

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В.ЛОМОНОСОВА

На правах рукописи

Калеева Галина Анатольевна

**Универсальная эквивалентность линейных групп над
кольцами**

1.1.5 — «Математическая логика, алгебра, теория чисел и дискретная
математика»

ДИССЕРТАЦИЯ
на соискание учёной степени
кандидата физико-математических наук

Научные руководители:
доктор физико-математических наук
Михалев Александр Александрович,
доктор физико-математических наук
Бунина Елена Игоревна

Москва — 2026

Оглавление

Введение	4
1 Предварительные сведения	11
1.1 Универсальная эквивалентность	11
1.2 Локальные кольца	13
1.3 Соглашения о сигнатурах	14
2 Полные и специальные линейные группы над полями	15
2.1 Из универсальной эквивалентности полей следует универсальная эквивалентность линейных групп	16
2.2 Поля характеристики 2	17
2.2.1 Свойства линейных групп, выражающиеся экзистенциальной формулой, в случае, когда в поле извлекаются корни третьей степени из единицы	18
2.2.2 Свойства линейных групп, выражающиеся экзистенциальной формулой, в случае, когда в поле не извлекаются корни третьей степени из единицы	21
2.2.3 Исследование свойств, выражающихся экзистенциальной формулой, без предположения о наличии корней третьей степени из единицы	29
2.2.4 Доказательство основной теоремы	33
2.3 Поля характеристики, отличной от 2	37
2.3.1 Случай характеристики 2 выделяется экзистенциальными формулами	38
2.3.2 Выделение размерности	39
2.3.3 Свойства инволюций	39
2.3.4 Выделение трансвекций в $GL_n(K)$ и при нечетном n в $SL_n(K)$	42
2.3.5 Сохранение матриц сложения и умножения в случае $GL_n(K)$ и при нечетном n в случае $SL_n(K)$	45
2.3.6 Случай $SL_2(K)$	46

2.3.7	Случай $SL_n(K)$ для четного $n \geq 4$	50
2.3.8	Замечания, завершающие доказательство	53
3	Полные и специальные линейные группы над локаль- ными коммутативными кольцами с $1/2$	54
3.1	Предварительные замечания, опирающиеся на ранее дока- занные факты	54
3.2	Инволюции	55
3.3	Матрицы с блоком $-E_{12} + E_{21}$ на диагонали	56
3.4	Сохранение трансвекций	59
4	Полные линейные группы над некоммутативными локаль- ными кольцами с $1/2$	63
4.1	Простая импликация: эквивалентность колец влечет экви- валентность групп	63
4.2	Сложная импликация: от групп к кольцам	64
4.2.1	Выделение размерности	64
4.2.2	Элементы порядка 2	66
4.2.3	Матрица $E + E_{12}$: общая часть	69
4.2.4	Случай 1: $\Phi(E + E_{12}) = E + E_{12}$	71
4.2.5	Случай 2: $\Phi(E + E_{12}) = E - E_{21}$	73
4.2.6	Соответствия, завершающие доказательство	74
	Заключение	76
	Литература	77

Введение

Общая характеристика работы

Диссертация относится к теории моделей. Во введении к своей классической книге «Теория моделей» Кейслер и Чэн [19] так определяют эту область:

теория моделей = универсальная алгебра + математическая логика.

Современная теория моделей изучает фундаментальную связь между синтаксисом, который представлен формальным языком, и семантикой, за которую отвечает математическая структура, описанная на этом языке. В диссертационной работе автором решается задача построения критерия универсальной эквивалентности для линейных групп над кольцами.

Актуальность темы и степень ее разработанности

Исследование логических свойств алгебраических структур восходит к работам А. И. Мальцева, который в 1961 году доказал [20], что элементарная эквивалентность групп $G_n(K)$ и $G_m(L)$, где $G = GL, SL, PGL, PSL$, $n, m \geq 3$, а K и L — поля характеристики 0, равносильна совпадению порядков $m = n$ и элементарной эквивалентности полей K и L . В дальнейшем были получены обобщения этой теоремы на другие типы колец и групп. Большим подспорьем в этой работе стали исследования изоморфизмов линейных групп над ассоциативными кольцами, которыми занимались И. З. Голубчик, А. В. Михалев [17] и другие. В дальнейшем К. И. Бейдар и А. В. Михалев разработали [2] общий подход к доказательству теорем мальцевского типа при помощи ультрапроизведений и обобщили теорему Мальцева на случай тел и простых ассоциативных колец.

Существует и иной путь, по которому может идти изучение вопроса, впервые поставленного Мальцевым, — это рассмотрение других видов эквивалентности. Мы можем обединить теорию, разрешив использование

только одного вида кванторов, и рассматривать алгебраические структуры в рамках этой обедненной — универсальной — теории. Первые критерии универсальной эквивалентности были установлены Ю. Ш. Гуревичем и А. И. Кокориным для упорядоченных абелевых групп [18] в 1963 г., Н. Г. Хисамиевым для структурно упорядоченных абелевых групп [25] в 1966 г., а затем П. С. Эклофом для произвольных абелевых групп [4] в 1972 г. Позднее другими исследователями были получены результаты об универсальной эквивалентности таких структур, как разрешимые группы (Е. И. Тимошенко [24]), частично коммутативные нильпотентные группы (А. А. Мищенко и Е. И. Тимошенко [7]), частично коммутативные метабелевы алгебры Ли (Е. Н. Порошенко и Е. И. Тимошенко [9]).

За последнее время в этой области были получены следующие результаты: доказан критерий мальцевского типа по отношению к элементарной эквивалентности для групп Шевалле с неразложимыми системами корней ранга > 1 над коммутативными кольцами (содержащими дополнительно $1/2$ для типов A_2, B_l, C_l, F_4 и G_2 и $1/3$ для типа G_2) (Е. И. Бунина [15]), доказано более сильное свойство жесткости первого порядка (first order rigidity) как для групп Шевалле над дедекиндовыми кольцами арифметического типа и локальными кольцами (D. Segal, K. Tent [10]), так и для арифметических решеток (N. Avni, A. Lubotzky, C. Meiri [1]; M. Sohrabi, A. Myasnikov [8]).

Естественными направлениями работы в этой области являются обобщения теорем мальцевского типа на другие виды групп или на другие типы логической эквивалентности. Автор настоящей работы следует по второму пути, занимаясь изучением универсальной эквивалентности линейных групп. В статье Е. И. Буниной и автора [26] изучена универсальная эквивалентность полных и специальных линейных групп над полями. Этот результат близок описанию изоморфизмов линейных групп, изложенному в уже упоминавшейся работе И. З. Голубчика и А. В. Михалева и статье А. С. Аткарской, Е. И. Буниной, А. В. Михалева [11], и опирается на них. Логическим продолжением предыдущего результата является результат автора для локальных коммутативных колец [27] и его обобщение на случай некоммутативных локальных колец [28].

Цели и задачи диссертации

Целью настоящей работы является построение критерия универсальной эквивалентности линейных групп. Для достижения этой цели были поставлены следующие задачи:

- 1) При помощи метода инволюций перенести критерий элементарной

эквивалентности линейных групп на случай универсальной эквивалентности линейных групп над полями характеристики, отличной от двойки.

- 2) Распространить критерий на случай полей характеристики 2.
- 3) Обобщить критерий на случай локальных ассоциативных колец, как коммутативных, так и некоммутиативных.

Положения, выносимые на защиту

На защиту выносятся

- 1) Критерий универсальной эквивалентности полных и специальных линейных групп над полями произвольной характеристики.
- 2) Критерий универсальной эквивалентности полных и специальных линейных групп порядков $n \geq 3$ над локальными коммутативными (ассоциативными с 1) кольцами с $1/2$.
- 3) Критерий универсальной эквивалентности полных линейных групп порядков $n \geq 3$ над локальными (ассоциативными с 1) кольцами с $1/2$.

Научная новизна

Результаты работы являются новыми и получены автором в соавторстве с научным руководителем (глава 2) и самостоятельно (главы 3 и 4).

Методы исследования

В работе используются методы теории моделей, теории групп, теории колец, линейной алгебры. Глава 2 существенным образом опирается на концепции линейной алгебры. Для случая полей характеристики, отличной от 2, используется классический метод инволюций. В случае полей характеристики 2 доказательство опирается на изучение элементов порядка 3. В дальнейшем в главах 3 и 4 используются методы коммутативной алгебры и теории ассоциативных (некоммутиативных) колец, здесь также находит применение метод инволюций.

Теоретическая и практическая ценность работы

Работа носит теоретический характер. Она дает понимание того, как соотносятся между собой логические свойства линейных групп и их колец коэффициентов. Результаты работы могут найти применение в теории групп и теории моделей. Разработанные методы могут быть полезны при дальнейших исследованиях линейных групп и построении критериев других типов логической эквивалентности.

Степень достоверности и апробация результатов

Достоверность полученных результатов обеспечивается строгими математическими доказательствами. Результаты работы хорошо согласуются с результатами, полученными другими авторами в смежных областях.

Результаты работы докладывались на следующих международных конференциях и научных семинарах:

- 1) Международная конференция «Мальцевские чтения» (Новосибирск, 2017).
- 2) Международная конференция «77th British Mathematical Colloquium» (Кардифф, Великобритания, 2026).
- 3) Семинар отдела математической логики «Теория доказательств» и «Logic Online Seminar» совместно с семинаром С. И. Адяна, МИАН (Москва, 2026).
- 4) Международная конференция «Logic Colloquium 2026 in conjunction with the British Logic Colloquium 2026» (Суонзи, Великобритания, 2026).
- 5) Научный семинар «Теория моделей» кафедры высшей алгебры механико-математического факультета МГУ под руководством проф. Буниной Е. И., многократные доклады с 2014 по 2021 гг.

Публикации автора

Результаты по теме диссертации изложены в 3 работах, все работы опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5 Математическая логика, алгебра, теория чисел и дискретная математика (физико-математические науки).

Объем и структура работы

Диссертация состоит из введения, 4 глав, заключения и списка литературы. Полный объем работы составляет 79 страниц. Список литературы содержит 28 наименований.

Основное содержание работы

Во **введении** описываются цели работы, освещается история и современное состояние области исследования, приводится краткая формулировка основных результатов.

В **главе 1** изложены необходимые сведения из теории моделей и теории колец.

В **первом параграфе** главы 1 вводятся определения универсальных и экзистенциальных формул, частичного изоморфизма, универсальной эквивалентности, а также приводится критерий универсальной эквивалентности.

Во **втором параграфе** главы 1 собраны необходимые факты о локальных кольцах (в коммутативном и некоммутативном случаях).

В **третьем параграфе** главы 1 определены сигнатуры рассматриваемых структур.

Глава 2 посвящена полным и специальным линейным группам над полями. Сначала формулируется основная теорема для случая полей:

Теорема 1. Пусть K и L — бесконечные поля. Группы $G_n(K)$ и $G_m(L)$ ($G = GL, SL, n, m \geq 2$) универсально эквивалентны тогда и только тогда, когда $n = m$ и поля K и L универсально эквивалентны.

В **первом параграфе** второй главы доказывается более легкая импликация: из универсальной эквивалентности полей следует универсальная эквивалентность групп. Доказательство использует тот факт, что все соотношения между матрицами можно записать поэлементно. Эта же идея позволяет доказать аналогичную импликацию и в случае более общих колец в дальнейших главах.

Далее доказательство разбито на два случая: 1) поле имеет характеристику 2, 2) характеристика поля отлична от 2. Во втором случае в доказательстве можно применить стандартный метод — метод инволюций, который не сработает при характеристике 2. Поэтому он претерпевает модификацию: вместо элементов порядка 2 мы рассматриваем элементы порядка 3. В обоих случаях доказательство идет по следующему плану. Сначала выделяется максимальное семейство попарно коммутирующих инволюций или элементов порядка 3. Далее выделяются элементарные

трансвекции, и с их помощью — матрицы, кодирующие сложение и умножение. Случай характеристики 2 дополнительно осложняется тем, что не всегда удастся диагонализировать элементы порядка 3, но это ограничение удастся обойти, если отдельно рассмотреть случай, когда в базовом поле не извлекаются корни третьей степени из единицы — доказано, что и в этом случае элементы порядка 3 приводятся к «красивому» виду.

В главе 3 теорема обобщается на случай коммутативных локальных колец. В начале главы сформулирована основная теорема и обозначены ограничения на кольцо и размерность, в рамках которых мы её доказываем (здесь мы требуем обратимость двойки, которая необходима для метода инволюций):

Теорема 2. Пусть R_1 и R_2 — локальные коммутативные кольца с $1/2$. Группы $G_n(R_1)$ и $G_m(R_2)$ ($G = GL, SL, n, m \geq 3$) универсально эквивалентны тогда и только тогда, когда $n = m$ и кольца R_1 и R_2 универсально эквивалентны.

В первом параграфе главы 3 доказана импликация от колец к группам, которая в коммутативном случае полностью аналогична случаю полей. Также случай конечных коммутативных колец сводится к известному ранее результату об изоморфизме.

Во втором параграфе главы 3 непосредственно применяется метод инволюций: выделяется максимальный набор попарно коммутирующих инволюций, которые диагональны в общем базисе. Далее при помощи инволюций выделяются матрицы, похожие на матрицы перестановок. С их помощью удастся выделить трансвекции, кодирующие сложение и умножение в кольце.

В главе 4 происходит дальнейшее ослабление требований к кольцам — они становятся не обязательно коммутативными (но остаются локальными). Основная теорема формулируется только для полных линейных групп:

Теорема 3. Пусть R_1 и R_2 — локальные (не обязательно коммутативные) кольца с $1/2$. Группы $GL_n(R_1)$ и $GL_m(R_2)$ ($n, m \geq 3$) универсально эквивалентны тогда и только тогда, когда $n = m$ и кольца R_1 и R_2 универсально эквивалентны либо $n = m$ и кольца R_1 и R_2^{op} универсально эквивалентны.

Интересно, что из-за некоммутативности колец критерий уже не формулируется в виде «группы универсально эквивалентны тогда и только тогда, когда кольца универсально эквивалентны», вместо этого возникает еще одна альтернатива: кольца могут быть «антиэквивалентны», то

есть одно кольцо универсально эквивалентно кольцу, противоположному другому кольцу. Это хорошо согласуется с ранее известными результатами об изоморфизмах.

Соответственно, в простой импликации возникает дополнительный случай: из универсальной «антиэквивалентности» колец получить универсальную эквивалентность групп. Это утверждение доказано в первом параграфе.

Также в некоммутативном случае усложняется обоснование конечного случая, но его удастся провести через промежуточные результаты для матричных колец (соответствующих группам) — это сделано во втором параграфе.

Далее проводится обобщение метода инволюций на некоммутативный случай. Благодаря локальности кольца удастся доказать результат, полностью аналогичный коммутативному случаю: получен максимальный набор попарно коммутирующих инволюций; все они диагонализированы в общем базисе, а на главной диагонали у них стоят ± 1 .

В заключение доказательства показано, что трансвекции «почти» сохраняют вид. Благодаря трансвекциям снова удастся выписать соотношения, в которых трансвекции кодируют операции в исходном или противоположном кольце. На этом доказательство теоремы полностью завершается.

Благодарности

Автор выражает глубокую благодарность своим научным руководителям доктору физико-математических наук, профессору Буниной Елене Игоревне — за постановку задач, постоянное внимание к работе и внимательное и доброе отношение — и доктору физико-математических наук, профессору Михалеву Александру Александровичу — за поддержание мотивации при подготовке диссертации и ценные советы. Автор хранит память об Александре Васильевиче Михалеве и благодарность за теплые воодушевляющие беседы и помощь в постановке задач. Автор выражает признательность сотрудникам кафедры высшей алгебры механико-математического факультета МГУ за доброжелательность и творческую атмосферу.

Глава 1

Предварительные сведения

1.1 Универсальная эквивалентность

Определение 1. Формула φ сигнатуры Σ называется *универсальной*, если ее предваренная нормальная форма имеет вид

$$\forall x_1 \dots \forall x_n \psi(x_1, \dots, x_n),$$

где ψ — бескванторная формула.

Определение 2. Формула φ сигнатуры Σ называется *экзистенциальной*, если ее предваренная нормальная форма имеет вид

$$\exists x_1 \dots \exists x_n \psi(x_1, \dots, x_n),$$

где ψ — бескванторная формула.

Определение 3. Две модели $\mathfrak{A}$ и $\mathfrak{B}$ сигнатуры Σ называются *универсально эквивалентными*, если для любого универсального предложения φ сигнатуры Σ выполнено

$$\mathfrak{A} \models \varphi \iff \mathfrak{B} \models \varphi.$$

Множество универсальных (экзистенциальных) предложений $\{\varphi \mid \mathfrak{A} \models \varphi\}$ сигнатуры Σ называется *универсальной (экзистенциальной) теорией* модели $\mathfrak{A}$ и обозначается $\text{Th}_\forall(\mathfrak{A})$ ($\text{Th}_\exists(\mathfrak{A})$). Таким образом, $\mathfrak{A} \equiv_\forall \mathfrak{B} \iff \text{Th}_\forall(\mathfrak{A}) = \text{Th}_\forall(\mathfrak{B})$ ($\mathfrak{A} \equiv_\exists \mathfrak{B} \iff \text{Th}_\exists(\mathfrak{A}) = \text{Th}_\exists(\mathfrak{B})$).

Замечание 1. В силу двойственности кванторов, $\text{Th}_\forall(\mathfrak{A}) = \text{Th}_\forall(\mathfrak{B}) \iff \text{Th}_\exists(\mathfrak{A}) = \text{Th}_\exists(\mathfrak{B})$.

Следуя [3], введем следующее определение.

Определение 4. Пусть A — произвольное подмножество элементов модели $\mathfrak{A}$ сигнатуры Σ . Тогда множество A вместе с индуцированными на нем предикатами, функциями и константами называется *частичной моделью* $\mathfrak{A}$. Более подробно,

- 1) для каждого n -местного предикатного символа $P \in \Sigma$

$$P_A = P_{\mathfrak{A}} \cap A^n;$$

- 2) для каждого n -местного функционального символа $F \in \Sigma$ операция

$$F_A(a_1, \dots, a_n)$$

определена тогда и только тогда, когда

$$F_{\mathfrak{A}}(a_1, \dots, a_n) \in A,$$

и в этом случае

$$F_A(a_1, \dots, a_n) = F_{\mathfrak{A}}(a_1, \dots, a_n);$$

- 3) для каждого константного символа $c \in \Sigma$ константа c определена в частичной модели тогда и только тогда, когда $c_{\mathfrak{A}} \in A$, и в этом случае её значение равно $c_{\mathfrak{A}}$.

Определение 5. Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — модели сигнатуры Σ , A и B — их частичные модели, а $f: A \rightarrow B$ — некоторое отображение. Отображение f называется *частичным изоморфизмом*, если выполнены следующие условия:

- 1) f инъективно;
 2) f сохраняет предикаты, функции и константы:

- а) для $P^n \in \Sigma$ и $a_0, \dots, a_{n-1} \in A$,

$$P_{\mathfrak{A}}a_0 \dots a_{n-1} \Leftrightarrow P_{\mathfrak{B}}f(a_0) \dots f(a_{n-1});$$

- б) для $F^n \in \Sigma$ и $a_0, \dots, a_{n-1}, a \in A$,

$$F_{\mathfrak{A}}(a_0, \dots, a_{n-1}) = a \Leftrightarrow F_{\mathfrak{B}}(f(a_0), \dots, f(a_{n-1})) = f(a);$$

- с) для $c \in \Sigma$ и $a \in A$,

$$c_{\mathfrak{A}} = a \Leftrightarrow c_{\mathfrak{B}} = f(a).$$

Определение 6. Частичный изоморфизм, у которого область определения конечна, называется *конечным частичным изоморфизмом*.

Теорема 4 (*критерий универсальной эквивалентности*, [23]). Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — модели сигнатуры Σ . Для того, чтобы модели $\mathfrak{A}$ и $\mathfrak{B}$ были универсально эквивалентны, необходимо и достаточно, чтобы для любой конечной подсигнатуры $\Sigma_1 \subset \Sigma$ любая конечная частичная модель структуры $\mathfrak{A}$ сигнатуры Σ_1 была частично изоморфна некоторой частичной модели структуры $\mathfrak{B}$ той же сигнатуры, и наоборот.

1.2 Локальные кольца

Здесь и далее мы считаем, что все кольца, которые участвуют в рассмотрении, являются ассоциативными и содержат единицу, не равную нулю.

Определение 7. Коммутативное ассоциативное кольцо с единицей называется *локальным*, если в нем содержится только один максимальный идеал.

Из определения следует, что если R — локальное коммутативное ассоциативное кольцо с 1, а I — его максимальный идеал, то I — множество всех необратимых элементов кольца R . Заметим также, что если в локальном кольце сумма двух элементов обратима, то хотя бы один из них обратим.

Более подробную информацию о локальных коммутативных кольцах можно найти в книге [12].

В случае, когда кольцо некоммутативно, эти свойства менее очевидны, тем не менее справедлива следующая лемма.

Лемма 1 (см. [5]). Для любого ненулевого кольца R следующие условия эквивалентны:

- 1) в R существует единственный максимальный левый идеал;
- 2) в R существует единственный максимальный правый идеал;
- 3) факторкольцо R по радикалу является телом;
- 4) множество необратимых элементов кольца R является идеалом;
- 5) множество необратимых элементов кольца R образует группу по сложению.

Определение 8. Кольцо, для которого выполняется хотя бы одно (а значит, и все) из условий предыдущей леммы, называется *локальным*.

Пусть R — локальное кольцо, а V — свободный правый R -модуль конечного ранга, тогда, согласно теореме 20.13 (2) из [5], ранг V однозначно определен. Рассмотрим $\mathrm{GL}(V)$ — группу обратимых R -линейных отображений V . Если фиксирован базис V , то можно отождествить $\mathrm{GL}(V)$ с группой обратимых матриц размера $n \times n$ с элементами из R , то есть с $\mathrm{GL}_n(R)$, где n — ранг модуля V .

1.3 Соглашения о сигнатурах

Мы рассматриваем кольца и группы в стандартных сигнатурах. Для групп сигнатура состоит из бинарного функционального символа групповой операции, унарного функционального символа взятия обратного элемента и константы для нейтрального элемента: $\langle \cdot, {}^{-1}, e \rangle$. Для колец сигнатура состоит из бинарных функциональных символов сложения и умножения, унарного функционального символа взятия противоположного элемента и констант для нуля и единицы: $\langle +, \cdot, -, 0, 1 \rangle$. По умолчанию все рассматриваемые сигнатуры — с равенством.

Глава 2

Полные и специальные линейные группы над полями

Данная глава посвящена доказательству следующей теоремы:

Теорема 1. Пусть K и L — бесконечные поля. Группы $G_n(K)$ и $G_m(L)$ ($G = GL, SL, n, m \geq 2$) универсально эквивалентны тогда и только тогда, когда $n = m$ и поля K и L универсально эквивалентны.

Замечание 2. Универсальная эквивалентность для полей и линейных групп не совпадает с элементарной эквивалентностью. Действительно, по теореме Мальцева, достаточно привести пример двух универсально эквивалентных, но не элементарно эквивалентных полей. Рассмотрим алгебраическое замыкание поля рациональных чисел $\overline{\mathbb{Q}}$ и поле рациональных дробей над ним $\overline{\mathbb{Q}}(t)$. Эти поля не элементарно эквивалентны, так как одно из них алгебраически замкнуто, а в другом не извлекаются квадратные корни, например, из t . При этом они являются универсально эквивалентными. Действительно, рассмотрим башню расширений

$$\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}(t) \subset \overline{\overline{\mathbb{Q}}(t)}.$$

Во-первых, $\overline{\mathbb{Q}} \equiv \overline{\overline{\mathbb{Q}}(t)}$, как алгебраически замкнутые поля характеристики 0. А во-вторых, для экзистенциальных теорий существует естественное вложение

$$\text{Th}_{\exists}(\overline{\mathbb{Q}}) \subset \text{Th}_{\exists}(\overline{\mathbb{Q}}(t)) \subset \text{Th}_{\exists}(\overline{\overline{\mathbb{Q}}(t)}),$$

но из элементарной эквивалентности следует, что экзистенциальные теории для крайних полей совпадают, а значит, все три экзистенциальные теории совпадают и $\overline{\mathbb{Q}} \equiv_{\forall} \overline{\mathbb{Q}}(t)$.

Замечание 3. Если поля K и L конечны, то универсальная эквивалентность совпадает с изоморфизмом, и можно сослаться на следующую теорему, изложенную в лекциях [21]:

Теорема 5. Пусть n и m — натуральные числа, $n, m \geq 2$, K и L — произвольные поля. Тогда следующие условия эквивалентны:

- 1) $n = m$ и $K \cong L$,
- 2) $\mathrm{GL}_n(K) \cong \mathrm{GL}_m(L)$,
- 3) $\mathrm{SL}_n(K) \cong \mathrm{SL}_m(L)$.

2.1 Из универсальной эквивалентности полей следует универсальная эквивалентность линейных групп

В этом разделе докажем более простую импликацию теоремы.

Предложение 1. Пусть K и L — универсально эквивалентные бесконечные поля. Тогда для любого натурального n

$$\mathrm{GL}_n(K) \equiv_{\forall} \mathrm{GL}_n(L), \mathrm{SL}_n(K) \equiv_{\forall} \mathrm{SL}_n(L).$$

Доказательство. Зададим линейные группы как подсистемы в K^{n^2} .

$$\begin{aligned} \mathrm{GL}_n(K) &= \left\{ (a_1, \dots, a_{n^2}) \in K^{n^2} \mid \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^n a_{(i-1)n+\sigma(i)} \neq 0 \right\}; \\ \mathrm{SL}_n(K) &= \left\{ (a_1, \dots, a_{n^2}) \in K^{n^2} \mid \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^n a_{(i-1)n+\sigma(i)} = 1 \right\}. \end{aligned}$$

Умножение в $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ задается следующей формулой:

$$(a_1, \dots, a_{n^2}) \cdot (b_1, \dots, b_{n^2}) = (c_1, \dots, c_{n^2}),$$

где

$$c_k = c_{(i-1)n+j} = \sum_{l=1}^n a_{(i-1)n+l} \cdot b_{(l-1)n+j}, k = 1, \dots, n^2, i, j = 1, \dots, n.$$

Таким образом, любую конечную подсистему в $\mathrm{GL}_n(K)$ или $\mathrm{SL}_n(K)$ мы можем задать как конечную подсистему в K^{n^2} , так как поля K и L

универсально эквивалентны, то для нее можем найти конечную частично изоморфную ей подсистему в L^{n^2} , а значит, для исходной подсистемы в $\text{GL}_n(K)$ или $\text{SL}_n(K)$ можем найти конечную частично изоморфную ей в $\text{GL}_n(L)$ или $\text{SL}_n(L)$ соответственно и наоборот.

Предложение доказано. $\square$

Доказательство противоположной импликации разобьем на два случая: 1) характеристика полей K и L равна двум; 2) характеристики полей K и L отличны от двух.

2.2 Поля характеристики 2

В настоящей части работы докажем следующую теорему.

Теорема 6. Пусть K и L — бесконечные поля характеристики 2, группы $G_n(K)$ и $G_m(L)$ ($G = \text{GL}, \text{SL}$, $n, m \geq 2$) универсально эквивалентны. Тогда $n = m$ и поля K и L универсально эквивалентны.

Здесь и далее в этом разделе все рассматриваемые поля имеют характеристику 2.

Лемма 2. Пусть поле K имеет характеристику 2, $n = 2$ или $n = 3$. Пусть при этом $A \in \text{GL}_n(K)$ ($A \in \text{SL}_n(K)$), $A \neq E$, $A^2 = E$. Тогда в некотором базисе матрица A имеет вид $E + E_{12}$.

Доказательство. Пусть $V_0 = \text{Ker}(A + E)$ — это ненулевое подпространство в K^n . Для любого вектора $t \in V_0$ выполнено $At = t$. Так как A не единичный оператор, то $\dim V_0 < n$.

Рассмотрим вектор $x \notin V_0$. Если $(A + E)x = \lambda x$, то $(A + E)^2x = \lambda^2x = 0$, следовательно, учитывая $x \neq 0$, $\lambda = 0$, а значит, $x \in V_0$. Противоречие.

Следовательно, $(A + E)x = y$, x и y — линейно независимые векторы. Из этого же равенства получаем, что $Ax = x + y$. Действие оператора A на векторе y : $Ay = A(Ax + x) = x + Ax = y$. Отсюда сразу получаем, что при $n = 2$ матрица оператора A в базисе $\{y, x\}$ равна $E + E_{12}$.

Если $n = 3$ и $\dim V_0 = 2$, то утверждение верно. Действительно, в базисе, состоящем из векторов y, x и некоторого вектора из V_0 , линейно независимого с y , матрица оператора A имеет искомый вид. Предположим теперь, что $\dim V_0 = 1$. Дополним линейно независимую систему $\{y, x\}$ до базиса вектором z и рассмотрим действие оператора A на векторе z : $Az = z + h$, z и h линейно независимы. Тогда $Ah = A(Az + z) = z + Az = h$, значит $h \in V_0$ и $h = \mu y$. Рассмотрим сумму $Az + \mu Ax = z + \mu y + \mu x + \mu y = z + \mu x$, отсюда следует, что $z + \mu x \in V_0$,

значит $z + \mu x = \nu y$, что противоречит линейной независимости x, y, z . Утверждение доказано. $\square$

Далее мы будем рассматривать два случая: когда в поле извлекаются корни третьей степени из единицы, т.е. существуют два таких числа $\xi_1 \neq \xi_2$, отличные от $\xi_0 = 1$, что $\xi_1^3 = \xi_2^3 = 1$, и противоположный случай — когда таких корней в поле нет.

2.2.1 Свойства линейных групп, выражающиеся экзистенциальной формулой, в случае, когда в поле извлекаются корни третьей степени из единицы

Лемма 3. Пусть в поле K характеристики 2 извлекаются корни третьей степени из единицы. Тогда в группе $\mathrm{GL}_n(K)$ существует подмножество максимум из $3^n - 1$ попарно коммутирующих матриц порядка 3, в группе $\mathrm{SL}_n(K)$ — из $3^{n-1} - 1$ попарно коммутирующих матриц порядка 3. В некотором базисе все они имеют вид $\mathrm{diag}[\xi_1, \dots, \xi_n]$, где все ξ_i — корни третьей степени из единицы.

Доказательство. Утверждение следует из того, что каждая такая матрица диагонализуема, а также из того, что множество попарно коммутирующих матриц имеет общий собственный вектор, таким образом, все эти матрицы имеют диагональный вид в общем базисе. $\square$

Обозначим через $\mathcal{A}(\mathrm{GL}_n(K))$ ($\mathcal{A}(\mathrm{SL}_n(K))$) или просто $\mathcal{A}$, если понятно, о какой группе идет речь) некоторый фиксированный максимальный набор матриц вида $\mathrm{diag}[\xi_1, \dots, \xi_n]$, существование которого доказано в лемме 3.

Лемма 4. Пусть в поле K извлекаются корни третьей степени из единицы и $n \geq 4$. Тогда в группах $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ такая матрица порядка 2, что при ее сопряжении всеми матрицами из набора $\mathcal{A}$ получаются ровно три различных коммутирующих между собой матрицы, имеет вид $E + E_{ij}$ ($i \neq j$) в базисе, в котором вид матриц системы $\mathcal{A}$ не изменится.

Доказательство. Пусть для матрицы A выполнено: $A \neq E$, $A^2 = E$, при сопряжении матрицы A всеми матрицами из набора $\mathcal{A}$ получаются ровно три различные матрицы. Предположим, что в матрице A есть, по крайней мере, два внедиагональных ненулевых элемента a_{pq} и a_{ts} таких, что $(p, q) \neq (s, t)$, тогда, сопрягая, можем добиться того, что a_{pq} и a_{ts} умножаются на любой корень третьей степени из единицы независимо

друг от друга, т. е. получим более трех различных матриц сопряжением — противоречие. Пусть теперь $(p, q) = (s, t)$ и других внедиагональных ненулевых элементов нет, тогда

$$A = \begin{pmatrix} 1 & 0 & \dots\dots\dots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & 1 & \vdots \\ \vdots & & & \vdots \\ \vdots & & a_{ii} & 0 & \dots & 0 & a_{ij} & \vdots \\ \vdots & & 0 & 1 & & & 0 & \vdots \\ \vdots & & \vdots & & \ddots & & \vdots & \vdots \\ \vdots & & 0 & & & 1 & 0 & \vdots \\ \vdots & & a_{ji} & 0 & \dots & 0 & a_{jj} & \vdots \\ \vdots & & & & & & & 1 & \vdots \\ \vdots & & & & & & & & \ddots & 0 \\ 0 & \dots\dots\dots & & & & & 0 & 1 \end{pmatrix}.$$

Значит, нужно рассмотреть блок вида

$$\begin{pmatrix} a_{ii} & a_{ij} \\ a_{ji} & a_{jj} \end{pmatrix}.$$

При его сопряжении диагональными матрицами из системы $\mathcal{A}$ получаются три матрицы:

$$\begin{pmatrix} a_{ii} & a_{ij} \\ a_{ji} & a_{jj} \end{pmatrix}, \begin{pmatrix} a_{ii} & \xi^2 a_{ij} \\ \xi a_{ji} & a_{jj} \end{pmatrix}, \begin{pmatrix} a_{ii} & \xi a_{ij} \\ \xi^2 a_{ji} & a_{jj} \end{pmatrix},$$

где ξ — неединичный корень третьей степени из 1.

Так как любые 2 из трех записанных выше матриц коммутируют, то получаем следующее соотношение:

$$\begin{pmatrix} a_{ii} & a_{ij} \\ a_{ji} & a_{jj} \end{pmatrix} \begin{pmatrix} a_{ii} & \xi a_{ij} \\ \xi^2 a_{ji} & a_{jj} \end{pmatrix} = \begin{pmatrix} a_{ii}^2 + \xi^2 a_{ij} a_{ji} & \xi a_{ii} a_{ij} + a_{ij} a_{jj} \\ a_{ii} a_{ji} + \xi^2 a_{ji} a_{jj} & \xi a_{ij} a_{ji} + a_{jj}^2 \end{pmatrix} = \\ = \begin{pmatrix} a_{ii} & \xi a_{ij} \\ \xi^2 a_{ji} & a_{jj} \end{pmatrix} \begin{pmatrix} a_{ii} & a_{ij} \\ a_{ji} & a_{jj} \end{pmatrix} = \begin{pmatrix} a_{ii}^2 + \xi a_{ij} a_{ji} & a_{ii} a_{ij} + \xi a_{ij} a_{jj} \\ \xi^2 a_{ii} a_{ji} + a_{ji} a_{jj} & \xi^2 a_{ij} a_{ji} + a_{jj}^2 \end{pmatrix},$$

откуда, в частности, следует, что $a_{ij}a_{ji} = 0$. Учитывая условие $A^2 = E$, получаем, что $a_{ii} = a_{jj} = 1$.

Пусть $a_{ij} \neq 0$. Если $a_{ij} \neq 1$, то сделаем замену базиса, порожденную матрицей $E + (a_{ij} + 1)E_{jj}$, которая коммутирует со всеми матрицами из системы $\mathcal{A}$:

$$\begin{pmatrix} 1 & 0 \\ 0 & a_{ij} \end{pmatrix} \begin{pmatrix} 1 & a_{ij} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{a_{ij}} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

что и требовалось. $\square$

Лемма 5. Пусть в поле K извлекаются корни третьей степени из единицы и $n \geq 4$. Тогда в группах $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ максимальный набор таких матриц порядка 2 с попарно различными централизаторами, что при сопряжении каждой из них всеми матрицами набора $\mathcal{A}$ получаются ровно три различных матрицы и любые две из них коммутируют, состоит из $n^2 - n$ матриц, имеющих вид $E + c_{ij}E_{ij}$ ($i, j = 1, \dots, n; i \neq j, c_{ij} \in K^*$) в базисе, в котором вид матриц системы $\mathcal{A}$ не изменится.

Доказательство. Из доказательства предыдущей леммы получаем, что все интересующие нас матрицы порядка 2 имеют в общем базисе (в котором вид матриц системы $\mathcal{A}$ не изменится) требуемый вид. Учитывая, что они имеют попарно различные централизаторы, получаем, что их не более $n^2 - n$ штук, и такое количество найдется. $\square$

Лемма 6. Пусть в полях K и L характеристики 2 извлекаются корни третьей степени из единицы и известно, что $\mathrm{G}_n(K) \equiv_{\forall} \mathrm{G}_m(L)$ ($\mathrm{G} = \mathrm{GL}$ или SL). Тогда $n = m$.

Доказательство. Пусть $\mathrm{GL}_n(K) \equiv_{\forall} \mathrm{GL}_m(L)$. Рассмотрим экзистенциальную формулу

$$\begin{aligned} \exists A_1 \dots \exists A_{3^{N-1}-1} \left(\bigwedge_{i=1}^{3^{N-1}-1} (\neg A_i = E) \& \bigwedge_{\substack{i,j=1 \\ i \neq j}}^{3^{N-1}-1} (\neg A_i = A_j) \& \right. \\ \left. \& \bigwedge_{i,j=1}^{3^{N-1}-1} (A_i A_j = A_j A_i) \& \bigwedge_{i=1}^{3^{N-1}-1} (A_i^3 = E) \right), \quad (2.1) \end{aligned}$$

утверждающую наличие набора из $3^{N-1} - 1$ попарно различных неединичных попарно коммутирующих матриц порядка 3. Наибольшее значение N , для которого формула (2.1) истинна в обеих группах, согласно лемме 3, одинаково и равно $N = n + 1 = m + 1$.

Аналогично в случае, когда $\mathrm{SL}_n(K) \equiv_{\forall} \mathrm{SL}_m(L)$, для наибольшего N , для которого формула (2.1) истинна в каждой паре групп, выполнено условие $N = m = n$. $\square$

2.2.2 Свойства линейных групп, выражающиеся экзистенциальной формулой, в случае, когда в поле не извлекаются корни третьей степени из единицы

Лемма 7. Если в поле K характеристики 2 не извлекаются корни третьей степени из единицы, то в группах $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ любая матрица порядка три в некотором базисе имеет блочно-диагональный вид, где каждый блок — это одна из матриц $E_{11} + E_{12} + E_{21}$, $E_{12} + E_{21} + E_{22}$ или E . Максимальный набор попарно коммутирующих матриц порядка 3 состоит из $3^{\lfloor n/2 \rfloor} - 1$ матриц, имеющих в некотором базисе блочно-диагональный вид, где каждый блок — это одна из матриц $E_{11} + E_{12} + E_{21}$, $E_{12} + E_{21} + E_{22}$ или E .

Доказательство. При доказательстве будем пользоваться приемом, изложенным в статье [14]. Рассмотрим такую неединичную матрицу A , что $A^3 = E$. Пусть $\sigma = E + A + A^2$. Заметим, что $\sigma^2 = \sigma$. Пространство K^n раскладывается в сумму подпространств $V_0 = \sigma K^n$ и $V_1 = (E + \sigma)K^n$, так как любой вектор $x \in K^n$ представим в виде $x = \sigma x + (E + \sigma)x$.

На подпространстве V_0 оператор A действует тождественно. Действительно, если $x \in V_0$, то $x = \sigma y$ для некоторого $y \in K^n$, тогда

$$Ax = A\sigma y = A(E + A + A^2)y = \sigma y = x.$$

Теперь покажем, что $V_1 = \mathrm{Ker} \sigma$. Пусть $x \in V_1$, тогда $x = (E + \sigma)y$ для некоторого $y \in K^n$. Далее,

$$\sigma x = \sigma(E + \sigma)y = (\sigma + \sigma^2)y = 0.$$

Для $x \in \mathrm{Ker} \sigma$, очевидно, $x = (E + \sigma)x \in V_1$.

Из доказанного также следует, что сумма V_0 и V_1 прямая: $K^n = V_0 \oplus V_1$.

Рассмотрим действие оператора A на подпространстве V_1 . Предположим сначала, что $x \in V_1$ — собственный вектор оператора A . Тогда $Ax = \lambda x$, значит, $\lambda^3 = 1$, поэтому $\lambda = 1$. В этом случае придем к противоречию: $0 = \sigma x = (E + A + A^2)x = x + x + x = x$.

Пусть теперь ненулевой вектор $x \in V_1$ и не является собственным вектором оператора A . Тогда $y = Ax \in V_1$ ($x = (E + \sigma)t$ для некоторого $t \in K^n$, $y = Ax = A(E + \sigma)t = (E + \sigma)(At) \in V_1$), x и y — линейно независимые векторы. Действие оператора A на y : $Ay = A^2x = (\sigma + A + E)x = y + x$. Таким образом, ограничение оператора A на инвариантное

подпространство $\langle x, Ax \rangle$ имеет вид

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

в базисе, составленном из векторов x и $y = Ax$.

Теперь покажем, что подпространство V_1 распадается в прямую сумму двумерных инвариантных подпространств такого же вида. По индукции, предположим, что уже построена прямая сумма подпространств $\langle x_1, Ax_1 \rangle, \dots, \langle x_k, Ax_k \rangle$ (она инвариантна относительно оператора A), не совпадающая со всем V_1 и вне линейной оболочки $\langle x_1, Ax_1, \dots, x_k, Ax_k \rangle$ есть несобственные векторы. Выберем такой вектор x_{k+1} и покажем, что Ax_{k+1} линейно независим со всеми предыдущими векторами. Предположим противное: $Ax_{k+1} = \lambda x_{k+1} + v$, где $v \in \langle x_1, Ax_1, \dots, x_k, Ax_k \rangle$. На факторпространстве $V_1 / \langle x_1, Ax_1, \dots, x_k, Ax_k \rangle$ выполняется $\overline{A}\overline{x}_{k+1} = \lambda \overline{x}_{k+1}$, а так как $\overline{A}^2 + \overline{A} + E = 0$, то $(\lambda^2 + \lambda + 1)\overline{x}_{k+1} = 0$. Согласно выбору вектора x_{k+1} , его класс $\overline{x}_{k+1}$ отличен от нуля, следовательно, $\lambda^2 + \lambda + 1 = 0$, откуда получаем, что λ — неединичный корень третьей степени из единицы. Противоречие.

Осталось показать, что все матрицы в общем базисе имеют требуемый вид. Пусть ξ — неединичный корень третьей степени из единицы, тогда все различные корни третьей степени из единицы: $1, \xi, \xi^2$. Над алгебраическим замыканием поля K и даже над расширением $K(\xi)$ все рассматриваемые матрицы одновременно диагонализированы, и на диагонали у них стоят $1, \xi, \xi^2$. Так как мы уже знаем, что над K они имеют блочный вид и характеристический многочлен каждого неединичного блока равен $x^2 + x + 1$, то собственные значения неединичных блоков равны ξ и ξ^2 , то есть в диагональных матрицах над $K(\xi)$ количество ξ и ξ^2 одинаково.

Теперь покажем, что мы можем собрать пары ξ и ξ^2 так, чтобы они шли подряд во всех матрицах одновременно. Пусть A, B — коммутирующие матрицы порядка 3 с коэффициентами из K и пусть v — их общий собственный вектор, соответствующий неединичным собственным значениям λ_A и λ_B соответственно (над $K(\xi)$):

$$Av = \lambda_A v, \quad Bv = \lambda_B v.$$

Пусть φ — автоморфизм расширения $K(\xi)$ над K , который переставляет ξ и ξ^2 . Применим его поэлементно к соотношениям выше и получим:

$$A\varphi(v) = \varphi(\lambda_A)\varphi(v), \quad B\varphi(v) = \varphi(\lambda_B)\varphi(v),$$

откуда мы видим, что вместе с собственным вектором v у матриц A и B есть собственный вектор $\varphi(v)$ с собственными значениями, которые сопряжены исходным. Этой паре собственных значений над K соответствуют блоки размера 2×2 с собственными значениями ξ и ξ^2 , стоящие в матрицах A и B на одних и тех же местах.

Если эти блоки размера 2×2 в диагональном виде над $K(\xi)$ совпадают, то и над K им соответствует один и тот же блок. Если же в диагональном виде это блоки $\text{diag}[\xi, \xi^2]$ и $\text{diag}[\xi^2, \xi]$ и первому соответствует блок $E_{11} + E_{12} + E_{21}$ над K , то второму над K соответствует обратный первому блок $E_{12} + E_{21} + E_{22}$. $\square$

Пусть $\mathcal{B}(\text{GL}_n(K))$ ($\mathcal{B}(\text{SL}_n(K))$) — некоторый фиксированный максимальный набор попарно коммутирующих матриц порядка 3 из леммы 7.

Лемма 8. Пусть в бесконечном поле K не извлекаются корни третьей степени из единицы и $n > 5$. Тогда в $\text{GL}_n(K)$ и $\text{SL}_n(K)$ матрица, имеющая в некотором базисе вид $E + E_{12}$, выделяется экзистенциальной формулой.

Доказательство. Матрицы из набора $\mathcal{B}(\text{GL}_n(K))$ ($\mathcal{B}(\text{SL}_n(K))$) в соответствующих группах выделяются экзистенциальной формулой: существует $3^{\lfloor \frac{n}{2} \rfloor} - 1$ различных попарно коммутирующих матриц порядка 3. Этот набор матриц разбивается на классы сопряженности — множества матриц, содержащих одинаковое количество неединичных блоков. Присвоим каждому классу номер, равный количеству неединичных блоков в каждой матрице класса. Таким образом, существует $\lfloor \frac{n}{2} \rfloor$ классов сопряженности, в k -м классе $2^k C_{\lfloor n/2 \rfloor}^k$ матриц, $k = 1, \dots, \lfloor \frac{n}{2} \rfloor$.

Будем последовательно нумеровать матрицы из всех классов сопряженности по убыванию номеров классов и выписывать соответствующие соотношения попарной сопряженности матриц каждого класса в нашу формулу, при этом она останется экзистенциальной.

Покажем, что не существует биекции классов сопряженности, не оставляющей на месте первый класс. Достаточно доказать, что

$$2 \lfloor \frac{n}{2} \rfloor < 2^k C_{\lfloor n/2 \rfloor}^k \text{ при } 1 < k \leq \lfloor \frac{n}{2} \rfloor.$$

Так как $n > 5$, то $\lfloor \frac{n}{2} \rfloor > 2$, тогда

$$\text{при } k = \lfloor \frac{n}{2} \rfloor \text{ получим } 2 \lfloor \frac{n}{2} \rfloor < 1 \cdot 2^{\lfloor n/2 \rfloor},$$

$$\text{а при } 1 < k < \lfloor \frac{n}{2} \rfloor \text{ получим } 2 \lfloor \frac{n}{2} \rfloor < 2^k \cdot \lfloor \frac{n}{2} \rfloor \leq 2^k \cdot C_{\lfloor n/2 \rfloor}^k.$$

Таким образом, мы можем выделить все матрицы, имеющие ровно один неединичный блок. Все эти матрицы разбиваются на пары взаимно обратных. Выберем из каждой пары по одной матрице и обозначим их $A_1, \dots, A_{[n/2]}$ и пусть $\mathcal{C} = \{A_1, \dots, A_{[n/2]}\}$. Можем считать, что блоки размерности 2 идут подряд, а номер матрицы равен номеру места, на котором у нее стоит неединичный блок.

Рассмотрим матрицу $B = (b_{ij})$, коммутирующую с A_1 , и докажем, что $b_{1i} = b_{2i} = 0$, $b_{i1} = b_{i2} = 0$, $i = 3, \dots, n$. Не умаляя общности, можем считать, что неединичный блок матрицы A_1 равен $E_{11} + E_{12} + E_{21}$. Тогда

$$\begin{pmatrix} 1 & 1 & & & \\ 1 & 0 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & b_{13} & \dots & b_{1n} \\ b_{21} & b_{22} & b_{23} & \dots & b_{2n} \\ b_{31} & b_{32} & b_{33} & \dots & b_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & b_{n3} & \dots & b_{nn} \end{pmatrix} =$$

$$= \begin{pmatrix} b_{11} + b_{21} & b_{12} + b_{22} & b_{13} + b_{23} & \dots & b_{1n} + b_{2n} \\ b_{11} & b_{12} & b_{13} & \dots & b_{1n} \\ b_{31} & b_{32} & b_{33} & \dots & b_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & b_{n3} & \dots & b_{nn} \end{pmatrix},$$

$$\begin{pmatrix} b_{11} & b_{12} & b_{13} & \dots & b_{1n} \\ b_{21} & b_{22} & b_{23} & \dots & b_{2n} \\ b_{31} & b_{32} & b_{33} & \dots & b_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & b_{n3} & \dots & b_{nn} \end{pmatrix} \begin{pmatrix} 1 & 1 & & & \\ 1 & 0 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} b_{11} + b_{12} & b_{11} & b_{13} & \dots & b_{1n} \\ b_{21} + b_{22} & b_{21} & b_{23} & \dots & b_{2n} \\ b_{31} + b_{32} & b_{31} & b_{33} & \dots & b_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ b_{n1} + b_{n2} & b_{n1} & b_{n3} & \dots & b_{nn} \end{pmatrix}.$$

Отсюда получаем, что $b_{1i} = b_{1i} + b_{2i} = b_{2i} = 0$, $b_{i1} = b_{i1} + b_{i2} = b_{i2} = 0$, $i = 3, \dots, n$.

Аналогично, если $B = (b_{ij})$ коммутирует с A_m , то $b_{2m-1,i} = b_{2m,i} = 0$, $b_{i,2m-1} = b_{i,2m} = 0$, $i = 1, \dots, 2m-1, 2m, \dots, n$.

Теперь рассмотрим матрицу C , коммутирующую с $\left[\frac{n}{2}\right] - 1$ из матриц A_i (можем считать, что это $A_1, \dots, A_{[n/2]-1}$, иначе сделаем замену

базиса, переставляющую блоки) и имеющую порядок 2. Согласно доказанному выше, матрица C имеет блочно-диагональную структуру: у нее либо $\lfloor \frac{n}{2} \rfloor = \frac{n}{2}$ блоков размерности 2, либо $\lfloor \frac{n}{2} \rfloor - 1$ блок размерности 2 и один блок (последний) размерности 3.

Кроме того, все блоки матрицы C в квадрате равны E , и все, кроме последнего, коммутируют с блоком порядка 3. Таким образом, для блока, коммутирующего с блоком порядка 3, имеем:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a+b & a \\ c+d & c \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ a & b \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Из матричных соотношений следует, что $b = c$ и $b(a+d) = 0$. Если $b = 0$, то $a = d = 1$, $b = c = 0$, иначе $a = d$, а так как $a = b+d$, то $b = 0$, значит, и $c = 0$, и снова $a = d = 1$.

Мы получили, что все, кроме последнего, блоки матрицы C — единичные, а последний имеет размерность 2 или 3 и порядок 2, значит, согласно лемме 2, в некотором базисе (в котором вид матриц системы $\mathcal{B}$, вообще говоря, изменится) матрица C имеет вид $E + E_{12}$. $\square$

Лемма 9. Пусть в бесконечном поле K не извлекаются корни третьей степени из единицы и $n > 5$. Если n четно, то в группах $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ для каждой матрицы из системы $\mathcal{C}$ (определенной в доказательстве леммы 8) не найдется двух таких различных коммутирующих между собой матриц порядка 2 с различными централизаторами, что они коммутируют со всеми матрицами из системы $\mathcal{C}$, кроме данной. Если n нечетно, то в группах $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ для матрицы из системы $\mathcal{C}$ существуют 2 таких различных коммутирующих между собой матрицы порядка 2 с различными централизаторами, что они коммутируют со всеми матрицами из системы $\mathcal{C}$, кроме данной.

Доказательство. Если n четно, то, согласно доказательству леммы 8, матрица A_e порядка 2, коммутирующая со всеми, кроме одной (назовем ее B_e и будем считать, что у нее неединичный только первый блок), матрицами системы $\mathcal{C}$ в некотором базисе (в котором все матрицы системы $\mathcal{C}$, кроме, быть может, B_e , будут иметь прежний вид, а у матрицы B_e

может поменяться только вид первого блока) имеет вид

$$A_e = \begin{pmatrix} 1 & 1 & & & \\ 0 & 1 & & & \\ & & E & & \\ & & & \ddots & \\ & & & & E \end{pmatrix},$$

где все единичные блоки имеют размерность 2, а разбиение на блоки соответствует разбиению на блоки в матрицах системы $\mathcal{C}$. А все матрицы порядка 2, коммутирующие со всеми матрицами из $\mathcal{C}$, кроме B_e , а также с матрицей A_e в том же базисе имеют вид

$$\begin{pmatrix} 1 & \alpha & & \\ 0 & 1 & & \\ & & E & \end{pmatrix},$$

но централизатор каждой такой матрицы совпадает с централизатором матрицы A_e .

Пусть теперь n нечетно, тогда, согласно лемме 8, матрица A_o порядка 2, коммутирующая со всеми, кроме одной (назовем ее B_o), матрицами системы $\mathcal{C}$ в том же базисе имеет вид

$$A_o = \begin{pmatrix} \tilde{A}_o & & & \\ & E & & \\ & & \ddots & \\ & & & E \end{pmatrix},$$

где блок $\tilde{A}_o$ имеет размерность 3, а все единичные блоки имеют размерность 2, и разбиение на блоки соответствует разбиению на блоки в матрицах системы $\mathcal{C}$. Тогда в качестве двух коммутирующих матриц порядка 2, имеющих различные централизаторы и коммутирующих со всеми матрицами системы $\mathcal{C}$, кроме B_o , мы можем взять следующие матрицы (в том же базисе):

$$\begin{pmatrix} 1 & 1 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \\ & & & E & \end{pmatrix} \text{ и } \begin{pmatrix} 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 1 & 1 & & \\ & & & E & \end{pmatrix}.$$

Лемма доказана. □

Прежде чем доказывать лемму, аналогичную лемме 6, для случая полей, в которых не извлекаются корни третьей степени из единицы, сделаем несколько замечаний об экзистенциальных формулах, истинных в группах $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ при $2 \leq n \leq 5$.

При $n = 2$ в группах $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ максимальный набор попарно коммутирующих матриц порядка 3 состоит из двух матриц, а матрица порядка 2 обладает следующим свойством: любая коммутирующая с ней матрица порядка 2 имеет такой же централизатор.

При $n = 3$ в группах $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ максимальный набор попарно коммутирующих матриц порядка 3 также состоит из двух матриц, но найдутся 2 коммутирующие матрицы порядка 2 с различными централизаторами.

При $n = 4$ и $n = 5$ в группах $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ максимальный набор попарно коммутирующих матриц порядка 3 состоит из 8 матриц. Покажем, как в этом случае различить размерности. Заметим, что матрица, которая в некотором базисе имеет вид максимальной жордановой клетки с собственным значением 1, имеет наибольший среди всех матриц группы порядок вида 2^k (возможно, есть матрицы с другой жордановой формой и таким же порядком, например, порядок 4 имеют жордановы клетки размерностей 3 и 4). Поэтому при $n = 4$ наибольшее такое k , что в группе есть элемент порядка 2^k , равно 2, порядок 4, как уже было замечено, имеет, например, жорданова клетка

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

а при $n = 5$ наибольший порядок вида 2^k равен 8, это порядок матрицы

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

Лемма 10. Пусть в бесконечных полях K и L характеристики 2 не извлекаются корни третьей степени из единицы и известно, что группы $G_n(K)$ и $G_m(L)$ универсально эквивалентны ($G = \mathrm{GL}$ или SL). Тогда $n = m$.

Доказательство. Рассмотрим формулу

$$\exists A_1 \dots \exists A_{3^N-1} \left(\bigwedge_{i=1}^{3^N-1} (\neg A_i = E) \& \bigwedge_{\substack{i,j=1 \\ i \neq j}}^{3^N-1} (\neg A_i = A_j) \& \right. \\ \left. \& \bigwedge_{i,j=1}^{3^N-1} (A_i A_j = A_j A_i) \& \bigwedge_{i=1}^{3^N-1} (A_i^3 = E) \right).$$

В ней утверждается существование набора из $3^N - 1$ различных попарно коммутирующих матриц порядка 3. Так как линейные группы универсально эквивалентны, то наибольшее N , при котором формула истинна в группах $G_n(K)$ и $G_m(L)$ ($G = GL, SL$), одинаково и, согласно лемме 7, $N = \left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{m}{2} \right\rfloor$.

Если $N = 1$, то формула

$$\exists A_1 \exists A_2 \exists C ((\neg A_1 = A_2) \& (\neg A_1 = E) \& (\neg A_2 = E) \& \\ \& (A_1 A_2 = A_2 A_1) \& (A_1^2 = E) \& (A_2^2 = E) \& (A_1 C = C A_1) \& (\neg A_2 C = C A_2)),$$

утверждающая наличие в группе двух различных коммутирующих матриц порядка 2, имеющих различные централизаторы, либо одновременно истинна, либо одновременно ложна в обеих группах. Если она истинна, то $n = m = 3$, иначе $n = m = 2$.

Если $N = 2$, то наибольшее k , для которого в обеих группах истинна формула

$$\exists J \left(\bigwedge_{i=1}^{2^k-1} (\neg J^i = E) \& (J^{2^k} = E) \right),$$

одинаково. Если наибольшее значение k равно 2, то $n = m = 4$, а если $k = 3$, то $n = m = 5$.

Пусть теперь $N \geq 3$, значит, $n, m \geq 6$, и мы можем использовать

приемы из лемм 8 и 9. Рассмотрим формулу

$$\begin{aligned}
& \exists A_{11} \dots \exists A_{1,2C_M^1} \exists A_{21} \dots \exists A_{2,2^2 C_M^2} \dots \exists A_{M,1} \dots \exists A_{M,2^M C_M^M} \\
& \quad \exists B_1 \exists B_2 \exists C \exists C_{k,i,j} (k = 1, \dots, M; i, j = 1, \dots, 2^k C_M^k) \\
& \quad \left(\bigwedge_{k=1}^M \bigwedge_{i=1}^{2^k C_M^k} (\neg A_{k,i} = E) \& \bigwedge_{k=1}^M \bigwedge_{i=1}^{2^k C_M^k} \bigwedge_{l=1}^M \bigwedge_{\substack{j=1 \\ (k,i) \neq (l,j)}}^{2^l C_M^l} (\neg A_{k,i} = A_{l,j}) \& \right. \\
& \quad \& \bigwedge_{k=1}^M \bigwedge_{i=1}^{2^k C_M^k} \bigwedge_{l=1}^M \bigwedge_{j=1}^{2^l C_M^l} (A_{k,i} A_{l,j} = A_{l,j} A_{k,i}) \& \bigwedge_{k=1}^M \bigwedge_{i=1}^{2^k C_M^k} (A_{k,i}^3 = E) \& \\
& \quad \& \bigwedge_{k=1}^M \bigwedge_{i=1}^{2^k C_M^k} \bigwedge_{j=1}^{2^k C_M^k} (A_{k,i} = C_{k,i,j}^{-1} A_{k,j} C_{k,i,j}) \& \bigwedge_{i=1}^{C_M^1} (A_{1,i} A_{1,i+C_M^1} = E) \& \\
& \quad \& (\neg B_1 = E) \& (\neg B_2 = E) \& \bigwedge_{i=1}^{C_M^1-1} (B_1 A_{1,i} = A_{1,i} B_1) \& \bigwedge_{i=1}^{C_M^1-1} (B_2 A_{1,i} = A_{1,i} B_2) \& \\
& \quad \left. \& (B_1^2 = E) \& (B_2^2 = E) \& (B_1 B_2 = B_2 B_1) \& (B_1 C = C B_1) \& (\neg B_2 C = C B_2) \right).
\end{aligned}$$

При M , равном целой части от половины размерности группы, эта формула выделяет среди матриц системы $\mathcal{B}$ класс сопряженности, состоящий из матриц, имеющих ровно один неединичный блок (это $A_{11}, \dots, A_{1,2C_M^1}$), и систему $\mathcal{C}$ среди них, $\mathcal{C} = \{A_{11}, \dots, A_{1,C_M^1}\}$. Далее утверждается наличие двух коммутирующих матриц порядка 2 с различными централизаторами, коммутирующих со всеми матрицами системы $\mathcal{C}$, кроме A_{1,C_M^1} . Это предложение истинно или ложно одновременно в обеих группах. Если при $N = M$ оно истинно в обеих группах, то $n = m = 2M + 1$, иначе $n = m = 2M$. $\square$

2.2.3 Исследование свойств, выражающихся экзистенциальной формулой, без предположения о наличии корней третьей степени из единицы

Предложение 2. Пусть бесконечные поля K и L имеют характеристику 2 и $G_n(K) \equiv_{\forall} G_m(L)$ ($G = \text{GL}$ или SL). Тогда $n = m$.

Доказательство. Выпишем две формулы:

$$\exists A_1 \dots \exists A_{3^N-1} \left(\bigwedge_{i=1}^{3^N-1} (\neg A_i = E) \& \bigwedge_{\substack{i,j=1 \\ i \neq j}}^{3^N-1} (\neg A_i = A_j) \& \right. \\ \left. \bigwedge_{i,j=1}^{3^N-1} (A_i A_j = A_j A_i) \& \bigwedge_{i=1}^{3^N-1} (A_i^3 = E) \right), \quad (2.2)$$

$$\exists J \left(\bigwedge_{i=1}^{2^k-1} (\neg J^i = E) \& (J^{2^k} = E) \right). \quad (2.3)$$

Так как группы универсально эквивалентны, то наибольшее N , для которого истинна формула (2.2), одинаково для обеих групп. Поэтому в случае полных линейных групп порядок групп может быть равен $N, 2N, 2N + 1$, а в случае специальных линейных групп порядок групп может быть равен $N + 1, 2N, 2N + 1$.

Наибольшее k , для которого истинна формула (2.3), также одинаково. Учитывая тот факт, что клетка максимального размера с собственным значением 1 имеет порядок 2^k , где k — такое наименьшее натуральное число, что $2^k \geq n$, $2^k \geq m$, получаем:

$$2^{k-1} < n \leq 2^k, \\ 2^{k-1} < m \leq 2^k.$$

Поэтому для полных линейных групп возможны следующие случаи:

1) только одно из чисел $N, 2N, 2N + 1$ принадлежит промежутку $(2^{k-1}; 2^k]$, тогда $n = m$ и совпадает с этим числом, мы также узнаем, извлекаются ли в полях K и L корни третьей степени из единицы;

2) $2N, 2N + 1 \in (2^{k-1}; 2^k]$, тогда в полях K и L не извлекаются корни третьей степени из единицы, значит, можем применить лемму 10 и установить, что $m = n$.

Для специальных линейных групп, кроме случаев, аналогичных рассмотренным выше (только одно из чисел $N + 1, 2N, 2N + 1$ принадлежит промежутку $(2^{k-1}; 2^k]$ и $2N, 2N + 1 \in (2^{k-1}; 2^k]$), нужно рассмотреть случай $N + 1, 2N \in (2^{k-1}; 2^k]$. В этом случае $N = 2^{k-1}$ и $N + 1$ — размер наименьшей жордановой клетки, имеющей порядок 2^k . В группе $\text{SL}_{N+1}(K)$ у жордановой клетки размера $N + 1$ централизатор коммутативен. Если $N = 1$, то порядок обеих групп равен $N + 1 = 2N = 2$. Если $N > 1$, то если в группах найдется матрица порядка 2^k с некоммутативным централизатором, то порядок групп равен $2N$, иначе порядок равен $N + 1$.

Действительно, при $N = 2$ в группе порядка $2N = 4$ имеются две некоммутирующие друг с другом матрицы

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

перестановочные с жордановой клеткой

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

При $N > 2$ разность $2N - (N + 1) \geq 2$ и привести пример двух некоммутирующих матриц из централизатора жордановой клетки порядка 2^k также нетрудно. $\square$

Определение 9. Назовем конечный частичный изоморфизм

$$\Phi: G_n(K) \rightarrow G_m(L) \quad (G = GL, SL)$$

особым, если $\text{dom}(\Phi)$ содержит следующий конечный набор матриц: единичная матрица, максимальная совокупность попарно коммутирующих матриц порядка 3 (система матриц $\mathcal{A}$ или $\mathcal{B}$ в зависимости от наличия в поле корней третьей степени), все матрицы вида $E + E_{ij}$ ($i, j = 1, \dots, n; i \neq j$) в соответствующем базисе, а также вспомогательные матрицы из формул, использованных при доказательстве леммы 10 и предложения 2, в том числе обратные матрицы и все промежуточные произведения, встречающиеся в соотношениях (их конечное число).

Лемма 11. Пусть бесконечные поля K и L имеют характеристику 2 и известно, что $G_n(K) \cong_{\mathcal{V}} G_m(L)$ ($G = GL, SL$). Тогда при любом особом конечном частичном изоморфизме

$$\Phi: G_n(K) \rightarrow G_m(L) \quad (G = GL, SL)$$

матрица $E + E_{12}$ отобразится в матрицу, имеющую в некотором базисе вид $E + E_{12}$.

Доказательство. Согласно предложению 2, порядки групп n и m совпадают. Если $n = m = 2$ или $n = m = 3$, то утверждение следует из леммы 2.

Пусть теперь $n = m \geq 4$. Из доказательства предложения 2 следует, что мы можем различить случаи, когда извлекаются и не извлекаются корни третьей степени в полях K и L . Если корни извлекаются, то утверждение следует из леммы 4, а если корни не извлекаются и $n = m \geq 6$, то из леммы 8. Таким образом, осталось рассмотреть два случая: корни третьей степени из единицы в полях не извлекаются, а $n = m = 4$ или $n = m = 5$.

Рассмотрим сначала случай $n = m = 4$. Так как матрицы $E + E_{12}$ и $E + E_{13}$ сопряжены, то достаточно доказать, что образ матрицы $E + E_{13}$ в некотором базисе имеет вид $E + E_{13}$. Действительно, матрицы порядка 4 в некотором базисе имеют вид:

$$A_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ или } A_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Добавим условие некоммутативности централизатора (т. е. добавим в экзистенциальную формулу утверждение о существовании двух дополнительных матриц, экзистенциальность формулы не нарушится), ему будет удовлетворять только матрица A_2 . $A_2^2 = E + E_{13}$. Таким образом, мы получили требуемое.

Пусть теперь $n = 5$. Как мы уже знаем, матрица, имеющая максимальный порядок, являющийся степенью двойки, — это максимальная жорданова клетка с собственным значением 1. Ее четвертая степень равна $E + E_{15}$. Значит, образ матрицы $E + E_{15}$ при конечном частичном изоморфизме имеет в некотором базисе тот же вид, отсюда получаем утверждение леммы. $\square$

Теперь мы знаем, что вид матрицы $E + E_{12}$ при отображении посредством особого конечного частичного изоморфизма сохраняется, и далее можем воспользоваться результатом из спецкурса [16], а именно леммами 2.20 и 2.21. Следовательно, верна следующая

Лемма 12. Пусть бесконечные поля K и L имеют характеристику 2 и известно, что $G_n(K) \equiv_{\forall} G_n(L)$ ($G = \text{GL}, \text{SL}$). Тогда при любом особом конечном частичном изоморфизме

$$\Phi: G_n(K) \rightarrow G_n(L) \quad (G = \text{GL}, \text{SL})$$

все матрицы вида $E + E_{ij}$ переходят в матрицы, которые с точностью до автоморфизма группы в некотором общем базисе имеют тот же вид.

2.2.4 Доказательство основной теоремы

Определение 10. Для данного ненулевого элемента α поля K матрицу $E + \alpha E_{12} \in \text{GL}_n(K)$ ($E + \alpha E_{12} \in \text{SL}_n(K)$) назовем *матрицей сложения*, а матрицу $\text{diag}[\alpha, 1/\alpha, 1, \dots, 1]$ — *матрицей умножения*.

Лемма 13. При умножении матриц сложения, соответствующих элементам α и β , получается матрица сложения, соответствующая элементу $\alpha + \beta$. При умножении матриц умножения, соответствующих элементам α и β , получается матрица умножения, соответствующая элементу $\alpha\beta$.

Доказательство. Прямая проверка. $\square$

Лемма 14. Пусть бесконечные поля K и L имеют характеристику 2 и

$$G_n(K) \equiv_{\forall} G_m(L) \quad (G = \text{GL} \text{ или } \text{SL}).$$

Тогда при любом особом конечном частичном изоморфизме

$$\Phi: G_n(K) \rightarrow G_m(L) \quad (G = \text{GL}, \text{SL})$$

матрицы сложения и умножения переходят в матрицы того же вида. Причем, если $\Phi(\text{diag}[\alpha, 1/\alpha, 1, \dots, 1]) = \text{diag}[\beta, 1/\beta, 1, \dots, 1]$ и $\Phi(E + \alpha E_{12}) = E + \gamma E_{12}$, то $\beta = \gamma$.

Доказательство. Централизатор матрицы $E + E_{ij}$ ($i \neq j$) состоит из всех таких матриц (a_{st}) , у которых $a_{si} = 0$, $1 \leq s \leq n$, $s \neq i$, $a_{jt} = 0$, $1 \leq t \leq n$, $j \neq t$, $a_{ii} = a_{jj}$. Отсюда следует, что матрицы сложения характеризуются следующим свойством: это матрицы порядка 2, коммутирующие с теми и только теми матрицами из $E + E_{ij}$ ($i \neq j$), с которыми коммутирует $E + E_{12}$.

Докажем, что матрицы умножения — это ровно те матрицы A , для которых верно следующее:

$$\begin{aligned} A(E + E_{ij}) &= (E + E_{ij})A \quad (3 \leq i \leq n, 3 \leq j \leq n, i \neq j), \\ (A(E + E_{12})A^{-1})(E + E_{12}) &= (E + E_{12})(A(E + E_{12})A^{-1}), \\ (A(E + E_{21})A^{-1})(E + E_{21}) &= (E + E_{21})(A(E + E_{21})A^{-1}), \\ (\sigma_{12}A)^2 &= E, \\ (\sigma_{13}A\sigma_{13})(\sigma_{23}A\sigma_{23}) &= A, \text{ где } \sigma_{ij} = (E + E_{ij})(E + E_{ji})(E + E_{ij}). \end{aligned}$$

(Там, где соотношение неприменимо из-за размера матриц, мы просто его опускаем.)

Рассмотрим сначала случай, когда $n = 2$ или $n \geq 4$. В этом случае из первого условия следует, что

$$A = \begin{pmatrix} a_{11} & a_{12} & 0 & \dots & 0 \\ a_{21} & a_{22} & 0 & \dots & 0 \\ 0 & 0 & \lambda & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \lambda \end{pmatrix}.$$

Далее,

$$\begin{aligned} A(E + E_{12})A^{-1} &= \\ &= \begin{pmatrix} a_{11} & a_{12} & 0 & \dots & 0 \\ a_{21} & a_{22} & 0 & \dots & 0 \\ 0 & 0 & \lambda & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \lambda \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & 1 \end{pmatrix} \begin{pmatrix} \frac{a_{22}}{a_{11}a_{22}+a_{12}a_{21}} & \frac{a_{12}}{a_{11}a_{22}+a_{12}a_{21}} & 0 & \dots & 0 \\ \frac{a_{21}}{a_{11}a_{22}+a_{12}a_{21}} & \frac{a_{11}}{a_{11}a_{22}+a_{12}a_{21}} & 0 & \dots & 0 \\ 0 & 0 & \frac{1}{\lambda} & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \frac{1}{\lambda} \end{pmatrix} = \\ &= \begin{pmatrix} a_{11} & a_{12} & 0 & \dots & 0 \\ a_{21} & a_{22} & 0 & \dots & 0 \\ 0 & 0 & \lambda & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \lambda \end{pmatrix} \begin{pmatrix} \frac{a_{21}+a_{22}}{a_{11}a_{22}+a_{12}a_{21}} & \frac{a_{11}+a_{12}}{a_{11}a_{22}+a_{12}a_{21}} & 0 & \dots & 0 \\ \frac{a_{21}}{a_{11}a_{22}+a_{12}a_{21}} & \frac{a_{11}}{a_{11}a_{22}+a_{12}a_{21}} & 0 & \dots & 0 \\ 0 & 0 & \frac{1}{\lambda} & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \frac{1}{\lambda} \end{pmatrix} = \\ &= \begin{pmatrix} * & * & 0 & \dots & 0 \\ \frac{a_{21}^2}{a_{11}a_{22}+a_{12}a_{21}} & * & 0 & \dots & 0 \\ 0 & 0 & 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & 1 \end{pmatrix} \end{aligned}$$

коммутирует с $E + E_{12}$, значит $a_{21} = 0$. Аналогично $a_{12} = 0$.

Теперь применим четвертое соотношение. Так как

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & E \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & E \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & E \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & E \end{pmatrix},$$

то получаем

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & E \end{pmatrix} \begin{pmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & \lambda E \end{pmatrix} = \begin{pmatrix} 0 & a_{22} & 0 \\ a_{11} & 0 & 0 \\ 0 & 0 & \lambda E \end{pmatrix},$$

$$\begin{pmatrix} 0 & a_{22} & 0 \\ a_{11} & 0 & 0 \\ 0 & 0 & \lambda E \end{pmatrix}^2 = \begin{pmatrix} a_{11}a_{22} & 0 & 0 \\ 0 & a_{11}a_{22} & 0 \\ 0 & 0 & \lambda^2 E \end{pmatrix} = E,$$

следовательно, $a_{11}a_{22} = 1$, $\lambda = 1$.

Рассмотрим случай $n = 3$. В этом случае первое условие мы пропускаем. Во втором условии сказано, что матрица $A(E + E_{12})A^{-1} = E + AE_{12}A^{-1}$ коммутирует с $E + E_{12}$, значит $AE_{12}A^{-1}$ коммутирует с E_{12} . Введем обозначения: $A = (a_{ij})_{i,j=1}^3$, $A^{-1} = (b_{ij})_{i,j=1}^3$. В этих обозначениях

$$AE_{12}A^{-1} = \begin{pmatrix} a_{11}b_{21} & a_{11}b_{22} & a_{11}b_{23} \\ a_{21}b_{21} & a_{21}b_{22} & a_{21}b_{23} \\ a_{31}b_{21} & a_{31}b_{22} & a_{31}b_{23} \end{pmatrix},$$

тогда условие коммутирования с E_{12} записывается в виде:

$$\begin{pmatrix} 0 & a_{11}b_{21} & 0 \\ 0 & a_{21}b_{21} & 0 \\ 0 & a_{31}b_{21} & 0 \end{pmatrix} = \begin{pmatrix} a_{21}b_{21} & a_{21}b_{22} & a_{21}b_{23} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Из этого соотношения мы получаем следующие условия на коэффициенты:

$$a_{21}b_{21} = 0, \quad a_{11}b_{21} = a_{21}b_{22}, \quad a_{21}b_{23} = 0, \quad a_{31}b_{21} = 0.$$

Сначала докажем, что $a_{21} = 0$. Пусть это не так, тогда b_{21}, b_{22}, b_{23} должны равняться нулю, что противоречит обратимости матрицы A^{-1} .

Далее, из условий $a_{11}b_{21} = a_{21}b_{22} = 0$ и $a_{31}b_{21} = 0$ и того факта, что хотя бы один из коэффициентов a_{11}, a_{31} должен быть отличен от нуля, мы получаем $b_{21} = 0$.

Выразим b_{21} через элементы матрицы A :

$$b_{21} = -\frac{\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix}}{\det A} = \frac{a_{23}a_{31} - a_{21}a_{33}}{\det A} = \frac{a_{23}a_{31}}{\det A} = 0,$$

следовательно, $a_{23}a_{31} = 0$.

Теперь, зная, что в матрице A выполнено $a_{21} = 0$ и $a_{23}a_{31} = 0$, применим последнее соотношение. Вычислим множители в левой части:

$$\sigma_{13}A\sigma_{13} = \begin{pmatrix} a_{33} & a_{32} & a_{31} \\ a_{23} & a_{22} & 0 \\ a_{13} & a_{12} & a_{11} \end{pmatrix}, \quad \sigma_{23}A\sigma_{23} = \begin{pmatrix} a_{11} & a_{13} & a_{12} \\ a_{31} & a_{33} & a_{32} \\ 0 & a_{23} & a_{22} \end{pmatrix}.$$

Из подсчета элемента на месте $(2, 1)$ в произведении:

$$a_{23}a_{11} + a_{22}a_{31} = 0.$$

Рассмотрим два случая: 1) $a_{23} = 0$ и 2) $a_{31} = 0$.

1) Если $a_{23} = 0$, то в обратной матрице $\sigma_{13}A\sigma_{13}$ во второй строке элемент a_{22} должен быть отличен от нуля, тогда из $a_{22}a_{31} = 0$ мы получаем $a_{31} = 0$.

2) Если $a_{31} = 0$, то в обратной матрице $\sigma_{23}A\sigma_{23}$ в первом столбце элемент a_{11} должен быть отличен от нуля, тогда из $a_{23}a_{11} = 0$ мы получаем $a_{23} = 0$.

Таким образом, в любом случае $a_{23} = 0$ и $a_{31} = 0$.

Рассмотрим еще несколько элементов произведения $(\sigma_{13}A\sigma_{13})(\sigma_{23}A\sigma_{23}) = A$:

$$\begin{pmatrix} a_{33} & a_{32} & 0 \\ 0 & a_{22} & 0 \\ a_{13} & a_{12} & a_{11} \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{13} & a_{12} \\ 0 & a_{33} & a_{32} \\ 0 & 0 & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & 0 \\ 0 & a_{32} & a_{33} \end{pmatrix}.$$

Из элемента на месте $(1, 1)$ получаем $a_{33}a_{11} = a_{11}$ ($a_{11} \neq 0$), значит $a_{33} = 1$.

На месте $(3, 1)$: $a_{13}a_{11} = 0$, следовательно $a_{13} = 0$.

На месте $(3, 2)$: $a_{13}^2 + a_{12}a_{33} = 0 + a_{12} = a_{32}$, следовательно $a_{12} = a_{32}$.

На месте $(1, 3)$: $a_{33}a_{12} + a_{32}^2 = a_{13}$, следовательно $a_{12} + a_{12}^2 = 0$, откуда $a_{12} = 0$ или $a_{12} = 1$. Если предположить, что $a_{12} = a_{32} = 1$, то из $(3, 3)$ получим $a_{13}a_{12} + a_{12}a_{32} + a_{11}a_{22} = a_{33}$, то есть $1 + a_{11}a_{22} = 1$, откуда $a_{11}a_{22} = 0$, что противоречит обратимости матрицы A . Значит, единственная возможность $a_{12} = a_{32} = 0$ и $a_{11}a_{22} = 1$. Таким образом, матрица A имеет требуемый вид.

Теперь докажем второе утверждение леммы. Пусть $\Phi(E + \frac{1}{\alpha}E_{21}) = E + \delta E_{21}$ (то, что вид сохраняется, доказывается аналогично сохранению вида $E + \alpha E_{12}$). В $\text{GL}_n(K)$ ($\text{SL}_n(K)$) выполнено следующее соотношение:

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \frac{1}{\alpha} & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix},$$

поэтому в $\text{GL}_n(L)$ ($\text{SL}_n(L)$) выполнено:

$$\begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \delta & 1 \end{pmatrix} \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \\ = \begin{pmatrix} \gamma^2\delta & 1 + \gamma\delta \\ 1 + \gamma\delta & \delta \end{pmatrix} = \begin{pmatrix} \beta & 0 \\ 0 & \frac{1}{\beta} \end{pmatrix}.$$

Отсюда получаем, что $\gamma\delta = 1$ и $\beta = \gamma^2\delta = \gamma$. Что и требовалось. $\square$

Доказательство теоремы 6. Утверждение о совпадении порядков групп уже доказано в предложении 2. Используя критерий универсальной эквивалентности, покажем, что поля K и L универсально эквивалентны.

Пусть $K_1 \subset K$ — некоторая конечная частичная модель поля K . Наша задача — найти для нее частично изоморфную ей частичную модель L_1 в поле L . Пусть $G_1 \subset G_n(K)$ ($G = \text{GL}, \text{SL}$) содержит все матрицы сложения $E + \alpha E_{12}$ и умножения $\text{diag}[\alpha, \frac{1}{\alpha}, 1, \dots, 1]$ для всех $\alpha \in K_1^*$, а также набор попарно коммутирующих матриц порядка 3, составляющих систему $\mathcal{A}$ или $\mathcal{B}$ в зависимости от наличия в полях корней третьей степени из единицы, единичную матрицу, все матрицы $E + E_{ij}$ ($i, j = 1, \dots, n; i \neq j$) и конечное число вспомогательных матриц из лемм 6, 10 и предложения 2. Так как группы универсально эквивалентны, то для частичной модели G_1 существует конечная частичная модель $G_2 \subset G_n(L)$ ($G = \text{GL}, \text{SL}$), частично изоморфная G_1 , причем конечный частичный изоморфизм $\Phi: G_1 \rightarrow G_2$ является особым. Поэтому матрицы сложения и умножения переходят в матрицы того же вида, и если матрица сложения S и матрица умножения P соответствовали одному элементу α поля K , то и их образы $\Phi(S)$ и $\Phi(P)$ соответствуют одному и тому же элементу β поля L . Тогда L_1 — множество всех элементов поля L , которые соответствуют парам образов матриц сложения и умножения для всех элементов из K_1 . Теорема доказана. $\square$

2.3 Поля характеристики, отличной от 2

В этом разделе мы докажем следующую теорему.

Теорема 7. Пусть K и L — бесконечные поля, $\text{char } K, \text{char } L \neq 2$, группы $G_n(K)$ и $G_m(L)$ ($G = \text{GL}, \text{SL}, n, m \geq 2$) универсально эквивалентны. Тогда $n = m$ и поля K и L универсально эквивалентны.

В этом разделе все рассматриваемые поля имеют характеристику, отличную от 2, если специально не указано обратное.

2.3.1 Случай характеристики 2 выделяется экзистенциальными формулами

Лемма 15. Пусть K — поле, $\text{char } K \neq 2$, n — натуральное число. В группе $\text{GL}_n(K)$ существует подмножество максимум из $2^n - 1$ попарно коммутирующих матриц порядка 2, а в группе $\text{SL}_n(K)$ — из $2^{n-1} - 1$ попарно коммутирующих матриц порядка 2.

Доказательство. Существует базис, в котором все попарно коммутирующие матрицы порядка 2 диагонализированы и имеют вид $\text{diag} [\pm 1, \dots, \pm 1]$, значит в $\text{GL}_n(K)$ $2^n - 1$ попарно коммутирующих матриц порядка 2, а в $\text{SL}_n(K)$ — $2^{n-1} - 1$. $\square$

Обозначим через $\mathcal{D}(\text{GL}_n(K))$ ($\mathcal{D}(\text{SL}_n(K))$) или просто $\mathcal{D}$, если понятно, о какой группе идет речь) некоторый фиксированный максимальный набор попарно коммутирующих матриц порядка 2, существование которого доказано в лемме 15. Ясно, что набор матриц $\mathcal{D}$ выделяется экзистенциальной формулой.

Заметим, что благодаря лемме 15 мы можем разделить случаи, когда поля имеют характеристику 2 и характеристику, отличную от 2. Действительно, справедлива следующая

Лемма 16. Пусть K и L — бесконечные поля произвольной характеристики, группы $\text{G}_n(K)$ и $\text{G}_m(L)$ ($\text{G} = \text{GL}, \text{SL}$) универсально эквивалентны. Тогда либо $\text{char } K = \text{char } L = 2$, либо $\text{char } K \neq 2$ и $\text{char } L \neq 2$.

Доказательство. Запишем следующую формулу:

$$\begin{aligned} \exists A_1 \dots \exists A_M \left(\bigwedge_{i=1}^M (\neg A_i = E) \& \bigwedge_{\substack{i,j=1 \\ i \neq j}}^M (\neg A_i = A_j) \& \right. \\ \left. \& \bigwedge_{i,j=1}^M (A_i A_j = A_j A_i) \& \bigwedge_{i=1}^M (A_i^2 = E) \right). \end{aligned}$$

Если для некоторого достаточно большого M она ложна в обеих группах, то характеристика обоих полей отлична от двух. В противном случае характеристика полей равна двум. Действительно, так как поле бесконечно, то для любого сколь угодно большого M в качестве $A_1, \dots, A_M$ можно взять набор матриц вида $E + \alpha_i E_{12}$, где $\alpha_1, \dots, \alpha_M$ — различные ненулевые элементы поля. $\square$

2.3.2 Выделение размерности

Все попарно коммутирующие инволюции из системы $\mathcal{D}$ разбиваются на классы сопряженности, каждый класс состоит из матриц, у которых на диагонали стоит одинаковое количество (-1) .

Предложение 3. Пусть бесконечные поля K и L имеют характеристику, отличную от 2, и $G_n(K) \equiv_{\forall} G_m(L)$ ($G = \text{GL}, \text{SL}$). Тогда $n = m$.

Доказательство. Выпишем формулу:

$$\begin{aligned} \exists A_1 \dots \exists A_{2^N-1} \left(\bigwedge_{i=1}^{2^N-1} (\neg A_i = E) \& \bigwedge_{\substack{i,j=1 \\ i \neq j}}^{2^N-1} (\neg A_i = A_j) \& \right. \\ \left. \& \bigwedge_{i,j=1}^{2^N-1} (A_i A_j = A_j A_i) \& \bigwedge_{i=1}^{2^N-1} (A_i^2 = E) \right). \quad (2.4) \end{aligned}$$

Так как группы универсально эквивалентны, то наибольшее N такое, что формула (2.4) истинна в группах, одинаково для обеих групп. В случае общих линейных групп $n = m = N$, а в случае специальных линейных групп $n = m = N + 1$. $\square$

2.3.3 Свойства инволюций

Лемма 17. Пусть K — бесконечное поле, $\text{char } K \neq 2$. В группе $\text{GL}_n(K)$ два подмножества системы $\mathcal{D}$, состоящие из матриц, у которых (-1) на диагонали встречается один или $(n - 1)$ раз, выделяются экзистенциальной формулой. Если n нечетно, то в группе $\text{SL}_n(K)$ подмножество системы $\mathcal{D}$, состоящее из матриц, у которых (-1) на диагонали встречается $(n - 1)$ раз, выделяется экзистенциальной формулой.

Доказательство. Утверждение следует из того, что среди всех инволюций необходимые нам лежат в $\text{GL}_n(K)$ в одном (при $n = 2$) или двух (при $n > 2$) классах сопряженности, содержащих по n элементов, а в $\text{SL}_n(K)$ в одном n -элементном классе сопряженности; во всех остальных классах сопряженности (кроме класса, состоящего из одной матрицы $-E$, в случае $\text{GL}_n(K)$) инволюций больше. $\square$

Определение 11. Обозначим через $\mathcal{E}$ подмножество матриц системы $\mathcal{D}$, у которых (-1) стоит на диагонали один или $(n - 1)$ раз (если реализуются обе возможности, то выберем в качестве $\mathcal{E}$ любое одно из двух этих подмножеств). Согласно предыдущей лемме, такое множество матриц выделяется экзистенциальной формулой.

Лемма 18. Пусть бесконечные поля K и L имеют характеристику, отличную от 2, и известно, что $G_n(K) \equiv_{\forall} G_n(L)$ ($G = GL, SL$), а также n нечетно в случае специальных линейных групп. Тогда при любом таком конечном частичном изоморфизме

$$\Phi: G_n(K) \rightarrow G_n(L) (G = GL, SL)$$

что $\text{dom } \Phi$ содержит все матрицы системы $\mathcal{D}$, диагональная матрица отобразится в диагональную матрицу.

Доказательство. Утверждение следует из того, что диагональная матрица коммутирует со всеми матрицами системы $\mathcal{E}$, значит, таким же свойством обладает и ее образ, следовательно, образ является диагональной матрицей. $\square$

Лемма 19. Пусть бесконечные поля K и L имеют характеристику, отличную от 2, и известно, что $G_n(K) \equiv_{\forall} G_n(L)$ ($G = GL, SL, n$ нечетно для специальных линейных групп). Тогда при любом таком конечном частичном изоморфизме

$$\Phi: G_n(K) \rightarrow G_n(L), G = GL, SL,$$

что $\text{dom } \Phi$ содержит все матрицы системы $\mathcal{D}$, а также конечный набор вспомогательных матриц из предыдущих лемм, матрица $-E + E_{11} + E_{22} + E_{12} + E_{21}$ отобразится в матрицу, имеющую вид

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & \pm 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \pm 1 \end{pmatrix}$$

в базисе, в котором вид матриц системы $\mathcal{D}$ не изменится.

Доказательство. Как мы уже знаем, множество матриц $\mathcal{E}$ выделяется экзистенциальной формулой. Известно, что $-E + E_{11} + E_{22} + E_{21} + E_{12}$ коммутирует со всеми, кроме двух, матрицами системы $\mathcal{E}$. Поэтому

$$\Phi(-E + E_{11} + E_{22} + E_{21} + E_{12}) = \begin{pmatrix} d_{11} & d_{12} & 0 & \dots & 0 \\ d_{21} & d_{22} & 0 & \dots & 0 \\ 0 & 0 & d_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & d_{nn} \end{pmatrix},$$

а так как $(-E + E_{11} + E_{22} + E_{21} + E_{12})^2 = E$, то

$$E = \begin{pmatrix} d_{11} & d_{12} & 0 & \dots & 0 \\ d_{21} & d_{22} & 0 & \dots & 0 \\ 0 & 0 & d_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & d_{nn} \end{pmatrix}^2 =$$

$$= \begin{pmatrix} d_{11}^2 + d_{12}d_{21} & d_{11}d_{12} + d_{12}d_{22} & 0 & \dots & 0 \\ d_{21}d_{11} + d_{22}d_{21} & d_{21}d_{12} + d_{22}^2 & 0 & \dots & 0 \\ 0 & 0 & d_{33}^2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & d_{nn}^2 \end{pmatrix}.$$

Далее, $(-E + E_{11} + E_{22} + E_{21} + E_{12})(-E + 2E_{11})(-E + E_{11} + E_{22} + E_{21} + E_{12}) = -E + 2E_{22}$ (аналогично для случая, когда у матриц системы $\mathcal{E}$ (-1) на диагонали встречается один раз), поэтому справедливо соотношение (запишем его только для углового блока):

$$\begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

следовательно,

$$\begin{pmatrix} d_{11}^2 - d_{12}d_{21} & d_{11}d_{12} - d_{12}d_{22} \\ d_{11}d_{21} - d_{21}d_{22} & d_{12}d_{21} - d_{22}^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Из записанных выше соотношений получаем, что $d_{12}d_{22} = 0$. Если предположить, что $d_{12} = 0$, то тогда $d_{22}^2 = 1$ и $-d_{22}^2 = 1$ — противоречие. Отсюда следует, что $d_{22} = 0$, далее из $d_{12}d_{21} + d_{22}^2 = 1$ получим $d_{12}d_{21} = 1$, следовательно, $d_{11} = 0$. Таким образом, образ матрицы $-E + E_{11} + E_{22} + E_{21} + E_{12}$ имеет вид:

$$A_\alpha = \begin{pmatrix} 0 & \alpha & 0 & \dots & 0 \\ \frac{1}{\alpha} & 0 & 0 & \dots & 0 \\ 0 & 0 & \pm 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \pm 1 \end{pmatrix}.$$

Сделав замену базиса при помощи матрицы $\text{diag}[1/\alpha, 1, \dots, 1]$, получим требуемое. $\square$

2.3.4 Выделение трансвекций в $\text{GL}_n(K)$ и при нечетном n в $\text{SL}_n(K)$

Лемма 20. Пусть K, L — бесконечные поля, $\text{char } K, \text{char } L \neq 2$. При любом конечном частичном изоморфизме между группами $G_n(K)$ и $G_n(L)$ ($G = \text{GL}, \text{SL}$ и n нечетно в случае специальных линейных групп), область которого содержит все попарно коммутирующие инволюции, матрицу $-E + E_{11} + E_{22} + E_{12} + E_{21}$, матрицу $\text{diag}[2, 1, \frac{1}{2}, 1, \dots, 1]$ (матрицу $\text{diag}[2, 1]$ при $G = \text{GL}$ и $n = 2$), а также конечный набор вспомогательных матриц, набор матриц вида $E + \alpha_i E_{12}, i = 1, \dots, k$ отображается в матрицы того же вида.

Доказательство. Мы уже знаем, что совокупность попарно коммутирующих инволюций сохраняет вид при конечном частичном изоморфизме, матрица $-E + E_{11} + E_{22} + E_{12} + E_{21}$ переходит в матрицу $E_{12} + E_{21} + \text{diag}[0, 0, \pm 1, \dots, \pm 1]$, а диагональные матрицы — в диагональные.

Теперь перейдем к рассмотрению матрицы $E + \alpha E_{12}$. Она коммутирует с теми и только теми матрицами из множества $\mathcal{E}$, с которыми перестановочна $-E + E_{11} + E_{22} + E_{12} + E_{21}$, значит, ее образ будет иметь вид

$$\begin{pmatrix} a & b & 0 & \dots & 0 \\ c & d & 0 & \dots & 0 \\ 0 & 0 & \lambda_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \lambda_n \end{pmatrix}.$$

Рассмотрим два случая: $\text{char } K = 3$ и $\text{char } K \neq 3$.

Если $\text{char } K = 3$, то $\text{char } L = 3$, в противном случае в $G_n(\bar{L})$ найдется не более 3^n различных попарно коммутирующих матриц порядка 3, а в $G_n(K)$ их сколь угодно много: $E + \beta_i E_{12}$, где β_i — всевозможные элементы поля.

Сначала разберем случай $n = 2$ (только для полных линейных групп). Так как в характеристике 3 для матрицы $E + \alpha E_{12}$ справедливо соотношение $(E + \alpha E_{12})^{-1} = E - \alpha E_{12} = (-E_{11} + E_{22})(E + \alpha E_{12})(-E_{11} + E_{22})$, а образ матрицы $-E_{11} + E_{22}$ — это инволюция из системы $\mathcal{E}$, то для образа $E + \alpha E_{12}$ выполнено следующее:

$$\begin{pmatrix} a & -b \\ -c & d \end{pmatrix} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Пусть теперь $n > 2$. Возьмем в системе матриц $\mathcal{E}$ две матрицы: одну коммутирующую с $E + \alpha E_{12}$ и одну не коммутирующую с ней.

Произведение этих двух матриц — матрица вида $\text{diag} [\pm 1, \dots, \pm 1]$, у которой на диагонали (-1) встречается ровно 2 раза, можем считать, что это матрица $E - 2E_{11} - 2E_{33}$. Так как справедливы соотношения: $(E - 2E_{11} - 2E_{33})(E + \alpha E_{12})(E - 2E_{11} - 2E_{33}) = (E + \alpha E_{12})^{-1} = (E + \alpha E_{12})^2$, то можем записать для образов (в левом верхнем углу получаются те же соотношения, что и для $n = 2$):

$$\begin{pmatrix} a & -b & 0 & \dots & 0 \\ -c & d & 0 & \dots & 0 \\ 0 & 0 & \lambda_3 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \lambda_n \end{pmatrix} = \begin{pmatrix} d/(ad-bc) & -b/(ad-bc) & 0 & \dots & 0 \\ -c/(ad-bc) & a/(ad-bc) & 0 & \dots & 0 \\ 0 & 0 & 1/\lambda_3 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & 1/\lambda_n \end{pmatrix} = \begin{pmatrix} a^2+bc & (a+d)b & 0 & \dots & 0 \\ (a+d)c & bc+d^2 & 0 & \dots & 0 \\ 0 & 0 & \lambda_3^2 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \lambda_n^2 \end{pmatrix}.$$

Из этого равенства получаем, что $\lambda_3 = \dots = \lambda_n = 1$. А так как b и c не могут быть одновременно равны 0 (иначе образ матрицы $E + \alpha E_{12}$ коммутирует со всеми матрицами системы $\mathcal{E}$, что неверно), то из $-b = -\frac{b}{ad-bc}$ или $-c = -\frac{c}{ad-bc}$ получаем, что $ad - bc = 1$, далее замечаем, что $a = d, a + d = -1$, значит, $a = d = 1$ и, наконец, $bc = 0$. Так как образы матриц $E + \alpha_i E_{12}$ попарно коммутируют, то в общем базисе ненулевой внедиагональный элемент матриц стоит на одном и том же месте. Таким образом, в случае $\text{char } K = 3$ утверждение доказано.

Пусть теперь $\text{char } K \neq 3$, тогда и $\text{char } L \neq 3$. Справедливо соотношение

$$(\text{diag} [2, 1, \frac{1}{2}, 1, \dots, 1])(E + \alpha E_{12})(\text{diag} [2, 1, \frac{1}{2}, 1, \dots, 1])^{-1} = (E + \alpha E_{12})^2.$$

Образ матрицы $\text{diag} [2, 1, \frac{1}{2}, 1, \dots, 1]$ при конечном частичном изоморфизме равен некоторой диагональной матрице $\text{diag} [\alpha_1, \dots, \alpha_n]$, причем из того, что матрица $(\text{diag} [2, 1, \frac{1}{2}, 1, \dots, 1])^2$ не коммутирует с $-E + E_{11} +$

$E_{12} + E_{21} + E_{22}$, следует, что $(\text{diag} [\alpha_1, \dots, \alpha_n])^2$ не коммутирует с $-E + E_{11} + E_{12} + E_{21} + E_{22}$, значит $\alpha_1^2 \neq \alpha_2^2$. Теперь мы можем записать соотношение для образов:

$$\begin{pmatrix} a & \frac{b\alpha_1}{\alpha_2} & 0 & \dots & 0 \\ \frac{c\alpha_2}{\alpha_1} & d & 0 & \dots & 0 \\ 0 & 0 & \lambda_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \lambda_n \end{pmatrix} = \begin{pmatrix} \alpha_1 & 0 & \dots & \dots & 0 \\ 0 & \ddots & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \dots & \dots & 0 & \alpha_n \end{pmatrix} \begin{pmatrix} a & b & 0 & \dots & 0 \\ c & d & 0 & \dots & 0 \\ 0 & 0 & \lambda_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \lambda_n \end{pmatrix}.$$

$$\cdot \begin{pmatrix} \frac{1}{\alpha_1} & 0 & \dots & \dots & 0 \\ 0 & \ddots & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \dots & \dots & 0 & \frac{1}{\alpha_n} \end{pmatrix} = \begin{pmatrix} a^2 + bc & ab + bd & 0 & \dots & 0 \\ ac + cd & bc + d^2 & 0 & \dots & 0 \\ 0 & 0 & \lambda_3^2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \lambda_n^2 \end{pmatrix}.$$

Отсюда получаем: $\lambda_i = 1, i = 3, \dots, n$. Если $bc \neq 0$, то т. к. $\frac{b\alpha_1}{\alpha_2} = b(a + d)$ и $\frac{c\alpha_2}{\alpha_1} = c(a + d)$, то $\frac{\alpha_1}{\alpha_2} = a + d = \frac{\alpha_2}{\alpha_1}$, следовательно, $\alpha_1^2 = \alpha_2^2$, что противоречит ранее доказанному. Значит, $bc = 0$ и $a = d = 1$. $\square$

Лемма 21. Пусть K, L — бесконечные поля, $\text{char } K, \text{char } L \neq 2$. При любом конечном частичном изоморфизме между группами $G_n(K)$ и $G_n(L)$ ($G = \text{GL}, \text{SL}$, n нечетно в случае специальных линейных групп), область которого содержит все попарно коммутирующие инволюции, матрицу $-E + E_{11} + E_{12} + E_{21} + E_{22}$, матрицу $\text{diag} [2, 1, 1/2, 1, \dots, 1]$ ($\text{diag} [2, 1]$ в случае $G = \text{GL}$, $n = 2$) и конечный набор вспомогательных матриц из предыдущих лемм, матрица $E + E_{12}$ отобразится в матрицу $E + E_{12}$.

Доказательство. Ранее доказано, что образ матрицы $E + E_{12}$ — это некоторая матрица $E + \alpha E_{12}$. Покажем, что $\alpha = 1$. Запишем соотношения, которые выполняются для элементов, лежащих в области конечного частичного изоморфизма (выписываем только угловой блок):

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

$$\left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right] \left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right],$$

значит, для матрицы $E + \alpha E_{12}$ выполнены соотношения:

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix} &= \left[\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right] \left[\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right] = \\ &= \begin{pmatrix} \alpha & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \alpha^2 - 1 & \alpha \\ \alpha & 1 \end{pmatrix}, \end{aligned}$$

откуда немедленно следует, что $\alpha = 1$. $\square$

2.3.5 Сохранение матриц сложения и умножения в случае $\text{GL}_n(K)$ и при нечетном n в случае $\text{SL}_n(K)$

Лемма 22. Пусть K, L — бесконечные поля, $\text{char } K, \text{char } L \neq 2$. При любом конечном частичном изоморфизме между группами $\text{G}_n(K)$ и $\text{G}_n(L)$ ($\text{G} = \text{GL}, \text{SL}$, n нечетно в случае $\text{G} = \text{SL}$), область которого содержит конечный набор матриц, использованных для доказательства предыдущих лемм, матрицы сложения переходят в матрицы сложения, а матрицы умножения переходят в матрицы умножения, причем если две матрицы соответствовали одному элементу поля K , то и их образы будут соответствовать одному элементу поля L .

Доказательство. То, что вид матриц сложения сохраняется при конечном частичном изоморфизме, уже доказано. Матрицу умножения можно выразить следующим образом (запишем соотношение только для углового блока):

$$\begin{aligned} \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} &= \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \frac{1}{\alpha} & 1 \end{pmatrix} \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \\ &= \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}^{-1} \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{\alpha} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right] \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}^{-1} \cdot \\ &\quad \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right] \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

тогда угловой блок образа рассматриваемой матрицы умножения (диагональная матрица со всеми, кроме первых двух, единичными элементами

на диагонали) будет равен произведению:

$$\begin{aligned}
& \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}^{-1} \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right] \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}^{-1} \\
& \quad \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right] \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \\
& = \begin{pmatrix} 1 & -\beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix} \begin{pmatrix} 1 & -\beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \\
& \quad = \begin{pmatrix} 2\beta - \beta^2\gamma & 1 - \beta\gamma \\ \beta\gamma - 1 & \gamma \end{pmatrix},
\end{aligned}$$

следовательно, $\beta\gamma = 1$, образ рассматриваемой матрицы умножения равен $E + (\beta - 1)E_{11} + \left(\frac{1}{\beta} - 1\right)E_{22}$, что и требовалось. $\square$

2.3.6 Случай $\text{SL}_2(K)$

Лемма 23. Пусть K — бесконечное поле, $\text{char } K \neq 2$. Тогда в группе $\text{SL}_2(K)$ матрица, имеющая в некотором базисе вид $E + E_{12}$, выделяется экзистенциальной формулой.

Доказательство. Докажем, что матрица A , удовлетворяющая формуле

$$\begin{aligned}
& \exists X \exists Y ((A^2 \neq E) \& (XAX^{-1}A = AXAX^{-1}) \& \\
& \& (X^2A \neq AX^2) \& (YAY^{-1} = A^4)),
\end{aligned}$$

в некотором базисе имеет требуемый вид.

Заметим, что для матрицы $A = E + E_{12}$ формула истинна при $X = \alpha E_{11} + \frac{1}{\alpha} E_{22}$, $\alpha \in K^*$, $\alpha^4 \neq 1$, $Y = 2E_{11} + \frac{1}{2}E_{22}$.

Пусть теперь для некоторой матрицы A истинна указанная выше формула. Если жорданова форма матрицы над $\overline{K}$ не диагональна, то, учитывая, что $A \in \text{SL}_2(K)$, она равна

$$A_+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ или } A_- = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}.$$

В первом случае все доказано, а второй не реализуется, т. к. матрица $A_-^4 = E - 4E_{12}$ не сопряжена с A_- (у первой собственное значение 1, а у второй (-1)).

Если матрица A диагонализируема над $\overline{K}$, то диагональная форма имеет вид $\alpha E_{11} + \frac{1}{\alpha} E_{22}$, причем $\alpha \neq \pm 1$, т. к. $A^2 \neq E$. Введем обозначение

для матрицы $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ и запишем соотношения из нашей формулы:

$$\begin{aligned} XAX^{-1}A &= \begin{pmatrix} \alpha a & \frac{b}{\alpha} \\ c\alpha & \frac{d}{\alpha} \end{pmatrix} \begin{pmatrix} \alpha d & -\frac{b}{\alpha} \\ -c\alpha & \frac{a}{\alpha} \end{pmatrix} = \begin{pmatrix} ad\alpha^2 - bc & -ab + \frac{ab}{\alpha^2} \\ cd\alpha^2 - cd & -bc + \frac{ad}{\alpha^2} \end{pmatrix} = \\ &= \begin{pmatrix} ad\alpha^2 - bc & ab - ab\alpha^2 \\ -\frac{cd}{\alpha^2} + cd & -bc + \frac{ad}{\alpha^2} \end{pmatrix} = \begin{pmatrix} \alpha a & \alpha b \\ \frac{c}{\alpha} & \frac{d}{\alpha} \end{pmatrix} \begin{pmatrix} \alpha d & -\alpha b \\ -\frac{c}{\alpha} & \frac{a}{\alpha} \end{pmatrix} = AXAX^{-1}, \\ X^2A &= \begin{pmatrix} (a^2 + bc)\alpha & \frac{ab+bd}{\alpha} \\ (ac + cd)\alpha & \frac{bc+d^2}{\alpha} \end{pmatrix} \neq \begin{pmatrix} (a^2 + bc)\alpha & (ab + bd)\alpha \\ \frac{ac+cd}{\alpha} & \frac{bc+d^2}{\alpha} \end{pmatrix} = AX^2. \end{aligned}$$

Из условия $XAX^{-1}A = AXAX^{-1}$ получаем:

$$cd \left(2 - \alpha^2 - \frac{1}{\alpha^2} \right) = 0 \text{ и } ab \left(2 - \alpha^2 - \frac{1}{\alpha^2} \right) = 0,$$

а так как $\alpha \neq \pm 1$, то $ab = cd = 0$. Если предположить, что $a = 0$, то $c \neq 0$ из невырожденности матрицы X , значит $d = 0$. Аналогично, если $b = 0$, то $c = 0$. В обоих случаях получим

$$\frac{ab + bd}{\alpha} = 0 = (ab + bd)\alpha \text{ и } (ac + cd)\alpha = 0 = \frac{ac + cd}{\alpha},$$

что противоречит условию $X^2A \neq AX^2$. Таким образом, A не диагонализуема над $\bar{K}$, что и требовалось. $\square$

Лемма 24. Пусть K — бесконечное поле, $\text{char } K \neq 2$. Тогда в группе $\text{SL}_2(K)$ матрица, имеющая в некотором базисе вид $-E_{12} + E_{21}$, выделяется экзистенциальной формулой.

Доказательство. Мы уже умеем выделять экзистенциальной формулой матрицу $E + E_{12}$. Заметим, что справедливы следующие соотношения:

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \\ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Пусть теперь некоторая матрица $B \in \text{SL}_2(K)$ порядка 4 такова, что

$$(E + E_{12})B(E + E_{12})B(E + E_{12}) = B \text{ и}$$

$$(E + E_{12})B^{-1}(E + E_{12})B^{-1}(E + E_{12}) = B.$$

Пусть $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, из записанных выше соотношений получим:

$$\begin{aligned} & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \\ & = \begin{pmatrix} a^2 + c(2a + b + c + d) & a(a + c) + b(a + c) + (c + d)(a + b + c + d) \\ ac + c^2 + cd & c(a + b + c + 2d) + d^2 \end{pmatrix} = \\ & = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \\ & = \begin{pmatrix} * & * \\ -ac + c^2 - cd & * \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \end{aligned}$$

Следовательно, $c(a + d) = 0$. Если предположить, что $c = 0$, то $a^2 = a$ и $d^2 = d$, значит, $a = d = 1$, далее $1 + b + 1 + b + 1 = b$ и $b = -3$. Так как $\text{char } K \neq 2$, то

$$\begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}^4 = \begin{pmatrix} 1 & -12 \\ 0 & 1 \end{pmatrix}$$

является единичной матрицей только при $\text{char } K = 3$, но тогда сама B — единичная матрица. Противоречие. Следовательно, $c \neq 0$.

Значит, $a = -d$. В этом случае из равенства $ac + c^2 + cd = c$ получим: $c = 1$. Если $a = 0$, то, т. к. $B \in \text{SL}_2(K)$, $b = -1$, и утверждение доказано. В противном случае сделаем замену базиса с матрицей перехода $E + aE_{12}$ (коммутирует с $E + E_{12}$), которая приведет B к виду

$$\begin{pmatrix} 0 & b + a^2 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

что и требовалось. $\square$

Лемма 25. Пусть K — бесконечное поле, $\text{char } K \neq 2$. Тогда в группе $\text{SL}_2(K)$ матрица, имеющая вид $\text{diag}[\alpha, \frac{1}{\alpha}]$ в том базисе, в котором вид матриц $E + E_{12}$ и $-E_{12} + E_{21}$ не изменится, выделяется экзистенциальной формулой.

Доказательство. Заметим, что диагональная матрица обладает следующими свойствами: $(\text{diag}[\alpha, \frac{1}{\alpha}])(E + E_{12})(\text{diag}[\alpha, \frac{1}{\alpha}])^{-1}$ коммутирует с $E + E_{12}$, $(-E_{12} + E_{21})(\text{diag}[\alpha, \frac{1}{\alpha}]) = (\text{diag}[\alpha, \frac{1}{\alpha}])^{-1}(-E_{12} + E_{21})$.

Пусть некоторая матрица $aE_{11} + bE_{12} + cE_{21} + dE_{22}$ удовлетворяет выписанным выше свойствам диагональной матрицы. Тогда

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad - ac - bc & a^2 \\ -c^2 & ac - bc + ad \end{pmatrix}$$

коммутирует с $E + E_{12}$, значит $c = 0$, $ad = 1$. Далее

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & \frac{1}{a} \end{pmatrix} = \begin{pmatrix} 0 & -\frac{1}{a} \\ a & b \end{pmatrix} = \begin{pmatrix} -b & -\frac{1}{a} \\ a & 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & -b \\ 0 & a \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

значит, $b = 0$, и рассматриваемая матрица диагональна. $\square$

Лемма 26. Пусть K, L — бесконечные поля, $\text{char } K, \text{char } L \neq 2$. При любом конечном частичном изоморфизме между группами $\text{SL}_2(K)$ и $\text{SL}_2(L)$, область которого содержит набор матриц, использованных при доказательстве предыдущих лемм, матрицы сложения переходят в матрицы сложения, а матрицы умножения переходят в матрицы умножения, причем если две матрицы соответствовали одному элементу поля K , то и их образы будут соответствовать одному элементу поля L .

Доказательство. Из предыдущей леммы получаем, что вид матриц умножения сохраняется. Покажем, что сохраняется и вид матриц сложения. Пусть $E + \alpha E_{12}$ — матрица сложения, она коммутирует с матрицей $E + E_{12}$, значит ее образ будет иметь вид $\pm E + \beta E_{12}$. Так как

$$\begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}^4,$$

то образ матрицы $E + \alpha E_{12}$ равен $E + \beta E_{12}$, в противном случае для некоторой диагональной матрицы $\text{diag}[\gamma, \frac{1}{\gamma}]$, в которую отобразится $\text{diag}[2, \frac{1}{2}]$ должно выполняться соотношение:

$$\begin{pmatrix} \gamma & 0 \\ 0 & \frac{1}{\gamma} \end{pmatrix} \begin{pmatrix} -1 & \beta \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\gamma} & 0 \\ 0 & \gamma \end{pmatrix} = \begin{pmatrix} -1 & \beta \\ 0 & -1 \end{pmatrix}^4,$$

но левая часть равенства равна

$$\begin{pmatrix} -1 & \beta\gamma^2 \\ 0 & -1 \end{pmatrix},$$

а правая —

$$\begin{pmatrix} 1 & -4\beta \\ 0 & 1 \end{pmatrix},$$

таким образом, получили противоречие.

Осталось доказать, что образы двух матриц сложения и умножения, соответствующих одному элементу поля K , соответствуют одному элементу поля L . Доказательство этого факта аналогично доказательству леммы 22, если заметить, что

$$\begin{pmatrix} 1 & 0 \\ \frac{1}{\alpha} & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & -\frac{1}{\alpha} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

$\square$

2.3.7 Случай $\mathrm{SL}_n(K)$ для четного $n \geq 4$

Лемма 27. Пусть K — бесконечное поле, $\mathrm{char} K \neq 2$, $n \geq 4$, n четно. Тогда в группе $\mathrm{SL}_n(K)$ подмножество системы $\mathcal{D}$, состоящее из матриц, имеющих ровно две (-1) на диагонали, выделяется экзистенциальной формулой.

Доказательство. Множество $\mathcal{D}$ разбивается на классы сопряженности. Подмножества, состоящие из матриц, имеющих $(n-2)$ или две (-1) на диагонали — это два класса сопряженности, состоящие из C_n^2 элементов каждый. В остальных классах сопряженности, кроме класса, состоящего из единственного элемента $-E$, элементов больше. Если $n = 4$, то класс сопряженности, состоящий из C_n^2 элементов, единственный, он является интересующим нас подмножеством.

Если $n = 6$, то, перемножив все элементы из класса сопряженности матриц с двумя (-1) на диагонали, получим $-E$, так как в этом классе $C_5^1 = 5$ матриц, у которых на фиксированном месте стоит (-1) ; если перемножить все элементы класса сопряженности, содержащего матрицы с четырьмя (-1) , то получится единичная матрица, так как среди матриц этого класса сопряженности существует ровно $C_5^3 = 10$ матриц с (-1) на некотором фиксированном месте. Таким образом, при $n = 6$ мы можем выделить среди матриц системы $\mathcal{D}$ те матрицы, у которых (-1) на диагонали встречается ровно 2 раза.

Если $n \geq 8$, то среди матриц с двумя (-1) на диагонали всегда найдутся три такие, что произведение первых двух равно третьей. Но при перемножении любых двух матриц, у которых (-1) на диагонали $(n-2)$ штуки, мы получим матрицу из другого класса сопряженности. $\square$

Лемма 28. Пусть бесконечные поля K и L имеют характеристику, отличную от 2, n четно, $n \geq 4$ и известно, что $\mathrm{SL}_n(K) \equiv_{\forall} \mathrm{SL}_n(L)$. Тогда при любом таком конечном частичном изоморфизме $\Phi: \mathrm{SL}_n(K) \rightarrow \mathrm{SL}_n(L)$, что $\mathrm{dom} \Phi$ содержит все матрицы системы $\mathcal{D}$, диагональная матрица отображается в диагональную матрицу.

Доказательство. Так как диагональная матрица коммутирует со всеми матрицами системы $\mathcal{D}$, то и ее образ коммутирует с образами матриц системы $\mathcal{D}$. Ранее показано, что матрицы системы $\mathcal{D}$ выделяются экзистенциальной формулой, значит, их образы сохраняют вид, следовательно, образ нашей матрицы коммутирует со всеми матрицами системы $\mathcal{D}$, значит, является диагональной матрицей. $\square$

Лемма 29. Пусть бесконечные поля K и L имеют характеристику, отличную от 2, n четно, $n \geq 4$ и известно, что $\mathrm{SL}_n(K) \equiv_{\forall} \mathrm{SL}_n(L)$. Тогда при любом таком конечном частичном изоморфизме $\Phi: \mathrm{SL}_n(K) \rightarrow$

$SL_n(L)$, что $\text{dom } \Phi$ содержит все матрицы системы $\mathcal{D}$, а также конечный набор вспомогательных матриц из предыдущих лемм, матрица $E - E_{11} - E_{22} - E_{12} + E_{21}$ отображается в матрицу, которая в некотором базисе (в котором вид матриц системы $\mathcal{D}$ не изменится) имеет вид

$$\begin{pmatrix} 0 & -1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & \pm 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \pm 1 \end{pmatrix}.$$

Доказательство. Введем обозначение для тех матриц системы $\mathcal{D}$, у которых ровно две (-1) на диагонали: через A_{ij} , $i < j$, будем обозначать матрицу, у которой (-1) стоят на i -ом и j -ом местах.

Фиксируем некоторую матрицу с двумя (-1) на диагонали, в некотором базисе это A_{12} . Матрицы A_{ij} , $2 < i < j$, характеризуются следующим свойством: это такие матрицы с двумя (-1) на диагонали, которые при умножении на A_{12} дают матрицу из $\mathcal{D}$, не сопряженную с A_{12} . Так как матрица $E - E_{11} - E_{22} - E_{12} + E_{21}$ коммутирует со всеми матрицами A_{ij} , $2 < i < j$, и с A_{12} , то это верно и для ее образа. Обозначим образ X . Следовательно,

$$X = \begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & \lambda_3 & e \\ 0 & 0 & f & \lambda_4 \end{pmatrix} \text{ при } n = 4 \text{ и } X = \begin{pmatrix} a & b & 0 & \dots & 0 \\ c & d & 0 & \dots & 0 \\ 0 & 0 & \lambda_3 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \lambda_n \end{pmatrix} \text{ при } n > 4.$$

Заметим, что $(E - E_{11} - E_{22} - E_{12} + E_{21})A_{13}(E - E_{11} - E_{22} - E_{12} + E_{21})^{-1} = A_{23}$. В системе $\mathcal{D}$ фиксируем такую матрицу с двумя (-1) , которая при умножении на A_{12} дает матрицу с двумя (-1) и назовем ее A_{13} , тогда $A_{23} = A_{12}A_{13}$. При $n = 4$ это соотношение для второго блока дает нам

$$\begin{pmatrix} \lambda_3 & e \\ f & \lambda_4 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda_3 & e \\ f & \lambda_4 \end{pmatrix},$$

откуда получаем $e = f = 0$.

Далее (для всех $n \geq 4$), $(E - E_{11} - E_{22} - E_{12} + E_{21})^2 = A_{12}$, значит, $X^2 = A_{12}$ и $\lambda_i = \pm 1$, $i = 3, \dots, n$.

Вернемся к предыдущему соотношению, но теперь запишем его для левого верхнего блока:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \left(\frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \right) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Из доказанного выше следует, что $ad - bc = \pm 1$. Рассмотрим сначала случай $ad - bc = 1$. Тогда

$$\begin{pmatrix} -ad - bc & 2ab \\ -2cd & ad + bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

следовательно, $ad = ab = cd = 0$, $bc = -1$ и окончательно получим: $a = d = 0$. Сделав замену базиса при помощи матрицы $E + (-1 - \frac{1}{b})E_{11}$, коммутирующей со всеми диагональными матрицами, получим искомый вид для матрицы X .

Осталось показать, что случай $ad - bc = -1$ не реализуется. Аналогично предыдущему случаю получим, что $a = d = 0$, $bc = 1$, но тогда

$$\begin{pmatrix} 0 & b \\ \frac{1}{b} & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

то есть $X^2 = E$, что противоречит условию $X^2 = A_{12}$. $\square$

Лемма 30. Пусть бесконечные поля K и L имеют характеристику, отличную от 2, n четно, $n \geq 4$ и известно, что $\text{SL}_n(K) \equiv_{\forall} \text{SL}_n(L)$. Тогда при любом таком конечном частичном изоморфизме $\Phi: \text{SL}_n(K) \rightarrow \text{SL}_n(L)$, что $\text{dom } \Phi$ содержит все матрицы системы $\mathcal{D}$, матрицу $E - E_{11} - E_{22} - E_{12} + E_{21}$ и матрицу $\text{diag}[2, 1, \frac{1}{2}, 1, \dots, 1]$, а также конечный набор вспомогательных матриц из предыдущих лемм, матрица вида $E + \alpha E_{12}$ отображается в матрицу того же вида.

Доказательство. Доказательство аналогично доказательству леммы 20, если учесть, что роль матрицы $-E + E_{11} + E_{12} + E_{21} + E_{22}$ в данном случае играет матрица $E - E_{11} - E_{22} - E_{12} + E_{21}$. $\square$

Лемма 31. Пусть бесконечные поля K и L имеют характеристику, отличную от 2, n четно, $n \geq 4$ и известно, что $\text{SL}_n(K) \equiv_{\forall} \text{SL}_n(L)$. Тогда для любого такого конечного частичного изоморфизма $\Phi: \text{SL}_n(K) \rightarrow \text{SL}_n(L)$, что $\text{dom } \Phi$ содержит все матрицы системы $\mathcal{D}$, матрицу $E - E_{11} - E_{22} - E_{12} + E_{21}$ и матрицу $\text{diag}[2, 1, \frac{1}{2}, 1, \dots, 1]$, а также конечный набор вспомогательных матриц из предыдущих лемм, верно $\Phi(E + E_{12}) = E + E_{12}$.

Доказательство. Так как выполняется следующее соотношение (снова выписаны только угловые блоки матриц):

$$A_{13} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} A_{12} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} A_{13} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

то, с учетом предыдущей леммы, для образов верно следующее:

$$A_{13} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} A_{12} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} A_{13} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix},$$

таким образом,

$$\begin{pmatrix} 1 - \alpha^2 & -\alpha \\ \alpha & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix},$$

откуда получаем $\alpha = 1$, что и требовалось. $\square$

2.3.8 Замечания, завершающие доказательство

Для завершения доказательства основной теоремы 1 воспользуемся ранее изложенными соображениями. Более подробно, мы уже умеем доказывать сохранение вида матриц сложения четного порядка в случае специальных линейных групп, про матрицы умножения мы знаем, что они сохраняют диагональный вид. Доказательство того, что матрицы умножения переходят в матрицы умножения, причем сохраняется соответствие пары матриц сложения и умножения одному элементу поля, полностью аналогично доказательству леммы 22 с учетом замечания из доказательства леммы 26. Теперь остается только почти дословно повторить рассуждение из доказательства теоремы 6 в условии теоремы 7. Так как благодаря лемме 16 мы можем различить случаи, в которых основные поля имеют характеристику 2 и характеристику, отличную от 2, то теорема 1 полностью доказана.

Глава 3

Полные и специальные линейные группы над локальными коммутативными кольцами с $1/2$

В настоящей главе мы доказываем следующую теорему:

Теорема 2. Пусть R_1 и R_2 — локальные коммутативные кольца с $1/2$. Группы $G_n(R_1)$ и $G_m(R_2)$ ($G = GL, SL, n, m \geq 3$) универсально эквивалентны тогда и только тогда, когда $n = m$ и кольца R_1 и R_2 универсально эквивалентны.

3.1 Предварительные замечания, опирающиеся на ранее доказанные факты

Сначала докажем простую импликацию. Если кольца R_1 и R_2 универсально эквивалентны и $n = m$, то, очевидно, $G_n(R_1) \equiv_\forall G_n(R_2)$, так как все соотношения между конечным числом матриц в матричной группе переписываются через конечное число элементов колец скаляров, между которыми есть соответствие. А именно, каждое экзистенциальное предложение в языке групп мы можем переписать в виде экзистенциального предложения в языке скаляров следующим образом: вместо каждой матрицы запишем ее n^2 элементов, соотношения между матрицами перепишем в виде соотношений между элементами колец скаляров, а также для каждой матрицы добавим существование n^2 элементов, представляющих обратную матрицу и соотношения, описывающие произведения

матрицы и ее обратной (в случае специальных линейных групп нужно будет также записать условия равенства определителей единице); полученная таким образом формула снова будет экзистенциальным предложением. Отметим, что утверждение остается справедливым и в случае, когда $n = m < 3$.

Далее мы докажем более сложную импликацию: из универсальной эквивалентности линейных групп следует совпадение порядков групп и универсальная эквивалентность соответствующих колец.

Заметим, что если линейные группы универсально эквивалентны, то кольца R_1 и R_2 либо оба конечны, либо оба бесконечны. В случае конечных моделей универсальная эквивалентность совпадает с изоморфизмом, поэтому утверждение теоремы автоматически следует из работы [17], в которой доказано, что при натуральных $n, m \geq 3$, следующие условия эквивалентны:

- 1) $n = m$ и $R_1 \cong R_2$,
- 2) $\mathrm{GL}_n(R_1) \cong \mathrm{GL}_m(R_2)$,
- 3) $\mathrm{SL}_n(R_1) \cong \mathrm{SL}_m(R_2)$,

где R_1 и R_2 — локальные коммутативные кольца с $1/2$.

Поэтому далее в этой главе будем считать кольца R_1 и R_2 бесконечными.

Утверждение о совпадении порядков — это следствие того факта, что в группе $G_n(R)$ ($G = \mathrm{GL}, \mathrm{SL}$) над локальным коммутативным кольцом R с обратимой двойкой все попарно коммутирующие инволюции диагонализированы в общем базисе, для случая локальных колец этот факт доказан в [22].

Далее считаем, что $n > 2$.

3.2 Инволюции

Обозначим через $\mathcal{MJ}$ некоторую фиксированную максимальную систему попарно коммутирующих инволюций. В некотором общем базисе все элементы системы $\mathcal{MJ}$ — диагональные матрицы, у которых на диагонали стоят ± 1 . Фиксируем один из таких базисов. Заметим, что $\mathcal{MJ}$ разбивается на классы сопряженности, каждый класс сопряженности состоит в точности из тех матриц, у которых на диагонали одинаковое количество -1 в выбранном ранее базисе. Далее введем обозначения для некоторых подмножеств $\mathcal{MJ}$.

Рассмотрим сначала случаи $\mathrm{SL}_n(R)$ при нечетном n и $\mathrm{GL}_n(R)$. В множестве $\mathcal{MJ}$ самые маленькие классы сопряженности, кроме одноэлементного (если есть), состоят из n элементов, а именно, это классы сопря-

женности, состоящие из матриц, у которых на диагонали -1 встречается 1 раз и $n-1$ раз (в $SL_n(R)$ реализуется только вторая возможность). Эти классы сопряженности выделяются экзистенциальной формулой. Заметим, что формула, основанная на подсчете числа элементов в классах сопряженности, выделяет каждый из этих двух классов, но не говорит, какой именно. Назовем J_1 один (неважно, какой) из этих классов.

В случае $SL_n(R)$ при четном $n \geq 4$ обозначим J_2 следующее подмножество системы $\mathcal{MJ}$: матрицы, у которых на диагонали -1 встречается ровно два раза. Подмножество J_2 выделяется экзистенциальной формулой так же, как в лемме 27.

Из того факта, что множество матриц $\mathcal{MJ}$ выделяется экзистенциальной формулой, также следует сохранение вида диагональных матриц при изоморфизме частичной модели, содержащей все матрицы из $\mathcal{MJ}$.

3.3 Матрицы с блоком $-E_{12} + E_{21}$ на диагонали

Лемма 32. Пусть R_1 и R_2 — бесконечные локальные коммутативные кольца с $1/2$, и известно, что $G_n(R_1) \equiv_{\forall} G_n(R_2)$ ($G = GL, SL$). Пусть также M_1 — произвольная конечная частичная модель $G_n(R_1)$, содержащая множество $\mathcal{MJ}$, а M_2 — конечная частичная модель $G_n(R_2)$, изоморфная M_1 (ее существование следует из критерия универсальной эквивалентности).

Тогда при любом изоморфизме

$$\Phi: M_1 \rightarrow M_2$$

матрица $\sigma_{12} = E - E_{11} - E_{22} - E_{12} + E_{21}$ отобразится в матрицу, имеющую вид

$$\begin{pmatrix} 0 & -1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & \pm 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \pm 1 \end{pmatrix}$$

в базисе, в котором вид матриц системы $\mathcal{MJ}$ не изменится.

Доказательство. Будем рассматривать два случая.

1 случай. Если $G = GL$ или $G = SL$ при нечетном n , то воспользуемся тем, что σ_{12} коммутирует со всеми, кроме двух, матрицами из множества J_1 . Назовем эти матрицы I_1 и I_2 , считая, что в I_j на j -м месте

на диагонали стоит элемент, отличный от всех остальных диагональных элементов. Далее при рассмотрении этого случая будем использовать обозначение $I_{ij} = I_i I_j$, $i \neq j$.

2 случай. Если $G = SL$ и n четно, то поступим следующим образом: сначала среди матриц системы J_2 фиксируем одну, назовем ее I_{12} и будем считать, что у нее (-1) стоят на первом и втором местах на диагонали, затем рассмотрим все матрицы из J_2 , которые в произведении с I_{12} дают матрицу не из J_2 ; все они, а также I_{12} коммутируют с σ_{12} . В каждом из случаев получим для образа следующий вид:

$$\Phi(\sigma_{12}) = \begin{pmatrix} d_{11} & d_{12} & 0 & 0 \\ d_{21} & d_{22} & 0 & 0 \\ 0 & 0 & d_{33} & a \\ 0 & 0 & b & d_{nn} \end{pmatrix} \text{ при } n = 4 \text{ или}$$

$$\Phi(\sigma_{12}) = \begin{pmatrix} d_{11} & d_{12} & 0 & \dots & 0 \\ d_{21} & d_{22} & 0 & \dots & 0 \\ 0 & 0 & d_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & d_{nn} \end{pmatrix} \text{ при четном } n \neq 4.$$

Далее при $n \neq 4$ воспользуемся соотношениями $\sigma_{12}^2 = I_{12}$. Отсюда получаем для образов:

$$\begin{pmatrix} d_{11}^2 + d_{12}d_{21} & d_{11}d_{12} + d_{12}d_{22} & 0 & \dots & 0 \\ d_{21}d_{11} + d_{22}d_{21} & d_{21}d_{12} + d_{22}^2 & 0 & \dots & 0 \\ 0 & 0 & d_{33}^2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & d_{nn}^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

откуда с учетом наличия в локальном кольце $1/2$ сразу следует, что $d_{ii} = \pm 1$ для всех $2 < i \leq n$.

Теперь рассмотрим отдельно первый случай. Используем еще одно соотношение: $\sigma_{12} I_1 \sigma_{12} = I_1$. Из него получим для образов следующее (записан только угловой блок):

$$\begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix} =$$

$$= \begin{pmatrix} -d_{11}^2 + d_{12}d_{21} & -d_{11}d_{12} + d_{12}d_{22} \\ -d_{21}d_{11} + d_{22}d_{21} & -d_{21}d_{12} + d_{22}^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Складывая и вычитая соответствующие элементы матриц из этого и предыдущего соотношений, получаем, что $2d_{12}d_{21} = -2$, т.е. $d_{12}d_{21} = -1$,

а также $2d_{22}d_{21} = 0$ и $2d_{11}d_{12} = 0$, откуда из обратимости d_{12}, d_{21} следует, что $d_{11} = d_{22} = 0$.

Рассмотрим отдельно второй случай. Здесь воспользуемся соотношением $\sigma_{12}I_{13}\sigma_{12}^{-1} = I_{23}$. (В системе $\mathcal{J}_2$ мы фиксировали такую матрицу, которая при умножении на I_{12} дает матрицу из $\mathcal{J}_2$, и обозначили ее I_{13} , тогда $I_{23} = I_{12}I_{13}$.) Заметим, что для случая $n = 4$ из этого соотношения следует, что второй блок диагонален, а значит, как и для $n \neq 4$, на диагонали стоят ± 1 .

Теперь запишем это соотношение для левого верхнего блока образов:

$$\begin{aligned} & \frac{1}{d_{11}d_{22} - d_{12}d_{21}} \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d_{22} & -d_{12} \\ -d_{21} & d_{11} \end{pmatrix} = \\ & = \frac{1}{d_{11}d_{22} - d_{12}d_{21}} \begin{pmatrix} -d_{11}d_{22} - d_{12}d_{21} & 2d_{11}d_{12} \\ -2d_{21}d_{22} & d_{11}d_{22} + d_{12}d_{21} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned}$$

Так как $d_{11}d_{12} = d_{21}d_{22} = 0$, матрица невырождена, а кольцо локально, то либо 1) $d_{11} = d_{22} = 0$, а d_{12} и d_{21} обратимы, либо 2) $d_{12} = d_{21} = 0$, а d_{11} и d_{22} обратимы. В случае 2) получим, что элемент на месте (1, 1) равен, с одной стороны, $-\frac{d_{11}d_{22}}{d_{11}d_{22}} = -1$, с другой стороны, 1, что невозможно. Значит, реализуется только случай 1), в условиях которого получаем из равенства на месте (1, 1) в соотношении $\sigma_{12}^2 = I_{12}$: $d_{12}d_{21} = -1$.

Теперь мы знаем, что

$$\Phi(\sigma_{12}) = \begin{pmatrix} 0 & -\alpha & 0 & \dots & 0 \\ \frac{1}{\alpha} & 0 & 0 & \dots & 0 \\ 0 & 0 & \pm 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \pm 1 \end{pmatrix},$$

где α — обратимый элемент кольца. Осталось только применить замену базиса, порожденную матрицей $\text{diag}[1/\alpha, 1, \dots, 1]$, коммутирующей со всеми матрицами из $\mathcal{MJ}$, и мы получим требуемое. $\square$

Замечание 4. Точно таким же методом можно доказать, что для матрицы σ_{23} , у которой блок $-E_{12} + E_{21}$ стоит на пересечении второй и третьей строк со вторым и третьим столбцами, вид сохраняется. Аналогично рассуждению из леммы 32 сначала получим, что

$$\Phi(\sigma_{23}) = \begin{pmatrix} \pm 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & -\beta & 0 & \dots & 0 \\ 0 & \frac{1}{\beta} & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \pm 1 & & \\ \vdots & \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & & & \pm 1 \end{pmatrix},$$

а затем сделаем замену базиса, порожденную матрицей $\text{diag}[1, 1, \beta, 1, \dots, 1]$, которая коммутирует и со всеми элементами системы $\mathcal{MJ}$, и с σ_{12} .

3.4 Сохранение трансвекций

Лемма 33. Пусть R_1 и R_2 — бесконечные локальные коммутативные кольца с $1/2$, и известно, что $G_n(R_1) \equiv_{\forall} G_n(R_2)$ ($G = \text{GL}, \text{SL}$). И пусть M_1 — произвольная конечная частичная модель $G_n(R_1)$, содержащая конечный набор матриц из предыдущей леммы и матрицу $\text{diag}[2, 1, 1/2, 1, \dots, 1]$, а M_2 — конечная частичная модель $G_n(R_2)$, изоморфная M_1 . Тогда при любом частичном изоморфизме

$$\Phi: M_1 \rightarrow M_2$$

матрица $E + E_{12}$ переходит с точностью до автоморфизма группы в матрицу того же вида в базисе, в котором вид матриц системы $\mathcal{MJ}$, σ_{12} и σ_{23} не изменится.

Доказательство. Как и в доказательстве леммы 32,

$$\Phi(E + E_{12}) = \begin{pmatrix} t_{11} & t_{12} & 0 & \dots & 0 \\ t_{21} & t_{22} & 0 & \dots & 0 \\ 0 & 0 & t_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & t_{nn} \end{pmatrix}.$$

Так как $\text{diag}[2, 1, 1/2, 1, \dots, 1]$ коммутирует со всеми матрицами из $\mathcal{MJ}$, то $\Phi(\text{diag}[2, 1, 1/2, 1, \dots, 1]) = \text{diag}[\alpha_1, \dots, \alpha_n]$, где все α_i обратимы. Из соотношения $\text{diag}[2, 1, 1/2, 1, \dots, 1](E + E_{12})(\text{diag}[2, 1, 1/2, 1, \dots, 1])^{-1} = (E + E_{12})^2$ для образов получаем, что $t_{ii}^2 = t_{ii}$ для всех $3 \leq i \leq n$, значит, так как все t_{ii} при $3 \leq i \leq n$ обратимы, все они единицы.

Теперь мы можем рассматривать при вычислениях только угловые блоки размерности 2 или, там где это необходимо, размерности 3. Используем три соотношения:

$$((E + E_{12})I_{23})^2 = E,$$

$$(\sigma_{12}(E + E_{12}))^3 = I_{12},$$

$$E + E_{12} \text{ коммутирует с } \sigma_{23}(E + E_{12})\sigma_{23}^{-1}.$$

(Из второго соотношения, в частности, следует, что у $\Phi(\sigma_{12})$ на диагонали, начиная с третьего места, стоят единицы.)

Запишем эти соотношения для образов, учитывая ранее доказанное сохранение вида некоторых матриц. Заметим, что у $\Phi(\sigma_{23})$ первый элемент на диагонали — единица, так как σ_{12} и σ_{23} сопряжены:

$$\begin{aligned} \left(\begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right)^2 &= \begin{pmatrix} t_{11}^2 - t_{12}t_{21} & t_{12}(-t_{11} + t_{22}) \\ t_{21}(t_{11} - t_{22}) & t_{22}^2 - t_{12}t_{21} \end{pmatrix} = E, \\ \left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \right)^3 &= \begin{pmatrix} -t_{21} & -t_{22} \\ t_{11} & t_{12} \end{pmatrix}^3 = \\ &= \begin{pmatrix} -t_{21}^3 + 2t_{11}t_{21}t_{22} - t_{11}t_{12}t_{22} & -t_{21}^2t_{22} + t_{11}t_{22}^2 + t_{12}t_{21}t_{22} - t_{12}^2t_{22} \\ * & t_{11}t_{21}t_{22} - 2t_{11}t_{12}t_{22} + t_{12}^3 \end{pmatrix} = -E, \end{aligned}$$

$$\begin{aligned} \begin{pmatrix} t_{11} & t_{12} & 0 \\ t_{21} & t_{22} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} t_{11} & t_{12} & 0 \\ t_{21} & t_{22} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} = \\ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} t_{11} & t_{12} & 0 \\ t_{21} & t_{22} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} t_{11} & t_{12} & 0 \\ t_{21} & t_{22} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \\ \text{или, что то же самое,} \quad \begin{pmatrix} t_{11}^2 & t_{12} & t_{11}t_{12} \\ t_{11}t_{21} & t_{22} & t_{12}t_{21} \\ t_{21} & 0 & t_{22} \end{pmatrix} = \begin{pmatrix} t_{11}^2 & t_{11}t_{12} & t_{12} \\ t_{21} & t_{22} & 0 \\ t_{11}t_{21} & t_{12}t_{21} & t_{22} \end{pmatrix}. \end{aligned}$$

Из последнего соотношения получаем $t_{12}t_{21} = 0$, значит из первого $t_{11}^2 = t_{22}^2 = 1$. Вычисляя определитель во втором, получаем $1 = (t_{11}t_{22} - t_{12}t_{21})^3 = (t_{11}t_{22})^3 = t_{11}^2t_{22}^2t_{11}t_{22} = t_{11}t_{22}$. Из этого же соотношения $t_{21}^2t_{22} - t_{12}t_{21}t_{22} + t_{12}^2t_{22} = t_{11}t_{22}^2$, учитывая равенство нулю $t_{12}t_{21} = 0$ и обратимость t_{22} , видим, что $t_{12}^2 + t_{21}^2 = t_{11}t_{22}$. Так как кольцо локально, то отсюда следует, что один из элементов t_{12} и t_{21} обратим, тогда другой равен нулю.

Если $t_{21} = 0$, то $t_{11}t_{12}t_{22} = 1$ (из второго), следовательно, $t_{12} = 1$, далее $t_{12} = t_{11}t_{12}$ (из третьего) дает нам $t_{11} = 1$ и, наконец, $t_{22} = 1$, что и требовалось.

Если $t_{12} = 0$, то снова из второго $t_{11}t_{21}t_{22} = -1$, значит $t_{21} = -1$, далее $t_{11} = 1 = t_{22}$. Осталось применить контраградиентный автоморфизм, который каждому элементу A группы сопоставляет $(A^T)^{-1}$, причем все элементы из $\mathcal{MJ}$, а также σ_{12} и σ_{23} оставляет на месте. $\square$

Лемма 34. Пусть R_1 и R_2 — бесконечные локальные коммутативные кольца с $1/2$, и известно, что $G_n(R_1) \equiv_{\forall} G_n(R_2)$ ($G = \text{GL}, \text{SL}$). И пусть

M_1 — произвольная конечная частичная модель $G_n(R_1)$, содержащая конечный набор матриц из предыдущих лемм и матрицу $\text{diag}[2, 1, 1/2, 1, \dots, 1]$, а M_2 — конечная частичная модель $G_n(R_2)$, изоморфная M_1 . Тогда при любом частичном изоморфизме

$$\Phi: M_1 \rightarrow M_2$$

любой конечный набор матриц вида $E + \alpha_i E_{12}$, $i = 1, \dots, k$ переходит в набор матриц вида $E + \beta_i E_{12}$, $i = 1, \dots, k$, в базисе, в котором вид матриц из предыдущих лемм не изменится.

Доказательство. Как в лемме 33, легко показать, что

$$\Phi(E + \alpha_i E_{12}) = \begin{pmatrix} s_{11}^i & s_{12}^i & 0 \\ s_{21}^i & s_{22}^i & 0 \\ 0 & 0 & E \end{pmatrix}.$$

Далее из перестановочности матриц $E + E_{12}$ и $E + \alpha_i E_{12}$ получим: $s_{21}^i = 0$, $s_{11}^i = s_{22}^i$.

Осталось показать, что на диагонали на первых двух местах единицы. Распишем соотношения с диагональной матрицей для углового блока, учитывая, что $\Phi(\text{diag}[2, 1, 1/2, 1, \dots, 1]) = \text{diag}[d_1, \dots, d_n]$:

$$\begin{pmatrix} s_{11}^i & d_1 s_{12}^i \\ 0 & s_{22}^i \end{pmatrix} = \begin{pmatrix} (s_{11}^i)^2 & 2s_{11}^i s_{12}^i \\ 0 & (s_{22}^i)^2 \end{pmatrix}.$$

Теперь мы видим, что из обратимости s_{11}^i, s_{22}^i следует, что оба эти элемента равны единице. $\square$

Сделаем два замечания о связи умножения элементов локального кольца R и операций над элементами группы $G_n(R)$ ($G = \text{GL}, \text{SL}$). Во-первых,

$$[E + \alpha E_{12}, E + \beta E_{23}] = E + \alpha\beta E_{13}.$$

А во-вторых,

$$E + \alpha E_{23} = \sigma_{12} \sigma_{23}^{-1} (E + \alpha E_{12})^{-1} \sigma_{23} \sigma_{12}^{-1},$$

$$E + \alpha E_{13} = [E + E_{12}, E + \alpha E_{23}].$$

Теперь основное утверждение будет следовать из предыдущих лемм, аналогично тому, как это получается в предыдущей главе. Более подробно, пусть $S_1 \subset R_1$ — некоторая конечная частичная модель кольца R_1 . Наша задача — найти для нее частично изоморфную ей частичную модель S_2 в кольце R_2 . Пусть $M_1 \subset G_n(R_1)$ ($G = \text{GL}, \text{SL}$) — конечная

частичная модель, содержащая все матрицы вида $E + \alpha E_{12}$ для всех $\alpha \in S_1$, а также конечное число вспомогательных матриц из предыдущих лемм. Так как группы универсально эквивалентны, то для частичной модели M_1 существует изоморфная частичная модель $M_2 \subset G_n(R_2)$ ($G = GL, SL$), причем любой изоморфизм $\Phi: M_1 \rightarrow M_2$ сохраняет вид матриц. Поэтому образы матриц $E + \alpha E_{12}, E + \alpha E_{13}, E + \alpha E_{23}$ будут в некотором общем базисе иметь вид $E + \beta_1 E_{12}, E + \beta_2 E_{13}, E + \beta_3 E_{23}$, причем $\beta_1 = \beta_2 = \beta_3 \in R_2$. Тогда S_2 — множество всех элементов кольца R_2 , которые соответствуют тройкам образов матриц $E + \alpha E_{12}, E + \alpha E_{13}, E + \alpha E_{23}$ для всех элементов $\alpha \in S_1$.

Глава 4

Полные линейные группы над некоммутативными локальными кольцами с $1/2$

В настоящей главе будет доказана следующая теорема:

Теорема 3. Пусть R_1 и R_2 — локальные (не обязательно коммутативные) кольца с $1/2$. Группы $\mathrm{GL}_n(R_1)$ и $\mathrm{GL}_m(R_2)$ ($n, m \geq 3$) универсально эквивалентны тогда и только тогда, когда $n = m$ и кольца R_1 и R_2 универсально эквивалентны либо $n = m$ и кольца R_1 и R_2^{op} универсально эквивалентны.

4.1 Простая импликация: эквивалентность колец влечет эквивалентность групп

Доказательство более простой импликации — из универсальной эквивалентности колец следует универсальная эквивалентность полных линейных групп — полностью аналогично доказательству для коммутативных локальных колец, изложенному в главе 3, и так же остается справедливым в случае, когда $n = m < 3$.

Если же кольца R_1 и R_2^{op} универсально эквивалентны, то группы $\mathrm{GL}_n(R_1)$ и $\mathrm{GL}_n(R_2^{op})$ универсально эквивалентны. Теперь заметим, что $\mathrm{GL}_n(R_2^{op}) \cong \mathrm{GL}_n(R_2)^{op}$ (в качестве изоморфизма выступает транспонирование), а $\mathrm{GL}_n(R_2)^{op} \cong \mathrm{GL}_n(R_2)$ (изоморфизм — взятие обратного). Таким образом, и в этом случае $\mathrm{GL}_n(R_1)$ и $\mathrm{GL}_n(R_2)$ универсально эквивалентны.

4.2 Сложная импликация: от групп к кольцам

Теперь перейдем к доказательству более сложной импликации. Заметим, что если линейные группы универсально эквивалентны, то кольца R_1 и R_2 либо оба конечны, либо оба бесконечны. В случае конечных моделей универсальная эквивалентность совпадает с изоморфизмом и элементарной эквивалентностью, поэтому утверждение теоремы следует из работы [13]. А именно, согласно теореме 4 из этой статьи, при отсутствии нетривиальных центральных идемпотентов (оно в условиях теоремы 3 выполняется, так как кольца локальны), мы получаем для матричных колец $M_n(R_1) \cong M_m(R_2)$ или $M_n(R_1) \cong M_m(R_2)^{op}$. В первом случае, так как кольца локальны, из изоморфизма матричных колец следует изоморфизм колец скаляров (следствие 17.31 из книги [6]). Во втором случае сначала воспользуемся изоморфизмом $M_m(R_2)^{op} \cong M_m(R_2^{op})$ (транспонирование), а уже потом применим то же самое следствие. Совпадение размерностей докажем далее, одновременно для случаев конечных и бесконечных колец.

4.2.1 Выделение размерности

Сначала изучим строение инволюций в полной линейной группе над некоммутативным локальным кольцом, следуя статье [22], где аналогичные рассуждения проведены для локальных коммутативных колец.

Лемма 35. Пусть R — локальное кольцо с $1/2$, $I \in GL_n(R)$ и $I^2 = E$. Тогда существует такой базис правого R -модуля V ранга n , что I представляется в нем матрицей вида $\text{diag}[1, \dots, 1, -1, \dots, -1]$, где на диагонали стоят t единиц, s минус единиц, $t + s = n$ и t, s определены однозначно.

Доказательство. Рассмотрим следующие подмодули:

$$N(I) = \{v \in V | I(v) = -v\}, \quad P(I) = \{v \in V | I(v) = v\}.$$

Пусть $u \in N(I) \cap P(I)$, тогда $I(u) = u = -u$, откуда с учетом наличия в кольце $1/2$ следует, что $u = 0$.

Пусть теперь u — произвольный элемент V . Справедливо равенство

$$u = (u - I(u))\frac{1}{2} + (u + I(u))\frac{1}{2},$$

причем $u - I(u) \in N(I)$, $u + I(u) \in P(I)$. Следовательно, $V = N(I) \oplus P(I)$.

Осталось сделать два замечания о строении подмодулей $N(I)$ и $P(I)$. Во-первых, $N(I)$ и $P(I)$ — проективные модули как прямые слагаемые свободного. Во-вторых, так как проективные модули над локальным (не обязательно коммутативным) кольцом свободны ([5], теорема 19.29), то $N(I)$ и $P(I)$ — свободные модули, причем их ранги конечны и однозначно определены. В базисе, состоящем из базисов подмодулей $P(I)$ и $N(I)$, I имеет требуемый вид. $\square$

Лемма 36. Пусть R — локальное кольцо с $1/2$, $I_1, \dots, I_m \in \text{GL}_n(R)$, $I_j^2 = E$ и $I_j I_k = I_k I_j$ для всех $j, k = 1, \dots, m$. Тогда в некотором базисе правого R -модуля ранга n все $I_1, \dots, I_m$ диагональны с ± 1 на диагонали.

Доказательство. Рассмотрим сначала два коммутирующих оператора порядка два I_1, I_2 . Согласно лемме 35, можем считать, что уже фиксирован некоторый базис модуля, в котором $I_1 = \text{diag}[1, \dots, 1, -1, \dots, -1]$ (t единиц и s минус единиц). Так как $I_1 I_2 = I_2 I_1$ и двойка обратима, то I_2 имеет в выбранном базисе блочно-диагональный вид, и на диагонали стоят блоки размера $t \times t$ и $s \times s$.

Пусть $v \in P(I_1)$, тогда $I_1 I_2(v) = I_2 I_1(v) = I_2(v)$, значит $I_2(v) \in P(I_1)$, то есть подмодуль $P(I_1)$ инвариантен относительно оператора I_2 , аналогичное верно и для подмодуля $N(I_1)$. Теперь достаточно поменять базис в каждом из подмодулей $P(I_1)$ и $N(I_1)$, чтобы оператор I_2 принял нужный вид, при этом вид оператора I_1 не изменится.

Для большего числа операторов это рассуждение можно продолжить по индукции. А именно, пусть для $I_1, \dots, I_k$ уже построен базис, в котором все операторы диагональны с ± 1 на диагонали. Тогда весь модуль разложен в прямую сумму всевозможных пересечений инвариантных подмодулей $P(I_j)$, $j = 1, \dots, k$ и $N(I_j)$, $j = 1, \dots, k$. Так как I_{k+1} коммутирует с каждым из $I_1, \dots, I_k$, то все прямые слагаемые инвариантны относительно I_{k+1} , значит, можно привести I_{k+1} к диагональному виду на каждом прямом слагаемом, что и требовалось. $\square$

Следствие 1. Пусть R — локальное кольцо с $1/2$. Мощность максимального подмножества $\text{GL}_n(R)$, состоящего из попарно коммутирующих инволюций, равна $2^n - 1$.

Следствие 2. Пусть R_1 и R_2 — локальные кольца с $1/2$, m и n — натуральные числа, и пусть группы $\text{GL}_n(R_1)$ и $\text{GL}_m(R_2)$ универсально эквивалентны. Тогда $n = m$.

Далее в этой главе будем считать, что $n > 2$, а кольца R_1 и R_2 бесконечны.

4.2.2 Элементы порядка 2

Фиксируем некоторое максимальное подмножество попарно коммутирующих инволюций и некоторый базис модуля, в котором все эти инволюции диагональны. Обозначим это множество инволюций $\mathcal{MJ}$. Заметим, что $\mathcal{MJ}$ разбивается на классы сопряженности, каждый класс сопряженности состоит в точности из тех элементов, у которых на диагонали одинаковое количество -1 . Среди всех классов сопряженности самый маленький по мощности — это $\{-E\}$, далее в порядке возрастания мощностей идут n -элементные классы сопряженности, состоящие из матриц, у которых на диагонали ровно одна минус единица и $n - 1$ минус единица. Эти классы сопряженности выделяются экзистенциальной формулой. Заметим, что формула, основанная на подсчете числа элементов в классе сопряженности, выделяет каждый из этих двух классов, но не говорит, какой именно. Назовем $\mathcal{J}_1$ класс матриц с одной минус единицей, а $\mathcal{J}_2$ класс с одной единицей. Для элементов $\mathcal{J}_1$ введем следующее обозначение: I_k — это матрица, у которой на k -м месте на диагонали стоит минус единица.

Заметим, что при любом изоморфизме частичной модели, содержащей множество $\mathcal{MJ}$, это множество переходит в множество элементов, которые в некотором общем базисе имеют тот же вид, что и $\mathcal{MJ}$ в ранее фиксированном базисе, а множество $\mathcal{J}_1$ переходит либо в множество того же вида, либо в $\mathcal{J}_2$. А если область дополнительно содержит диагональную матрицу, то ее образ тоже диагонален, так как диагональные матрицы и только они коммутируют со всеми элементами из $\mathcal{MJ}$.

Далее нам пригодится следующая вспомогательная

Лемма 37. Пусть R — локальное кольцо с $1/2$, $x \in R$ и $x^2 = 1$, тогда $x = \pm 1$.

Доказательство. Элемент $\frac{1}{2}(x+1)$ является идемпотентом. Так как кольцо R локально, то этот идемпотент тривиален: $\frac{1}{2}(x+1) = 0$ или 1 . В первом случае $x = -1$, во втором $x = 1$. $\square$

Теперь приступим непосредственно к доказательству сохранения вида необходимых нам матриц при изоморфизмах частичных моделей.

Лемма 38. Пусть R_1 и R_2 — бесконечные локальные кольца с $1/2$, и известно, что $\mathrm{GL}_n(R_1) \equiv_{\forall} \mathrm{GL}_n(R_2)$ ($n > 2$). Пусть также M_1 — произвольная конечная частичная модель $\mathrm{GL}_n(R_1)$, содержащая множество $\mathcal{MJ}$ и сопрягающие его элементы матрицы, а M_2 — конечная частичная модель $\mathrm{GL}_n(R_2)$, изоморфная M_1 (ее существование следует из критерия универсальной эквивалентности).

Тогда при любом изоморфизме

$$\Phi: M_1 \rightarrow M_2$$

матрица $\sigma_{12} = E - E_{11} - E_{22} + E_{12} + E_{21}$ отобразится в матрицу, имеющую вид

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & \pm 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \pm 1 \end{pmatrix}$$

в базисе, в котором вид матриц системы $\mathcal{MJ}$ не изменится.

Доказательство. Обозначим образ $\Phi(\sigma_{12}) = (d_{ij})$.

Так как σ_{12} удовлетворяет трем следующим соотношениям:

$$\text{для } k = 3, \dots, n \quad (\sigma_{12} I_k = I_k \sigma_{12}), \quad (4.1)$$

$$\sigma_{12}^2 = E, \quad (4.2)$$

$$\sigma_{12} I_1 \sigma_{12} = I_2, \quad (4.3)$$

то аналогичные соотношения выполнены и для образов.

Из первого соотношения следует, что

$$\Phi(\sigma_{12}) = \begin{pmatrix} d_{11} & d_{12} & 0 & \dots & 0 \\ d_{21} & d_{22} & 0 & \dots & 0 \\ 0 & 0 & d_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & d_{nn} \end{pmatrix},$$

причем с учетом второго соотношения $d_{kk} = \pm 1$ для $3 \leq k \leq n$.

Выпишем подробно второе и третье (с точностью до умножения обеих частей равенства на $-E$) соотношения для угловых блоков:

$$\begin{aligned} \begin{pmatrix} d_{11}^2 + d_{12}d_{21} & d_{11}d_{12} + d_{12}d_{22} \\ d_{21}d_{11} + d_{22}d_{21} & d_{21}d_{12} + d_{22}^2 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\ \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix} &= \\ = \begin{pmatrix} -d_{11}^2 + d_{12}d_{21} & -d_{11}d_{12} + d_{12}d_{22} \\ -d_{21}d_{11} + d_{22}d_{21} & -d_{21}d_{12} + d_{22}^2 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned}$$

Складывая элементы, стоящие на местах $(1, 1)$, и вычитая элементы на местах $(2, 2)$ в равенствах выше, получим: $2d_{12}d_{21} = 2$ и $2d_{21}d_{12} = 2$,

значит $d_{12} = \alpha$, $d_{21} = 1/\alpha$, где α — некоторый обратимый элемент кольца R_2 .

Сложив элементы на местах $(1, 2)$, видим, что $2d_{12}d_{22} = 0$. Элемент $2d_{12}$ обратим, следовательно, $d_{22} = 0$, аналогично получается и $d_{11} = 0$.

Теперь сделаем замену базиса, порожденную обратимой матрицей

$$\text{diag}[1/\alpha, 1, \dots, 1],$$

которая коммутирует со всеми матрицами из $\mathcal{MJ}$, тем самым получим требуемый вид для $\Phi(\sigma_{12})$. $\square$

Следствие 3. Пусть R_1 и R_2 — бесконечные локальные кольца с $1/2$, и известно, что $\text{GL}_n(R_1) \equiv_{\forall} \text{GL}_n(R_2)$ ($n > 2$). Пусть также M_1 — произвольная конечная частичная модель $\text{GL}_n(R_1)$, содержащая множество $\mathcal{MJ}$ и сопрягающие его элементы матрицы, а M_2 — конечная частичная модель $\text{GL}_n(R_2)$, изоморфная M_1 .

Тогда при любом изоморфизме

$$\Phi: M_1 \rightarrow M_2$$

матрица $\sigma_{23} = E - E_{22} - E_{33} + E_{23} + E_{32}$ отобразится в матрицу, имеющую вид

$$\begin{pmatrix} \pm 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \pm 1 & & \\ \vdots & \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & & & \pm 1 \end{pmatrix}$$

в базисе, в котором вид матриц системы $\mathcal{MJ}$ не изменится.

Доказательство. Аналогично доказательству предыдущей леммы, можно показать, что

$$\Phi(\sigma_{23}) = \begin{pmatrix} \pm 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \beta & 0 & \dots & 0 \\ 0 & \frac{1}{\beta} & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \pm 1 & & \\ \vdots & \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & & & \pm 1 \end{pmatrix},$$

где β — обратимый элемент кольца R_2 . Осталось сделать замену базиса, порожденную матрицей $\text{diag}[1, 1, \beta, 1, \dots, 1]$, коммутирующей со всеми матрицами из множества $\mathcal{MJ}$ и с σ_{12} . $\square$

4.2.3 Матрица $E + E_{12}$: общая часть

Лемма 39. Пусть R_1 и R_2 — бесконечные локальные кольца с $1/2$, и известно, что $\mathrm{GL}_n(R_1) \equiv_{\forall} \mathrm{GL}_n(R_2)$ ($n > 2$). И пусть M_1 — произвольная конечная частичная модель $\mathrm{GL}_n(R_1)$, содержащая конечный набор матриц из предыдущей леммы и следствия, а также $\mathrm{diag}[2, 1, 1/2, 1, \dots, 1]$, а M_2 — конечная частичная модель $\mathrm{GL}_n(R_2)$, изоморфная M_1 . Тогда при любом изоморфизме

$$\Phi: M_1 \rightarrow M_2$$

матрица $E + E_{12}$ переходит в матрицу вида $E + E_{12}$ или $E - E_{21}$ в базисе, в котором вид матриц системы $\mathcal{MJ}$, σ_{12} и σ_{23} не изменится, или в базисе, который отличается от предыдущего базиса сопряжением матрицей $\mathrm{diag}[-1, 1, -1, 1, \dots, 1]$.

Доказательство. Как и в доказательстве леммы 38,

$$\Phi(E + E_{12}) = \begin{pmatrix} t_{11} & t_{12} & 0 & \dots & 0 \\ t_{21} & t_{22} & 0 & \dots & 0 \\ 0 & 0 & t_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & t_{nn} \end{pmatrix}.$$

Так как $D = \mathrm{diag}[2, 1, 1/2, 1, \dots, 1]$ коммутирует со всеми матрицами из $\mathcal{MJ}$, то $\Phi(\mathrm{diag}[2, 1, 1/2, 1, \dots, 1]) = \mathrm{diag}[\alpha_1, \dots, \alpha_n]$, где все α_i обратимы.

Выпишем все необходимые для дальнейшего доказательства соотношения, которые выполняются в M_1 (аналогичные соотношения будут выполнены и для образов изоморфизма в M_2):

$$D(E + E_{12})D^{-1} = (E + E_{12})^2, \quad (4.4)$$

$$(I_2(E + E_{12}))^2 = E, \quad (4.5)$$

$$((I_2\sigma_{12})(E + E_{12}))^3 = E, \quad (4.6)$$

$$(I_3\sigma_{23})(E + E_{12})(I_3\sigma_{23})^{-1} \text{ коммутирует с } E + E_{12}. \quad (4.7)$$

Заметим, что из соотношения (4.5) следует, что для элементов на диагонали выполнено $t_{kk}^2 = 1$ (для $k = 3, \dots, n$), значит $t_{kk} = \pm 1$, по лемме 37, и, в частности, являются центральными элементами кольца.

Тогда из соотношения (4.4) получаем: $\alpha_k t_{kk} \alpha_k^{-1} = t_{kk} = t_{kk}^2 = 1$ при $k = 3, \dots, n$.

Сначала рассмотрим случай, когда образ I_2 содержит ровно одну минус единицу на диагонали. В этом случае образ I_3 также содержит ровно

одну минус единицу. Тогда из соотношения (4.6) следует, что на диагонали у образа σ_{12} начиная с третьего места стоят единицы. Далее, из соотношения $(\sigma_{12}\sigma_{23})^3 = E$ следует, что на диагонали у образа σ_{23} на всех местах, кроме второго и третьего, стоят единицы.

Теперь запишем соотношения (4.4) – (4.7) для угловых блоков:

$$\begin{pmatrix} t_{11}^2 + t_{12}t_{21} & t_{11}t_{12} + t_{12}t_{22} \\ t_{21}t_{11} + t_{22}t_{21} & t_{21}t_{12} + t_{22}^2 \end{pmatrix} = \begin{pmatrix} \alpha_1 t_{11} \alpha_1^{-1} & \alpha_1 t_{12} \alpha_2^{-1} \\ \alpha_2 t_{21} \alpha_1^{-1} & \alpha_2 t_{22} \alpha_2^{-1} \end{pmatrix}, \quad (4.8)$$

$$\begin{pmatrix} t_{11}^2 - t_{12}t_{21} & t_{11}t_{12} - t_{12}t_{22} \\ -t_{21}t_{11} + t_{22}t_{21} & -t_{21}t_{12} + t_{22}^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (4.9)$$

$$\begin{pmatrix} t_{21}^3 - t_{22}t_{11}t_{21} - t_{21}t_{22}t_{11} + t_{22}t_{12}t_{11} & t_{21}^2t_{22} - t_{22}t_{11}t_{22} - t_{21}t_{22}t_{12} + t_{22}t_{12}^2 \\ -t_{11}t_{21}^2 + t_{12}t_{11}t_{21} + t_{11}t_{22}t_{11} - t_{12}^2t_{11} & -t_{11}t_{21}t_{22} + t_{12}t_{11}t_{22} + t_{11}t_{22}t_{12} - t_{12}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (4.10)$$

$$\begin{pmatrix} t_{11}^2 & t_{11}t_{12} & t_{12} \\ t_{21} & t_{22} & 0 \\ t_{21}t_{11} & t_{21}t_{12} & t_{22} \end{pmatrix} = \begin{pmatrix} t_{11}^2 & t_{12} & t_{11}t_{12} \\ t_{21}t_{11} & t_{22} & t_{21}t_{12} \\ t_{21} & 0 & t_{22} \end{pmatrix}. \quad (4.11)$$

Из (4.11) видим, что $t_{21}t_{12} = 0$, подставим в (4.9) на место (2, 2) и получим, что $t_{22}^2 = 1$, значит $t_{22} = \pm 1$ — элемент центра кольца R_2 . Теперь из элемента на месте (2, 2) в соотношении (4.8) получаем: $t_{22}^2 = \alpha_2 t_{22} \alpha_2^{-1} = t_{22}$, значит $t_{22} = 1$.

Рассмотрим два случая: 1) t_{12} обратим, 2) t_{11} обратим (хотя бы одно из этих условий выполняется, так как $\Phi(E + E_{12})$ — обратимый элемент, а кольцо локально).

1 случай: t_{12} обратим.

Снова обратимся к (4.9), на месте (1, 2) получаем равенство $(t_{11} - 1)t_{12} = 0$, значит $t_{11} = 1$. Тогда на месте (1, 1) в (4.8) выполнено равенство $1 + t_{12}t_{21} = 1$, следовательно, $t_{21} = 0$.

Чтобы доказать, что в этом случае $t_{12} = 1$, обратимся к соотношению (4.10), в котором на месте (1, 1) стоит $1 = t_{21}^3 - t_{22}t_{11}t_{21} - t_{21}t_{22}t_{11} + t_{22}t_{12}t_{11} = t_{12}$.

2 случай: t_{11} обратим. Подставим $t_{22} = 1$ и $t_{21}t_{12} = 0$ на место (1, 2) в соотношении (4.10):

$$t_{21}^2t_{22} - t_{22}t_{11}t_{22} - t_{21}t_{22}t_{12} + t_{22}t_{12}^2 = t_{21}^2 - t_{11} + t_{12}^2 = 0,$$

так как t_{11} обратим, то из равенства $t_{21}^2 + t_{12}^2 = t_{11}$ следует, что хотя бы один из элементов t_{12}, t_{21} обратим. Если t_{12} обратим, то все доказано выше. Пусть теперь t_{21} обратим. Тогда из равенства (4.11) следует, что

$t_{11} = 1$ и $t_{12} = 0$ (места $(3, 1)$ и $(3, 2)$ соответственно). Найдём t_{21} . На местах $(1,1)$ и $(1,2)$ в (4.10) выполнены равенства

$$t_{21}^3 - 2t_{21} = 1, \quad -t_{21}^2 + 1 = 0,$$

откуда находим $t_{21} = -1$.

Теперь рассмотрим случай, когда образ I_2 содержит ровно одну единицу на диагонали. В этом случае образ I_3 также содержит ровно одну единицу. Тогда из соотношения (4.6) следует, что на диагонали у образа σ_{12} начиная с третьего места стоят минус единицы. Далее, из соотношения $(\sigma_{12}\sigma_{23})^3 = E$ следует, что на диагонали у образа σ_{23} на всех местах, кроме второго и третьего, стоят минус единицы. В этом случае сначала сделаем замену базиса, порожденную матрицей $\text{diag}[-1, 1, -1, 1, \dots, 1]$. Она коммутирует со всеми диагональными инволюциями, поэтому их вид не изменится. А угловые блоки образов матриц σ_{12} и σ_{23} примут вид:

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

соответственно. При этом условия (4.8) – (4.11) не изменятся, поэтому и в этом случае образ $E + E_{12}$ имеет заявленный вид. $\square$

Далее разобьём доказательство на два случая:

1) $\Phi(E + E_{12}) = E + E_{12}$

или

2) $\Phi(E + E_{12}) = E - E_{21}$

в базисе, в котором вид матриц системы $\mathcal{MJ}$, σ_{12} и σ_{23} не изменится.

4.2.4 Случай 1: $\Phi(E + E_{12}) = E + E_{12}$

Лемма 40. Пусть R_1 и R_2 — бесконечные локальные кольца с $1/2$, и известно, что $\text{GL}_n(R_1) \equiv_{\forall} \text{GL}_n(R_2)$. И пусть M_1 — произвольная конечная частичная модель $\text{GL}_n(R_1)$, содержащая конечный набор матриц из предыдущих лемм и матрицу $\text{diag}[2, 1, 1/2, 1, \dots, 1]$, а M_2 — конечная частичная модель $\text{GL}_n(R_2)$, изоморфная M_1 . Тогда при любом частичном изоморфизме

$$\Phi: M_1 \rightarrow M_2,$$

при котором $\Phi(E + E_{12}) = E + E_{12}$, любой конечный набор матриц вида $E + \alpha_i E_{12}$, $i = 1, \dots, k$ переходит в набор матриц вида $E + \beta_i E_{12}$,

$i = 1, \dots, k$, в базисе, в котором вид матриц из предыдущих лемм не изменится.

Доказательство. Как в лемме 39 (используя перестановочность с матрицами $I_3, \dots, I_n$ и соотношения, аналогичные (4.4) и (4.5)), легко показать, что

$$\Phi(E + \alpha_i E_{12}) = \begin{pmatrix} s_{11}^i & s_{12}^i & 0 \\ s_{21}^i & s_{22}^i & 0 \\ 0 & 0 & E \end{pmatrix}.$$

Далее из перестановочности матриц $E + E_{12}$ и $E + \alpha_i E_{12}$ получим, что $s_{11}^i = s_{22}^i$ и $s_{21}^i = 0$.

Осталось показать, что на диагонали на первых двух местах единицы. Распишем соотношения с диагональной матрицей для углового блока, учитывая, что $\Phi(\text{diag}[2, 1, 1/2, 1, \dots, 1]) = \text{diag}[d_1, \dots, d_n]$:

$$\begin{pmatrix} d_1 s_{11}^i d_1^{-1} & d_1 s_{12}^i d_2^{-1} \\ 0 & d_2 s_{11}^i d_2^{-1} \end{pmatrix} = \begin{pmatrix} (s_{11}^i)^2 & s_{11}^i s_{12}^i + s_{12}^i s_{11}^i \\ 0 & (s_{11}^i)^2 \end{pmatrix}.$$

Также заметим, что $(I_2(E + \alpha_i E_{12}))^2 = E$, поэтому для образов выполнено соотношение:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} s_{11}^i & s_{12}^i \\ 0 & -s_{11}^i \end{pmatrix}^2 = \begin{pmatrix} (s_{11}^i)^2 & s_{11}^i s_{12}^i - s_{12}^i s_{11}^i \\ 0 & (s_{11}^i)^2 \end{pmatrix}$$

или

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -s_{11}^i & -s_{12}^i \\ 0 & s_{11}^i \end{pmatrix}^2 = \begin{pmatrix} (s_{11}^i)^2 & s_{11}^i s_{12}^i - s_{12}^i s_{11}^i \\ 0 & (s_{11}^i)^2 \end{pmatrix}.$$

Из записанных равенств следует, что $s_{11}^i = \pm 1$ — центральный элемент, значит $1 = (s_{11}^i)^2 = d_1 s_{11}^i d_1^{-1} = s_{11}^i$. $\square$

Сделаем некоторые замечания о связи операций над элементами локального кольца R и операций над элементами группы $\text{GL}_n(R)$. Во-первых,

$$(E + \alpha E_{12})(E + \beta E_{12}) = E + (\alpha + \beta)E_{12}, \quad (4.12)$$

а во-вторых,

$$[E + \alpha E_{12}, E + \beta E_{23}] = E + \alpha\beta E_{13},$$

причем

$$E + \alpha E_{23} = \sigma_{12}\sigma_{23}(E + \alpha E_{12})\sigma_{23}\sigma_{12}, \quad (4.13)$$

$$E + \alpha E_{13} = [E + E_{12}, E + \alpha E_{23}]. \quad (4.14)$$

Теперь основное утверждение будет следовать из предыдущих лемм, аналогично тому, как это получается в главе 3. Более подробно, пусть $S_1 \subset R_1$ — некоторая конечная частичная модель кольца R_1 . Наша задача — найти для нее изоморфную ей частичную модель S_2 в кольце R_2 . Пусть $M_1 \subset \text{GL}_n(R_1)$ — конечная частичная модель, содержащая все матрицы вида $E + \alpha E_{12}$ для всех $\alpha \in S_1$, а также конечное число вспомогательных матриц из предыдущих лемм. Так как группы универсально эквивалентны, то для частичной модели M_1 существует изоморфная частичная модель $M_2 \subset \text{GL}_n(R_2)$, причем любой изоморфизм $\Phi: M_1 \rightarrow M_2$ сохраняет вид матриц. Поэтому образы матриц $E + \alpha E_{12}, E + \alpha E_{13}, E + \alpha E_{23}$ будут в некотором общем базисе иметь вид $E + \beta_1 E_{12}, E + \beta_2 E_{13}, E + \beta_3 E_{23}$, причем $\beta_1 = \beta_2 = \beta_3 \in R_2$. Тогда S_2 — множество всех элементов кольца R_2 , которые соответствуют тройкам образов матриц $E + \alpha E_{12}, E + \alpha E_{13}, E + \alpha E_{23}$ для всех элементов $\alpha \in S_1$.

4.2.5 Случай 2: $\Phi(E + E_{12}) = E - E_{21}$

Лемма 41. Пусть R_1 и R_2 — бесконечные локальные кольца с $1/2$, и известно, что $\text{GL}_n(R_1) \equiv_{\forall} \text{GL}_n(R_2)$. И пусть M_1 — произвольная конечная частичная модель $\text{GL}_n(R_1)$, содержащая конечный набор матриц из предыдущих лемм и матрицу $\text{diag}[2, 1, 1/2, 1, \dots, 1]$, а M_2 — конечная частичная модель $\text{GL}_n(R_2)$, изоморфная M_1 . Тогда при любом изоморфизме

$$\Phi: M_1 \rightarrow M_2,$$

при котором $\Phi(E + E_{12}) = E - E_{21}$, любой конечный набор матриц вида $E + \alpha_i E_{12}$, $i = 1, \dots, k$ переходит в набор матриц вида $E + \beta_i E_{21}$, $i = 1, \dots, k$, в базисе, в котором вид матриц из предыдущих лемм не изменится.

Доказательство. Аналогично доказательству леммы 39, легко показать, что

$$\Phi(E + \alpha_i E_{12}) = \begin{pmatrix} s_{11}^i & s_{12}^i & 0 \\ s_{21}^i & s_{22}^i & 0 \\ 0 & 0 & E \end{pmatrix}.$$

Далее из перестановочности матриц $E + E_{12}$ и $E + \alpha_i E_{12}$ получим, что $s_{11}^i = s_{22}^i$ и $s_{12}^i = 0$.

Осталось показать, что на диагонали на первых двух местах единицы. Распишем соотношения с диагональной матрицей для углового блока, учитывая, что $\Phi(\text{diag}[2, 1, 1/2, 1, \dots, 1]) = \text{diag}[d_1, \dots, d_n]$:

$$\begin{pmatrix} d_1 s_{11}^i d_1^{-1} & 0 \\ d_2 s_{21}^i d_1^{-1} & d_2 s_{11}^i d_2^{-1} \end{pmatrix} = \begin{pmatrix} (s_{11}^i)^2 & 0 \\ s_{21}^i s_{11}^i + s_{11}^i s_{21}^i & (s_{11}^i)^2 \end{pmatrix}.$$

Также заметим, что $(I_2(E + \alpha_i E_{12}))^2 = E$, поэтому для образов выполнено соотношение:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} s_{11}^i & 0 \\ -s_{21}^i & -s_{11}^i \end{pmatrix}^2 = \begin{pmatrix} (s_{11}^i)^2 & 0 \\ -s_{21}^i s_{11}^i + s_{11}^i s_{21}^i & (s_{11}^i)^2 \end{pmatrix}$$

или

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -s_{11}^i & 0 \\ s_{21}^i & s_{11}^i \end{pmatrix}^2 = \begin{pmatrix} (s_{11}^i)^2 & 0 \\ -s_{21}^i s_{11}^i + s_{11}^i s_{21}^i & (s_{11}^i)^2 \end{pmatrix}.$$

Из записанных равенств следует, что $s_{11}^i = \pm 1$ — центральный элемент, значит $1 = (s_{11}^i)^2 = d_1 s_{11}^i d_1^{-1} = s_{11}^i$. $\square$

4.2.6 Соответствия, завершающие доказательство

Теперь опишем соответствие между элементами группы $\text{GL}_n(R)$ и кольца R , которое мы используем для завершения доказательства. Как и в первом случае, будем использовать соотношение (4.12), которое для образов Φ примет вид

$$(E - \alpha E_{21})(E - \beta E_{21}) = E - (\alpha + \beta)E_{21}.$$

Далее, согласно равенству (4.13), образ матрицы $E + E_{23}$ равен

$$\sigma_{12}\sigma_{23}(E - E_{21})\sigma_{23}\sigma_{12} = E - E_{32},$$

а матрицы $E + \alpha E_{23}$ —

$$\sigma_{12}\sigma_{23}(E + \beta E_{21})\sigma_{23}\sigma_{12} = E + \beta E_{32}.$$

Для коммутатора из равенства (4.14) получим

$$[E - E_{21}, E + \alpha E_{32}] = E + \alpha E_{31}.$$

Пусть теперь $S_1 \subset R_1$ — некоторая конечная частичная модель кольца R_1 и пусть $M_1 \subset \text{GL}_n(R_1)$ — конечная частичная модель, содержащая все матрицы вида $E + \alpha E_{12}$ для всех $\alpha \in S_1$, а также конечное число вспомогательных матриц из предыдущих лемм. Так как группы универсально эквивалентны, то для частичной модели M_1 существует изоморфная

частичная модель $M_2 \subset \text{GL}_n(R_2)$. Здесь мы также дополнительно предполагаем, что изоморфизм $\Phi: M_1 \rightarrow M_2$ переводит матрицу $E + E_{12}$ в $E - E_{21}$. Поэтому образы матриц $E + \alpha E_{12}, E + \alpha E_{13}, E + \alpha E_{23}$ будут в некотором общем базисе иметь вид $E - \beta E_{21}, E - \beta E_{31}, E - \beta E_{32}$. Тогда S_2 — множество всех элементов кольца R_2 , которые соответствуют тройкам образов матриц $E + \alpha E_{12}, E + \alpha E_{13}, E + \alpha E_{23}$ для всех элементов $\alpha \in S_1$. Причем произведение матриц вида $E + \alpha E_{12}$ и их образов, как и в первом случае, соответствует сложению элементов кольца, а коммутатор теперь дает

$$[E - \alpha E_{21}, E - \beta E_{32}] = E - \beta \alpha E_{31},$$

что соответствует умножению в кольце R_2^{op} .

Заключение

В данной диссертации была достигнута основная цель — построение критерия универсальной эквивалентности линейных групп. В процессе работы удалось решить все поставленные задачи, сформулировать и доказать критерий универсальной эквивалентности для полных и специальных линейных групп над произвольными полями и коммутативными локальными кольцами с $1/2$, а также для полных линейных групп над (не обязательно коммутативными) локальными кольцами с $1/2$.

Часть результатов (при наличии обратимой двойки) удалось получить методом инволюций, для других потребовалось использовать дополнительные методы. В случае локальных некоммутативных колец также потребовалось расширить формулировку результата, чтобы учесть возникающее в этом случае противоположное кольцо.

Полученные результаты расширяют знания об универсальной эквивалентности и могут стать основой для новых исследований. Естественным образом ставится вопрос об обобщении полученного результата на более широкий класс групп и колец. Также полезно исследовать, какие приложения существуют у построенного при доказательстве соответствия между линейными группами и кольцами. Отдельно хочется отметить такую задачу: описать все группы, универсально эквивалентные $GL_n(K)$.

Литература

- [1] Avni N., Lubotzky A., Meiri C. First order rigidity of non-uniform higher-rank arithmetic groups // *Inventiones mathematicae*. — 2019. — Vol. 217, № 1. — P. 219–240.
- [2] Beidar C. I., Mikhalev A. V. On Mal'cev's theorem on elementary equivalence of linear groups. Proceedings of the International Conference on Algebra // *Contemporary Mathematics*. — 1992. — Vol. 131, part 1. — P. 29–35.
- [3] Duncan A. J., Kazatchkov I. V., Remeslennikov V. N. Centraliser dimension and universal classes of groups // *Сибирские электронные математические известия*. — 2006. — Vol. 3. — P. 197–215.
- [4] Eklof P. C. Some model theory for Abelian groups // *Journal of Symbolic Logic*. — 1972. — Vol. 37, № 2. — P. 335–342.
- [5] Lam T. Y. *A First Course in Noncommutative Rings*. — Springer, 1991.
- [6] Lam T. Y. *Lectures on Modules and Rings*. — Springer, 1998.
- [7] Mishchenko A. A., Timoshenko E. I. Universal equivalence of partially commutative nilpotent groups // *Siberian Mathematical Journal*. — 2011. — Vol. 52, № 5. — P. 884–891.
- [8] Myasnikov A., Sohrabi M. Bi-interpretability with $\mathbb{Z}$ and models of the complete elementary theories of $SL_n(\mathcal{O})$, $T_n(\mathcal{O})$ and $GL_n(\mathcal{O})$, $n \geq 3$ // arXiv:2004.03585. — 2020. — 19 pp.
- [9] Poroshenko E. N., Timoshenko E. I. Universal equivalence of partially commutative metabelian Lie algebras // *Journal of Algebra*. — 2013. — Vol. 384. — P. 143–168.
- [10] Segal D., Tent K. Defining R and $G(R)$ // *Journal of the European Mathematical Society*. — 2023. — Vol. 25, № 8. — P. 3325–3358.

- [11] Аткарская А. С., Бунина Е. И., Михалев А. В. Изоморфизмы общих линейных групп над ассоциативными кольцами, градуированными абелевой группой // *Фундаментальная и прикладная математика*. — 2010. — Т. 16, № 3. — С. 5–40.
- [12] Атья М., Макдональд И. Введение в коммутативную алгебру. — М.: Мир, 1972.
- [13] Брагин В. А., Бунина Е. И. Элементарная эквивалентность линейных групп над кольцами с конечным числом центральных идемпотентов и булевыми кольцами // *Фундаментальная и прикладная математика*. — 2013. — Т. 18, № 1. — С. 45–55.
- [14] Бунина Е. И. Автоморфизмы групп Шевалле типов A_l, D_l, E_l над локальными кольцами с необратимой двойкой // *Фундаментальная и прикладная математика*. — 2009. — Т. 15, № 7. — С. 47–80.
- [15] Бунина Е. И. Изоморфизмы и элементарная эквивалентность групп Шевалле над коммутативными кольцами // *Математический сборник*. — 2019. — Т. 210, № 8. — С. 3–28.
- [16] Бунина Е. И. Применение метода локализации для описания автоморфизмов линейных групп над коммутативными кольцами: конспекты спецкурса. — 2010. — 58 с. — URL: <http://halgebra.math.msu.su/wiki/lib/exe/fetch.php/specialcourses:speckurs10.pdf> (дата обращения: 12.08.2026).
- [17] Голубчик И. З., Михалев А. В. Изоморфизмы полной линейной группы над ассоциативным кольцом // *Вестник Московского университета. Серия 1: Математика. Механика*. — 1983. — Вып. 3. — С. 61–72.
- [18] Гуревич Ю. Ш., Кокорин А. И. Универсальная эквивалентность упорядоченных абелевых групп // *Алгебра и логика*. — 1963. — Т. 2, № 1. — С. 37–39.
- [19] Кейслер Г., Чэн Ч. Ч. Теория моделей. — М.: Мир, 1977.
- [20] Мальцев А. И. Об элементарных свойствах линейных групп // *Некоторые проблемы математики и механики*. — Новосибирск, 1961. — С. 110–132.
- [21] О’Мира О. Лекции о линейных группах // *Аutomорфизмы классических групп*. — М.: Мир, 1976. — С. 57–167.

- [22] Помфрэ Ж., Макдональд Б. Автоморфизмы группы GL_n над локальным кольцом // Автоморфизмы классических групп. — М.: Мир, 1976. — С. 176–187.
- [23] Тайманов А. Д. Характеристики аксиоматизируемых классов моделей // Алгебра и логика. Семинар. — 1962. — Т. 1, № 4. — С. 5–31.
- [24] Тимошенко Е. И. Об универсально эквивалентных разрешимых группах // Алгебра и логика. — 2000. — Т. 39, № 2. — С. 227–240.
- [25] Хисамиев Н. Г. Универсальная теория структурно упорядоченных абелевых групп // Алгебра и логика. — 1966. — Т. 5, № 3. — С. 71–76.

Публикации автора по теме диссертации

Статьи в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5 «Математическая логика, алгебра, теория чисел и дискретная математика»

- [26] Бунина Е. И., Калеева Г. А. Универсальная эквивалентность общих и специальных линейных групп над полями // Фундаментальная и прикладная математика. — 2016. — Т. 21, № 3. — С. 73–106.
EDN: BUOZFJ. Импакт-фактор: 0,1 (SJR). Объем: 3,93 п.л./ авторский вклад: 1,97 п.л.
- [27] Калеева Г. А. Универсальная эквивалентность линейных групп над локальными коммутативными кольцами с $1/2$ // Алгебра и логика. — 2019. — Т. 58, № 4. — С. 467–478.
EDN: IFALNG. Импакт-фактор: 0,196 (РИНЦ). Объем: 1,39 п.л.
- [28] Калеева Г. А. Универсальная эквивалентность полных линейных групп над локальными кольцами с $1/2$ // Математический сборник. — 2025. — Т. 216, № 10. — С. 29–41.
EDN: USRTEW. Импакт-фактор: 0,845 (РИНЦ). Объем: 1,5 п.л.