классом Cn всех кардинальных чисел.

Формула

$$\begin{aligned} Pret(P) := (P \text{ — проективный}) \wedge (P \text{ — образующий}) \wedge \\ \wedge \exists M \in Obj \exists f \in Mor(P,M)(Simp(M) \wedge (f \text{ — эпиморфизм})) \end{aligned}$$

выполняется для всех проективных образующих модулей, имеющих максимальные подмодули, в том числе она обязана выполняться для проективных образующих конечно порожденных (*прообразующих*) модулей.

Через $\langle M, f\rangle^P$ (или $\langle M^P, f^P\rangle$) мы будем обозначать пару (простой модуль M, эпиморфизм f из P на M) для модуля P такого, что $Pret(P)$.

Рассмотрим модуль N, удовлетворяющий формуле $Sum^{Fin}_{M^P}(N)$. Такой модуль N должен иметь вид $M^{(n)}$ для некоторого натурального n. Будем обозначать такой модуль через $N_{fd}(M)$.

Рассмотрим теперь формулу

$$\begin{gathered} Under(P,M,N,X) := Under_{M^P,N}(X) := N \cong N_{fd}(M) \wedge \\ \wedge \exists g \in Mor(X,N)(g \text{ — эпиморфизм} \wedge \\ \wedge \forall i_M \in Mor(M,N) \forall p_M \in Mor(N,M)(p_m \circ i_M = 1_M \Rightarrow \\ \Rightarrow \exists i \in Mor(P,X) \exists p \in Mor(X,P)(p \circ i = 1_P \wedge g \circ i = i_M \circ f \wedge f \circ p = p_M \circ g)) \wedge \\ \wedge \forall i_M, i_M{}' \in Mor(M,N) \forall p_M, p_M{}' \in Mor(M,M) \forall i, i' \in Mor(P,X) \\ \forall p, p' \in Mor(X,P)(p_M \circ i_M = p_M{}' \circ i_M{}' = 1_M \wedge p \circ i = p' \circ i' = 1_P \wedge \\ \wedge g \circ i = i_M \circ f \wedge f \circ p = p_M \circ g \wedge g \circ i' = i_M{}' \circ f \wedge f \circ p' = p_M{}' \circ g \wedge \\ \wedge p_M \circ i_M{}' = p_M{}' \circ i_M = 0 \Rightarrow p \circ i' = p' \circ i = 0). \end{gathered}$$

Эта формула означает, что

1) для модуля X существует такой эпиморфизм $g : X \to N$, что для любой пары (i_M, p_M), состоящей из вложения модуля M в модуль N и обратной проекции модуля N на модуль M существует пара (i,p), состоящая из вложения модуля P в модуль X и обратной проекции модуля X на модуль P, что диаграммы

$$\begin{array}{ccc} P & \xrightarrow{i} & X \\ \downarrow f & & \downarrow g \\ M & \xrightarrow{i_M} & N \end{array} \quad \text{и} \quad \begin{array}{ccc} P & \xleftarrow{p} & X \\ \downarrow f & & \downarrow g \\ M & \xleftarrow{p_M} & N \end{array}$$

коммутативны;

2) если вложения i_M и $i_M{}'$ модуля M в модуль N таковы, что из образы в N не пересекаются, то у соответствующих вложений $i, i' : P \to X$ образы также не пересекаются.

Посмотрим, как в этом случае устроен модуль X.

Предположим, что $N \cong M^{(n)} \cong M_1 \oplus \dots \oplus M_n$, где $M_i \cong M$ для любого $1 \leqslant i \leqslant n$. Пусть $i_l^M : M \to N$ и $p_l^M : N \to M$ таковы, что $rng\, i_l^M = M_l$ и $p_l^M \circ i_l^M = 1_M$. Этим парам вложений и проекций соответствуют пары (i_l, p_l) такие, что $i_l : P \to X$, $p_l : X \to P$, $p_l \circ i_l = 1_P$, при этом образы вложений i_l и i_m для различных l и m не пересекаются и независимы. Из этого следует, что модуль $P^{(n)}$ выделяется в X в виде прямого слагаемого. Нам остается рассмотреть модуль X' удовлетворяющий формуле

$$Und(P, M, N, X') := Und_{N,M^P}(X') := \forall X(Under_{M^P,N}(X) \Rightarrow \exists Q(X \cong X' \oplus X')).$$

Тогда мы получим модуль X', являющийся прямым слагаемым модуля $P^{(n)}$ и выделяющийся в $P^{(n)}$ прямым слагаемым.

Теперь рассмотрим следующую формулу:

$$Finite(P, X) \equiv Finite_P(X) \equiv \exists(M^P, f^P)\exists Y \in Obj\ (Sum_M^{Fin}(Y) \wedge Und_{Y,M^P}(X)))$$

Эта формула выделяет модули X со свойством

$$\exists n \in \omega \exists Q, Q'(X \oplus Q \cong P^{(n)} \wedge X \cong P^{(n)} \oplus Q'),$$

т. е. все модули вида $P^{(n)}$ и еще какие-то *конечно порожденные* модули.

Любой проективный конечно порожденный модуль есть прямое слагаемое модуля $R^{(n)}$ для некоторого $n \in \omega$, и, соответственно, если P — конечно порожденный проективный, то для любого образующего модуля S

$$P \oplus Q \cong S^{(m)}$$

для некоторого $m \in \omega$ и некоторого модуля Q. Если же модуль P не является конечно порожденным, то существует такой прообразующий модуль S, что P не может быть вложен в $S^{(n)}$ ни для какого $n \in \omega$.

Отсюда следует, что формула

$$\begin{aligned} Proobr(P) \equiv Pret(P) \wedge \forall S \in Obj \\ (Pret(S) \Rightarrow \exists X \in Obj(Finite_S(X) \wedge \exists Q \in Obj(P \oplus Q \cong X))) \end{aligned}$$

выполняется на прообразующих модулях, и только на них.

Таким образом, имея категорию mod-R, мы автоматически имеем (с помощью формулы $Proobr()$) класс всех прообразующих модулей этой категории.

Заметим также, что имея некоторый фиксированный прообразующий модуль P, мы также имеем класс модулей, являющихся прямыми слагаемыми в $P^{(I)}$ и одновременно содержащих $P^{(I)}$ в качестве прямого слагаемого. Очевидно, что такие модули имеют вид $P^{(I)} \oplus X$, где X — некоторый проективный модуль, вкладывающийся в $P^{(I)}$. Любой такой модуль можно представить в виде $R^{(I)} \oplus Y$, где Y — проективный модуль равзмерности, не большей $|I|$. Будем называть такие модули *почти свободными модулями размерности* $|I|$ *над кольцом* R.

4.2.3 Кольцо $\mathrm{End}_R P$

Рассмотрим некоторый прообразующий модуль P и множество $Mor(P, P)$. Операция умножения на этом множестве вводится как

$$(f = g \times h) := (f = g \circ h).$$

Введем теперь операцию сложения. Для этого рассмотрим модуль $P \oplus P$ с вложениями $i_1, i_2 \in Mor(P, P \oplus P)$ и проекциями $p_1, p_2 \in Mor(P \oplus P, P)$ с условиями $p_1 \circ i_1 = p_2 \circ i_2 = 1_P$, $p_1 \circ i_2 = p_2 \circ i_1 = 0$.

Для данного $f \in Mor(P, P)$ рассмотрим морфизм $Gr_f \in Mor(P \oplus P, P \oplus P)$, определяемый условиями

$$\begin{aligned} p_1 \circ Gr_f \circ i_1 &= 1_P, \\ p_2 \circ Gr_f \circ i_2 &= 1_P, \\ p_2 \circ Gr_f \circ i_1 &= 0, \\ p_1 \circ Gr_f \circ i_2 &= f. \end{aligned}$$

Очевидно, что отображение

$$Gr : Mor(P, P) \to Mor(P \oplus P, P \oplus P),$$
$$f \mapsto Gr_f$$

инъективно и что для любого морфизма $g \in Mor(P \oplus P, P \oplus P)$, удовлетворяющего условиям $p_1 \circ g \circ i_1 = p_2 \circ g \circ i_2 = 1_P$, $p_2 \circ g \circ i_1 = 0$ существует морфизм $f \in Mor(P, P)$ такой, что $Gr_f = g$.

Определим

$$(f = g + h) := (Gr_f = Gr_g \circ Gr_h).$$

Таким образом, мы ввели на множестве $Mor(P, P)$ структуру кольца, изоморфного кольцу $End_R(P)$.

Чтобы показать, что это действительно так, достаточно убедиться, что для любых трех эндоморфизмов $f, g, h \in \mathrm{End}_R P = Mor(P, P)$ соотношение $f = g + h$ выполнено тогда и только тогда, когда $Gr_f = Gr_g \circ Gr_h$. Рассмотрим морфизмы Gr_g и Gr_h и морфизм $G = Gr_g \circ Gr_h$. Отображения $k_1 \equiv i_1 \circ p_1$ и $k_2 \equiv i_2 \circ p_2$ из $Mor(P \oplus P, P \oplus P)$ таковы, что $\forall x \in P \oplus P (x = k_1(x) + k_2(x))$, т. е. $k_1 + k_2 = 1_{P \oplus P}$. Таким образом, $p_1 \circ G \circ i_1 = p_1 \circ Gr_g \circ Gr_h \circ i_1 = p_1 \circ Gr_g \circ 1_{P \oplus P} \circ Gr_h \circ i_1 = p_1 \circ Gr_g \circ (i_1 \circ p_1 + i_2 \circ p_2) \circ Gr_h \circ i_1 = p_1 \circ Gr_g \circ (i_1 \circ p_1 \circ Gr_h \circ i_1 + i_2 \circ p_2 \circ Gr_h \circ i_1) = p_1 \circ Gr_g \circ i_1 \circ 1_P + 0 = 1_P$, аналогично, $p_2 \circ G \circ i_2 = 1_P$, $p_2 \circ G \circ i_1 = 0$ и, наконец, $p_1 \circ G \circ i_2 = p_1 \circ Gr_g \circ Gr_h \circ i_2 = p_1 \circ Gr_g \circ (i_1 \circ p_1 + i_2 \circ p_2) \circ Gr_h \circ i_2 = (p_1 \circ Gr_g \circ i_1) \circ (p_1 \circ Gr_h \circ i_2) + (p_1 \circ Gr_g \circ i_2) \circ (p_2 \circ Gr_h \circ i_2) = g \circ 1_P + 1_P \circ h = g + h$. Отсюда следует искомая эквивалентность.

4.2.4 Случай конечных колец

Лемма 4.1. *Кольцо эндоморфизмов* $\mathrm{End}_R P$ *любого прообразующего модуля* P *категории* $mod\text{-}R$ *с конечным кольцом* R *конечно.*

Доказательство. Модуль P является подмодулем модуля $R^{(n)}$ для некоторого n. Так как кольцо R конечно, то модуль $R^{(n)}$ конечен, а значит, конечен и модуль P. Очевидно, что кольцо эндоморфизмов конечного модуля конечно. □

Лемма 4.2. *Для любого конечного кольца R существует предложение φ_R языка первого порядка теории колец, истинное в кольце X тогда и только тогда, когда $X \cong R$.*

Доказательство. Рассмотрим конечное кольцо R. Пусть оно содержит ровно m различных элементов $a_1, \ldots, a_m$, причем $a_i + a_j = a_{s(i,j)}$, $a_i \cdot a_j = a_{p(i,j)}$. Тогда искомое предложение φ_R имеет вид

$$\exists x_1 \ldots \exists x_m \left(\bigwedge_{i,j \in m, i \neq j} x_i \neq x_j \right) \wedge \\ \wedge \left(\forall x \bigvee_{i \in m} x = x_i \right) \wedge \left(\bigwedge_{i,j \in m} a_i + a_j = a_{s(i,j)} \right) \wedge \left(\bigwedge_{i,j \in m} a_i \cdot a_j = a_{p(i,j)} \right).$$

□

Теорема 4.3. *Если категории mod-R и mod-S элементарно эквивалентны и кольцо R конечно, то $R \cong \mathrm{End}_S P$ для некоторого прообразующего модуля P категории mod-S.*

Доказательство. В категории mod-R истинно предложение

$$\xi := \exists P \in Obj(Proobr(P) \wedge \varphi_{Mor(P,P)}).$$

Значит, предложение ξ должно быть истинно и в категории mod-S, т. е. кольцо эндоморфизмов некоторого прообразующего модуля изоморфно кольцу R. □

Следствие 4.1. *Категории mod-R и mod-S, где R — конечное кольцо, элементарно эквивалентны тогда и только тогда, когда они Морита-эквивалентны.*

Доказательство. Если категории mod-R и mod-S изоморфны, то они очевидно элементарно эквивалентны.

Если же категории mod-R и mod-S элементарно эквивалентны и кольцо R конечно, то по теореме 4.3 $R \cong End_S P$ для некоторого прообразующего модуля P категории mod-S, т. е. кольца R и S подобны. По теореме Мориты в этом случае категории mod-R и mod-S изоморфны. □

Во всех следующих пунктах этого параграфа мы будем предполагать, что кольца R и S бесконечны.

4.2.5 Красивые линейные комбинации

В этом пункте мы основываемся на статье С. Шелаха [148].

Пусть у нас фиксировано кольцо R, категория mod-R, в категории mod-R выделен некоторый простой модуль M, соответствующий выделенному прообразующему модулю P, $V = M^{(I)}$, $|I| = \mu$, где μ — бесконечный кардинал. Пусть множество $A = \{a_i | i \in I\}$ таково, что $\forall i \in I (a_i \in M_i \wedge a_i \neq 0)$.

Для любого $f \in Mor(A, B)$ пусть $Rng\, f$ — это образ f в B, $Cl\, B$ — замыкание множества $B \subset V$ в V, т. е. наименьший подмодуль в V, содержащий множество B. Пусть, кроме того, $\widetilde{b} = Cl\,\{b\}$.

Как обычно, $\vec{x}$ обозначает конечную последовательность переменных $\vec{x} = \langle x_1, \dots, x_n \rangle$. Линейную комбинацию $\alpha_1 x_1 + \dots + \alpha_n x_n$, где $\alpha_i \in R$, будем обозначать также через $\tau(x_1, \dots, x_n)$ или $\tau(\vec{x})$. Будем называть такую линейную комбинацию *приведенной*, если все α_i отличны от нуля.

Линейную комбинацию $\tau(x_1, \dots, x_n) = \alpha_1 x_1 + \dots + \alpha_n x_n$ назовем *красивой* (см. [148], где аналогичные термы были названы *beautiful terms*), если

(а) для любой линейной комбинации $\sigma(x_1, \dots, x_m) = \beta_1 x_1 + \dots + \beta_m x_m$ имеет место

$$\tau(\sigma(x_1^1, \dots, x_m^1), \sigma(x_1^2, \dots, x_m^2), \dots, \sigma(x_1^n, \dots, x_m^n)) = \\ = \sigma(\tau(x_1^1, x_1^2, \dots, x_1^n), \tau(x_2^1, \dots, x_2^n), \dots, \tau(x_m^1, x_m^2, \dots, x_m^n));$$

(б) имеет место равенство

$$\tau(\tau(x_1^1, \dots, x_n^1), \tau(x_1^2, \dots, x_n^2), \dots \tau(x_1^n, \dots, x_n^n)) = \tau(x_1^1, \dots, x_n^n);$$

(в) имеет место равенство

$$\tau(x, \dots, x) = x.$$

Легко показать, что все красивые линейные комбинации имеют вид

$$\alpha_1 x_1 + \dots + \alpha_n x_n, \quad \alpha_i \in Z(R),\ \alpha_i \alpha_j = \delta_{ij} \alpha_i,\ \sum_{i=1}^{n} \alpha_i = 1.$$

Теорема 4.4. *Существует формула φ_m, удовлетворяющая следующему условию. Пусть для каждого $i < i_0 < \mu^+$ $\overline{f}_i$ — это m-ка элементов $Mor(V, M)$. Тогда можно найти вектор $\overline{g}$ такой, что формула $\varphi_m(\overline{f}, \overline{g})$ истинна в mod-R тогда и только тогда, когда $\overline{f} = \tau(\overline{f}_{i_1}, \dots, \overline{f}_{i_n})$ для некоторой красивой линейной комбинации τ и $i_1 < \dots < i_n < i_0 < \mu^+$.*

4.2.6 Порождающее множество модуля V

Напомним, что через V мы обозначаем модуль $M^{(\mu)}$ для некоторого бесконечного кардинального числа $\varkappa$ и фиксированного простого модуля M.

Пусть $V = \bigoplus_{t \in \mu} M_t$, где $M_t \cong M$ для каждого $t \in \mu$, и пусть в модуле M фиксирован некоторый порождающий (т. е. ненулевой) элемент a, а в каждом модуле M_t — соответствующий ему при вложении элемент $a_t \in M_t$.

Воспользуемся теоремой 4.4 для $m = 1$ и $f_i \in Mor(V, M)$ таких, что $f_i(a_t) = \delta_{it} a$. Тогда существует $\overline{g}^*$ и формула $\varphi(f, \overline{g}^*)$ такие, что формула $\varphi(f, \overline{g}^*)$ выполнена в том и только том случае, когда $f = \tau(f_{i_1}, \dots, f_{i_n})$, где $i_1 < \dots < i_n < \mu$, где линейная комбинация τ красива.

Мы знаем, что в этом случае $\tau(x_1, \dots, x_n) = r_1 x_1 + \dots + r_n x_n$, где $r_i r_j = \delta_{ij} r_i$ для любых $i, j = 1, \dots, n$ и $r_1 + \dots + r_n = 1$.

Рассмотрим функцию $r_k f_{i_k} : V \to M$. Мы знаем, что $r_k f_{i_k}(a_{i_k}) = r_k \cdot a$ и $r_k f_{i_k}(a_t) = 0$ для $t \neq i_k$. В модуле M рассмотрим множество $N \subseteq M$ такое, что $n \in N \Leftrightarrow r_k \cdot n = 0$. Если $n_1, n_2 \in N$, то $r_k(n_1+n_2) = 0$, откуда $n_1+n_2 \in N$. Если $r \in R$, $n \in N$, то $r_k(rn) = r(r_k n) = 0$, откуда $rn \in N$. Следовательно, N является идеалом в M, т. е. $N = \{0\}$ или $N = M$. Пусть для разных k и l $r_k a \neq 0$ и $r_l a \neq 0$. Тогда $r_k b \neq 0$ и $r_l b \neq 0$ для всех $b \in M$, т. е. $r_l(r_k a) \neq 0$, что невозможно. Таким образом, $r_k a \neq 0$ только для одного $k \in \{1, \dots, n\}$. Из $r_1 + \dots + r_n = 1$, т. е. из $(r_1 + \dots + r_n)a = a$ следует, что такое k обязательно существует и, к тому же, $r_k a = a$. Значит, для некоторого k $r_k f_{i_k}(a_{i_k}) = a$ и $r_k f_{i_k}(a_t) = 0$ при $t \neq i_k$, а для $l \neq k$ $r_l f_{i_l}(a_t) = 0$ при всех $t \in I^*$. Значит, $f = f_{i_k}$ для некоторого $k \in \{1, \dots, n\}$.

Таким образом, мы показали, что существует такое $\overline{g}^*$, что формула $\varphi(f, \overline{g}^*)$ выделяет в V некоторое множество, состоящее из μ независимых проекторов из V на M. Записав формулу, утверждающую, что $\overline{g}^*$ таково, что пространство, порожденное образами таких $i \in Mor(M, V)$, что $\exists f(\varphi(f, \overline{g}^*) \wedge f \circ i = 1_M)$, изоморфно V, и при выкидывании любой пары (f, i) из этого пространства новое пространство не будет совпадать с изначальным, мы получим искомое $\overline{g}^*$.

Вспомним, что вместе с простым модулем M у нас фиксирован прообразующий модуль P вместе с эпиморфизмом $h : P \to M$, а вместе с модулем $V \cong M^{(\mu)}$ — модуль V', являющийся почти свободным модулем размерности μ над P, вместе с эпиморфизмом $h' : V' \to V$ таким, что для любой проекции $i : V \to M$ существует и единственна проекция $i' : V' \to P$ такая, что $i \circ h' = h \circ i'$.

Множество, состоящее из проекторов $g \in Mor(V, M)$, удовлетворяющих формуле $\varphi(\overline{g_*}, g)$, будем обозначать через $Gen_{\overline{g_*}}(V, M)$. Множество, состоящее из проекторов $g \in Mor(V', P)$, удовлетворяющих формуле $\exists f \in Gen_{\overline{g_*}}(V, M)(f \circ h' = h \circ g)$, обозначим через $Gen_{\overline{g_*}, h}(V', P)$.

4.2.7 Логика второго порядка и структура $\langle Cn, ring \rangle$, алгоритм перевода формул

Рассмотрим структуру $\langle Cn, ring \rangle$, состоящую из класса Cn всех кардинальных чисел, который состоит из множеств мощности $\varkappa$ для каждого $\varkappa \in Cn$, и кольца $ring$ с отношениями суммы и произведения. Логика второго порядка такой структуры $(L_2(\langle Cn, ring \rangle))$ позволяет в формулах использовать произвольные предикатные символы вида

$$P_{\lambda_1, \dots, \lambda_k}(c_1, \dots, c_k; v_1, \dots, v_n),$$

где $\lambda_1, \dots, \lambda_k$ — фиксированные кардинальные числа, $c_1, \dots c_k$ — переменные для элементов из $\lambda_1, \dots, \lambda_k$ соответственно, $v_1, \dots, v_n$ — переменные для элементов кольца.

Таким образом, формулы языка $L_2(\langle Xn, ring \rangle)$ могут содержать следующие знакосочетания:

1. $\forall r \in ring$;
2. $\exists r \in ring$;

3. $\forall\varkappa \in Cn$;

4. $\exists\varkappa \in Cn$;

5. $\forall\alpha \in \varkappa$;

6. $\exists\alpha \in \varkappa$, где в последних двух знакосочетаниях $\varkappa$ или является свободной переменной формулы φ, или определена в формуле φ раньше, чем α (с помощью подформулы $\forall\varkappa \in Cn$ или $\exists\varkappa \in Cn$);

7. $r_1 = r_2 + r_3$; $r_1 = r_2 \times r_3$; $r_1 = r_2$, где каждая из переменных r_1, r_2, r_3 либо является свободной переменной формулы φ, либо определена в формуле φ раньше (с помощью подформулы $\forall r_i \in ring$ или $\exists r_i \in ring$);

8. $\varkappa_1 = \varkappa_2$, где каждая из переменных $\varkappa_1, \varkappa_2$ либо является свободной переменной формулы φ, либо определена в формуле φ раньше (с помощью подформулы $\forall\varkappa_i \in Cn$ или $\exists\varkappa_i \in Cn$);

9. $\alpha_1 = \alpha_2$, где каждая из переменных α_1, α_2 либо является свободной переменной формулы φ, либо определена в формуле φ (с помощью подформулы $\forall\alpha_i \in \varkappa_i$ или $\exists\alpha_i \in \varkappa_i$);

10. $\forall P_{\varkappa_1,\dots,\varkappa_k}(c_1,\dots,c_k; v_1,\dots,v_n)$; $\exists P_{\varkappa_1,\dots,\varkappa_k}(c_1,\dots,c_k; v_1,\dots,v_n)$, где каждая из переменных $\varkappa_1,\dots,\varkappa_k$ либо является свободной переменной формулы φ, либо определена в формуле φ раньше (с помощью подформулы $\forall\varkappa_i \in Cn$ или $\exists\varkappa_i \in Cn$);

11. $P_{\varkappa_1,\dots,\varkappa_k}(\alpha_1,\dots,\alpha_k; r_1,\dots,r_n)$, где каждая из переменных $\varkappa_1,\dots,\varkappa_k, \alpha_1,\dots,\alpha_k, r_1,\dots,r_n$, а также “предикатная переменная”

$$P_{\varkappa_1,\dots,\varkappa_k}(c_1,\dots,c_k; v_1,\dots,v_n)$$

либо являются свободными переменными формулы φ, либо определены в формуле φ раньше (с помощью подформул $\forall\varkappa_i \in Cn$, $\exists\varkappa_i \in Cn$, $\forall\alpha_i \in \varkappa_i$, $\exists\alpha_i \in \varkappa_i$, $\forall r_i \in ring$, $\exists r_i \in ring$, $\forall P_{\varkappa_1,\dots,\varkappa_k}(c_1,\dots,c_k; v_1,\dots,v_n)$ или $\exists P_{\varkappa_1,\dots,\varkappa_k}(c_1,\dots,c_k; v_1,\dots,v_n)$), причем $\varkappa_i$ вводится в формуле раньше α_i для любого $i = 1,\dots,k$, а $P_{\varkappa_1,\dots,\varkappa_k}(c_1,\dots,c_k; v_1,\dots,v_n)$ — позже всех $\varkappa_1,\dots,\varkappa_k$.

Теорема 4.5. *Пусть даны кольца R и S и существует предложение ψ языка $L_2(\langle Cn, ring\rangle)$, истинное в теории $\langle Cn, R\rangle$ и ложное в теории $\langle Cn, R'\rangle$, если кольцо R' подобно кольцу R, но не эквивалентно ему в логике $L_2(\langle Cn, ring\rangle)$. Пусть, кроме того, категории mod-R и mod-S элементарно эквивалентны. Тогда существует кольцо S', подобное кольцу S и такое, что структуры $\langle Cn, R\rangle$ и $\langle Cn, S'\rangle$ эквивалентны в логике L_2.*

Доказательство. Предположим сначала, что мы каким-то образом фиксировали прообразующий модуль P в категории mod-T, где T — некоторое кольцо. Тогда, в соответствии с предыдущими пунктами, мы имеем формулы, выделяющие простой модуль M, соответствующий модулю P, модули $M^{(\varkappa)}$ для всех $\varkappa \in Cn$, модули $M^{(n)}$ для всех $n \in \omega$, модули $M^{(\alpha)}$ для бесконечных $\alpha \in \mathbf{Cn}$, почти свободные модули $V^\varkappa$ размерности $\varkappa \in \mathbf{Cn}$, $\varkappa \in \omega$, $\varkappa \geqslant \omega$, и, кроме того, для каждого модуля $M^{(\varkappa)}$ (или $V^\varkappa$) его порождающие множества $Gen_{g*}(M^{(\varkappa)}, M)$ (или $Gen_{g*}(V^\varkappa, R)$). Кроме того (см. п. 2.3) для любых $f, g \in Mor(P, P)$ мы считаем известной их сумму $f \oplus g \in Mor(P, P)$ и произведение $f \otimes g \in Mor(P, P)$.

Рассмотрим некоторое произвольное предложение φ в языке $L_2(\langle Cn, ring\rangle)$. Как мы уже написали выше, в это предложение могут входит подформулы

1. $\forall r \in ring$;

2. $\exists r \in ring$;
3. $\forall \varkappa \in \mathbf{Cn}$;
4. $\exists \varkappa \in \mathbf{Cn}$;
5. $\forall \alpha \in \varkappa$;
6. $\exists \alpha \in \varkappa$;
7. $r_1 = r_2 + r_3$;
8. $r_1 = r_2 \cdot r_3$;
9. $r_1 = r_2$;
10. $\varkappa_1 = \varkappa_2$;
11. $\alpha_1 = \alpha_2$.
12. $\forall P_{\varkappa_1,\dots,\varkappa_k}(c_1,\dots,c_k;v_1,\dots,v_n)$;
13. $\exists P_{\varkappa_1,\dots,\varkappa_k}(c_1,\dots,c_k;v_1,\dots,v_n)$;
14. $P_{\varkappa_1,\dots,\varkappa_k}(\alpha_1,\dots,\alpha_k;r_1,\dots,r_n)$.

Переведем это предложение в предложение $\widetilde{\varphi}_P$ (зависящее от изначально фиксированного модуля P) языка первого порядка теории категорий по следующему алгоритму:

1. подформула $\forall r \in ring$ переводится в подформулу $\forall f_r \in Mor(P,P)$, т. е. каждому элементу кольца $ring$ ставится в соответствие элемент кольца $End_T(P)$;

2. подформула $\exists r \in ring$ переводится в подформулу $\exists f_r \in Mor(P,P)$;

3. подформула $\forall \varkappa \in Cn$ переводится в подформулу $\forall X_\varkappa \in Obj \forall \overline{g}_\varkappa * (X_\varkappa = M^{(\varkappa)} \wedge Gen_{\overline{g}_\varkappa *}(X_\varkappa, M) \Rightarrow \dots)$, т. е. каждому элементу $\varkappa \in Cn$ ставится в соответствие некоторый модуль вида $M^{(\varkappa)}$ для простого модуля M (мы уже упоминали, что существует естественное отождествление класса Cn и класса всех прямых сумм модуля M), и при этом сразу фиксируется множество $Gen_{\overline{g}_\varkappa *}(M^{(\varkappa)}, M)$ проекторов из $M^{(\varkappa)}$ на M;

4. подформула $\exists \varkappa \in Cn$ переводится в подформулу $\exists X_\varkappa \in Obj \exists \overline{g}_\varkappa * (X_\varkappa = M^{(\varkappa)} \wedge Gen_{\overline{g}_\varkappa *}(X_\varkappa, M) \wedge \dots)$;

5. подформула $\forall \alpha \in \varkappa$ переводится в подформулу $\forall f^\alpha_{X_\varkappa} \in Gen_{\overline{g}_\varkappa *}(X_\varkappa, M)$, т. е. элементы множеств $\varkappa$ переводятся в функции из множества $Gen_{\overline{g}_\varkappa *}(M^{(\varkappa)}, M)$, которое содержит именно $\varkappa$ линейно независимых проекторов;

6. подформула $\exists \alpha \in \varkappa$ переводится в подформулу $\exists f^\alpha_{X_\varkappa} \in Gen_{\overline{g}_\varkappa *}(X_\varkappa, M)$;

7. подформула $r_1 = r_2 + r_3$ переводится в подформулу $f_{r_1} = f_{r_2} \oplus f_{r_3}$, т. е. сумме элементов из кольца $ring$ соответствует сумма элементов кольца $End_T(P)$;

8. подформула $r_1 = r_2 \cdot r_3$ переводится в подформулу $f_{r_1} = f_{r_2} \otimes f_{r_3}$, т. е. произведению элементов кольца $ring$ соответствует произведение элементов кольца $End_T(P)$;

9. подформула $r_1 = r_2$ переводится в подформулу $f_{r_1} = f_{r_2}$, т. е. равным элементам кольца $ring$ соответствуют равные элементы кольца $End_T(P)$;

10. подформула $\varkappa_1 = \varkappa_2$ переводится в подформулу

$$\exists g_{\varkappa_1,\varkappa_2} \in Mor(X_{\varkappa_1}, X_{\varkappa_2})(g \text{ — изоморфизм}),$$

т. е. равным множествам класса Cn соответствуют изоморфные модули вида $M^{(I)}$ и $M^{(J)}$, т. е. такие модули, что $|I| = |J| = \varkappa$;

11. подформула $\alpha_1 = \alpha_2$ для $\alpha_1, \alpha_2 \in \varkappa$ переводится в подформулу $f^{\alpha_1}_{X_\varkappa} = f^{\alpha_2}_{X_\varkappa}$, а подформула $\alpha_1 = \alpha_2$ при $\alpha_1 \in \varkappa_1$, $\alpha_2 \in \varkappa_2$ и $\varkappa_1 = \varkappa_2$ переводится в подформулу $f^{\alpha_1}_{X_{\varkappa_1}} = f^{\alpha_2}_{X_{\varkappa_2}} \circ g$,

т. е. равным элементам в множестве $\varkappa \in Cn$ сопоставляются соответствующие друг другу проекторы в $Gen_{\overline{g}_{\varkappa_1}*}(M^{(I)}, M)$ и $Gen_{\overline{g}_{\varkappa_2}*}(M^{(J)}, M)$, при этом соответствие фиксируется изоморфизмом между $M^{(I)}$ и $M^{(J)}$;

Перед последними тремя переводами введем следующие новые формулы.

Для каждой $f_t \in Gen_{\overline{g}_\varkappa *}(M^{(\varkappa)}, M)$ через $f_t{}'$ будем обозначать соответствующую ей функцию из $Gen_{\overline{g}_\varkappa *}(V^\varkappa, P)$, через $\overline{f}_t$ — функцию из $Mor(M, M^{(\varkappa)})$ такую, что $f_t \circ \overline{f}_t = 1_M$, через $\overline{f_t}'$ — функцию из $Mor(P, V^\varkappa)$ такую, что $f_t{}' \circ \overline{f_t}' = 1_P$. Про функцию $f \in Mor(V^\varkappa, V^\varkappa)$ будем писать, что $f \in Ring_{\overline{g}_\varkappa *}(V^\varkappa)$, если

$$\forall f_t{}', f_s{}' \in Gen_{\overline{g}_\varkappa *, h}(V^\varkappa, P)(f_t{}' \neq f_s{}' \Rightarrow f_t{}' \circ f \circ \overline{f_s}' = 0).$$

Про функцию $f \in Mor(M^{(\varkappa_1)}, M^{(\varkappa_2)})$ будем писать, что

$$f \in Sets_{\overline{g}_{\varkappa_1}*, \overline{g}_{\varkappa_2}*}(M^{(\varkappa_1)}, M^{(\varkappa_2)}),$$

если

$$\forall f_t \in Gen_{\overline{g}_{\varkappa_1}*}(M^{(\varkappa_1)}, M) \forall f_s \in Gen_{\overline{g}_{\varkappa_2}*}(M^{(\varkappa_2)}, M)(f_s \circ f \circ \overline{f}_t = 1_M \vee f_s \circ f \circ \overline{f}_t = 0).$$

Таким образом, элементы из $Ring_{\overline{g}_\varkappa *}(V^\varkappa)$ — это такие эндоморфизмы модуля $V^\varkappa$, которые диагональны в некотором изначально фиксированном базисе, поэтому эти эндоморфизмы можно рассматривать как функции из $\varkappa$ в кольцо $\mathrm{End}_T(P)$, ставя в соответствие каждому $\alpha \in \varkappa$ элемент, стоящий на диагонали в месте с индексом α. Элементы из $Sets_{\overline{g}_{\varkappa_1}*, \overline{g}_{\varkappa_2}*}(M^{(\varkappa_1)}, M^{(\varkappa_2)})$ — это такие морфизмы из $M^{(\varkappa_1)}$ в $M^{(\varkappa_2)}$, которые в данном фиксированном базисе имеют матрицы, состоящие только из нулей и единиц. Эти матрицы можно воспринимать как соответствия F между множествами $\varkappa_1$ и $\varkappa_2$, если считать, что пара $\langle x, y\rangle$ принадлежит соответствию F тогда и только тогда, когда на пересечении строки с индексом x и столбца с индексом y в матрице стоит единица.

Воспользуемся этими замечаниями для оставшихся переводов:

12. Пусть $\varkappa = \max\{\varkappa_1, \dots, \varkappa_k, |ring|\}$. Тогда подформула

$$\forall P_{\varkappa_1, \dots, \varkappa_k}(c_1, \dots, c_k; v_1, \dots, v_n)$$

переводится в подформулу

$$\forall f_P^{c_1} \in Sets_{\overline{g}_\varkappa *, \overline{g}_{\varkappa_1}*}(M^{(\varkappa)}, M^{(\varkappa_1)}) \dots \forall f_P^{c_k} \in Sets_{\overline{g}_\varkappa *, \overline{g}_{\varkappa_k}*}(M^{(\varkappa)}, M^{(\varkappa_k)})$$
$$\forall f_P^{v_1} \in Ring_{\overline{g}_\varkappa *}(V^\varkappa) \dots \forall f_P^{v_n} \in Ring_{\overline{g}_\varkappa *}(V^\varkappa),$$

т. е. любому предикатному символу вида $P_{\varkappa_1, \dots, \varkappa_k}(c_1, \dots, c_k; v_1, \dots, v_n)$ ставится в соответствие k функций, отвечающих за множества $\varkappa_1, \dots, \varkappa_k$, и n функций, отвечающих за элементы кольца, связанных между собой с помощью модуля $M^{(\varkappa)}$;

13. подформула

$$\exists P_{\varkappa_1, \dots, \varkappa_k}(c_1, \dots, c_k; v_1 \dots, v_n)$$

переводится в подформулу

$$\exists f_P^{c_1} \in Sets_{\overline{g}_\varkappa *, \overline{g}_{\varkappa_1}*}(M^{(\varkappa)}, M^{(\varkappa_1)}) \dots \exists f_P^{c_k} \in Sets_{\overline{g}_\varkappa *, \overline{g}_{\varkappa_k}*}(M^{(\varkappa)}, M^{(\varkappa_k)})$$
$$\exists f_P^{v_1} \in Ring_{\overline{g}_\varkappa *}(V^\varkappa) \dots \exists f_P^{v_n} \in Ring_{\overline{g}_\varkappa *}(V^\varkappa);$$

14. подформула

$$P_{\varkappa_1,\dots,\varkappa_k}(\alpha_1,\dots,\alpha_k;r_1,\dots,r_n)$$

переводится в подформулу

$$\exists f \in Gen_{\overline{g}_\varkappa{}^*}(M^{(\varkappa)},M)$$
$$(f^{\alpha_1}_{X_{\varkappa_1}}\circ f^{c_1}_P\circ\overline{f}=1\wedge\dots\wedge f^{\alpha_k}_{X_{\varkappa_k}}\circ f^{c_k}_P\circ\overline{f}=1\wedge f'\circ f^{v_1}_P\circ\overline{f}'=f_{r_1}\wedge\dots\wedge f'\circ f^{v_n}_P\circ\overline{f}'=f_{r_n}).$$

Пусть теперь некоторое предложение φ истинно в модели $\langle Cn,\,\mathrm{End}_T P\rangle$. Пусть все связанные переменные предложения φ содержатся среди переменных $x_1,\dots,x_q$ (где $x_1,\dots,x_q$ — это либо переменные для элементов кольца, либо для элементов класса Cn, либо для элементов каких-то $\varkappa\in Cn$, либо предикатные переменные). Так как предложение φ истинно в модели $\langle Cn,\,\mathrm{End}_T P\rangle$, то существует некоторая последовательность $y_1,\dots,y_q$ элементов этой модели, на которой предложение φ выполняется. Переведем последовательность $y_1,\dots,y_q$ элементов модели $\langle Cn,\,\mathrm{End}_T P\rangle$ в последовательность $z_1,\dots,z_s$ элементов модели mod-T.

Если $y_i\in\mathrm{End}_T(P)$, то переведем элемент y_i в элемент $z_i:=y_i=f_{y_i}\in Mor(P,P)$.

Если $y_i\in Cn$ и $y_i=\varkappa$, то переведем y_i в пару $z_i^{(1)}:=M^{(\varkappa)}\in Obj$ и $z_i^{(2)}:=\overline{g}^*_\varkappa$ такое, что верно $Gen_{\overline{g}_\varkappa}(M^{(\varkappa)},M)$.

Если $y_i\in\varkappa$ и $y_i=\alpha$, где α — ординальное число, то переведем y_i в $z_i:=f^\alpha\in Gen_{\overline{g}_\varkappa{}^*}(M^{(\varkappa)},M)$ — проектор из этого множества, имеющий индекс α.

Если $y_i=P_{\varkappa_1,\dots,\varkappa_k}(c_1,\dots,c_k;v_1,\dots v_n)$, то есть отношение $\overline{P}$ на множестве

$$\varkappa_1\times\dots\times\varkappa_k\times End_TP\times\dots\times End_TP,$$

то положим $\varkappa:=\max\{\varkappa_1,\dots,\varkappa_k,|End_TP|\}$ и переведем y_i в последовательность $z_i^1,\ \dots,\ z_i^k;\ z_i^{k+1},\ \dots,\ z_i^{k+n}$ морфизмов из множеств

$$Sets_{\overline{g}_\varkappa{}^*,\overline{g}_{\varkappa_1}{}^*}(M^{(\varkappa)},M^{(\varkappa_1)}),\dots,Sets_{\overline{g}_\varkappa{}^*,\overline{g}_{\varkappa_k}{}^*}(M^{(\varkappa)},M^{(\varkappa_k)}),Ring_{\overline{g}_\varkappa{}^*}(V^\varkappa),\dots,Ring_{\overline{g}_\varkappa{}^*}(V^\varkappa)$$

соответственно, такую, что $\langle\alpha_1,\dots,\alpha_k;r_1,\dots,r_n\rangle\in\overline{P}$ тогда и только тогда, когда существует $\alpha\in\varkappa$ такое, что в каждой из матриц z_i^l, $1\leqslant l\leqslant k$, На пересечении столбца с номером α и строки с номером α_l стояла единица, а в каждой из матриц z_i^l, $k<l\leqslant k+n$, На диагонали на месте с номером α стоит элемент r_l.

Таким образом, мы получим новую последовательность $z_1,\dots,z_s$. Покажем, что на этой последовательности в модели mod-T выполнено предложение $\widetilde{\varphi}_P$.

Проведем доказательство по индукции по длине формулы.

1. Если формула имеет вид

$$r_1=r_2+r_3,$$

то ее перевод имеет вид

$$f_{r_1}=f_{r_2}\oplus f_{r_3},$$

при этом $r_1=r_2+r_3$ в $\mathrm{End}_T P$ тогда и только тогда, когда $f_{r_1}=f_{r_2}\oplus f_{r_3}$ в $Mor_T(P,P)$ так как кольца $\mathrm{End}_T P$ и $Mor_T(P,P)$ изоморфны. Поэтому

$$\langle Cn,\,\mathrm{End}_T P\rangle_{L_2}\vDash r_1=r_2+r_3$$

тогда и только тогда, когда

$$\text{mod-}T \vDash f_{r_1} = f_{r_2} \oplus f_{r_3}.$$

2. Доказательство в случае формул $r_1 = r_2 \cdot r_3$ и $r_1 = r_2$ аналогично предыдущему пункту.

3. Если формула имеет вид

$$\varkappa_1 = \varkappa_2,$$

то ее перевод имеет вид

$$\exists g \in Mor(M^{(\varkappa_1)}, M^{(\varkappa_2)})(g \text{ — изоморфизм}).$$

Если кардинальные числа $\varkappa_1$ и $\varkappa_2$ совпадают. то модули $M^{(\varkappa_1)}$ и $M^{(\varkappa_2)}$ изоморфны, а если модули $M^{(I)}$ и $M^{(J)}$ изоморфны, то $|I| = |J|$. Отсюда следует, что

$$\langle Cn, \operatorname{End}_T P\rangle_{L_2} \vDash \varkappa_1 = \varkappa_2$$

тогда и только тогда, когда

$$\text{mod-}T \vDash \exists g_{\varkappa_1,\varkappa_2} \in Mor(M^{(\varkappa_1)}, M^{(\varkappa_2)})(g \text{ — изоморфизм}).$$

4. Аналогичное утверждение о формуле $\alpha_1 = \alpha_2$ совершенно аналогично предыдущему.

5. Если формула имеет вид

$$P_{\varkappa_1,\ldots,\varkappa_k}(\alpha_1,\ldots,\alpha_k; r_1,\ldots,r_n),$$

а ее перевод имеет вид

$$\widetilde{P}_{\varkappa_1,\ldots,\varkappa_k}(\alpha_1,\ldots,\alpha_k; r_1,\ldots,r_n)_P,$$

то если

$$\langle Cn, \operatorname{End}_T P\rangle_{L_2} \vDash P_{\varkappa_1,\ldots,\varkappa_k}(\alpha_1,\ldots,\alpha_k; r_1,\ldots,r_n),$$

то для последовательности

$$\langle \alpha_1,\ldots,\alpha_k, r_1,\ldots,r_n\rangle \in \varkappa_1 \times \cdots \times \varkappa_k \times \operatorname{End}_T P \times \cdots \times \operatorname{End}_T P$$

выполнено

$$\langle \alpha_1,\ldots,\alpha_k; r_1,\ldots,r_n\rangle \in \overline{P},$$

где $\overline{P}$ — отношение, соответствующее предикату $P_{\varkappa_1,\ldots,\varkappa_k}$, т. е.

$$\overline{P} \subset \varkappa_1 \times \cdots \times \varkappa_k \times \operatorname{End}_T P \times \cdots \times \operatorname{End}_T P.$$

Это отношение есть множество последовательностей, имеющее мощность, не большую чем

$$|\varkappa_1 \times \cdots \times \varkappa_k \times |T| \times \cdots \times |T|| \leqslant |\varkappa \times \cdots \times \varkappa| = \varkappa.$$

Таким образом, все последовательности из $\overline{P}$ можно пронумеровать элементами из $\varkappa$. Пусть $\overline{P}(\alpha)$ — это последовательность из $\overline{P}$ с номером α, и она имеет вид $\langle \alpha_1,\ldots,\alpha_k; r_1,\ldots,r_n\rangle$. Тогда α-й столбец матрицы z_i^l для $l = 1,\ldots,k$ будет содержать 1 на месте с номером α_l, и 0 на всех остальных местах, а α-й столбец матрицы z_i^l для $l = k+1, \ldots, k+n$ — будет содержать r_{l-n} на α-ом месте и 0 на всех остальных местах. Отсюда видно, что

$$\langle Cn, \operatorname{End}_T P\rangle_{L_2} \vDash P_{\varkappa_1,\ldots,\varkappa_k}(\alpha_1, \ldots, \alpha_k; r_1, \ldots, r_n)$$

тогда и только тогда, когда

$$\text{mod-}T \vDash \widetilde{P}_{\varkappa_1,\ldots,\varkappa_k}(\alpha_1, \ldots, \alpha_k; r_1, \ldots, r_n)_P.$$

Все остальные части индукции доказываются совершенно очевидно.

Теперь мы легко можем увидеть, что предложение φ истинно в структуре $\langle Cn, \operatorname{End}_T(P)\rangle$ тогда и только тогда, когда соответствующее ему предложение $\widetilde{\varphi}_P$ истинно в mod-T.

Формула

$$Select(P) := P \in Obj \wedge Proobr(P) \wedge \widetilde{\psi}^P \wedge \forall P' \in Obj(Proobr(P') \wedge P' \ncong P \Rightarrow \neg\widetilde{\psi}^{P'})$$

по условию теоремы истинна в mod-R только для $P \cong R$.

Пусть теперь категории mod-R и mod-S элементарно эквивалентны и φ — предложение в языке второго порядка L_2 структуры $\langle Cn, ring\rangle$, истинное в $\langle Cn, R\rangle$. Тогда предложение $\forall P \in Obj(Select(P) \Rightarrow \widetilde{\varphi}^P)$ истинно в категории mod-R, а значит, и в категории mod-S. Отсюда следует, что предложение φ истинно в $\langle Cn, \operatorname{End}_S(P)\rangle$ для любого модуля P, удовлетворяющего в категории mod-S формуле $Select(P)$, но для всех модулей P, удовлетворяющих формуле φ, кольца $\operatorname{End}_S P$ эквивалентны в логике $\langle Cn, ring\rangle$, Поэтому если положить $S' := \operatorname{End}_S P$ для некоторого P, Удовлетворяющего формуле $Select(P)$ то мы получим, что предложение φ истинно в $\langle Cn, S'\rangle$, причем кольцо S' не зависит от предложения φ. Следовательно, структуры $\langle Cn, R\rangle$ и $\langle Cn, S'\rangle$ эквивалентны в логике L_2. □

4.2.8 Обратная теорема

Прежде чем доказывать обратную теорему, выразим различные понятия, которые понадобятся нам в дальнейшем в языке $L_2(\langle Cn, ring\rangle)$.

Одноместное отношение вида $P_{\varkappa_1}(c)$ будем называть *подмножеством кардинального числа* $\varkappa_1$. Определимое множество $\{\alpha \in \varkappa_1 | P_{\varkappa_1}(\alpha)\}$ будем обозначать через $P_{\varkappa_1}$ и использовать запись $\alpha \in P_{\varkappa_1}$.

Одноместное отношение вида $P(v)$ будем называть *подмножеством кольца* $ring$, и, аналогично предыдущему, использовать запись $r \in P$.

Любое двухместное отношение $F_{\varkappa_1,\varkappa_2}(c_1, c_2)$ (или $F_{\varkappa_1}(c_1, v_1)$, или $F(v_1, v_2)$) будем называть *соответствием* между кардинальными числами $\varkappa_1$ и $\varkappa_2$ (или между кардинальным числом $\varkappa_1$ и кольцом, или в кольце). Будем использовать запись $\langle\alpha_1, \alpha_2\rangle \in P_{\varkappa_1,\varkappa_2}$ ($\langle\alpha_1, v_1\rangle \in P_{\varkappa_1}$ или $\langle v_1, v_2\rangle \in P$) для формулы $P_{\varkappa_1,\varkappa_2}(\alpha_1, \alpha_2)$ (и т. п.)

Соответствие $F_{\varkappa_1,\varkappa_2}(c_1, c_2)$ ($F_{\varkappa_1}(c_1, v_1)$ или $F(v_1, v_2)$), для которого выполняется формула

$$\forall\alpha \in \varkappa_1 \exists\beta \in \varkappa_2(\langle\alpha, \beta\rangle \in F_{\varkappa_1,\varkappa_2}) \wedge \forall\alpha \in \varkappa_1 \forall\beta_1, \beta_2 \in \varkappa_2$$
$$(\langle\alpha, \beta\rangle \in F_{\varkappa_1,\varkappa_2} \wedge \langle\alpha, \beta_2\rangle \in F_{\varkappa_1,\varkappa_2} \Rightarrow \beta_1 = \beta_2)$$

(аналогично для других видов соответствий), называется *функцией из кардинального числа $\varkappa_1$ в кардинальное число $\varkappa_2$* (соответственно, из кардинального числа $\varkappa_1$ в кольцо, или из кольца в себя) То, что $F_{\varkappa_1,\varkappa_2}$ ($F_{\varkappa_1}$ или F) является функцией, мы будем записывать через $Func(F_{\varkappa_1,\varkappa_2})$ ($Func(F_{\varkappa_1})$ или $Func(F)$).

Функция $F_{\varkappa_1,\varkappa_2}(c_1,c_2)$ ($F_{\varkappa_1}(c_1,v_1)$ или $F(v_1,v_2)$), для которой выполнена формула

$$\forall\beta\in\varkappa_2\exists\alpha\in\varkappa_2(\langle\alpha,\beta\rangle\in F_{\varkappa_1,\varkappa_2})$$

(аналогично для других видов функций), называется *сюръективной* (обозначение: $Surj(F)$ или $surj(F_{\varkappa_1})$ или $Surj(F)$).

Функция $F_{\varkappa_1,\varkappa_2}(c_1,c_2)$ (или $F_{\varkappa_1}(c_1,v_1)$, или $F(v_1,v_2)$), для которой выполнена формула

$$\forall\alpha_1,\alpha_2\in\varkappa_1\forall\beta\in\varkappa_2(\langle\alpha_1,\beta\rangle\in F_{\varkappa_1,\varkappa_2}\wedge\langle\alpha_2,\beta\rangle\in F_{\varkappa_1,\varkappa_2}\Rightarrow\alpha_1=\alpha_2)$$

(аналогично для других видов функций), называется *инъективной* (обозначение: $Inj(F_{\varkappa_1,\varkappa_2})$ или $Inj(F_{\varkappa_1})$ или $Inj(F)$).

Функция, являющаяся одновременно сюръективной и инъективной, называется *биективной* (обозначение: $Bij(F_{\varkappa_1,\varkappa_2})$ или $Bij(F_{\varkappa_1})$ или $Bij(F)$).

Для данной функции $F_{\varkappa_1,\varkappa_2}(c_1,c_2)$ ($F_{\varkappa_1}(c_1,v_1)$ или $F(v_1,v_2)$) *обратной* функцией называется функция $F'_{\varkappa_1,\varkappa_2}(c_1,c_2)$ ($F'_{\varkappa_1}(c_1,v_1)$ или $F'(v_1,v_2)$), удовлетворяющая формуле

$$\forall\alpha\in\varkappa_1\forall\beta\in\varkappa_2(\langle\alpha,\beta\rangle\in F_{\varkappa_1,\varkappa_2}\Leftrightarrow\langle\beta,\alpha\rangle\in F'_{\varkappa_1,\varkappa_2}).$$

Областью определения соответствия $F_{\varkappa_1,\varkappa_2}(c_1,c_2)$ ($F_{\varkappa_1}(c_1,v_1)$ или $F(v_1,v_2)$) называется множество $A_{\varkappa_1}\subset\varkappa_1$ ($A\subset ring$), удовлетворяющее формуле

$$\forall\alpha\in\varkappa_1(\alpha\in A_{\varkappa_1}\Leftrightarrow\exists\beta\in\varkappa_2\langle\alpha,\beta\rangle\in F_{\varkappa_1,\varkappa_2}).$$

Область определения обозначается через $Dom(F_{\varkappa_1,\varkappa_2})$.

Образом соответствия $F_{\varkappa_1,\varkappa_2}(c_1,c_2)$ (или $F_{\varkappa_1}(c_1)$, или $F(v_1,v_2)$) называется множество $A_{\varkappa_2}\subset\varkappa_2$ ($A\subset ring$), удовлетворяющее формуле

$$\forall\beta\in\varkappa_2(\beta\in A_{\varkappa_2}\Leftrightarrow\exists\alpha\in\varkappa_1\langle\alpha,\beta\rangle\in F_{\varkappa_1,\varkappa_2})$$

(обозначение $Rng(F_{\varkappa_1,\varkappa_2})$.

Про кардинальное число $\mu\in Cn$ будем говорить, что оно *бесконечно* (в обозначениях $\mu\in Inf$ или $Inf(\mu)$), если оно удовлетворяет формуле

$$\exists F_{\mu,\mu}(c_1,c_2)(Inj(F_{\mu,\mu}\wedge Rng(F_{\mu,\mu}\neq\mu).$$

Про кардинальное число $\mu\in Cn$ будем говорить, что оно *конечно* (в обозначениях $\mu\in Fin$ или $Fin(\mu)$), если $\mu\notin Inf$.

Мощностью множества $M_\varkappa\subset\varkappa$ ($M\subset ring$) будем называть кардинальное число $\mu\in Cn$, для которого выполнена формула

$$\exists F_{\mu,\varkappa}(c_1,c_2)(Inj(F_{\mu,\varkappa})\wedge Dom(F_{\mu,\varkappa}=\mu\wedge Rng(F_{\mu,\varkappa}=M_\varkappa).$$

Мощность множества $M_\varkappa$ (M) будем обозначать через $|M_\varkappa|$ ($|M|$).

Множество $M_\varkappa$ (M) будем называть *конечным*, если его мощность является конечным кардинальным числом.

Рассмотрим некоторое конечное множество $M_\varkappa$ (M). Соответствие $\overline{M}_{\varkappa,\varkappa}(c_1,c_2)$ ($\overline{M}(v_1,v_2)$) будем называть *отношением последовательного порядка* на этом множестве, если

$$\forall \alpha_1,\alpha_2,\alpha_3 \in M_\varkappa((\langle\alpha_1,\alpha_2\rangle \in \overline{M_{\varkappa,\varkappa}} \wedge \langle\alpha_1,\alpha_3\rangle \in \overline{M_{\varkappa,\varkappa}} \Rightarrow \alpha_2=\alpha_3)\wedge$$
$$\wedge (\langle\alpha_1,\alpha_3\rangle \in \overline{M_{\varkappa,\varkappa}} \wedge \langle\alpha_2,\alpha_3\rangle \in \overline{M_{\varkappa,\varkappa}} \Rightarrow \alpha_1=\alpha_2))\wedge$$
$$\wedge \exists \alpha_{\min},\alpha_{\max} \in M_\varkappa \forall \alpha \in M_\varkappa((\alpha=\alpha_{\max} \vee \exists \alpha' \in M_\varkappa$$
$$(\langle\alpha,\alpha'\langle \in \overline{M_{\varkappa,\varkappa}})) \wedge (\alpha=\alpha_{\min} \vee \exists \alpha' \in M_\varkappa(\langle\alpha',\alpha\rangle \in \overline{M_{\varkappa,\varkappa}})))\wedge$$
$$\wedge \forall \alpha \in M_\varkappa(\langle\alpha_{\max},\alpha\rangle \notin \overline{M_{\varkappa,\varkappa}} \wedge \langle\alpha,\alpha_{\min}\rangle \notin \overline{M_{\varkappa,\varkappa}})).$$

Будем обозначать свойство предиката $\overline{M}_{\varkappa,\varkappa}(c_1,c_2)$ ($\overline{M}(v_1,v_2)$) быть последовательным порядком на множестве $M_\varkappa$ (M) через $Next_{M_\varkappa}(\overline{M}_{\varkappa,\varkappa})$ ($Next_M(\overline{M})$).

Если $\overline{M}_{\varkappa,\varkappa}(c_1,c_2)$ ($\overline{M}(v_1,v_2)$) — фиксированный последовательный порядок на множестве $M_\varkappa$ (M), то для $\alpha_1,\alpha_2 \in \varkappa$ ($r_1,r_2 \in ring$) таких, что $\langle\alpha_1,\alpha_2\rangle \in \overline{M}_{\varkappa,\varkappa}$ ($\langle r_1,r_2\rangle \in \overline{M}$) будем писать $\alpha_2=\alpha_1 \oplus_{\overline{M}} 1$ ($r_2=r_1 \oplus_{\overline{M}} 1$).

Пусть $M \subset ring$ — некоторое подмножество кольца. Через $\sum\limits_{r\in M} r$ мы будем обозначать элемент $\overline{r}$ кольца $ring$, удовлетворяющий формуле

$$\exists \overline{M}(v_1,v_2)\exists S(v_1,v_2)(Next_M(\overline{M}) \wedge Bij(S) \wedge \langle r_{\min}(\overline{M}), r_{\min}(\overline{M})\rangle \in S\wedge$$
$$\wedge \forall r_1,r_2,r_3,r_4 \in M(r_2=r_1 \oplus_{\overline{M}} 1 \wedge \langle r_1,r_3\rangle \in S\wedge$$
$$\wedge \langle r_2,r_4\rangle \in S \Rightarrow r_4=r_3+r_2) \wedge \langle r_{\max}(\overline{M}),\overline{r}\rangle \in S).$$

Легко увидеть, что формула $\sum\limits_{r\in M} r$ задает обычное сложение в кольце $ring$.

Матрицей размера $\varkappa_1 \times \varkappa_2$ называется отношение $M_{\varkappa_1,\varkappa_2}(c_1,c_2,v_1)$, удовлетворяющее формуле

$$\forall \alpha \in \varkappa_1 \forall \beta \in \varkappa_2 \exists r \in ring(\langle\alpha,\beta,r\rangle \in M_{\varkappa_1,\varkappa_2}\wedge$$
$$\wedge \forall \alpha \in \varkappa_1 \forall \beta \in \varkappa_2 \forall r_1,r_2 \in ring(\langle\alpha,\beta,r_1\rangle \in M_{\varkappa_1,\varkappa_2} \wedge \langle\alpha,\beta,r_2\rangle \in M_{\varkappa_1,\varkappa_2} \Rightarrow r_1=r_2)\wedge$$
$$\wedge \forall \beta \in \varkappa_2 \forall M_{\varkappa_1} \subset \varkappa_1(\forall \alpha \in \varkappa_1(\alpha \in M_{\varkappa_1} \Leftrightarrow \exists r \in ring(\langle\alpha,\beta,r\rangle \in M_{\varkappa_1,\varkappa_2} \wedge r \neq 0)) \Rightarrow$$
$$\Rightarrow |M_{\varkappa_1}| \in Fin).$$

Отношения, $M_{\varkappa_1,\varkappa_2}(c_1,c_2;v_1)$, являющиеся матрицами, мы будем обозначать через $Matrix(M_{\varkappa_1,\varkappa_2})$.

Теорема 4.6. *Если структуры $\langle Cn,R\rangle$ и $\langle Cn,S\rangle$ эквивалентны в логике второго порядка L_2, то категории mod-R и mod-S элементарно эквивалентны.*

Доказательство. Рассмотрим произвольное предложение φ в языке теории категорий, истинное в категории mod-R.

Переведем его в предложение языка второго порядка структуры $\langle Cn,R\rangle$.

Сначала дадим неформальное описание перевода.

Каждая объектная переменная переводится в пару, первый элемент которой — кардинальное число $\varkappa$ (соответствующий размерности свободного модуля над R), второй элемент — матрица размера $\varkappa \times \varkappa$ с элементами из кольца R такая, что в каждом столбце она содержит лишь конечное число ненулевых элементов. Этой матрице естественным образом соответствует подмодуль модуля $R^{(\varkappa)}$ (столбцы — это порождающие элементы подмодуля). Мы будем ассоциировать такую пару с фактормодулем свободного модуля $R^{(\varkappa)}$ по этому подмодулю.

Каждая переменная для морфизма переводится в тройку, состоящую из двух объектов, зашифрованных так, как описано выше (обозначим соответствующие кардинальные числа через $\varkappa$ и $\varkappa'$, а получающиеся подмодули — через A и A'), и еще одной матрицы размера $\varkappa \times \varkappa'$, определяющей линейное отображение из $R^{(\varkappa)}$ в $R^{(\varkappa')}$, такое, что образ подмодуля A лежит в модуле A'.

Любой тождественный морфизм переводится в тройку, где первые две компоненты совпадают, а матрица, являющаяся третьей компонентой, является тождественной матрицей.

Композиция двух морфизмов (двух троек) переводится в тройку, в которой первый объект — это первый объект первой тройки, второй объект — второй объект второй тройки, а третий объект — композиция матриц из первой и второй тройки.

Теперь перейдем к формальному переводу.

Теперь произведем следующие замены в предложении φ.

1. Подформулу $\forall X \in Obj$ мы заменим на подформулу

$$\forall \varkappa_X \in Cn \forall P^X_{\varkappa_X,\varkappa_X}(c_1, c_2, v)(Matrix(P^X_{\varkappa_X,\varkappa_X}) \Rightarrow \dots).$$

2. Подформулу $\exists X \in Obj$ мы заменим на подформулу

$$\exists \varkappa_X \in Cn \exists P^X_{\varkappa_X,\varkappa_X}(c_1, c_2, v)(Matrix(P^X_{\varkappa_X,\varkappa_X}) \wedge \dots).$$

Сейчас нам потребуется выписать условие на матрицу для морфизма, утверждающее, что эта матрица переводит первый объект во второй, т. е. все вектор-столбцы матрицы первого объекта под действием этой матрицы перейдут в линейные комбинации векторов-столбцов матрицы второго объекта. Чтобы записать это условие, нам требуется ввести формулу, выражающую сумму бесконечного множества элементов кольца, если известно, что лишь конечное их число отлично от нуля.

Для удобства для матрицы $M_{\varkappa_1,\varkappa_2}(c_1, c_2, v_1)$ и фиксированных $\alpha \in \varkappa_1$ и $\beta \in \varkappa_2$ то единственное $r \in ring$, для которого $\langle \alpha, \beta, r \rangle \in M_{\varkappa_1,\varkappa_2}$, будем обозначать через $M_{\varkappa_1,\varkappa_2}(\langle \alpha, \beta \rangle)$.

Пусть имеется некоторая функция $F_\varkappa(c, v)$, образ которой есть подмножество кольца $ring$ и о которой известно, что множество таких $\alpha \in \varkappa$, для которых соответствующее $r \in ring$, такое, что $\langle \alpha, r \rangle \in F_\varkappa$, Не равно 0, конечно. Тогда через

$$\sum_{\alpha \in \varkappa} F_\varkappa(\langle \alpha \rangle)$$

будем обозначать элемент $r \in ring$, удовлетворяющий формуле

$$\forall M_\varkappa(c, v)(\forall \alpha \in \varkappa \forall r' \in ring(\langle \alpha, r' \rangle \in M_\varkappa \Leftrightarrow r' \neq 0 \wedge \langle \alpha, r' \rangle \in F_\varkappa) \Rightarrow \\ \Rightarrow r = \sum_{\alpha \in Dom(M_\varkappa)} M_\varkappa(\langle \alpha \rangle)).$$

Теперь мы готовы дать перевод 3.

3. Подформулу $\forall f \in Mor$ мы заменим на подформулу

$$\forall \varkappa_f \forall P^f_{\varkappa_f,\varkappa_f} \in \widetilde{Obj} \forall \varkappa'_f \forall {P^f_{\varkappa'_f,\varkappa'_f}}' \in \widetilde{Obj} \forall Q^f_{\varkappa_f,\varkappa'_f}(c_1,c_2,v)(Matrix(Q^f_{\varkappa_f,\varkappa'_f})\wedge$$
$$\wedge \forall \beta \in \varkappa_f \exists S_{\varkappa'_f}(c,v)(Func(S_{\varkappa'_f})\langle Dom\rangle \wedge |Dom(S_{\varkappa'_f}| \in Fin\wedge$$
$$\wedge \forall \gamma \in \varkappa'_f(\gamma \in Dom(S_{\varkappa'_f} \wedge \sum_{\alpha\in\varkappa_f} Q^f_{\varkappa_f,\varkappa'_f}(\langle\alpha,\gamma\rangle)\cdot P^f_{\varkappa_f,\varkappa_f}(\langle\alpha,\beta\rangle) =$$
$$= \sum_{\xi\in\varkappa'_f} S(\gamma)\cdot {P^f_{\varkappa'_f,\varkappa'_f}}'(\langle\xi,\gamma\rangle))\vee$$
$$\vee(\gamma\notin Dom(S_{\varkappa'_f})\wedge \sum_{\alpha\in\varkappa_f} Q_{\varkappa_f,\varkappa'_f}(\langle\alpha,\gamma\rangle)\cdot P^f_{\varkappa_f,\varkappa_f}(\langle\alpha,\beta\rangle)=0)\Rightarrow\dots).$$

4. Подформулу $\exists f \in Mor$, аналогично предыдущей, мы заменим на подформулу

$$\exists \varkappa_f \exists P^f_{\varkappa_f,\varkappa_f} \in \widetilde{Obj} \exists \varkappa'_f \exists {P^f_{\varkappa'_f,\varkappa'_f}}' \in \widetilde{Obj} \forall Q^f_{\varkappa_f,\varkappa'_f}(c_1,c_2,v)(Matrix(Q^f_{\varkappa_f,\varkappa'_f})\wedge$$
$$\wedge \forall \beta \in \varkappa_f \exists S_{\varkappa'_f}(c,v)(Func(S_{\varkappa'_f})\langle Dom\rangle \wedge |Dom(S_{\varkappa'_f}| \in Fin\wedge$$
$$\wedge \forall \gamma \in \varkappa'_f(\gamma \in Dom(S_{\varkappa'_f} \wedge \sum_{\alpha\in\varkappa_f} Q^f_{\varkappa_f,\varkappa'_f}(\langle\alpha,\gamma\rangle)\cdot P^f_{\varkappa_f,\varkappa_f}(\langle\alpha,\beta\rangle) =$$
$$= \sum_{\xi\in\varkappa'_f} S(\gamma)\cdot {P^f_{\varkappa'_f,\varkappa'_f}}'(\langle\xi,\gamma\rangle))\vee$$
$$\vee(\gamma\notin Dom(S_{\varkappa'_f})\wedge \sum_{\alpha\in\varkappa_f} Q_{\varkappa_f,\varkappa'_f}(\langle\alpha,\gamma\rangle)\cdot P^f_{\varkappa_f,\varkappa_f}(\langle\alpha,\beta\rangle)=0)\wedge\dots).$$

5. Подформулу $X = Y$ для $X, Y \in Obj$ мы заменим на подформулу

$$\varkappa_X = \varkappa_Y \wedge \forall\alpha,\beta\in\varkappa_X \forall r \in ring(P^X_{\varkappa_X,\varkappa_X}(\alpha,\beta,r)\Leftrightarrow P^Y_{\varkappa_X,\varkappa_X}(\alpha,\beta,r)),$$

а подформулу $f = g$ для $f, g \in Mor$ — на формулу

$$\varkappa_f = \varkappa_g \wedge \varkappa'_f = \varkappa'_g \wedge \forall \alpha_1,\alpha_2\in\varkappa_f\forall\beta_1,\beta_2\in\varkappa'_f\forall r\in ring$$
$$((P^f_{\varkappa_f,\varkappa_f}(\alpha_1,\alpha_2,r)\Leftrightarrow P^g_{\varkappa_f,\varkappa_f}(\alpha_1,\alpha_2,r))\wedge$$
$$\wedge({P^f_{\varkappa'_f,\varkappa'_f}}'(\beta_1,\beta_2,r)\Leftrightarrow {P^f_{\varkappa'_f,\varkappa'_f}}'(\beta_1,\beta_2,r))\wedge(Q^f_{\varkappa_f,\varkappa'_f}(\alpha_1,\beta_1,r)\Leftrightarrow Q^g_{\varkappa_f,\varkappa'_f}(\alpha_1,\beta_1,r))).$$

6. Подформулу $f \in Mor(X,Y)$ для данных $f \in Mor$, $X, Y \in Obj$ мы заменим на подформулу

$$\varkappa_f = \varkappa_X \wedge \varkappa'_f = \varkappa_Y \wedge \forall\alpha_1,\alpha_2\in\varkappa_X\forall\beta_1,\beta_2\in\varkappa_Y\forall r\in ring$$
$$(P^f_{\varkappa_X,\varkappa_X}(\alpha_1,\alpha_2,r)\Leftrightarrow P^X_{\varkappa_X,\varkappa_X}(\alpha_1,\alpha_2,r))\wedge {P^f_{\varkappa_Y,\varkappa_Y}}'(\beta_1,\beta_2,r)\Leftrightarrow(P^Y_{\varkappa_Y,\varkappa_Y}(\beta_1,\beta_2,r)).$$

7. Подформулу $f = 1_X$ для данных $f \in Mor$, $X \in Obj$ мы заменим на подформулу

$$\begin{aligned}\varkappa_f = \varkappa_X \wedge \varkappa_f' = \varkappa_X \wedge \forall \alpha, \beta \in \varkappa_X \forall r \in ring \\ (P^X_{\varkappa_X,\varkappa_X}(\alpha,\beta,r) \Leftrightarrow P^f_{\varkappa_X,\varkappa_X}(\alpha,\beta,r) \Leftrightarrow {P^f_{\varkappa_X,\varkappa_X}}'(\alpha,\beta,r))\wedge \\ \wedge \forall \gamma \in \varkappa_X (Q^f_{\varkappa_X,\varkappa_X}(\gamma,\gamma,1)) \wedge \forall \gamma,\eta \in \varkappa_X(\gamma \neq \eta \Rightarrow Q^f_{\varkappa_X,\varkappa_X}(\gamma,\eta,0)).\end{aligned}$$

8. Подформулу $f = g \circ h$ для данных $f, g, h \in Mor$ мы заменим на подформулу

$$\begin{aligned}\varkappa_f = \varkappa_h \wedge \varkappa_f' = \varkappa_g' \wedge \varkappa_h' = \varkappa_g \wedge \forall \alpha_1, \alpha_2 \in \varkappa_f \\ \forall \beta_1, \beta_2 \in \varkappa_f' \forall \gamma_1, \gamma_2 \in \varkappa_g \forall r \in ring((P^f_{\varkappa_f,\varkappa_f}(\alpha_1,\alpha_2,r) \Leftrightarrow P^h_{\varkappa_f,\varkappa_f}(\alpha_1,\alpha_2,r))\wedge \\ \wedge ({P^f_{\varkappa_f',\varkappa_f'}}'(\beta_1,\beta_2,r) \Leftrightarrow {P^g_{\varkappa_f',\varkappa_f'}}'(\beta_1,\beta_2,r))\wedge \\ \wedge (P^g_{\varkappa_g,\varkappa_g}(\gamma_1,\gamma_2,r) \Leftrightarrow {P^h_{\varkappa_g,\varkappa_g}}'(\gamma_1,\gamma_2,r)))\wedge \\ \forall \xi \in \varkappa_f \forall \eta \in \varkappa_f'(Q^f_{\varkappa_f,\varkappa_f'}(\langle \xi,\eta\rangle) = \sum_{\alpha \in \varkappa_g} Q^g_{\varkappa_g,\varkappa_g'}(\langle \alpha,\eta\rangle)\cdot Q^h_{\varkappa_h,\varkappa_h'}(\langle \xi,\alpha\rangle)).\end{aligned}$$

Таким образом, мы можем каждое предложение φ в логике первого порядка теории категорий перевести в предложение $\widetilde{\varphi}$ в логике второго порядка L_2 структуры $\langle Cn, ring\rangle$, причем алгоритм перевода никак не зависит от базисного кольца, при этом предложение φ истинно в категории mod-R тогда и только тогда, когда предложение $\widetilde{\varphi}$ истинно в структуре $\langle Cn, R\rangle$.

Рассмотрим некоторое предложение φ (формулу φ) языка первого порядка теории категорий.

Пусть все связанные (свободные и связанные) переменные предложения (формулы) φ содержатся среди $x_1, \dots, x_q$ (каждая x_l — это либо переменная для элементов класса Obj, либо переменная для элемента класса Mor). Рассмотрим некоторую последовательность элементов модели mod-R $y_1, \dots, y_q$ такую, что если x_l — переменная для объектов, то $y_l \in Obj$, а если x_l — переменная для морфизмов, то $y_l \in Mor$.

Переведем последовательность $y_1, \dots, y_q$ в последовательность $z_1, \dots, z_s$ элементов модели $\langle Cn, R\rangle_{L_2}$ следующим образом.

Если $y_l \in Obj$, то y_l является некоторым модулем над кольцом R. Как мы знаем, то в этом случае существует $\varkappa_l \in Cn$ и подмодуль M_l модуля $R^{(\varkappa_l)}$ такие, что

$$y_l \cong R^{(\varkappa_l)}/M_l.$$

Тогда переведем элемент y_l в пару $\langle z_l^1, z_l^2\rangle$, где $z_l^1 = \varkappa_l$, z_l^2 — это матрица размера $\varkappa_l \times \varkappa_l$ над кольцом R, у которой каждый столбец — это вектор порождающего множества векторов модуля M_l. Естественно, каждый столбец матрицы M_l в этом случае содержит лишь конечное число ненулевых элементов.

Если $y_l \in Mor$, то y_l Является морфизмом из модуля M_1 в модуль M_2. Пусть

$$M_1 \cong R^{(\varkappa_1)}/N_1, \quad M_2 \cong R^{(\varkappa_2)}/N_2.$$

Тогда для $m \in M_1$

$$m = r_1 e_{\alpha_1} + \dots + r_k e_{\alpha_k} + N_1,$$

где $r_1, \dots, r_k \in R$, $e_{\alpha_1}, \dots, e_{\alpha_k}$ — элементы базиса модуля $R^{(\varkappa_1)}$. Пусть $y_l(m) = n \in M_2$, т. е. $n = s_1 e_{\beta_1} + \dots + s_n e_{\beta_n}$, где $s_1, \dots, s_n \in R$, $e_{\beta_1}, \dots, e_{\beta_n}$ — элементы базиса модуля $R^{(\varkappa_2)}$.

Отсюда видно, что такой морфизм полностью определяется матрицей размерности $\varkappa_1 \times \varkappa_2$ такой, что $y_l(N_1) \subset N_2$. Поэтому переведем морфизм y_l в элементы z_l^1, z_l^2, z_l^3, z_l^4, z_l^5, где z_l^1 и z_l^2 — это переводы объекта, из которого происходит морфизм, z_l^3 и z_l^4 — это переводы объекта, в который переходит морфизм, а z_l^5 — это матрица $\varkappa_1 \times \varkappa_2$, определяемая следующей формулой: для каждого $\alpha \in \varkappa_1$, α-й столбец матрицы z_l^5 содержит r_i в строке с номером $\beta_i \in \varkappa_2$, если $y_l(e_\alpha) = \sum r_i e_{\beta_i}$, и 0 во всех остальных строках.

Таким образом, мы получим новую последовательность $z_1, \dots, z_s$. Так же, как и в предыдущей теореме, легко показать по индукции, что на этой последовательности в модели $\langle Cn, R \rangle_{L_2}$ предложение $\widetilde{\varphi}$ выполнено тогда и только тогда, когда предложение φ выполнено в модели mod-R на последовательности $y_1, \dots, y_q$.

Отсюда аналогично предыдущему пункту выводим, что если $\langle Cn, R \rangle \equiv_{L_2} \langle Cn, S \rangle$, то mod-$R \equiv$ mod-S. □

4.2.9 Аналог теоремы Мориты и следствия

Прямым следствием из теорем 4.5 и 4.6 является

Теорема 4.7. *Пусть даны кольца R и S и существует предложение ψ языка $L_2(\langle Cn, ring \rangle)$, истинное в кольце R и ложное во всех кольцах, ему подобных и не эквивалентных ему в языке $L_2(\langle Cn, ring \rangle)$. Тогда категории mod-$R$ и mod-S элементарно эквивалентны в том и только том случае, когда существует кольцо S', подобное кольцу S и такое, что структуры $\langle Cn, R \rangle$ и $\langle Cn, S' \rangle$ эквивалентны в логике L_2.*

Наиболее очевидными следствиями из теоремы 4.7 являются следующие два утверждения:

Следствие 4.1. *Для произвольных тел F_1 и F_2 категории mod-F_1 и mod-F_2 элементарно эквивалентны тогда и только тогда, когда структуры $\langle Cn, F_1 \rangle$ и $\langle Cn, F_2 \rangle$ эквивалентны в логике второго порядка L_2.*

Следствие 4.2. *Для произвольных коммутативных колец R_1 и R_2 категории mod-R_1 и mod-R_2 элементарно эквивалентны тогда и только тогда, когда структуры $\langle Cn, R_1 \rangle$ и $\langle Cn, R_2 \rangle$ эквивалентны в логике второго порядка L_2.*

Доказательство. В категории mod-R, где R — коммутативное кольцо, формула $Proobr(X)$ выделяет все прообразующие модули X, а формула

$$Comm(X) := Proobr(X) \wedge \forall f, g \in Mor(X, X)(f \circ g = g \circ f)$$

выделяет все объекты, изоморфные кольцу R (см. теорему 4.2). □

Также на поверхности лежат следствия из теоремы 4.7 для *локальных колец* и *областей главных идеалов.*

Напомним, что в [7] (лемма 1.2, стр. 15) доказано, что

Предложение 4.6. *Если R — локальное кольцо, то любой конечно порожденный проективный R-модуль свободен.*

Следствие 4.3. *Для произвольных локальных колец R_1 и R_2 категории mod-R_1 и mod-R_2 элементарно эквивалентны тогда и только тогда, когда структуры $\langle Cn, R_1\rangle$ и $\langle Cn, R_2\rangle$ эквивалентны в логике второго порядка L_2.*

Доказательство. В категории mod-R, где R — локальное кольцо, формула

$$\begin{aligned}Local(X) := Proobr(X) \wedge \forall f, g, h \in Mor(X, X) \\ ((\forall f' \in Mor(X, X) \neg(f \circ f' = f' \circ f = 1_X))\wedge \\ \wedge (\forall g' \in Mor(X, X) \neg(g \circ g' = g' \circ g = 1_X))\wedge \\ \wedge\, h = f \oplus g \Rightarrow (\forall h' \in Mor(X, X) \neg(h \circ h' = h' \circ h = 1_X))\end{aligned}$$

истинна только для модулей, изоморфных модулю R_R.

Действительно, из предложения 4.6 следует, что формула $Proobr(X)$ выполнена только для $X \circ R^{(n)}$. Пусть $e_1, \dots, e_n$ базис кольца $R^{(n)}$, $n \geqslant 1$. Тогда рассмотрим $f, g, h \in Mor(X, X)$ такие, что $f(e_1) = e_1$, $f(e_i) = 0$ при $i = ne1$, $g(e_1) = 0$, $g(e_i) = e_i$ при $i \neq 1$, $h(e_i) = e_i$ для любого $i = 1, \dots, n$.

Тогда для морфизмов f, g, h

$$\begin{aligned}(\forall f' \in Mor(X, X) \neg(f \circ f' = f' \circ f = 1_X)) \wedge (\forall g' \in Mor(X, X) \\ \neg(g \circ g' = g' \circ g = 1_X)) \wedge (h = f \oplus g) \wedge \exists h' \in Mor(X, X) \\ (h \circ h' = h' \circ h = 1_X)),\end{aligned}$$

где $h' = h$.

Отсюда следует, что в модуле X формула $Local(X)$ не выполнена. □

Кольцо R называется *кольцом главных идеалов*, если не содержит делителей нуля и каждый его идеал — *главный* (порождается одним элементов).

Предложение 4.7. (см. [39], гл. XV, § 2). *Пусть P — прообразующий модуль над кольцом главных идеалов. Тогда модуль P свободен.*

Следствие 4.4. *Для произвольных областей главных идеалов R_1 и R_2 категории mod-R_1 и mod-R_2 элементарно эквивалентны тогда и только тогда, когда структуры $\langle Cn, R_1\rangle$ и $\langle Cn, R_2\rangle$ эквивалентны в логике L_2.*

Доказательство. В категории mod-R, где R — область главных идеалов, формула

$$Principal(X) := Proobr(X) \wedge \forall f \in Mor(X, X) \forall g \in Mor(X, X)(f \circ g \neq 0 \wedge g \circ f \neq 0)$$

истинна только для модулей, изоморфных модулю R_R, что легко следует из предложения 4.7. □

Модуль M над кольцом R называется *артиновым*, если выполняются следующие эквивалентные условия:

1) всякое непустое множество подмодулей модуля M, упорядоченное по включению, имеет минимальный элемент;

2) всякая убывающая последовательность подмодулей модуля M стационарна.

Кольцо R называется *артиновым*, если модуль R_R артинов.

Модуль M называется *разложимым*, если существуют такие модули M_1 и M_2, что $M = M_1 \oplus M_2$. В противном случае модуль M называется *неразложимым.*

В книге [35], стр. 139 доказана следующая теорема:

Теорема 4.8. *Пусть M — конечно порожденный модуль над артиновым кольцом R.*

а) *Модуль M разлагается в прямую сумму конечного семейства $(M_i)_{1 \leqslant i \leqslant m}$ неразложимых ненулевых подмодулей.*

б) *Если модуль M является прямой суммой другого семейства $(M'_j)_{1 \leqslant j \leqslant n}$ неразложимых ненулевых подмодулей, то $m = n$, и существуют перестановка π множества $\{1, \ldots, n\}$ и автоморфизм α модуля M такие, что*

$$\alpha(M'_j) = M_{\pi(j)}, \quad 1 \leqslant j \leqslant n.$$

Теперь введем следующие предложения языка структуры $\langle Cn, ring \rangle$.

1. Для подмножества кольца M формула

$$Mod(M) := \forall r \in ring \forall m \in M \exists n \in M (rm = n) \wedge \forall l, m \in M \exists n \in M (n = l + m)$$

означает, что множество M является модулем над кольцом $ring$.

2. Для множеств M и N формула

$$\begin{aligned}(M \cong N) := Mod(N) \wedge \\ \wedge Mod(N) \wedge \exists F(v_1, v_2)(Dom(F) = M \wedge Rng(F) = N \wedge Bij(F) \wedge \\ \wedge \forall r_1, r_2 \in ring \forall m_1, m_2 \in M \forall n_1, n_2 \in N \\ (\langle m_1, n_1 \rangle \in F \wedge \langle m_2, n_2 \rangle \in F \Rightarrow \langle r_1 m_1 + r_2 m_2, r_1 n_1 + r_2 n_2 \rangle \in F))\end{aligned}$$

означает, что множества M и N являются $ring$-модулями, и что они изоморфны.

3. Для множеств $L, M, N \subset ring$ формула

$$\begin{aligned}(N = M \oplus L) := Mod(M) \wedge Mod(L) \wedge Mod(N) \wedge \\ \wedge \forall n \in N \exists m \in M \exists l \in L (n = m + l) \wedge \\ \wedge \forall m \in M \forall l \in L (m = l \Rightarrow m = 0)\end{aligned}$$

означает, что модуль N является прямой суммой модулей M и L.

4. Для множества $M \subset ring$ формула

$$Undir(M) := Mod(M) \wedge \forall L(c), N(c) \neg (M = L \oplus N)$$

означает, что модуль M неразложим.

5. Для множества $M \subset ring$ формула

$$\begin{aligned}Dir_N(M) := Mod(M) \wedge \exists M_1(c), \ldots, \exists M_N(c) \\ (Mod(M_1) \wedge \cdots \wedge Mod(M_N)) \wedge \\ \wedge \bigwedge_{i \neq j} \neg(M_i \cong M_j) \wedge M = M_1 \oplus \cdots \oplus M_N \wedge \\ \wedge (Undir(M_1) \wedge \cdots \wedge Undir(M_N))\end{aligned}$$

означает, что модуль M является прямой суммой неразложимых не изоморфных друг другу модулей $M_1, \ldots, M_N$.

Предположим, что мы имеем некоторое артиново кольцо R. Тогда модуль R_R артинов, а значит, является прямой суммой n неразложимых модулей. Пусть это модули

$$M_1^1, \ldots, M_1^{i_1}, M_2^1, \ldots, M_2^{i_2}, \ldots, M_k^1, \ldots, M_k^{i_k},$$

причем при $k \neq l$

$$M_k^i \ncong M_l^j,$$

а для любого k

$$M_k^i \cong M_k^j.$$

Рассмотрим модуль

$$M := M_1^1 \oplus \cdots \oplus M_k^1.$$

Так как модуль M является прямым слагаемым модуля R_R, то он проективен и конечно порожден. Так как модуль R_R является прямым слагаемым модуля $M^{(\max(i_1,\ldots,i_k))}$, то M — образующий модуль. Значит, модуль M является прообразующим, а кольцо $End_R M$ подобно кольцу R.

Таким образом, для некоторого $N \in \omega$ формула

$$\psi(P) := Proobr(P) \wedge Undir_N(P)$$

выделяет единственный, с точностью до изоморфизма, прообразующий модуль

$$M := M_1^1 \oplus \cdots \oplus M_k^1.$$

Следовательно, нами доказано

Следствие 4.5. *Для произвольных артиновых колец R_1 и R_2 категории mod-R_1 и mod-R_2 элементарно эквивалентны тогда и только тогда, когда существуют кольца S_1 и S_2, подобные кольцам R_1 и R_2 соответственно, такие, что структуры $\langle Cn, S_1\rangle$ и $\langle Cn, S_2\rangle$ эквивалентны в логике L_2.*

4.3 Элементарная эквивалентность колец эндоморфизмов модулей бесконечных рангов

4.3.1 Кольца эндоморфизмов модулей и категории $C_{M(V)}$

Предположим, что мы имеем ассоциативное кольцо R с единицей, бесконечное кардинальное число $\varkappa$ и свободный модуль $V = V_\varkappa^R$ ранга $\varkappa$ над R.

На протяжении всего этого параграфа будем считать, что каждый идеал кольца R порождается не более, чем $\varkappa$ элементами кольца. Это всегда так, когда $\varkappa \geqslant |R|$, когда R — кольцо главных идеалов или когда кольцо R полупросто.

Мы хотим интерпретировать в кольце $\mathrm{End}\,_R V$ категорию $C_{M(V)}$, состоящую из модуля V, всех его фактормодулей и всех гомоморфизмов между ними. Под словом "интерпретировать" мы имеем в виду, что существует алгоритм, переводящий каждую формулу φ языка теории категорий в формулу $\widetilde{\varphi}$ языка теории колец таким образом, что формула φ истинна в $C_{M(V)}$ тогда и только тогда, когда $\widetilde{\varphi}$ истинна в $\mathrm{End}\,_R(V)$.

Сначала дадим неформальное описание перевода.

1. Каждому объекту X категории $C_{M(V)}$ мы сопоставим элемент $\widetilde{X}$ кольца $\mathrm{End}\,_R V$ следующим образом: если $X \in C_{M(V)}$, то $X = V/X'$ для некоторого X' — подмодуля модуля V. Каждый подмодуль модуля V можно задать порождающими его векторами, мощность множества которых не превышает $\varkappa$. Эти векторы можно записать как столбцы матрицы размера $\varkappa \times \varkappa$ (если их меньше, то можно дополнить матрицу нулевыми столбцами), т. е. как элемент кольца $\mathrm{End}\,_R V$. Обратно, если $\widetilde{X} \in \mathrm{End}\,_R V$, то можно рассмотреть модуль, порожденный векторами-столбцами матрицы $\widetilde{X}$, а затем фактор-модуль $X := V/\widetilde{X}$.

2. Каждому морфизму f категории $C_{M(V)}$ мы сопоставим тройку $\langle X_f, Y_f, \widetilde{f}\rangle$ элементов кольца $\mathrm{End}\,_R V$ такую, что если $f \in Mor(X,Y)$, то $X_f = \widetilde{X}$, $Y_f = \widetilde{Y}$, а $\widetilde{f}$ — это матрица, осуществляющая такой гомоморфизм $\widetilde{f} \in Mor(V,V)$, что

$$\widetilde{f} \circ p_Y = p_X \circ f,$$

где p_X и p_Y — стандартные эпиморфизмы модуля V на модули X и Y соответственно.

Из этого соотношения видно, что матрица $\widetilde{f}$ должна переводить векторы модуля X' в векторы модуля Y', т. е. матрица $\widetilde{f}\widetilde{X}$ должна порождать подмодуль модуля, порожденного матрицей $\widetilde{Y}$, что означает, что существует $A \in \mathrm{End}\,_R V$ такое, что

$$\widetilde{f}\widetilde{X} = \widetilde{Y}A.$$

Два эндоморфизма модуля V задают один и тот же морфизм из модуля X в модуль Y, если их разность задает нулевой морфизм из модуля X в модуль Y, то есть образ этого морфизма весь лежит в модуле Y'.

Таким образом, будем считать тройки $\langle X_f, Y_f, \widetilde{f}_1\rangle$ и $\langle X_f, Y_f, \widetilde{f}_2\rangle$ равными, если

$$\exists A (f_1 - f_2 = Y_f A).$$

Перейдем теперь к формальному описанию.

1. Подформула $\forall X \in Obj$ перейдет в подформулу $\forall \widetilde{X}$ (аналогично для подформулы $\exists X \in Obj$).

2. Подформула $\forall f \in Mor$ перейдет в подформулу

$$\forall X_f \forall Y_f \forall \widetilde{f}(\exists A(\widetilde{f} \circ X_f = Y_f \circ A) \Rightarrow \dots)$$

(аналогично для подформулы $\exists f \in Mor$).

3. Подформула $f \in Mor(X, Y)$ перейдет в подформулу $X_f = \widetilde{X} \wedge Y_f = \widetilde{Y}$.

4. Подформула $h = f \circ g$ перейдет в подформулу $\widetilde{h} = \widetilde{f} \circ \widetilde{g}$.

5. Подформула $f = 1_X$ перейдет в подформулу $X_f = Y_f = \widetilde{X} \wedge \widetilde{f} = 1$.

Алгоритм построен. Совершенно аналогично предыдущим параграфам можно показать, что предложение φ истинно в категории $C_{M(V)}$ тогда и только тогда, когда предложение $\widetilde{\varphi}$ истинно в кольце $\mathrm{End}_R V$.

Заметим теперь, что мы будем рассматривать не просто алгебраическую структуру $C_{M(V)}$, язык которой является языком теории категорий, а структуру $C_{M(V)}$ с выделенным модулем V, т. е. с возможностью в формулах писать подформулу $X = V$ для $X \in Obj$. Такой подформуле, очевидно, мы поставим в соответствие подформулу $\widetilde{X} = 0$.

Таким образом, если кольца $\mathrm{End}_R V$ и $\mathrm{End}_S W$ элементарно эквивалентны, то и категории $C_{M(V)}$ и $C_{M(W)}$ элементарно эквивалентны.

Докажем теперь обратную импликацию.

Для этого мы должны внутри категории $C_{M(V)}$ с выделенным объектом V интерпретировать кольцо $\mathrm{End}_R V$.

Действительно, в категории $C_{M(V)}$ фиксируем некоторый $V^2 \in Obj$ такой, что $V^2 \cong V \oplus V$ (например, $V \cong V \oplus V$) и такие морфизмы $i_1, i_2 \in Mor(V, V^2)$ и $p_1, p_2 \in Mor(V^2, V)$, что $p_1 \circ i_1 = p_2 \circ i_2 = 1_V \wedge p_1 \circ i_2 = p_2 \circ i_1 = 0 \wedge \forall i \in Mor(V, V^2)(i \neq 0_{V,V^2} \Rightarrow p_1 \circ i \neq 0_V \vee p_2 \circ i \neq 0_V)$.

Очевидно, что в этом случае морфизмы i_1 и i_2 Являются такими вложениями модуля V в модуль $V \oplus V$, что их образы не пересекаются, а в сумме составляют все $V \oplus V$.

Теперь переведем подформулы $\forall f$ и $\exists f$ в подформулы $\forall f \in Mor(V, V)$ и $\exists f \in Mor(V, V)$; а подформулы $h = f \cdot g$ и $h = f + g$ — в подформулы $h = f \circ g$ и $h = f \oplus g$ (см. § 2.5).

Следовательно, мы получаем, что из $C_{M(V_1)} \equiv C_{M(V_2)}$ следует $\mathrm{End}_{R_1}(V_1) \equiv \mathrm{End}_{R_2}(V_2)$.

Таким образом, мы свели вопрос элементарной эквивалентности колец эндоморфизмов $\mathrm{End}_{R_1}(V_1)$ и $\mathrm{End}_{R_2}(V_2)$ к вопросу элементарной эквивалентности категорий $C_{M(V_1)}$ и $C_{M(V_2)}$ с выделенными объектами V_1 и V_2 соответственно.

4.3.2 Элементарная эквивалентность в категориях вида $C_{M(V)}$

Итак, наша ситуация очень сильно напоминает ситуацию § 2. Мы имеем категорию $C_{M(V)}$, являющуюся подкатегорией в mod-R, замкнутой относительно взятия фактормодулей, а также прямых произведений мощности не большей некоторой бесконечной мощности $\varkappa$. Такая категория во многом напоминает категорию mod-R, но является малой и ограничена данной мощностью $\varkappa$. Кроме того, в этой категории модуль V является выделенным.

Перенесем на нее все возможные результаты из § 2.

Формула $Simp(M)$ также выделяет в категории $C_{M(V)}$ простые модули, так как эта категория замкнута относительно взятия фактормодулей. Формула $Sum^{\omega}(X, M)$ также выделит модуль $X \simeq M^{(\omega)}$, так как кардинал $\varkappa$ по условию не меньше, чем ω. Очевидно, что формула $Sum^{Fin}(X, M)$ будет истинна для конечных прямых сумм модуля M, а формула $Sum(X, M)$ — для всех прямых сумм модуля M, принадлежащих категории $C_{M(V)}$.

Точно так же переносятся на случай категории C_V все формулы из п. 2.2, в том числе и формула $Proobr(P)$, выделяющая в этой категории все прообразующие модули.

После выделения некоторого прообразующего модуля P совершенно аналогично п. 2.3 строится аналог кольца $\mathrm{End}\,_R P$, так как п. 2.3 используется только замкнутость категории mod-R относительно конечных прямых сумм.

Так как результаты п. 2.4 также легко переносятся на наш случай, то верна

Теорема 4.9. *Категории $C_{M(V_1^R)}$ и $C_{M(V_2^S)}$, где R — конечное кольцо, элементарно эквивалентны тогда и только тогда, когда $R \cong \mathrm{End}\,_S P$ для некоторого прообразующего модуля P категории $C_{M(V_2^S)}$.*

Легко также видеть, что мы, следуя пп. 2.5 и 2.6, можем найти формулу $\varphi(f)$, истинную для некоторого независимого множества отображений $f : V \to P$ мощности $\varkappa$ таких, что для каждого такого f существует $g : P \to V$ такое, что $f \circ g = 1_P$, $g \circ f$ — проектор из V в V.

Структуру $\langle Cn, ring\rangle$, описанную в п. 2.7, мы в случае категории $C_{M(V)}$ заменим на структуру $\langle \varkappa, ring\rangle$, состоящую из множества $\varkappa$ (т. е. просто множества мощности $\varkappa$) и кольца $ring$ с отношениями суммы и произведения.

Напомним, что *теорией* T модели $\mathcal{U}$ языка $\mathcal{L}$ называется множество всех предложений языка $\mathcal{L}$, истинных в модели $\mathcal{U}$.

Если нам дано конкретное кольцо R, т. е. модель R, то также мы имеем модель $\langle \varkappa, R\rangle$ и теорию $T_2(\langle \varkappa, R\rangle)$, состоящую из всех предложений языка $L_2(\langle \varkappa, ring\rangle)$, истинных в модели $\langle \varkappa, R\rangle$. Через $T_2^{\varkappa}(\langle \varkappa, R\rangle)$ мы будем обозначать подмножество множества $T_2(\langle \varkappa, R\rangle)$, состоящее из всех предложений теории $T_2(\langle \varkappa, R\rangle)$, в которых используются только предикатные символы

$$P(c_1, \ldots, c_k; v_1, \ldots, v_{)},$$

где $c_1, \ldots, c_k$ — переменные для элементов множества $\varkappa$, $v_1, \ldots, v_n$ — переменные для элементов кольца, с условием

$$|\{\langle \alpha_1, \ldots, \alpha_k, r_1, \ldots, r_n\rangle \mid \alpha_1, \ldots, \alpha_k \in \varkappa \wedge r_1, \ldots, r_n \in R \wedge (\alpha_1, \ldots, \alpha_k, r_1, \ldots, r_n)\}| \leqslant \varkappa.$$

Теорема 4.10. *Пусть даны два свободных модуля V_1 и V_2 бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над кольцами R_1 и R_2 соответственно, и существует предложение $\psi \in Th_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$, ложное во всех кольцах, подобных кольцу R_1 и имеющих другую теорию $Th_2^{\varkappa_1}$. Пусть, кроме того, категории $C_{M(V_1)}$ и $C_{M(V_2)}$ элементарно эквивалентны. Тогда существует кольцо S, подобное кольцу R_2 и такое, что теории $Th_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$ и $Th_2^{\varkappa_2}(\langle \varkappa_2, S\rangle)$ совпадают.*

Доказательство. Доказательство этой теоремы во многом похоже на доказательство теоремы 4.5 § 2, но приведем его достаточно подробно, чтобы показать отличия.

Предположим сначала, что мы каким-то образом фиксировали прообразующий модуль P в категории $C_{M(V)}$, где $V = V_T^{\varkappa}$, $\varkappa$ — бесконечное кардинальное число, T — кольцо (очевидно, что все прообразующие модули категории mod-T содержатся в категории $C_{M(V)}$). Тогда мы имеем формулы, выделяющие простой модуль M, соответствующий модулю P, модули $M^{(\alpha)}$ для всех $\alpha \in Cn \cap \varkappa + 1$, модули $M^{(n)}$ для всех $\alpha \in \omega$, модули $M^{(\alpha)}$ для бесконечных $\alpha \in Cn \cap \varkappa + 1$, почти свободные модули V^{α} рангов $\alpha \in Cn \cap \varkappa + 1$, $\alpha \in \omega$,

$\alpha \in Cn \cap \varkappa{+}1 \setminus \omega$, а также выделенный свободный модуль V, являющийся почти свободным над модулем P.

Для модуля $M^{(\varkappa)}$ (V) выделим (в соответствии с § 2.5) его порождающее множество проекторов $Gen_{\overline{g}*}(M^{(\varkappa)}, M)$ (или $Gen_{\overline{g}*}(V, P)$).

Кроме того (см. п. 2.3) для любых $f, g \in Mor(P, P)$ мы считаем известной их сумму $f \oplus g \in Mor(P, P)$ и произведение $f \otimes g \in Mor(P, P)$.

Рассмотрим некоторое произвольное предложение φ языка $L_2(\langle \varkappa, ring \rangle)$. В это предложение могут входить подформулы

1) $\forall(\exists) r \in ring$;
2) $\forall(\exists) \alpha \in \varkappa$;
3) $r_1 = r_2 + r_3$;
4) $r_1 = r_2 \cdot r_2$;
5) $r_1 = r_2$;
6) $\alpha_1 = \alpha_2$;
7) $\forall(\exists) P(c_1, \ldots, c_k; v_1, \ldots, v_n)$;
8) $P(\alpha_1, \ldots, \alpha_k; r_1, \ldots, r_n)$.

Переведем это предложение в предложение $\widetilde{\varphi}_P$ (зависящее от фиксированного изначально модуля P) языка первого порядка теории категорий по следующему алгоритму:

1) подформула $\forall(\exists) r \in ring$ переводится в подформулу $\forall(\exists) f_r \in Mor(P, P)$, т. е. каждому элементу кольца $ring$ ставится в соответствие элемент кольца $\mathrm{End}_T P$:
2) подформула $\forall(\exists) \alpha \in \varkappa$ переводится в подформулу $\forall(\exists) F^\alpha \in Gen_{\overline{g}*}(M^{(\varkappa)}, M)$;
3) подформула $r_1 = r_2 + r_3$ переводится в подформулу $f_{r_1} = f_{r_2} \oplus f_{r_3}$;
4) подформула $r_1 = r_2 \cdot r_3$ переводится в подформулу $f_{r_1} = f_{r_2} \otimes f_{r_3}$;
5) подформула $r_1 = r_2$ переводится в подформулу $f_{r_1} = f_{r_2}$;
6) подформула $\alpha_1 = \alpha_2$ переводится в подформулу $f^{\alpha_1} = f_{\alpha_2}$;
7) подформула $\forall(\exists) P(c_1, \ldots, c_k; v_1, \ldots, v_n)$ переводится в подформулу

$$\forall(\exists) f_P^{c_1} \in Sets(M^{(\varkappa)}, M^{(\varkappa)}) \ldots \forall(\exists) f_P^{c_k} \in Sets(M^{(\varkappa)}, M^{(\varkappa)})$$
$$\forall(\exists) f_P^{v_1} \in Ring(V) \ldots \forall(\exists) f_P^{v_n} \in Ring(V);$$

8) подформула

$$P(\alpha_1, \ldots, \alpha_k; r_1, \ldots, r_n)$$

переводится в подформулу

$$\exists f \in Gen(M^{(\varkappa)}, M)$$
$$(f^{\alpha_1} \circ f_P^{c_1} \circ \overline{f} = 1 \wedge \cdots \wedge f^{\alpha_k} \circ f_P^{c_k} \circ \overline{f} = 1 \wedge f' \circ f_P^{v_1} \circ \overline{f}' = f_{r_1} \wedge \cdots \wedge f' \circ f_P^{v_n} \circ \overline{f}' = f_{r_n}).$$

Аналогично тому, как это делалось в теореме 2.5, можно показать, что предложение φ истинно в теории $\langle \varkappa, End_T P \rangle$ тогда и только тогда, когда предложение $\widetilde{\varphi}_P$ истинно в модели $C_{M(V_T^\varkappa)}$, откуда, аналогично теореме 2.5, доказывается утверждение теоремы. □

Теорема 4.11. *Если $\varkappa_1$ и $\varkappa_2$ — бесконечные кардинальные числа, V_1 и V_2 — свободные модули рангов $\varkappa_1$ и $\varkappa_2$ над кольцами R_1 и R_2 соответственно, и теории $Th_2^{\varkappa_1}\langle \varkappa_1, R_1 \rangle$ и $Th_2^{\varkappa_2}\langle \varkappa_2, R_2 \rangle$ совпадают, то категории $C_{M(V_1)}$ и $C_{M(V_2)}$ элементарно эквивалентны.*

Доказательство. Доказательство этой теоремы отличается от доказательства теоремы 4.6 § 2 только тем, что модуль V должен быть выделенным объектом категории $C_{M(V)}$. Но так как по условию теоремы мы рассматриваем свободные модули (именно здесь важно то, что модули свободны, а не почти свободны), то выделенным объектом категории будет считаться нулевая матрица. □

Прямым следствием из теорем 4.10 и 4.11 является

Теорема 4.12. *Пусть V_1 и V_2 — свободные модули бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над кольцами R_1 и R_2 соответственно, и существует предложение $\psi \in T_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$, ложное во всех кольцах, подобных кольцу R_1 и имеющих другую теорию $Th_2^{\varkappa_1}$. Тогда категории $C_{M(V_1)}$ и $C_{M(V_2)}$ элементарно эквивалентны в том и только том случае, когда существует кольцо S, подобное кольцу R_2 и такое, что теории $Th_2^{\varkappa_1}\langle \varkappa_1, R_1\rangle$ и $Th_2^{\varkappa_2}\langle \varkappa_2, S\rangle$ совпадают.*

4.3.3 Основная теорема

Из результатов предыдущих двух пунктов легко получаем

Теорема 4.13. *Пусть V_1 и V_2 — свободные модули бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над кольцами R_1 и R_2 соответственно, и существует предложение $\psi \in Th_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$, ложное во всех кольцах, подобных кольцу R_1 и имеющих другую теорию $Th_2^{\varkappa_1}$. Тогда кольца $\mathrm{End}_{R_1}(V_1)$ и $\mathrm{End}_{R_2}(V_2)$ элементарно эквивалентны в том и только том случае, когда существует кольцо S, подобное кольцу R_2 и такое, что теории $Th_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$ и $Th_2^{\varkappa_2}(\langle \varkappa_2, S\rangle)$ совпадают.*

Следствие 4.1. *Для пространств V_1 и V_2 бесконечных размерностей $\varkappa_1$ и $\varkappa_2$ над произвольными телами (областями главных идеалов) F_1 и F_2 кольца $\mathrm{End}_{F_1} V_1$ и $\mathrm{End}_{F_2} V_2$ элементарно эквивалентны тогда и только тогда, когда теории $Th_2^{\varkappa_1}(\langle \varkappa_1, F_1\rangle)$ и $Th_2^{\varkappa_2}(\langle \varkappa_2, F_2\rangle)$ совпадают.*

Следствие 4.2. *Предположим, что $\varkappa_1$ и $\varkappa_2$ — бесконечные кардинальные числа, R_1 и R_2 — коммутативные (локальные) кольца, и каждый максимальный идеал кольца R_1 порожден не более, чем $\varkappa_1$ элементами кольца. Тогда для свободных модулей V_1 и V_2 рангов $\varkappa_1$ и $\varkappa_2$ над кольцами R_1 и R_2 соответственно, кольца $\mathrm{End}_{R_1} V_1$ и $\mathrm{End}_{R_2} V_2$ элементарно эквивалентны тогда и только тогда, когда теории $Th_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$ и $Th_2^{\varkappa_2}(\langle \varkappa_2, R_2\rangle)$ совпадают.*

Следствие 4.3. *Предположим, что $\varkappa_1$ и $\varkappa_2$ — бесконечные кардинальные числа, R_1 и R_2 — артиновы кольца, и каждый максимальный идеал кольца R_1 порожден не более, чем $\varkappa_1$ элементами кольца. Тогда для свободных модулей V_1 и V_2 рангов $\varkappa_1$ и $\varkappa_2$ над кольцами R_1 и R_2 соответственно, кольца $\mathrm{End}_{R_1} V_1$ и $\mathrm{End}_{R_2} V_2$ элементарно эквивалентны тогда и только тогда, когда существуют кольца S_1 и S_2, подобные кольцам R_1 и R_2 соответственно, такие, что теории $Th_2^{\varkappa_1}(\langle \varkappa_1, S_1\rangle)$ и $Th_2^{\varkappa_2}(\langle \varkappa_2, S_2\rangle)$ совпадают.*

Следствие 4.4. *Для свободных модулей V_1 и V_2 бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над полупростыми кольцами R_1 и R_2 соответственно, кольца $\mathrm{End}_{R_1}(V_1)$ и $\mathrm{End}_{R_2}(V_2)$ элементарно эквивалентны тогда и только тогда, когда Существуют кольца S_1 и S_2, подобные кольцам R_1 и R_2 соответственно, такие, что теории $Th_2^{\varkappa_1}\langle\varkappa_1, S_1\rangle)$ и $Th_2^{\varkappa_2}(\langle\varkappa_2, S_2\rangle)$ совпадают.*

4.4 Проективная геометрия модуля V

4.4.1 Язык проективной геометрии и основные понятия, определимые в этом языке

Предположим, что мы имеем некоторый свободный модуль V бесконечного ранга $\varkappa$ над кольцом R. *Проективной геометрией* (*решеткой подмодулей*) $P(V)$ модуля V называется алгебраическая структура, состоящая из всех подмодулей модуля V, с отношением $\subset$ (пишем $M \subset N$, если модуль M является подмодулем модуля N).

На протяжении всего этого параграфа мы будем полагать, что всякий подмодуль модуля V порожден не более чем $\varkappa$ элементами модуля V (это так, если $\varkappa \geqslant |R|$, или если кольцо R полупросто, или является областью главных идеалов).

Пусть $M_1, M_2, M_3 \in P(V)$.

Будем писать, что $M_1 = V$, если $\forall M(M \subset M_1)$.

Будем писать, что $M_1 = \emptyset$, если $\forall M(M_1 \subset M)$.

Формула $M_1 = M_2 \cap M_3$ будет обозначением для формулы

$$M_1 \subset M_2 \wedge M_1 \subset M_3 \wedge \forall M_4(M_4 \subset M_2 \wedge M_4 \subset M_3 \Rightarrow M_4 \subset M_1).$$

Формула $M_1 = M_2 + M_3$ — обозначением для формулы

$$M_2 \subset M_1 \wedge M_3 \subset M_1 \wedge \forall M_4(M_2 \subset M_4 \wedge M_3 \subset M_4 \Rightarrow M_1 \subset M_4),$$

а формула $M_1 = M_2 \oplus M_3$ — обозначением для формулы

$$M_1 = M_2 + M_3 \wedge M_2 \cap M_3 = \emptyset.$$

Легко увидеть, что при $M_1 = M_2 \cap M_3$ модуль M_1 является пересечением модулей M_2 и M_3, при $M_1 = M_2 + M_3$ — суммой модулей M_2 и M_3, при $M_1 = M_2 \oplus M_3$ — прямой суммой модулей M_2 и M_3.

Рассмотрим теперь для данных модулей P_1 и P_2 формулу

$$P_1 \cap P_2 = \emptyset \wedge \exists P(P \subset P_1 \oplus P_2 \wedge P \neq \emptyset \wedge P \cap P_1 = \emptyset \wedge \\ \wedge P \cap P_2 = \emptyset \wedge P \oplus P_1 = P_1 \oplus P_2 \wedge P \oplus P_2 = P_1 \oplus P_2).$$

Пусть модули P_1 и P_2 не пересекаются и существует модуль P, удовлетворяющий всем условиям, перечисленным в формуле. Так как $P \subset P_1 \oplus P_2$, то любое $x \in P$ имеет вид $x = y+z$, где $y \in P_1$, $z \in P_2$, причем элементы z и y однозначно определяются вектором x. Рассмотрим соответствие $F \subset P_1 \times P_2$, определяемое формулой $\forall y \in P_1 \forall z \in P_2 \langle y, z\rangle \in F \Leftrightarrow \exists x \in P(x = y + z)$. Покажем, что F является изоморфизмом между модулями P_1 и P_2.

1. Если $y_1, y_2 \in P_1, z \in P_2$, $\langle y_1, z\rangle \in F$ и $\langle y_2, z\rangle \in F$, то $\exists x_1, x_2 \in P(x_1 = y_1+z \wedge x_2 = y_2+z$, т. е. $x := x_1 - x_2 = y_1 - y_2 \in P$. Так как при этом $y_1 - y_2 \in P$, то $y_1 - y_2 \in P \cap P_1 \Rightarrow y_1 - y_2 = 0 \Rightarrow y_1 = y_2$.

2. Аналогично из $y \in P_1$, $z_1, z_2 \in P_2$, $\langle y, z_1\rangle \in F$ и $\langle y, z_2\rangle \in F$ следует $z_1 = z_2$.

3. Рассмотрим произвольный вектор $y \in P_1$. Так как $y \in P_1 \oplus P_2$, то $y \in P \oplus P_2$, т. е. $\exists x \in P \exists z \in P_2(y = x+z)$, т. е. $x = y-z$, откуда следует, что $\langle y_1 - z\rangle \in F$, т. е. $Dom(F) = P_1$.

4. Аналогично доказывается, что $Rng(F) = P_2$.

5. Мы показали, что F — биекция между модулями P_1 и P_2. Осталось показать, что F является гомоморфизмом, т. е. что из $\langle y_1, z_1\rangle, \langle y_2, z_2\rangle \in F$ следует

$$\langle \alpha_1 y_1 + \alpha_2 y_2, \alpha_1 z_1 + \alpha_2 z_2\rangle \in F.$$

Действительно, из $\langle y_1, z_1\rangle, \langle y_2, z_2\rangle \in F$ следует

$$\begin{aligned} &y_1 + z_1, y_2 + z_2 \in P \Rightarrow \alpha_1(y_1 + z_1) + \alpha_2(y_2 + z_2) \in P \Rightarrow \\ &\qquad \Rightarrow (\alpha_1 y_1 + \alpha_{@} y_2) + (\alpha_1 z_1 + \alpha_2 z_2) \in P \Rightarrow \langle \alpha_1 y_1 + \alpha_2 y_2, \alpha_1 z_1 + \alpha_2 z_2\rangle \in F. \end{aligned}$$

Таким образом, модули P_1 и P_2, удовлетворяющие нашей формуле, не пересекаются и изоморфны. Наоборот, если два модуля P_1 и P_2 не пересекаются и изоморфны, то они удовлетворяют нашей формуле, поэтому будем обозначать ее через $P_1 \cong_d P_2$.

Предположим, что модули P_1 и P_2 “не слишком велики”, т. е. существуют модули P_1' и P_2' такие, что $P_1 \cap P_1' = P_2 \cap P_2' = \emptyset$ и модуль P_1' содержит подмодуль, изоморфный P_1, а модуль P_2' содержит подмодуль, изоморфный P_2. Тогда формула

$$\exists P \exists P'(P \cong_D P_1 \wedge P' \cong_d P_2 \wedge P \cong_d P')$$

истинна в том и только том случае, когда модули P_1 и P_2 изоморфны.

Мы знаем, что модуль P проективен тогда и только тогда, когда он изоморфен прямому слагаемому свободного модуля. Поэтому формула

$$Proj(P) := \exists Q(V = P \oplus Q)$$

выделяет в пространстве $P(V)$ проективные модули.

Рассмотрим некоторый проективный модуль P. Его подмодуль M мы будем называть *максимальным* подмодулем модуля P ($M = \max(P)$), если выполнена формула

$$\forall P'(M \subset P' \wedge P' \subset P \Rightarrow P' = M \vee P' = P).$$

Для каждого конечно порожденного модуля P найдется максимальный подмодуль M.

Пусть фиксирован проективный модуль P и его максимальный подмодуль M.

Формула $X \subset_\circ Y$ будет обозначать, что модуль X является прямым слагаемым модуля Y.

Рассмотрим пару модулей $\langle X, Y\rangle$, удовлетворяющую следующей формуле:

$$\begin{aligned}\overline{Sum}_{P,M}(X,Y) := Y \subset X \wedge \exists Q \exists Q'(Q \oplus P = X \wedge Q \cong X \wedge Q' \oplus M = Y \wedge \\ \wedge\, Q' \cong Y \wedge \forall N \subset_\circ X (N \cong P \Rightarrow N \cap Y \cong M \wedge (N \cap Y) \subset_\circ Y))) \wedge \\ \wedge\, \forall Z (Z \subset X \wedge \forall N (N \subset_\circ Z \Rightarrow N \ncong P) \Rightarrow Z \subset Y).\end{aligned}$$

Посмотрим, какие модули X и Y удовлетворяют формуле $\overline{Sum}_{P,M}$.

Из того, что $\exists Q(Q \oplus P = X \wedge Q \cong X)$ мы видим, что модуль P выделяется прямым слагаемым в модуле X причем дополнение Q изоморфно X. Значит, существует некоторое бесконечное кардинальное число α, а также модули X_1 и X_2 такие, что $X_1 \oplus X_2 = X$, $X_1 \cong P^{(\alpha)}$, в модуле X_2 модуль P не выделяется прямым слагаемым. Часть формулы

$$\forall Z (Z \subset X \wedge (\forall N (N \subset_\circ Z \Rightarrow N \ncong P) \Rightarrow Z \subset Y)$$

показывает, что если Z — некоторый подмодуль модуля X такой, что модуль P не выделяется в нем прямым слагаемым, то Z является подмодулем также и в Y. Если положить $X_2 := Z$, то получим $X_2 \subset Y$. Возьмем произвольное $y \in Y$. Так как $y \in X$, то $y = x_1 + x_2$, где $x_1 \in X_1$, $x_2 \in X_2$. Так как $X_2 \subset Y$, то $x_1 \in Y$, т. е. $Y = (X_1 \cap Y) \oplus X_2$.

Теперь из оставшихся условий легко увидеть, что $X_1 \cap Y \cong M^{(\alpha)}$. Таким образом, если X и Y удовлетворяют формуле $\overline{Sum}_{P,M}(X,Y)$, то существует модуль Q и бесконечное кардинальное число α такие, что $X \cong Q \oplus P^{(\alpha)}$, $Y \cong Q \oplus M^{(\alpha)}$. Обратная импликация очевидна, если модуль X "не слишком большой".

Теперь рассмотрим формулу

$$\begin{aligned}Sum^{\omega}_{P,M}(X,Y) := \forall Z \forall T (\overline{Sum}_{P,M}(Z,T) \Rightarrow \\ \Rightarrow \exists X_1 \exists X_2 \exists Y' X_1 \oplus X_2 = Z \wedge X_1 \cap T = Y' \wedge X_1 \cong X \wedge Y' \cong Y) \wedge \overline{Sum}_{P,M}(X,Y).\end{aligned}$$

Из подформулы $\overline{Sum}_{P,M}(X,Y)$ следует, что $X \cong Q \oplus P^{(\alpha)}$, $Y \cong Q \oplus M^{(\alpha)}$ для некоторого кардинального числа α. Из первой части формулы следует, что X выделяется прямым слагаемым в любом модуле вида $Q' \oplus P^{(\beta)}$ (β — бесконечное кардинальное число), а значит, и в модуле $P^{(\omega)}$. Отсюда следует, что $\alpha = \omega$, модуль Q проективен и счетно порожден.

Теперь рассмотрим формулу

$$\begin{aligned}Sum^{Fin}_{P,M}(X,Y) := \neg Sum^{\omega}_{P,M}(X,Y) \wedge \exists X', Y' (Sum^{\omega}(X',Y') \wedge \\ \wedge\, \exists X'' (X' = X \oplus X' \wedge Y = X \cap Y')).\end{aligned}$$

Любой модуль X, удовлетворяющий формуле $Sum^{Fin}_{P,M}(X,Y)$, является прямым слагаемым в модуле $Q \oplus P^{(\omega)}$, т. е. имеет вид $Q' \oplus P^{(n)}$ (возможно, $n = 0$, но $n \in \omega$), причем Q' есть прямое слагаемое модуля Q. Пусть модули X_1, X_2, Y_1, Y_2 таковы, что $Sum^{Fin}_{P,M}(X_1,Y_1)$ и $Sum^{Fin}_{P,M}(X_2,Y_2)$. Если $\exists X_1', Y_1' (Sum^{Fin}_{P,M}(X_1',Y_1') \wedge X_1' \cong X_1 \wedge Y_1' \cong Y_1)$ и при этом

$$\begin{aligned}\forall P' \forall M' (P' \cong P \wedge M' \cong M \wedge M' = \max(P') \wedge \\ \wedge\, \exists P'') P' \oplus P'' = X_1' \wedge P' \cap Y_1' = M') \Rightarrow P' \subset_\circ X_1' \cap X_2') \wedge \\ \wedge\, \forall P' \forall M' (P' \cong P \wedge M' \cong M \wedge M' = \max(P') \wedge \\ \wedge\, \exists P'') P' \oplus P'' = X_2' \wedge P' \cap Y_2' = M') \Rightarrow P' \subset_\circ X_1' \cap X_2'),\end{aligned}$$

то будем называть пары (X_1, Y_1) и (X_2, Y_2) *эквивалентными* ($(X_1, Y_1) \sim (X_2, Y_2)$). Очевидно, что если $(X_1, Y_1) \sim (X_2, Y_2)$, $X_1 \cong Q_1 \oplus P^{(n_1)}$, $X_2 \cong Q_2 \oplus P^{(n_2)}$, то $n_1 = n_2$. Будем обозначать классы эквивалентности таких пар через $Cl^n_{P,M}$.

Для двух классов $Cl^m_{P,M}$ и $Cl^n_{P,M}$ будем писать $Cl^m_{P,M} < Cl^n_{P,M}$, если

$$\forall (X_1, Y_1) \in Cl^m_{P,M} \exists (X_2, Y_2) \in Cl^n_{P,M} \exists X_3 (X_1 \cong X_3 \wedge X_1 \subset_\circ X_2).$$

Очевидно, что соотношение $Cl^m_{P,M} < Cl^n_{P,M}$ равносильно соотношению $m < n$.

Аналогично модулям вида $Q \oplus P^{(n)}$, можно той же формулой ввести классы эквивалентности $Cl^{(\alpha)}_{P,M}$ и для бесконечных кардинальных чисел α, а также отношение $<$ между ними.

Модуль P мы назовем *образующим*, если

$$\exists Cl^{\alpha}_{P,M} \forall V_1 \forall V_2 \forall X \forall Y (V_1 \oplus V_2 = V \wedge (X, Y) \in Cl^{\alpha}_{P,M} \Rightarrow V_1 \subset_\circ X \vee V_2 \subset_\circ X).$$

Эту формулу будем обозначать через $Gener(P)$.

Формула

$$Pret(P) := Proj(P) \wedge Gener(P) \wedge \exists M \subset P (M = \max(P))$$

выполняется для всех проективных образующих модулей, имеющих максимальные подмодули, в том числе она обязана выполняться для всех прообразующих модулей.

Формула

$$FDSum_{P,M}(X) := \exists Cl^{(n)}_{P,M} \exists Y (X, Y) \in Cl^{(n)}_{P,M} \wedge \\ \wedge \forall X', Y' (X', Y') \in Cl^{(n)}_{P,M} \Rightarrow (X, Y) \subset_\circ (X', Y')$$

выделяет для данного n модуль $Q \oplus P^{(n)}$ с подмодулем $Q \oplus M^{(n)}$ такой, что для любой пары $(Q' \oplus P^{(n)}, Q' \oplus M^{(n)})$ модуль $Q \oplus P^{(n)}$ выделяется в $Q' \oplus P^{(n)}$ прямым слагаемым и $Q' \oplus M^{(n)} \subset Q \oplus P^{(n)}$. Рассмотрим в качестве модулей $Q' \oplus P^{(n)}$ и $Q' \oplus M^{(n)}$ просто пару $(P^{(n)}, M^{(n)})$. Тогда $P^{(n)} \cong P^{(n)} \oplus Q$ и $M^{(n)} \cap P^{(n)} \oplus Q = M^{(n)} \oplus Q$.

Эта формула выделяет все модули вида $P^{(n)}$, $n \in \omega$ и еще какие-то *конечно порожденные* модули.

Любой проективный конечно порожденный модуль есть прямое слагаемое модуля $R^{(n)}$ для некоторого $n \in \omega$. Значит, если P — конечно порожденный проективный модуль, то для любого образующего модуля S

$$P \oplus Q \cong S^{(m)}$$

для некоторого $m \in \omega$ и некоторого модуля Q. Если же модуль P не является конечно порожденным, но проективен и является образующим, то он не может быть вложен в $R^{(n)}$ ни для какого $n \in \omega$.

Отсюда следует, что формула

$$Proobr(P) := Pret(P) \wedge \forall S (Pret(S) \Rightarrow \exists M \exists X (FDSum_{S,M}(X) \wedge P \subset_\circ X)))$$

выполняется на прообразующих модулях, и только на них.

Заметим, что выделив с помощью формулы $Proobr()$ некоторый фиксированный прообразующий модуль P, мы имеем также множество почти свободных модулей рангов $\leqslant \varkappa$ над кольцом R.

4.4.2 Кольцо $End_R P$

В этом пункте мы будем считать, что имеем фиксированный прообразующий модуль P.

Пусть P_1, P_2 и P_3 — три попарно непересекающихся модуля, каждый из который изоморфен модулю P.

Модуль $U_{1,2}$ определим формулой

$$U_{1,2} \subset P_1 \oplus P_2 \wedge P_1 \subset U_{1,2} \oplus V_2 \wedge V_2 \subset U_{1,2} \oplus V_1.$$

Как мы уже знаем, в этом случае модуль $U_{1,2}$ состоит из сумм $e + f(e)$, где $e \in P_1$, $f : P_1 \to P_2$ — изоморфизм между модулями P_1 и P_2. Ясно, что можно считать, что изоморфизм f совпадает с изоморфизмом, отождествляющим модули P_1 и P_2, т. е. модуль $U_{1,2}$ состоит из векторов $f_1(e) + f_2(e)$, где $f_1 : P \to P_1$, $f_2 : P \to P_2$ — изоморфизмы, отождествляющие модули P, P_1 и P_2.

Аналогично введем модуль $U_{2,3}$, состоящий из векторов вида $f_2(e) + f_3(e)$.

Модуль $U_{1,2,3}$ введем формулой

$$U_{1,2,3} := (P_1 \oplus U_{2,3}) \cap (P_3 \oplus U_{1,2}).$$

Тогда если $v \in U_{1,2,3}$, то $v \in P_1 \oplus U_{2,3}$, т. е.

$$v = f_1(e) + f_2(e') + f_3(e'),$$

а из $v \in P_3 \oplus U_{1,2}$ следует

$$v = f_1(g) + f_2(g) + f_3(g').$$

Значит,

$$f_1(e) + f_2(e') + f_3(e') = f_1(g) + f_2(g) + f_3(g'),$$

откуда следует, что

$$v = f_1(e) + f_2(e) + f_3(e).$$

Модуль $U_{1,3}$ вводится формулой $(P_1 \oplus P_3) \cap (U_{1,2,3} \oplus P_2)$.

Таким образом, мы имеем модули, порожденные элементами $f_1(e) = e_1$, $f_2(e) = e_2$, $f_3(e) = e_3$, $f_1(e) + f_2(e) = e_1 + e_2$, $f_2(e) + f_3(e) = e_1 + e_3$, $f_1(e) + f_2(e) + f_3(e) = e_1 + e_2 + e_3$ при $e \in P$.

Введем теперь множество модулей V_q^3 формулой

$$V_q^3 \subset U_{1,2} \oplus P_3 \wedge U_{1,2} \subset V_q^3 \oplus P_3.$$

Так как $V_q^3 \subset U_{1,2} \oplus P_3$, то из $v \in V_q$ следует

$$v = f_1(e) + f_2(e) + f_3(e').$$

Из того, что $U_{1,2} \subset V_q \oplus P_3$ следует, что для любого $e \in P$ существует $v = f_1(e) + f_2(e) + f_3(e')$.

Для каждого $e \in P$ существует и единственно $e' \in P$ такое, что $f_1(e) + f_2(e) + f_3(e') \in V_q^3$.

Легко увидеть, что соответствие, сопоставляющее элементу e элемент e', является гомоморфизмом модуля P в себя, который мы будем обозначать через q. Для каждого модуля V_q^3 через $W_q^{1,3}$ обозначим модуль, определенный формулой

$$W_q^{1,3} \subset (P_1 \oplus P_3) \cap (V_q^3 \oplus P_2) \wedge P_1 \subset W_q^{1,3} \oplus P_3.$$

Если $w \in W_q^{1,3}$, то из $w \in P_1 \oplus P_3$ следует, что $w = f_1(e) + f_3(e')$, а из $w \in V_q^3 \oplus P_2$ следует, что

$$w = f_1(e'') + f_2(e'') + f_3(qe'') + f_2(e''').$$

Отсюда видно, что $w = f_1(e) + f_3(qe)$.

Совершенно аналогично вводится модуль $W_q^{2,3}$, состоящий из векторов

$$w = f_2(e) + f_3(qe).$$

Для данных V_q^3 и V_r^3 рассмотрим модуль V, определенный формулой

$$V := (U_{1,2} \oplus P_3) \cap (W_q^{1,3} \oplus W_r^{2,3}).$$

Если $v \in V$, то, с одной стороны,

$$v = f_1(e) + f_2(e) + f_3(e'),$$

с другой стороны,

$$v = f_1(e'') + f_3(qe'') + f_2(e''') + f_3(re''').$$

Мы видим, что $E'' = e''' = e$, т. е.

$$v = f_1(e) + f_2(e) + f_3(qe) + f_3(re) = f_1(e) + f_2(e) + f_3((q+r)e),$$

откуда следует, что

$$V = V_{q+r}^3.$$

Таким образом, на множестве модулей $\{V_q \mid q \in End_R P\}$ мы имеем операцию сложения $\langle V_q, V_r\rangle \mapsto V_{q+r}$. Очевидно, что в этом случае мы также имеем операцию взятия противоположного элемента

$$V_q \mapsto V_{-q}.$$

Через $X_q^{2,3}$ обозначим модуль

$$(W_q^{2,3} \oplus P_2) \cap U_{2,3}.$$

Он состоит из векторов вида

$$f_2(qe) + f_3(qe), \quad e \in P.$$

Теперь рассмотрим модуль W, задаваемый формулой

$$W \subset P_2 \oplus P_3 \wedge P_3 \subset P_2 \oplus W \wedge X_q^{2,3} = (((W \oplus P_3) \cap P_2) \oplus ((W_q^{2,3} \oplus P_2) \cap P_3)) \cap U_{2,3}.$$

Легко увидеть, что такой модуль состоит из векторов вида

$$f_3(e) + f_2(qe).$$

Будем обозначать его через $W_q^{3,2}$.

Модуль

$$(W_q^{3,2} \oplus P_1) \cap (U_{1,3} \oplus P_2)$$

будем обозначать через V_q^2. Он состоит из векторов вида

$$f_1(e) + f_2(qe) + f_3(e).$$

Модуль $V_q^2 \oplus P_3 \cap P_1 \oplus P_2$ обозначается через $W_q^{1,2}$ и состоит из векторов вида $f_1(e) + f_2(qe)$.

Если нам дан модуль $W_q^{1,2}$, то формулой

$$(W_{q'}^{1,2} \oplus W_q^{1,3}) \cap U_{2,3} = X_q^{2,3}$$

мы получим $q' = q$, т. е. имея модуль $W_q^{1,2}$ мы автоматически имеем модуль $W_q^{1,3}$, а значит, и V_q^3.

Теперь, написав формулу

$$W_s^{1,2} = (W_q^{3,2} \oplus W_{-r}^{1,3}) \cap (P_1 \oplus P_2),$$

мы получим для $w \in W_s^{1,2}$

$$w = f_1(e) + f_3(-re) + f_3(e') + f_2(qe) = f_1(e'') + f_2(e'').$$

Отсюда следует, что

$$f_3(-re) + f_3(e') = 0,$$

т. е. $e' = re$, откуда

$$w = f_1(e) + f_2(qre),$$

т. е. $s = qr$.

Таким образом, по модулям V_r^3 и V_q^3 мы умеем строить модуль V_{qr}^3, т. е. на множестве $\{V_q^3 \mid q \in \operatorname{End}_R P\}$ мы ввели операции сложения и умножения так, что оно стало изоморфно кольцу $\operatorname{End}_R P$.

4.4.3 Построение кольца $\operatorname{End}_R V$

Для данного прообразующего модуля P выделим в модуле V два непересекающихся подмодуля V_1 и V_2 из одного класса эквивалентности $Cl^{\alpha}_{P,M}$, максимального среди всех других $Cl^{\beta}_{P,M}$. Очевидно, что в этом случае $\alpha = \varkappa$. Пусть, кроме того, $V_1 \oplus V_2 \oplus P = V$.

Пусть $V_1 = Q_1 \oplus \sum\limits_{i \in \varkappa} P_i$, $V_2 = Q_2 \oplus \sum\limits_{i \in \varkappa} P_i'$, где для любого $i \in \varkappa$

$$P_i \cong P_i' \cong P.$$

Зафиксируем изоморфизмы

$$f_i : P \to P_i,$$
$$f_i' : P \to P_i'.$$

Пусть формула $End(X)$ утверждает о модуле X следующее.

1. $\forall T(T \subset_\circ V_1 \wedge T \cong P \Rightarrow \exists T'(T' \subset_\circ V_2 \wedge T' \cong P \wedge \exists V_q^3(P,T,T') \subset_\circ X))$, т. е. для каждого прямого слагаемого P_i модуля V_1 Существует прямое слагаемое P' (линейная комбинация каких-то P_i') модуля V_2 такое, что для некоторого $q \in \operatorname{End}_R P$ модуль

$$\{e + f_i(e) + f'(qe) \mid e \in P\}$$

является прямым слагаемым модуля P.

2. $X \cap V_2 = 0$, откуда следует, что для каждого прямого слагаемого P_i модуля V_1 существует лишь единственное прямое слагаемое P' модуля V_2 такое, что модуль

$$\{e + f_i(e) + f'(qe) \mid e \in P\}$$

является прямым слагаемым модуля X для некоторого $q \in \operatorname{End}_R P$.

3. $X \cap P = 0$.

Такой модуль следующим образом представляет эндоморфизм модуля $P^{(\varkappa)}$ над кольцом $End_R P$.

Для любого вектора $v \in P^{(\varkappa)}$ существует P' — прямое слагаемое модуля $P^{(\varkappa)}$, изоморфное P и такое, что $v \in P'$. По условию 1) в модуле V_2 существует прямое слагаемое P'', а также эндоморфизм $q \in End_R P$ такие, что $V_q^3(P, P', P'') \subset X$. Тогда в модуле V_q^3 содержится единственный элемент

$$(f')^{-1}(v) + v + f''(q(f')^{-1}(v)).$$

Будем считать $X(v) := f''(q(f')^{-1}(v))$. Покажем, что полученное отображение корректно определено и линейно.

Действительно, однозначность разложения следует из условия 2). Проверим линейность.

Если $v_1, v_2 \in P_i$ для некоторого $i \in \varkappa$, то для любых $q_1, q_2 \in R$ условие $X(q_1v_1 + q_2v_2) = q_1X(v_1) + q_2X(v_2)$ следует из линейности соответствующего эндоморфизма q:

$$\begin{aligned}
V_q^3(P, P_i, P') \subset X \Rightarrow\Rightarrow &\begin{cases} f_i^{-1}(v_1) + v_1 + f'(qf_i^{-1}(v_1)) \in X, \\ f_i^{-1}(v_2) + v_2 + f'(qf_i^{-1}(v_2)) \in X \end{cases} \Rightarrow \\
\Rightarrow &\begin{cases} q_1f_i^{-1}(v_1) + q_1v_1 + q_1f'(qf_i^{-1}(v_1)) \in X, \\ q_2f_i^{-1}(v_2) + q_2v_2 + q_2f'(qf_i^{-1}(v_2)) \in X \end{cases} \Rightarrow \\
\Rightarrow q_1f_i^{-1}(v_1) + q_2f_i^{-1}(v_2) + q_1v_1 + q_2v_2 &+ q_1f'(qf_i^{-1}(v_1)) + q_2f'(qf_i^{-1}(v_2)) \in X \Rightarrow \\
\Rightarrow f_i^{-1}(q_1v_1 + q_2v_2) + (q_1v_1 + q_2v_2) &+ f'(q_1q(f_i^{-1}(v_1)) + q_1q(f_i^{-1}(v_2))) \in X,
\end{aligned}$$

т. е.

$$X(q_1v_1 + q_2v_2) = q_1X(v_1) + q_2X(v_2).$$

Два модуля X_1 и X_2, удовлетворяющие формуле $End(X)$, будем считать *эквивалентными*, если
$$\forall T \subset_\circ V_1 \forall S \subset_\circ V_2 (V_q^3(P,T,S) \subset X_1 \Leftrightarrow V_q^3(P,T,S) \subset X_2).$$
Видно, что в каждом классе эквивалентности существует модуль вида
$$\sum_{i \in \varkappa} V_{q_i}^3(P, P_i, T_i),$$
где T_i — тот единственный модуль для P_i, при котором
$$V_{q_i}^3(P, P_i, T_i) \subset X.$$

Рассмотрим некоторый модуль X_0, удовлетворяющий формуле $End(X)$ и такой, что $X_0 \subset P \oplus V_1$. Очевидно, что модулю X_0 соответствует нулевой эндоморфизм модуля V_1. Мы будем теперь рассматривать только модули X, удовлетворяющие формуле
$$End^{X_0}(X) := End(X) \wedge X \subset X_0 \oplus V_2.$$
Теперь определим сумму двух модулей X_1 и X_2, удовлетворяющих формуле $End^{X_0}(X)$.
$$\begin{aligned}(X = X_1 + X_2) := \forall T \subset_\circ V_1 \forall V_q^3(P,T,S_1) \subset_\circ X_1 \forall V_r^3(P,T,S_r) \subset_\circ X_2 \\ (X_0 \oplus V_2) \cap (W_q^{1,3}(V_q^3(P,T,S_q)) \oplus W_r^{2,3}(V_r(P,T,S_r))) \subset_\circ X.\end{aligned}$$
Легко увидеть (ср. с п. 4.2), что модуль X удовлетворяющий формуле $X = X_1 + X_2$, является суммой эндоморфизмов X_1 и X_2.

Теперь введем некоторый модуль X_e, удовлетворяющий формуле $End_{X_0}(X)$ и такой, что
$$\begin{aligned}X_e \cap X_0 = 0 \wedge \forall S \subset_\circ V_2 (S \cong P \Rightarrow \exists T \subset_\circ V_1 (\exists V_q(P,T,S) \subset X_e \wedge \\ \wedge V_q^3(P,T,S) \text{ — изоморфизм между } T \text{ и } S)).\end{aligned}$$
Очевидно, что такой модуль X_e осуществляет изоморфизм между модулями V_1 и V_2. Таким образом, X_e станет единицей кольца $End_R V$.

Теперь рассмотрим три модуля X_1, X_2 и X, удовлетворяющих формуле $End^{X_0}(X)$. Нам нужно определить формулу $X = X_1 \circ X_2$. Опишем эту формулу словами, чтобы проще было понять ее суть.

Пусть $V_q^3(P,T,S_q) \subset_\circ X_1$ для некоторых $T \subset_\circ V_1$, $S_q \subset_\circ V_2$. Как мы уже говорили, для каждой суммы $v + f_T(v) + f_{S_q}(qv)$ мы считаем, что X_1 переводит вектор $f_T(v) \in T \subset V_1$ в вектор $f_{S_q}(qv) \in S_q \subset V_2$.

Для данного $S_q \subset_\circ V_2$ существует и единственно T_q такое, что $V_e(P,T_q,S_q) \subset_\circ X_e$. Для произвольного вектора $v \in P$ если $v + f_{T_q}(v) + f_{S_q}(v) \in V_e(P,T_q,S_q)$, то векторы $f_{T_q}(v)$ и $f_{S_q}(v)$ совпадают при отождествлении V_1 и V_2, т. е. X_1 переводит $f_T(v)$ в $f_{T_q}(qv)$.

Далее, для данного $T_q \subset_\circ V_1$ существует и единственно $S_{rq} \subset_\circ V_2$ такое, что
$$V_r(P, T_q, S_{rq}) \subset_\circ X_2.$$

Если
$$v + f_{T_q}(v) + f_{S_{rq}}(rv) \in V_r(P, T_q, S_{rq}),$$
то отображение X_2 переводит вектор $f_{T_q}(v) \in T_q \subset V_1$ в вектор $f_{S_{rq}}(rv)$, т. е. композиция X_2X_1 переводит вектор $f_T(v)$ в вектор $f_{S_{rq}}(zqv)$, т. е. отображение X тогда и только тогда является композицией отображений X_1 и X_2, когда для всякого $T \subset_\circ V_1$
$$V_3(P, T, S_{rq}) \subset_\circ X,$$
при этом $V_s(P, T, S_{rq})$ состоит из векторов вида
$$v + f_T(v) + f_{S_{rq}}(rqv).$$
Можно легко убедиться, что это выполнено формула
$$(V_q(P, T, S_q) \oplus V_e(P, T_q, S_q)) \cap X_0 = (V_r(P, T_q, S_{rq}) \oplus V_s(P, T, S_q)) \cap X_0,$$
откуда получим формулу, эквивалентную
$$X = X_2 \circ X_1.$$
Таким образом, мы в решетке подмодулей модуля V интерпретировали кольцо, изоморфное кольцу $\mathrm{End}_{\,\mathrm{End}_{\,R}P}V$, откуда, как и выше, получаем, что если две решетки подмодулей $P(R_1, V_1)$ и $P(R_2, V_2)$ элементарно эквивалентны, то и кольца $\mathrm{End}_{\,\mathrm{End}_{\,R_1}P_1}(V_1)$ и $\mathrm{End}_{\,\mathrm{End}_{\,R_2}P_2}(V_2)$ для некоторых прообразующих модулей P_1 и P_2 элементарно эквивалентны, а значит, кольца $\mathrm{End}_{\,R_1}V_1$ и $\mathrm{End}_{\,R_2}V_1$ элементарно эквивалентны. Таким образом, мы доказали следующую теорему.

Теорема 4.14. *Для свободных модулей V_1 и V_2 бесконечных рангов над произвольными кольцами R_1 и R_2 соответственно из элементарной эквивалентности решеток подмодулей $P(V_1)$ и $P(V_2)$ следует элементарная эквивалентность колец эндоморфизмов $\mathrm{End}_{\,R_1}(V_1)$ и $\mathrm{End}_{\,R_2}(V_2)$.*

4.4.4 Обратная теорема

Теперь нам требуется доказать обратную теорему.

Теорема 4.15. *Предположим, что V_1 и V_2 — свободные модули бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над кольцами R_1 и R_2 соответственно, и каждый подмодуль модуля V_1 (V_2) имеет не более $\varkappa_1$ ($\varkappa_2$) порождающих элементов (например, это так, если $\varkappa_1 \geqslant |R_1|$ и $\varkappa_2 \geqslant R_2$ или если R_1, R_2 — полупростые кольца или кольца главных идеалов). Тогда из*
$$\mathrm{End}_{\,R_1}(V_1) \equiv \mathrm{End}_{\,R_2}(V_2)$$
следует
$$P(V_1) \equiv P(V_2).$$

Доказательство. Предположим, что мы имеем ассоциативное кольцо R с единицей, бесконечное кардинальное число $\varkappa$ и свободный модуль $V = V_\varkappa^R$ ранга $\varkappa$ над R.

Кроме того, пусть каждый идеал кольца R порождается не более, чем $\varkappa$ элементами кольца.

Мы хотим интерпретировать в кольце $\mathrm{End}_R V$ решетку $P(V)$, состоящую их всех подмодулей модуля V, с отношением $\subset$. Как и раньше, под словом "интерпретировать" мы понимаем, что существует алгоритм, переводящий каждую формулу φ языка проективной геометрии в формулу $\widetilde{\varphi}$ языка теории колец таким образом, что формула φ истинна в $P(V)$ тогда и только тогда, когда $\widetilde{\varphi}$ истинна в $\mathrm{End}_R(V)$.

Чтобы не писать снова множество формул, дадим только неформальное описание перевода.

1. Мы знаем, что каждый объект геометрии $P(V)$ — это подмодуль модуля V, а он порожден не более чем $\varkappa$ векторами из модуля V. Каждый из этих векторов является линейной комбинацией некоторого конечного числа элементов базиса модуля V, т. е. каждый такой вектор можно записать в виде столбца матрицы, у которого лишь конечное число элементов ненулевое. Записав в матрицу все порождающие векторы, мы получим матрицу размера $\varkappa \times \varkappa$, то есть элемент из $\mathrm{End}_R V$. В случае, когда подмодуль порождается менее чем $\varkappa$ векторами, дополним матрицу необходимым количеством нулевых столбцов. Две такие матрицы X_1 и X_2 описывают один и тот же подмодуль модуля V, если

$$\exists A \exists B (X_1 = X_2 A \wedge X_2 = X_1 B).$$

В этом случае элементы X_1 и X_2 будем считать эквивалентными.

Таким образом, каждому подмодулю модуля V мы сопоставим соответствующий ему класс эквивалентности элементов кольца $\mathrm{End}_R V$.

2. Очевидно, что модуль Y_1, порожденный матрицей X_1, является подмодулем модуля Y_2, порожденного матрицей X_2 тогда и только тогда, когда

$$\exists A (X_1 = X_2 A).$$

Эту формулу будем обозначать через $X_1 \subset X_2$.

Из всего этого очевидно следует утверждение теоремы. □

4.5 Элементарная эквивалентность групп автоморфизмов модулей бесконечных рангов

4.5.1 Изоморфизм групп $\mathrm{Aut}_{\mathbf{R}}(\mathbf{V})$

В этом пункте мы будем основываться на работе [15] И.З. Голубчика и А. В. Михалева.

Рассмотрим некоторое кольцо R и свободный модуль $V (= V_\varkappa^R)$ над этим кольцом бесконечного ранга $\varkappa$.

Пусть $I_\varkappa$ — множество мощности $\varkappa$.

Как и раньше, через $\mathrm{End}_R(V)$ мы будем обозначать кольцо эндоморфизмов модуля V, а через $\mathrm{Aut}_R(V)$ — группу автоморфизмов модуля V.

Пусть, кроме того, $E_R(V)$ — группа, порожденная автоморфизмами $E_{\gamma\beta}$ вида

$$v_\gamma \mapsto n_\gamma + rv_\beta, \quad \gamma, \beta \in I_\varkappa, \gamma \neq \beta, \ r \in R$$

и

$$v_\alpha \mapsto v_\alpha, \quad \alpha \in I_\varkappa, \alpha \neq \gamma,$$

где $\{v_\alpha\}$ — базис модуля V; $D_R(V)$ — диагональная группа (автоморфизмы вида $v_\gamma \mapsto r_\gamma v_\gamma$ $\forall \gamma \in I_\varkappa$); $DE_R(V)$ — подгруппа, порожденная $E_R(V)$ и $D_R(V)$.

Подмножество $\{e_{ij}\}_{i,j\in I_\varkappa}$ кольца $\mathrm{End}_R(V)$ называется *системой матричных единиц*, если

1) $e_{ij} \circ e_{st} = \delta_{js} e_{it}$ (δ_{js} — дельта Кронекера);

2) для любого $a \in \mathrm{End}_R(V)$ и любого $k \in I$ существуют $i_1, \ldots, i_n \in I$ такие, что $(e_{i_1 i_1} + \cdots + e_{i_n i_n})a = a(e_{i_1 i_1} + \cdots + e_{i_n i_n}) = a$.

Пусть I — идеал кольца R; $E_R(V, I)$ — подгруппа группы $\mathrm{Aut}_R(V)$, порожденная автоморфизмами $1 + e_{ij} \circ \lambda$, где $\lambda \in I$, $i \neq j \in I_\varkappa$, $\mathrm{Aut}_R(V, I)$ — ядро канонического гомоморфизма $\varphi_I : \mathrm{Aut}_R(V) \to \mathrm{Aut}_{R/I}(V)$, $C_R(V, I)$ прообраз центра при гомоморфизме φ_I. Пусть, кроме того, $[A, B] \equiv A^{-1} \circ B^{-1} \circ A \circ B$.

Лемма 4.3. *Пусть R — ассоциативное кольцо с $1/2$, N и M — нормальные подгруппы группы $\mathrm{Aut}_R(V)$ такие, что $N \cap M = \{1\}$, $NM = \mathrm{Aut}_R(V)$. Тогда существуют идеалы I, J кольца R, для которых*

$$R = I \oplus J, \ E_R(V, I) \subseteq N \subseteq C_R(V, I), \ E_R(V, J) \subseteq M \subseteq C_R(V, J).$$

Доказательство. По условию

$$(1 - 2e_{ii}) = a_i \circ b_i, \quad a_i \in N, b_i \in M \tag{4.1}$$

для всех $i \in I_\varkappa$. Так как $N \cap M = \{1\}$ и $[1 - 2e_{11}, 1 - 2e_{ii}] = 1$, то $[a_1, 1 - 2e_{ii}] = 1$. Поскольку $1/2 \in R$, то элемент a_1 диагонален в том смысле, что $e_{ii} \circ a_1 \circ e_{jj} = 0$ для всех $i \neq j \in I_\varkappa$. То же самое верно и для b_1. Пусть $\forall i \in I_\varkappa$

$$e_{ii} \circ a_1 \circ e_{ii} = \lambda_i, \quad e_{ii} \circ b_1 \circ e_{ii} = \mu_i. \tag{4.2}$$

Из (4.2) следует, что

$$a_1 \circ (1 - e_{12}) \circ a_1^{-1} \circ (1 + e_{12}) = 1 + (1 - \lambda_1 \lambda_2^{-1}) \circ e_{12} \in N.$$

Так как $[1 + \lambda e_{12}, 1 + re_{2k}] = 1 + \lambda r e_{1k}$ для всех $\lambda, r \in R$ и $k \in I_\varkappa$, то из нормальности группы N следует, что $E_R(V, I) \subseteq N$, где $I = R(\lambda_1 - \lambda_2)R$, Аналогично, $E_R(V, J) \subseteq M$, где $J = R(\mu_1 - \mu_2)R$. Из (4.1) и (4.2) вытекает, что

$$\lambda_1 \mu_1 = -1, \ \lambda_2 \mu_2 = 1, \ \mu_1 = -\lambda_1^{-1}, \ \mu_2 = \lambda_2^{-1}.$$

По определению идеалов I и J

$$1-\lambda_1\lambda_2^{-1}\in I,\ 1-\mu_1\mu_2^{-1}=1+\lambda_1^{-1}\lambda_2\in J$$

и

$$\lambda_1(1+\lambda_1^{-1}\lambda_2)\lambda_2^{-1}=1+\lambda_1\lambda_2^{-1}\in J.$$

Следовательно, $1=1/2(1-\lambda_1\lambda_2^{-1}+1+\lambda_1\lambda_2^{-1})\in I+J$ и $R=I+J$. Кроме того, $E_R(V,I\cap J)\subseteq N\cap M=\{1\}$, и, значит $I\cap J=\{0\}$. Тем самым $I\oplus J=R$.

Если $a\in N$, то $a=a_1\circ a_2$, где $a_1\in\operatorname{Aut}_R(V,I)$, $a_2\in\operatorname{Aut}_R(V,J)$. При этом $[a,E_R(V,J)]\subseteq N\cap M=\{1\}$. Следовательно, a_2 — центральный идемпотент группы $\operatorname{Aut}_R(V,J)$ и $N\subseteq C_R(V,I)$. Аналогично, $M\subseteq C_R(V,J)$. □

Следующая лемма является основной в доказательстве.

Лемма 4.4. *Пусть R,S — ассоциативные кольца с $1/2$, $I_1=I_\varkappa, I_2=I_{\varkappa'}$ — бесконечные множества мощностей $\varkappa$ и $\varkappa'$ соответственно, $V=V_{I_1}^R$ и $V'=V_{I_2}^S$ — свободные модули над кольцами R и S и множествами I_1 и I_2 соответственно, $\{e_{ij}\}_{i,j\in I_\varkappa}$ — система матричных единиц кольца $\operatorname{End}_R(V)$, $\varphi:\operatorname{Aut}_R(V)\to\operatorname{Aut}_S(V')$ — изоморфизм групп. Тогда существует центральный идемпотент $q\in\operatorname{End}_S(V')$ и системы матричных единиц $\{f_{ij}\}_{i,j\in I_2}$, $\{h_{ij}\}_{i,j\in I_2}$ колец $q\circ\operatorname{End}_s(V')$ и $(1-q)\circ\operatorname{End}_S(V')$ соответственно такие, что*

$$\varphi(1-2e_{ii})=(q-2f_{ii})-(1-q-2h_{ii}),\quad i\in I_1.$$

Доказательство. Доказательство совершенно аналогично доказательству той же леммы работы [15]. □

Доказательство следующей теоремы является практически прямым выводом из доказательства основной теоремы работы [15].

Теорема 4.16. *Пусть R,S — ассоциативные кольца с $1/2$, $V=V_\varkappa^R$ и $V'=V_{\varkappa'}^S$ — свободно порожденные модули над R и S бесконечных рангов $\varkappa$ и $\varkappa'$ соответственно, $\varphi:\operatorname{Aut}_R(V)\to\operatorname{Aut}_S(V')$ — изоморфизм групп. Тогда существуют центральные идемпотенты e и f колец $\operatorname{End}_R(V)$ и $\operatorname{End}_S(V')$ соответственно, кольцевой изоморфизм $\theta_1:e\operatorname{End}_R(V)\to f\operatorname{End}_S(V')$, кольцевой антиизоморфизм $\theta_2:(1-e)\operatorname{End}_R(V)\to(1-f)\operatorname{End}_S(V')$ и групповой гомоморфизм $\chi:DE_R(V)\to C(\operatorname{Aut}_S(V'))$ такие, что $\varphi(A)=\chi(A)(\theta_1(A)+\theta_2(A^{-1}))$ для всех $A\in E_R(V)$.*

Доказательство. По лемме 4.4

$$\varphi(1-2e_{ii})=(q-2f_{ii})-(1-q-2h_{ii}),\tag{4.3}$$

где q — центральный идемпотент кольца $\operatorname{End}_S(V')$, e_{ij}, f_{ij}, h_{ij} — матричные единицы колец $\operatorname{End}_R(V)$, $q\operatorname{End}_S(V')$ и $(1-q)\operatorname{End}_S(V')$ соответственно.

Положим

$$f\equiv f_{11}+f_{22}+h_{11}+h_{22}.$$

1. Пусть $\{e'_{ij}\}_{i,j\in I_1}$ — некоторая система матричных единиц кольца $\mathrm{End}_R(V)$, причем $\forall i \neq 1,2$ $(e'_{ii}=e_{ii})$. Тогда

$$\varphi(1-2e'_{ii}) = q-(-q)+x, \text{ где } x\in f\,\mathrm{End}_S(V')f. \tag{4.4}$$

По условию $[1-2e'_{kk}, 1-2e'_{ii}]=1$ При $k=1,2$, $i\neq 1,2$. По (4.3), (4.4)

$$\varphi(1-2e'_{kk}) = 1-2e_k+c_k, \tag{4.5}$$

где $k=1,2$, $e_k\in f\,\mathrm{End}_S(V')f$, $c_k\in(1-f)\,\mathrm{End}_S(V')(1-f)$. Заметим, что

$$(1-2e'_{11})(1-2e'_{22}) = (1-2e_{11})(1-2e_{22}).$$

В силу равенств (4.3),(4.4), (4.5)

$$(f-2e_1)(f-2e_2) = -f$$

и

$$e_1+e_2=f,\ \ e_1e_2=0. \tag{4.6}$$

По лемме 4.4 существует центральный идемпотент q' кольца $\mathrm{End}_S(V')$ такой, что

$$(q'-2f'_{ii})-(1-q'-2h'_{ii}) = \varphi(1-2e'_{ii}).$$

Следовательно, для $k=1,2$ имеем

$$q'(1-\varphi(1-2e'_{kk}))(1-\varphi(1-2e'_{33}))=0, \tag{4.7}$$
$$(1-q')(1+\varphi(1-2e'_{kk}))(1+\varphi(1-2e'_{33}))=0. \tag{4.8}$$

Умножив (4.7) слева на $1-f$ и справа на q и использовав соотношения (4.3), (4.5), получим, что $q'c_k\cdot 2f_{33}=0$,

$$q'c_kf_{33}=0. \tag{4.9}$$

Умножив равенство (4.8) слева на f и справа на fg и использовав (4.3), (4.5), получим

$$(1-q')2(f-e_k)2fq=0.$$

В силу равенства (4.6) $f=e_1+e_2$. Итак, $(1-q')e_kq=0$ и $(1-q')fq=0$. Так как $f=f_{11}+f_{22}+h_{11}+h_{22}$, то $\mathrm{End}_S(V')f\,\mathrm{End}_S(V')=\mathrm{End}_S(V')$ и в силу равенства $(1-q')fq=0$

$$0=(1-q')q\,\mathrm{End}_S(V')f\,\mathrm{End}_S(V')=(1-q')q\,\mathrm{End}_S(V').$$

Таким образом,

$$(1-q')q=0. \tag{4.10}$$

Из (4.9), (4.10) вытекает, что

$$c_kf_{33}=c_kqf_{33}=q(q'c_kf_{33})+(1-q')qc_kf_{33}=0+0=0.$$

Аналогично, $c_k f_{ii} - 0$ для всех $i \in I_2$. В силу (4.5) $c_k \in (1-f)\operatorname{End}_S(V')(1-f)$ и $c_k q = c_k(1-f)q$, т. е.

$$c_k q = 0. \tag{4.11}$$

Умножив равенство (4.7) слева на f и справа на $(1-q)f$, получим

$$q' \cdot 2e_{kk} \cdot 2f(1-q) = 0.$$

Таким образом,

$$q'(1-q) = 0. \tag{4.12}$$

Из (4.11), (4.12) следует, что $q = q'$, а из (4.3), (4.5) и (4.8) — $(2 - 2e_k + c_k)2h_{33} = 0$.

Так как $e_k h_{33} = e_k f(1-f)h_{33} = 0$, то $2h_{33} + c_k h_{33} = 0$. Аналогично, $2h_{ii} + c_k h_{ii} = 0$ для всех $i \in I_2$. Следовательно, $c_k(1-q) = c_k(1-f)(1-q)$ и для любых $i, j \in I_2$ при $i \neq 1,2$ $c_k q \cdot h_{ij} = c_k h_{ij} = -2h_{ij}$ и для любых $j \in I_2$ $i = 1,2$ $c_k q \cdot h_{ij} = 0$. Тем самым показано, что

$$c_k(1-q) = -2(1-q) + 2(1-q)f. \tag{4.13}$$

Из (4.5), (4.11) и (4.13) следует $1 + c_k - q + (1-q) \in F\operatorname{End}_S(V')f$ и $\varphi(1-2e'_{kk}) - q + (1-q) \in f\operatorname{End}_S(V')f$ для $k = 1,2$.

2. Покажем, что в (4.3) матричные единицы можно выбрать так, чтобы

$$\varphi(1 - e_{ii} - e_{jj} + e_{ij} + e_{ji}) = (q - f_{ii} - f_{jj} + f_{ij} + f_{ji}) - (1 - q - h_{ii} - h_{jj} + h_{ij} + h_{ji}) \tag{4.14}$$

для всех $i, j \in I_1, i \neq j$.

Действительно, положим

$$e'_{11} = 1/2(e_{11} + e_{22} - e_{12} - e_{21}),\ e'_{22} = 1/2(e_{11} + e_{22} + e_{12} + e_{21}), e'_{ii} = e_{ii}\ \forall i \neq 1,2.$$

Систему $\{e'_{ii}\}$ можно дополнить до системы матричных единиц $\{e'_{ij}\}_{i,j\in I_1}$ кольца $\operatorname{End}_R(V)$. В силу п. 1

$$\varphi(1 - e_{11} - e_{22} + e_{12} + e_{21}) = \varphi(1 - 2e'_{11}) = q - (1-q) + x,$$

где $x \in f\operatorname{End}_S(V')f$ и f из (4.4). Следовательно,

$$\varphi(1 - e_{11} - e_{22} + e_{12} + e_{21}) = \begin{pmatrix} a_{11} & a_{12} & 0 & \vdots \\ a_{21} & a_{22} & 0 & \vdots \\ \multicolumn{2}{c}{\dots\dots\dots} & 1 & \vdots \\ \multicolumn{3}{c}{\dots\dots\dots\dots} & \ddots \end{pmatrix} - \begin{pmatrix} b_{11} & b_{12} & 0 & \vdots \\ b_{21} & b_{22} & 0 & \vdots \\ \multicolumn{2}{c}{\dots\dots\dots} & 1 & \vdots \\ \multicolumn{3}{c}{\dots\dots\dots\dots} & \ddots \end{pmatrix}, \tag{4.15}$$

где $a_{ij} \in f_{11}\operatorname{End}_S(V')f_{11}$, $b_{ij} \in h_{11}\operatorname{End}_S(V')h_{11}$. Так как

$$(1 - e_{11} - e_{22} + e_{12} + e_{21})(1 - 2e_{11}) = (1 - 2e_{22})(1 - e_{11} - e_{22} + e_{12} + e_{21}),$$

то из (4.3) и (4.15) получаем, что

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

$$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

и

$$a_{11} = a_{22} = 0, \quad b_{11} = b_{22} = 0. \tag{4.16}$$

Далее, $(1 - e_{11} - e_{22} + e_{12} + e_{21})^2 = 1$. В силу (4.15) и (4.16)

$$a_{21} = a_{12}^{-1}, \quad b_{21} = b_{12}^{-1}.$$

Аналогично,

$$\varphi(1 - e_{ii} + r_{i+1,i+1} + e_{i,i+1} + e_{i+1,i}) =$$
$$= (q - f_{ii} - f_{i+1,i+1} + a_i f_{ii+1} + a^{-1} f_{i+1,i}) = (1 - q - h_{i+1,i+1} - h_{ii} + b_i h_{i,i+1} + b^{-1} h_{i+1,i})$$

для всех $i \in I_1$.

Положим по трансфинитной индукции $c_1 \equiv 1$, $c_{i+1} \equiv c_i \cdot a_i^{-1}$, $c_i \equiv 1$ для предельного ординального числа i, аналогично, $d_1 \equiv 1$, $d_{i+1} \equiv d_i \cdot b_i^{-1}$, $b_i \equiv 1$ для предельного ординального числа i. Пусть, кроме того, $C \equiv \operatorname{diag}(c_1, \dots, c_n, \dots) + \operatorname{diag}(d_1, \dots, d_n, \dots)$, $h'_{ij} \equiv C h_{ij} C^{-}1$. Тогда $h'_{ii} = h_{ii}$, $f'_{ii} = f_{ii}$, $f'_{i,i+1} = a_i f_{i,i+1}$, $f_{i+1,i} = a_i^{-1} f_{i+1,i}$, $h'_{i,i+1} = b_1 h_{i,i+1}$, $h'_{i+1,i} = b_i^{-1} h_{i+1,i}$.

Тем самым

$$\varphi(1 - e_{ii} - e_{i+1,i+1} + e_{i,i+1} + e_{i+1,i}) =$$
$$= (q - f'_{ii} - f'_{i+1,i+1} + f'_{i,i+1} + f'_{i+1,i}) - (1 - q - h'_{ii} - h'_{i+1,i} + h'_{i,i+1} + h'_{i+1,i}).$$

Итак, пункт 2 доказан.

3. Положим $g_{ij} = f_{ij} + h_{ij}$, где f_{ij}, h_{ij} — матричные единицы, для которых выполнены условия (4.3), (4.14). Тогда $\{g_{ij}\}_{i,j \in \varkappa}$ — система матричных единиц кольца $\operatorname{End}_S(V')$. Произвольный элемент $C \in \operatorname{End}_S(V')$ будем записывать в виде

$$C \equiv \begin{pmatrix} c_{11} & \dots & c_{1n} & \vdots \\ \dots & \ddots & \dots & \vdots \\ c_{n1} & \dots & c_{nn} & \vdots \\ \dots & \dots & \dots & \ddots \end{pmatrix}, \quad \text{где } c_{ij} \in g_{ij} End_S(V') g_{ij}.$$

4. Покажем, что для любого элемента $r \in R$

$$\varphi(1 + r e_{12}) = \begin{pmatrix} a_r & b_r & 0 & \vdots \\ c_r & d_r & 0 & \vdots \\ \dots & \dots & 1 & \vdots \\ \dots & \dots & \dots & \ddots \end{pmatrix}, \tag{4.17}$$

где $a_r, b_r, c_r, d - r \in g_{11} \operatorname{End}_S(V') g_{11}$, и что

$$\varphi(1 - e_{ii} - e_{jj} + e_{ij} - e_{ji}) = 1 - g_{ii} - g_{jj} + g_{ij} i g_{ji} \tag{4.18}$$

для $i \neq j$.

Действительно,

$$1 - e_{ii} - e_{jj} + e_{ij} - e_{ji} = (1 - e_{ii} - e_{jj} + e_{ij} + e_{ji})(1 - 2e_{ii}).$$

В силу (4.3) и (4.14)

$$\begin{aligned}&\varphi(1 - e_{ii} - e_{jj} + e_{ij} - e_{ji}) = \\ &\qquad = (e - f_{ii} - f_{jj} + f_{ij} - f_{ji}) + (1 - e - h_{ii} - h_{jj} + h_{ij} - h_{ji}) = 1 - g_{ii} - g_{jj} + g_{ij} - g_{ji}.\end{aligned}$$

Положим

$$e''_{ij} = (1 + 1/2re_{12})e_{ij}(1 + 1/2re_{12})^{-1}.$$

Тогда в силу п. 1

$$\varphi(1 - 2e''_{11}) = q - (1 - q) + x,$$

и

$$x_1 \in f \operatorname{End}_S(V')f, \text{ где } f = h_{11} + h_{22} + f_{11} + f_{22}.$$

Далее,

$$1 - 2e''_{11} = 1 - 2e_{11} + re_{12} = (1 + re_{12})(1 - 2e_{11})$$

и по (4.3)

$$\varphi(1 + re_{12}) = \varphi((1 - 2e''_{11})(1 - 2e_{11})) = 1 + x_2,$$

где $x_2 \in f \operatorname{End}_S(V')f$.

Но из $f \operatorname{End}_S(V')f = (g_{11} + g_{22}) \operatorname{End}_S(V')(g_{11} + g_{22})$ следует

$$\varphi(1 + re_{12}) = \begin{pmatrix} a_r & b_r & 0 & \vdots \\ c_r & d_r & 0 & \vdots \\ \ldots\ldots & & 1 & \vdots \\ \ldots\ldots\ldots & & & \ddots \end{pmatrix}.$$

5. Используя равенства (4.17) и (4.18) и равенство

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & r & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & r \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

получим

$$\varphi(1 + re_{13}) = \begin{pmatrix} a_r & 0 & b_r & 0 & \vdots \\ 0 & 1 & 0 & 0 & \vdots \\ c_r & 0 & d_r & 0 & \vdots \\ 0 & 0 & 0 & 1 & \vdots \\ \ldots\ldots\ldots\ldots & & & & \ddots \end{pmatrix}, \tag{4.19}$$

где a_r, b_r, c_r, d_r взяты из (4.17).

Из (4.17) и (4.19) получаем, что для всех $r, s \in R$

$$\begin{pmatrix} a_r & b_r & 0 \\ c_r & d_r & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_s & 0 & b_s \\ 0 & 1 & 0 \\ c_s & 0 & d_s \end{pmatrix} = \begin{pmatrix} a_s & 0 & b_s \\ 0 & 1 & 0 \\ c_s & 0 & d_s \end{pmatrix} \begin{pmatrix} a_r & b_r & 0 \\ c_r & d_r & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

и

$$b_r = a_s b_r,\ c_r a_s = c_r,\ c_r b_s = 0. \tag{4.20}$$

Аналогично, используя равенства

$$\varphi(1 + re_{23}) = \begin{pmatrix} 1 & 0 & 0 & 0 & \vdots \\ 0 & a_r & b_r & 0 & \vdots \\ 0 & c_r & d_r & 0 & \vdots \\ 0 & 0 & 0 & 1 & \vdots \\ \ldots & \ldots & \ldots & \ldots & \ddots \end{pmatrix} \tag{4.21}$$

и $[(1 + se_{23}), (1 + re_{13})]$, получаем, что для всех $r, s \in R$

$$b_r = b_r d_s,\ d_s c_r = c_r,\ b_s c_r = 0. \tag{4.22}$$

Из равенств

$$(1 + re_{ij})^{-1} = (1 - re_{ij}) = (1 - 2e_{ii})(1 + r_{ij})(1 - 2e_{ii})$$

и (4.3), (4.17) следует, что для всех $r \in R$

$$\varphi(1 + re_{12})^{-1} = \begin{pmatrix} a_r & -b_r & 0 & \vdots \\ -c_r & d_r & 0 & \vdots \\ 0 & 0 & 1 & \vdots \\ \ldots & \ldots & \ldots & \ddots \end{pmatrix} \tag{4.23}$$

и в силу (4.23), (4.22)

$$a_r^2 = d_r^2 = 1. \tag{4.24}$$

Из равенств

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

и (4.17), (4.18) получаем

$$\varphi(1 - e_{21}) = \begin{pmatrix} d_1 & -c_1 & \vdots \\ -b_1 & a_1 & \vdots \\ \ldots & \ldots & \ddots \end{pmatrix}. \tag{4.25}$$

Далее,

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

Из (4.17), (4.25), (4.18) и (4.22) следует, что

$$a_1 d_1 - b_1^2 = -c_1, \tag{4.26}$$

$$-c_1^2 + d_1 a_1 = b_1 \tag{4.27}$$

Умножим равенство (4.27) справа на b_1 и, использовав (4.20), получим $b_1^2 = d_1 b_1$. Умножив (4.27) слева на b_1, получим $b_1^2 = b_1 a_1$. Тем самым показано, что $b_1 a_1 = d_1 b_1 = b_1^2$, $d_1 b_1 d_1 b_1 = d_1 b_1^2 = d_1^2 b_1 = b_1$, $d_1 b_1 d_1 b_1 = d_1 b_1^2 a_1 = d_1^2 b_1 a_1 = b_1 a_1 b_1^2$ и $b_1 = b_1^2$.

Из (4.26) следует

$$a_1 c_1 = c_1 d_1 = c_1 = -c_1^2. \tag{4.28}$$

Из (4.27) и (4.28) получаем

$$d_1 a_1 = b_1 + c_1^2 = b_1 c_1.$$

Из (4.20) и (4.22) вытекает

$$b_1 c_1 = c_1 b_1 = 0.$$

Таким образом,

$$(d_1 a_1)^2 = b_1^2 + c_1^2 = b_1 - c_1 = d_1 a_1.$$

В силу (4.24) элемент $d_1 a_2$ обратим. Следовательно,

$$1 = d_1 a_1 = b_1 - c_1. \tag{4.29}$$

По (4.20), (4.22), (4.29) $b_s c_r = c_r b_s = 0$ и

$$b_r \in b_1 f_{11} \operatorname{End}_S(V') f_{11} b_1, \;\; c_r \in (1 - b_1) f_{11} \operatorname{End}_S(V') f_{11} (1 - b_1) \tag{4.30}$$

для всех $r, s \in R$. Далее, согласно (4.20),

$$(a_s - 1) b_1 = c_1 (a_s - 1) = 0.$$

По (4.29)

$$a_s - 1 = -b_1 (a_s - 1) c_1.$$

В силу (4.20), (4.22), (4.24)

$$b_1 c_1 = c_1 b_1 = 0, \;\; 1 = a_s^2 = (1 - b_1 a_s c_1)^2 = 1 - 2 b_1 a_s c_1,$$

и $a_s = 1$. Аналогично, $d_s = 1$. Итак,

$$a_r = d_r = 1 \tag{4.31}$$

для всех $r \in R$. Положим $e_1 = b_1 \cdot 1$, тогда e_1 — идемпотент кольца $\operatorname{End}_S(V')$. По (4.17), (4.30), (4.31)

$$e_1 \varphi(1 + r e_{12}) = \varphi(1 + r e_{12}) e_1 = e_1 + b_r g_{12},$$

$$[1 - 2e_1, \varphi(1 + r e_{12})] = 1.$$

Аналогично,
$$[1-2e_1, \varphi(1-e_{ii}-e_{jj}+e_{ij}-e_{ji})]=1.$$
Следовательно, матрица $\varphi^{-1}(1-2e_1)$ лежит в централизаторе группы $E_R(V)$ и является центральной матрицей. Таким образом, матрица $1-2e_1$ лежит в центре кольца $\mathrm{End}\,_S(V')$, e_1 — центральный идемпотент кольца $\mathrm{End}\,_S(V')$,
$$e_1 \,\mathrm{End}\,_S(V') \oplus (1-e_1)\,\mathrm{End}\,_S(V') = \mathrm{End}\,_S(V'). \tag{4.32}$$
Положим $\theta_3(r)\equiv b_r$, $\theta_4(r)\equiv -c_r$. Из равенств
$$[1+re_{12}, 1-se_{23}] = 1+(rs)e_{13},$$
$$[1+c_rg_{21}, 1-c_sg_{32}] = 1-(c_sc_r)g_{31}$$
и (4.17), (4.30), (4.31), (4.19), (4.21), (4.23) получаем
$$\begin{pmatrix} 1 & 0 & b_{rs} \\ 0 & 1 & 0 \\ c_{rs} & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & b_rb_s \\ 0 & 1 & 0 \\ -c_sc_r & 0 & 1 \end{pmatrix}$$
Следовательно, $\theta_3 : R \to b_1(f_{11}\,\mathrm{End}\,_S(V')f_{11})$ — гомоморфизм колец, $\theta_4 : R \to (1-b_1)(f_{11}\,\mathrm{End}\,_S(V')f_{11}$ — антигомоморфизм колец. Кроме того, по (4.17), (4.18), (4.31)
$$\varphi(1+re_{ij}) = 1+\theta_3(r)g_{ij}-\theta_4(r)g_{ji}. \tag{4.33}$$

Положим для каждого $a_{ij}e_{ij}\in \mathrm{End}\,_R(V)$
$$\theta_1(a)=\theta_3(a_{ij})g_{ij},$$
$$\theta_2(a)=\theta_4(a_{ij})g_{ji},$$
а для остальных элементов кольца $\mathrm{End}\,_R(V)$ продолжим эти гомоморфизмы естественным образом.Тогда $\theta_1 : \mathrm{End}\,_R(V) \to e_1\,\mathrm{End}\,_S(V')$ — гомоморфизм колец, $\theta_2 : \mathrm{End}\,_R(V) \to (1-e_1)\,\mathrm{End}\,_S(V')$ — антигомоморфизм колец и по (4.29), (4.33)
$$\varphi(A)=\theta_1(A)+\theta_2(A^{-1}) \tag{4.34}$$
для всех $A\in E_R(V)$. Пусть I, J — идеалы кольца S такие, что $\mathrm{End}\,_I(V')=e_1\,\mathrm{End}\,_S(V')$ и $\mathrm{End}\,_J(V')=(1-e_1)\,\mathrm{End}\,_S(V')$. В силу (4.32) $I\oplus J=S$. Положим $N_1\equiv\varphi^{-1}(\,\mathrm{Aut}\,_S(V',I))$, $M_1\equiv\varphi^{-1}(\,\mathrm{Aut}\,_S(V',J))$. По лемме 4.3
$$E_R(V,eR)\subseteq N_1,\ E_R(V,(1-e)R)\subseteq M_1,$$
где e — некоторый центральный идемпотент кольца $\mathrm{End}\,_R(V)$. Пусть $B\in E_R(V,eR)$. Тогда $\varphi(B)-1\in \mathrm{End}\,_I(V')=e_1\,\mathrm{End}\,_S(V')$.

По (4.34)
$$\varphi(B)-1=\theta_1(B-1)+\theta_2(B^{-1}-1)$$
и
$$\theta_1(B-1)\in e_2\,\mathrm{End}\,_S(V'),\ \theta_2(B^{-1}-1)\in(1-e_2)\,\mathrm{End}\,_S(V').$$

Следовательно, $\theta_2(B^{-1}-1)=0$ и $\mathrm{End}_{eR}(V)\subseteq ker\,\theta_2$. Аналогично, $\mathrm{End}_{(1-e)R}(V)\subseteq ker\,\theta_1$. Поскольку φ — изоморфизм групп, то по (4.34)

$$ker\,\theta_1\cap ker\,\theta_2=\{0\}.$$

Таким образом,

$$\mathrm{End}_{eR}(V)=ker\,\theta_2,\ \ \mathrm{End}_{(1-e)R}(V)=ker\,\theta_1$$

и

$$ker\,\theta_1\oplus ker\,\theta=\mathrm{End}_R(V).$$

Проведя аналогичные рассуждения для отображения φ^{-1}, получаем, что

$$Im\,\theta_1\oplus Im\,\theta_2=\mathrm{End}_S(V').$$

Положим

$$\varphi_1(B)=\varphi^{-1}(\theta_1(B)+\theta_2(B^{-1}))$$

для всех $B\in\mathrm{Aut}_R(V)$. Тогда φ_1 — автоморфизм группы $\mathrm{Aut}_R(V)$ и, по (4.34),

$$\varphi_1(A)=A \text{ для всех } A\in E_R(V).$$

Теорема доказана. $\square$

Предположим, что кольца R и S с $1/2$ не содержат центральных идемпотентов, отличных от 0 и 1. Тогда имеет место следующая теорема:

Теорема 4.17. *Группы* $\mathrm{Aut}_R(V)$ *и* $\mathrm{Aut}_S(V')$ *изоморфны тогда и только тогда, когда* $\mathrm{End}_R(V)\cong\mathrm{End}_S(V')$.

Доказательство. По теореме 4.16 любой изоморфизм φ групп $\mathrm{Aut}_R(V)$ и $\mathrm{Aut}_S(V')$ на группе $DE_R(V)$ совпадает с изоморфизмом $\chi(\cdot)(\theta_1(\cdot)+\theta_2(\cdot^{-1}))$, где $\chi(\cdot)$ — групповой гомоморфизм $DE_R(V)\to C(\mathrm{Aut}_S(V'))$, $\theta_1: e\,\mathrm{End}_R(V)\to f\,\mathrm{End}_S(V')$ — кольцевой изоморфизм, $\theta_2:(1-e)\,\mathrm{End}_R(V)\to(1-f)\,\mathrm{End}_S(V')$ — кольцевой антиизоморфизм, e,f — центральные идемпотенты колец $\mathrm{End}_R(V_1)$ и $M_S(V_2)$ соответственно. Так как кольца R и S не содержат центральных идемпотентов, отличных от 0 и 1, то кольца $\mathrm{End}_R(V)$ и $\mathrm{End}_S(V')$ также не содержат центральных идемпотентов, отличных от 0 и 1, то есть либо $e=f=1$, либо $e=f=0$.

1. Если $e=f=1$, то $\varphi(\cdot)$ на $DE_R(V)$ совпадает с изоморфизмом колец $\mathrm{End}_R(V)$ и $\mathrm{End}_S(V')$ вида $\chi(\cdot)\theta_1(\cdot)$, т.е. кольца $\mathrm{End}_R(V)$ и $\mathrm{End}_S(V')$ изоморфны.

2. Если $e=f=0$, то φ на $DE_R(V)$ совпадает с антиизоморфизмом $\chi(\cdot)\theta_2(\cdot^{-1})$, т.е. кольца $\mathrm{End}_R(V)$ и $\mathrm{End}_S(V')^{op}$ изоморфны.

Предположим, что это так. Рассмотрим в $\mathrm{End}_R(V)$ систему коммутирующих сопряженных ортогональных идемпотентов с условием

$$\sum_{i\in I}e_{ii}\sim 1.$$

(Это выражение означает, что для любого элемента a и любого $i \in I$ существуют $i_1, \ldots, i_n \in \varkappa$ такие, что
$$\left(\sum_{j=1}^{n} e_{i_j i_j}\right) a e_{ii} = a e_{ii} \left(\sum_{j=1}^{n} e_{i_j i_j}\right) = a e_{ii}.\Big)$$

Теперь, как и выше, введем *систему матричных единиц* e_{ij} $(i, j \in \varkappa)$ условием
$$e_{ij} e_{kl} = \delta_{jk} e_{il}.$$

Очевидно, что такой системе $\{e_{ij}\}$ в $\mathrm{End}_R(V)$ соответствует система $\{f_{ij}\}$ в $\mathrm{End}_S(V')$, определяемая условием
$$f_{ij} f_{kl} = \delta_{il} f_{kj}.$$

В $\mathrm{End}_R(V)$ существует элемент
$$x \sim \sum_{i \in I} e_{1i},$$
но в $\mathrm{End}_S(V_2)$ соответствующего элемента
$$y \sim \sum_{i \in I} f_{1i}$$
существовать не может.

Покажем это.

Пусть W_i — носитель идемпотента f_{ii}. Тогда
$$f_{1i}(W_1) = f_{ii} f_{1i}(W_1) \Rightarrow f_{1i}(W_1) \subset W_i.$$
Кроме того,
$$W_1 = f_{11}(W_1) = f_{i1} f_{1i}(W_1),$$
то есть f_{ij} переводит W_j в W_i, то есть существование элемента $f \sim \sum\limits_{i \in I} f_{1i}$ означало бы, что f переводило бы некоторый вектор w из W_1 в сумму бесконечного числа векторов $w_j \in W_j$, что невозможно.

Таким образом, соотношение
$$\mathrm{End}_R(V) \cong \mathrm{End}_S(V')^{op}$$
невозможно.

Обратная импликация очевидна. □

4.5.2 Элементарная эквивалентность групп автоморфизмов и колец эндоморфизмов модулей бесконечных рангов

Лемма 4.5. *Для любого ультрафильтра D*

$$\prod_D \mathrm{End}_R(V) \cong \mathrm{End}_{\prod\limits_D}(V).$$

Доказательство. По определению ультрапроизведения любой элемент $\prod\limits_D \mathrm{End}_R(V)$ есть функция (точнее, ее класс эквивалентности) $f : I \to \mathrm{End}_R(V)$, т. е. множество пар $\langle i, A\rangle$, где $i \in I$, $A \in \mathrm{End}_R(V)$, $\forall i \in I \exists! A \in \mathrm{End}_R(V)(\langle i, A\rangle \in f)$. Каждый элемент $A \in \mathrm{End}_R(V)$ — это отображение $a : \varkappa \times \varkappa \to R$ такое, что для любого $\alpha \in \varkappa$ существует лишь конечное число $\beta_j \in \varkappa$ таких, что $a(\langle \alpha, \beta_j\rangle) \neq 0$, т. е. каждый элемент $A \in \mathrm{End}_R(V)$ — это множество упорядоченных троек $\langle \alpha, \beta, r\rangle$, где $\alpha, \beta \in \varkappa$, $r \in R$, $\forall \alpha \forall \beta \exists! r \in R(\langle \alpha, \beta, r\rangle \in A)$. Таким образом, любой элемент ультрапроизведения $\prod\limits_D \mathrm{End}_R(V)$ — это множество f упорядоченных четверок $\langle i, \alpha, \beta, r\rangle$ с $i \in I, \alpha, \beta \in \varkappa, r \in R$ и условием $\forall i, \alpha, \beta \exists! r(\langle i, \alpha, \beta, r\rangle \in f)$, а иначе говоря — это функция $f : I \times \varkappa \times \varkappa \to R$ с единственным условием, что $\forall i \in I \forall \alpha \in \varkappa$ существует лишь конечное число $\beta_j \in \varkappa$ таких, что $f(i, \alpha, \beta_j) \neq 0$.

Две такие функции $f, g : I \times \varkappa \times \varkappa \to R$ будут равны, если и только если

$$\{i \in I \mid \forall \alpha, \beta \in \varkappa(f(i, \alpha, \beta) = g(i, \alpha, \beta))\} \in D.$$

Для трех функций $f, g, h : I \times \varkappa \times \varkappa \to R$ выполнено $h = f + g$, если и только если

$$\{i \in I | \forall \alpha, \beta \in \varkappa(h(i, \alpha, \beta) = f(i, \alpha, \beta) + g(i, \alpha, \beta))\} \in D.$$

Аналогично, для трех функций $f, g, h : I \times \varkappa \times \varkappa \to R$ выполнено $h = fg$, если и только если

$$\{i \in I | \forall \alpha, \beta \in \varkappa(h(i, \alpha, \beta) = \sum_{\gamma \in \varkappa} f(i, \alpha, \gamma) \cdot g(i, \gamma, \beta))\} \in D.$$

Понятно, что мы имеем право ставить знак суммы в этом выражении, потому что лишь конечное число элементов этой суммы отлично от нуля.

Теперь рассмотрим кольцо $\mathrm{End}_{\prod\limits_D}(V)$. Совершенно аналогично предыдущим рассуждениям получим, что элементами этого кольца являются отображения $f : \varkappa \times \varkappa \times I \to R$ с тем же самым условием конечности и совершенно аналогичными равенством, суммой и произведением. Таким образом, искомый изоморфизм получается естественным образом (с помощью естественного отображения $I \times (\varkappa \times \varkappa) \to (\varkappa \times \varkappa) \times I$). $\square$

Теорема 4.18. *Предположим, что кольца R, S содержат $1/2$ и не содержат центральных идемпотентов, отличных от 1 и 0. Тогда группы $\mathrm{Aut}_R(V)$ и $\mathrm{Aut}_S(V')$ элементарно эквивалентны в том и только том случае, когда кольца $\mathrm{End}_R(V)$ и $\mathrm{End}_S(V')$ элементарно эквивалентны.*

Доказательство. Пусть кольца $\mathrm{End}_R(V)$ и $\mathrm{End}_S(V')$ элементарно эквивавалентны.

Рассмотрим произвольное предложение φ в языке теории групп. С помощью предложения φ построим предложение φ' языка теории колец следующим образом: каждое знакосочетание вида $\forall x(\dots)$, входящее в предложение φ, заменим на знакосочетание $\forall x(\exists x'(xx' = x'x = 1) \Rightarrow (\dots)$, а каждое знакосочетание вида $\exists x(\dots)$ — на знакосочетание $\exists x(\exists x'(xx' =$

$x'x = 1) \wedge (\dots))$. Очевидно, что если предложение φ истинно в группе $Aut_R(V)$, то предложение φ' истинно в кольце $\mathrm{End}\,_R(V)$, а значит, благодаря элементарной эквивалентности колец $\mathrm{End}\,_R(V)$ и $\mathrm{End}\,_S(V')$, оно истинно и в кольце $\mathrm{End}\,_S(V')$, откуда следует истинность предложения φ в группе $\mathrm{Aut}\,_S(V')$. Таким образом, группы $\mathrm{Aut}\,_R(V)$ и $\mathrm{Aut}\,_S(V')$ элементарно эквивалентны.

Пусть операция $*$ в применении к некоторому кольцу A (A^*) — это взятие группы обратимых элементов этого кольца. Очевидно, что для любого ультрафильтра D $\prod\limits_D \mathrm{Aut}\,_R(V) = \prod\limits_D(\mathrm{End}\,_R(V))^* \cong (\prod\limits_D \mathrm{End}\,_R(V))^*$, т. е. что операции $*$ и $\prod\limits_D$ перестановочны друг с другом.

Пусть теперь элементарно эквивалентны группы $\mathrm{Aut}\,_R(V)$ и $\mathrm{Aut}\,_S(V')$. Тогда по теореме п. 1.4 существуют ультрастепени $G = \prod\limits_D \mathrm{Aut}\,_R(V)$ и $G' = \prod\limits_D \mathrm{Aut}\,_S(V')$ этих групп такие, что $G \cong G'$. Таким образом, $(\prod\limits_D \mathrm{End}\,_R(V))^* \cong (\prod\limits_D \mathrm{End}\,_S(V')^*$, а по лемме 4.5 $\mathrm{Aut}\,_{\prod_D R}(V) \cong \mathrm{Aut}\,_{\prod_D S}(V')$. По теореме 4.17 предыдущего пункта в этом случае $\mathrm{End}\,_{\prod_D R}(V) \cong \mathrm{End}\,_{\prod_D S}(V')$, а следовательно, по теореме об Изоморфизме $\mathrm{End}\,_R(V) \equiv \mathrm{End}\,_S(V')$. Теорема доказана. $\square$

Таким образом, в случае ассоциативных колец с $1/2$, не содержащих центральных идемпотентов, отличных от 0 и 1, мы можем вместо вопроса об элементарной эквивалентности общих линейных групп рассматривать вопрос об элементарной эквивалентности колец эндоморфизмов.

4.5.3 Основная теорема

В этом пункте будем считать, что кардинальное число $\varkappa_1$ таково, что существует максимальный идеал кольца R_1, порожденный не более чем $\varkappa_1$ элементами.

Из теоремы 4.13 § 3 и теоремы 4.18 очевидно следует

Теорема 4.19. *Предположим, что кольца R_1 и R_2 содержат $1/2$ и не содержат центральных идемпотентов, отличных от 1 и 0. Пусть, кроме того, V_1 и V_2 — свободные модули бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над кольцами R_1 и R_2 соответственно, и пусть существует предложение $\psi \in Th_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$, ложное во всех кольцах, подобных кольцу R_1 и имеющих другую теорию $Th_2^{\varkappa_1}$. Тогда группы $\mathrm{Aut}\,_{R_1}(V_1)$ и $\mathrm{Aut}\,_{R_2}(V_2)$ элементарно эквивалентны в том и только том случае, когда существует кольцо S, подобное кольцу R_2 и такое, что $Th_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle) = Th_2^{\varkappa_2}(\langle \varkappa_2, S\rangle)$.*

Следствие 4.1. *Для свободных модулей V_1 и V_2 бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над телами (коммутативными или локальными кольцами, не содержащими центральных идемпотентов, отличных от 1 или 0, областями целостности) F_1 и F_2, содержащими $1/2$, соответственно, группы $\mathrm{Aut}\,_{F_1}(V_1)$ и $\mathrm{Aut}\,_{F_2}(V_2)$ элементарно эквивалентны тогда и только тогда, когда $Th_2^{\varkappa_1}(\langle \varkappa_1, F_1\rangle) = Th_2^{\varkappa_2}(\langle \varkappa_2, F_2\rangle)$.*

Следствие 4.2. *Для свободных модулей V_1 и V_2 бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над артиновыми кольцами R_1 и R_2, не содержащими центральных идемпотентов, отличных от 0* *или* 1*, содержащими* $1/2$*, соответственно, группы* $\operatorname{Aut}_{R_1}(V_1)$ *и* $\operatorname{Aut}_{R_2}(V_2)$ *элементарно эквивалентны тогда и только тогда, когда существуют кольца* S_1 *и* S_2*, подобные кольцам* R_1 *и* R_2 *соответственно, такие, что* $Th_2^{\varkappa_1}(\langle \varkappa_1, S_1\rangle) = Th_2^{\varkappa_2}(\langle \varkappa_2, S_2\rangle)$*.*

4.6 Элементарная эквивалентность колец эндоморфизмов абелевых p-групп

4.6.1 Предварительные сведения об абелевых группах

Здесь мы приведем самые основные сведения об абелевых группах, которые понадобятся нам в дальнейшем.

Абелевы p-группы

Примарной группой или *p-группой* называется группа, порядки элементов которой являются степенями фиксированного простого числа p.

Если $a \in A$, то наибольшее неотрицательное целое число r, для которого уравнение $p^r x = a$ имеет решение $x \in A$, назовем *p-высотой* $h_p(a)$ элемента a. Если уравнение $p^r x = a$ имеет решение при любом r, то a называется элементом *бесконечной p-высоты*, $h_p(a) = \infty$.

Пусть p — простое число. Корни степени p из единицы, где $n \in \mathbb{N} \cup \{0\}$, образуют бесконечную мультипликативную группу; мы перейдем к аддитивной записи. Получится группа, называемая *квазициклической* или *группой типа* p^∞ ($\mathbb{Z}(p^\infty)$), которую можно определить следующим образом: она порождается элементами $c_1, c_2, \dots, c_n, \dots$, где $pc_1 = 0$, $pc_2 = c_1$, $\dots$, $pc_{n+1} = c_n$, $\dots$. Здесь $o(c_n) = p^n$ и всякий элемент из $\mathbb{Z}(p^\infty)$ кратен некоторому c_n. Очевидно, что все квазициклические группы, соответствующие одному и тому же простому числу p, изоморфны между собой.

Ранги абелевых групп

Система $\{a_1, \dots, a_k\}$ ненулевых элементов группы A называется *независимой*, если из равенства

$$n_1 a_1 + \dots + n_k a_k = 0 \quad (n_i \in \mathbb{Z})$$

всегда вытекает, что

$$n_1 a_1 = \dots = n_k a_k = 0.$$

Система элементов называется *зависимой*, если она не независима.

Бесконечная система $L = \{a_i\}_{i \in I}$ элементов группы A называется *независимой*, если в L всякая конечная подсистема независима. Независимая система M элементов группы A называется *максимальной*, если в A не существует независимой системы, строго содержащей M. *Рангом* $r(A)$ группы A называется мощность ее максимальной независимой системы, содержащей только элементы бесконечного порядка или порядка, равного степени простого числа.

Предложение 4.8. *Ранг $r(A)$ группы A является инвариантом этой группы.*

Теорема 4.20. ([144], [77]) *Ограниченная группа является прямой суммой циклических групп.*

Теорема 4.21. ([63]) *Любые два разложения группы в прямую сумму циклических групп бесконечного порядка и порядков, равных степеням простых чисел, изоморфны.*

Теорема 4.22. ([33]) *Подгруппы прямых сумм циклических групп сами являются прямыми суммами циклических групп.*

Делимые абелевы группы

Будем говорить, что элемент a группы A *делится* на натуральное число n $(n|a)$, если уравнение $nx = a$ $(a \in A)$ имеет решение в группе A. Группа D называется *делимой*, если $n|a$ для всех $a \in D$ и всех натуральных чисел n. Группы $\mathbb{Q}$, $\mathbb{Z}(p^\infty)$ служат примерами делимых групп.

Теорема 4.23. *Всякая делимая группа D является прямой суммой квазициклических групп и групп, изоморфных $\mathbb{Q}$. Мощности множеств компонент $\mathbb{Z}(p^\infty)$ (для каждого p) и $\mathbb{Q}$ составляют полную и независимую систему инвариантов группы D.*

Таким образом, всякая делимая p-группа D является прямой суммой групп $\mathbb{Z}(p^\infty)$. Мощность множества компонент $\mathbb{Z}(p^\infty)$ является единственным инвариантом группы D.

Теорема 4.24. ([63]) *Для группы D эквивалентны следующие условия*:
1) *D — делимая группа*;
2) *D служит прямым слагаемым для всякой содержащей ее группы.*

Сервантные подгруппы

Подгруппа G группы A называется *сервантной*, если уравнение $nx = g \in G$, имеющее решение во всей группе A, имеет решение и в G. Подгруппа G сервантна в группе A тогда и только тогда, когда
$$\forall n \in \mathbb{Z} \quad nG = G \cap nA.$$

Предложение 4.9. ([164]) *Предположим, что подгруппа B группы A является прямой суммой циклических групп одного и того же порядка p^k. Тогда эквивалентны следующие утверждения*:
1) *B — сервантная подгруппа группы A*;
2) *B — прямое слагаемое в A.*

Таким образом, всякий элемент порядка p и конечной высоты можно вложить в конечное циклическое прямое слагаемое группы.

Теорема 4.25. ([32]) *Всякая ограниченная сервантная подгруппа выделяется прямым слагаемым.*

Следствие 4.3. ([101]) *p-группу B группы A можно вложить в ограниченное прямое слагаемое группы A тогда и только тогда, когда высоты отличных от нуля элементов группы B (взятые в совокупности) ограничены.*

Следствие 4.4. *Элемент a, порядок которого — степень простого числа, принадлежит конечному прямому слагаемому группы тогда и только тогда, когда подгруппа $\langle a\rangle$ не содержит отличных от нуля элементов бесконечной высоты.*

Базисные подгруппы

Подгруппа B группы A называется *p-базисной*, если выполнены следующие три условия:

1) подгруппа B является прямой суммой циклических p-групп и бесконечных циклических групп;

2) B есть сервантная подгруппа группы A;

3) факторгруппа A/B является p-делимой группой.

Подгруппа B обладает базисом, который называется *p-базисом* группы A.

Всякая группа для любого простого числа p содержит p-базисные подгруппы ([104]).

Нам в дальнейшем будут важны p-группы и их p-базисные подгруппы. Если A есть p-группа и q — простое число, отличное от p, то группа A имеет лишь одну q-базисную подгруппу, равную 0. Поэтому в случае p-групп мы будем называть p-базисные подгруппы просто *базисными.*

Теорема 4.26. ([165]) *Подгруппа $B = \bigoplus\limits_{n=1}^{\infty} B_n$, где B_n — прямая сумма групп $\mathbb{Z}(p^n)$, служит базисной подгруппой для p-группы A тогда и только тогда, когда при любом целом $n > 0$ подгруппа $B_1 \oplus \dots \oplus B_n$ является максимальным p^n-ограниченным прямым слагаемым группы A.*

Теорема 4.27. (Бэр; Бойер [84]) *Предположим, что B — подгруппа p-группы A,*

$$B = B_1 \oplus B_2 \oplus \dots \oplus B_n \oplus \dots,$$

где

$$B_n \cong \bigoplus_{\mu_n} \mathbb{Z}(p^n).$$

Подгруппа B является базисной подгруппой группы A тогда и только тогда, когда

$$A = B_1 \oplus B_2 \oplus \dots \oplus B_n \oplus (B_n^* + p^n A),$$

где $n \in \mathbb{N}$,

$$B_n^* = B_{n+1} \oplus B_{n+2} \oplus \dots$$

Так как подгруппа B имеет базис, а факторгруппа A/B — прямая сумма групп, изоморфных группе $\mathbb{Z}(p^\infty)$ (т. е. A/B также имеет систему образующих, которую легко описать), то естественно объединить эти системы образующих и таким путем получить систему образующих группы A.

Запишем

$$B = \bigoplus_{i \in I} \langle a_i \rangle \text{ и } A/B = \bigoplus_{j \in J} C_j^*, \text{ где } C_j^* = \mathbb{Z}(p^\infty).$$

Если прямое слагаемое C_j^* порождается смежными классами $c_{j1}^*, \dots, c_{jn}^*, \dots$ по подгруппе B, для которых $pc_{j1}^* = 0$, $pc_{j,n+1}^* = c_{jn}^*$ $(n = 1, 2, \dots)$, то в группе A можно выбрать элементы $c_{jn} \in c_{jn}^*$ того же порядка, что и c_{jn}^*. Тогда получится следующая система соотношений:

$$pc_{j1} = 0, \ pc_{j,n+1} = c_{jn} = b_{jn} \quad (n \geqslant 1, b_{jn} \in B),$$

где элемент b_{jn} должен иметь порядок $\leqslant p^n$, так как $o(c_{jn}) = p^n$.

Систему элементов $\{a_i, c_{jn}\}_{i \in I, j \in J, n \in \omega}$ мы будем называть *квазибазисом* группы A.

Предложение 4.10. ([103]) *Если $\{a_i, c_{jn}\}$ — квазибазис p-группы A, то любой элемент $a \in A$ можно записать в виде*

$$a = s_1 a_{i_1} + \dots + s_m a_{i_m} + t_1 a_{j_1 n_1} + \dots + t_r a_{j_r n_r}, \tag{4.35}$$

где s_i и t_j — целые числа, ни одно t_j не делится на p и индексы $i_1, \dots, i_m$, так же как и индексы $j_1, \dots, j_r$ все различны. Запись (4.35) *единственна в том смысле, что в ней однозначно определены члены sa_i и tc_{jn}.*

Теорема 4.28. Куликов [34]) *Если B — базисная подгруппа редуцированной p-группы A, то*

$$|A| \leqslant |B|^\omega.$$

Финальным рангом базисной подгруппы B p-группы A назовем минимум кардинальных чисел $r(p^n B)$. Заметим, что если ранг группы B равен μ_1, а финальный ранг B равен μ_2, то $A = A_1 \oplus A_2$, где группа A_1 ограниченна и имеет ранг μ_1, а базисная подгруппа группы A_2 имеет ранг μ_2, совпадающий с ее финальным рангом.

Теорема 4.29. *Если два эндоморфизма редуцированной абелевой группы совпадают на некоторой ее базисной подгруппе, то они равны.*

Кольца эндоморфизмов абелевых групп

Эндоморфизмы абелевой группы A образуют кольцо относительно операций сложения и композиции гомоморфизмов. Это кольцо мы будем обозначать через $\mathrm{End}\,(A)$.

Нам понадобится несколько утверждений о кольце $\mathrm{End}\,(A)$:

1) *Существует взаимно-однозначное соответствие между конечными прямыми разложениями*

$$A = A_1 \oplus \dots \oplus A_n$$

группы A и разложениями кольца $\mathrm{End}\,(A)$ *в конечные прямые суммы левых идеалов*

$$\mathrm{End}\,(A) = L_1 \oplus \dots \oplus L_n;$$

именно, если $A_i = e_i A$, где $e_1, \dots, e_n$ — попарно ортогональные идемпотенты, то $L_i =$ $\mathrm{End}\,(A) e_i$.

2) *Идемпотент $e \neq 0$ называется примитивным, если его нельзя представить в виде суммы двух ненулевых ортогональных идемпотентов. Если $e \neq 0$ — идемпотент кольца* $\mathrm{End}\,(A)$, *то eA является неразложимым прямым слагаемым группы A тогда и только тогда, когда e — примитивный идемпотент.*

3) *Пусть $A = B \oplus C = B' \oplus C'$ — прямые разложения группы A и $e : A \to B$, $e' : A \to B'$ — соответствующие проекции. Тогда $B \cong B'$ в том и только том случае, когда существуют такие элементы $\alpha, \beta \in$* $\mathrm{End}\,(A)$, *что*

$$\alpha\beta = e \text{ и } \beta\alpha = e'.$$

Теорема 4.30. (Бэр [78], Капланский [116]) *Если A и C — периодические группы, кольца изоморфизмов которых изоморфны, то группы A и C изоморфны.*

Теорема 4.31. (Шарль [87], Капланский [116]) *Центр кольца эндоморфизмов* $\mathrm{End}\,(A)$ *любой p-группы A состоит из умножения на целые p-адические числа или на вычеты по модулю p^k в зависимости от того, является ли группа A неограниченной или p^k служит наименьшей верхней гранью порядков ее элементов.*

Красивые линейные комбинации

В этом параграфе мы снова будем полностью следовать статье С. Шелаха [148], нам нужно будет переформулировать ее результаты на случай абелевых групп и их колец эндоморфизмов.

Пусть у нас фиксирована абелева p-группа $A \cong \bigoplus\limits_{\mu} \mathbb{Z}(p^l)$, где μ — бесконечное кардинальное число, и кольцо $End(A)$ ее эндоморфизмов.

Пусть множество $\{a_i \mid i \in I\} \subset A$ независимо, все его элементы имеют один и тот же порядок p^l, и пусть $A' = Cl\{a_i | i \in I\}$.

Тогда из статьи Шелаха теми же методами можно получить следующую теорему:

Теорема 4.32. *Существует формула $\widetilde{\varphi}(\dots)$, удовлетворяющая следующему условию. Пусть $\{f_i\}_{i\in\mu}$ — множество элементов из $End(A')$. Тогда можно найти вектор $\overline{g}$ такой, что формула $\widetilde{\varphi}(f, \overline{g})$ истинна в $End(A')$ тогда и только тогда, когда $f = f_i$ для некоторого $i \in \mu$.*

4.6.2 Формулировка основной теоремы, обратные теоремы, разбиение на случаи.

Язык второго порядка абелевой группы

Как мы уже упоминали, мы будем рассматривать модели второго порядка абелевых групп, т. е. рассматривать групповой язык второго порядка, в котором трехместный предикатный символ будет обозначать не умножение, а сложение (т. е. мы будем писать $x_1 = x_2 + x_3$ вместо $P^3(x_1, x_2, x_3)$).

Как мы видим, формулы $\varphi(\dots)$ языка $\mathcal{L}_2$ должны состоять из следующих подформул:

1) $\forall x$ $(\exists x)$;

2) $x_1 = x_2$ и $x_1 = x_2 + x_3$, где каждая из переменных x_1, x_2, x_3 либо является свободной переменной формулы φ, либо определена в формуле φ ранее (с помощью подформул $\forall x_i$ или $\exists x_i$, $i = 1, 2, 3$);

3) $\forall P(v_1, \dots, v_n)$ $(\exists P(v_1, \dots, v_n))$, $n > 0$;

4) $P(x_1, \dots, x_n)$, где каждая из переменных $x_1, \dots, x_n$, а также “предикатная” переменная $P(v_1, \dots, v_n)$ либо являются свободными переменными формулы φ, либо определены в этой формуле с помощью подформул $\forall x_i$, $\exists x_i$, $\forall P(v_1, \dots, v_n)$, $\exists P(v_1, \dots, v_n)$.

Эквивалентность двух абелевых групп A_1 и A_2 в языке $\mathcal{L}_2$ мы будем обозначать через

$$A_1 \equiv_{\mathcal{L}_2} A_2 \text{ или } A_1 \equiv_2 A_2.$$

Как мы помним, *теорией* данного языка $\mathcal{L}$ на модели $\mathcal{U}$ называется множество всех предложений языка $\mathcal{L}$, выполненных в этой модели. В некоторых случаях мы, наравне с теориями вида $Th_2(A) = Th_{\mathcal{L}_2}(A)$, будем рассматривать теории вида $Th_2^{\varkappa}(A)$, в которые входят только те предложения φ языка $\mathcal{L}_2$, которые выполнены на любой последовательности

$$\langle a_1, \dots, a_q, b_1^{l_1}, \dots, b_s^{l_s} \rangle,$$

где $a_1, \dots, a_q \in A$, $b_i^{l_i} \subset A^{l_i}$ и $|b_i^{l_i}| \leqslant \varkappa$. При $\varkappa \geqslant |A|$ $Th_2(A)$ и $Th_2^{\varkappa}(A)$ совпадают.

Формулировка основной теоремы

Если группа $A = D \oplus G$, где группа D делима, группа G редуцированна, то *выразимым рангом группы* A мы будем называть кардинальное число

$$r_{exp} = \mu = \max(\mu_D, \mu_G),$$

где μ_D — это ранг группы D, а μ_G — это ранг базисной подгруппы группы G.

Мы хотим доказать следующую теорему:

Теорема 4.33. *Для любых бесконечных p-групп A_1 и A_2 из элементарной эквивалентности колец эндоморфизмов* $\mathrm{End}\,(A_1)$ *и* $\mathrm{End}\,(A_2)$ *следует совпадение теорий второго порядка* $Th_2^{r_{exp}(A_1)}(A_1)$ *и* $Th_2^{r_{exp}(A_2)}(A_2)$ *групп A_1 и A_2, ограниченных кардинальными числами* $r_{exp}(A_1)$ *и* $r_{exp}(A_2)$ *соответственно.*

В следующих трех пунктах мы будем по отдельности доказывать эту теоремы для абелевых групп A_1 и A_2 с различными свойствами, а в конце параграфа соберем их воедино и докажем основную теорему.

Заметим, что если группа A конечна, то и кольцо $\mathrm{End}\,(A)$ также конечно. Так как в случае конечных моделей элементарная эквивалентность (а также эквивалентность в языке $\mathcal{L}_2$) равносильна изоморфности, то в случае, когда одна из групп A_1 и A_2 конечна, теорема 4.33 следует из теоремы 4.30. Таким образом, мы далее можем считать группы A_1 и A_2 бесконечными.

Доказательство "обратных" теорем

Докажем две теоремы, в некотором смысле обратных к нашей основной теореме.

Теорема 4.34. *Для любых абелевых групп A_1 и A_2 если группы A_1 и A_2 эквивалентны в языке второго порядка $\mathcal{L}_2$, то кольца* $\mathrm{End}\,(A_1)$ *и* $\mathrm{End}\,(A_2)$ *элементарно эквивалентны.*

Доказательство. Любую двуместную предикатную переменную $P(v_1, v_2)$ мы будем называть *соответствием на группе* A. Соответствие $P(v_1, v_2)$ на группе A будем называть *функцией на группе* A (и писать в этом случае $Func(P(v_1, v_2))$ или просто $Func(P)$), если оно удовлетворяет условию

$$(\forall x \exists y P(x, y)) \wedge (\forall x \forall y_1 \forall y_2 P(x, y_1) \wedge P(x, y_2) \Rightarrow y_1 = y_2).$$

Функцию $P(v_1, v_2)$ будем называть *эндоморфизмом на группе* A (и писать в этом случае $Endom(P(v_1, v_2))$ или просто $Endom(P)$), если она удовлетворяет дополнительному условию

$$\forall x_1 \forall x_2 \forall y_1 \forall y_2 P(x_1, y_1) \wedge P(x_2, y_2) \Rightarrow P(x_1 + x_2, y_1 + y_2).$$

Теперь рассмотрим некоторое произвольное предложение φ языка первого порядка теории колец. В это предложение могут входить подформулы

1) $\forall x$;
2) $\exists x$;
3) $x_1 = x_2$;
4) $x_1 = x_2 + x_3$;
5) $x_1 = x_2 \cdot x_3$.

Переведем это предложение в предложение $\widetilde{\varphi}$ языка второго порядка теории групп по следующему алгоритму.

1) подформула $\forall x(\dots)$ переводится в подформулу

$$\forall P^x(v_1, v_2)(Endom(P^x) \Rightarrow \dots);$$

2) подформула $\exists x(\dots)$ переводится в подформулу

$$\exists P^x(v_1, v_2)(Endom(P^x) \wedge \dots);$$

3) подформула $x_1 = x_2$ переводится в подформулу

$$\forall y_1 \forall y_2 (P^{x_1}(y_1, y_2) \Leftrightarrow P^{x_2}(y_1, y_2));$$

4) подформула $x_1 = x_2 + x_3$ переводится в подформулу

$$\forall y \forall z_1 \forall z_2 \forall z_3 (P^{x_2}(y, z_2) \wedge P^{x_3}(y, z_3) \Rightarrow (P^{x_1}(y, z_1) \Leftrightarrow z_1 = z_2 + z_3));$$

5) подформула $x_1 = x_2 \cdot x_3$ переводится в подформулу

$$\forall y \forall z (P^{x_1}(y, z) \Rightarrow \exists t (P^{x_2}(y, t) \wedge P^{x_3}(t, z))).$$

Нам нужно показать, что предложение φ истинно в модели $End(A)$ тогда и только тогда, когда предложение $\widetilde{\varphi}$ истинно в модели A.

Если A — это модель абелевой группы, то модель $\mathrm{End}\,(A)$ состоит из множеств пар элементов модели A $x = \{\langle u_1, u_2 \rangle \mid u_1, u_2 \in A\}$ с условиями

1) $\forall u_1 \exists u_2 \langle u_1, u_2 \rangle \in x$;

2) $\forall u_1 \forall u_2 \forall u_3 (\langle u_1, u_2 \rangle \in x \wedge \langle u_1, u_3 \rangle \in x \Rightarrow u_2 = u_3)$;

3) $\forall u_1 \forall u_2 \forall u_3 \forall u_4 (\langle u_1, u_3 \rangle \in x \wedge \langle u_2, u_4 \rangle \in x \Rightarrow \langle u_1 + u_2, u_3 + u_4 \rangle \in x)$.

Таким образом, последовательность $a_1, \ldots, a_q$, на которой должна выполняться формула φ в модели $\mathrm{End}\,(A)$, — это последовательность множеств пар элементов модели A, удовлетворяющих условиям 1)–3).

Установим тождественную биекцию между элементами модели $\mathrm{End}\,(A)$ и соответствующими множествами пар модели A. Пусть при этой биекции элементу a_i модели $\mathrm{End}\,(A)$ соответствует множество $A_i \subset A \times A$.

1. Если формула φ имеет вид $x_i = x_j$, то выполнимость формулы φ на последовательности $a_1, \ldots, a_q$ означает, что $a_i = a_j$, т. е. a_i и a_j — совпадающие эндоморфизмы модели $\mathrm{End}\,(A)$, а множества A_i и A_j состоят из одних и тех же элементов, т. е. в модели A на последовательности $A_1, \ldots, A_q$ выполнена формула

$$\forall y_1 \forall y_2 (P^{x_i}(y_1, y_2) \Leftrightarrow P^{x_j}(y_1, y_2)).$$

2. Если формула φ имеет вид $x_i = x_j + x_k$, то выполнимость формулы φ на последовательности $a_1, \ldots, a_q$ означает, что $a_i = a_j + a_k$, т. е. эндоморфизм a_i есть сумма эндоморфизмов a_j и a_k, а это означает, что в модели A для каждого элемента $b \in A$ и для каждых $b_1, b_2, b_3 \in A$ таких, что $\langle b, b_1 \rangle \in A_i$, $\langle b, b_2 \rangle \in A_j$, $\langle b, b_3 \rangle \in A_k$, мы имеем $b_1 = b_2 + b_3$ (т. е., формально говоря, $\langle b_1, b_2, b_3 \rangle \in I(Q_1^3)$). Это и равносильно выполнимости в модели A формулы $\widetilde{\varphi}$.

3. Если формула φ имеет вид $x_i = x_j \cdot x_k$, то выполнимость формулы φ на последовательности $a_1, \ldots, a_q$ означает, что $a_i = a_j \cdot a_k$, т. е. эндоморфизм a_i есть композиция эндоморфизмов a_j и a_k, а это означает, что в модели A для каждого элемента $b_1 \in A$ и для каждого $b_2 \in A$ такого, что $\langle b_1, b_2 \rangle \in A_i$, существует $b_3 \in A$ такое, что $\langle b_1, b_3 \rangle \in A_j$ и $\langle b_3, b_2 \rangle \in A_k$. Это и равносильно выполнимости в модели A формулы $\widetilde{\varphi}$.

4. Если φ имеет вид $\theta_1 \wedge \theta_2$, θ_1 и θ_2 выполняются в модели $\mathrm{End}\,(A)$ на последовательности $a_1, \ldots, a_q$ тогда и только тогда, когда $\widetilde{\theta}_1$ и $\widetilde{\theta}_2$ выполняются в модели A на последовательности $A_1, \ldots, A_q$, то очевидно, что формула φ выполняется в модели $\mathrm{End}\,(A)$ на последовательности $a_1, \ldots, a_q$ тогда и только тогда, когда формула $\widetilde{\varphi}$ выполняется в модели A на последовательности $A_1, \ldots, A_q$, так как

$$\widetilde{\theta_1 \wedge \theta_2} = \widetilde{\theta}_1 \wedge \widetilde{\theta}_2.$$

5. Аналогично обстоит дело с формулой φ, имеющей вид $\neg\theta$, так как

$$\widetilde{\neg\theta} = \neg\widetilde{\theta}.$$

6. Наконец, предположим, что формула φ имеет вид $\forall x_i \psi$. Формула φ выполняется в модели $\mathrm{End}\,(A)$ на последовательности $a_1, \ldots, a_q$ тогда и только тогда, когда формула ψ выполняется в модели $\mathrm{End}\,(A)$ на последовательности $a_1, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_q$ для любого $a \in \mathrm{End}\,(A)$, т. е. формула $\widetilde{\psi}$ выполняется в модели A на последовательности $A_1, \ldots, A_{i-1}, \overline{A}, A_{i+1}, \ldots, A_q$ для любого множества $\overline{A} \subset A \times A$, являющегося эндоморфизмом кольца A, т. е. удовлетворяющего формуле *Endom*. Таким образом, формула φ выполняется в модели $\mathrm{End}\,(A)$ на последовательности $a_1, \ldots, a_q$ тогда и только тогда, когда формула

$$\widetilde{\forall x_i \psi} := \forall P^{x_i}(v_1, v_2)(Endom(P^{x_i}) \Rightarrow \widetilde{\psi})$$

выполняется на последовательности $A_1, \ldots, A_q$ в модели A.

Предположим теперь, что абелевы группы A_1 и A_2 эквивалентны в языке $\mathcal{L}_2$. Рассмотрим произвольное предложение φ языка первого порядка теории колец, истинное в кольце $\mathrm{End}\,(A_1)$. Тогда предложение $\widetilde{\varphi}$ истинно в группе A_1, а значит, и в группе A_2. Следовательно, предложение φ истинно в кольце $\mathrm{End}\,(A_2)$. Таким образом, кольца $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$ элементарно эквивалентны. $\square$

Для следующей теоремы нам понадобится написать несколько формул.

1. Формула

$$Gr(P(v)) := \forall a \forall b(P(a) \wedge P(b) \Rightarrow \exists c(c = a + b \wedge P(c)) \wedge P(0) \wedge \\ \wedge \forall a(P(a) \Rightarrow \exists b(b = -a \wedge P(b)))$$

истинна для множеств $\{a \in A \mid P(a)\}$, являющихся подгруппами в A, и только для них.

2. Формула

$$Cycl(P(v)) := Gr(P(v)) \wedge \exists a(P(a) \wedge \forall P_a(v)(Gr(P_a(v)) \wedge P_a(a) \Rightarrow \forall b(P(b) \Rightarrow P_a(b)))$$

характеризует циклические подгруппы в A.

3. Формула

$$DCycl(P(v)) := Gr(P(v)) \wedge \forall a(P(a) \Rightarrow \exists P_1(v) \exists P_2(v)(P_1(a) \wedge Cycl(P_1(v)) \wedge \\ \wedge \forall b \neg(P_1(b) \wedge P_2(b)) \wedge \forall b(P(b) \Rightarrow \exists b_1 \exists b_2(P_1(b_1) \wedge P_2(b_2) \wedge b = b_1 + b_2)))$$

характеризует подгруппы в A, являющиеся прямыми суммами циклических групп.

4. Для любых $a, a_1, a_2 \in A$ формула

$$Gr_a(P_a(v)) := P_a(a) \wedge Gr(P_a(v)) \wedge \forall P(v)(P(a) \wedge Gr(P(v)) \Rightarrow \forall b(P_a(b) \Rightarrow P(b)))$$

выделяет в A подгруппу $\{b \in A \mid P_a(b)\}$ всех степеней элемента a; формула

$$(o(a_1) \leqslant o(a_2)) := \exists P_1(v) \exists P_2(v) \exists P(v_1, v_2)(Gr_{a_1}(P_1) \wedge Gr_{a_2}(P_2) \wedge \\ \wedge \forall b_1(P_1(b_1) \Rightarrow \exists b_2(P_2(b_2) \wedge P(b_1, b_2))) \wedge \forall b_1 \forall b_2 \forall c_1 \forall c_2(P_1(b_1) \wedge \\ \wedge P_1(c_1) \wedge b_1 \neq c_1 \wedge P_2(b_2) \wedge P_2(c_2) \wedge P(b_1, b_2) \wedge P(c_1, c_2) \Rightarrow b_2 \neq c_2))$$

истинна тогда и только тогда, когда порядок элемента a_1 не больше порядка элемента a_2; формула

$$(o(a_1) = o(a_2)) := (o(a_1) \leqslant o(a_2)) \wedge (o(a_2) \leqslant o(a_1))$$

показывает, что порядки элементов a_1 и a_2 совпадают; формула

$$(o(a_1) < o(a_2)) := (o(a_1) \leqslant o(a_2)) \wedge \neg(o(a_2) \leqslant o(a_1))$$

показывает, что порядок элемента a_1 строго меньше порядка элемента a_2.

5. Для любого элемента $a \in A$ формула

$$GOrd_a(P(v)) := Gr(P) \wedge \forall b(P(b) \Rightarrow o(b) \leqslant o(a))$$

выполняется для подгрупп, ограниченных порядком элемента a, и только для них.

6. Формула

$$\begin{aligned} Mult_a(x, b) := \exists P(v) \exists P_{x,b}(v_1, v_2)(Cycl(P) \wedge P(x) \wedge P(b) \wedge \\ \wedge \forall b_1(P(b_1) \Rightarrow \exists b_2(P(b_2) \wedge P_{x,b}(b_1, b_2)) \wedge \\ \wedge (\forall b_1 \forall b_2 \forall b_3 P(b_1) \wedge P_{x,b}(b_1, b_2) \wedge P_{x,b}(b_1, b_3) \Rightarrow b_2 = b_3) \wedge \\ \wedge (\forall b_1 \forall b_2 \forall b_3 \forall c_1 \forall c_2 \forall c_3 P(b_1) \wedge P(b_2) \wedge P(b_3) \wedge \\ \wedge b_3 = b_1 + b_2 \wedge c_3 = c_1 + c_2 \wedge P_{x,b}(b_1, c_1) \wedge P_{x,b}(b_2, c_2) \Rightarrow \\ \Rightarrow P_{x,b}(b_3, c_3)) \wedge P_{x,b}(x, 0) \wedge \forall y(P(y) \wedge py = x \Rightarrow \\ \Rightarrow \neg P_{x,b}(y, 0)) \wedge \exists c(P(b, c) \wedge o(c) = o(a))) \end{aligned}$$

выполняется для тех и только тех элементов x и b, для которых $x = o(a) \cdot b$.

7. Формула

$$Serv(P(v)) := Gr(P) \wedge \forall a \forall x(P(x) \Rightarrow \exists b(Mult_a(x, b) \Rightarrow \exists c(P(c) \wedge Mult_a(x, c)))$$

выполняется для сервантных подгрупп группы A, и только для них.

8. Формула

$$FD(P(v)) := Gr(P) \wedge \forall a \exists b \exists x_1 \exists x_2(P(x_1) \wedge P(x_2) \wedge a + x_1 = p(b + x_2))$$

выполняется для подгрупп $G = \{x \mid P(x)\}$, таких, что A/G — делимая группа, и только для них.

9. Из всего этого следует, что формула

$$Base(P(v)) := Gr(P) \wedge DCycl(P) \wedge Serv(P) \wedge FD(P)$$

определяет базисные подгруппы группы A.

Очевидно, что если у нас есть некоторая подгруппа G' группы G, то мы аналогичным образом можем написать формулу $Base_{G'}(P)$, истинную для базисных подгрупп группы G', и только для них.

10. Формула

$$D(P(v)) := Gr(P) \wedge \forall a(P(a) \Rightarrow \exists b(P(b) \wedge a = pb))$$

определяет в A делимые группы.

11. Предложение

$$
\begin{aligned}
Exept := \forall P(Gr(P) \Rightarrow \neg(D(P))) \wedge \forall P(v)(Base(P) \Rightarrow \\
\Rightarrow \neg(\exists F(v_1, v_2)(\forall a(P(a) \Rightarrow \exists b(F(a,b))\wedge \\
\wedge \forall b \exists a(P(a) \wedge F(a,b)) \wedge \forall a \forall b(F(a,b) \Rightarrow P(a))\wedge \\
\wedge \forall a_1 \forall a_2 \forall b_1 \forall b_2(a_1 \neq a_2 \wedge F(a_1,b_1) \wedge F(a_2,b_2) \Rightarrow b_1 \neq b_2)\wedge \\
\wedge \forall b_1 \forall b_2 \forall a_1 \forall a_2(b_1 \neq b_2 \wedge F(a_1,b_1) \wedge F(a_2,b_2) \Rightarrow a_1 \neq a_2))
\end{aligned}
$$

выполняется для редуцированных p-групп, базисные подгруппы которых меньше их по мощности (и поэтому счетны), и только для них.

Таким образом, если B_1 — базисная подгруппа группы A_1, B_2 — базисная подгруппа группы A_2, $\varkappa_1 = |B_1|$, $\varkappa_2 = |B_2|$, то из

$$Th_2^{\varkappa_1}(A_1) = Th_2^{\varkappa_2}(A_2)$$

следует, что либо обе группы A_1 и A_2 редуцированны, их базисные подгруппы счетны, а сами они несчетны, либо это не так для обеих групп A_1 и A_2.

В первом случае $\varkappa_1 = \varkappa_2 = \omega$.

Теорема 4.35. *Если абелевы группы A_1 и A_2 редуцированны и их базисные подгруппы счетны, то из $Th_2^{\omega}(A_1) = Th_2^{\omega}(A_2)$ следует элементарная эквивалентность колец* $\mathrm{End}\,(A_1)$ *и* $\mathrm{End}\,(A_2)$.

Доказательство. Мы знаем (см. теорему 4.29), что для редуцированной p-группы A действие любого эндоморфизма $\varphi \in \mathrm{End}\,(A)$ полностью определяется его действием на базисной подгруппе B. Более того, пусть $A' \subset A$, B также является и базисной подгруппой в A'. Тогда любой гомоморфизм $\varphi : A' \to A$ также полностью определяется своим действием на B. Действительно, если $\varphi_1, \varphi_2 : A' \to A$, $\varphi_1(b) = \varphi_2(b)$ для всех $b \in B$, то для $\varphi := \varphi_1 - \varphi_2 : A' \to A$ мы имеем $\varphi(b) = 0$ для всех $b \in B$. Значит, φ индуцирует гомоморфизм $\widetilde{\varphi} : A'/B \to A$. Но группа A'/B делима, а группа A редуцированная, т. е. $\widetilde{\varphi} = 0$. Следовательно, $\varphi = 0$.

Заметим, что для любого элемента $a \in A$ существует счетная подгруппа $A' \subset A$, содержащая a и группу B в качестве базисной подгруппы.

Действительно, рассмотрим квазибазис группы A, имеющий вид

$$\{a_i, c_{j,n}\}_{i \in \omega, j \in \varkappa, n \in \omega},$$

где $\{a_i\}$ — базис группы B, $pc_{j,1} = 0$, $pc_{j,n+1} = c_{j,n} - b_{j,n}$, $b_{j,n} \in B$, $o(b_{j,n}) \leqslant p^n$, $o(c_{j,n}) = p^n$.

Как мы помним, любой элемент $a \in A$ можно записать в виде

$$a = s_1 a_{i_1} + \dots + s_m a_{i_m} + t_1 c_{j_1,n_1} + \dots + t_r c_{j_r,n_r},$$

где s_i и t_j — целые числа, ни одно t_j не делится на p и индексы $i_1, \dots, i_m$, $j_1, \dots, j_r$ все различны. Кроме того, эта запись единственна в том смысле, что в ней однозначно определены члены sa_i и $tc_{j,n}$.

Рассмотрим разложение нашего элемента a и подгруппу в A, порожденную группой B и всеми $c_{k,n}$, где $n \in \omega$, $k \in \{j_1, \dots, j_r\}$. Эта группа A' счетна, содержит a и $B \subset A'$ является ее базисной подгруппой.

Пусть теперь предикат $B(v)$ удовлетворяет в A формуле $Base(B)$, т. е. определяет в A базисную подгруппу $B = \{x \mid B(x)\}$.

Соответствие $P(v_1, v_2)$ называется *гомоморфизмом группы B в группу A* (обозначение: $Hom_B(P)$), если

$$\forall x(B(x) \Leftrightarrow \exists y(P(x,y))) \wedge \forall x \forall y_1 \forall y_2 (P(x,y_1) \wedge P(x,y_2) \Rightarrow y_1 = y_2) \wedge \\ \wedge \forall x_1 \forall x_2 \forall y_1 \forall y_2 (P(x_1,y_1) \wedge P(x_2,y_2) \Rightarrow P(x_1+x_2, y_2+y_2))).$$

Очевидно, что такой предикат $P(v_1, v_2)$ может употребляться в предложениях из $Th_2^{\omega}(A)$, так как группа B счетна.

Рассмотрим некоторую $B(v)$ такую, что выполняется формула $Base(B)$, предикат $\Phi(v_1, v_2)$ такой, что $Hom_B(\Phi)$, и $a \in A$.

Будем писать $b = \Phi(a)$, если

1) $B(a) \wedge \Phi(a,b)$ или

2) $\neg B(a) \wedge \forall G(v)(Gr(G) \wedge G(a) \wedge \forall x(G(x) \Rightarrow B(x)) \wedge Base_G(B) \Rightarrow \exists \varphi(v_1,v_2)(\forall x(G(x) \Leftrightarrow \exists y(\varphi(x,y)) \wedge \forall x \forall y_1 \forall y_2(\varphi(x,y_1) \wedge \varphi(x,y_2) \Rightarrow y_1 = y_2) \wedge \forall x_1 \forall x_2 \forall y_1 \forall y_2(\varphi(x_1,y_1) \wedge \varphi(x_2,y_2) \Rightarrow \varphi(x_1+x_2, y_1+y_2)) \wedge \forall x \forall y(\Phi(x,y) \Rightarrow \varphi(x,y)) \wedge \varphi(a,b))$.

Очевидно, что для каждого $a \in A$ существует не более одного $b \in A$ такого, что $b = \Phi(a)$, и что если гомоморфизм $\Phi : B \to A$ продолжается до эндоморфизма $A \to A$, то он всегда существует.

Теперь будем рассматривать такие $\Phi(v_1, v_2)$, что

$$Endom_B(\Phi) := Hom_B(\Phi) \wedge \forall a \exists b(b = \Phi(a)) \wedge \\ \wedge \forall a_1 \forall a_2 \forall b_1 \forall b_2 (b_1 = \Phi(a_1) \wedge b_2 = \Phi(a_2) \Rightarrow b_1 + b_2 = \Phi(a_1 + a_2)).$$

Эти $\Phi(v_1, v_2)$ и будут в нашем случае кодировать эндоморфизмы из $End(A)$.

Покажем алгоритм перевода формул в этом случае.

Предложение φ переводится в предложение

$$\widetilde{\varphi} = \exists B(v)(Base(B) \wedge \varphi'(B)),$$

где формула φ' получается из предложения φ следующим образом:

1) подформула $\forall x(\dots)$ переводится в подформулу

$$\forall \Phi^x(v_1, v_2)(Endom_B(\Phi^x) \Rightarrow \dots);$$

2) подформула $\exists x(\dots)$ переводится в подформулу

$$\exists \Phi^x(v_1, v_2)(Endom_B(\Phi^x) \wedge \dots);$$

3) подформула $x_1 = x_2$ переводится в подформулу

$$\forall y_1 \forall y_2 (\Phi^{x_1}(y_1, y_2) \Leftrightarrow \Phi^{x_2}(y_1, y_2));$$

4) подформула $x_1 = x_2 + x_3$ переводится в подформулу

$$\forall y \forall z_1 \forall z_2 \forall z_3 (\Phi^{x_2}(y, z_2) \wedge \Phi^{x_3}(y, z_3) \Rightarrow (\Phi^{x_1}(y, z_1) \Leftrightarrow z_1 = z_2 + z_3));$$

5) подформула $x_1 = x_2 \cdot x_3$ переводится в подформулу

$$\forall y \forall z (\Phi^{x_1}(y, z) \Rightarrow \exists t (\Phi^{x_2}(y, t) \wedge z = \Phi^{x_3}(t)).$$

Далее доказательство аналогично доказательству предыдущей теоремы. □

Разделение задачи на случаи

Следуя теореме 4.30, разделим класс всех абелевых p-групп на следующие три подкласса:

1) ограниченные p-группы;

2) группы вида $D \oplus G$, где D — ненулевая делимая группа, G — ограниченная группа;

3) группы с неограниченной базисной подгруппой.

Покажем, как найти предложения, разделяющие группы из разных типов.

Если группа A ограничена, то существует натуральное $n = p^k$ такое, что

$$\forall a (na = 0)$$

в группе A. Это означает, что в кольце $\mathrm{End}\,(A)$ также

$$\forall x (nx = 0).$$

Однако если группа A не является ограниченной, то ни для какого n такое предложение верно быть не может. Значит, мы отделили случай 1) от всех остальных, а также научились находить то число, которым ограничена в этом случае группа A. Будем обозначать предложение $\forall x (nx = 0)$ через φ_n.

Теперь рассмотрим предложение

$$\begin{aligned}\psi_n := \exists \rho_1 \exists \rho_2 (\rho_1 \rho_2 = \rho_2 \rho_1 = 0 \wedge \rho_1^2 = \rho_1 \wedge \rho_2^2 = \rho_2 \wedge \rho_1 + \rho_2 = 1 \wedge \\ \wedge \forall x (n \cdot \rho_2 x \rho_2 = 0) \wedge \forall \rho \forall \rho' (\rho^2 = \rho \wedge {\rho'}^2 = \rho' \wedge \rho \rho' = \rho' \rho = 0 \wedge \rho + \rho' = \rho_1 \wedge \\ \wedge \forall \tau_1 \forall \tau_2 (\tau_1^2 = \tau_1 \wedge \tau_2^2 = \tau_2 \wedge \tau_1 \tau_2 = \tau_2 \tau_1 = 0 \Rightarrow \tau_1 + \tau_2 \neq \rho) \Rightarrow \\ \Rightarrow \forall x (\rho x \rho = 0 \vee p(\rho x \rho) \neq 0))).\end{aligned}$$

Объясним словами, что означает это предложение.

1. Существуют ортогональные проекции ρ_1 и ρ_2, дающие в сумме 1 в кольце $End(A)$. Это означает, что $A = \rho_1 A \oplus \rho_2 A$, при этом $\rho_1 \,\mathrm{End}\,(A) \rho_1 = \mathrm{End}\,(\rho_1 A)$, $\rho_2 \,\mathrm{End}\,(A) \rho_2 = \mathrm{End}\,(\rho_2 A)$.

2. Условие $\forall x (n \cdot \rho_2 x \rho_2 = 0)$, как и выше, означает, что в кольце $\mathrm{End}\,(\rho_2 A)$ все элементы ограничены числом $n = p^k$, т.е. что группа $\rho_2 A$ ограничена.

3. Остальная часть предложения ψ_n утверждает, что если в кольце $\mathrm{End}\,(\rho_1 A)$ рассмотреть примитивный идемпотент ρ (т.е. проекцию на неразложимое прямое слагаемое

$\rho A = \rho\rho_1 A$), то это прямое слагаемое не имеет ни одного эндоморфизма порядка p. Отсюда следует, что в группе $\rho_1 A$ нет циклических прямых слагаемых, т. е. она делима.

Отсюда следует, что кольцо $\mathrm{End}\,(A)$ удовлетворяет предложению ψ_n тогда и только тогда, когда $A = D \oplus G$, где группа D делима, а группа G ограничена числом n.

Следовательно, для любых двух групп A_1 и A_2 из разных классов существует предложение, на котором различаются кольца $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$.

Таким образом, в дальнейшем мы можем считать, что если кольца $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$ элементарно эквивалентны, то группы A_1 и A_2 лежат в одном классе, и, если они обе лежат в первом или втором классе, то соответственно они сами или их редуцированные прямые слагаемые ограничены одним и тем же числом $n = p^k$, которое можно считать известным.

4.6.3 Ограниченные p-группы

Разделение идемпотентов

Как мы видели выше (см. п. 4.4), свойство элемента $\rho \in \mathrm{End}\,(A)$ быть неразложимым идемпотентом, выделяемым в прямую сумму, является свойством, выразимым в логике первого порядка. Будем обозначать формулу, выражающую это свойство, через $Idem^*(\rho)$, в то время как формула, выражающая свойство элемента $\rho \in \mathrm{End}\,(A)$ быть просто идемпотентом (не обязательно неразложимым), будет обозначаться через $Idem(\rho)$.

Мы рассматриваем группу $A = \sum\limits_{i=1}^{k} A_i$, где $A_i \cong \bigoplus\limits_{\mu_i} \mathbb{Z}(p^i)$. Так как группа A бесконечна, то $\mu_l = \max\limits_{i=1,\dots,k} \mu_i$ бесконечно и совпадает с мощностью группы A.

Рассмотрим для каждого $i = 1, \dots, k$ формулу

$$Idem_i^*(\rho) = Idem^*(\rho) \wedge p^{i-1}\rho \neq 0 \wedge p^i \cdot \rho = 0.$$

Для каждого i эта формула выполняется для проекторов на прямые слагаемые группы A, изоморфные $\mathbb{Z}(p^i)$, и только для них.

Теперь рассмотрим следующую формулу:

$$\begin{aligned} Comp(\rho_1, \dots, \rho_k) = (\rho_1 + \dots + \rho_k = 1) \wedge \Big(\bigwedge_{i \neq j} \rho_i\rho_j = \rho_j\rho_i = 0\Big) \wedge \\ \wedge \Big(\bigwedge_{i=1}^{k} \rho_i^2 = \rho_i\Big) \wedge \Big(\bigwedge_{i=1}^{k} p^i\rho_i = 0\Big) \wedge \\ \wedge \Big(\bigwedge_{i=1}^{k} p^{i-1}\rho_i \neq 0\Big) \wedge \Big(\bigwedge_{i=1}^{k} \forall \rho (Idem^*(\rho) \wedge \\ \wedge \exists \rho' (\rho + \rho' = \rho_i \wedge \rho\rho' = \rho'\rho = 0 \wedge Idem(\rho')) \Rightarrow Idem_i^*(\rho)\Big). \end{aligned}$$

Мы видим, что группа A (соответственно этой формуле) должна раскладываться в прямую сумму $\rho_1 A \oplus \rho_2 A \oplus \cdots \oplus \rho_k A = A$, причем в каждой из подгрупп $\rho_i A$ все неразложимые прямые слагаемые имеют порядок p_i. Отсюда следует, что $\rho_1 A \oplus \cdots \oplus \rho_k A$ — это разложение группы A, изоморфное разложению $\sum\limits_{i=1}^{k} A_i$.

Будем считать, что проекции $\rho_1, \ldots, \rho_k$ из формулы $Comp(\ldots)$ фиксированы. Для того, чтобы отличать их от других идемпотентов, будем обозначать их через $\overline{\rho}_1, \ldots, \overline{\rho}_k$. Имея фиксированные идемпотенты $\overline{\rho}_1, \ldots, \overline{\rho}_k$ кольца $\mathrm{End}\,(A)$, мы имеем также и его фиксированные подкольца

$$\overline{E}_i = \overline{\rho}_i End(A) \overline{\rho}_i,$$

каждое из которых изоморфно кольцу

$$\mathrm{End}\,(\rho_i A) \cong \mathrm{End}\,(A_i).$$

Формулу, выражающую для идемпотента ρ, удовлетворяющего формуле $Idem_i^*(\rho)$ $(Idem_i(\rho))$, то, что он выделяется прямым слагаемым в группе $\overline{\rho}_i A$ (т. е. $\exists \rho'(Idem(\rho') \wedge \rho\rho' = \rho'\rho = 0 \wedge \rho + \rho' = \overline{\rho}_i)$, мы будем записывать через $\overline{Idem_i^*}(\rho)$ $(\overline{Idem_i}(\rho))$. Эта формула означает, что подгруппа ρA является прямым слагаемым в группе $\overline{\rho}_i A = A_i$.

Число l из множества $\{1, \ldots, k\}$, для которого выполнено предложение

$$Card_l = \bigwedge_{i=1, i \neq l}^{k} \exists a \forall \rho (\overline{Idem_i^*}(\rho) \Rightarrow \rho a \overline{\rho_l} \neq 0),$$

является номером группы A_l с $|A_l| = |A| = \mu$, так как это предложение означает, что существует эндоморфизм $a \in \mathrm{End}\,(A)$, отображающий A_l в A так, что на любом прямом слагаемом подгруппы A_i он является ненулевым. Это означает, что $|A_l| \geqslant |A_i|$, т. е. мощность $|A_l|$ максимальна. Будем считать число l также фиксированным.

Формула $Card_l$ показывает, что можно написать формулы, определяющие для любых двух проекторов ρ_1 и ρ_2, выполенно ли $|\rho_1 A| < |\rho_2 A|$, $|\rho_1 A| > |\rho_2 A|$ или $|\rho_1 A| = |\rho_2 A|$. Будем обозначать эти формулы через $|\rho_1| < |\rho_2|$, $|\rho_1| > |\rho_2|$ и $|\rho_1| = |\rho_2|$ соответственно.

Формула

$$\begin{aligned} Fin(\rho) := \forall \rho_1 \forall \rho_2 (Idem(\rho_1) \wedge Idem(\rho_2) \wedge Idem(\rho) \wedge \\ \wedge\, \rho_1 = \rho + \rho_2 \wedge \rho\rho_2 = \rho_2\rho = 0 \Rightarrow |\rho| < |\rho_1|) \end{aligned}$$

означает, что группа ρA конечно порождена. Соответственно, формула

$$Inf(\rho) := Idem(\rho) \wedge \neg Fin(\rho)$$

выполнена для проекций на бесконечно порожденные группы.

Формула

$$Count(\rho) := Inf(\rho) \wedge \forall \rho_1 (Inf(\rho_1) \Rightarrow |\rho| \leqslant |\rho_1|)$$

выполняется для проекций на счетно порожденные группы, и только для них.

Наконец, нам потребуется формула

$$\overline{Idem_l^{\omega}}(\rho) = \overline{Idem_l}(\rho) \wedge Count(\rho),$$

означающая, что группа ρA является счетно порожденным прямым слагаемым группы A_l.

Специальные множества

Сначала сформулируем, какие специальные множества мы хотим получить. Нам требуется получить два множества. Первое из них должно содержать μ_i независимых неразложимых проекторов на элементы подгруппы A_i, для каждого $i = 1, \ldots, k$, второе — $\mu = \mu_l$ проекторов на независимые между собой счетно порожденные прямые слагаемые группы A_l.

По теореме 4.4 мы видим, что существует формула $\varphi(\overline{g}; f)$, удовлетворяющая следующему условию. Если $\{f_i\}_{i\in\mu}$ — множество элементов из $\mathrm{End}\,(A')$, то существует вектор $\overline{g}$ такой, что формула $\varphi(\overline{g}; f)$ истинна в $\mathrm{End}\,(A')$ тогда и только тогда, когда $f = f_i$ для некоторого $i \in \mu$. Зафиксируем эту формулу φ.

Пусть мы имеем некоторое фиксированное $i \in \{1, \ldots, k\}$. Мы уже показали, что от кольца $\mathrm{End}\,(A)$ можно перейти к кольцу $\mathrm{End}\,(A_i)$. Пусть мы рассуждаем уже в кольце $\mathrm{End}\,(A_i)$ (удовлетворяющем условиям теоремы 4.4). В этом кольце рассмотрим следующую формулу:

$$
\begin{aligned}
\widetilde{\varphi}_i(\overline{g}) := \forall f'(\varphi(\overline{g}, f') \Rightarrow \overline{Idem_i^*}(f'))\wedge \\
\forall f'(\overline{Idem_i}(f') \wedge \forall f_1(\varphi(\overline{g}, f_1) \Rightarrow \\
\Rightarrow \exists f_2(\overline{Idem_i}(f_2) \wedge f_1 f_2 = f_2 f_1 = 0 \wedge f_1 + f_2 = f')) \Rightarrow |f'| = |\rho_i|)\wedge \\
\wedge\, \forall f'(\varphi(\overline{g}, f') \Rightarrow (\exists f(\overline{Idem_i}(f) \wedge \forall f_1(\varphi(\overline{g}, f_1)\wedge \\
\wedge\, f_1 \neq f' \Rightarrow f_1 f = f f_1 = f_1) \wedge f f' = f' f = 0)).
\end{aligned}
$$

Часть $\forall f'(\varphi(\overline{g}, f') \Rightarrow \overline{Idem_i^*}(f'))$ означает, что вектор $\overline{g}$ таков, что формула $\varphi(\overline{g}, f)$ выполняется только для проекторов f на неразложимые прямые слагаемые группы A_i.

Часть $\forall f'(\overline{Idem_i}(f') \wedge \forall f_1(\varphi(\overline{g}, f_1) \Rightarrow \exists f_2(\overline{Idem_i}(f_2) \wedge f_1 f_2 = f_2 f_1 = 0 \wedge f_1 + f_2 = f')) \Rightarrow |f'| = |\rho_i|)$ означает, что любая подгруппа группы A_i, содержащая все такие слагаемые fA, что $\varphi(\overline{g}, f)$, имеет ту же мощность, что и A_i, т. е. что мощность множества этих f равна μ.

Последняя часть формулы означает, что для любого f' такого, что $\varphi(\overline{g}, f')$, группа, порожденная всеми остальными f такими, что $\varphi(\overline{g}, f)$, не пересекается с f', т. е. множество всех f таких, что $\varphi(\overline{g}, f)$, независимо.

Это множество мы будем обозначать через $\mathbf{F}_i$. Оно состоит из μ_i независимых проекторов на неразложимые прямые слагаемые группы A_i. Естественно, такое множество получается для любого вектора $\overline{g}_i$, удовлетворяющего формуле $\widetilde{\varphi}_i(\overline{g}_i)$, поэтому следовало бы писать не $\mathbf{F}_i$, а $\mathbf{F}_i(\overline{g}_i)$, что мы и будем делать далее. Однако в случаях, когда параметр несущественен, мы будем его опускать.

Объединение всех $\mathbf{F}_i$ для $i = 1, \ldots, k$ мы будем обозначать через $\mathbf{F}$. Множество $\mathbf{F}$ зависит от параметра $\overline{g} = (\overline{g}_1, \ldots, \overline{g}_k)$.

Теперь нам нужно получить множество $\mathbf{F}'$, состоящее из $\mu_l = \mu$ независимых между собой проекторов на счетно порожденные прямые слагаемые группы A_l. Это будет сделано совершенно аналогично предыдущему случаю, следует только заменить в формуле $\widetilde{\varphi}_l(\overline{g}')$ следующие части: $\overline{Idem_l^*}(f)$ на $\overline{Idem_l^\omega}(f)$; кроме того, мы будем рассматривать такие векторы $\overline{g}'$, что

1) $\forall f \in \mathbf{F}_l(\exists f'(\varphi(\overline{g}', f') \wedge ff' = f)$, т. е. для каждого циклического прямого слагаемого fA ($f \in \mathbf{F}_l$) группы A_l существует счетно порожденное слагаемое $f'A$ группы A_l такое, что $\varphi(\overline{g}', f')$ и $fA \subset f'A$;

2) (напишем словами, чтобы не выписывать сложных формул) любое прямое слагаемое в A_l, содержащее все fA для всех таких проекторов f, что $\varphi(\overline{g}_l, f)$ содержит все $f'A$ такие, что $\varphi(\overline{g}', f')$.

Обозначим соответствующую формулу через $\widetilde{\widetilde{\varphi}}_l(\overline{g}')$, а полученное множество проекторов назовем $\mathbf{F}' = \mathbf{F}'(\overline{g}')$.

Интерпретация группы A для каждого элемента $\mathbf{F}'$

Под интерпретацией группы A для каждого элемента из $\mathbf{F}'$ мы будем понимать следующее. Мы имеем μ независимых прямых слагаемых $\mathcal{F}_i = f_i A$ ($i \in \mu$), каждое из которых есть прямая сумма счетного числа циклических групп порядка p^l. Любой эндоморфизм группы A на каждом слагаемом $\mathcal{F}_i$ действует совершенно независимо, поэтому если мы сможем для каждого эндоморфизма $\varphi \in \mathrm{End}\,(A)$ сопоставлять каждому элементу $\mathcal{F}_i$ некоторый элемент группы A, то мы научимся сопоставлять каждому эндоморфизму $\varphi \in \mathrm{End}\ A$ множество элементов группы A мощности μ, что нам и будет далее требоваться для получения теории второго порядка группы A. По этой причине в этом пункте мы сосредоточимся на биективном соответствии между некоторыми гомоморфизмами из группы $\mathcal{F}_i$ в группу A и элементами группы A, причем введем на множестве таких гомоморфизмов операцию $\oplus$, которая при этой биекции будет соответствовать сложению на группе A.

Фиксируем некоторую проекцию $g \in \mathbf{F}'$. Рассмотрим множество End_g всех гомоморфизмов $h : gA \to A$, удовлетворяющих следующим условиям:

1) $\forall f \in \mathbf{F}_l(fg = f \Rightarrow (hf = 0 \vee \exists f' \in \mathbf{F}(hf = f'hf \neq 0)))$, что означает, что для любого проектора f из нашего специального множества $\mathbf{F}_l$, проектирующего A на неразложимое прямое слагаемое fA модуля gA, либо $h(fA) = 0$, либо $h(fA) \subset f'A$ для некоторого проектора $f' \in \mathbf{F}$;

2) $\exists f(Fin(f) \wedge Idem(f) \wedge fh = h)$, что означает, что образ группы gA при эндоморфизме h конечномерен;

3) $\bigwedge\limits_{i=1}^{k} \forall f \in \mathbf{F}_i \neg(\exists f_1 \ldots \exists f_{p^i}(\bigwedge\limits_{q \neq s} f_q \neq f_s \wedge f_1, \ldots, f_{p^i} \in F_l \wedge f_1 g = g_1 \wedge \cdots \wedge f_{p^i} g = f_{p^i} \wedge hf_1 = fhf_1 \neq 0 \wedge \cdots \wedge hf_{p^i} = fhf_{p^i} \neq 0))$, что означает, что для каждого $i = 1, \ldots, k$ прообраз каждого $fA \subset A_i$, где $f \in \mathbf{F}_i$, не может содержать более $p^i - 1$ различных элементов $f_m A$, где $f_m A \subset gA$ и $f_m \in \mathbf{F}_l$.

Два элемента h_1 и h_2 множества End_g будем считать эквивалентными ($h_1 \sim h_2$), если выполняется следующая формула:

$$\begin{aligned}\exists f_1 \exists f_2((gf_1g) \cdot (gf_2g) = (gf_2g) \cdot (gf_1g) = g \wedge \\ \wedge \forall f \in \mathbf{F}_l(fg = f \Rightarrow \forall f' \in \mathbf{F}(h_1 f = f'h_1 f \neq 0 \Leftrightarrow (gf_1gh_2)f = f'(gf_1gh_2)f \neq 0)).\end{aligned}$$

Это означает, что существует автоморфизм gf_1g группы gA, переводящий h_2 в такой эндоморфизм $(gf_1g \cdot h_2)$, что для любого проектора из F_l, проектирующего на подгруппу группы gA оба эндоморфизма h_1 и gf_1gh_2 отображают эту подгруппу или в ноль, или в одно и то же $f'A$ ($f' \in \mathbf{F}$). Таким образом получившееся множество $End_g/\sim$ обозначим через $\widetilde{End_g}$. Элементы этого множества можно интерпретировать как множество, состоящее из конечных наборов проекторов множества $\mathbf{F}$ с тем условием, что каждый проектор из $\mathbf{F}_i$ может входить в такой набор не более $p^i - 1$ раз. Соответственно, каждый элемент множества $\widetilde{End_g}$ можно интерпретировать как множество пар, где первый элемент в паре — это проектор f из $\mathbf{F}$, а второй элемент — это целое число от 0 до p^i-1, где i таково, что $f \in \mathbf{F}_i$, причем почти все (все, кроме конечного числа) вторые компоненты пар равны 0. Теперь можно построить биективное отображение между множеством $\widetilde{End_g}$ и группой A, положив образом описанного выше множества $\{\langle f_j, l_j\rangle | j \in J\}$ элемент $\sum\limits_{j\in J} l_j\xi_j = a \in A$, где ξ_j — это некоторый заранее фиксированный образующий циклической группы f_jA.

Осталось ввести на множестве $\widetilde{End_g}$ сложение так, чтобы полученное нами биективное отображение стало изоморфизмом абелевых групп.

Зададим сложение формулой ($h_1, h_2, h_3 \in \widetilde{End_g}$)

$$\begin{aligned}(h_3 = h_1 \oplus h_2) := \bigwedge_{i=1}^{k} \forall f \in \mathbf{F}_i \Big(\bigwedge_{j=0}^{p^i-1} \exists g_1 \ldots \exists g_j \in \mathbf{F}_l \bigwedge_{q\neq s} (g_q \neq g_s \wedge g_q g = g_q \wedge \\ \wedge\, h_3 g_q = f h_3 g_q \neq 0 \wedge \neg(\exists g_1 \ldots \exists g_{j+1} \in \mathbf{F}_l \bigwedge_{q\neq s} (g_q \neq g_s \wedge g_q g = g_q \wedge \\ \wedge\, h_3 g_q = f h_3 g_q \neq 0 \wedge)) \Rightarrow \\ \Rightarrow \Big(\bigvee_{m=0}^{j} \exists g_1 \ldots \exists g_m \in \mathbf{F}_l \bigwedge_{q\neq s} (g_q \neq g_s \wedge g_q g = g_q \wedge h_1 g_q = f h_1 g_q \neq 0) \wedge \\ \wedge\, \neg(\exists g_1 \ldots \exists g_{m+1} \in \mathbf{F}_l \bigwedge_{q\neq s} (g_q \neq g_s \wedge g_q g = g_q \wedge h_1 g_q = f h_1 g_q \neq 0)) \wedge \\ \wedge\, \exists g_1 \ldots \exists g_{\gamma(j,m)} \in \mathbf{F}_l \bigwedge_{q\neq s} (g_q \neq g_s \wedge g_q g = g_q \wedge h_2 g_q = f h_2 g_q \neq 0) \wedge \\ \wedge\, \neg(\exists g_1 \ldots \exists g_{\gamma(j,m)+1} \in \mathbf{F}_l \bigwedge_{q\neq s} (g_q \neq g_s \wedge g_q g = g_q \wedge h_2 g_q = f h_2 g_q \neq 0))\Big)\Big),\end{aligned}$$

где $\gamma(j, m) = j - m$ при $j \geqslant m$, и $\gamma(j, m) = p^i + j - m$ при $j < m$.

Теперь мы видим, что для каждого $g \in \mathbf{F}'$ имеется формульное множество $\widetilde{End_g}$ с операцией сложения $\oplus$, изоморфное группе A.

Доказательство первого случая в теореме

Предложение 4.11. *Для двух бесконечных абелевых p-групп A_1 и A_2, ограниченных числом p^k, из элементарной эквивалентности колец* $\mathrm{End}\,(A_1)$ *и* $\mathrm{End}\,(A_2)$ *следует эквивалентность групп A_1 и A_2 в языке $\mathcal{L}_2$.*

Доказательство. Для каждого $\widetilde{g} \in \mathbf{F}'$ через $Resp_{\widetilde{g}}(h)$ будем обозначать следующую формулу:

$$Resp_{\widetilde{g}}(h) := \forall g \in \mathbf{F}' \exists h'((\widetilde{g}hg)(gh'\widetilde{g}) = \widetilde{g} \wedge (gh'\widetilde{g})(\widetilde{g}hg) = g).$$

Эта формула означает, что эндоморфизм h изоморфно отображает каждое слагаемое gA ($g \in \mathbf{F}'$) на слагаемое $\widetilde{g}A$.

Как и раньше, рассмотрим произвольное предложение φ в логике второго порядка теории групп и укажем алгоритм, переводящий это предложение ψ в предложение $\widetilde{\psi}$ первого порядка языка теории колец такое, что $\widetilde{\psi}$ выполняется в $\mathrm{End}\,(A)$ тогда и только тогда, когда φ выполняется в A.

Переведем предложение ψ в предложение

$$\begin{aligned}\exists \overline{g}_1 \ldots \exists \overline{g}_k (\widetilde{\varphi}_1(\overline{g}_1) \wedge \ldots \widetilde{\varphi}_k(\overline{g}_k) \wedge \\ \wedge \exists \overline{g}' (\widetilde{\widetilde{\varphi}}_l(\overline{g}', \overline{g}_l) \wedge \exists \widetilde{g} \in \mathbf{F}'(\overline{g}') \exists h (Resp_{\widetilde{g}}(h) \wedge \\ \wedge \psi'(\overline{g}_1, \ldots, \overline{g}_k, \overline{g}', \widetilde{g}, h)))),\end{aligned}$$

где формула $\psi'(\ldots)$ получается из предложения ψ с помощью следующих замен подформул, входящих в ψ:

1) подформула $\forall x$ заменяется на подформулу $\forall x \in \widetilde{End_{\widetilde{g}}}$;
2) подформула $\exists x$ заменяется на подформулу $\exists x \in \widetilde{End_{\widetilde{g}}}$;
3) подформула $\forall P_m(v_1, \ldots, v_m)(\ldots)$ заменяется на подформулу

$$\forall f_1^P \ldots \forall f_m^P (\forall g \in \mathbf{F}'(\overline{g}') (\bigwedge_{i=1}^{m} (f_i^P g \in End_g)) \Rightarrow \ldots);$$

4) подформула $\exists P_m(v_1, \ldots, v_m)(\ldots)$ заменяется на подформулу

$$\exists f_1^P \ldots \exists f_m^P (\forall g \in \mathbf{F}'(\overline{g}') (\bigwedge_{i=1}^{m} (f_i^P g \in End_g)) \wedge \ldots);$$

5) подформула $x_1 = x_2$ заменяется на подформулу $x_1 \sim x_2$;
6) подформула $x_1 = x_2 + x_3$ заменяется на подформулу $x_1 \sim x_2 \oplus x_3$;
7) Подформула $P_m(x_1, \ldots, x_m)$ заменяется на подформулу

$$\exists g \in \mathbf{F}'(\overline{g}') \Big(\bigwedge_{i=1}^{m} f_i^P g = x_i h g \Big).$$

Объясним словами, что означают переводы. Благодаря наличию множества $\mathbf{F}'$, мы имеем μ групп $\widetilde{End_g}$ для $g \in F'$, каждая из которых изоморфна группе A. Мы фиксируем один заранее выбранный элемент $\widetilde{g} \in \mathbf{F}'$, и, таким образом, фиксируем одну группу $\widetilde{End_{\widetilde{g}}}$, изоморфную A. Естественно, все подформулы $\forall x$, $\exists x$, $x_1 = x_2$, $x_1 = x_2 + x_3$ (относящиеся к логике первого порядка) мы будем переводить в соответствующие подформулы для группы $\widetilde{End_{\widetilde{g}}}$. Теперь нам нужно каким-то образом интерпретировать в кольце $\mathrm{End}\,(A)$ произвольное отношение $P_m(v_1, \ldots, v_m)$ на множестве A. Такое отношение есть некоторое подмножество в A^m, т. е. набор упорядоченных m-ок элементов из A. Всего таких m-ок не может больше μ, поэтому множество $P_m(v_1, \dots, v_m)$ можно считать множеством из μ m-ок элементов из A (некоторые из них могут совпадать). Мы рассматриваем m эндоморфизмов $f_1^P, \dots, f_m^P \in \mathrm{End}\,(A)$, ограничение каждого из которых на любую gA ($g \in \mathbf{F}'$) является элементом $\widetilde{End}_g$. Таким образом, для каждого $g \in \mathbf{F}'$ ограничение эндоморфизмов $f_1^P, \dots, f_m^P$ на gA является m-кой элементов группы $\widetilde{End}_{\widetilde{g}}$ ($\cong A$), где изоморфизм между $\widetilde{End}_{\widetilde{g}}$ и $\widetilde{End}_g$ осуществляется с помощью заранее фиксированного отображения h, изоморфно отображающего каждый модуль gA на $\widetilde{g}A$.

Отсюда видно, что предложение ψ выполняется в группе A тогда и только тогда, когда предложение $\widetilde{\psi}$ выполняется в кольце $\mathrm{End}\,(A)$. Отсюда, как и в предыдущем параграфе, следует окончание доказательства. □

4.6.4 Прямые суммы делимых и ограниченных p-групп

Конечно порожденные группы

Любая бесконечная конечно порожденная абелева p-группа A имеет вид $D \oplus G$, где D — делимая конечно порожденная группа, G — конечная группа. Не нуждается в доказательстве следующее предложение.

Предложение 4.12. *Если абелевы p-группы A_1 и A_2 конечно порождены, то из элементарной эквивалентности их колец эндоморфизмов* $\mathrm{End}\,(A_1)$ *и* $\mathrm{End}\,(A_2)$ *следует, что группы A_1 и A_2 изоморфны.*

Бесконечно порожденные делимые группы

Как и в п. 5.1, формула $Idem^*(\rho)$ будет обозначать свойство эндоморфизма ρ быть неразложимым идемпотентом, в то время как $Idem(\rho) := (\rho^2 = \rho)$. Если в делимой группе D выполнено $Idem^*(\rho)$, то $\rho A \cong \mathbb{Z}(p^\infty)$.

Заметим, что несмотря на то, что в п. 1 мы рассматривали прямые суммы циклических групп одного порядка, теорема Шелаха остается справедливой и для делимых групп, так как делимая группа является объединением групп

$$\bigoplus_{\mu} \mathbb{Z}(p) \subset \bigoplus_{\mu} (p^2) \subset \dots \subset \bigoplus_{\mu} \mathbb{Z}(p^n) \subset \dots$$

(доказательство даже более общего случая дано в следующем параграфе). Значит, аналогично предыдущему пункту, мы имеем формульное множество $\mathbf{F} = \mathbf{F}(\overline{g})$, состоящее из μ неразложимых проекторов на линейно независимые прямые слагаемые группы D, а также формульное множество $\mathbf{F}' = \mathbf{F}'(\overline{g}')$, состоящее из μ проекторов на линейно независимые счетно порожденные прямые слагаемые группы D.

Фиксируем некоторый элемент $g \in \mathbf{F}'$ и снова построим для него интерпретацию группы D.

Именно, рассмотрим множество End_g всех гомоморфизмов $h : gA \to A$, удовлетворяющих следующим условиям:

1) $\forall f \in \mathbf{F}(fg = f \Rightarrow (hf = 0 \vee \exists \widetilde{f} \in \mathbf{F}(\widetilde{h}f = \widetilde{f}hf \neq 0)))$, что означает, что для любого проектора f из множества $\mathbf{F}$ такого, что $fA \subset gA$, либо $h(fA) = 0$, либо $h(fA) \subset \widetilde{f}A$ для некоторого $\widetilde{f} \in \mathbf{F}$;

2) $\exists f(Fin(f) \wedge Idem(f) \wedge fh = h)$, что означает, что образ группы gA при эндоморфизме h конечномерен;

3) $\forall f \in \mathbf{F}(\exists f' \in \mathbf{F}(f'g = g' \wedge hf' = fhf' \neq 0) \Rightarrow \exists \widetilde{f} \in \mathbf{F}(\widetilde{f}g = \widetilde{f} \wedge h\widetilde{f} = fh\widetilde{f} \neq 0) \wedge \forall f' \in \mathbf{F}(f'g = f' \wedge hf' = fhf' \neq 0 \Rightarrow \exists \alpha(\alpha hf' = h\widetilde{f})))$, что означает, что для любого элемента $f \in \mathbf{F}$ либо прообраз fA пуст, либо он содержит такой $\widetilde{f}A \subset gA$ ($\widetilde{f} \in \mathbf{F}$), что ядро $\widetilde{f}A$ при отображении h имеет максимальный порядок из всех ядер $f'A$ для $f' \in \mathbf{F}$, $f'A \subset gA$.

Перед последним условием введем новые обозначения. Пусть h — некоторый эндоморфизм, $f_1, f_2 \in \mathbf{F}$.

Будем писать $f_1 \sim_h f_2$, если выполняется формула

$$\exists \alpha(\alpha^2 = 1 \wedge \alpha f_1 = f_2\alpha \wedge \alpha f_2 = f_1\alpha \wedge hf_1 = h\alpha f_1 \wedge hf_2 = h\alpha f_2).$$

Эта формула означает, что образы групп f_1A и f_2A при эндоморфизме h совпадают, а ядра групп f_1A и f_2A при этом эндоморфизме изоморфны.

Теперь для эндоморфизма h и проекторов $f_1, f_2 \in \mathbf{F}$ введем формулу

$$\exists \alpha(\alpha^2 = 1 \wedge \alpha f_1 = f_2\alpha \wedge \alpha f_2 = f_1\alpha \wedge hf_1 = ph\alpha f_1).$$

Эта формула утверждает, что образы группы f_1A и f_2A при эндоморфизме h совпадают, а ядро группы f_1A в p раз больше ядра группы f_2A. Эту формулу будем обозначать через $f_1 \sim_h f_2 + 1$.

Теперь перейдем к последнему условию:

4) $\neg(\exists f_1, \ldots, f_p \in \mathbf{F}((\bigwedge\limits_{i \neq j} f_i \neq f_j) \wedge f_1g = f_1 \wedge \cdots \wedge f_pg = f_p \wedge hf_1 = fhf_1 \neq 0 \wedge \cdots \wedge hf_p = fhf_p \neq 0 \wedge (\bigwedge\limits_{i \neq j} f_i \sim f_j)))$, что означает, что существует не более $p - 1$ проекторов из $\mathbf{F}$ на подгруппы из gA таких, что их ядра изоморфны.

Два элемента h_1 и h_2 множества End_g будем считать эквивалентными ($h_1 \sim h_2$), если выполняется следующая формула:

$$\exists f_1 \exists f_2((gf_1g) \cdot (gf_2g) = (gf_2g) \cdot (gf_1g) = g \wedge \\ \wedge \forall f \in \mathbf{F}(fg = f \Rightarrow h_1f = (gf_1g)h_2f \wedge h_2f = (gf_2g)h_1f)).$$

Это означает, что существуют взаимно обратные автоморфизмы gf_1g и gf_2g группы gA, переводящие h_2 и h_1 в такие автоморфизмы $(gf_1g)h_2$ и $(gf_2g)h_1$, что для любого проектора из $\mathbf{F}$, проектирующего на подгруппу группы gA, $h_2 = (\widetilde{gf_2g})h_1$ и $h_1 = (gf_1g)h_2$ на gA.

Получившееся множество $End_g/\sim$ обозначим через $\widetilde{End}_g$.

Пусть имеется две квазицикличиские группы C и C', одна из которых имеет образующие $c_1, \ldots, c_n, \ldots$ $(pc_1 = 0, pc_{n+1} = c_n)$, другая — $c'_1, \ldots, c'_n, \ldots$ $(pc'_1 = 0, pc'_{n+1} = c'_n)$.

Рассмотрим множество гомоморфизмов $\alpha \in Hom(C, C')$. Два гомоморфизма $\alpha_1, \alpha_2 \in Hom(C, C')$ переводятся друг в друга некоторым автоморфизмом группы C тогда и только тогда, когда их ядра изоморфны, т. е. имеют один и тот же порядок. Таким образом, все гомоморфизмы из $Hom(C, C')$ разделяются на счетное число классов, и каждому классу единственным образом соответствует неотрицательное целое число i такое, что $|Ker\,\alpha| = p^i$.

Следовательно, каждому классу $h \in \widetilde{End}_g$ можно поставить в соответствие конечный набор конечных последовательностей

$$\langle f, m(f), l_1(f), \ldots, l_{m(f)}(f)\rangle,$$

где $f \in \mathbf{F}$, $m(f) \in \mathbb{N}$, $l_i(f) = 0, \ldots, p-1$. Очевидно, что эндоморфизмам из одного класса эквивалентности соответствуют одинаковые наборы, а эндоморфизмам из разных классов — разные. Кроме того, очевидно, что любому конечному набору последовательностей соответствует некоторый класс эндоморфизмов. Теперь каждому такому множеству последовательностей поставим в соответствие элемент

$$\sum_{f \in \mathbf{F}} l_1(f)c_1(f) + \cdots + l_m(f)c_m(f),$$

где $c_1(f), \ldots, c_n(f), \ldots$ — заранее фиксированные образующие группы fA.

Таким способом мы получим биекцию между множеством $\widetilde{End}_g$ и группой $A \cong \bigoplus\limits_{\mu} \mathbb{Z}(p^\infty)$.

Теперь введем на множестве $\widetilde{End}_g$ сложение ($h_3 = h_1 \oplus h_2$) так, чтобы эта биекция стала изоморфизмом между абелевыми группами.

Пусть $h_1, h_2, h_3 \in \widetilde{End}_g$.

$$
\begin{aligned}
(h_3 = h_1 \oplus h_2) := \forall f \in \mathbf{F}\Big(\forall f' \in \mathbf{F}\Big(f'g = f' \wedge h_1 f' = f h_1 f' \neq 0 \Rightarrow \\
\Rightarrow \bigwedge_{i=0}^{p-1}\Big(\exists f_1 \ldots \exists f_i \in \mathbf{F} \bigwedge_{q\neq s}(f_q \neq f_s \wedge f_q \sim_{h_1} f' \wedge f_q g = f_q \wedge h_1 f_q = f h_1 f_q \neq 0)\wedge \\
\wedge \neg\Big(\exists f_1, \ldots, \exists f_{i+1} \in \mathbf{F} \bigwedge_{q\neq s}(f_q \neq f_s \wedge f_q \sim_{h_1} f' \wedge f_q g = f_q \wedge h_1 f_q = f h_1 f_q \neq 0)\Big) \Rightarrow \\
\Rightarrow \bigvee_{j=0}^{p-1}\Big(\exists f_1 \ldots \exists f_j \in \mathbf{F} \bigwedge_{q\neq s}(f_q \neq f_s \wedge f_q \sim_{h_2} f' \wedge f_q g = f_q \wedge h_2 f_q = f h_2 f_q \neq 0)\wedge \\
\wedge \neg\Big(\exists f_1 \ldots \exists f_{j+1} \in \mathbf{F} \bigwedge_{q\neq s}(f_q \neq f_s \wedge f_q \sim_{h_2} f' \wedge f_q g = f_q \wedge h_2 f_q = f h_2 f_q \neq 0)\Big)\wedge \\
\wedge \Big(\Big(\exists f_1 \ldots \exists f_{(i+j) mod\, p} \in \mathbf{F} \bigwedge_{q\neq s}(f_q \neq f_s \wedge f_q \sim_{h_3} f' \wedge f_q g = f_q \wedge h_3 f_q = f h_3 f_q \neq 0)\wedge \\
\wedge \neg\Big(\exists f_1 \ldots \exists f_{(i+j)\, mod\, p+1} \in \mathbf{F} \bigwedge_{q\neq s}(f_q \neq f_s \wedge f_q \sim_{h_3} f' \wedge f_q g = f_q \wedge h_3 f_q = f h_3 f_q \neq 0)\Big)\wedge \\
\wedge \neg\Big(\exists f_1 \ldots f_p \in \mathbf{F} \bigwedge_{q\neq s}(f_q \neq f_s \wedge f_q \sim_{h_3} f' + 1 \wedge \\
\wedge f_q g = f_q \wedge (h_1 f_q = f h_1 f_q \neq 0 \vee h_2 f_q = f h_2 f_q \neq 0))\Big)\Big)\vee \\
\vee \Big(\exists f_1 \ldots \exists f_{(i+j) mod\, p+1} \in \mathbf{F} \bigwedge_{q\neq s}(f_q \neq f_s \wedge f_q \sim_{h_3} f' \wedge f_q g = f_q \wedge h_3 f_q = f h_3 f_q \neq 0)\wedge \\
\wedge \neg\Big(\exists f_1 \ldots \exists f_{(i+j)\, mod\, p+2} \in \mathbf{F} \bigwedge_{q\neq s}(f_q \neq f_s \wedge f_q \sim_{h_3} f' \wedge f_q g = f_q \wedge h_3 f_q = f h_3 f_q \neq 0)\Big)\wedge \\
\wedge \exists f_1 \ldots f_p \in \mathbf{F} \bigwedge_{q\neq s}(f_q \neq f_s \wedge f_q \sim_{h_3} f' + 1 \wedge f_q g = f_q \wedge \\
\wedge (h f_q = f h_1 f_q \neq 0 \vee h_2 f_q = f h_2 f_q \neq 0))\Big)\Big)\Big)\Big)\Big)\Big).
\end{aligned}
$$

Таким образом, для каждого $g \in \mathbf{F}'$ имеется формульное множество $\widetilde{End}_g$, с операцией сложения $\oplus$, изоморфное группе A.

Предложение 4.13. *Для двух бесконечно порожденных делимых p-групп A_1 и A_2 из элементарной эквивалентности колец* $\mathrm{End}\,(A_1)$ *и* $\mathrm{End}\,(A_2)$ *следует эквивалентность групп A_1 и A_2 в языке $\mathcal{L}_2$.*

Доказательство. После того, как мы для каждого $g \in \mathbf{F}'$ получили интерпретацию группы A, доказательство этого предложения совершенно аналогично доказательству предложения 4.11. □

Прямые суммы делимых p-групп и ограниченных p-групп не бо́льшей мощности

В этом пункте мы рассмотрим группы вида $D \oplus G$, где D — бесконечно порожденная делимая группа, G — группа, ограниченная числом p^k, причем $|G| \leqslant |D|$. Этот случай является практически объединением двух предыдущих.

Именно, пусть мы имеем идемпотенты ρ_D и ρ_G из формулы ψ_{p^k}, т. е. идемпотенты, являющиеся проекциями на делимую и ограниченную части группы A, соответственно, а также идемпотенты $\rho_1, \ldots, \rho_k$, $\rho_1 + \cdots + \rho_k = \rho_G$, являющиеся проекциями на прямые слагаемые вида $\bigoplus\limits_{\mu_1} \mathbb{Z}(p)$, …, $\bigoplus\limits_{\mu_k} \mathbb{Z}(p^k)$, соответственно. Пусть $|A| = |D| = \mu$. Как и раньше, имеем формульные множества:

1) $\mathbf{F} = \mathbf{F}(\overline{g})$ — множество из μ неразложимых проекторов на линейно независимые прямые слагаемые группы D;

2) множество $\mathbf{F}' = \mathbf{F}'(\overline{g}')$, состоящее из μ проекторов на линейно независимые счетно порожденные прямые слагаемые группы D;

3) для каждого $i = 1, \ldots, k$ множество $\mathbf{F}_i = \mathbf{F}_i(\overline{g}_i)$, состоящее из μ_i проекторов на независимые неразложимые прямые слагаемые группы $\rho_i A$;

4) эндоморфизм $\varphi \in \mathrm{End}\,(A)$, удовлетворяющий следующей формуле:

$$
\begin{gathered}
\forall f \in \mathbf{F}(\overline{g})(\varphi f \in \mathbf{F}) \wedge \\
\wedge \bigwedge_{i=1}^{k} (\rho_D \varphi \rho_i = \varphi \rho_i \wedge \forall f_i \in \mathbf{F}_i(\overline{g}_i) \exists f \in \mathbf{F}(\overline{g})(\varphi f_i = f \varphi f_i \neq 0)) \wedge \\
\wedge \forall f_1, f_2 \in \mathbf{F}(\overline{g})(f_1 \neq f_2 \Rightarrow \forall f_1', f_2' \in \mathbf{F}(\overline{g}) \\
(\varphi f_1 = f_1' \varphi f_1 \neq 0 \wedge \varphi f_1 = f_2' \varphi f_2 \neq 0 \Rightarrow f_1' \neq f_2') \wedge \\
\wedge \bigwedge_{i=1}^{k} \forall f \in \mathbf{F}(\overline{g}) \forall f_i \in \mathbf{F}_i(\overline{g}_i) \forall f' \in F(\overline{g})(f' = \varphi f \Rightarrow f' \varphi f_i = 0) \wedge \\
\wedge \bigwedge_{i,j=1}^{k} \forall f_1, f_2 \in \mathbf{F}(\overline{g}) \forall f_i \in \mathbf{F}_i(\overline{g}_i) \forall f_j \in \mathbf{F}_j(\overline{g}_j) \\
(f_i \neq f_j \wedge \varphi f_i = f_1 \varphi f_i \neq 0 \wedge \varphi f_j = f_2 \varphi f_j \neq 0 \Rightarrow f_1 \neq f_2).
\end{gathered}
$$

Мы видим, что такой эндоморфизм φ вкладывает множество

$$\mathbf{F}(\overline{g}) \cup \mathbf{F}_1(\overline{g}_1) \cup \cdots \cup \mathbf{F}_k(\overline{g}_k)$$

во множество $\mathbf{F}(\overline{g})$. Таким образом, для данного φ мы можем рассмотреть множества

$$
\begin{aligned}
&\mathbf{F}^D = \mathbf{F}^D(\overline{g}, \varphi) = \{f \in \mathbf{F}(\overline{g}) | \exists f' \in \mathbf{F}(\overline{g})(f \varphi f' = f \varphi = \varphi f' \neq 0)\}, \\
&\mathbf{F}_1^D = \mathbf{F}_1^D(\overline{g}_1, \varphi) = \{f \in \mathbf{F}(\overline{g}) | \exists f' \in \mathbf{F}_1(\overline{g}_1)(f \varphi f' = f \varphi = \varphi f' \neq 0)\}, \\
&\ldots \\
&\mathbf{F}_k^D = \mathbf{F}_k^D(\overline{g}_k, \varphi) = \{f \in \mathbf{F}(\overline{g}) | \exists f' \in \mathbf{F}_k(\overline{g}_k)(f \varphi f' = f \varphi = \varphi f' \neq 0)\}.
\end{aligned}
$$

Множества $\mathbf{F}^D, \mathbf{F}_1^D, \ldots, \mathbf{F}_k^D$ состоят из соответственно $\mu, \mu_1, \ldots, \mu_k$ проекторов на неразложимые линейно независимые прямые слагаемые группы D. Мы будем записывать их в формулах, иногда опуская параметры, но имея в виду, что они зависят от параметров $\overline{g}, \overline{g}_1, \ldots, \overline{g}_k, \varphi$.

Фиксируем некоторый элемент $g \in \mathbf{F}'$ и построим для него интерпретацию группы $A = D \oplus G$.

Именно, рассмотрим множество End_g всех гомоморфизмов $h : gA \to A$, удовлетворяющих следующим условиям:

1) $\forall f \in \mathbf{F}(fg = f \Rightarrow (hf = 0 \vee \exists \widetilde{f} \in \mathbf{F}(hf = \widetilde{f}hf \neq 0) \vee \bigwedge\limits_{i=1}^{k} \exists \widetilde{f} \in \mathbf{F}_i^D(\widetilde{f}h = \widetilde{f}hf = hf \neq 0)))$, что означает, что для любого проектора f из множества $\mathbf{F}$ такого, что $fA \subset gA$, либо $h(fA) = 0$, либо $h(fA) \subset \widetilde{f}A$ для некоторого $\widetilde{f} \in \mathbf{F}^D$, либо $h(fA) = \widetilde{f}A$ для некоторого $\widetilde{f} \in \mathbf{F}_i^D$.

2) $\exists f(Fin(f) \wedge Idem(f) \wedge fh = h)$, что означает, что образ группы gA при эндоморфизме h конечномерен.

3) $\bigwedge\limits_{i=1}^{k} \forall f \in \mathbf{F}_i^D \neg(\exists f_1, \ldots, \exists f_{p^i} \in \mathbf{F}((\bigwedge\limits_{q \neq s} f_q \neq f_s) \wedge f_1 g = f_1 \wedge \cdots \wedge f_{p^i} g = f_{p^i} \wedge fhf_1 = fh = hf_1 \neq 0 \wedge \cdots \wedge fhf_{p^i} = fh = hf_{p^i} \neq 0))$, что означает, что для каждого $i = 1, \ldots, k$ прообраз каждого $fA \subset D$, где $f \in \mathbf{F}_i^D$, не может содержать более $p^i - 1$ различных элементов $f_m A$, где $f_m A \subset gA$ и $f_m \in \mathbf{F}$.

4) $\forall f \in \mathbf{F}^D \exists f' \in \mathbf{F}(f'g = g' \wedge hf' = fhf' \neq 0 \Rightarrow \exists \widetilde{f} \in \mathbf{F}(\widetilde{f}g = \widetilde{f} \wedge h\widetilde{f} = fh\widetilde{f} \neq 0) \wedge \forall f' \in \mathbf{F}(f'g = f' \wedge hf' = fhf' \neq 0 \Rightarrow \exists \alpha(\alpha hf' = h\widetilde{f})))$, что означает, что для любого элемента $f \in \mathbf{F}$ либо прообраз fA пуст, либо он содержит такой $\widetilde{f} \in \mathbf{F}$, $\widetilde{f}A \subset gA$, что ядро $\widetilde{f}A$ при отображении h имеет максимальный порядок из всех ядер $f'A$ для $f' \in \mathbf{F}$, $f'A \subset gA$.

5) $\neg(\exists f_1, \ldots, f_p \in \mathbf{F}((\bigwedge\limits_{q \neq s} f_q \neq f_s) \wedge f_1 g = f_1 \wedge \cdots \wedge f_p = gf_p \wedge hf_1 = fhf_1 \neq 0 \wedge \cdots \wedge hf_p = fhf_p \neq 0 \wedge (\bigwedge\limits_{q \neq s} f_q \sim_h f_s)))$, что означает, что существует не более $p - 1$ проекторов из $\mathbf{F}$ на подгруппы из gA таких, что их образы попадают в $\mathbf{F}^D$, а их ядра изоморфны.

Два элемента h_1 и h_2 множества End_g будем считать эквивалентными ($h_1 \sim h_2$), если выполняется формула

$$\exists f_1 \exists f_2((gf_1g) \cdot (gf_2g) = (gf_2g) \cdot (gf_1g) = g \wedge \\ \wedge \forall f \in \mathbf{F}(fg = f \Rightarrow h_1 f = (gf_1g)h_2 f \wedge h_2 f = (gf_2g)h_1 f)),$$

т. е. существуют взаимно обратные автоморфизмы gf_1g и gf_2g группы gA, переводящие h_2 и h_1 в такие автоморфизмы $(gf_1g)h_2$ и $(gf_2g)h_1$, что для любого проектора из $\mathbf{F}$, проектирующего на подгруппу группы gA, имеет место $h_2 = (gf_2g)h_1$ и $h_1 = (gf_1g)h_2$ на gA.

Получившееся множество $End_g/\sim$ снова обозначим через $\widetilde{End}_g$.

Каждому классу $h \in \widetilde{End}_g$ можно поставить в соответствие множество, состоящее из следующих $k+1$ компонент: i-ая его компонента при $i = 1, \ldots, k$ — это множество пар

$$M_i = \{\langle f, m(f) \rangle | f \in \mathbf{F}_i^D, m = 1, \ldots, p^i - 1\},$$

где m — это размерность прообраза $f \in \mathbf{F}_i^D$, если она не равна нулю;

$(k+1)$-ая его компонента — это множество последовательностей

$$M = \{\langle f, m(f), l_0(f), \dots, l_{m(f)}(f)\rangle | f \in \mathbf{F}^D, m \in \mathbb{N}, l_1, \dots, l_m = 0, \dots, p-1\},$$

где p^m — это максимальный порядок ядра прообраза подгруппы fA, лежащего в gA и имеющего вид $f'A$ для $f' \in \mathbf{F}'$, $l_1, \dots, l_m$ — это размерности прообразов подгруппы fA, ядра которых при отображении h имеют порядок p^i.

Очевидно, что эндоморфизмам из одного класса эквивалентности соответствуют одинаковые множества $M_1, \dots, M_k, M$, а из разных классов — разные. Кроме того, очевидно, что любой последовательности $M_1, \dots, M_k, M$ конечных множеств описанного выше вида соответствует некоторый класс из $\widetilde{End}_g$. Теперь каждой такой последовательности множеств $M_1, \dots, M_k, M$ поставим в соответствие элемент

$$\sum_{\langle f, m(f)\rangle \in M_1} m(f)a(f) + \dots + \sum_{\langle f, m(f)\rangle \in M_k} m(f)a(f) + \sum_{\langle f, m(f), l_0, \dots, l_{m(f)}\rangle \in M} l_1 c_1(f) + \dots + l_{m(f)} c_{m(f)}(f),$$

где $a(f)$ — заранее фиксированный образующий циклической группы fA при $f \in \mathbf{F}_1 \cup \dots \cup \mathbf{F}_k$, $c_1(f), \dots, c_n(f), \dots$ — заранее фиксированные образующие квазициклической группы fA при $f \in \mathbf{F}$.

Таким способом мы получим биекцию между множеством $\widetilde{End}_g$ и группой A.

Сложение ($h_3 = h_1 \oplus h_2$) на множестве $\widetilde{End}_g$ вводится формулой, аналогичной объединению формул п. 5.3 и п. 6.2, поэтому мы не будет приводить здесь эту формулу.

Предложение 4.14. *Пусть $A_1 = D_1 \oplus G_1$, $A_2 = D_2 \oplus G_2$, группы D_1 и D_2 делимы и бесконечно порождены, группы G_1 и G_2 ограничены числом p^k, $|D_1| \geqslant |G_1|$, $|D_2| \geqslant |G_2$. Тогда* $\mathrm{End}\,(A_1) \equiv \mathrm{End}\,(A_2) \Rightarrow A_1 \equiv_{\mathcal{L}_2} A_2$.

Доказательство. Доказательство совершенно аналогично доказательству предложения 4.13, поэтому мы не будем его приводить. □

Прямые суммы делимых p-групп и ограниченных p-групп большей мощности

Данный случай существенно отличается от двух предыдущих, он скорее ближе к случаю ограниченных p-групп, но со значительными усложнениями.

Мы рассмотрим группы вида $D \oplus G$, где D — бесконечно порожденная делимая группа, G — группа, ограниченная числом p^k, причем $|G| > |D|$, $G = \sum\limits_{i=1}^{k} G_i$, $G_i \cong \bigoplus\limits_{\mu_i} \mathbb{Z}(p^i)$, $\mu_l = \max\limits_{i=1,\dots,k} \mu_i$, $D \cong \bigoplus\limits_{\mu} \mathbb{Z}(p^\infty)$, $\mu < \mu_l$.

Пусть, как и в предыдущем пункте, мы имеем идемпотенты ρ_D и ρ_G, являющиеся проекциями на делимую и ограниченную части группы A, соответственно, а также проекции $\rho_1, \dots, \rho_k$, $\rho_1 + \dots + \rho_k = \rho_G$, на прямые слагаемые $G_1, \dots, G_k$. Кроме того, известно слагаемое G_l с максимальной мощностью μ_l, равной мощности всей группы A.

Как и прежде, выделяем различные формульные множества:

1) множество $\mathbf{F} = \mathbf{F}(\overline{g})$, состоящее из μ неразложимых проекторов на линейно независимые прямые слагаемые группы D;

2) для каждого $i = 1, \ldots, k$ множество $\mathbf{F}_i = \mathbf{F}_i(\overline{g}_i)$, состоящее из μ_i проекторов на независимые неразложимые прямые слагаемые группы $G_i = \rho_i A$;

3) множество $\mathbf{F}' = \mathbf{F}'(\overline{g}')$, состоящее из μ_l проекторов на линейно независимые счетно порожденные прямые слагаемые группы G_l;

4) идемпотент γ, удовлетворяющий следующему условию:

$$\Gamma(\gamma) := (\gamma\rho_l = \gamma \wedge \gamma^2 = \gamma \wedge \forall f \in \mathbf{F}' \exists \beta (f\gamma = \gamma f = \beta \wedge Idem^{\omega}(\beta))).$$

Это условие означает, что γ является проекцией на прямое слагаемое в G_l такое, что его пересечение с любой подгруппой fA, $f \in \mathbf{F}'$, есть счетно порожденное слагаемое в G_l.

5) Для каждого идемпотента γ, удовлетворяющего формуле $\Gamma(\gamma)$, через Γ_γ мы обозначим множество $\{f \in \mathbf{F}_l | f\gamma = f\}$, а через $\Gamma_\gamma(g)$ для $g \in \mathbf{F}'$ — множество $\{f \in \mathbf{F}_l | f\gamma = f \wedge fg = f\}$. Фиксируем два таких идемпотента γ_0 и γ_1 с условиями: 1) $\Gamma_{\gamma_0} \cap \Gamma_{\gamma_1} = \emptyset$; 2) для всякого $g \in \mathbf{F}'$ множество $\mathbf{F}_l \setminus (G_{\gamma_0} \cup G_{\gamma_1}) \cap \{f \in \mathbf{F}_l | fg = f\}$ счетно.

Обозначим Γ_{γ_0} через Γ_0, Γ_{γ_1} — через Γ_1.

6) Фиксируем эндоморфизм $\varphi \in \operatorname{End}(A)$, удовлетворяющий следующей формуле:

$$\begin{gathered}
\Phi(\varphi) := \forall h (Idem(h) \wedge \forall g \in \mathbf{F}'(hg = gh = 0) \Rightarrow \varphi h = h\varphi = 0) \wedge \\
\wedge \forall g \in \mathbf{F}'(\forall f \in \Gamma_0(g)(\varphi f = f \wedge \forall f \in \Gamma_1(g) \exists f' \in \mathbf{F}_l(f' \notin \Gamma_1(g) \wedge f' \notin \Gamma_0(g) \wedge \\
\wedge f'g = f' \wedge f'\varphi f = \varphi f \neq 0) \wedge \forall f \in \mathbf{F}_l(f \notin \Gamma_0(g) \wedge fg = f \Rightarrow \\
\Rightarrow \exists f' \in \mathbf{F}_l(f' \neq f \wedge f' \notin \Gamma_0(g) \wedge f' \notin \Gamma_1(g) \wedge f'g = f' \wedge f'\varphi f = \varphi f \neq 0) \wedge \\
\wedge \forall f_1, f_2 \in \mathbf{F}_l(f_1 \neq f_2 \wedge f_1 g = f_1 \wedge f_2 g = f_2 \Rightarrow \\
\Rightarrow \neg(\exists f' \in \mathbf{F}_l(f'g = f' \wedge f'\varphi f_1 = \varphi f_1 \wedge f'\varphi f_2 = \varphi f_2)) \wedge \\
\wedge \forall f' \in \mathbf{F}_l(f'g = f' \wedge f' \in \Gamma_1(g) \Rightarrow \exists f \in \mathbf{F}_l(fg = f \wedge f'\varphi = f'\varphi f = \varphi f)) \wedge \\
\wedge \forall h (Idem(h) \wedge hg = h \wedge h\gamma_0 = \gamma_0 h = 0 \wedge \\
\wedge \forall f (Idem^*(f) \wedge fg = f \wedge fh = f \Rightarrow \\
\Rightarrow \exists f'(Idem^*(f') \wedge f'g = f' \wedge f'h = f' \wedge f'\varphi f = \varphi f) \Rightarrow Idem^{\omega}(f)))).
\end{gathered}$$

Данное условие представляет эндоморфизм φ, переводящий прямое дополнение к $\sum\limits_{g \in \mathbf{F}'} gA$ в 0, т. е. действующий только на $\sum\limits_{g \in \mathbf{F}'} gA$ следующим образом: для каждого $g \in \mathbf{F}'$ элементы αA, $\alpha \in \Gamma_0(g)$, переводятся сами в себя, а элементы αA, $\alpha \in \Gamma_1(g)$ переводятся куда-то в элементы $\mathbf{F}_l A$, не принадлежащие ни $\Gamma_0(g)A$, ни $\Gamma_1(g)A$, но принадлежащие gA. При этом φ является мономорфизмом на gA, и его образ есть

$$\langle \Gamma_0(g)A \rangle \oplus \langle \{fA | f \in \mathbf{F}_l \wedge fg = f \wedge f \notin \Gamma_1(g)A\} \rangle.$$

Кроме того, вне $\Gamma_0(A)$ нет конечномерных собственных подпространств этого эндоморфизма. Отсюда следует, что можно занумеровать все элементы из $\mathbf{F}_l$, проектирующие на подгруппы из gA (обозначим это множество через $F_l(g)$) так: $f_i^j = f_i^j(g)$, $i = 0, 1, \ldots$, $j = 1, \ldots$, что

a) $f_0^j \in \Gamma_0(g)$;

b) $f_1^j \in \Gamma_1(g)$;

c) $\varphi(f_i^j A) = f_{i+1}^j A$ при $i > 0$;

d) $\varphi(f_0^j A) = f_0^j A$.

Обозначим множество $\{f_i^j\}_{j=1,\ldots}$ через $\Gamma_i(g)$ (заметим, что для произвольного i это множество не является формульным).

7) Объединение $\bigcup\limits_{g\in\mathbf{F}'} \mathbf{F}_l(g)$ обозначим через $\mathbf{F}'_l$. Это множество формульно.

8) Заметим, что на группе $B = \langle \mathbf{F}'_l A\rangle$ у эндоморфизма φ существует левый обратный эндоморфизм ψ такой, что $\psi \circ \varphi = 1_B$. Для каждого g он устроен на gA следующим образом:

$$\begin{cases} \psi(f_0^j A) = f_0^j A; \\ \psi(f_i^j A) = f_{i-1}^j A \text{ при } i > 1, \\ \psi(f_1^j A) \text{ может быть любым.} \end{cases}$$

Мы будем рассматривать ψ с условием $\psi(f_i^j A) = 0$. Тогда два элемента $f_1, f_2 \in \mathbf{F}_l(g)\setminus\Gamma_0(g)$ (или, более общо, $\mathbf{F}'_l \setminus \Gamma_0$) назовем *$\varphi$-эквивалентными* ($f_1 \sim_\varphi f_2$), если

$$\begin{gathered} \exists h_1 \exists h_2 \exists \alpha (h_1 g = h_1 \wedge h_2 g = h_2 \wedge Idem(h_1) \wedge Idem(h_2) \wedge \\ \wedge\, \alpha^2 = 1 \wedge \bigwedge_{i=1}^{2} \forall f (Idem^*(f) \wedge fg = f \wedge fh_i = f \Rightarrow \\ \Rightarrow \exists f' (Idem^*(f') \wedge f'g = f' \wedge f'h_i = f' \wedge f'\psi f = \psi f)) \wedge \\ \wedge\, f_1 h_1 = f_1 \wedge f_2 h_2 = f_2 \wedge \bigwedge_{i=1}^{2} \forall h (Idem(h) \wedge hg = h \wedge \\ \wedge\, \forall f (Idem^*(f) \wedge fg = f \wedge fh = f \Rightarrow \\ \Rightarrow \exists f' (Idem^*(f') \wedge f'g = f' \wedge f'h = f' \wedge f'\psi f = \psi f) \wedge f_i h f_i \Rightarrow \\ \Rightarrow h_i h = h_i)) \wedge h_1 \alpha h_2 = \alpha h_2 = h_1 \alpha \wedge h_2 \alpha h_1 = h_2 \alpha). \end{gathered}$$

Это означает, что минимальные собственные подпространства эндоморфизма ψ ($h_1 A$ и $h_2 A$), содержащие группы $f_1 A$ и $f_2 A$ соответственно, имеют одинаковую размерность, т. е. $f_1 A, f_2 A \in Ker\, \psi^m \setminus Ker\, \psi^{m+1}$ для некоторого натурального m, или $f_1 A, f_2 A \in \varphi^m(\Gamma_1)$. Очевидно, что в этом случае $f_1 = f_m^j(g)$ и $f_2 = f_m^i(g)$ (или, в более общем случае, $f_1 = f_m^j(g_1)$ и $f_2 = f_m^j(g_2)$).

Назовем элемент $f_1 \in \mathbf{F}_l(g)$ *φ-последователем* элемента $f_2 \in \mathbf{F}_l(g)$ ($f_1 \sim_\varphi f_2 + 1$), если

$$\exists f (f \sim_\varphi f_1 \wedge f\varphi f_2 = \varphi f_2 = f\varphi).$$

Аналогичной формулой введем понятие *φ-бóльшего элемента* ($f_1 >_\varphi f_2$) как элемента, у которого минимальное собственное подпространство эндоморфизма ψ, содержащее $f_1 A$, имеет бóльшую размерность, чем соответствующее подпространство для $f_2 A$.

Фиксируем $g \in \mathbf{F}'_l$ и для него построим интерпретацию группы $A = D \oplus G$.

Рассмотрим множество End_g всех гомоморфизмов $h : gA \to A$, удовлетворяющих следующим условиям:

1) $\forall f \in \mathbf{F}_l(fg = f \Rightarrow (hf = 0 \vee \exists \widetilde{f} \in \mathbf{F}^D(hf = \widetilde{f}hf \neq 0) \vee (\bigvee\limits_{i=1}^{k} \exists \widetilde{f} \in \mathbf{F}_i(hf = \widetilde{f}hf \neq 0))))$.

2) $\exists f(Fin(f) \wedge Idem(f) \wedge fh = h)$.

3) $\bigwedge\limits_{i=1}^{k} \forall f \in \mathbf{F}_i \neg(\exists f_1, \ldots, \exists f_{p^i} \in \mathbf{F}(\bigwedge\limits_{q \neq s} f_q \neq f_s \wedge f_1, \ldots, f_{p^i} \in \Gamma_0(g) \wedge hf_1 = fhf_1 \neq 0 \wedge \cdots \wedge hf_{p^i} = fhf_{p^i} \neq 0) \wedge \forall f' \in \mathbf{F}_l(hf' = fhf' \neq 0 \Rightarrow f' \in \Gamma_0(g)))$, что, вдобавок к предыдущим случаям означает, что прообразы элементов ограниченного слагаемого могут содержаться только во множестве $\Gamma_0(g)$.

4) $\forall f \in \mathbf{F}^D \exists f' \in \mathbf{F}_l(hf' = fhf' \neq 0 \Rightarrow f' \notin \Gamma_0)$, что означает, что, в противоположность к предыдущему, прообразы элементов делимого слагаемого не могут содержаться в $\Gamma_0(g)$.

5) $\forall f \in \mathbf{F}^D \neg(\exists f_1, \ldots, f_p \in \mathbf{F}_l((\bigwedge\limits_{q \neq s} f_q \neq f_s \wedge f_q \sim_\varphi f_s) \wedge f_1 g = f_1 \wedge \cdots \wedge f_p g = f_p \wedge hf_1 = fhf_1 \neq 0 \wedge \cdots \wedge hf_p = fhf_p \neq 0))$, что означает, что у каждого элемента из $\mathbf{F}_D$ не может быть более $p-1$ φ-эквивалентных прообраза.

6) $\forall f \in \mathbf{F}^D \exists f' \in \mathbf{F}_l \neg(\exists f'' \in \mathbf{F}_l(f'' >_\varphi f' \wedge hf'' = fhf'' \neq 0))$, т. е. любой элемент из $\mathbf{F}_D$ содержит лишь конечное число прообразов в $\mathbf{F}_l$.

Два элемента h_1 и h_2 множества End_g будем считать эквивалентными (в обозначениях $h_1 \sim h_2$), если выполняется следующая формула:

$$\begin{gathered}\exists f_1 \exists f_2((gf_1g) \cdot (gf_2g) = (gf_2g) \cdot (gf_1g) = g \wedge \forall f \in \mathbf{F}_l(fg = f \Rightarrow \\ \Rightarrow \forall f' \in \mathbf{F}^D \cup \mathbf{F}_1 \cup \cdots \cup \mathbf{F}_k(h_1 f = f'h_1 f \neq 0 \Leftrightarrow (gf_1gh_2)f = f'(gf_1gh_2)f \neq 0)) \wedge \\ \wedge \forall f \in \mathbf{F}_l(gf_1g \cdot f \sim_\varphi f)).\end{gathered}$$

Получившееся множество $End_g/\sim$ обозначим через $\widetilde{End}_g$.

Покажем, как осуществить биекцию между множеством $\widetilde{End}_g$ и группой A. Рассмотрим некоторое $h \in \widetilde{End}_g$. Для каждого $f \in \mathbf{F}_i$ рассмотрим пересечение прообраза fA с множеством $\Gamma_0 A$. Пусть этот прообраз состоит из m_f элементов. Так мы получим множество

$$M_G = \bigcup_{i=1}^{k} \{\langle f, m_f \rangle | f \in \mathbf{F}_i, m_f = 1, \ldots, p^i - 1\}.$$

Для каждого $f \in \mathbf{F}^D$ и каждого натурального j рассмотрим пересечение прообраза fA с множеством $\Gamma_j(g)$. Пусть этот прообраз состоит из l_f^j элементов, и при этом максимальное ненулевое j равно γ_f. Тогда мы получим множество

$$M_D = \{\langle f, \gamma_f, l_f^1, \ldots, l_f^{\gamma_f} \rangle | f \in \mathbf{F}^D, \gamma_f \in \mathbb{N}, l_f^1, \ldots, l_f^{\gamma_f} \in \{0, \ldots, p-1\}\}.$$

Теперь сопоставим элементу h следующую сумму:

$$\sum_{f \in M_G} m_f a(f) + \sum_{f \in M_D} l_f^1 c_1(f) + \cdots + l_f^{\gamma_f} c_{\gamma_f}(f) \in A.$$

Очевидно, что такое отображение осуществляет биекцию между множествами $\widetilde{End}_g$ и A, которую мы превратим в изоморфизм, введя на множестве $\widetilde{End}_g$ сложение с помощью формулы, аналогичной формулам предыдущих разделов. Отсюда следует

Предложение 4.15. *Пусть* $A_1 = D_1 \oplus G_1$, $A_2 = D_2 \oplus G_2$, *группы* D_1 *и* D_2 *делимы, группы* G_1 *и* G_2 *бесконечны и ограничены числом* p^k, $|D_1| < |G_1|$, $|D_2| < |G_2|$. *Тогда* $\mathrm{End}\,(A_1) \equiv \mathrm{End}\,(A_2) \Rightarrow A_1 \equiv_{\mathcal{L}_2} A_2$.

4.6.5 Группы с неограниченной базисной подгруппой

Случай $A = D \oplus G$, $|D| \geqslant |G|$, и другие случаи

Разделим нашу задачу на следующие случаи:

1. $A = D \oplus G$, $|D| \geqslant |G|$, G — любая неограниченная группа. Этот случай мы не будем рассматривать подробно, так как его доказательство аналогично случаю $A = D \oplus G$, $|D| \geqslant |G|$, D — делимая группа, G — ограниченная группа. Мы не будем разбирать его подробно, приведем только схему доказательства.

Так как $|G| \leqslant |D|$, то базисная подгруппа группы G (группы A) имеет мощность, не превосходящую мощности D. Значит, существует вложение $\varphi_1 : B \to D_1$, где $D = D_1 \oplus D_2 \oplus D_3$, где $|D| = |D_1| = |D_2| = |D_3|$. Это вложение мы зафиксируем, после чего можно будет считать группу B подгруппой группы D_1. Кроме того, из $|G| \leqslant |D|$ следует, что $|G/B| \leqslant |D|$, поэтому существует вложение $\varphi_2 : G/B \to D_2$ (т. е. отображение из G в D_2, равное нулю на B). Значит, группу G/B мы также можем считать подгруппой в D_2.

Теперь выделим формульные множества:

1) множество $\mathbf{F}_1$ из $|B|$ независимых неразложимых проекторов на квазициклические прямые слагаемые в минимальном прямом слагаемом в D_1, содержащем $\varphi_1(B)$ в качестве подгруппы;

2) множество $\mathbf{F}_2$ из $|G/B|$ независимых неразложимых проекторов на квазициклические прямые слагаемые из $\varphi_2(G/B)$;

3) множества $\mathbf{F}$ и $\mathbf{F}_3$ из $\mu = |D|$ независимых проекторов на квазициклические прямые слагаемые групп D и D_3 соответственно;

4) множество $\mathbf{F}'$ из μ независимых проекторов на счетно порожденные прямые слагаемые группы D.

Для каждого $g \in \mathbf{F}'$ интерпретация группы A будет построена следующим образом: мы рассмотрим гомоморфизмы $h : gA \to A$ такие, что образы подгрупп Fa ($f \in \mathbf{F}$, $fA \subset gA$) либо нулевые, либо попадают в $f'A$ ($f' \in \mathbf{F}_1 \cup \mathbf{F}_2 \cup \mathbf{F}_3$), причем $h(gA)$ конечномерно.

Прообразы группы fA, $f \in \mathbf{F}_1$, будут интерпретировать слагаемые из B в разложении элемента $a \in A$ в квазибазис; прообразы групп fA, $f \in \mathbf{F}_2$, — слагаемые из G/B, т. е. $c_{i,j}$ для $i \in \omega$, $j \in |G/B|$, прообразы групп fA, $f \in \mathbf{F}_3$, — слагаемые из D. Дальнейшая процедура аналогична тому, что делалось в предыдущих параграфах.

Таким образом, мы дали схему доказательства следующего предложения:

Предложение 4.16. *Пусть* $A_1 = D_1 \oplus G_1$, $A_2 = D_2 \oplus G_2$, *где группы* D_1, D_2 *делимы, группы* G_1, G_2 *редуцированны,* $|D_1| \geqslant |G_1|$, $|D_2| \geqslant |G_2|$. *Тогда* $\mathrm{End}\,(A_1) \equiv \mathrm{End}\,(A_2) \Rightarrow A_1 \equiv_{\mathcal{L}_2} A_2$.

На протяжении этого пункта мы будем считать, что $A = D \oplus G$, $|D| < |G|$.

2. $A = D \oplus G$, $|D| < |G|$, B — базисная подгруппа в G, $r(B) = r_{fin}(B)$.

Сначала мы рассматриваем случай $r_{fin}(B) > \omega$, потом — случай $r_{fin} = \omega$.

Если $r(B) > \omega$, то $|A| = r(B)$, $|D| < r(B)$. Если же $r(B) = \omega$, то $|A| \leqslant |\mathcal{P}(\omega)|$, поэтому, в случае, если мы не принимаем континуум-гипотезу, то может возникнуть ситуация, когда $\omega < |D| < |A| \leqslant 2^\omega$, которая нам нежелательна. Поэтому для простоты рассуждений примем континнум-гипотезу.

Таким образом, если $A = D \oplus G$, где $|D| < |G|$, $r(B) = r_{fin}(B)$, то мы будем интерпретировать в кольце $\mathrm{End}\,(A)$ теорию $Th_2^{r(B)}(A)$.

3. $A = D \oplus G$, $|D| < |G|$, $r(B) \neq r_{fin}(B)$. Если в этом случае $r_{fin}(B) > \omega$, то мы можем получить полную теорию второго порядка группы A.

Если $r_{fin}(B) = \omega$, то, в предположении континуум-гипотезы, в группе A можно выделить ограниченное прямое слагаемое мощности A, и в этом случае можно выделить полную теорию второго порядка группы A.

В следующих подпунктах мы рассмотрим выделение формульных объектов, важных для всех случаев.

Выделение формульных объектов

Всегда далее в этом пункте мы будем предполагать, что $A = D \oplus G$, группа D делима (она может быть нулевой), группа G редуцирована и имеет неограниченную базисную подгруппу B,

$$B = B_1 \oplus \dots \oplus B_n \oplus \dots,$$

где

$$B_n \cong \bigoplus_{\mu_n} \mathbb{Z}(p^n),$$

$r(D) = \mu_D$, $|B| = \bigcup\limits_{n \in \mathbb{N}} \mu_n = \mu_B$, $|G| = \mu_G$ (при $\mu_B > \omega$ всегда $\mu_G = \mu_B$), $\mu = |A| = \max(\mu_D, \mu_G)$.

Мы считаем фиксированными проекции ρ_D и ρ_G на слагаемые D и G группы A, соответственно.

Через Z будем обозначать центр кольца $\mathrm{End}\,(A)$. Как мы помним (см. теорему 2.12), он состоит из умножения группы A на целые p-адические числа.

Для любых неразложимых проекторов ρ_1 и ρ_2 в группе G будем писать $o(\rho_1) \leqslant o(\rho_2)$, если

$$\forall c \in Z (c\rho_2 = 0 \Rightarrow c\rho_1 = 0).$$

Очевидно, эта формула равносильна тому, что порядок конечного циклического прямого слагаемого $\rho_1 A$ не больше порядка слагаемого $\rho_2 A$.

Аналогично,

$$(o(\rho_1) < o(\rho_2)) := (o(\rho_1) \leqslant o(\rho_2)) \wedge \neg(o(\rho_2) \leqslant o(\rho_1)),$$
$$(o(\rho_1) = o(\rho_2)) := (o(\rho_1) \leqslant o(\rho_2)) \wedge (o(\rho_2) \leqslant o(\rho_1)).$$

Для каждой неразложимой проекции ρ рассмотрим следующие формульные множества:

1. Формула

$$Ord_\rho(f) := Idem(f) \wedge \forall f'(Idem^*(f') \wedge f'f = f' \Rightarrow o(f') = o(\rho))$$

выделяет проекторы f на прямые слагаемые fA в A, являющиеся прямыми суммами циклических групп порядка $o(\rho A)$.

2. Формула

$$MaxOrd_\rho(f) := Idem(f) \wedge Ord_\rho(f) \wedge \forall f'(Ord_\rho(f') \Rightarrow \neg(ff' = f))$$

выделяет проекторы f на максимальные прямые слагаемые fA в A, являющиеся прямыми суммами циклических групп порядка $o(\rho A)$.

3. Формула

$$Rest_\rho(f) := Idem(f) \wedge \forall f'(Idem^*(f') \wedge f'f = f' \Rightarrow o(f') \leqslant o(\rho))$$

выделяет проекторы f на прямые слагаемые fA в A, являющиеся прямыми суммами циклических групп порядка, не большего $o(\rho A)$.

4. Формула

$$MaxRest_\rho(f) := Idem(f) \wedge Ord_\rho(f) \wedge \forall f'(Ord_\rho(f') \Rightarrow \neg(ff' = f))$$

выделяет проекторы f на максимальные прямые слагаемые fA в A, являющиеся прямыми суммами циклических групп порядка, не большего $o(\rho A)$.

5. Формула

$$\begin{aligned}\overline{Base}(\varphi) := \forall \rho \exists f(MaxRest_\rho(f) \wedge \forall f'(Idem^*(f') \Rightarrow \\ \Rightarrow (f'f = f' \Leftrightarrow \forall c \in Z(cf' \neq 0 \Rightarrow c(f'\varphi) \neq 0)))\end{aligned}$$

утверждает, что для каждого натурального числа n существует некоторое максимальное p^n-ограниченное прямое слагаемое группы A, принадлежащее φA. Таким образом, группа φA обязательно должна содержать некоторую базисную подгруппу группы A.

6. Формула

$$\begin{aligned}Base(\varphi) := \overline{Base}(\varphi) \wedge \forall f^*(Idem^*(f^*) \wedge f^*\varphi \neq 0 \Rightarrow \exists \rho \exists f(MaxRest_\rho(f) \wedge \\ \wedge \forall f'(Idem^*(f') \Rightarrow (f'f = f' \Leftrightarrow \forall c \in Z(cf' \neq 0 \Rightarrow c(f\varphi) \neq 0))) \wedge f^*f = f^*)).\end{aligned}$$

выполняется для тех эндоморфизмов $\varphi \in \mathrm{End}\,(A)$, образ которых — базисная подгруппа в A.

Будем считать, что эндоморфизм φ_B такой, что $Base(\varphi_B)$, фиксирован.

Выделение специальных множеств

Рассмотрим два различных случая:
1) $\mu_B = \omega$;
2) $\mu_B > \omega$.
Случай 1. $\mu_B = \omega$.
Рассмотрим формулу

$$\begin{gathered}
Intr(f) := [\forall f'(Idem(f') \wedge f'\varphi_B \neq 0 \Rightarrow f'f \neq 0)] \wedge \\
\wedge [\forall f_1 \forall f_2 (Idem^*(f_1) \wedge Idem^*(f_2) \wedge o(f_1) = o(f_2) \wedge \\
\wedge \forall c \in Z(cf_1 \neq 0 \Rightarrow cf_1 f \neq 0) \wedge \forall c \in Z(cf_2 \neq 0 \Rightarrow cf_2 f \neq 0) \Rightarrow f_1 f_2 \neq 0 \wedge f_2 f_1 \neq 0)] \wedge \\
\wedge [\forall \rho'(Idem^*(\rho') \Rightarrow \exists f'(Idem^*(f') \wedge o(f') > o(\rho') \wedge \\
\wedge \forall c \in Z(cf' \neq 0 \Rightarrow cf'f \neq 0)))].
\end{gathered}$$

Первая часть формулы, заключенная в квадратные скобки, утверждает, что $fA \subset \varphi_B A = B$. Вторая часть, заключенная в квадратные скобки, утверждает, что в образе fA содержится не более одного циклического прямого слагаемого одного порядка. Третья часть утверждает, что порядок прямых слагаемых в fA неограничен.

Эта формула, таким образом, дает нам эндоморфизм f, образ которого B' есть циклическое прямое слагаемое в B,

$$B' \cong \bigoplus_{i \in \mathbb{N}} \mathbb{Z}(p^{n_i}),$$

где (n_i) — возрастающая по i последовательность.

Этот эндоморфизм можно считать фиксированным и обозначать через f_B.

Теперь мы будем рассматривать эндоморфизмы из B' в A. Именно, будем рассматривать только функции f с условием

$$\forall \rho(Idem(\rho) \wedge \rho f_B = 0 \Rightarrow \rho f = 0).$$

Две функции f_1 и f_2, удовлетворяющие этому условию, мы будем считать равными, если

$$\forall \rho(Idem^*(\rho) \wedge \forall c \in Z(c\rho \neq 0 \Rightarrow c\rho f \neq 0) \Rightarrow f_1 \rho = f_2 \rho),$$

т. е. если они совпадают на группе B'.

Следовательно, профакторизовав множество всех описанных функций по этому равенству, мы получим группу $Hom(B', A)$.

Введем теперь формулу

$$o(\rho_1) \geqslant o(\rho_2)^2.$$

для неразложимых идемпотентов ρ_1 и ρ_2 следующим образом:

$$\forall c \in Z(c\rho_2 \neq 0 \Rightarrow c^2 \rho_1 \neq 0).$$

Эта формула означает, что $|\rho_1 A| \geqslant |\rho_2 A|^2$.

Аналогичным образом можно ввести формулы

$$o(\rho_1) > o(\rho_2)^2 \text{ и } o(\rho_1) = o(\rho_2)^2.$$

Пусть наша функция f_B удовлетворяет дополнительному условию

$$\begin{aligned}\forall f'(Idem^*(f') \wedge \forall c \in Z(cf' \neq 0 \Rightarrow cf'f_B \neq 0) \Rightarrow pf' \neq 0)\wedge \\ \wedge \forall\rho'\forall f'(Idem^*(f') \wedge \forall c \in Z(cf' \neq 0 \Rightarrow cf'f_B \neq 0) \wedge o(f') = o(\rho') \Rightarrow \\ \Rightarrow \forall f(Idem^*(f) \wedge \forall c \in Z(cf \neq 0 \Rightarrow cff_B \neq 0)\wedge \\ \wedge o(f) > o(\rho') \Rightarrow o(f) > o(\rho')^2)).\end{aligned}$$

Этим условием мы гарантируем, что:

1) циклическое прямое слагаемое в B' самого маленького порядка имеет порядок, бóльший p (т. е. по крайней мере не мéньший p^2);

2) для любого прямого циклического слагаемого в B' порядка p^k следующее за ним циклическое слагаемое бóльшего порядка имеет порядок, бóльший p^{2k}.

Таким образом,

$$B' \cong \bigoplus_{i\in\omega} \mathbf{Z}(p^{n_i}),$$

где $n_1 \geqslant 2$, $n_{i+1} > 2n_i$.

Теперь рассмотрим формулу

$$\begin{aligned}Ins(\psi) := [\exists f(Idem^*(f) \wedge \forall c \in Z(cf \neq 0 \Rightarrow cff_B \neq 0)\wedge \\ \wedge \forall f'(Idem^*(f') \wedge \forall c \in Z(cf' \neq 0 \Rightarrow cf'f_B \neq 0) \Rightarrow \\ \Rightarrow o(f) \leqslant o(f')) \wedge \psi f = pf)]\wedge \\ \wedge [\forall f_1 \forall c_1 \in Z(Idem^*(f_1) \wedge \forall c \in Z(cf_1 \neq 0 \Rightarrow cf_1f_B \neq 0) \wedge (\psi f_1 = c_1 f_1 \Rightarrow \\ \Rightarrow \exists f_2(Idem^*(f_2) \wedge \forall c \in Z(cf_2 \neq 0 \Rightarrow cf_2f_B \neq 0) \wedge o(f_2) > o(f_1)\wedge \\ \wedge \forall f'(Idem^*(f') \wedge \forall c \in Z(cf' \neq 0 \Rightarrow cf'f_B \neq 0) \Rightarrow \\ \Rightarrow o(f') \leqslant o(f_1) \vee o(f') \geqslant o(f_2)) \wedge \psi f_2 = pc_1 f_2))].\end{aligned}$$

Условие, заключенное в первые квадратные скобки, утверждает, что существует прямое циклическое слагаемое самого маленького порядка, на котором действие эндоморфизма ψ есть умножение на p. Условие, заключенное во вторые квадратные скобки, утверждает, что для каждого натурального i существует прямое циклическое слагаемое $\langle a_i\rangle$ порядка p^{n_i}, на котором ψ есть умножение на p^i.

Пусть для некоторых двух несовпадающих циклических прямых слагаемых $\langle a_i\rangle$ и $\langle b_i\rangle$ в B' действие ψ на них есть умножение на p^i. Пусть $b_i = \sum \alpha_k a_k + \sum \beta_l a_l + a_i$, где $o(a_k) < o(b_i)$, $o(a_l) > o(b_i)$, $k < i$, $l > i$,

$$\psi(b_i) = p^i b_i = \sum p^k \alpha_k a_k + \sum p^l \beta_l a_l + p^i a_i = \sum p^i \alpha_k a_k + \sum p^i \beta_l a_l + p^i a_i.$$

Пусть $k < i$. Тогда должно быть $p^i \alpha_k a_k = p_k \alpha_k a_k = 0$, т. е. α_k делится на $p^{n_k - k}$, которое, в свою очередь, делится на p^k. Значит, можно написать

$$b_i = \sum \alpha_k p^k a_k + \sum \beta_k p^{n_l - n_i} a_l + a_i.$$

Мы имеем $p^i\beta_l p^{n_l-n_i}a_l = p^l\beta_l p^{n_l-n_i}a_l = 0$. Заметим, что любому циклическому прямому слагаемому $\langle a\rangle$ либо можно однозначно сопоставить элемент центра кольца $c \in Z$ такой, что $\psi a = ca$, либо такого элемента нет. Мы будем рассматривать только те слагаемые, которым сопоставляется элемент центра.

Пусть имеется некоторый гомоморфизм $f : B' \to A$ такой, что $o(f(a_i)) \leqslant p^i$. Пусть $\psi(a_i) = p^i a_i$, $\psi(b_i) = p^i b_i$. Найдем $f(b_i)$:

$$f(b_i) = \sum \alpha_k p^k f(a_k) + \sum \beta_l p^{n_l-n_i} f(a_l) + f(a_i).$$

Так как $o(f(a_k)) \leqslant p^k$, то $\sum \alpha_k p^k f(a_k) = 0$. Так как $o(f(a_l)) \leqslant p^l$, то $\sum \beta_l p^{n_l-n_i} f(a_l) = 0$. Значит, $f(b_i) = f(a_i)$. Значит, каждому элементу центра Z вида $p^n \cdot E$ соответствует при данному гомоморфизме $f : B' \to A$ некоторый однозначно определенный элемент $a \in A$ с условием $o(a) \leqslant p^n$.

Случай 2. $\forall k \in \omega \exists n \in \omega (n > k \wedge \mu_n = \mu_B)$.

Рассмотрим формулу

$$\begin{aligned} ECard(\rho) := Idem^*(\rho) \wedge \exists\psi\forall f(Idem^*(f) \wedge \forall c \in Z(cf \neq 0 \Rightarrow cf\varphi_B \neq 0) \Rightarrow \\ \Rightarrow \exists f'(Idem^*(f') \wedge \forall c \in Z(cf' \neq 0 \Rightarrow cf'\varphi_B \neq 0) \wedge \\ \wedge\, o(f') = o(\rho) \wedge f\psi f' \neq 0)). \end{aligned}$$

Эта формула утверждает, что множество независимых циклических слагаемых порядка $o(\rho)$ равномощно всей группе B, так как существует гомоморфизм ψ из прямого слагаемого группы B, равного сумме циклических групп порядка $o(\rho)$ такой, что его образ пересекается с каждым циклическим слагаемым в B. Значит, $\mu_{o(\rho)} = \mu_B$.

Теперь рассмотрим формулу

$$\begin{aligned} Fine(f) := [\forall f'(Idem(f') \wedge f'\varphi_B \neq 0 \Rightarrow f'f \neq 0)] \wedge \\ \wedge [\forall f_1 \forall f_2 (Idem^*(f_1) \wedge Idem^*(f_2) \wedge o(f_1) = o(f_2) \wedge \\ \wedge \forall c \in Z(cf_1 \neq 0 \Rightarrow cf_1 f \neq 0) \wedge \forall c \in Z(cf_2 \neq 0 \Rightarrow cf_2 f \neq 0) \Rightarrow f_1 f_2 \neq 0 \wedge f_2 f_1 \neq 0)] \wedge \\ \wedge [\forall \rho'(ECard(\rho') \Leftrightarrow \exists f'(Idem^*(f') \wedge o(f') = o(\rho') \wedge \forall c \in Z(cf' \neq 0 \Rightarrow cf'f \neq 0)))]. \end{aligned}$$

Первая часть формулы, заключенная в квадратные скобки, утверждает, что $fA \subset \varphi_B A = B$. Вторая часть, заключенная в квадратные скобки, утверждает, что в образе fA содержится не более одного циклического прямого слагаемого одного порядка. Третья часть утверждает, что все прямые циклические слагаемые имеют порядок p^n, где $\mu_n = \mu_B$.

Аналогично предыдущим пунктам мы можем считать, что имеем формулу (с параметрами), истинную для независимого множества проекторов f, удовлетворяющих формуле $Fine(f)$, мощности μ_B. Значит, мы можем считать, что имеем множество проекторов на μ_B независимых прямых слагаемых группы B, изоморфных группе

$$\bigoplus_{i\in\omega} \mathbb{Z}(p^{n_i}).$$

Это множество будем обозначать через $\mathbf{F}$.

Случай, когда финальный ранг базисной подгруппы несчетен

Немного исправим формулу $Fine(f)$:

$$\begin{gathered}Fine(f) := [\forall f'(Idem(f') \wedge f'\varphi_B \neq 0 \Rightarrow f'f \neq 0)] \wedge \\ \wedge [\forall f_1 \forall f_2 (Idem^*(f_1) \wedge Idem^*(f_2) \wedge o(f_1) = o(f_2) \wedge \\ \wedge \forall c \in Z(cf_1 \neq 0 \Rightarrow cf_1 f \neq 0) \wedge \forall c \in Z(cf_2 \neq 0 \Rightarrow cff_2 \neq 0) \Rightarrow f_1 f_2 \neq 0 \wedge f_2 f_1 \neq 0)] \wedge \\ \wedge [\forall \rho'(Idem^*(\rho') \Rightarrow \exists f'(Idem^*(f') \wedge o(f') > o(\rho') \wedge \\ \wedge \forall c \in Z(cf' \neq 0 \Rightarrow cf'f \neq 0)))] \wedge [\forall f'(Idem^*(f') \wedge \\ \wedge \forall c \in Z(cf' \neq 0 \Rightarrow cf'f_B \neq 0) \Rightarrow pf' \neq 0)] \wedge \\ \wedge [\forall \rho' \forall f'(Idem^*(f') \wedge \forall c \in Z(cf' \neq 0 \Rightarrow cf'f_B \neq 0) \wedge o(f') = o(\rho') \Rightarrow \\ \Rightarrow \forall f(Idem^*(f) \wedge \forall c \in Z(cf \neq 0 \Rightarrow cff_B \neq 0) \wedge o(f) > o(\rho') \Rightarrow o(f) > o(\rho')^2))].\end{gathered}$$

Первая часть формулы, заключенная в квадратные скобки, утверждает, что $fA \subset \varphi_B A = B$. Вторая часть, заключенная в квадратные скобки, утверждает, что в образе fA содержится не более одного циклического прямого слагаемого одного порядка. Третья часть утверждает, что порядок прямых слагаемых в fA неограничен. Четвертая часть утверждает, что циклическое прямое слагаемое в fA самого маленького порядка имеет порядок, бо́льший p (т. е. по крайней мере не ме́ньший p^2). Наконец, пятая часть утверждает, что для любого прямого циклического слагаемого в fA порядка p^k следующее за ним циклическое слагаемое бо́льшего порядка имеет порядок, бо́льший p^{2k}.

Снова напишем формулу $Ins(\psi)$, утверждающую, что 1) для каждой группы fA, где $f \in \mathbf{F}$, существует прямое циклическое слагаемое самого маленького порядка, на котором действие эндоморфизма ψ есть умножение на p; 2) для каждого натурального i и каждого $f \in \mathbf{F}$ существует прямое циклическое слагаемое $\langle a_i \rangle \subset fA$ порядка p^{n_i}, на котором ψ есть умножение на p^i.

Фиксируем некоторый эндоморфизм Ψ, удовлетворяющий формуле $Intr(\Psi)$.

Кроме того, фиксируем эндоморфизм $\Gamma : B' \to B'$, удовлетворяющий для каждого $f \in \mathbf{F}$ следующим условиям:

1) $f\Gamma f = f\Gamma = \Gamma f$, т. е. эндоморфизм Γ переводит fA в fA;

2) $\forall \rho(Idem^*(\rho) \wedge \rho f = \rho \wedge \forall \rho'(Idem^*(\rho') \wedge \rho' f = \rho' \Rightarrow o(\rho') \geqslant o(\rho)) \Rightarrow \Gamma\rho = 0)$, т. е. эндоморфизм Γ переводит циклические слагаемые наименьшего порядка в группе fA в ноль;

3) $\forall \rho_1(Idem^*(\rho_1) \wedge \rho_1 f = \rho_1 \Rightarrow \exists \rho_2(Idem^*(\rho_2) \wedge \rho_2 f = \rho_2 \wedge o(\rho_1) < o(\rho_2) \wedge \forall \rho(Idem^*(\rho) \wedge \rho f = \rho \Rightarrow \neg(o(\rho) > o(\rho_1) \wedge o(\rho) < o(\rho_2))) \wedge \rho_1 \Gamma \rho_2 = \Gamma \rho_2 \wedge \forall c \in Z(c\rho_1 \neq 0 \Rightarrow c\rho_1 \Gamma \rho_2 \neq 0)))$, что означает, что эндоморфизм Γ переводит каждую образующую a_i циклического прямого слагаемого группы fA, изоморфного $\mathbb{Z}(p^{n_i})$ в образующую a_{i-1} циклического прямого слагаемого группы fA, изоморфного $\mathbb{Z}(p^{n_{i-1}})$.

Этот эндоморфизм дает нам соответствие между образующими циклических слагаемых в группе fA для каждого $f \in \mathbf{F}$. Мы будем считать его фиксированным.

Предположим сначала для простоты, что финальный ранг базисной подгруппы группы A совпадает с ее рангом, и что он несчетен. Тогда $|A| = |B| = \mu$. Мы считаем фиксированным множество $\mathbf{F}$, состоящее из μ независимых проекторов на прямые слагаемые группы B, изоморфные

$$\bigoplus_{i\in\omega}\mathbb{Z}(p^{n_i}),$$

где последовательность (n_i) такова, что $n_1 \geqslant 2$, $n_{i+1} > 2n_i$. Фиксируем $f \in \mathbf{F}$ и интерпретируем для него группу A.

Рассмотрим множество End_f всех гомоморфизмов $h : fA \to A$, удовлетворяющих следующему условию:

$$\begin{aligned}&\exists\rho(Idem^*(\rho)\wedge\exists c\in Z(\Psi\rho=c\rho)\wedge\\ &\qquad\rho f=\rho\wedge\forall\rho'(Idem^*(\rho')\wedge\exists c\in Z(\Psi\rho'=c\rho')\wedge\rho' f=\rho'\wedge\\ &\qquad\qquad\wedge(o(\rho')<o(\rho)\vee o(\rho')>o(\rho))\Rightarrow h\rho'=0)\wedge\\ &\qquad\qquad\qquad\wedge\forall c\in Z(\Psi\rho=c\rho\Rightarrow pch\rho=0)).\end{aligned}$$

Это условие означает, что:

1) существует такое $i \in \omega$, что $h(a_k) = 0$ для любого $k \neq i$;

2) $o(h(a_i)) \leqslant p^i$.

Естественно, два таких гомоморфизма должны считаться эквивалентными, если они совпадают с точностью до выбора числа i.

Поэтому два гомоморфизма h_1 и h_2 из End_f мы будем считать эквивалентными, если существует гомоморфизм h, удовлетворяющий следующим двум условиям:

1) $\forall\rho(Idem^*(\rho)\wedge\rho f=\rho\wedge\exists c\in Z(\Psi\rho=c\rho)\wedge h_1\rho\neq 0\Rightarrow h\rho=h_1\rho)\wedge\forall\rho(Idem^*(\rho)\wedge\rho f=\rho\wedge\exists c\in Z(\Psi\rho=c\rho)\wedge h_2\rho\neq 0\Rightarrow h\rho=h_2\rho)$, что означает, что гомоморфизм h совпадает с h_1 на том a_i, на котором $h_1(a_i)\neq 0$, и совпадает с h_2 на том a_j, на котором $h_2(a_j)\neq 0$;

2) $\forall\rho(Idem^*(\rho)\wedge\rho f=\rho\wedge\exists c\in Z(\Psi\rho=c\rho)\wedge\exists\rho_1\exists\rho_2(Idem^*(\rho_1)\wedge Idem^*(\rho_2)\wedge\rho_1 f=\rho_1\wedge\rho_2 f=\rho_2\wedge\exists c_1\in Z(\Psi\rho_1=c_1\rho_1)\wedge\exists c_2\in Z(\Psi\rho_2=c_2\rho_2)\wedge h_1\rho_1\neq 0\wedge h_2\rho_2\neq 0\wedge o(\rho)>o(\rho_1)\wedge o(\rho)\leqslant o(\rho_2))\Rightarrow h\Gamma\rho=h\rho)$, что означает, что $h(a_j)=h(a_{j-1})=\cdots=h(a_{i+1})=h(a_i)$.

Отсюда следует, что $h_1(a_i)=h(a_i)=h(a_j)=h_2(a_j)$, что нам и требовалось.

Теперь профакторизуем множество End_f по этой эквивалентности и получим множество $\widetilde{End_f}$. Биекция между этим множеством и группой A очевидна. Нам осталось ввести сложение. Именно,

$$\begin{aligned}&(h_3=h_1\oplus h_2):=\exists h_1'\exists h_2'(h_1'\sim h_1\wedge h_2'\sim h_2\wedge\\ &\qquad h_3=h_1+h_2\wedge\forall\rho(Idem^*(\rho)\wedge\rho f=\rho\wedge\forall c\in Z(\Psi\rho=c\rho)\Rightarrow\\ &\qquad\qquad\Rightarrow(h_1\rho=0\Leftrightarrow h_2\rho=0))).\end{aligned}$$

Теперь, когда мы интерпретировали группу A для каждого $f \in \mathbf{F}$, нам нужно доказать основную теорему для этого случая:

Предложение 4.17. *Пусть p-группы A_1 и A_2 являются прямыми суммами $D_1 \oplus G_1$ и $D_1 \oplus G_2$, где группы D_1 и D_2 делимы, группы G_1 и G_2 редуцированны и неограниченны, $|D_1| \leqslant |G_1|$, $|D_2| \leqslant |G_2|$, B_1 и B_2 — базисные подгруппы групп A_1 и A_2 соответственно, финальные ранги групп B_1 и B_2 совпадают с их рангами и несчетны. Тогда из элементарной эквивалентности колец* $\operatorname{End}(A_1)$ *и* $\operatorname{End}(A_2)$ *следует эквивалентность групп A_1 и A_2 в языке $\mathcal{L}_2$.*

Доказательство. Как всегда, рассмотрим произвольное предложение ψ группового языка второго порядка и укажем алгоритм, переводящий это предложение ψ в предложение $\widetilde{\psi}$ кольцевого языка первого порядка такое, что $\widetilde{\psi}$ выполняется в $\mathrm{End}\,(A)$ тогда и только тогда, когда ψ выполняется в A.

Рассмотрим формулу

$$\begin{aligned} Min(f) := f \in \mathbf{F} \wedge \forall f'(f' \in \mathbf{F} \Rightarrow \\ \Rightarrow \forall c \forall \rho' \forall \rho (c \in Z \wedge Idem^*(\rho') \wedge Idem^*(\rho) \wedge \\ \wedge \rho f = \rho \wedge \rho' f' = \rho' \wedge \Psi \rho' = c\rho' \wedge \Psi\rho = c\rho \Rightarrow o(\rho) \leqslant o(\rho'))). \end{aligned}$$

Эта формула выделяет нам такое слагаемое $f(A)$ в B, что для каждого $i \in \omega$ $n_i(f)$ минимально из всех $n_i(f')$ для $f' \in \mathbf{F}$.

Рассмотрим формулу

$$\begin{aligned} Basic(\Lambda) := \exists f(f \in \mathbf{F} \wedge Min(f) \wedge \\ \wedge \forall f' \forall c \forall \rho'(f' \in \mathbf{F} \wedge c \in Z \wedge Idem^*(\rho') \wedge \rho' f' = \rho' \wedge \\ \wedge \Psi\rho' = c\rho' \Rightarrow \exists \rho(Idem^*(\rho) \wedge \rho f = \rho \wedge \Psi\rho = c\rho \wedge \\ \wedge \rho\Lambda\rho' = \Lambda\rho' \wedge \forall c' \in Z(c\rho \neq 0 \Rightarrow c\rho\Lambda\rho' \neq 0)))). \end{aligned}$$

Эта формула задает эндоморфизм Λ, переводящий a_t^i в a_0^i для каждого $i \in \omega$ и каждого $t \in \mu$.

Такой эндоморфизм и соответствующее f_0 обозначим через Λ и f_{min} соответственно.

Переведем предложение ψ в предложение

$$\widetilde{\psi} := \exists \overline{g} \exists \Gamma \exists \Psi \exists \Lambda \exists f_{min} \in \mathbf{F} \psi'(\overline{g}, \Gamma, \Psi, \Lambda, f_{min}),$$

где формула $\psi'(\dots)$ получается из предложения ψ с помощью следующих замен подформул, входящих в ψ:

1) подформула $\forall x$ заменяется на подформулу $\forall x \in \widetilde{End_{f_{min}}}$;

2) подформула $\exists x$ заменяется на подформулу $\exists x \in \widetilde{End_{f_{min}}}$;

3) подформула $\forall P_m(v_1, \dots, v_m)(\dots)$ заменяется на подформулу

$$\forall f_1^P \dots \forall f_m^P (\forall g \in \mathbf{F}(\bigwedge_{i=1}^{m}(f_i^P g \in End_g)) \Rightarrow \dots);$$

4) подформула $\exists P_m(v_1, \dots, v_m)(\dots)$ заменяется на подформулу

$$\exists f_1^P \dots \exists f_m^P (\forall g \in \mathbf{F}(\bigwedge_{i=1}^{m}(f_i^P g \in End_g)) \wedge \dots);$$

5) подформула $x_1 = x_2$ заменяется на подформулу $x_1 \sim x_2$;

6) подформула $x_1 = x_2 + x_3$ заменяется на подформулу $x_1 \sim x_2 \oplus x_3$;

7) подформула $P_m(x_1, \dots, x_m)$ заменяется на подформулу

$$\exists g \in \mathbf{F}(\bigwedge_{i=1}^{m}(f_i^P g) = x_i \Lambda g).$$

Далее доказательство аналогично предыдущим. □

Теперь перейдем к случаю, когда финальный ранг группы B, бо́льший ω, не совпадает с ее рангом.

В этом случае $A = G \oplus G'$, где группа G удовлетворяет условиям предыдущего предложения, а группа G' ограничена и имеет бо́льшую, чем у G мощность. Пусть $|G| = \mu$, $|A| = |G'| = \mu'$.

Тогда выделим множество $\mathbf{F}$ для группы G, о котором говорится в предложении 4.17, и множество $\mathbf{F}'$, состоящее из μ' независимых проекторов на счетно порожденные подгруппы группы G'.

Формула

$$Add(\varphi) := \forall f' \in \mathbf{F}' \exists f \in \mathbf{F} \forall \rho' (Idem^*(\rho') \wedge \rho' f' = \rho' \Rightarrow \\ \Rightarrow \exists \rho (Idem^*(\rho) \wedge \rho f = \rho \wedge \varphi \rho' = \rho \varphi \rho' \neq 0))$$

задает функцию из множества $\mathbf{F}'$ на множество $\mathbf{F}$.

Предложение 4.18. *Пусть p-группы A_1 и A_2 являются прямыми суммами $D_1 \oplus G_1$ и $D_1 \oplus G_2$, где группы D_1 и D_2 делимы, группы G_1 и G_2 редуцированны и неограниченны, $|D_1| < |G_1|$, $|D_2| < |G_2|$, B_1 и B_2 — базисные подгруппы групп A_1 и A_2 соответственно, финальные ранги групп B_1 и B_2 не совпадают с их рангами и несчетны. Тогда из элементарной эквивалентности колец* $\mathrm{End}\,(A_1)$ *и* $\mathrm{End}\,(A_2)$ *следует эквивалентность групп A_1 и A_2 в языке $\mathcal{L}_2$.*

Доказательство. Сразу напишем алгоритм перевода формул:

заменим предложение ψ на предложение

$$\widetilde{\psi} := \exists \overline{g} \exists \Gamma \exists \Psi \exists \Lambda \exists f_{min} \in \mathbf{F} \exists \overline{g}_1 \ldots \exists \overline{g}_k \exists \overline{g}' \exists \widetilde{g} \in \mathbf{F}' \psi'(\overline{g}, \Gamma, \Psi, \Lambda, f_{min}),$$

где формула $\psi'(\ldots)$ получается из предложения ψ с помощью следующих замен подформул, входящих в ψ:

1) подформула $\forall x$ заменяется на подформулу $\forall x \in \widetilde{End}_{f_{min}} \forall x' \in \widetilde{End}_{\widetilde{g}}$;

2) подформула $\exists x$ заменяется на подформулу $\exists x \in \widetilde{End}_{f_{min}} \exists x' \in \widetilde{End}_{\widetilde{g}}$;

3) подформула $\forall P_m(v_1, \ldots, v_m)(\ldots)$ заменяется на подформулу

$$\forall f_1^P \ldots \forall f_m^P \forall f_1^{P'} \ldots \forall f_m^{P'} \forall \varphi_1^P \ldots \forall \varphi_m^P (\bigwedge_{i=1}^m Add(\varphi_i^P) \wedge \\ \wedge \forall g \in \mathbf{F}(\bigwedge_{i=1}^m f_i^P g \in End_g) \wedge \forall g \in \mathbf{F}'(\bigwedge_{i=1}^m f_i^{P'} g \in End_g) \Rightarrow \ldots);$$

4) подформула $\exists P_m(v_1, \ldots, v_m)(\ldots)$ заменяется на подформулу

$$\exists f_1^P \ldots \exists f_m^P \exists f_1^{P'} \ldots \exists f_m^{P'} \exists \varphi_1^P \ldots \exists \varphi_m^P (\bigwedge_{i=1}^m Add(\varphi_i^P) \wedge \\ \wedge \forall g \in \mathbf{F}(\bigwedge_{i=1}^m f_i^P g \in End_g) \wedge \forall g \in \mathbf{F}'(\bigwedge_{i=1}^m f_i^{P'} g \in End_g) \wedge \ldots);$$

5) подформула $x_1 = x_2$ заменяется на подформулу $x_1 \sim x_2 \wedge x_1' \sim x_2'$;
6) подформула $x_1 = x_2 + x_3$ заменяется на подформулу $x_1 \sim x_2 \oplus x_3 \wedge x_1' \sim x_2' \oplus x_3'$;
7) подформула $P_m(x_1, \dots, x_m)$ заменяется на подформулу

$$\exists g \in \mathbf{F} \exists g' \in \mathbf{F}' (\bigwedge_{i=1}^{m} (\varphi_i^P(g') = g \wedge (f_i^P g) = x_i \Lambda g \wedge f_i^{P'} g' = x_i' \widetilde{g} h)).$$

□

Выделение счетного ограничения теории второго порядка группы в случае, когда ранг базисной подгруппы счетен

Пусть группа A имеет счетную базисную подгруппу B. Мы, как и раньше, считаем фиксированным эндоморфизм φ_B с образом, совпадающим с группой B.

Кроме того, будем считать фиксированным эндоморфизм f_B, рассмотренный в этом пункте, и эндоморфизм Ψ, удовлетворяющий формуле $Ins(\Psi)$. Как мы помним,

$$B = \varphi_B(A) \supset B' = f_B(A) \cong \bigoplus_{i \in \omega} \mathbb{Z}(p^{n_i}),$$

где $n_0 \geqslant 2$, $n_{i+1} > 2n_i$. Образующие циклических слагаемых в $f_B(A)$, для которых $\Psi(a_i) = p^i a_i$, мы обозначаем через a_i $(i \in \omega)$.

Кроме того, как и в п. 7.4, фиксируем гомоморфизм $\Gamma : B' \to B'$, удовлетворяющий условиям

1) $\forall f(Idem^*(f) \wedge \forall c \in Z(cf \neq 0 \Rightarrow cff_B \neq 0) \Rightarrow f\Gamma f = f\Gamma = \Gamma f)$, т. е. $f \in End(B')$;

2) $\forall \rho(Idem^*(\rho) \wedge \forall c \in Z(c\rho \neq 0 \Rightarrow c\rho f_B \neq 0) \wedge \forall \rho'(Idem^*(\rho') \wedge \forall c \in Z(c\rho' \neq 0 \Rightarrow c\rho' f_B \neq 0) \Rightarrow o(\rho') \geqslant o(\rho)) \Rightarrow \Gamma\rho = 0)$, т. е. эндоморфизм Γ переводит циклические слагаемые наименьшего порядка в группе в 0;

3) $\forall \rho_1(Idem^*(\rho_1) \wedge \forall c \in Z(\rho_1 \neq 0 \Rightarrow c\rho_1 f_B \neq 0) \Rightarrow \exists \rho_2(Idem^*(\rho_2) \wedge \forall c \in Z(c\rho_2 \neq 0 \Rightarrow c\rho_2 f_B \neq 0) \wedge o(\rho_1) < o(\rho_2) \wedge \forall \rho(Idem^*(\rho) \wedge \forall c \in Z(c\rho \neq 0 \Rightarrow c\rho f_B \neq 0) \Rightarrow \neg(o(\rho) > o(\rho_2) \wedge o(\rho) < o(\rho_2))) \wedge \rho_1\Gamma = \Gamma\rho_2 = \rho_1\Gamma\rho_2 \wedge \forall c \in Z(c\rho_1 \neq 0 \Rightarrow c\rho_1\Gamma\rho_2 \neq 0)))$, т. е. Γ переводит каждую образующую a_i циклического прямого слагаемого группы B', изоморфного $\mathbb{Z}(p^{n_i})$, в образующую a_{i-1} циклического прямого слагаемого, изоморфного $\mathbb{Z}(p^{n_{i-1}})$.

Очевидно, что для интерпретации группы A для нашей функции f_B мы можем воспользоваться множествами End_{f_B} и $\widetilde{End}_{f_B}$ из предыдущего пункта. Таким образом, каждому элементу $a \in A$ соответствует класс гомоморфизмов $g : B' \to A$ с условием $g(a_i) = a$, $g(a_j) = 0$ при $j \neq i$, i таково, что $p^i \geqslant o(a)$.

Теперь предположим, что мы хотим интерпретировать в кольце $End(A)$ некоторое не более чем счетное множество $X = \{x_i\}_{i \in I} \subset A$. Очевидно, что существует некоторая последовательность (k_i), $i \in I$, и гомоморфизм $h : B' \to A$ такой, что

$$h(a_{k_i}) x_i, \quad i \in I,$$

и при этом $o(x_i) \leqslant p^{k_i}$. Ясно, что по гомоморфизму h и последовательности (k_i) множество $\{x_i\}$ восстанавливается однозначно. Значит, каждому множеству $\{x_i\}$ можно сопоставить пару эндоморфизмов, состоящую из проекции на подгруппу $\langle\{a_{k_i}|i \in I\}\rangle$ и гомоморфизма h.

Аналогично, любому n-мерному отношению на A соответствует проекция на $\langle\{a_{k_i}|i \in I\}\rangle$ и n-ка гомоморфизмов $h_1, \dots, h_n$.

Введем формулы

$$\begin{aligned}Proj(\rho) := \forall\rho'(Idem^*(\rho') \wedge \forall c \in Z(c\rho' \neq 0 \Rightarrow c\rho'\rho \neq 0) \Rightarrow \\ \Rightarrow \forall c \in Z(c\rho' \neq 0 \Rightarrow c\rho' f_B \neq 0) \wedge \exists\rho''(Idem^*(\rho'') \wedge \forall c \in Z(c\rho'' \neq 0 \Rightarrow c\rho''\rho \neq 0) \wedge \\ \wedge\, o(\rho'') = o(\rho') \wedge \exists c \in Z(\Psi\rho'' = c\rho'')) \wedge \exists c \in Z(\Psi\rho' = c\rho'))\end{aligned}$$

(проекция на прямое слагаемое в B', порожденное $\{a_{k_i}|i \in I\}$) и

$$\begin{aligned}Hom(h) := \forall\rho'(Idem^*(\rho') \wedge \forall c \in Z(c\rho' \neq 0 \Rightarrow c\rho' f_B \neq 0) \Rightarrow \\ \Rightarrow \exists c \in Z(\Psi\rho' = c\rho' \Rightarrow pch\rho' = 0)).\end{aligned}$$

Теперь мы готовы доказать следующее

Предложение 4.19. *Пусть p-группы A_1 и A_2 неограниченны и имеют счетные базисные подгруппы. Тогда из* $\mathrm{End}\,(A_1) \equiv \mathrm{End}\,(A_2)$ *следует* $Th_2^{\omega}(A_1) = Th_2^{\omega}(A_2)$.

Доказательство. Пусть мы имеем предложение $\psi \in Th_2^{\omega}(A_1)$. Тогда для каждого предиката $P_n(v_1, \dots, v_n)$, входящего в ψ, множество $\{\langle a_1, \dots, a_n\rangle \in A^n | P(a_1, \dots, a_n)\}$ не более чем счетно.

Укажем перевод предложения ψ в предложение $\widetilde{\psi}$ первого порядка, принадлежащее $Th_1(End(A_1))$.

Заменим предложение ψ на предложение

$$\widetilde{\psi} = \exists\varphi_B \exists f_B \exists\Psi\exists\Gamma\psi'(\varphi_B, f_B, \Psi, \Gamma),$$

где формула $\psi'(\dots)$ получается из предложения ψ с помощью следующих замен подформул, входящих в ψ:

1) подформула $\forall x$ заменяется на подформулу $\forall x \in \widetilde{End}_{f_B}$;

2) подформула $\exists x$ заменяется на подформулу $\exists x \in \widetilde{End}_{f_B}$;

3) подформула $\forall P_m(v_1, \dots, v_m)(\dots)$ заменяется на подформулу

$$\forall\rho^P \forall h_1^P \dots \forall h_m^P (Proj(\rho^P) \wedge Hom(h_1^P) \wedge \dots \wedge Hom(h_m^P) \Rightarrow \dots);$$

4) подформула $\exists P_m(v_1, \dots, v_m)(\dots)$ заменяется на подформулу

$$\exists\rho^P \exists h_1^P \dots \exists h_m^P (Proj(\rho^P) \wedge Hom(h_1^P) \wedge \dots \wedge Hom(h_m^P) \wedge \dots);$$

5) подформула $x_1 = x_2$ заменяется на подформулу $x_1 \sim x_2$;

6) подформула $x_1 = x_2 + x_3$ заменяется на подформулу $x_1 \sim x_2 \oplus x_3$;

7) подформула $P_m(x_1, \dots, x_m)$ заменяется на подформулу

$$\exists\rho(Idem^*(\rho) \wedge \rho\rho^P = \rho \wedge \exists c \in Z(\Psi\rho = c\rho) \wedge h_1^P\rho = x_1 \wedge \dots \wedge h_m^P\rho = x_m),$$

что означает, что существует такое циклическое слагаемое $\langle a_{k_i}\rangle$ в B', что $i \in I$ и $h_1(a_{k_i}) = x_1$, …, $h_m(a_{k_i}) = x_m$. □

Случай, когда финальный ранг базисной подгруппы равен ω и не совпадает с ее рангом

Напомним, что мы предполагаем, что $A = D \oplus G$, где группа D делима, группа G редуцированна и $|D| < |G|$. Пусть базисная подгруппа $\overline{B}$ группы A (и группы G) имеет вид $B \oplus B'$, где $|B'| = |\overline{B}|$, $|B| = \omega$, B' ограничена.

Заметим, что из $|D| < |G|$ следует $|D| \leqslant \omega$, так как мы принимаем континуум-гипотезу, из которой следует $|B'| = |\overline{B}| = \omega_1 = 2^\omega = c$.

Условие $|D| \leqslant \omega$ означает, что если группы $A_1 = D_1 \oplus G_1$ и $A_2 = D_2 \oplus G_2$ имеют описанный только что вид, и при этом $\mathrm{End}\,(A_1) \equiv \mathrm{End}\,(A_2)$, то $D_1 \cong D_2$, и для того, чтобы доказать $A_1 \equiv_{\mathcal{L}_2} A_2$, нам достаточно, в принципе, доказать $G_1 \equiv_{\mathcal{L}_2} G_2$ (при условии фиксации эндоморфизма между D и G).

Поэтому для простоты рассуждений предположим, что группа A редуцированна, т. е. $A = G$, $D = 0$.

Мы фиксируем эндоморфизм φ_B с образом, совпадающим с базисной подгруппой B группы A. Кроме того, фиксируем эндоморфизм f_B с образом B', являющимся прямым слагаемым в B, изоморфным

$$\bigoplus_{i\in\omega} \mathbb{Z}(p^{n_i}),$$

где $n_0 \geqslant 2$, $n_{i+1} > 2n_i$.

Естественно, мы также предполагаем фиксированными эндоморфизмы Ψ и Γ.

Пусть ρ_1 и ρ_2 — неразложимые проекторы на циклические прямые слагаемые группы B', удовлетворяющие формулам $\exists c \in Z(\Psi\rho_1 = c\rho_1) \wedge \exists c \in Z(\Psi\rho_2 = c\rho_2)$ и $o(\rho_1) > o(\rho_2)$. Тогда будем писать $\gamma \in \langle\Gamma\rangle_{\rho_1,\rho_2}$, если эндоморфизм γ удовлетворяет формуле

$$\exists\gamma'(\gamma'\rho_2 = \rho_2 \wedge \forall\rho(Idem^*(\rho) \wedge \forall c \in Z(c\rho \neq 0 \Rightarrow c\rho f_B \neq 0)\wedge \\ \wedge \exists c \in Z(\Psi\rho = c\rho) \wedge o(\rho) \leqslant o(\rho_1) \wedge o(\rho) > o(\rho_2) \Rightarrow \gamma'\rho = \gamma'\Gamma\rho) \wedge \gamma\rho_1 = \gamma'\rho_1).$$

Эта формула означает, что существует эндоморфизм $\gamma' : B' \to B'$ такой, что для a_i — образующей в $\rho_2 A$ и a_{i+k} — образующей в $\rho_1 A$ выполнено

1) $\gamma'(a_i) = a_i$;

2) $\forall l \in \{1, \dots, k\}$ имеет место $\gamma'(a_{i+k}) = \gamma'(a_{i+k-1}) = \dots = \gamma'(a_{i+1}) = \gamma'(a_i) = a_i$.

Кроме того, $\gamma(a_{i+k}) = \gamma'(a_{i+k}) = a_i$. Отсюда мы получаем $\gamma(a_{i+k}) = a_i$.

Теперь рассмотрим формулу

$$Onto(\Lambda) := [\forall\overline{\rho}\forall\overline{c}(Idem^*(\overline{\rho}) \wedge \forall c \in Z(c\overline{\rho} \neq 0 \Rightarrow c\overline{\rho}\varphi_B \neq 0)\wedge$$

$$\wedge\, \overline{c} \in Z \wedge \overline{c\rho} \neq 0 \Rightarrow \exists\rho_1 \dots \exists\rho_{p-1}((\bigwedge_{i,j=1}^{p-1} \rho_i\rho_j = \rho_j\rho_i = 0) \wedge Idem^*(\rho_1) \wedge \dots \wedge Idem^*(\rho_{p-1})\wedge$$

$$\wedge\, (\bigwedge_{i=1}^{p-1} \forall c \in Z(c\rho_i \neq 0 \Rightarrow c\rho_i f_B \neq 0)) \wedge (\bigwedge_{i=1}^{p-1} \exists c \in Z(\Psi\rho_i = c\rho_i))\wedge$$

$$\wedge\, (\bigwedge_{i=1}^{p-1} \overline{c\rho}\Lambda\rho_i \neq 0) \wedge (\bigwedge_{i=1}^{p-1} \forall c \in Z(c\overline{c\rho} \neq 0 \Rightarrow c\overline{c\rho}\Lambda\rho_i \neq 0))\wedge$$

$$\wedge\, (\bigwedge_{i,j=1; i\neq j}^{p-1} o(\rho_i) > o(\rho_j) \Rightarrow \forall\gamma \in \langle\Gamma\rangle_{\rho_i,\rho_j}(\Lambda\gamma\rho_i \neq \Lambda\rho_i))))]\wedge$$

[это означает, что для любого порождающего b циклического прямого слагаемого $\langle b\rangle$ группы B и для любого p-адического целого числа c существует по крайней мере $p-1$ чисел $i_1, \dots, i_{p-1} \in \omega$ таких, что $\Lambda(a_{i_k}) = \xi_k c \cdot b$, где ξ_k различны, не кратны p, $\xi_k c \cdot b \neq \xi_l c \cdot b$ для любых $k \neq l$.]

$$\wedge\, [Hom(\Lambda)] \wedge [\forall\rho_1\forall\rho_2(Idem^*(\rho_1) \wedge Idem^*(\rho_2)\wedge$$

$$\wedge\, \forall c \in Z(c\rho_1 \neq 0 \Rightarrow c\rho_1 f_B \neq 0) \wedge \forall c \in Z(c\rho_2 \neq 0 \Rightarrow c\rho_2 f_B \neq 0)\wedge$$

$$\wedge\, \exists c \in Z(\Psi\rho_1 = c\rho_1) \wedge \exists c \in Z(\Psi\rho_2 = c\rho_2) \wedge o(\rho_1) \geqslant o(\rho_2) \Rightarrow$$

$$\Rightarrow \exists\rho_3(Idem^*(\rho_3) \wedge \forall c \in Z(c\rho_3 \neq 0 \Rightarrow c\rho_3 f_B \neq 0) \wedge \exists c \in Z(\Psi\rho_3 = c\rho_3)\wedge$$

$$\wedge\, ((o(\rho_3) > o(\rho_1) \wedge o(\rho_3) > o(\rho_2) \wedge \exists\gamma_1 \in \langle\Gamma\rangle_{\rho_3,\rho_1}\exists\gamma_2 \in \langle\Gamma\rangle_{\rho_3,\rho_2}(\Lambda\rho_3 = \Lambda\gamma_1\rho_3 + \Lambda\gamma_2\rho_3))\vee$$

$$\wedge\, (o(\rho_3) < o(\rho_1) \wedge o(\rho_3) < o(\rho_2) \wedge \exists\gamma_2 \in \langle\Gamma\rangle_{\rho_1,\rho_2}\exists\gamma_3 \in \langle\Gamma\rangle_{\rho_1,\rho_3}(\Lambda\gamma_3\rho_1 = \Lambda\rho_1 + \Lambda\gamma_2\rho_1))\vee$$

$$\wedge\, (o(\rho_3) < o(\rho_1) \wedge o(\rho_3) > o(\rho_2) \wedge \exists\gamma_2 \in \langle\Gamma\rangle_{\rho_1,\rho_2}\exists\gamma_3 \in \langle\Gamma\rangle_{\rho_1,\rho_3}(\Lambda\gamma_3\rho_1 = \Lambda\gamma_1 + \Lambda\gamma_2\rho_1))))]$$

[Это условие означает, что для любых a_i и a_j существует такое a_k, что $\Lambda(a_k) = \Lambda(a_)$ + $\Lambda(a_j)$. Таким образом, эндоморфизм Λ является эпиморфизмом $B' \to B$.]

$$\wedge\, [\forall\rho_1\rho_2(Idem^*(\rho_1) \wedge Idem^*(\rho_2) \wedge \forall c \in Z(c\rho_1 \neq 0 \Rightarrow c\rho_1 f_B \neq 0)\wedge$$

$$\wedge\, \forall c \in Z(c\rho_2 \neq 0 \Rightarrow c\rho_2 f_B \neq 0) \wedge \exists c \in Z(\Psi\rho_1 = c\rho_1) \wedge \exists c \in Z(\Psi\rho_2 = c\rho_2)\wedge$$

$$\wedge\, o(\rho_1) > o(\rho_2) \Rightarrow \exists\rho(Idem^*(\rho) \wedge \forall c \in Z(c\rho \neq 0 \Rightarrow c\rho\varphi_B \neq 0) \wedge \rho\Lambda\rho_2 \neq 0)\wedge$$

$$\wedge\, \forall\gamma \in \langle\Gamma\rangle_{\rho_1,\rho_2}(\Lambda\rho_1 \neq \Lambda\gamma\rho_1))].$$

[Это условие означает, что эндоморфизм Λ индуцирует биекцию между множеством $\{a_i | i \in \omega\}$ и группой B с условием $o(\Lambda(a_i)) \leqslant p^i$.]

Фиксируем эндоморфизм Λ.

Теперь вспомним, что мы имеем ограниченную группу B' некоторой несчетной мощности μ, в которой мы можем выделить формульное множество $\mathbf{F} = \mathbf{F}(\overline{g})$, состоящее из

μ независимых неразложимых проекторов на прямые слагаемые группы B' и множество $\mathbf{F}' = \mathbf{F}'(\overline{g}')$, состоящее из μ независимых проекторов на счетно порожденные прямые слагаемые группы B', причем для каждого $f \in \mathbf{F}'$ множество таких $f_t \in \mathbf{F}$, что f_tA есть прямое слагаемое в fA, Счетно. Обозначим подмножество в $\mathbf{F}$ вида $\{f_t \in \mathbf{F} | f_tA \subset fA\}$ через $\mathbf{F}_f$. Очевидно, что множество $\mathbf{F}_f$ формульно.

Фиксируем эндоморфизмы Π_1, Π_2, задающие порядок на каждом $f(A)$, $f \in \mathbf{F}$:

$$Order(\Pi_1, \Pi_2) := \forall f \in \mathbf{F}(\exists! f_0 \in \mathbf{F}_f(\Pi_2 f_0 = 0 \wedge$$
$$\wedge \forall f_1(f_1 \in \mathbf{F}_f \wedge f_1 \neq f_0 \Rightarrow \exists f_2 \in \mathbf{F}_f(f_1 \neq f_2 \wedge$$
$$\wedge f_2\Pi_2 = \Pi_2 f_1 = f_2\Pi_2 f_1 \wedge \forall c \in Z(cf_1 \neq 0 \Rightarrow c\Pi_2 f_1 \neq 0) \wedge$$
$$\wedge f_1\Pi_1 = \Pi_1 f_2 = f_1\Pi_1 f_2 \wedge \forall c \in Z(cf_2 \neq 0 \Rightarrow c\Pi_1 f_2 \neq 0)) \wedge$$
$$\wedge \forall f_1 \forall f_2 \in \mathbf{F}_f(f_1 \neq f_2 \Rightarrow \bigwedge_{i=1}^{2} \forall f_3, f_4 \in \mathbf{F}_f$$
$$(f_3\Pi_i f_1 = f_3\Pi_i = \Pi f_1 \neq 0 \wedge f_4\Pi_i f_2 = f_4\Pi_i f_2 = f_4\Pi_i = \Pi_i f_2 \neq 0 \Rightarrow f_3 \neq f_4)) \wedge$$
$$\wedge \forall f_1 \in \mathbf{F}_f \exists f_2 \mathbf{F}_f(\Pi_2 f_2 = f_1\Pi_2 = f_1\Pi_2 f_2 \neq 0) \wedge \forall f_1 \in \mathbf{F}_f(\Pi_2\Pi_1 f = f \wedge$$
$$\wedge \forall f'(Idem^*(f') \wedge f'f = f' \wedge Fin(f') \wedge f' \neq 0 \Rightarrow$$
$$\Rightarrow \exists f_1, f_2 \in mathbfF_f(f_1 f = f_1 \wedge f_2 f = f_2 \wedge f_2\Pi_2 = f_2\Pi_2 f_1 = \Pi_2 f_1 \neq 0)))).$$

Относительно порядка Π_1 мы можем считать, что для каждого $f_t \in \mathbf{F}$ $(t \in \mu)$ мы имеем базис в $f_t(A)$, состоящий из $f_t^0, f_t^1, \ldots$, где $\Pi_1(f_t^i A) = f_t^{i+1} A$.

Теперь выпишем условия для гомоморфизма Δ:

1) $\forall f \in \mathbf{F} \exists \beta(Hom(\beta) \wedge \forall \rho(Idem^*(\rho) \wedge \forall c \in Z(c\rho \neq 0 \Rightarrow c\rho f_B \neq 0) \wedge \exists c \in Z(\Psi\rho = c\rho) \Rightarrow \forall c \in Z(\Psi\rho = c\rho \Rightarrow c\beta\rho \neq 0 \wedge pc\beta\rho = 0)) \wedge$ (это означает, что $o(\beta(a_i)) = p^i$) $\wedge \forall \rho \forall \rho'(Idem^*(\rho) \wedge Idem^*(\rho') \wedge \forall c \in Z(c\rho \neq 0 \Rightarrow c\rho f_B \neq 0) \wedge \forall c \in Z(c\rho' \neq 0 \Rightarrow c\rho'\varphi_B \neq 0) \wedge \exists c \in Z(\Psi\rho = c\rho) \Rightarrow \neg(\rho'\beta\rho = \beta\rho)) \wedge$ (это означает, что $\beta(a_i) \notin B$) $\wedge \forall \rho(Idem^*(\rho) \wedge \forall c \in Z(c\rho \neq 0 \Rightarrow c\rho f_B \neq 0) \wedge \exists c \in Z(\Psi\rho = c\rho) \Rightarrow p\beta\rho = p\beta(\Gamma\rho) + \Lambda\Delta\rho_{on,f}\rho)$, где $\rho_{on,f} : B' \to f_tA$, $\rho_{on,f}(a_i) = f_t^i$ (это означает $p\beta(a_i) = \rho(a_{i-1}) + \Lambda\Delta(f_t i))$ $\wedge \forall c \in Z(c\Lambda\Delta\rho_{on,f}\rho \neq 0 \Rightarrow c\beta\rho \neq 0))$ (это означает $o(\Lambda\Delta(f_t^i)) \leqslant p^i$).

Это условие означает, что для каждого f_t, $t \in \mu$ Δ — это отображение из $\{f_t^i | i \in \omega\}$ в $\{a_i | i \in \omega\}$ такое, что существует последовательность $c_{1,t}, \ldots, c_{m,t}, \ldots$ элементов из A, не принадлежащих B, с условиями $o(c_{i,t}) = p^i$, $pc_{i,t} = c_{i-1,t} + b_{i,t}$, где $b_{i,t} \in B$, $b_{i,t} = \beta(\Delta(f_t^i))$, $o(b_{i,t}) \leqslant p^i$.

Как мы знаем, такую последовательность можно считать последовательностью элементов квазибазиса группы A, при этом ее можно считать однозначно определенной с помощью последовательности

$$(b_{i,t} | i \in \omega, b_{i,t} = \beta(\Delta(f_t^i A))).$$

Эндоморфизм β однозначно определяется каждым $f \in \mathbf{F}$, будем для краткости писать $Quasi_f(\beta)$.

2) Любое множество элементов из Γ задает нам множество последовательностей элементов квазибазиса

$$\{f_t | t \in J\} \leftrightarrow \{(c_{1,t}, \ldots, c_{i,t}, \ldots) | t \in J\} = C_J,$$

а множество C_J задает нам линейную оболочку $\overline{C}_J = \langle C_J \rangle$ таким образом, что мы можем определить, когда последовательность принадлежит этой линейной оболочке, а когда нет. Мы не будем выписывать для краткости формулы, а лишь наложим устные условия, что (а) любая существующая последовательность принадлежит $\overline{C}_I$; (б) линейные оболочки $\langle C_{J_1} \rangle$ и $\langle C_{J_2} \rangle$ при $J_1 \cap J_2 = \emptyset$ пересекаются по B.

Таким образом, наш гомоморфизм Δ будет осуществлять взаимно-однозначное отображение между множеством $\{f_t^i | t \in I\}$ и квазибазисом $\{c_{it} | i \in \omega, t \in \mu\}$ группы A. Мы будем считать гомоморфизм Δ фиксированным.

Теперь мы можем заняться интерпретацией теории второго порядка группы A. Сделаем это следующим образом.

Помимо множества $\mathbf{F}$, состоящего из μ независимых проекторов на счетно порожденные прямые слагаемые группы B, мы рассмотрим также аналогичное множество $\mathbf{G}$ с единственным дополнением, что для каждого $g \in \mathbf{G}$ будет выделен один фиксированный проектор g_0 на счетно порожденное прямое слагаемое $g_0 A$ в gA такое, что если $gA = g_0 A \oplus A'$, то A' также счетно порождено.

Фиксируем некоторое $g \in \mathbf{G}$ и рассмотрим гомоморфизм h такой, что $h(g_0 A) \in \langle a_i \rangle$ для некоторого $i \in \omega$, а если $g_t \in \mathbf{G}_g \setminus \mathbf{G}_g^0$, то либо $h(g_t A) \subset fA$ для некоторого $f \in \mathbf{F}$, либо $h(g) = 0$.

Кроме того, пусть образ h на gA конечномерен, а прообраз каждого $f \in \mathbf{F}$ содержит не более $p - 1$ элементов из $\mathbf{G}_g$.

Тогда каждому такому h следующим образом сопоставляется элемент из A: если h на $\mathbf{G}_g \setminus \mathbf{G}_g^0$ есть конечное подмножество $\mathcal{F}$ множества $\{g_t^i | t \in \mu, i \in \omega\}$, а $h(g_t^0) = a_k$, то мы получаем элемент

$$\sum_{f_t^i \in \mathcal{F}} \alpha_{ti} c_{it} + b,$$

где α_{it} — это кратность прообраза f_t^i, а $b = \Lambda(a_k)$.

Очевидно, что мы, как и раньше, для такого отображения h можем писать $h \in End_g$. Также очевидно, что два элемента $h_1, h_2 \in End_g$ мы будем считать эквивалентными, если существует автоморфизм α группы gA, переставляющий местами элементы $\mathbf{G}_g$ и оставляющий $g_0 \in \mathbf{G}_g^0$ на месте такой, что $h_1 \alpha$ и h_2 совпадают. Множество End_g, профакторизованное по такой эквивалентности, как обычно, обозначим через $\widetilde{End}_g$. Сложение на множестве $\widetilde{End}_g$ также очевидно: образы элемента g_0 складываются, количество прообразов каждого f_{it} суммируется и, если оно превышает $p - 1$, то остается остаток от деления на p прообразов f_{it}, при этом добавляется один лишний прообраз $f_{i-1,t}$ и к образу g_0 добавляется известное нам $b_{it} = \beta(\Delta(f_{it}))$.

Дальнейшее доказательство аналогично предыдущим пунктам, так как мы имеем μ независимых элементов g_t в множестве $\mathbf{G}$, для каждого из которых умеем интерпретировать теорию $Th(A)$.

4.6.6 Основная теорема

Напомним, что если группа $A = D \oplus G$, где группа D делима, группа G редуцированна, то *выразимым рангом группы* A мы будем называть кардинальное число

$$r_{exp} = \mu = \max(\mu_D, \mu_G),$$

где μ_D — это ранг группы D, а μ_G — это ранг базисной подгруппы группы G.

Тогда имеет место теорема

Теорема 4.36. *Для любых бесконечных p-групп A_1 и A_2 из элементарной эквивалентности колец эндоморфизмов $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$ следует совпадение теорий второго порядка $Th_2^{r_{exp}(A_1)}(A_1)$ и $Th_2^{r_{exp}(A_2)}(A_2)$ групп A_1 и A_2, ограниченных кардинальными числами $r_{exp}(A_1)$ и $r_{exp}(A_2)$ соответвенно.*

Доказательство. Так как кольца $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$ элементарно эквивалентны, то они удовлетворяют одним и тем же предложениям первого порядка. Если в кольце $\mathrm{End}\,(A_1)$ для некоторого натурального k выполняется предложение

$$\forall x(p^k x = 0) \wedge \exists x(p^{k-1}x \neq 0),$$

то группа A_1 является ограниченной и максимум порядков ее элементов равен p^k. Очевидно, что в этом случае таковой же является и группа A_2, и теорема для этого случая доказана в пункте 3.

Теперь предположим, что ни группа A_1, ни группа A_2 не являются ограниченными. Пусть для некоторого натурального k в кольце $\mathrm{End}\,(A_1)$ выполняется предложение ψ_{p^k}.

Тогда это предложение выполняется также и в кольце $\mathrm{End}\,(A_2)$, а значит, группы A_1 и A_2 представляются в виде прямых сумм $D_1 \oplus G_1$ и $D_2 \oplus G_2$ соответственно, где группы D_1 и D_2 делимы, а группы G_1 и G_2 ограничены числом p^k. Кроме того, предложение ψ_{p^k} фиксирует проекторы ρ_D и ρ_G на группы D и G соответственно. Если $\rho_G = 0$, то группы A_1 и A_2 делимы и в этом случае утверждение теоремы следует из пункта 4.

Пусть кольца $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$ удовлетворяют предложению

$$\begin{aligned}
\widetilde{\psi}^2_{p^k} := \exists \rho_D \exists \rho_G(\psi_{p^k}(\rho_D, \rho_G) \wedge \exists h(\rho_D h \rho_G = h\rho_G \wedge \\
\wedge \forall \rho_1 \forall \rho_2 (Idem^*(\rho_1) \wedge Idem^*(\rho_2) \wedge \rho_1\rho_G = \rho_1 \wedge \rho_2\rho_G = \rho_2 \wedge \rho_1\rho_2 = \rho_2\rho_1 = 0 \Rightarrow \\
\Rightarrow \exists \rho_1' \exists \rho_2' (Idem^*(\rho_1') \wedge Idem^*(\rho_2') \wedge \rho_1'\rho_D = \rho_1' \wedge \rho_2'\rho_D = \rho_2' \wedge \\
\wedge \rho_1'\rho_2' = \rho_2'\rho_1' = 0 \wedge \rho_1' h \rho_1 = h\rho_1 \neq 0 \wedge \rho_2' h \rho_2 = h\rho_2 \neq 0)))).
\end{aligned}$$

Это предложение (вдобавок к утверждениям предложения ψ_{p^k}), утверждает, что существует такой эндоморфизм h группы A, переводящий G в D, что любые два независимых циклических слагаемых $\rho_1 A$ и $\rho_2 A$ группы G отображаются в независимые квазициклические слагаемые $\rho_1' A$ и $\rho_2' A$ группы D, т.е. что существует вложение группы G в группу D. Из этого следует, что $|G| \leqslant |D|$, т.е. если предложение $\psi^2_{p^k}$ выполняется в кольцах $End(A_1)$ и $End(A_2)$, то группы A_1 и A_2 изоморфны прямым суммам $D_1 \oplus G_1$ и $D_2 \oplus G_2$, где $|D_1| \geqslant |G_1|$, $|D_2| \geqslant |G_2|$. В этом случае утверждение теоремы следует из первых подпунктов пункта 4.

Если же в кольцах $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$ предложение ψ_{p^k} выполняется, но при этом не выполняется предложение $\psi^2_{p^k}$, то группы A_1 и A_2 являются прямыми суммами $D_1 \oplus G_1$

и $D_2 \oplus G_2$, где $|D_1| < |G_1|$, $|D_2| < |G_2|$. В этом случае утверждение теоремы следует из последних подпунктов пункта 5.

Если ни для какого натурального k предложение ψ_{p^k} не принадлежит теории $Th(\mathrm{End}\,(A_1))$, то ни для какого натурального k предложение ψ_{p^k} не принадлежит теории $Th(\mathrm{End}\,(A_2))$, и, таким образом, обе группы A_1 и A_2 обладают неограниченными базисными подгруппами.

Рассмотрим формулу

$$\begin{aligned}\psi(\rho_D, \rho_G) := Idem(\rho_D) \wedge Idem(\rho_G) \wedge (\rho_D\rho_G = \rho_G\rho_D = 0) \wedge (\rho_D + \rho_G = 1)\wedge\\ \wedge \forall x(\rho_D x\rho_D = 0 \vee p(\rho_D x\rho_D) \neq 0)\wedge\\ \wedge \forall \rho'(Idem^*(\rho') \wedge \rho'\rho_G = \rho' \Rightarrow \neg(\forall x(\rho' x\rho' = 0 \vee p(\rho' x\rho') \neq 0))).\end{aligned}$$

Эта формула утверждает, что группа A есть прямая сумма своих подгрупп $\rho_D A$ и $\rho_G A$, причем группа $\rho_D A$ делима, а группа $\rho_G A$ редуцированна.

Рассмотрим предложение

$$\begin{aligned}\psi^2 := \exists \rho_D \exists \rho_G \exists h(\psi(\rho_D, \rho_G) \wedge \rho_D h\rho_G = h\rho_G\wedge\\ \wedge \forall \rho(Idem^*(\rho) \wedge \rho\rho_G = \rho \Rightarrow \forall c \in Z(c\rho \neq 0 \Rightarrow ch\rho \neq 0))).\end{aligned}$$

Это предложение утверждает, что группа A есть прямая сумма делимой подгруппы $D = \rho_D A$ и редуцированной подгруппы $G = \rho_G A$ и что существует вложение $h : G \to D$, откуда следует, что $|G| \leqslant |D|$. Если кольца $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$ удовлетворяют предложению ψ^2, то для групп A_1 и A_2 мы имеем $A_1 = D_1 \oplus G_1$, $A_2 = D_2 \oplus G_2$, $|D_1| \geqslant |G_1|$, $|D_2| \geqslant |G_2|$, и утверждение теоремы следует из предложения 4.16.

Теперь предположим, что кольца $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$ не удовлетворяют предложению ψ^2. В этом случае $A_1 = D_1 \oplus G_1$, $A_2 = D_2 \oplus G_2$, $|D_1| < |G_1|$, $|D_2| < |G_2|$.

Вспомним формулы предыдущего пункта.

Рассмотрим предложение

$$\begin{aligned}\psi^3 := \exists \rho_D \exists \rho_G(\psi(\rho_D, \rho_G) \wedge \neg\psi^2\wedge\\ \wedge \exists \varphi_B(Base(\varphi_B) \wedge \forall \rho(Idem^*(\rho) \Rightarrow \exists \rho'(Idem^*(\rho') \wedge o(\rho') > o(\rho)\wedge\\ \wedge \exists f(Ord_{\rho'}(f) \wedge \forall f'(Idem^*(f') \wedge f'f = f' \Rightarrow \forall c \in Z(cf' \neq 0 \Rightarrow cf'\varphi_B \neq 0))\wedge\\ \wedge \exists h(\forall f_1(Idem^*(f_1) \wedge \forall c \in Z(cf_1 \neq 0 \Rightarrow cf_1\varphi_B \neq 0) \Rightarrow\\ \Rightarrow \exists f_2(Idem^*(f_2) \wedge f_2 f = f_2 \wedge f_1 h = hf_2 = f_1 hf_2 \neq 0)))))))).\end{aligned}$$

Это предложение утверждает, что

1) $A = \rho_D A \oplus \rho_G A = D \oplus G$, где D делима, G редуцированна, $|D| < |G|$;

2) φ_B — эндоморфизм на A с образом $\varphi_B(A)$, совпадающим с некоторой базисной подгруппой B;

3) для любого натурального k существует такое натуральное n, что в группе B существует прямое слагаемое, являющееся суммой циклических групп порядка p^n, равномощное самой группе B.

Таким образом, предложение ψ^3 утверждает, что финальный ранг базисной подгруппы группы G совпадает с ее рангом.

Предложение

$$\begin{aligned}\psi^4 := \exists\varphi_B(Base(\varphi_B) \wedge \forall\rho(Idem^*(\rho) \Rightarrow \\ \Rightarrow \forall f(Ord_\rho(f) \Rightarrow Fin(f) \vee \exists h(\forall f_1(Idem^*(f_1)\wedge \\ \wedge \forall c \in Z(cf_1 \neq 0 \Rightarrow cf_1\varphi_B \neq 0) \Rightarrow \exists f_2(Idem^*(f_2)\wedge \\ \wedge f_2 f = f_2 \wedge f_1 h = hf_2 = f_1 h f_2 \neq 0)))))\end{aligned}$$

означает, что в базисной подгруппе B для любого натурального n любое прямое слагаемое, являющееся прямой суммой циклических групп порядка p^n, или конечно, или равномощно группе B, откуда следует, что группа B счетна.

Таким образом, если кольца $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$ удовлетворяют предложению $\psi^3\wedge\neg\psi^4$, то группы A_1 и A_2 являются прямыми суммами $D_1\oplus G_1$ и $D_2\oplus G_2$, $|D_1| < |G_1|$, $|D_1| < |G_2$, финальные ранги базисных подгрупп групп A_1 и A_2 совпадают с их рангами и несчетны. В этом случае утверждение теоремы следует из предложения 4.16. Если кольца $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$ удовлетворяют предложению $\psi^3 \wedge \psi^4$, то их базисные подгруппы счетны и в этом случае утверждение теоремы следует из предложения 4.19. Нам остаются еще два случая, для различения которых мы напишем предложение

$$\begin{aligned}\psi^5 := \exists\varphi_B\exists\overline{\rho}(Base(\varphi_B) \wedge Idem^*(\overline{\rho})\wedge \\ \wedge \forall\rho(Idem^*(\rho) \wedge o(\rho) > o(\overline{\rho}) \Rightarrow \forall f(Ord_\rho(f) \Rightarrow Fin(f)\vee \\ \vee \exists h(\forall f_1(Idem^*(f_1) \wedge o(f_1) > o(\rho) \wedge \forall c \in Z(cf_1 \neq 0 \Rightarrow cf_1\varphi_B \neq 0) \Rightarrow \\ \Rightarrow \exists f_2(Idem^*(f_2) \wedge f_2 f = f_2 \wedge f_1 h = hf_2 = f_1 h f_2 \neq 0)))))),\end{aligned}$$

означающее, что существует число k такое, что в базисной подгруппе B для любого натурального n, бо́льшего k, любое прямое слагаемое, являющееся суммой циклических групп порядка p^n, либо конечно, равномощно прямому слагаемому группы B, порожденному всеми образующими порядка $> p^k$.

Естественно, это означает, что финальный ранг группы B счетен.

Теперь, если кольца $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$ удовлетворяют предложению $\neg\psi^3 \wedge \neg\psi^5$, то финальные ранги базисных подгрупп групп A_1 и A_2 несчетны и не совпадают с их рангами. В этом случае утверждение теоремы следует из предложения 4.18.

Если же кольца $\mathrm{End}\,(A_1)$ и $\mathrm{End}\,(A_2)$ удовлетворяют предложению $\neg\psi^3\wedge\psi^5$, то финальные ранги базисных подгрупп групп A_1 и A_2 счетны и не совпадают с их рангами, и в этом случае утверждение теоремы следует из последних подпунктов предыдущего пункта. □

Литература

[1] Абе Э. Автоморфизмы групп Шевалле над коммутативными кольцами. Алгебра и анализ, 1993, 5(3), 74–90.

[2] Блошицын В.Я. Автоморфизмы общей линейной группы над коммутативным кольцом, не порождаемым делителями нуля. Алгебра и логика, 1978, 17(6), 639–642.

[3] Борель А. Свойства и линейные представления групп Шевалле. Семинар по алгебраическим группам, М., 1973, 9–59.

[4] Е.И. Бунина, П.П. Семенов. Автоморфизмы полугруппы обратимых матриц с неотрицательными элементами над частично упорядоченными коммутативными кольцами. Фундаментальная и прикладная математика. 2008, 14(2), 65-100

[5] Е.И. Бунина, П.П. Семенов. Элементарная эквивалентность полугрупп обратимых матриц с неотрицательными элементами над частично упорядоченными коммутативными кольцами. Фундаментальная и прикладная математика. 2008, 14(4), 3-17.

[6] Бунина Е.И., Доброхотова-Майкова А.С. Элементарная эквивалентность обобщенных колец инцидентности. Фундаментальная и прикладная математика, 2008, 14(7), 37-42.

[7] Н. Бурбаки. Алгебра. Модули, кольца, формы. Москва, Наука, 1966.

[8] Бурбаки Н. Группы и алгебры Ли. Группы Кокстера и системы Титса, группы, порожденные отражениями, системы корней. Москва, Мир, 1972.

[9] Вавилов Н.А. Параболические подгруппы групп Шевалле над коммутативным кольцом. Записки научных семинаров ЛОМИ, 1982, 116, 20–43.

[10] Вавилов Н.А., Гаврилович М.Р. A_2-доказательство структурных теорем для групп Шевалле типов E_6 и E_7. Алгебра и Анализ, 2004, 116(4), 54–87.

[11] Вавилов Н.А, Гаврилович М.Р., Николенко С.И. Строение групп Шевалле: доказательство из книги. Записки научных семинаров ЛОМИ, 2006, 330, 36–76.

[12] Вавилов Н.А., Лузгарев А.Ю. Нормализатор группы шевалле типа E_6. Алгебра и анализ, 2007, 19(5), 37Ц-64.

[13] Вавилов Н.А., Петров В.А. О надгруппах $Ep(2l, R)$. Алгебра и Анализ, 2003, 15(3), 72–114.

[14] Голубков А.Ю. Первичный радикал классических групп над ассоциативными кольцами. Диссертация к.ф.-м.н., Москва, 2001.

[15] И.З. Голубчик. Линейные группы над ассоциативными кольцами. Диссертация на соискание степени доктора физико-математических наук. Уфа, 1997.

[16] Голубчик И.З., Михалев А.В. Изоморфизмы общей линейной группы над ассоциативным кольцом. Вестник МГУ, серия математика, 1983, 3, 61–72.

[17] Гоулд В., Михалев А.В., Палютин Е.А., Степанова А.А. Теоретико-модельные свойства свободных, проективных и плоских S-полигонов. Фундаментальная и прикладная математика, 2008, 14(7), 63–110.

[18] Дроботенко В.С., Погориляк Е.Я. Автоморфизмы полной линейной группы над некоммутативным полулокальным кольцом. УМН, 1977, 32(2), 157–158.

[19] Дьедонне Ж. Геометрия классических групп. Мир, М., 1974.

[20] Ершов Ю. Л., Лавров И. А., Тайманов А. Д., Тайцлин М. А. Элементарные теории. Успехи мат. наук, 1965, 20(4), 37–108.

[21] Ершов Ю. Л., Палютин Е. А. Математическая логика. М. Наука, 1979.

[22] Ершов Ю. Л. Проблемы разрешимости и конструктивные модели. М. Наука, 1980.

[23] Залесский А.Е. Линейные группы. Итоги науки. Фундаментальные направления, М., 1989, 114–228.

[24] Зельманов Е.И. Изоморфизмы полных линейных групп над ассоциативными кольцами. Сибирский математический журнал, 1985, 26(4), 49–67.

[25] Зильбер Б. И. Пример двух элементарно эквивалентных, но не изоморфных конечно порожденных метабелевых групп. Алгебра и логика, 1971, 10(3), 309–315.

[26] С. Н. Ильин. Обратимые матрицы над (неассоциативными) антикольцами. Универсальная алгебра и ее приложения. — Волгоград, Перемена, 2000, С. 81–89.

[27] Каргаполов М. И. Об элементарной теории абелевых групп. — Алгебра и логика, 1963, 1(6), 26–36.

[28] Кейслер Г., Чэн Ч.Ч. Теория моделей. Москва, Мир, 1977.

[29] Козлов Г. Т., Кокорин А. И. Элементарная теория абелевых групп без кручения с предикатом, выделяющим подгруппу. Алгебра и логика, 1969, 8(3), 320–334.

[30] Козлов Г. Т., Кокорин А. И. Доказательство леммы о модельной полноте. Алгебра и логика, 1975, 14(5), 533–535.

[31] Кокорин А. И., Пинус А. Г. Вопросы разрешимости расширенных теорий. Успехи мат. наук, 1978, 33(2), 49–84.

[32] Куликов Л.Я. К теории абелевых групп произвольной мощности. Мат. сборник, 1941, 9, 165–182.

[33] Куликов Л.Я. К теории абелевых групп произвольной мощности. Мат. сборник, 1945, 16, 129–162.

[34] Куликов Л.Я. Обобщенные примарные группы, I. Труды ММО, 1 (1952), 247–326; II. Труды ММО, 2 (1953), 85–167.

[35] С. Ленг. Алгебра. Мир, Москва, 1968.

[36] Мальцев А. И. Алгебраические системы. — М.: Наука. — 1970.

[37] Мальцев А.И. Об элементарных свойствах линейных групп. Проблемы математики и механики, Новосибирск, 1961, 110–132.

[38] Э. Мендельсон. Введение в математическую логику. Москва, Наука, 1976.

[39] Дж. Милнор, Введение в алгебраическую K-теорию, Мир, Москва, 1974.

[40] А. В. Михалев, М. А. Шаталова. Автоморфизмы и антиавтоморфизмы полугруппы обратимых матриц с неотрицательными элементами. Математический сборник. 1970, 81(4), 600–609.

[41] Мясников А. Г., Ремесленников В. Н. Изоморфизмы и элементарные свойства нильпотентных степенных групп. В кн. *Мат. логика и теория алгоритмов*, Новосибирск, Наука, 1982, 56–87.

[42] Мясников А. Г., Ремесленников В. Н. Изоморфизмы и элементарные свойства нильпотентных степенных групп. ДАН СССР, 1981, 258(5), 1056–1059.

[43] Мясников А. Г., Ремесленников В. Н. Формульность множества мальцевских баз и элементарные теории конечных алгебр. I., 1982, 23(5), 152–167.

[44] Мясников А. Г., Ремесленников В. Н. Элементарная эквивалентность свободных произведений групп. Препринт, ВЦ СО АН СССР, 1987, 719, 2–3.

[45] Носков Г.А. Автоморфизмы группы $\mathrm{GL}_n(O)$ при $\dim Max(O) \leqslant n-2$. Мат. Заметки, 1975, 17(2), 285–291.

[46] Петечук В.М. Автоморфизмы матричных групп над коммутативными кольцами. Математический сборник, 1982, 117(4), 534–547.

[47] Петечук В.М. Автоморфизмы групп SL_n, GL_n над некоторыми локальными кольцами. Математические заметки, 28(2), 1980, 187–206.

[48] Петечук В.М. Автоморфизмы групп $\mathrm{SL}_3(K)$, $\mathrm{GL}_3(K)$. Математические заметки, 31(5), 1982, 657–668.

[49] Пинус А. Г., Роуз Г. Элементарная эквивалентность решеток подалгебр свободных алгебр. Алгебра и логика, 2000, 39(5), 595–601.

[50] Пинус А. Г. Элементарная эквивалентность решеток разбиений. — Сибирский математический журнал. — 1988. — т. 29. — в. 3. — с. 211–212.

[51] Постников М.М. Лекции по геометрии. Группы и алгебры Ли. Семестр V. Наука, 1982.

[52] Ремесленников В. Н., Романьков В. А. Теоретико-модельные и алгоритмические вопросы теории групп. Алгебра. Геометрия. Топология. Итоги науки. ВИНИТИ, 1983, 3–79.

[53] Ремесленников В. Н. Нестандартные свободные произведения. Тезисы докладов 7-го Всесоюзн. симпозиума по теории групп, Красноярск, 1980, 97.

[54] Сакс Дж. Теория насыщенных моделей. — Пер. с англ. М.: Мир, 1976.

[55] Саркисян Р. А. Об одной проблеме равенства для когомологий Галуа. Алгебра и логика, 1980, 19(6), 707–725.

[56] Стейнберг Р. Лекции о группах Шевалле. Москва, Мир, 1975.

[57] Суслин А.А. Об одной теореме Кона. Записки научных семинаров ЛОМИ, 1976, 64, 127–130.

[58] Теория моделей. Справочная книга по математической логике. Часть I. Перев. с англ. М.: Наука, 1982.

[59] Тимошенко Е. И. О сохранении элементарной и универсальной эквивалентности при сплетении. Алгебра и логика, 1968, 7(4), 114–119.

[60] Тимошенко Е. И, Некоторые элементарные свойства сплетений. Новосибирский инж.-строит. инст-т, Новосибирск, 1977.

[61] Тимошенко Е. И. Об элементарных теориях сплетений. Вопр. теории групп и гомологий алгебры, Ярославль, 1979, 2, 169–174.

[62] К. Фейс. Алгебра: кольца, модули и категории, 1. Москва, Мир, 1977.

[63] Фукс Л. Бесконечные абелевы группы. т. 1,2. Мир, Москва, 1974.

[64] Дж. Хамфрис. Введение в теорию алгебр Ли и их представлений. Москва, МЦНМО, 2003.

[65] Шевалле К. О некоторых простых группах. Математика. Период. сб. перев. иностр. статей, 1958, 2(1), 3–58.

[66] Abe E. Whitehead groups of Chevalley groups over Laurent polynomial rings. Comm. algebra, 1983, 11(12), 1271–1308.

[67] Abe E. Whitehead groups of Chevalley groups over Laurent polynomial rings. Preprint Univ. Tsukuba, 1988.

[68] Abe E., Suzuki K. On normal subgroups of Chevalley groups over commutative rings. Tohoku Math. J., 1976, 28(1), 185–198.

[69] Abe E. Automorphisms of Chevalley groups over commutative rings. Algebra and Analysis, 5(2), 1993, 74–90.

[70] Abe E. Chevalley groups over local rings. Tohoku Math. J., 1969, 21(3), 474–494.

[71] Abe E. Chevalley groups over commutative rings. Proc. Conf. Radical Theory, Sendai — 1988, 1–23.

[72] Abe E. Normal subgroups of Chevalley groups over commutative rings. Contemp. Math., 1989, 83, 1–17.

[73] Abe E., Hurley J. Centers of Chevalley groups over commutative rings. Comm. Algebra, 1988, 16(1), 57–74.

[74] Bak A. Nonabelian K-theory: The nilpotent class of K_1 and general stability. K-Theory, 1991, 4, 363–397.

[75] Bak A., Vavilov Normality of the elementary subgroup functors. Math. Proc. Cambridge Philos. Soc., 1995, 118(1), 35–47.

[76] Bass H., Milnor J., Serr J.-P. Solution of the congruence subgroups problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$. Publ. Math. Inst. Hautes Et. Sci., 1967, 33, 59–137.

[77] Baer R. Der kern, eine charakteristische Untergruppe. Compositio Math., 1 (1934), 254–283.

[78] Baer R. Automorphism rings of primary abelian operator groups. Ann. Math., 44 (1943), 192–227.

[79] Baudish A. A note on the elementary theory of torsion free Abelian groups with one predicate of subgroups, Wiss. Humboldt-Univ, Berlin, Math.-natur wiss. R., 1977, 26(5), 611–612.

[80] Baudish A. Tensor products of modules and elementary equivalence. Algebra Universalis, 1984, 19, 120–127.

[81] Beidar C.I., Michalev A.V. On Malcev's theorem on elementary equivalence of linear groups. Contemporary mathematics, 1992, 131, 29–35.

[82] Borel A. Properties and linear representations of Chevalley groups. Lect. Notes in Math., Berlin; Heidelberg; N.Y.: Springer, 1970, 131, 1–55.

[83] Borel A., Tits J. Homomorphismes "abstraits" de groupes algébriques simples. Ann. Math., 1973, 73, 499–571.

[84] Boyer D.L. On the theory of p-basic subgroups of abelian groups. Topics in Abelian Groups, 323–330 (Chicago, Illinois, 1963).

[85] Carter R.W. Simple groups of Lie type, 2nd ed., Wiley, London et al., 1989.

[86] Carter R.W., Chen Yu. Automorphisms of affine Kac–Moody groups and related Chevalley groups over rings. J. Algebra, 1993, 155, 44–94.

[87] Charles B. Le centre de l'aneeau des endomorphismes d'un groupe abélien primaire. C.R. Acad. Sci. Paris, 1953, 236, 1122-1123.

[88] Chen Yu. Isomorphic Chevalley groups over integral domains. Rend. Sem. Mat. univ. Padova, 1994, 92, 231–237.

[89] Chen Yu. On representations of elementary subgroups of Chevalley groups over algebras. proc. Amer. Math. Soc., 1995, 123(8), 2357–2361.

[90] Chen Yu. Automorphisms of simple Chevalley groups over $\mathbb{Q}$-algebras. Tohoku Math. J., 1995, 348, 81–97.

[91] Chen Yu. Isomorphisms of adjoint Chevalley groups over integral domains. Trans. Amer. Math. Soc., 1996, 348(2), 1–19.

[92] Chen Yu. Isomorphisms of Chevalley groups over algebras. J. Algebra, 2000, 226, 719–741.

[93] Chevalley C. Certain schemas des groupes semi-simples. Sem. Bourbaki, 1960–1961, 219, 1–16.

[94] Cohn P. On the structure of the GL_2 of a ring. Publ. Math. Inst. Hautes Et. Sci., 1966, 30, 365–413.

[95] Costa D.L. Zero-dimensionality and the GE_2 of polynomial rings, J. Pure Appl. Algebra, 1988, 50, 223–229.

[96] Demazure M., Gabriel P. Groupes algébriques. I. North Holland, Amsterdam et al., 1970, 1–770.

[97] Demazure M., Grothendieck A. Schémas en groupes. I, II, III, Lecture Notes Math., 1971, 151, 1-564; 152, 1–654; 153, 1–529.

[98] Dieudonne J. On the automorphisms of the classical groups. Mem. Amer. Math. Soc., 1951, 2, 1–95.

[99] Dries Van Den, Glass A. M. W., Macintyre A., Mekler A. H., Polland J. Elementary equivalence and the commutator subgroup. Glasgow Math. J., 1982, 23, 115–117.

[100] Eklof P. C., Fisher E. R. The elementary theory of Abelian groups. Ann Math. Logic, 1972, 4(2), 115–171.

[101] Erdélyi M. Direct Summands of abelian torsion groups. Acta Univ. Debrecen, 1955, 2, 145–149.

[102] Felgner U. Problem Notebook Model Theory and groups. LMS Durham Symp., 16–28 July 1988.

[103] Fuchs L. On the srtucture of abelian p-groups. Acta Math. Acad. Sci. Hungar., 1953, 4, 267–288.

[104] Fuchs L. Notes on abelian groups, I. Ann. Univ. Sci. Budapest, 1959, 2, 5–23; II, Acta Math. Acad. Sci. Hungar., 1960, 11, 117–125.

[105] Golubchik I.Z. Isomorphisms of the linear general group $\mathrm{GL}_n(R)$, $n \geq 4$, over an associative ring. Contemp. Math., 1992, 131(1), 123–136.

[106] Grothendieck A. Eléments de géoméntie algébrique (rédigés avec la collaboration de Jean Dieudonné). IV. Etude locale des schémas et des morphisms de schémas, 1967, 32, Publ. Math. IHES, 5–361.

[107] Grünewald F., Mennicke J., Vaserstein L.N. On symplectic groups over polynomial rings. Math. Z., 1991, 206(1), 35–56.

[108] Hahn A.J., O'Meara O.T. The classical groups ans K-theory. Springer, Berlin et al., 1989.

[109] Hazrat R., Vavilov N.A. K_1 of Chevalley groups are nilpotent. J. Pure Appl. Algebra, 2003, 179, 99–116.

[110] Hua L.K., Reiner I., Automorphisms of unimodular groups, Trans. Amer. Math. Soc., 71, 1951, 331–348.

[111] Humphreys J. F., On the automorphisms of infinite Chevalley groups, Canad. J. Math., 21, 1969, 908-911.

[112] Humphreys J.E. Introduction to Lie algebras and representation theory. Springer–Verlag New York, 1978.

[113] Jantzen J.C. Representations of algebraic groups. Academic Press, N.Y., 1987.

[114] Fuan Li, Zunxian Li. Automorphisms of $\mathrm{SL}_3(R)$, $\mathrm{GL}_3(R)$. Contemp. Math., 1984, 82, 47–52.

[115] Kaplansky I. Some results on abelian groups. Proc. Nat. Acad. Sci. USA, 1952, 38, 538–540.

[116] Kaplansky I. Infinite abelian groups. University of Michigan Press., Ann. Arbor, Michigan, 1954 and 1969.

[117] Kharlampovich Olga, Myasnikov Alexei. Elementary theory of free non-abelian groups. Journal of Algebra, 2006, 302, 451–552

[118] Kharlampovich O., Myasnikov A. TarskiЎs problem about the elementary theory of free groups has a positive solution, Electron. Res. Announc. Amer. Math. Soc. 4 (December 1998) 101–108.

[119] Kharlampovich O., Myasnikov A., Irreducible affine varieties over a free group: I. Irreducibility of quadratic equations and nullstellensatz, J. Algebra 1998, 200, 472–516.

[120] Kharlampovich O., Myasnikov A., Irreducible affine varieties over a free group: II. Systems in triangular quasiquadratic form and description of residually free groups, J. Algebra, 1998, 200, 517–570.

[121] Klyachko Anton A. Automorphisms and isomorphisms of Chevalley groups and algebras. arXiv:math/0708.2256v3 (2007).

[122] Kopeiko V.I. The stabilization of symplectic groups over a polynomial ring, Math. U.S.S.R. Sbornik, 1978, 34, 655-669.

[123] Kopeiko V.I. Unitary and orthogonal groups over rings with involution. Algebra and discrete Math., 1985, 3–14.

[124] Landein I., Reiner I. Automorphisms of the general linear group over a principal ideal domain. Ann. Math., 1957, 65(3), 519–526.

[125] Madigor M., Rosental J., Rubin M., Srour G. Some highly undecidable laticces. Ann Pure Appl. Logic, 1990, 46, 41–63.

[126] Mackey G.W. Isomorphisms of normed spaces. Ann. Math., 1942, 43, 244–260.

[127] Matsumoto H. Sur les sous-groupes arithmétiques des groupes semi-simples deployés. Ann. Sci. Ecole Norm. Sup., 4eme ser., 1969, 2, 1–62.

[128] McDonald B.R., Automorphisms of $\mathrm{GL}_n(R)$., Trans. Amer. Math. Soc., 215, 1976, 145–159.

[129] O'Meara O.T., The automorphisms of linear groups over any integral domain, J. reine angew. Math., 223, 1966, 56–100.

[130] Oger F. Elementary equivalence and profinite completions: a characterixation of finitely generated abelian-by-finite groups. Proceedings of the American Mathematical Society, 1988, 103(4), 1041–1047.

[131] Oger F. Finite images and elementary equivalence of completely regular inverse semigroups. Semigroup Forum, Springer-Verlag NY Inc, 1992, 45, 322–331.

[132] Oger F. Cancellation and elementary equivalence of groups. Journal of Pure and Applied Algebra, North Holland, 1983, 30, 293–299.

[133] Oger F. Equivalence élémentaire entre groups finis-par-abéliens de type fini. Comment. Math. Helvetici, 1982, 57, 469–480.

[134] Oger F. Cancellation and elementary equivalence of finitely generated finite-by-nilpotent groups. J. London Math. Society, 1991, 44, 173–183.

[135] Oger F. Cancellation of abelian groups of finite rank modulo elementary equivalence. Mathematica Scandinavica, 1990, 67, 5–14.

[136] Oger F. Elementary equivalence of finitely generated nilpotent groups and multilinear maps. Bull. Austral. Math. Soc., 1998, 58(3), 479–493.

[137] Oger F. Elementary equivalence of a polycyclic-by-finite group and its profinite completion. Arch. Math., 1989, 52(6), 521–525.

[138] Oger F. Elementary equivalence and genus of finitely generated abelian groups. G.R.Acad. Sc. Paris., 293 (6.07.1981).

[139] Oger F. Elementary equivalence and genus of finitely generated nilpotent groups. Bull. Australian Math. Society, 1988, 61–68.

[140] Oger F. The model theory of finitely generated finite-by-abelian groups. J. Symbolic Logic, 1984, 49(4), 1115–1124.

[141] Olin P. Elementary properties of V-free products of groups. J.Algebra, 1977, 47(1), 105–114.

[142] Pinus A. G., Rose H. Second order equivalence of cardinals: an algebraic approach, Contributions to General algebra. 13, Verlag J. Heyn, Klagenfurt, 2001, 275–284.

[143] Pomfret I., McDonald B.R. Automorphisms of $\mathrm{GL}_n(R)$, R a local ring. Trans. Amer. Math. Soc., 1972, 173, 379–388.

[144] Prufer H. Untersuchungen uber die Zerlegbarkeit der abzahlbaren primaren abelschen Gruppen. Math. Z., 1923, 17, 35–61.

[145] Rickart C.E. Isomorphic group of linear transformations. Amer. J. Math, 1950, 72, 451–464.

[146] Rubin M., Shelah S. On the elementary equivalence of automorphism groups of Boolean algebras, downward Skolem–Lowenheim theorems and completness of related quantifiers. J. Symbolic Logic, 1980, 45, 263–283.

[147] Schreier O., van der Varden B.L. Die Automorphismen der projektiven Gruppen. Abh. Math. Sem. Univ. Hamburg, 1928, 6, 303–322.

[148] S. Shelah. Interpreting set theory in the endomorphism semi-group of a free algebra or in the category. Annales Scientifiques L'universite Clermont, 1976, 13, 1–29.

[149] Shelah S. First order theory of permutation groups, Israel J. Math., 1973, 14, 149–162.

[150] Shelah S. errata to: First order theory of permutation groups. Israel J. Math., 1973, 15, 437–441.

[151] Shi-jian Yan. Linear groups over a ring. Chinese Math., 1965, 7(2), 163–179.

[152] Szmielew W. Elementary properties of Abelian groups. — Fundamenta Mathematica, 1955, 41, 203–271.

[153] R.M. Solovay. Real-valued mesurable cardinals. Proceedings of Simposia in Pure Math XIII Part I. ed D. Scott, AMS Providence R.I. 1971

[154] Stein M.R. Generators, relations and coverings of Chevalley groups over commutative rings. Amer. J. Math., 1971, 93(4), 965–1004.

[155] Stein M.R. Surjective stability in dimension 0 for K_2 and related functors, Trans. Amer. Soc., 1973, 178(1), 165–191.

[156] Stein M.R. Stability theorems for K_1, K_2 and related functors modeled on Chevalley groups. Japan J. Math., 1978, 4(1), 77–108.

[157] Steinberg R. Lectures on Chevalley groups, Yale University, 1967.

[158] Steinberg R., Automorphisms of finite linear groups, Canad. J. Math., 121, 1960, 606–615.

[159] Suslin A.A. On a theorem of Cohn. J. Sov. Math., 1981, 17(2), 1801–1803.

[160] Suslin A.A. On the structure of geneal linear group over polynomial ring. Soviet Math. Izv., 1977, 41(2), 503–516.

[161] Suslin A.A., Kopeiko V.I. Quadratic modules and orthogonal groups over polynomial rings. J. Sov. Math., 1982, 20(6), 2665–2691.

[162] Suzuki K., On the automorphisms of Chevalley groups over p-adic integer rings, Kumamoto J. Sci. (Math.), 16(1), 1984, 39–47.

[163] Swan R. Generators and relations for certain special linear groups. Adv. Math., 1971, 6, 1–77.

[164] Szele T. On direct decomposition of abelian groups. J. London Math. Soc., 1953, 28, 247–250.

[165] Szele T. On the basic subgroups of abelian p-groups. Acta Math. Acad. Sci. Hungar., 1954, 5, 129–141.

[166] Taddei G. Normalité des groupes élémentaire dans les groupes de Chevalley sur un anneau. Contemp. Math., Part II, 1986, 55, 693–710.

[167] Tarski A., Mostowski A., Robinson R. M. Undecidable theories. Amsterdam. North-Holland Publishing Comp., 1953.

[168] Tolstyh V. Set theory is interpretable in the automorphism group of an infinitely generated free group. J. London Math. Soc., 2000, 62(1), 17–26.

[169] Tolstykh V. Elementary equivalence of infinite-dimensional classical groups. Annals of Pure and Applied Logic, 2000, 105, 103–156.

[170] Vaserstein L.N. On normal subgroups of Chevalley groups over commutative rings. Tohoku Math. J., 1986, 36(5), 219–230.

[171] Vavilov N.A. Structure of Chevalley groups over commutative rings. Proc. Conf. Non-associative algebras and related topics (Hiroshima – 1990). World Sci. Publ., London et al., 1991, 219–335.

[172] Vavilov N.A. An A_3-proof of structure theorems for Chevalley groups of types E_6 and E_7. J. Pure Appl. Algebra, 2007, 1-16.

[173] Vavilov N.A., Plotkin E.B. Chevalley groups over commutative rings. I. Elementary calculations. Acta Applicandae Math., 1996, 45, 73–115.

[174] Vorst T. The general linear group of polynomial rings over regular rings. Comm. Algebra, 1981, 9(5), 499–509.

[175] Wan C.A. The automorphism of linear group over a noncommutative principal ideal domain of characteristic $\neq 2$. Acta Math. Sinica, 1957, 7, 533–573.

[176] Waterhouse W.C. Introduction to affine group schemes. Springer-Verlag, N.Y. et al., 1979.

[177] Waterhouse W.C. Automorphisms of $GL_n(R)$. Proc. Amer. Math. Soc., 1980, 79, 347–351.

[178] Waterhouse W.C. Automorphisms of quotients of $\prod GL(n_i)$. Pacif. J. Math., 1982, 79, 221–233.

[179] Waterhouse W.C. Automorphisms of $det(X_{ij})$: the group scheme approach. Adv. Math., 1987, 65(2), 171–203.

[180] Weeler W. H. Model theory of strictly upper triangular matrix rings. J. Symb. Logic, 1980, 45(3), 455–463.

Публикации автора по теме диссертации.

[181] Бунина Е.И. Элементарная эквивалентность унитарных линейных групп над полями. Фундаментальная и прикладная математика, 1998, 4, 1–14.

[182] Бунина Е.И. Элементарная эквивалентность унитарных линейных групп над кольцами и телами. Успехи математических наук, 1998, 53(2), 137–138.

[183] Бунина Е.И. Элементарная эквивалентность групп Шевалле. Успехи Мат. наук, 2001, 56(1), 157–158.

[184] Бунина Е.И., Михалев А.В. Элементарные свойства категорий модулей над кольцом, колец эндоморфизмов и групп автоморфизмов модулей. Фундаментальная и прикладная математика, 2004, 10(2), 51-134 (диссертанту принадлежат результаты о связи элементарной эквивалентности производных структур с эквивалентностью в логике второго порядка исходных структур).

[185] Бунина Е.И. Группы Шевалле над полями и их элементарные свойства. Успехи мат. наук, 2004, 59(5), 952–953.

[186] Бунина Е.И., Михалев А.В. Элементарная эквивалентность колец эндоморфизмов абелевых p-групп. Фундаментальная и прикладная математика, 2004, 10(2), 135-224 (диссертанту принадлежат результаты о необходимых и достаточных условиях элементарной эквивалентности колец эндоморфизмов абелевых p-групп).

[187] Bunina E.I., Mikhalev A.V. Combinatorial and Logical Aspects of Linear Groups and Chevalley Groups. Acta Applicandae Mathematicae, 2005, 85(1-3), 57-74. (это обзорная статья, в которой собраны результаты авторов).

[188] Е.И. Бунина, А.В. Михалев. Автоморфизмы полугруппы обратимых матриц с неотрицательными элементами. Фундаментальная и прикладная математика, 2005, 11(2), 3-23 (диссертанту принадлежит структурная теорема об автоморфизмах полугрупп обратимых матриц с неотрицательными коэффициентами над линейно упорядоченными кольцами).

[189] Бунина Е.И. Элементарные свойства групп Шевалле над локальными кольцами. Успехи математических наук, 2006, 61(2), 349-350.

[190] Е.И. Бунина, А.В. Михалев. Элементарная эквивалентность полугрупп обратимых матриц с неотрицательными элементами. Фундаментальная и прикладная математика, 2006, 12(2), 39-53 (диссертанту принадлежит описание необходимых и достаточных условий элементарной эквивалентности полугрупп обратимых матриц с неотрицательными коэффициентами над линейно упорядоченными кольцами).

[191] E.I. Bunina, A.V. Mikhalev. Elementary Theories of Abelian p-groups and second-order theories of their automorphism rings. The Bulletin of Symbolic Logic, 2006, 12(2), p.326 (диссертанту принадлежат результаты о необходимых и достаточных условиях элементарной эквивалентности колец эндоморфизмов абелевых p-групп).

[192] Бунина Е.И. Элементарная эквивалентность групп Шевалле над полями. Фундаментальная и прикладная математика, 2006, 12(8), 29-77.

[193] Бунина Е.И., Михалев А.В. Элементарные свойства категории полигонов над моноидом. Алгебра и логика, 2006, 45(6), 687-709 (диссертанту принадлежат необходимые и достаточные условия элементарной эквивалентности категорий полигонов над моноидами).

[194] Бунина Е.И. Автоморфизмы групп Шевалле некоторых типов над локальными кольцами. Успехи математических наук, 2007, 62(5), 143–144.

[195] Бунина Е.И. Автоморфизмы присоединенных групп Шевалле типов B_2 и G_2 над локальными кольцами. Фундаментальная и прикладная математика, 2007, 13(4), 3–27.

[196] Бунина Е.И. Автоморфизмы элементарных присоединенных групп Шевалле типов A_l, D_l, E_l над локальными кольцами. Алгебра и логика, 2009, 48(1), 443–470 (arXiv:math/0702046).

[197] Бунина Е.И. Элементарная эквивалентность групп Шевалле над локальными кольцами. Математический сборник, 2010, 201(3), 3–20.

[198] Bunina E.I. Automorphisms of Chevalley groups of type F_4 over local rings with 1/2. Journal of Algebra, 2010, 323, 2270–2289 (arXiv:0907.5592).

[199] Bunina E.I., Mikhalev A.V. Elementary properties of linear and algebraic groups. Journal of Mathematical Sciences, 2002, 110(3), 2595-2659 (обзорная работа, в которой §§ 3–5 — это результаты диссертанта).

[200] Bunina E.I., Mikhalev A.V. Elementary properties of linear groups and related questions. Journal of Mathematical Sciences, 2004, 123(2), 3921-3985 (обзорная работа, в которой §§ 4–6 — это результаты диссертанта).

[201] Е.И. Бунина, А.В. Михалев. Элементарная эквивалентность моноидов эндоморфизмов свободных полигонов. Чебышевский сборник, 2005, 6(4), 49-63 (диссертанту принадлежат необходимые и достаточные условия элементарной эквивалентности категорий полигонов над моноидами).

[202] Bunina E.I., Mikhalev A.V. Elementary equivalence of categories of modules and other algebraic structures, Journal of Mathematical Sciences, 2005, 131(5), 6004-6013 (диссертанту принадлежат результаты о связи элементарной эквивалентности производных структур с эквивалентностью в логике второго порядка исходных структур).

[203] Balmasov E.S., Bunina E.I. Elementary equivalence of unitary linear groups over rings. Journal of Mathematical Sciences, 2009, 162(5), 594–604 (диссертанту принадлежат результаты об элементарной эквивалентности унитарных линейных групп).

[204] Бунина Е.И. Автоморфизмы и нормализаторы групп Шевалле типов A_l, D_l, E_l над локальными кольцами с 1/2. Фундаментальная и прикладная математика, 2009, 15(2), 35–59 (arXiv:0907.5595).

[205] Бунина Е.И. Автоморфизмы групп Шевалле типа B_l над локальными кольцами с 1/2. Фундаментальная и прикладная математика, 2009, 15(7), 47–80. (arXiv:0911.4243).

[206] Бунина Е.И. Автоморфизмы групп Шевалле типов A_l, D_l, E_l над локальными кольцами с необратимой двойкой. Фундаментальная и прикладная математика, 2009, 15(7), 3–46.